



FREE
eBook

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

1500+ VA/PT Tools

200+ References

Pro-tips

1000+ Job aids & KB

Discord goodies!

50+ List of BoK

Bonus Chapters

SHAHAB AL YAMIN CHAUDHURY
MSc | Enterprise Architect
4th April 2024, Version: 6.2

This Book is Dedicated to:

My Daughter - Airah

Who understands me as she shares the same flair.

I am grateful to the people who spent their life's time to post KB articles and their tireless efforts are acknowledged rarely, and those who supported me from my forum and my cybersecurity career and made this book possible. My wife has been my constant source of patience and encouragement, and without her, I could not have reached millions of people around the world with my work. My technology forum, and the people I have mentored have inspired me with their messages of gratitude and their passion for cybersecurity. Different organizations challenged me to overcome my self-doubt and achieve my goals. As you read this book and grow and enrich your cybersecurity career, I hope you will also appreciate the people who help you along the way and lend a hand back to help others with their journey.

- Shahab Al Yamin Chawdhury

BUILD YOUR OWN SECURITY OPERATION CENTER © 2024 by SHAHAB AL YAMIN CHAWDHURY | This study is licensed under [Attribution-NonCommercial-ShareAlike 4.0 International](#)



CC BY-NC-SA 4.0 DEED

Attribution-NonCommercial-ShareAlike 4.0 International

Disclaimer

The information in this book is for general informational purposes only and is not intended as professional advice. The author and/or publisher make no representations or warranties, guarantees regarding the accuracy or completeness of the information provided and will not be held liable for any errors or omissions.

The strategies and tactics discussed in this book may not be suitable for every individual or brand or organization, and readers should seek professional advice before designing & implementing them. The author and publisher are not responsible for any negative effects that may occur as a result of using the information provided in this book.

Any opinions expressed in this document are those of the author and do not necessarily reflect the official policy or position of any agency or organization or registered & copyright owners. The author and owner of this document are not responsible for any actions taken in reliance on the information provided in this post and readers should seek professional advice before taking any actions.

Please contact the author in LinkedIn if any attribution is missing.



Get in Touch

Feedback from you is always welcome. The final release of the book version is v6.2.

General feedback: If you have questions about any aspect of this book, connect with me on LinkedIn and send me your message.

Errata: Although I have tried to take every care to ensure the accuracy of the book's content, mistakes always tend to happen. If you have found a mistake in this book, I would be grateful if you would report this to me. I would like to correct any error that cannot be in the book in the upcoming versions.

Share Your Thoughts: I would appreciate your feedback on to book "*Build Your Own Security Operation Center*", Please use LinkedIn to leave your comment or anything that you would like to include in this book in the future. Your opinion matters to me and I would like to enrich this book as much as possible within my capacity, which will help the community even further.



Reviewer Note by Brad Voris

This book stands as a beacon of knowledge for security enthusiasts, seamlessly weaving together insights from diverse online sources into a comprehensive resource. Shahab's commitment to acknowledging and respecting the ownership rights of original content creators while providing invaluable insights is commendable. With a focus on key perspectives including SOC operations, threat detection, incident response, and various security frameworks, it serves as a guiding light for navigating the complex landscape of cybersecurity. Emphasizing the importance of continuous improvement and proactive risk management, this book not only equips readers with essential knowledge but also inspires them to strive for operational excellence in safeguarding digital infrastructures. Its authenticity reflects a dedication to preserving the core meanings and functionalities while adapting to the evolving security landscape, making it an indispensable tool for security professionals striving to excel in their field.

Brad Voris, CISSP, CISM, CCSP, CCSK, is lead information security architect for Walmart. He has 25 years of experience in information technology, cyber security, and information security. As an author he's co-authored two books: *Intrusion Detection Guide* (Chapter 10: Compliance Frameworks), *Essentials of Cybersecurity* (Chapter 8: Understanding Central Areas of Enterprise Defense), and written numerous articles for Microsoft TechNet and LinkedIn. Brad also has an accomplished mentorship program, where he has mentored over one hundred security and technology professionals. Before his IT and security journey, Brad served in the U.S. Army. You can connect with Brad at LinkedIn at www.linkedin.com/in/brad-voris or www.victimoftechnology.com






Contents

- Preface 20
 - How to Use This Book 21
- 1. **Overview** 23
 - PPTD (People, Process, Technology, Data) 25
 - Software Deployment Roadmap – 3yrs Planning Tool 27
 - Why Enterprise Architecture 27
 - Business Goal Alignment to Technology 29
 - The Sad Story of Enterprise Architecture Formulation 30
- 2. **An Enterprise Architecture Strategy** 32
 - Azure Well Architected Frameworks 33
 - Example: E-Commerce Application 36
 - Partner Tools with Azure Monitor Integration 37
 - ASIM and the Open Source Security Events Metadata (OSSEM) 38
 - ASIM Components 38
 - Normalized Schemas 39
 - AWS Well Architected Frameworks 42
 - Example: E-Commerce Application 43
 - So How Do You Build a Rightly Sized Architecture? 44
 - Key System Design Fundamentals 45
 - The Service Integration Layer 51
 - Background 51
 - Key Components of the Service Integration Layer 51
 - API Gateway: 51
 - Message Broker: 51
 - Data Integration Hub: 52
 - Event Processing Engine: 52



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Workflow Orchestration:	52
Benefits of the Service Integration Layer	52
Improved Interoperability:	52
Enhanced Agility:	52
Optimized Resource Utilization:	52
Increased Scalability:	52
Streamlined Maintenance:	52
Implementation Strategies.....	53
Assessment of Current Infrastructure:.....	53
Selection of Integration Technologies:.....	53
Development of Integration Standards:	53
Security Measures:	53
Testing and Validation:.....	53
Case Studies	53
E-commerce Platform:	53
Healthcare System Integration:	53
Popular OMG.ORG Standards	54
Another Architecture Mapping (BPM)	54
Enterprise Architecture in Cybersecurity	57
Enterprise Security Risk Management	60
Knowledge Areas That Will Pay You for Life	61
C2, C4ISR & C4ISTAR.....	67
C4ISR Defense in Depth Core Function Descriptions	69
Predict attacks on an organization’s assets:	69
Prevent attacks on an organization’s assets:	69
Advanced tools and procedures:	70
Detect attacks on an organization’s assets:	70
Respond to attacks on an organization’s assets:	71

	3. SIEM & SOAR – Better Together	77
	What is SIEM?	78
	What is SOAR?	78
	How SIEM and SOAR Work Better Together.....	78
	SIEM & SOAR Architecture	79
	Importance of Required Applications in a Disaster Recovery Plan	82
	Hot, Cold and Warm Sites	84
	Some of The Disaster Recovery Application Platform	84
	Benefits of a Functional Security Operations Center (SOC)	85
	24/7 Staffing Requirements for the CSOC Monitoring	87
	So, You Want to be a CISO?.....	87
	Dunning-Kruger Effect – The Imposter Syndrome.....	91
	Attack Surface Management (ASM).....	92
	Implement Risk Based Vulnerability Management.....	93
	Cybersecurity Reference Architecture by Microsoft	94
	4. SOC Functions	97
	Open Security Architecture (OSA) Architecture Patterns	99
	SOC Methodology	102
	SOC – Capability Maturity Model (SOC-CMM).....	103
	Cybersecurity by Bill Ross	104
	NOC & SOC Visibility Requirement	105
	Integrated Intelligence for a Threat-informed Defense	110
	The Importance of Having a Data Scientist Team in Cyber Security Operation Center ..	113
	How Data Science Can Help Cyber Security	113
	Why Having a Data Scientist Team in SOC is Important	114
	Challenges of Having a Data Scientist Team in CSOC	115
	Data Scientist's Data Requirements From a SOC	115
	Common Data Science Methods and Techniques Used in SOC.....	116



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Limitations of Using Data Science in SOC	117
Ethical Considerations When Using Data Science in Cyber Security.....	118
Examples of Unethical Use of Data Science in Cyber Security.....	119
Does Offensive Security Mean to Attack the Attacker?.....	120
5. Foundational Information Security Principles	121
Network Segmentation – A 4-Step Approach.....	123
Cyber Resiliency Scoreboard® (CRS®).....	125
Threat Driven Modeling in SOC	126
Microsoft Threat Modeling Tool STRIDE.....	127
STRIDE Model	128
Web server:	129
Database server:.....	130
Browser:	131
Sunburst Visualization of STRIDE-LM to Security Controls	131
Threat Modeling: 12 Available Methods.....	132
Threat Modeling Using MITRE ATT&CK	134
Threat Modeling with MITRE ATT&CK Framework	134
Cyber Security Roadmap	147
EXAMPLE: Security Operations Center (SOC) in Practice	149
ISO/IEC 27001:2022 Control Requirements.....	149
6. Processes for a SOC	159
Documentation Framework for a Security Operation Center	162
Escalation Process.....	165
Incident Distribution	165
Investigation	166
Challenges for SOC Development.....	166
Cyber Resiliency Scoring and Metrics	167
CREF At-a-glance	171

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

	CREF Objectives (The Purple Column).....	171
	MITRE's CREF Navigator	172
	Cyber Resilience Framework (World Economic Forum & Accenture)	173
	Visibility Tuning.....	173
	Content Engineering.....	174
	How a SOC is Typically Operated.....	174
	Security Operations Mindmap	175
	SOC Workstation Security Requirements.....	176
	7. Processes for a SOC	177
	Cybersecurity Teams: Red, Blue & Purple.....	180
	Red Team Exercises are Typically Conducted in Three Phases	180
	Benefits of Red Teaming	181
	Top Red Team Frameworks: TIBER, AASE & CBEST.....	181
	A few challenges common in security teams include:.....	182
	Differences Between Red Teaming and Penetration Testing.....	183
	A Better Choice Between the In-house Red Team and Outsourced Red Team.....	183
	The Blue team's Objectives and Duties	185
	The Blue Team's Methods	185
	The Purple Team Model Has Three Levels of Maturity	186
	The Purple Team's Objectives and Duties Include.....	186
	Purple Team Exercises Usually Follow Four Steps.....	187
	Purple Team Exercise Tools.....	188
	Purple Team Tactics.....	189
	Steps for Building a Successful Purple Team.....	189
	8. Processes for a SOC	191
	How a Security Operations Center (SOC) Works in Practice.....	193
	Functions of the Sigma Rules in SOC	194
	Sigma Allows Defenders to Share Detections in a Common Language	196

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

EQL Analytics Library	196
SOC Capabilities Matrix – Gartner.....	197
SOC Roles & Responsibilities.....	198
A Cyber Security Analyst Maturity Curve.....	201
CMMC Maturity Model 2.0	201
Deriving Your Job Description or Resume	203
Security Triage in Cybersecurity	206
Importance of Triage in Incident Response	207
Security Triage Analysis Process	207
DevSecOps At A Glance	207
The Transition from a Siloed SOC to DevSecOps	208
Key Components of a DevSecOps Approach.....	209
Functions of a SOC Analyst (L1, L2, L3)	210
Functions of a Triage Specialist (Tier 1 Analyst), in a SOC	211
Functions of an Incident Responder (Tier 2 Analyst), in a SOC	213
Functions of A Threat Hunter (Tier 3 Analyst) in a SOC.....	214
Functions of a Cyber Threat Intelligence (CTI) Manager	215
Functions of a ‘SOC Manager’ in a SOC	216
Functions of a Security Architect in a SOC	217
9. Zero Trust Security	218
Benefits of The Principle of The Least Privileged (PoLP)	219
Functions of a SOC Compliance Auditor in a SOC	222
Knowledge Area (not an exhaustive list).....	223
Your 1-Stop Point for all Benchmark Checklists from CISECURITY	223
Malware Sandbox Tools for Analysis	233
Indicators of Compromise (IoC)	235
TTP (Tactics, Techniques, Procedures).....	236
Map of Attack Scenarios to TTP (Sample)	237

	Certification & Knowledge Mapping	238
	Security Career Roadmap	239
10. Incident Response		241
Incident Response Roles		244
Generic Incident Response Playbook		245
Prioritizing Log Sources		246
Windows Event Logs Artifact.....		247
Windows Reports – What to look for?		247
Common Windows Log Events Used in Security Investigations		248
Windows Events: Valuable, but Expensive		254
Registry Keys to Monitor		255
Which Are The Most Critical Linux Logs to Monitor?		257
Using Linux Event Logs for Security		257
Common Log Sources for Cloud Services		258
Determine the Best Log Data Sources		258
Logs to Avoid		259
Best Practices for MacOS Logging & Monitoring		259
Challenges of MacOS Logging		260
Choosing a MacOS Logging Method		260
Choose What to Monitor in MacOS		261
Logging Solution for MacOS.....		262
Common Ports Monitored by The SOC Analysts.....		262
Common Tools Used by SOC		265
Best Linux Distros for Cybersecurity		265
11. SOC Reference Architecture		268
Microsoft Reference Architecture for Security Operations		270
Raw Data and Classic SecOps.....		271
Automation (SOAR) and Integration.....		271

Microsoft Sentinel and SIEM Modernization	272
Demonstrating Privacy Accountability (NYMITY)	274
Penetration Testing ROI Template by risk3sixty	277
Automated Penetration Testing	277
12. Frameworks Used by SOC	281
The Famous Non-Controlling Body - NIST	284
Building an Effective Security Operations Center (SOC) Playbook	286
SOC Services, Playbooks and Responsibilities	288
Services:	288
Playbooks:	289
Responsibilities:	290
Designing Security Automation Playbooks	292
Security Automation	295
How SOC Handles an Ongoing Attack	295
13. Frameworks Used by SOC	297
Detection Maturity Level Model	299
Benefits of Detection Engineering	300
Detection Engineering vs Threat Hunting	301
Evasive Techniques	302
14. OSINT Tools and Their Usage	303
OSINT Framework	304
OSINT is Primary Used for Different Visibilities	305
Most Commonly Used OSINT's	305
15. SOC and CSIRT, Better Together	308
FIRST Services Framework – Typical CSIRT Services	310
Current Maturity Level	310
5 CSIRT Pillars	315
CSIRT Documentation Framework	315



	16. Digital Forensics and Incident Response (DFIR)	317
	Digital Forensic Mindmap	319
	Another Mindmap of DFIR.....	320
	How is Digital Forensics Used in the Incident Response Plan	320
	The Value of Integrated Digital Forensics and Incident Response (DFIR)	321
	Types of Forensics	321
	DFIR Timeline Generator	322
	CVE, CVSS, NVD, KEV	323
	17. Continuous Threat Exposure Management - CTEM	325
	How is CTEM Different from Cloud Security Posture Management (CSPM)?	326
	Readiness Requirements to Implement CTEM and CSPM	327
	Threat Intelligence Platform for SOC Security.....	328
	18. SOC Policies & Processes	330
	Cyber Security Domains	333
	Cybersecurity & Data Privacy by Design Principles	335
	Building a SOC by Rafeeq Rehman.....	336
	19. Generating and Consuming SOC Reports	338
	Case Documentation	340
	Difference Between TTP and IoC.....	341
	KPI's for a Security Operation Center	341
	Benefits of SOC KPI's	342
	Failure Metrics Timeline.....	348
	Defining Success for Your Ideal Reporting Model.....	348
	20. Cybersecurity Tabletop Exercises	350
	How to Prepare for Cybersecurity Tabletop Exercises	351
	How to Conduct Cybersecurity Tabletop Exercises.....	352
	Desired Results and Awareness	353
	Outcome of the Cybersecurity Tabletop Exercise	354





- 21. **Artificial Intelligence in Cybersecurity Operation Center** 358
 - Security Teams Need AI to Help Them Find Threats 359
 - Limitations of AI in SOC 360
 - Ensure the Transparency and Explainability of AI Outputs in SOC 361
 - Possibilities of Implementing AI in SOC 362
 - Challenges of Using AI in SOC 362
 - Common Pitfalls of AI Performance Optimization 363
 - Ensure the Fairness of the AI System 364
 - Examples of AI Bias and Discrimination in SOC 366
 - Algorithmic Debiasing 367
 - Mitigate the Risks of AI in SOC 367
 - Emerging Trends in AI Security 368
 - Examples of AI solutions for the SOC 369
 - Ethical Use of AI in SOC 371
 - Offensive AI Tools 371
 - Privacy and Confidentiality of Data Used by AI Systems 373
 - Legal and Regulatory Frameworks for AI Security 373
 - Measure ROI of AI in SOC 375
 - Optimize AI Performance for Better ROI 376
 - Can AI Replace Human Analysts in SOC? 377
- 22. **Open-Source SOC** 378
 - Designing the Open-source SOC 380
 - Wazuh and Associated Components Integrations 383
 - Create a New Detection Rule in CSOC 384
 - An Example of a Detection Rule 384
 - Custom rule creation in Snort 385
 - Testing Your Custom Rules to Ensure They Work as Expected 386
 - Generate a Detection Rule for APT-41 387



	The Network Design	388
	Back-office Network Design (1500 Users)	390
	Back-office Network Design (350K Users)	391
	VM List for Open-Source SOC Deployment	392
	Physical Server BoQ (DELL): 2 Servers Required	393
	Networking Device BoQ	396
	Fortinet Firewall BoQ	402
	23. BONUS-CHAPTER-1: Project Management	404
	Project Management by PMI Terms	405
	Project Charter	406
	Project WBS	413
	Virtual Machine Allocation Plan	413
	24. BONUS-CHAPTER-2: VA/PT Plan	415
	Plan Document	415
	Purpose	415
	Scope of the Project	416
	Description of VAPT Services	417
	Vulnerability Assessment and Penetration Testing	418
	Lifecycle of VAPT	418
	Vulnerability Assessment & penetration testing techniques	419
	Vulnerability Assessment technique	420
	Static analysis	420
	Manual Testing	420
	Automated Testing	420
	Fuzz Testing	420
	Penetration Testing Techniques	420
	Black Box Testing	420
	Grey Box Testing	421



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

White Box Testing.....	421
Vulnerability Assessment and Penetration Testing Tools.....	421
VA/PT As A Cyber Defense Technology.....	422
Conclusion and Future Work.....	423
Point of Contact.....	423
Project Manager Nomination.....	424
Computer Forensic & Cyber Security Tools, Open-Source).....	425
Disk Tools & Data Capture	425
Email Analysis.....	426
General Tools	426
File and Data Analysis	427
Mac OS Tools.....	428
Mobile Devices.....	429
Data Analysis Suites.....	429
File Viewers.....	430
Internet Analysis	431
Registry Analysis	432
Application Analysis.....	433
For Reference.....	434
Password Protection	434
Password Hacking Protection	434
Browsing Security.....	435
Redirect Checkers.....	435
Website URL Checkers	435
Data Removal.....	436
25. BONUS-CHAPTER-3: IT Service Strategy IT Service Strategy Planning.....	437
Process & Functions.....	438
IT Service Design –Modeling the IT Services.....	439

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

IT Service Transition - Implementing the IT Services	440
People	440
Process	440
Products	440
IT Service Operation – Managing the IT Services	440
People	441
Process	441
Products	441
IT Continual Service Improvement – Measuring the IT Services	441
People	441
Process	442
Products	442
Standardize the IT Service Desk	442
IT Governance & Management Principles	442
EIM Vision and Strategy	443
EIM Governance	443
EIM Core Processes	444
EIM Organization	444
EIM Infrastructure	444
Most Used Frameworks	445
COBIT Framework v5	445
COBIT 5 Process Reference Model	445
Common Service Desk Challenges	446
Ways That the Service Desk Handles Cybersecurity	447
26. BONUS-CHAPTER-4: Project Management	449
References	451
Body of Knowledge & Control Frameworks	461
Acronyms	464

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Preface

This is a collaged document (where data, pictures, illustrations are collected from the web, LinkedIn, different blog posts, web sites, official channels etc.), and from years of derived documents over the past 15yrs time, which is combined into one document to help security enthusiasts to enrich their knowledge, and provided as is without claiming any liability whatsoever. It's not a registered document, and all the respective license ownership has rights on their contents, writeups, illustrations. The baseline of this document consists of the following perspectives:

- Knowledge required to know what to do with your SOC.
- From threat detection to incident response.
- Processes & frameworks.
- Threat intelligence.
- Documentations.
- All about PPT.
- KPI for SOC.

As you know that what we are doing here is just to minimize exposure risks, identifying risks, and announcing the risks to the relevant stakeholders and in doing so, we are adopting to the following as well, gradually:

- Enterprise risk management.
- Engagement and training.
- Asset management.
- Architecture and configuration.
- Vulnerability management.
- Identity and access management.
- Data security.
- Logging and monitoring.
- Incident management.

And the outline is reflected below to provide an understanding of how to manage an enterprise grade infrastructure, what specific skillset is required to maintain a secured and networked services, how to maintain operational excellence as you are the true fighter each day and you are the one who are doing it whether an organization understands this or not, just your inner fire is something that fuels your efforts, and why not excel at what you do? Fine tuning all aspects of the security operations.

The definitions of the terms and their functions and procedures are kept as authentic as possible without changing the core meaning and functionality. You may find tonal changes, as this book was not collaged or developed by creative writers.

How to Use This Book

I started developing this document for my own use, but then I realized that it could be useful for my colleagues & peers as well, as it could enhance their knowledge, and I don't have to explain all the things to them 😊 which leaves me in an exhaustive state. However, there is so much information to share, that each topic could fill a book. The purpose of this book is to serve as a reference document that contains the main elements and sources for each topic, so that you can look for more details as needed, and it's in a searchable content, therefore, if you want to revisit this book, you can search for it and compose your own content as you see fit, by collaging multiple content into your document, by copying the requirements directly from this book and produce your own document. Also do remember that this document is not developed as a formal book that was not professionally developed. My personal views are heavily impacted my decisions for the development of SOC, how it was operated in the past, how it should be operated now as things have changed, who should report to which hierarchy, the line managers, the dotted reports and things of this sort.

It is almost impossible to document the entire SOC processes in terms of PPTD (people, process, technology and data), especially for technology. But this reference can be used as:

1. How to develop your own SOC (Security Operation Center) project, in a minimized form. Start simple and grow to become a complex one.
2. Develop your own SOC strategy; the governance program for a SOC.
3. Develop your own JD from the sources and from the reference links.
4. Content central for your SOC project.
5. Source reference of different points of views.
6. How to generate HW/SW requirements for your SOC.
7. Frameworks to adopt in a SOC.
8. Compliance requirements for SOC.
9. Documentations, workflows, metrics, policies, processes and procedures etc.
10. Lastly, you can use this document in part, in full as part of your documentation requirement as well to develop presentations, take the pictures from source links etc. (make sure you provide credit to the writers of their content, avoid plagiarism), as it is quite impossible to claim that everything is derived by a single person.

This document *does not provide*:

1. Insights of daily analysts' operation and its processes for
 - a. OSINT search & mapping.
 - b. Threat intelligence, hunting and its work methods.
 - c. Integration of hash functions, map threat category, framework mapping up to ticket generations for incident management .
 - d. VA & PT operations on devices or applications.
 - e. Daily SOC operation's tasks & activities carried out
 - f. Daily administrator's tasks (L1, L2, L3).
 - g. Security benchmark or checklists for networked devices, web, application configuration assessments.
 - h. Infrastructure assessment checklist based on Framework guidelines.

It is also assumed that the people can benefit from this, could be a fresher trying to break into the cybersecurity domain or could be a seasoned professional, either way, this book can help you out formulate your own, map out things that are required for documentational purpose, and most prominently, work activities must be in sync throughout the world, as we are all working towards the same goal, securing the enterprise, while exposing the full risk factors to the board, and minimize them gradually to an acceptable level. It is understood that not all enterprises pose same levels of complexity in their network infrastructure and not all of the enterprise requires a fully deployed SOC.

NOTE: The company names, their products mentioned here are being used at some point in deployments to client side, and therefore mentioned here for addressing their features and capabilities, not for monetary benefits and certainly is not promoting any partner products.

To keep the book to a minimized size, I did not explain everything where a human readable picture, mindmap or a workflow is present, which are self-explanatory, and larger resolution files are shared in the job aids. As you will realize, the bullet points are condensed to minimize the size of the book, the reason why the font (Roboto @10) is a bit heavy, though clear to read, is used.

Also, this book does not comply with APA formatting, styles & guidelines.



CHAPTER

1

Overview

PULL YOURSELF TOGETHER FOR THE FIRST STEP, YOU WILL NEVER KNOW WHAT'S OUT THERE FOR YOU IF YOU DON'T TAKE THE FIRST STEP, IT'S ALL IN YOUR HEAD!


The cybersecurity operations center (CSOC) is a vital entity within any enterprise structure. Its responsibilities are governed by the size of the enterprise, whether the enterprise is multinational, the enterprise's preference for centralized or decentralized cybersecurity management and operations, and whether the CSOC is in-house or outsourced. In addition, the CSOC mission and charter are highly correlated with how well the enterprise's executive team understands the intricacies of cybersecurity. C-cybersecurity, A-Advanced SOC is some of the SOC types, and we will be sticking to simply SOC, and will repeat throughout the book.

The CSOC is valuable because it combines and maximizes skilled resources, best practices, and technology solutions for the purpose of timely detection, real-time monitoring and correcting, and responding to cyberthreats to protect the organization's assets. In addition, the CSOC has the platform to collect the status of various incidents, infrastructure status and the effectiveness of the enterprise's defense preparedness




through the reporting of predesigned key performance indicator (KPI) metrics intended for various stakeholders. Many factors play a role in establishing and investing in a CSOC. According to a 2019 survey by the SANS Institute, the greatest challenges in establishing a service model for a CSOC are:

1. Lack of knowledge and available documentation and frameworks.
2. Lack of skilled staff.
3. Lack of automation and orchestration.
4. Too many tools that are not integrable.
5. Lack of management support.
6. Lack of processes or playbooks.
7. Lack of enterprise-wide visibility.
8. Too many alerts that we can't investigate (lack of correlation between alerts).
9. Non-compliance, depth of audit is not understood.
10. Unaware of insider threats: exposed code repo, code stolen, developer's laptops are not secured, can clone git, can run scans on their own network for resource mapping.
11. Unaware of external threats: bad network design, Public-IP exposure can cause hits into your laptops and your servers as well, servers are exposed to external networks, ACL's are not in place, faulty BGP announcements and authentications, NTP authentication is disabled and continuous sync cannot be established.
12. Unaware of advanced persistent threats (APTs) and zero days on all accords, not having knowledge on CVE's and not caring to patch accordingly as update comes in, not following market research of current threats that can be found within the infrastructure but never scanning for potential ransomware & malware threats.
13. Potentially stolen IP: IP reputation is never checked, SMTP relays are open where attackers can bounce emails using those relays and SPF, DKIM, DMARC is misconfigured.
14. ITIL functions and practices are missing.
15. Infrastructure vulnerabilities are not assessed & remediated properly.
16. Threat defense requirements, documentations are not effectively mapped, properly communicated, stakeholder's engagements are not controlled and not properly addressed and projected, operational challenges are not regularly presented or addressed by the senior management team etc.
17. Security monitoring and detection, Data protection and monitoring, Security administration, Remediation, devising Security roadmap and planning, SOC architecture and engineering (specific to the systems running your SOC from), Security architecture and engineering (of systems in your infrastructure environment), Threat research, Compliance support, Digital forensics, SOC team requirements, Incident response.
18. NOC and SOC are isolated and functioning independently.

- 
19. Silo mentality between security, IR and operations.
 20. Lack of context related to what we are seeing to take actions upon.
 21. Regulatory or legal requirements.
 22. Baseline SOC functions are inadequate - Application log monitoring, Continuous monitoring and assessment, Behavioral analysis and detection, Endpoint monitoring and logging, DNS log monitoring, Customized or tailored SIEM use-case monitoring, AI or machine learning, E-discovery (support legal requests for specific information collection), lawful interception requests from regulators, External threat intelligence (for online precursors), Frequency analysis for network connections, Full packet capture, net-flow analysis, Network intrusion detection system (IDS)/Intrusion prevention system (IPS), network access control, priority based transmissions, Packet analysis (other than full PCAP), Network traffic analysis/Network traffic monitoring, Security orchestration and automation (SOAR), Threat hunting, Threat intelligence (open source, vendor-provided), User behavior and entity monitoring etc.
 23. Device firmware updates are not up to date nor patched, installing these firmware updates before placing device in production mode is a necessity but mostly ignored.

Pro-Tip

- 
- Port and protocol controls aren't enough to protect your critical and business-critical services. ACL's for trusted trasmission only and must be in place. Enterprise risk management what we will be doing throughout the book.

We will be talking about these above items repeatedly, specially on PPTD, until it imprints into your brain, and that's the reason why this study material is produced for.

When an enterprise is committed to establishing and investing in a CSOC, these pitfalls must be avoided, and valuable lessons can be learned from other enterprises. After all, what we are doing here is to minimize risks across the organizational networks, connected devices by securing them from misuse and for data protections, essentially ERM (Enterprise Risk Management), BCP (Business Continuity Planning) & DRP (Disaster Recovery Planning).

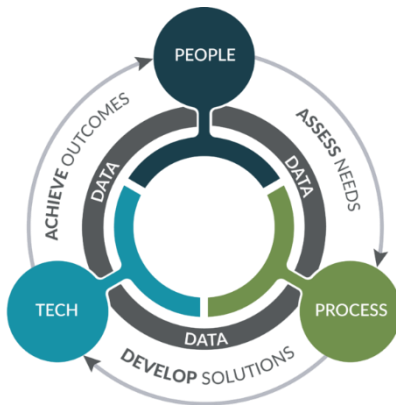
PPTD (People, Process, Technology, Data)

Let's break down the importance of people, process, technology, and data in a Cybersecurity Operations Center (SOC):



People: The SOC is staffed by a team of skilled security professionals, including security analysts, incident responders, threat intelligence analysts, and security engineers. These experts are responsible for monitoring security events, analyzing alerts, investigating security incidents, and responding to them. They also improve the systems and processes needed to optimize and transform world-class security operations. A diverse team with a variety of backgrounds and experiences is required to handle the complexity of security.

Process: Well-defined processes and procedures govern SOC operations. These include incident response plans, escalation procedures, and incident handling guidelines. Effective processes ensure a systematic and organized approach to cybersecurity. The SOC manages operational cybersecurity activities and identifies, detects, protects against, responds to, and recovers from unauthorized activities affecting the enterprise's digital footprint.



Technology: The SOC uses sophisticated technology to monitor, detect, and respond in real-time to cybersecurity threats. It combines and maximizes skilled resources, best practices, and technology solutions for the purpose of timely detection, real-time monitoring and correcting, and responding to cyber threats to protect the organization's assets. The SOC also selects, operates, and maintains the organization's cybersecurity technologies.

Data: Data is the lifeblood of a SOC3. It includes logs, alerts, network traffic data, and threat intelligence feeds. Analyzing this data provides insights into potential threats and vulnerabilities. The SOC also uses data analytics, external feeds, and product threat reports to gain insight into attacker behavior, infrastructure, and motives.

In summary, an efficient Cyber Security Operations Center is an orchestrated blend of sophisticated technology, carefully defined roles, synchronized communication, and a highly resilient team. It's important to note that the effectiveness of a SOC is highly dependent on the interplay of these four elements. Each one is crucial and the absence or weakness of any one element could potentially hinder the SOC's effectiveness.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

By effectively balancing and integrating these four elements, a SOC can enhance its ability to detect and respond to cybersecurity threats, thereby improving the overall security posture of the organization.

Software Deployment Roadmap – 3yrs Planning Tool

With this excel file, plan ahead of your service and components deployment, you can change the layout as you see fit for SOC deployment services as well (the excel file is provided in the job aids named 'software deployment planning'):

THREE YEAR SOFTWARE DEPLOYMENT PLANNING TOOL - Roadmap


PLATFORM BASED SOLUTION	Engagement Type	Year One (Basic)		Year Two (Standardized)		Year Three (Rationalized)		Fourth Year (Dynamic)	
		YES/NO	YES/NO	YES/NO	YES/NO	YES/NO	YES/NO	YES/NO	YES/NO
Windows Server 2019 (Identity Management) (START DATE:) (END DATE:)									
Identity Management	LOCAL	YES	NO						
Rights Management	LOCAL								
File Server FSRM	LOCAL								
Print Server	LOCAL								
Distributed File Server	LOCAL								
Web Server (IIS)	LOCAL								
Virtualization with Hyper-V	LOCAL								
RemoteFX	LOCAL								
Power Management	LOCAL								
Server Management	LOCAL								
Web Application Platform	LOCAL								
Integrated Experience with Windows 10	LOCAL								
Branch Cache	LOCAL								
Direct Access	LOCAL								
Active Directory Certificate Services	LOCAL								
Active Directory Domain Services	LOCAL								
Active Directory Federation Services (ADFS)	LOCAL								
Active Directory Lightweight Directory Services. Previously known as Active Directory Application Mode (ADAM)	LOCAL								
Dynamic Host Configuration Protocol (DHCP) Server	LOCAL								
DNS Server	LOCAL								
Cluster Services	LOCAL								
Network Policy and Access Services.	LOCAL								
Terminal Services	LOCAL								
Universal Description, Discovery, and Integration (UDDI) Services	LOCAL								
Windows Deployment Services (WDS)	LOCAL								
Windows PowerShell	LOCAL								
Smart Card Integration (Yubico, RSA SecurID)	LOCAL								

Why Enterprise Architecture

Source: [How Enterprise Architecture Drives Strategy, Innovation and Facilitation - Software. Technology. Consulting | 27Global](#)

Technology groups need to be able to execute strategic projects that fundamentally alter the way the company operates and does business. A [2019-2021 study from Accenture](#) on enterprise technology strategies and their impact on company performance showed that leaders in tech adoption and innovation were growing revenues at 5x the speed of tech laggards. We believe the strategy and execution of that strategy is key to drive transformation.

The key word is 'transformation & collaboration' in digitalization. We are positioned to help CEOs, CISO's, COOs, CIOs and CTOs become the chief transformation leader. Enterprise Architecture (EA) is a transition to managing strategy and transformation as an anticipatory discipline. Transformation execution primarily stems from strategy, innovation, and facilitation.



EA can be the catalyst to bring together the current and future needs of the organization and develop a solid plan to make them a reality. This brings about meaningful change. Without the right approach, companies pursuing digital transformation risk failure. Failure can range from increased tech costs to a company's inability to grow and reach its potential.

EA can avoid these pitfalls by balancing actionable projects with dynamic, long-term strategy and a practical approach. This new practical approach can help:

- Accelerate decision-making and delivery of business outcomes.
- Organize and optimize infrastructure to align with business goals.
- Modernize and grow your IT department.
- Foster collaboration and alignment between business and IT leadership to generate tech-enabled innovations and operating models.

In Majority there are four key items that are hindrances to transformation:

1. Execution Skills Missing – Modern efforts require modern skills. Cloud, virtualization, automation, services, containers, APIs, machine learning and AI all require continuous learning, so lack of skills will prevent change.
2. Organizational Inertia – Organizational culture can impede shifts in behavior. Resistance to change and optimization can stop all transformational efforts.
3. Lack of Strategy and Strategy Blindness – Without aligning your coherent technology strategy, business strategy and go-to-market priorities, you risk failure in value creation.
4. Inadequate Planning – Without a plan of how to get where you want to be, you're likely to fail. This is not about proper project methodology, it's about proper preparation for practical strategy execution.

The strategic appetite for a Cybersecurity Operations Center (CSOC) is essentially the level of cyber risk an organization is willing to accept in pursuit of its business objectives. This is typically articulated in a documented cyber risk appetite statement.



27 Global's five-phase approach to Enterprise Architecture



Source: [How Enterprise Architecture Drives Strategy, Innovation and Facilitation - Software, Technology, Consulting | 27Global](#)

Business Goal Alignment to Technology

Business goal alignment to technology is the process of ensuring that the IT department's objectives are aligned with the goals of the organization and each group within. It helps the IT team to deliver value to the business and the customers, improve agility and innovation, and optimize the use of resources and budget.

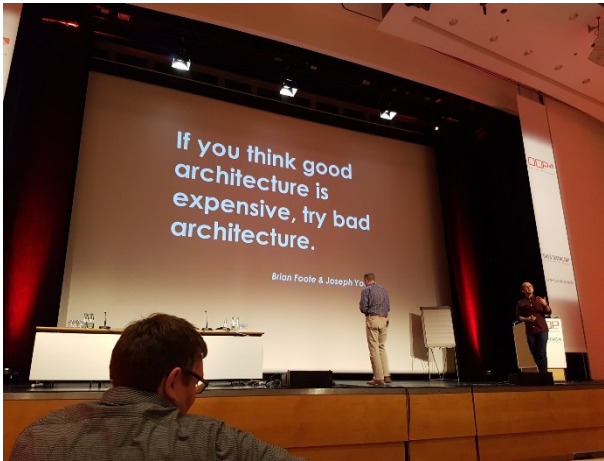
Some of the ways to achieve business goal alignment to technology are:

- Researching how other businesses have implemented new technology trends and evaluating their impact and benefits.
- Being the cheerleader of change and promoting a culture of continuous learning and improvement within the IT team and the organization.
- Gathering additional support from other stakeholders and collaborating with them to define and prioritize the business needs and expectations.
- Listening and keeping an open mind to feedback and suggestions from the business and the customers and adapting the IT strategy accordingly.
- Reducing human capital overhead and automating repetitive and low-value tasks, while focusing on high-value and strategic initiatives.

- Educating outside the IT team and communicating the value and benefits of the IT projects and solutions to the business and the customers.
- Working like a start-up and adopting agile and lean methodologies, such as iterative development, testing, and deployment, and measuring the outcomes and impact of the IT deliverables.

The Sad Story of Enterprise Architecture Formulation

In almost all the cases, the startup companies or the legacy companies which is in




gigantic size now, they all went through such transformation from a bad setup to a service operational excellence. Carnegie Mellon & Microsoft has CoE based specialized pathways defined on how to enable and achieve center of excellence.

As the picture depicts, the investments went down the drain, portals couldn't cope-up with the sheer volume of users, maintaining their access levels, employees

waiting for hours for the T-SQL to complete for a report, this sort of thing happened in the past. Back then the architects could sleep well in the night as there were very little virus infections at large, didn't destroy documents, only applications were targeted, which were easily removed. But as time passed, things got complicated, attacks on different layers confused architects, OEMs, so they adopted all the types of threats, started patching devices, applications, changed application designs, access layers were born or separated, scrutinization on data accuracy were re-calibrated, and a true server-client communications RFC's got updated and got in place, and in time these outlines became the gold standard.



Developers can change how their product works, but it may not work always. **The knowledge that created the problem must not be used to solve the problem.** Integrating different imported libraries and building software



using different platforms will almost always fail to produce desired results (the performance); and this isn't the best way to do it. You will need to create your own libraries to fulfill your requirements, importing libraries will come with its flaws and vulnerabilities, and when a proper scan on code reviews and Pentesting takes place, these will lead to catastrophic failures, and you will end up developing something unrecognizable just like the picture!

At that time, the frameworks, the standards, the whole workouts were completely absent. The people who understood this, rotated back to learn those, came back and updated or upgraded the same infrastructure over and over again for a king's treasures cost. Organizations soon found out that the easiest found languages are not the best when a scalable application couldn't be derived, even though it couldn't serve the requirements, and then came the spider, multi-tenancy requirements were in the rise, and it became monumental that you need to design or architect your infrastructure in the right way to support your business needs, and applications which were built in a monolithic way started to design better architecture with microservices.

But still, arguably, if you can design it the right way, it will support the scale and the TPS requirements as well, and if you use Kubernetes, these comes with humongous challenges to maintain thousands of nodes, and at some point, you will announce to have professional services, which will lead you to spend more and more. Check before if you really need to have Kubernetes or not, save your life first! This is where the value of Enterprise Architecture Design comes in and once more, everything went upside down, there is no such thing if an adopted system architecture would be able to deliver or not. Now a days, every bit of engagement comes with a checklist, from project management to delivery and calculated with man-hours, WBS's are getting more and more sophisticated as visibilities, cost involvements are included in every study, and now a days AI enable project management software is also on the rise.

I will try to formulate how best to derive and adopt to an EA and how to map some of the common requirements.



CHAPTER 2

An Enterprise Architecture Strategy

YOU NEED TO UNDERSTAND THE PRE-REQUISITES PRIOR ENTERING INTO THE SECURITY INFRASTRUCTURE OPERATIONS

The role of enterprise architecture is to help organizations align their technology strategy with their overall business objectives. Enterprise architects design and implement a technology architecture that can support the organization's goals and objectives, while also ensuring that all technology systems and applications work together seamlessly.

Some of the responsibilities of enterprise architects are:



- Envisioning, communicating, and evolving the organization's enterprise architecture.
- Establishing the portfolio's technology vision, strategy, and roadmap.
- Researching and evaluating new and innovative technologies and trends.
- Collaborating and coordinating with other stakeholders and architects across the organization.
- Providing guidance and governance for the development and implementation of IT projects and solutions.
- Measuring and assessing the outcomes and impact of the IT deliverables.

Lastly, a well architected infrastructure platform will pay you forever, some benefits are:

1. SOC would love to have minimized events per seconds/minutes. The better the infrastructure the easier it is to connect to the SOC.
2. SOC or your ASM (Attack Surface Management) team will find problems on the networked devices, application flaws, API flaws, access configuration flaws and will generate reports to mediate, these change request can generate a cascade of failures, and a hefty amount of CR charges.
3. Framework based platform will produce lesser challenges should it go through device replacements and contracted device replacements after 3yrs running periods, insurances for cost minimizations etc.
4. Integration throughout the infrastructure will be easier for log shipping, and different portals for visibilities.


It is somewhat out of context for the study of SOC for this chapter, but if you want to learn more about the role of enterprise architecture, you can check out some of these resources (look for the BoK at the end of this book):

- [Enterprise Architecture Roles and Responsibilities](#)
- [What is an enterprise architect? A vital role for IT operations](#)
- [Enterprise Architect - Scaled Agile Framework](#)

Azure Well Architected Frameworks

The **Azure Well-Architected Framework (WAF)** encompasses five essential tenets that guide solution architects in building robust and efficient workloads on **Microsoft Azure**:

1. **Reliability:**

- 
- Ensures that your workload meets **uptime and recovery targets** by incorporating redundancy and resiliency at scale.
 - Key considerations include **high availability, fault tolerance, and disaster recovery** strategies.
2. **Security:**
 - Safeguards your workload from attacks by maintaining **confidentiality** and **data integrity**.
 - Focus areas include **identity and access management (IAM), encryption, and network security**.
 3. **Cost Optimization:**
 - Encourages an **optimization mindset** at organizational, architectural, and tactical levels.
 - Strategies involve **right-sizing resources**, leveraging **reserved instances**, and optimizing spending within budget.
 4. **Operational Excellence:**
 - Aims to reduce issues in production by building **holistic observability** and **automated systems**.
 - Consider **monitoring, logging, and automation** practices.
 5. **Performance Efficiency:**
 - Allows your workload to adapt to changing demands through **horizontal scaling** and **testing** changes before deployment.
 - Optimize resource usage and performance.

These tenets collectively provide a strong foundation for designing and operating workloads on Azure, ensuring they deliver business value over time. Whether you're hosting Oracle databases, optimizing SAP workloads, or building mission-critical applications, adhering to these principles contributes to a successful cloud journey!



Source: [Azure Well-Architected Framework - Microsoft Azure Well-Architected Framework | Microsoft Learn](#)

Let's explore how you can implement the **five tenets** of the **Azure Well-Architected Framework (WAF)** in your architecture:

1. **Reliability:**

- **High Availability:** Design your workload to run across multiple **Azure Availability Zones** for redundancy. Use **Azure Load Balancer** to distribute traffic.
- **Fault Tolerance:** Implement **Azure Application Gateway** with multiple instances to handle failures gracefully.
- **Disaster Recovery:** Set up **Azure Site Recovery** for seamless failover to a secondary region.

2. **Security:**

- **Identity and Access Management (IAM):** Use **Azure Active Directory (AD)** for user authentication and authorization.
- **Encryption:** Encrypt data at rest using **Azure Disk Encryption** or **Azure Storage Service Encryption**.

- **Network Security:** Configure **Azure Network Security Groups (NSGs)** to control inbound and outbound traffic.
- 3. **Cost Optimization:**
 - **Resource Sizing:** Right-size your VMs and databases based on workload requirements.
 - **Reserved Instances:** Leverage **Azure Reserved VM Instances** for predictable workloads.
 - **Monitoring and Cost Analysis:** Use **Azure Cost Management and Billing** to track spending.
- 4. **Operational Excellence:**
 - **Monitoring and Logging:** Set up **Azure Monitor** for real-time insights into performance and issues.
 - **Automation:** Use **Azure Logic Apps** or **Azure Functions** for automated tasks.
 - **Change Management:** Implement **Azure DevOps** for continuous integration and deployment.
- 5. **Performance Efficiency:**
 - **Horizontal Scaling:** Use **Azure Autoscale** to dynamically adjust resources based on demand.
 - **Testing and Optimization:** Load test your application using **Azure Application Insights**.
 - **Content Delivery:** Utilize **Azure Content Delivery Network (CDN)** for efficient content distribution.

Example: E-Commerce Application

- 1. **Reliability:**
 - **High Availability:** Design your application to run across multiple **Azure Availability Zones** for redundancy. Use **Azure Load Balancer** to distribute traffic.
 - **Fault Tolerance:** Implement **Azure Application Gateway** with multiple instances to handle failures gracefully.
 - **Disaster Recovery:** Set up **Azure Site Recovery** for seamless failover to a secondary region.
- 2. **Security:**
 - **Identity and Access Management (IAM):** Use **Azure Active Directory (AD)** for user authentication and authorization.
 - **Encryption:** Encrypt data at rest using **Azure Disk Encryption** or **Azure Storage Service Encryption**.
 - **Network Security:** Configure **Azure Network Security Groups (NSGs)** to control inbound and outbound traffic.
- 3. **Cost Optimization:**

- **Resource Sizing:** Right-size your VMs and databases based on workload requirements.
 - **Reserved Instances:** Leverage **Azure Reserved VM Instances** for predictable workloads.
 - **Monitoring and Cost Analysis:** Use **Azure Cost Management and Billing** to track spending.
4. **Operational Excellence:**
- **Monitoring and Logging:** Set up **Azure Monitor** for real-time insights into performance and issues.
 - **Automation:** Use **Azure Logic Apps** or **Azure Functions** for automated tasks.
 - **Change Management:** Implement **Azure DevOps** for continuous integration and deployment.
5. **Performance Efficiency:**
- **Horizontal Scaling:** Use **Azure Autoscale** to dynamically adjust resources based on demand.
 - **Testing and Optimization:** Load test your application using **Azure Application Insights**.
 - **Content Delivery:** Utilize **Azure Content Delivery Network (CDN)** for efficient content distribution.

Partner Tools with Azure Monitor Integration

Routing your monitoring data to an event hub with Azure Monitor enables you to easily integrate with external SIEM and monitoring tools. The following table lists examples of tools with Azure Monitor integration.

Tool	Hosted in Azure	Description
IBM QRadar	No	The Microsoft Azure DSM and Microsoft Azure Event Hubs Protocol are available for download from the IBM support website .
Splunk	No	Splunk Add-on for Microsoft Cloud Services is an open-source project available in Splunkbase. If you can't install an add-on in your Splunk instance and, for example, you're using a proxy or running on Splunk Cloud, you can forward these events to the Splunk HTTP Event Collector



		by using Azure Function for Splunk . This tool is triggered by new messages in the event hub.
SumoLogic	No	Instructions for setting up SumoLogic to consume data from an event hub are available at Collect Logs for the Azure Audit App from Event Hubs .
ArcSight	No	The ArcSight Azure Event Hubs smart connector is available as part of the ArcSight smart connector collection .
Syslog server	No	If you want to stream Azure Monitor data directly to a Syslog server, you can use a solution based on an Azure function .
LogRhythm	No	Instructions to set up LogRhythm to collect logs from an event hub are available at this LogRhythm website .
Logz.io	Yes	For more information, see Get started with monitoring and logging by using Logz.io for Java apps running on Azure .

ASIM and the Open Source Security Events Metadata (OSSEM)

OSSEM is a community-led project that focuses primarily on the documentation and standardization of security event logs from diverse data sources and operating systems. The project also provides a Common Information Model (CIM) that can be used for data engineers during data normalization procedures to allow security analysts to query and analyze data across diverse data sources.

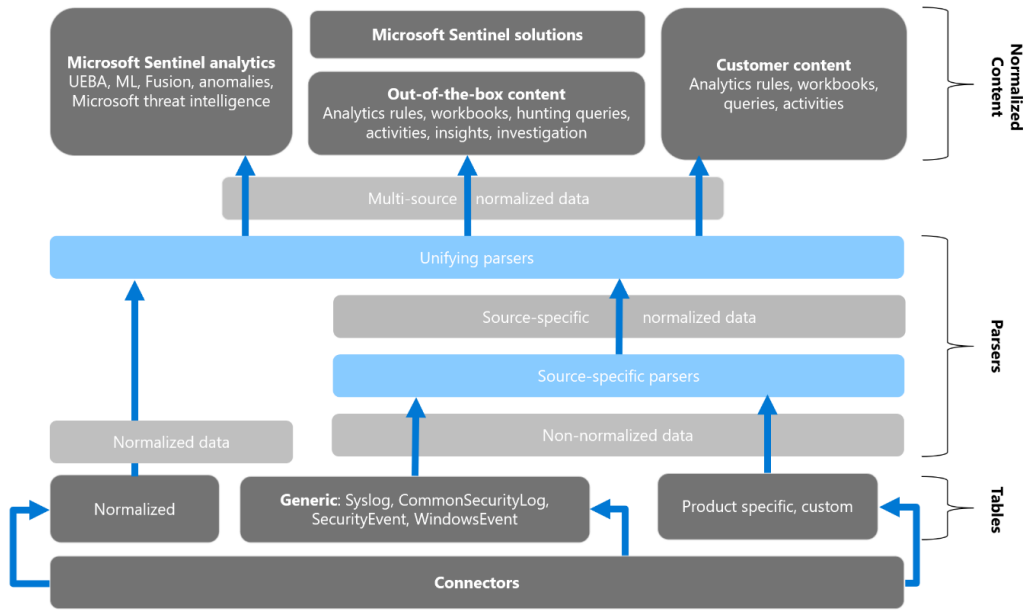
ASIM aligns with the [Open Source Security Events Metadata \(OSSEM\)](#) common information model, allowing for predictable entities correlation across normalized tables.

ASIM Components

The following image shows how non-normalized data can be translated into normalized content and used in Microsoft Sentinel. For example, you can start with a custom, product-specific, non-normalized table, and use a parser and a normalization schema to convert that table to normalized data. Use your normalized data in both Microsoft and custom analytics, rules, workbooks, queries, and more.



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Source: [Normalization and the Advanced Security Information Model \(ASIM\) | Microsoft Learn](#)

ASIM includes the following components:

Normalized Schemas

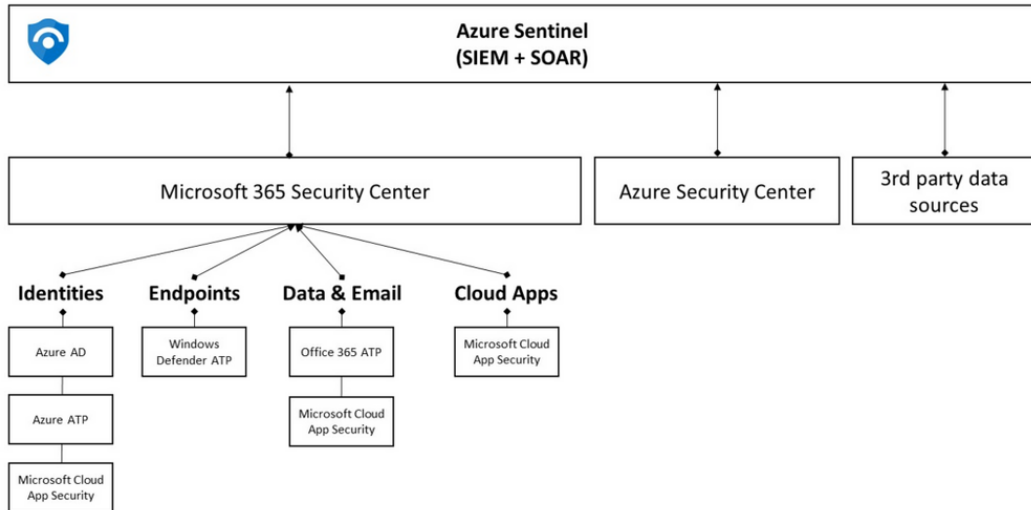
Normalized schemas cover standard sets of predictable event types that you can use when building unified capabilities. Each schema defines the fields that represent an event, a normalized column naming convention, and a standard format for the field values.

ASIM currently defines the following schemas:

- [Audit Event](#)
- [Authentication Event](#)
- [DHCP Activity](#)
- [DNS Activity](#)
- [File Activity](#)
- [Network Session](#)

- [Process Event](#)
- [Registry Event](#)
- [User Management](#)
- [Web Session](#)

Azure Sentinel in other hand is a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) tool. Azure Sentinel's role is to ingest data from different data sources and perform data correlation across these data sources. On top of that, Azure Sentinel leverages intelligent security analytics and threat intelligence to help with alert detection, threat visibility, proactive hunting, and threat response. The diagram below shows how Azure Sentinel is positioned across different data sources:



Source: [Integrating Azure Security Center with Azure Sentinel - Microsoft Community Hub](#)

Integrating Security Center with Azure Sentinel

When you configure this integration, the *Security Alerts* generated by Security Center will be streamed to Azure Sentinel. You only need to follow a few steps to configure this integration, and you can follow those steps by reading this article. Once the integration is configured, the alerts generated by Security Center will start appearing in Azure Sentinel.

End-to-end visibility

One advantage of using Azure Sentinel as your SIEM is the capability to have [data correlation](#) across data sources, which enables you to have an end-to-end visibility of the security related events, as shown in the diagram below:

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Source: [Integrating Azure Security Center with Azure Sentinel - Microsoft Community Hub](#)

In this example, Azure Sentinel created a [case](#) based on data correlation that is coming from different Microsoft products.

AWS Well Architected Frameworks


The **AWS Well-Architected Framework** is a comprehensive set of guidelines and best practices for designing and operating reliable, secure, efficient, and cost-effective systems in the **Amazon Web Services (AWS) cloud**. Let's delve into the details:

- 1. Purpose and Benefits:**
 - The framework helps you understand the **pros and cons** of decisions you make while building systems on AWS.
 - It provides a consistent approach to **evaluate and improve** your architectures against cloud qualities.
 - By following the framework, you can enhance the likelihood of business success.
- 2. Key Aspects:**
 - **Foundational Questions:** The framework includes a set of foundational questions that help you assess if a specific architecture aligns well with cloud best practices.
 - **Qualities:** It evaluates systems against the qualities expected from modern cloud-based systems (reliability, security, efficiency, cost-effectiveness, and sustainability).
 - **Constructive Conversation:** Reviewing an architecture is a constructive conversation about architectural decisions, not an audit.
 - **AWS Solutions Architects:** These experts have years of experience architecting solutions across various business verticals and use cases.
- 3. Who Should Use It?:**
 - The framework is intended for technology roles such as **CTOs, architects, developers, and operations team members**.
 - It provides valuable insights and recommendations for anyone involved in the lifecycle of a workload.
- 4. Additional Resources:**
 - **AWS Well-Architected Tool:** A service in the cloud that reviews and measures your architecture using the framework, providing recommendations for improvement.
 - **AWS Well-Architected Labs:** Hands-on experience implementing best practices.

the five pillars of AWS Well-Architected Framework


The **five pillars** of the **AWS Well-Architected Framework** are:

- 1. Operational Excellence:**
 - Focuses on running and monitoring systems to deliver business value.

- 
- Key areas include managing workloads, automating processes, and improving operational procedures.
 - 2. **Security:**
 - Ensures that systems are secure and protected.
 - Covers areas such as identity and access management, data protection, and infrastructure security.
 - 3. **Reliability:**
 - Aims to prevent and recover from failures.
 - Includes strategies for fault tolerance, disaster recovery, and scaling.
 - 4. **Performance Efficiency:**
 - Optimizes resource usage and cost.
 - Addresses aspects like selecting the right instance types, monitoring performance, and efficient data storage.
 - 5. **Cost Optimization:**
 - Focuses on minimizing costs while maintaining performance.
 - Involves analyzing spending patterns, using cost-effective resources, and optimizing workloads.

example of a well-architected system on AWS

Example: E-Commerce Application

- 
1. **Operational Excellence:**
 - **Automation:** The application uses **AWS Lambda** for serverless functions, automatically scaling based on demand.
 - **Monitoring:** **Amazon CloudWatch** monitors performance metrics, and alarms trigger notifications for any anomalies.
 - **Change Management:** **AWS CodePipeline** automates code deployment, ensuring consistent updates.
 2. **Security:**
 - **Identity and Access Management (IAM):** Fine-grained permissions control access to resources.
 - **Encryption:** Data at rest is encrypted using **Amazon S3** and **AWS Key Management Service (KMS)**.
 - **Network Security:** **Amazon VPC** isolates resources, and security groups restrict inbound traffic.
 3. **Reliability:**
 - **Multi-AZ Deployment:** The application runs across multiple availability zones for high availability.
 - **Auto Scaling:** **Amazon EC2 Auto Scaling** adjusts capacity based on traffic fluctuations.

- **Backup and Recovery:** Regular snapshots of databases are stored in **Amazon RDS**.
- 4. **Performance Efficiency:**
 - **Caching:** **Amazon ElastiCache** accelerates frequently accessed data.
 - **Content Delivery:** **Amazon CloudFront** serves static content globally, reducing latency.
 - **Database Optimization:** Properly sized **Amazon RDS** instances optimize performance.
- 5. **Cost Optimization:**
 - **Reserved Instances:** The application uses reserved instances for predictable workloads.
 - **Spot Instances:** Non-critical batch processing runs on **Amazon EC2 Spot Instances**.
 - **Right-Sizing:** Regular analysis ensures resources match workload requirements.

So How Do You Build a Rightly Sized Architecture?

Primarily I will just outline some of the core things that required for competitive advantage (you should engage a professional organization to do these activities & mapping, it is impossible to do this even by an internal team, suggested for companies like Deloitte, EY, PWC engagements – they already have these ready to deliver with clients engagements, and they have been doing it for a long time, and perfected those documents with an astounding amount of research, but everything has a cost attached to it, they don't come cheap):

- **Business requirements:** business strategy, capability maps, market stakeholders, distribution channels, people/process/technology mapping, corporate strategy (mission & vision), business architecture, data architecture, technology architecture, application architecture, total solution architecture, project management by PMO etc.
- **Roles in the organizational structure:** organizational need for business and technology drivers, strategic directions, PESTLE analysis, SWOT, challenges, tactical advantage over market players, external interested parties etc.
- **EA Scope (roadmap for industry – government future guidelines):** EA principles, CIA triad, AAA services, goals and objectives, agile, EA principles outline, EA operating model & governance, capability model, start of authority, limits of authority, stakeholder communication plan,

required outcomes, degree of centralization and decentralization, DevSecFinOps, stakeholder strength & power map etc.

- **Technology target state:** service requirements, ITIL, 5W1H, measurements of time and cost reductions, reworks decreased, risk reduction etc.
- **Foundational enterprise requirements:** business, data architecture, technology, integrations, access types by users (RBAC), application architecture, enterprise principles and methods, capability mapping with business processes, integration architecture etc.
- **Security architecture considerations:** firewalls, network zoning, SDN based traffic engineering and policy-based traffic prioritization, data that's getting out of the network is encrypted or not, security standards, policies,
- **Physical servers:** management from a single console like DELL iDRAC, distribution switch, management switch etc.
- **Model:** cloud or hybrid, data architecture, application architecture.
- **Backup of data** and data at rest security, data in transition security etc.
- **Enterprise risk management:** business & IT strategy, maturity of the EA, agile services, robust and scalable application platform.
- **Supply chain** services, due delivery and operations.
- **Compliance:** frameworks, ERM, BCP, DRP, ISMS, QMS, and laws of the land on data privacy, GDPR etc.

Key System Design Fundamentals

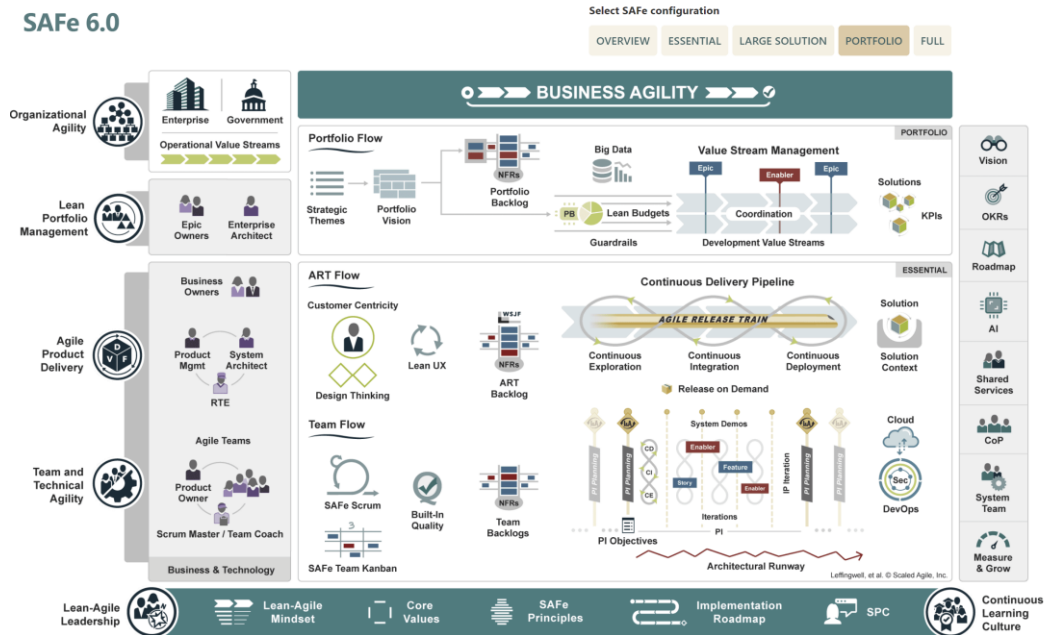
Just to keep in mind of the following items when designing a system or a platform (not an exhaustive list) (goes both for networked and application infrastructure):

- Scalability – large scale Availability
- Consistency
- Robustness
- Security architecture & accountability
- Maintainability
- Modularity
- Fault tolerance
- Circuit breaker
- Replica services
- Retrievable Backups
- Sharding

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

- Code repository
- Efficiency on resource consumption
- Device configuration backups
- MapReduce
- Accessibility
- Reliability engineering
- system architecture
- P2P

You can go through the SAFe site for a better understanding of the Agile Architecture:
[Advanced Topic - Agile Architecture in SAFe - Scaled Agile Framework](#)



Source: [SAFe 6.0 \(scaledagileframework.com\)](https://scaledagileframework.com)

In some cases, there are more than meets the eye, documenting all the necessary items into a really big picture would help understanding the business processes to develop the:

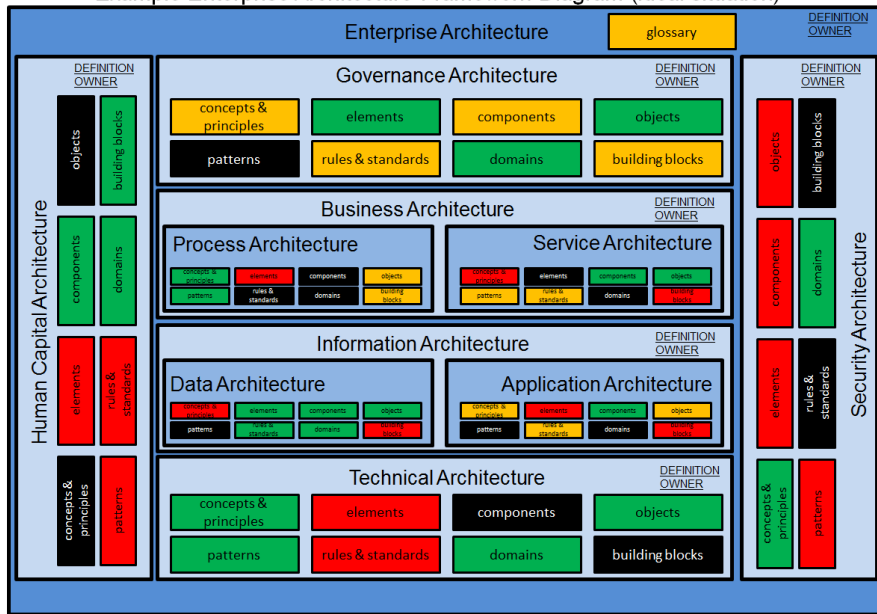
- 
1. **Business architecture:** Business strategy map, Business process flows, Value streams, Business capability map, Business model canvas, Service portfolio.
 2. **Infrastructure architecture:** Technology requirements, standards or framework outlines, demographic challenges for datacenters, platform design, full blown network diagram.
 3. **Application architecture:** application design & architecture with all components of the ERP mapped, various types of access requirements, web and mobile app or tablet view requirements, scalable systems for geo-location placements, application capability map or features etc.
 4. **Data architecture:** privacy requirements, data fields encryptions, useability of supplying reserved code to the application for discovering or unencrypting certain data fields like salary or incentive programs for the employees, law of the land, logical and conceptual data model, DB relations, DFD and lifecycle management, live data requirements, data at rest requirements etc.
 5. **Security architecture:** enterprise data security model, application security, transmission security, access security, internal application account security requirements, data processing services etc.

One of such design can be referenced to Dragon1's EA design:



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Example Enterprise Architecture Framework Diagram (ideal situation)



(c) Copyright 2014, Dragon1 – open EA Method / Visualization Standard, <http://wiki.dragon1.org>

In an operational perspective, Business Architects are the ones who connects all the dots (stakeholder onboarding – take buy ins and inform them of the architecture, its benefits, usability, dashboards for the senior management to take decisions based on the analytics), where:

1. **Business architects** would choose key business challenges with business architecture model.
2. **Business operators** are responsible for: processes, data, infrastructure.
3. **Business unit leads** are responsible for: sending out their requirements to the business architect where the BA folks would map out infrastructure and application requirements.
4. **Experts of different sorts** are responsible for business operations, who receive the requirements from business lines, operations, infrastructure development teams etc.
5. **Lastly, the business architect** will identify strategic business objectives, and would map out your vision and strategy, generate value streams that connects business goals to the organization's value realization activities which also aligns to business capability requirements.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

A business capability map could be something like the below picture from LeanIX:

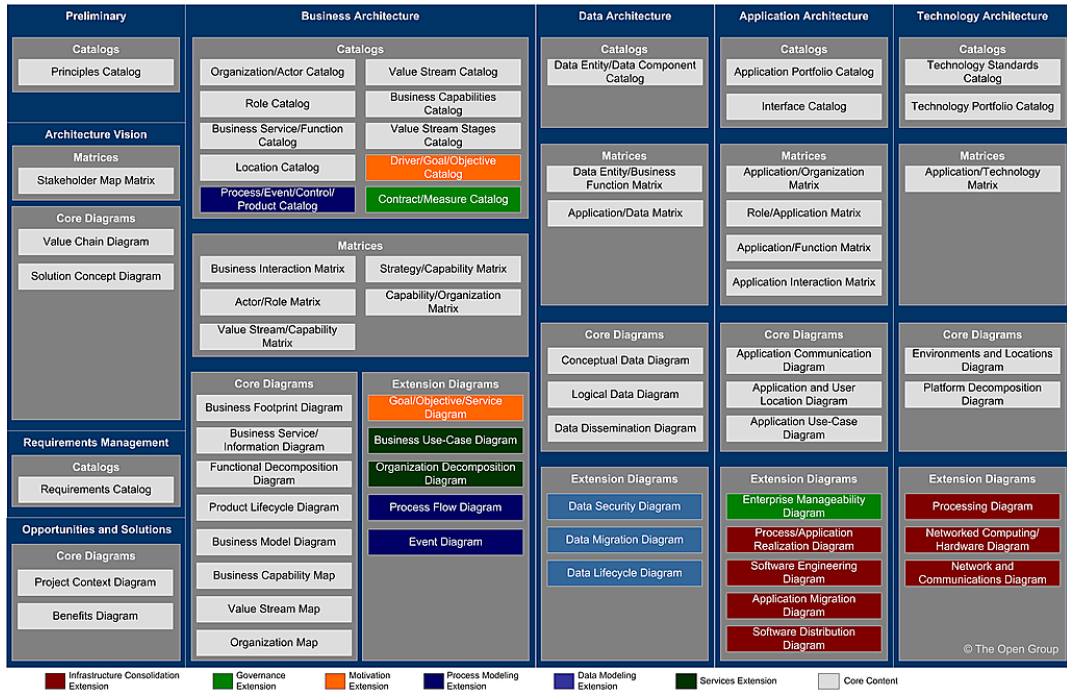


Source: [Business Capability Map and Model - The Definitive Guide | LeanIX](#)

You can use their freely provided excel worksheet to map yours which also can be mapped to your ERP components as OSS/BSS or for LoB application requirements mapping.

Another one from The Open Group (ADM – Architecture Development Method): *Artifacts Associated with the Core Content Metamodel and Extensions* @ [Architectural Artifacts \(opengroup.org\)](#)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



This is a wonderful playground if you want to explore designing a business plan to deploy technical services, then this document repo is for you. So, when you say you are an enterprise architect, do keep these in mind.

Some of the things that should be kept in mind is that:

1. Value streams are mapped to business capabilities. At times it may look like too much works are being done for understanding the business rather than focusing what the infrastructure were supposed to be and ended up with nothing, problems cannot be identified, where we did wrong and investors perspective in this regard will be horrible. Rather do it once, assign personnel to keep these documents tracked and always updated, and you should take help using a software.
2. Prioritization of value streams and identify and map its capabilities, do it one by one as pre-requisites will be there, and complete the design with mapped requirements to the infrastructure. Select key priorities that need to be in place for a year, then plan for the next year. You can take advantage of the "BLUE OCEAN STRATEGY" for your business perspective as well.
3. Align the business objectives of your organization to your value streams.

4. A single capability may support multiple value stages in the stream.
5. Build a business architecture for the prioritized value stream with a map of business capabilities.
6. Business value realization

Pro-Tip

- Value, goals, and outcomes cannot be achieved without business capabilities are outlined, mapped

The Service Integration Layer

The Service Integration Layer (SIL) emerges as a pivotal solution, providing a unified platform to seamlessly integrate, manage, and optimize services across an organization. Let's delve into the foundational aspects, benefits, and implementation strategies of the Service Integration Layer.

Background

As organizations adopt an increasing number of specialized services and applications, the need for a cohesive framework to integrate these disparate elements becomes paramount. The Service Integration Layer acts as an intermediary, facilitating communication and data flow between different services, systems, and applications. This layer is instrumental in achieving interoperability, reducing redundancy, and streamlining processes.

Key Components of the Service Integration Layer

API Gateway:

- Acts as the entry point for external applications and services.
- Enforces security policies, manages access control, and ensures efficient routing of requests.

Message Broker:

- Facilitates asynchronous communication between services.
- Manages message queues, ensuring reliable delivery and decoupling of services.

Data Integration Hub:

- Synchronizes and manages data flow between disparate databases and data sources.
- Supports data transformation, validation, and enrichment processes.

Event Processing Engine:

- Monitors and processes real-time events, enabling quick response to changing conditions.
- Supports event-driven architectures, fostering agility and responsiveness.

Workflow Orchestration:

- Coordinates the execution of business processes across multiple services.
- Manages the flow of tasks, dependencies, and error handling in complex workflows.

Benefits of the Service Integration Layer

Improved Interoperability:

- Enables seamless communication between diverse applications and services, fostering interoperability and reducing integration challenges.

Enhanced Agility:

- Facilitates a modular and scalable architecture, allowing organizations to quickly adapt to changing business requirements.

Optimized Resource Utilization:

- Reduces redundancy and optimizes resource utilization by avoiding duplicated efforts and data storage.

Increased Scalability:

- Provides a scalable infrastructure that can easily accommodate the addition of new services and adapt to growing workloads.

Streamlined Maintenance:

- Centralizes management and monitoring, simplifying the maintenance and troubleshooting of integrated services.

Implementation Strategies

Assessment of Current Infrastructure:

- Conduct a thorough analysis of existing applications, services, and data sources to identify integration points and requirements.

Selection of Integration Technologies:

- Choose appropriate technologies for each component of the Service Integration Layer based on the organization's needs and existing infrastructure.

Development of Integration Standards:

- Establish standardized protocols, data formats, and communication patterns to ensure consistency and compatibility across integrated services.

Security Measures:

- Implement robust security measures, including encryption, authentication, and authorization, to safeguard the integrity and confidentiality of data flowing through the Service Integration Layer.

Testing and Validation:

- Conduct comprehensive testing to validate the functionality, performance, and reliability of the Service Integration Layer before deployment.

Case Studies

E-commerce Platform:

- *Scenario:* An e-commerce platform integrates order processing, inventory management, and payment processing systems.
- *Outcome:* The Service Integration Layer streamlines the order fulfillment process, reduces errors, and enhances customer satisfaction.

Healthcare System Integration:

- *Scenario:* A healthcare organization integrates electronic health records, billing systems, and diagnostic services.

- *Outcome:* The Service Integration Layer enables real-time access to patient data, improves billing accuracy, and enhances overall healthcare delivery.

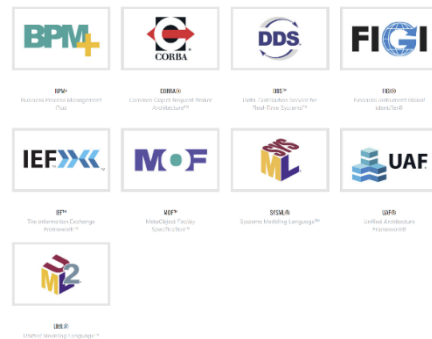
By providing a unified platform for seamless communication and data flow, the Service Integration Layer contributes to improved interoperability, enhanced agility, and streamlined resource utilization. Organizations that strategically implement and leverage the Service Integration Layer are better equipped to navigate the complexities of the digital landscape, fostering innovation and competitiveness in today's dynamic business environment.

Popular OMG.ORG Standards

Please download the specifications if you want to learn more about why and how they have planned and designed the architecture and integrations. These are the specifications that were mostly adopted and expanded as required:

Source: [OMG Standards Introduction | Object Management Group](#)

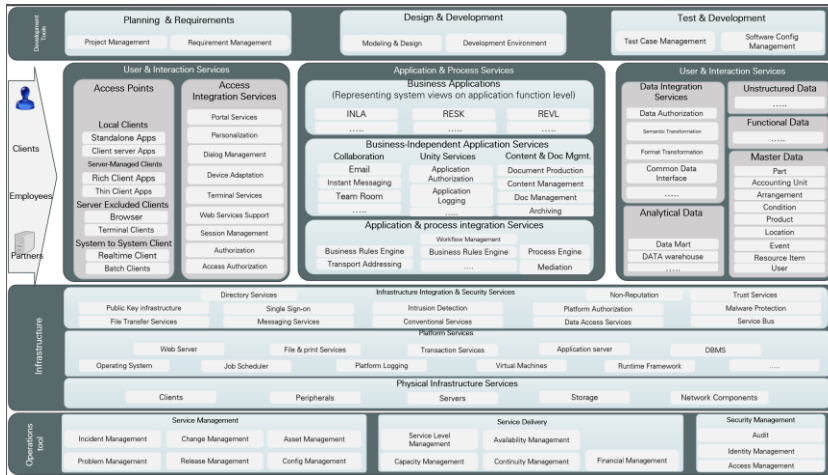
Source: [OMG Standards Introduction | Object Management Group](#)



Another Architecture Mapping (BPM)

This one is also mapped to business requirements, but by all means, do map your as per your organizational requirements (the ppt file is also provided in the job aids), and when options are available, do use ArchiMate or Dragon1 or LeanIX to develop yours:

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Before you jump into developing your own SOC program, I would strongly recommend that you assess the current infrastructure either using NIST, CISEcurity, or Homeland Security's CRR framework (Developed by Carnegie Mellon University, shared from CISA's site) (also provided in the job aids folder named "1_CRR_v4.0_Self-Assessment-Reader_April_2020.pdf").

This effort will provide you with a holistic view of the readiness of your infrastructure, and a chance to fix whatever is necessary to define your SOC's operational activities.

But do browse the web for different architecture patterns and their service lineups, and learn to develop your own as you observe having an ERP in place. Find out the modules listed in the ERP and map them to your line of business requirements, soon you will have a map that provides an outline for the BPM, aka, Business Process Management. Reverse engineering!

CIS also provides a spreadsheet for their assessment, and a summary picture of the screenshot is provided below (this file is provided in the job aids named "CIS-8_Cybersecurity Posture Assessment.xlsx"):

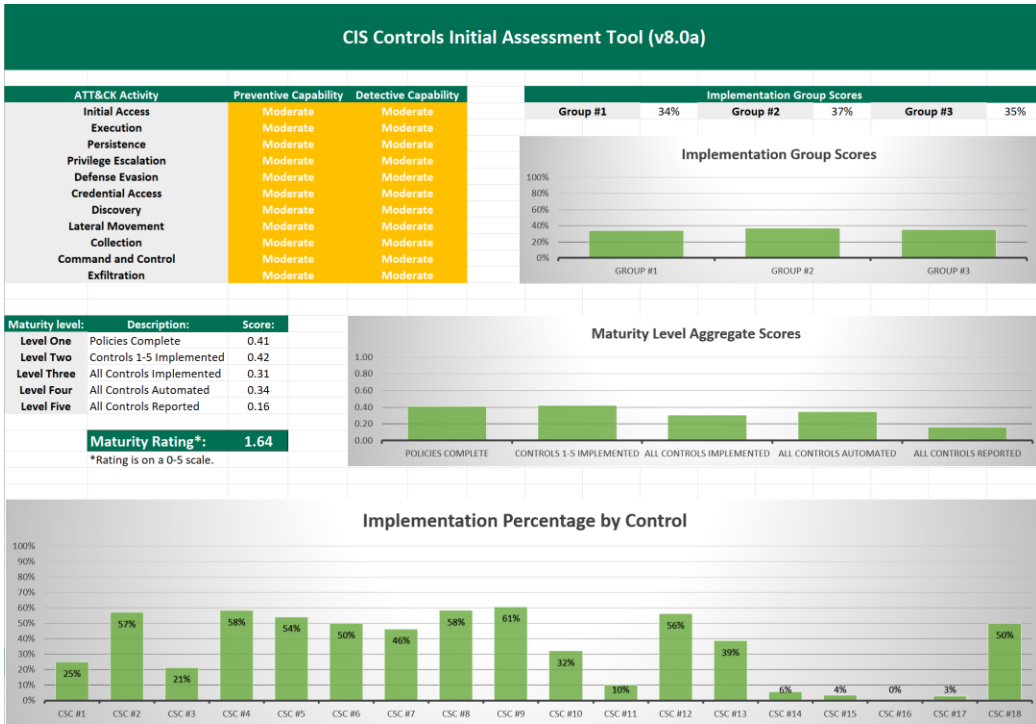


CYBER RESILIENCE REVIEW (CRR)

Self-Assessment Package

APRIL 2020

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Enterprise Architecture in Cybersecurity

Enterprise architecture in cybersecurity is the practice of designing and implementing a holistic and integrated security strategy for an organization. It aligns the security objectives and capabilities with the business goals and needs, and covers all aspects of the enterprise, such as people, processes, technology, and data. Enterprise architecture in cybersecurity helps to protect the organization from cyber threats, optimize the use of resources, and create value for IT investments.

Security architecture is part of enterprise architecture, which also includes connected networks, remote sites, business continuity plans and disaster recovery plans. It should be designed in the network planning phase, not later, to meet both security and business needs. Enterprise architecture designs specify the type of applications required, type of workstations (standardized) and device portals that connect to the network, and their limitations. They may not cover network configurations, but they do cover infrastructure that provides security and productivity, and the processes for making and keeping architecture flowcharts and diagrams. The enterprise architecture team tells the security

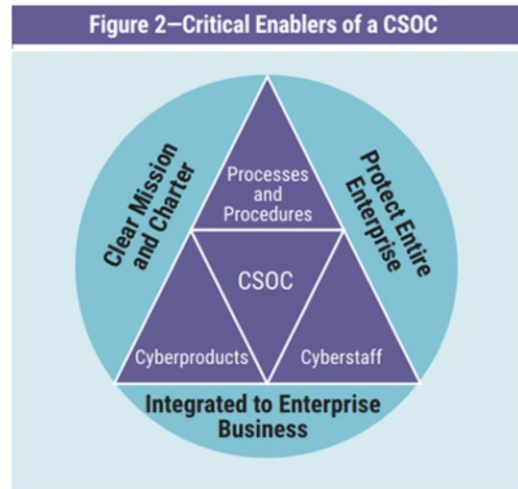
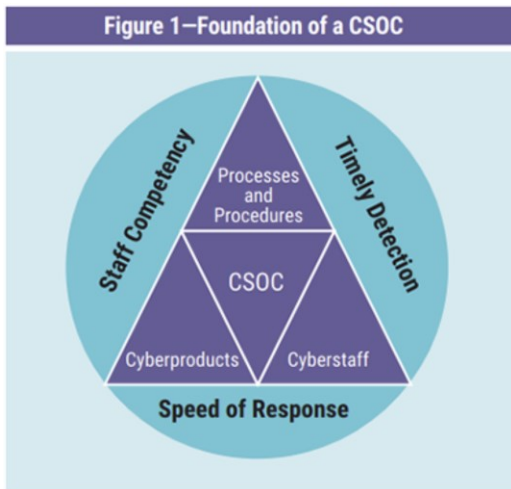


COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

operations team about the increased attack surface when new networks are set up or devices are replaced with newer lines or their firmwares are upgraded. In all cases, the security team is protecting the organizational data, the better architected the network, the better and easier visibility the SOC can provide.

Pro-Tip

- An enterprise's ERM, BCP, DRP is somewhat the broadest scope, as per ISO 27xxx series, NIST 800-53 and 171



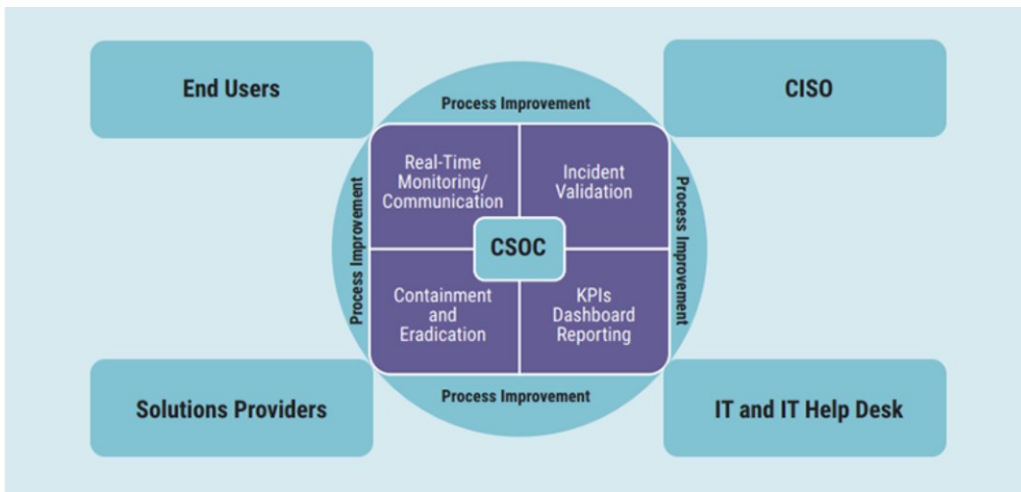
Source: [Best Practices for Setting Up a Cybersecurity Operations Center \(isaca.org\)](https://www.isaca.org/resources/whitepapers/2017/best-practices-for-setting-up-a-cybersecurity-operations-center)

For the SOC to carry out its functions successfully, critical enablers must be in place. The SOC must protect the entire enterprise, have a clear mission and charter, and be integrated into the business of the enterprise.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER


Critical Attributes of Effectiveness and Challenges						
Critical Attributes of Effectiveness	Enterprise-level function	Integrated with the business objective of the enterprise	Has the focus of the BoD	Has full visibility of the enterprise's digital infrastructure	Inclusive in cybersecurity jurisdiction	Equipped with competent staff
Critical Attributes of Functional Responsibilities	Real-time monitoring	Incident validation	Threat containment and eradication	KPIs and dashboard reporting	Continuous process improvement	Maximized automation
Critical Attributes of Challenges	Operates as an IT help desk	Unsuitability with the enterprise culture	Operates in isolation	Insufficient funding	Unable to capture and quantify success	Outsourcing critical functions

Source: [Best Practices for Setting Up a Cybersecurity Operations Center \(isaca.org\)](https://www.isaca.org/insights/whitepapers/2017/04/best-practices-for-setting-up-a-cybersecurity-operations-center)



Source: [Best Practices for Setting Up a Cybersecurity Operations Center \(isaca.org\)](https://www.isaca.org/insights/whitepapers/2017/04/best-practices-for-setting-up-a-cybersecurity-operations-center)

The sad part of the cybersecurity is that the activity domains are not clear, lack of frameworks, the knowledgebase is not clear, scarcity of the mentor is not available to follow, or people are not open to things they know, where appropriate tools are not grouped together for performing a set of activities and so on. But rest assured, amongst all these problems we still have tons of tools available, bits and pieces of information is scattered across the web, and its troublesome to the extent of a Rubik's cube.



Nonetheless, we have problems at hand that needs to be solved, and that's not going to be solved at one go, but millions of people across the globe joint forces against the attackers, and because of them we have tools that's freely available to us, and from the bottom of my heart, I thank them for their selfless efforts. And because of them we get to know how these tools work and the knowledge is priceless, which is also scattered the globe, if all of us can be grouped together and share their knowledge, what a wonderful world it could be.

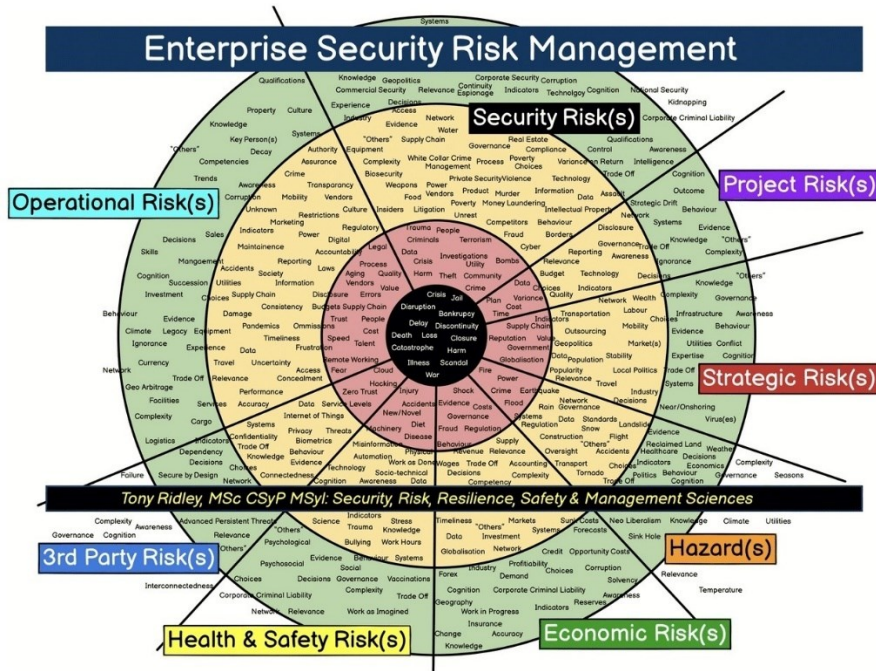
Enterprise Security Risk Management

Enterprise Security Risk Management (ESRM) is a strategic approach to security management that ties an organization's security practice to its overall strategy using globally established and accepted risk management principles. The process of ESRM involves identifying risks and threats, determining how to mitigate them, and documenting policies and best practices to address future occurrences proactively and reactively.

There is no easy way to put it as vast as the topic goes, but most comprehensive area coverage is derived by frameworks, but none the less, a combined picture is produced by Tony Ridley:



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Knowledge Areas That Will Pay You for Life

It is obvious that these knowledge areas are only achievable over time, some luck and some opportunities, networking with the right personnel where you would be able to acquire efficient knowledge. Be careful of ingesting garbage or wrong knowledge, take a lead, study yourself, and if you trust the source of knowledge, then by all means go ahead, but do verify, as when time comes for you to excel, things will go south very quickly, and you can imagine the end result. Always try to be a technical advisor to your peers, clients and give them something to trust you, ego aside. I am not saying I have acquired all the knowledge stated below, not even for a long shot, but corelated knowledge is essential, grab it whenever possible, and always make friends with a person with higher knowledge & intellect, it's a blessing, not your challenger (maybe not on all cases), still, step-up. In an active office, you will find many peers to work with, who are good at something, take the knowledge and enrich yourself.

Below are some knowledge areas that you should be aware of (this is really an exhaustive list, and not meant for one person to know all of them):

SL	Description	Remarks
----	-------------	---------



<p>1 Organizational Development</p>	<p>Communication process, requirements management process, evidence based management, policy development, cybersecurity leadership, team management, team building, coaching/mentoring, awareness and competence assurance process, internal audit process, risk assessment process, security implementation process, conflict resolution time management, information security improvement process, government contract management, SRS of ERP development, information security governance process, security policy management process, records control process, supplier management process, information security incident management process, risk treatment process, performance evaluation processes specially on financials, ISMS change management processes, change control etc.</p>
<p>Enterprise Architecture</p>	<p>Enterprise architecture, cybersecurity strategy, architecture roadmaps, enterprise cybersecurity, database security architecture, system security architecture, cloud security architecture, application security architecture, business architecture, automation with ansible or terraform, architecture review board, network security architecture, model driven architecture, ArchiMate for designing your desired services aligning to business processes, BPMN, UML, SIEM, DLP, IAM, PAM, ACI, DRM, BPM, DAM, RMM, SDWAN, SDN, SDDC, OSINT, SPF, RPA, UEBA, EDR, DFIR, EMM, SOAR, HCI, DCIM, EMS, ZTNA, CASB, CSPM, SSE & SASE, CIG, TVM, CTEM etc.</p>
<p>Application Architecture Design</p>	<p>Architecture design, SRS development, scalability, storage requirement, DB cluster design, performance & TPS testing, transmission, DB backup & replication web / mobile / tab compatibility, security & threat defense, API security, oauth-v2 or higher, SSO with LDAP, system platform, DB server</p>





	<p>platform, DB consolidation mapping, data streaming services event bus, cryptography & internal encryptions & salting, HSM key generator & key management, react, html, CSS, director or profiler, high-performance data pipelines, streaming analytics, data integration, service bus, zookeeper, Kafka, distributed tracing, database, cache, streaming engine, and message broker, DB warehouse, multi-cluster service mesh routing, eBPF-based networking, observability, blockchain – Hyperledger, API architecture & protocols (REST, Webhooks, GraphQL, EDA, EDI, gRPC, MQTT, SSE, WebSocket, SSE, AMQP), API gateway, payment gateway, session management, API testing, dynamic reporting portals, KYC, log management & shipping, elk stack for monitoring, mobile app development, platform reliability engineering, microservices, web application firewall & CASB, load balancing & routing, cache mechanisms, file management, Cron jobs, API protocols, ci/cd pipelines, storage management in CEPH, Grafana, Prometheus, Kubernetes with storage and node & pod management, docker and other container services, ansible & terraform automation, data pipelines, tokenization, DevOps functions, architecture patterns, api performance, secure coding, code repo security, bi analytics, service registry, mesh patterns, CQRS patterns, bulkhead strangler & sidecar patterns, SLDC, iso 8583 for message transfer controls for PCI, AML/CFT, data privacy, PII, code review, application transmission requirements per service, test for vulnerabilities by scanning etc.</p>
<p>Code Repositories</p>	<p>Mono repositories and multi-repositories, but must have full, incremental, differential backup systems on all cases as per schedules. Most commons are Azure DevOps, Monday, Redmine, Git, JIRA & Confluence, ClickUp etc.</p>



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Database	Most popular one's like MS-SQL, Oracle, PostgreSQL, MongoDB etc.
BI Analytics	Power BI, Tableau, Board, QLIK, IBM Cognos, GoodData, Dundas BI, Style Intelligence, Oracle BI, Domo, Datapine, SAS BI, Infor Birst, SAP Business Objects, test for vulnerabilities
Cybersecurity	Playbooks, runbooks, operation center design basics for infrastructure, cybersecurity governance, cyber resilience (DRP, BCP, IRM), vulnerability management, enterprise risk management, risk management, risk assessment, risk analysis, cybersecurity regulation, adaptive insights, threat driven modeling activities, event driven activities, analytics, OSINT, threat engineering, data science, ai in cyber, unknown process installation investigation, OSINT or reputation check tools, phishing emails, malware investigation, brute force analysis, DoS/DDoS attacks, log investigation, Windows & Linux event log analysis, Network and server firewalls, Configuration management, Incident management, Server and endpoint antivirus protection, Web application firewalls, Two-factor authentication (2FA), Identity management, Security information and event monitoring (SIEM), Database monitoring Whitelisting, Blacklisting, Network anomaly detection, Email antispam protection, Email antimalware protection, Email anti-spoofing protection, Validation of vulnerabilities, Patch management, Data leakage protection Encryption, File integrity monitoring, System backups, case documentation, initial investigation, AppSec, DevSecFinOps, attack surface management, cloud security, analysis tools, asset management, endpoint security, encrypted traffic visibility, IIoT & ICS, data correlation, cloud security, operational technology, PLC programming & SCADA systems, threat intelligence management,





	vulnerability management tools, behavioral analysis, VPN security, DNS security, email security, Active Directory or LDAP or ID provider security, federated SSO security, log storage and access, deception techniques, AI & ML, network device access control, secured access service edge, proxy servers, reverse proxy servers, web application firewalls, DDoS firewalls, networked devices configuration security and benchmarks, regulatory compliance, tabletop exercises, SOC infrastructure development & implementation and maintenance, IaaS, PaaS, SaaS models and its integrations services, 3 rd party security risks, supply chain risks, breach response, capability improvement and training services for continual improvement, quality review, visibility tuning for SOC applications and event reporting services, secured developer laptops etc.
WAF with Scrubbing Services	Cloudflare, Akamai, Amazon AWS CloudFront, Bunny.net, CacheFly, CDN77, Fastly, G-Core, KeyCDN, Medianova, StackPath, Universal CDN
Network Architecture	SDN, ACI, policy-based traffic control, trust-based ACL, authentication by protocol, network operations, network security, device configuration benchmark, DNS, NTP, RADIUS, LDAP Integrated ISE, device BoQ generation, operations management, configuration script generation, NOC development
Desktop & Server OS Configuration	Windows, Linux, Mac, Patch Management, EDR or EDX, UEBA integration, OS & Service cluster design, drive encryption like BitLocker etc.
ITIL Services	34 ITIL controls
Network Device Configurations	Cisco, Juniper, Huawei, Aruba, DNS & recursive queries, NTP with authentication, SMTP with authentications & relay, VPN, Key management for IKEv2, DNSSEC, Configuration script generation
IP Telephony	Cisco, Avaya, SigTran, monitoring, ACD, Dashboard, test for vulnerabilities



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Wireless Controllers & AP	Cisco Meraki, Linksys, Aruba, Cambium, LOS Wireless 5GHz or isolated bands, test for vulnerabilities
Routers	Cisco, Juniper, baseline secured configurations, BoQ generation, configuration script generation, global VPN Access, test for vulnerabilities
Switches	Cisco, Juniper, baseline secured configurations, BoQ generation, Configuration script generation, test for vulnerabilities
Firewall, WAF, DDoS Appliance	PaloAlto, CheckPoint, FortiNet, FireEye, IPS, IDS, HIDS, UTM box types, WAF, DDoS & scrubbing center, baseline configuration checklist development, test for vulnerabilities
Load Balancers	F5, Types of load balancing methods
High Availability	Design types, ring network for Lambda transfers across region
Bandwidth Shapers	PacketController, NetBalancer, NetLimiter, Aruba, Cisco, Huawei, Allot
Storage Servers	IBM, HP, DELL, Kubernetes native operations on storage drives
HSM Appliance	Hardware Security Modules - Thales
Physical Servers	IBM, HP, DELL configurations, R/W ratio determination, RAM to Core requirements, IOPS calculations, RAID calculations, 10G/100G SFP+ Cards, NIC teaming, choice of the right NIC card, HBA selection, redundant power supply for the power count equal to your HDD/SSD, load calculations, generator or UPS's power purity calibrations etc.
Blade Servers with Controllers	BoQ generations, load calculations
Operating Systems	Hardware abstraction layers, service integration layer, anti-ransomware, patch management, security configuration baseline
Technical Writing	Policies, standards, guidelines, plans (IR, BC, DR), standard operating procedures, business process development, use cases, business cases, presentations, program charters, risk reporting, business reporting
Project & Portfolio Management	Setup a PMO, Derive PMO functions and performance requirements, portfolio management, program management, project





	management, budgeting, stakeholder management etc.
Frameworks	COBIT, CIS, DHS-CDM Program, GCHQ Cyber, UK Cyber Essentials, , NERC-CIP, HIPAA, ISO 27000 Series, FFIEC, ENISA, IEC 31010, NIST 800-53 & 171, CSA-Matrix, PCI-DSS, NIST CSF, GDPR, ETSI TR 103305-1, TR 103305-2, TR 103305-3, TR 103305-4, TR 103305-5, FISMA, Australian Cyber etc. (lookout for a chapter at the end of this document where all these BoK and guidelines are provided)
Regulations	Law of the land applies for privacy, regulations, governance, artificial intelligence, blockchain, crypto currency, cybersecurity etc.

The network security team will establish a communication channel with the group implementing the network security policy, which may or may not be a separate team. Change control processes will include any specific information required for network security updates and follow the standard change control steps established for other changes within the business.

Please understand that these lists of knowledgebase requirements are not even close to an exhaustive list, and as you walk down the road, the more you would get confused about the incomplete frameworks, there is no magic wand of checklists for each item, and there is no 1 book of everything. Though their effort is remarkable, selfless, enormous man-hour is put in for designing and outlining the frameworks; the problem is, they don't talk much and collaborated to generate a full option one single framework.

C2, C4ISR & C4ISTAR

C2 (Wikipedia): Command and control often called as C2 is a "set of organizational and technical attributes and processes ... that employs human, physical, and information resources to solve problems and accomplish missions" to achieve the goals of an organization or enterprise, according to a 2015 definition by military scientists Marius Vassiliou, David S. Alberts, and Jonathan R. Agre. The term often refers to a military system.

C4ISR may refer to:



- The C4ISR concept of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance, the U.S. term for C4ISTAR
- The C4ISR architectural framework (C4ISR AF), now known as Department of Defense Architecture Framework (DoDAF)

New concepts of operations and approaches to Command and Control are able to provide significantly increased capabilities to deal with these challenges.

Some of the most common variations are:

- AC2 - Aviation command & control
- C2I – Command, control & intelligence
- C2I – command, control & information (a less common usage)
- R2C2I - rapid advanced manufacturing, command, control & intelligence [developed by SICDRONE]
- C2IS – command and control information systems
- C2ISR – C2I plus surveillance and reconnaissance
- C2ISTAR – C2 plus ISTAR (intelligence, surveillance, target acquisition, and reconnaissance)
- C3 – command, control & communication (human activity focus)
- C3 – command, control & communications (technology focus)
- C3 – consultation, command, and control [NATO]
- C3I – 4 possibilities; the most common is command, control, communications and intelligence
- C3ISTAR – C3 plus ISTAR
- C3ISREW – C2ISR plus communications plus electronic warfare (technology focus)
- C3MS - cyber command and control mission system
- C3/SA - C3 plus situational awareness
- C4, C4I, C4ISR, C4ISTAR, C4ISREW, C4ISTAREW – plus computers (technology focus) or computing (human activity focus)
- C4I2 – command, control, communications, computers, intelligence, and interoperability
- C5I – command, control, communications, computers, collaboration and intelligence
- C5I – command, control, communications, computers, cyber and intelligence (US Army)
- C6ISR – command, control, communications, computers, cyber-defense and combat systems and intelligence, surveillance, and reconnaissance

- MDC2 - multi-domain command and control
- NC2 – nuclear command and control
- NC3 – nuclear command and control and communications

C4ISR Defense in Depth Core Function Descriptions

More specifically, as mentioned above, the CIOC (DoD- Cyber Intelligence Operation Center) is the cyber battle management function that manages the multiple attack vectors against an organization’s vital assets through the CIOC management of the organization’s security management posture. Specific actions behaviors required for the defense in depth concept and functional management include:

Predict attacks on an organization’s assets:

- Serious consideration of the results of the ongoing intelligence reports generated by the CIOC intelligence analyses and report team.
- Analyses of internal vulnerabilities, risks and exposures and the likelihood that specific exposures can be realized against the organization due unmitigated exposures.
- Review SIEM and all other awareness dashboards that you might have at least twice a day.
- Constant analyses of the types of attacks that happen every day on the organization that might provide indications and warnings (I&W) of site enumeration.
- The introduction of new technologies that could cause a disruption of current processes and procedures. Cloud adoption could be considered a disruptive technology that could present new exposures non mitigated exposure.
- High vigilance to Cyber Open-Source Intelligence (COSI) information and intelligence sources to include multiple information security magazines, blogs, threat reports.
- Get feedback from other teams like network engineering on possible Indications and warnings you can integrate into you Prediction Strategy
- Relationships with local law enforcement.

Prevent attacks on an organization’s assets:

- Define and build a state of the art security architecture that is aligned with an organizations risk profile.
- Build excellent security architecture documents.

- Tune all tools such as firewalls, access control functions, logging and alerting systems for maximum efficiency and regularly test the same.
- Write process and procedures for all major procedures such as patch management, vulnerability management, Intelligence development, incident response and etc.
- Ensure that security is aggressively built into the enterprise architecture and requirements documents.
- Base security management on IT governance such as ITIL.
- Define security standards and policies.
- Ensure the basic security blocking and tackling is done before implementing.

Advanced tools and procedures:

- Use change control for all things that could affect the IT environment.
- Harden all platforms and applications against attack.
- Select a control environment such as SANS Top 20, FISMA, NIST 800-53, ISO 27000 series.
- Implement a superb patch management process that sets metric for current patch status at 95 per cent for all platforms, end points, data bases, applications, network devices and etc.
- Strictly limit administrative access and manage with privilege management tools.
- Monitor access in real time.
- Implement robust static and in transit data loss protection plans (DLP).
- Implement a robust secure software development program.
- 100 per cent compliance to government regulation and business compliance requirements like PCI.
- Conduct regular internal scans and pen tests using anyone of the host vulnerability assessment tools for platform and applications exposures.
- Implement a ongoing security training program that is not given once a year .
- Invest in training the security staff.
- Build robust security metrics briefed by the CISO to executives once a month to C level and once a quarter to Board level executives.
- Lead your staff and all organization personnel in data protection.

Detect attacks on an organization's assets:

- Prevent incidents from happening in the first place.

- Ensure a 24 X 7 detection capability is available.
- Deploy state of the art static and dynamic detection tools that your organization can fund.
- Define real time detection processes.
- Ensure employees are aware of how to report suspicious end point, platform and network intrusions.
- Extend detection to all BYOD and external systems.
- Manage threat detection in all cloud based services.
- Define SLAs for responding to threats.
- Determine which security systems should be in your DR and BC planning.
- Ensure you have managed out as many false positives and false negatives as possible.
- Use the CWE tools whenever possible <http://cwe.mitre.org/>. CWE is tuned to application security but it is an excellent but complex framework..

Respond to attacks on an organization's assets:

- Determine what the company's appetite for incident response is. Is it willing to accept automated shut down of business processes and network segments.
- Determine if you want to hire a DDoS threat mitigation service.
- Create and practice detailed incident response process.
- Define response thresholds based on the attack areas and magnitude of same.
- Ensure global partners and external business customers are aware of incident response processes.
- Define escalation process.
- Conduct table top exercises to train entire staff on incident response and cyber crises management.
- Contract with external forensics investigator.
- Ensure two incident management lines are established, one for executives and one for those doing the work to manage and terminate the incident.
- Develop and train on the RACI chart for incident management. Platform security incidents could possibly be managed by the platform manager.
- Train internal staff for forensics investigations.
- Conduct prior planning with all technical and CxO level staff.
- Know obligations and response procedures for such laws concerning a data breach. Let legal and marketing work the customer notification obligations.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

- Ensure incident response team is aware of all threat intelligence generated by the SOC.
- Ensure systems are configured to respond to attacks, is your IPS set to deny attacks.
- Oversee and be aware of all preventive measures that should prevent incidents from happening in the first place.
- Ensure that you have proper incident close out processes.

The below table shows C4ISR can apply within the intelligence cycle or mapped to the SANS Top 20 Operational Security Controls (Source: Bill Ross):

Intelligence Cycle Framework	Command	Control	Communication	Computers	Intel	Surveillance	Rece
Requirements	X	X	X	X	X	X	X
Planning and Direction	X	X	X	X	X	X	X
Collection				X	X	X	X
Processing and exploitation				X	X	X	X
Analyses and production				X	X	X	X
Dissemination		X	X	X	X	X	X
SANS 20 Critical Controls	Command	Control	Communication	Computers	Intel	Surveillance	Rece
1: Inventory of Authorized and Unauthorized Devices	X	X	X	X	X	X	

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



2: Inventory of Authorized and Unauthorized Software	X	X	X	X	X	X	
3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	X	X	X	X	X	X	
4: Continuous Vulnerability Assessment and Remediation	X	X	X	X	X	X	X
5: Malware Defenses	X	X	X	X	X	X	X
6: Application Software Security	X	X	X	X	X	X	
7: Wireless Device Control	X	X	X	X	X	X	X



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



8: Data Recovery Capability	X	X	X				
9: Security Skills Assessment and Appropriate Training to Fill Gaps	X	X	X	X	X	X	X
10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	X	X	X	X	X	X	
11: Limitation and Control of Network Ports, Protocols, and Services	X	X	X	X	X	X	
12: Controlled Use of Administrative Privileges	X	X	X	X	X	X	



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



13: Boundary Defense	X	X	X	X	X	X
14: Maintenance, Monitoring, and Analysis of Audit Logs	X	X	X	X		
15: Controlled Access Based on the Need to Know	X	X	X	X	X	
16: Account Monitoring and Control	X	X	X	X	X	X
17: Data Loss Prevention	X	X	X	X	X	
18: Incident Response and Management	X	X	X	X	X	X
19: Secure Network Engineering	X	X	X	X	X	
20: Penetration Tests and	X	X	X	X	X	X





Red Team Exercises





CHAPTER 3

SIEM & SOAR - Better Together

UNDERSTAND THE INTEGRATED FUNCTIONAL REQUIREMENTS BOTH FOR SIEM & SOAR SO THAT MAJORITY OF THE EVENT CORRELATION IS DONE AND PRESENTED TO YOU FOR YOU TO TAKE THE NEXT STEP

Managing security operations can be daunting and causes burnout for the analysts even faster, as security teams must deal with a large volume of alerts, a shortage of skilled analysts, and a lack of integration and automation across tools and processes. We will talk about the SIEM's capabilities which provide primary correlations of data as events, from where, the analysts take over each case.

Fortunately, there are two technologies in the market that's available right now that can help security teams overcome these challenges and improve their security posture: SIEM and SOAR.



What is SIEM?

SIEM stands for Security Information and Event Management. It is a technology that collects, analyzes, and correlates security data from various sources, such as network devices, systems, and applications. SIEM provides real-time visibility into the security status of an organization, by detecting anomalies, generating alerts, and supporting compliance and incident management.

SIEM is essential for security monitoring and threat detection, as it provides a centralized view of the security events and incidents across the organization. SIEM can also provide threat intelligence by identifying patterns and trends in security data and creating dashboards and reports for easy reference.

What is SOAR?

SOAR stands for Security Orchestration, Automation, and Response. It is a technology that streamlines and automates security operations, by integrating data and tools, prioritizing, and responding to alerts, and orchestrating workflows and actions. SOAR aims to improve the efficiency and effectiveness of security operations, by reducing manual tasks, human errors, and response times.

SOAR is essential for security response and remediation, as it helps security teams manage and resolve security incidents faster and more accurately. SOAR can also provide security automation and orchestration, by executing predefined actions and workflows based on triggers and conditions and coordinating tasks and resources across different teams and tools.

How SIEM and SOAR Work Better Together

While both SIEM and SOAR are valuable technologies for security operations, they are not mutually exclusive. In fact, they work better together, as they complement each other's capabilities and functions.

By integrating SIEM and SOAR, security teams can leverage the best of both worlds: SIEM's powerful data collection and analysis capabilities, and SOAR's advanced automation and orchestration capabilities.

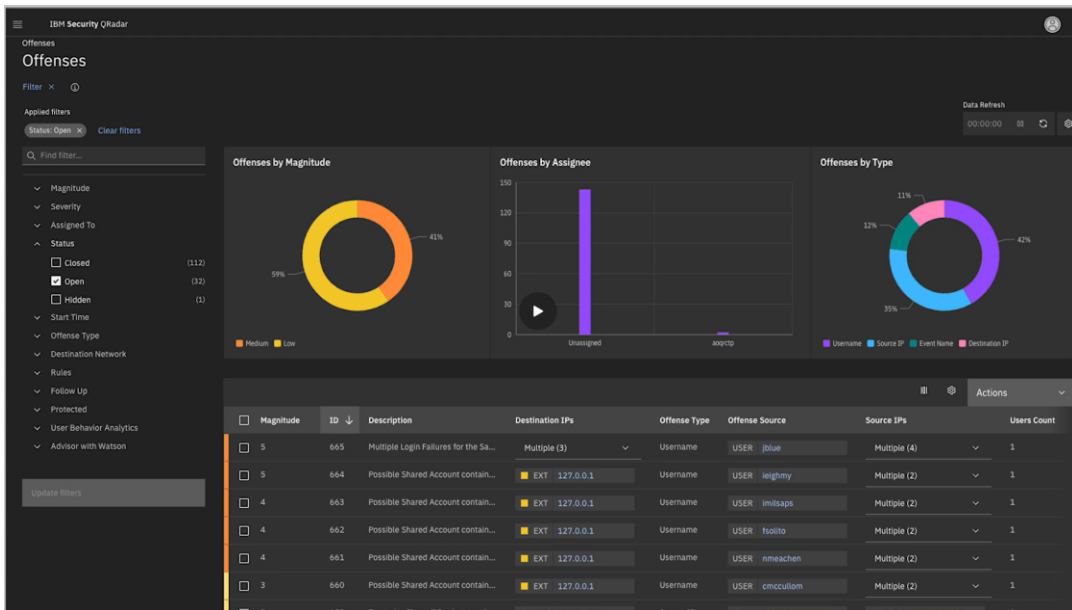
Some of the benefits of integrating SIEM and SOAR are:

- **Faster and more accurate threat detection:** SIEM can provide SOAR with rich and relevant security data, which SOAR can use to prioritize and respond to alerts more effectively. SOAR can also enrich SIEM data with additional threat


intelligence from external sources and provide feedback to SIEM to improve its detection accuracy and reduce false positives.

- **Faster and more effective threat response:** SOAR can automate and orchestrate the response actions and workflows based on the alerts generated by SIEM and execute them in a timely and consistent manner. SOAR can also coordinate the response activities across different teams and tools and provide SIEM with the status and outcome of the response actions.
- **Improved security performance and productivity:** By integrating SIEM and SOAR, security teams can reduce the workload and complexity of security operations and focus on the most critical and strategic tasks. SIEM and SOAR can also provide security teams with comprehensive and actionable insights into the security performance and metrics and help them optimize and improve their security processes and practices.

A screenshot of a SIEM: IBM QRader [IBM Security QRadar SIEM](#)



SIEM & SOAR Architecture



The below picture illustrates operational architecture of the SIEM & SOAR in an integrated function (the Visio file is provided in the Job Aids named “SIEM & SOAR Architecture”).

This is where the big picture comes in, from ingress to egress. As you can see in the picture the data collectors need to be configured in each device, either by agent or agentless or by default the OS or firmware has data plane, management plane and console plane pre-configured, and if you have the ERP or identical solution in place, they most likely have some sort of API or service wise and identifiable services that can be automatically scanned, configured to generate and produce actionable logs that can be fed into the SIEM & SOAR combined.

Now, that you have configured your data or log shipping to a central repository, you should have a data retention plan of how many days you need to keep them or to append them in a certain day or not. As it will prove to be a serious burden in longer times. When SIEM gets its hands on the logs, it starts correlations, and types of events are grouped together, to have a more meaningful insight. As the SIEM starts you will get a burst of events populated, don't worry, apply those visibility rules for data correlations. Ingestion rules will minimize the log correlations, and only when required, enable, or disable certain rules which is not required. Do remember, approve all documents, as the moment you have raised things for approval, it would be known to the SOC manager and to the SOC director, the moment you will not be asked or been accountable anymore.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER


SIEM & SOAR FUNCTIONAL ARCHITECTURE



Pro-Tip

In most cases, people do not configure SNMP with a custom public string, you must change that, have a naming convention in place in the policy framework, to identify and name each device (hostname) by its location, segments by racks, etc. into the DCIM as well. So that you can revisit those artifacts later, and fine tune its trap strings. Practice for a banner for network devices as well. This is particularly important, if an event is detected, the analyst will find the device where it's located and the escalation starts from there. This activity also relates to the ASM - Attack Surface Management.

Afterwards, SIEM and SOAR will continuously check for the rules for flow analysis, and will gather information for review and detection engineering takes place for the notifications, real-time alerts may take place or the event will go through alert analysis



and policy filtering, if the event is known or unknown kind. Data analysis finalized by deep investigation and a managed orchestration takes place within the integrated SIEM and SOAR to produce actionable results, and a case is generated with all of OSINT data, correlations, attack type mapping, and compliance mapping with kill-chain and actionable content put together for the analysts to take on a deeper investigation. Playbooks are then initiated for a manual case investigation, and by type, the rollout takes place. The identified source and its data can be quarantined in this phase should it required. A ticket gets generated with a severity class, hash data reviewed, remediated, and action API gets executed for KB generation and if a tune-up required for the data aggregation, it flags for a revisiting of rules for the defensive, offensive, forensic and deception automation services.

Any thoughts on disaster recovery on your SOC?

Since you are going to deploy a SOC, how would you deploy these SOC servers? Standalone mode? You should at least have multiple servers in HA mode with either in OS cluster or service cluster mode. I would recommend for the OS cluster mode and have a separate DB cluster as well for faster indexing and R/W requirements. And the primary requirements should be made, if one of the servers or VM is down, it should be automatically re-routed to another server as a replica VM, where operational effect must be zero.

Importance of Required Applications in a Disaster Recovery Plan

A disaster recovery plan is a strategy that helps organizations recover their IT systems and data after a disruptive event, such as a natural disaster, a cyberattack, or a human error. A disaster recovery plan is important because it ensures business continuity, resilience, and compliance. It also reduces the impact of data loss, downtime, and operational disruption, which are a core component of ERM, BCP & DRP.

This is not the end of the story, there are much design considerations that takes place all over your requirements which also defines

1. how data travels to multiple sites
2. network availability and lambda providers for a ring circuit
3. what types of operating systems needs data replication

4. software's are aware of replication stages, integrations and replication movement is smooth, steady and synchronous, while having witness server types to ensure steady heartbeat.
5. live data, data at rest, and geo located data replication and restoral services.
6. SDN capabilities that can prioritize policy based data transmission requirements
7. Lastly, security considerations

Pro-Tip

• try not to backup data if the sourc files cyclic redundancy check (CRC), MD5 cannot be confirmed. same goes with infected data storing.

These points need to be understood thoroughly and laid out within your infrastructure and readiness.

Some of the benefits of having a disaster recovery plan are:

- **Faster recovery time:** A disaster recovery plan outlines the steps and procedures to restore critical systems, applications, and data as quickly as possible after a disaster. This minimizes the duration and severity of business interruption and customer dissatisfaction.
- **Reduced data loss:** A disaster recovery plan includes backup and restore solutions that protect data from being corrupted, deleted, or stolen during a disaster. This prevents data breaches, legal liabilities, and reputational damage.
- **Enhanced resilience:** A disaster recovery plan prepares organizations for various types of disasters and scenarios, enabling them to adapt and respond effectively. This improves the ability to cope with uncertainty and change, and reduces the risk of failure.
- **Improved compliance:** A disaster recovery plan helps organizations meet the regulatory and industry standards for data protection and security. This avoids penalties, fines, and audits, and demonstrates the commitment to operational reliability and customer service.

Some of the applications that are associated with a disaster recovery plan are:

- **Backup and restore solutions:** These are tools that create copies of data and store them in a secure location, such as the cloud, a remote server, or a physical device. They allow organizations to retrieve and recover data in case of data loss or corruption.
- **Replication and synchronization solutions:** These are tools that create duplicates of data and systems and keep them updated across different

locations, such as the primary and secondary sites. They allow organizations to switch to the backup site in case of a disaster or outage at the primary site.

- **Monitoring and testing solutions:** These are tools that track the performance and availability of systems and data, and alert organizations of any issues or anomalies. They also allow organizations to test and validate their disaster recovery plan regularly and ensure its effectiveness and readiness.

Hot, Cold and Warm Sites

Disaster recovery sites are locations where a business can resume its operations after a disaster. There are three types of disaster recovery sites:

- **Hot site:** A location where the target environment is already up and running and can be immediately activated by a failover. This is the most expensive and reliable option.
- **Cold site:** A location where the target environment needs to be activated once a recovery process is initiated. This is the cheapest and least reliable option.
- **Warm site:** A location where the target environment has some components installed and configured, but not fully operational. This is a middle ground between hot and cold sites.

Consider your desired Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs):

- **RTO:** Time from disaster occurrence to system functionality.
- **RPO:** How far back in time data can be restored without affecting business continuity.

Assess your budget, criticality of data, and acceptable downtime to make an informed decision.

Some of The Disaster Recovery Application Platform

There are many disaster recovery applications available in the market, each with its own features and benefits. You need to drive a PoC to look out which application can send granular data to a DR site and can retrieve it with ease while maintaining data accuracy.

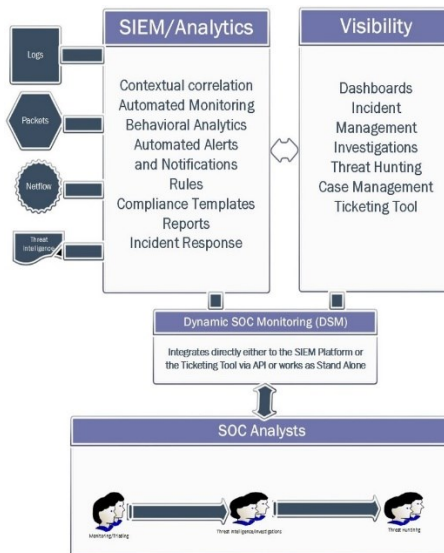
Some of the best ones are:

- | | | |
|-------------------------|-----------------------|------------------------|
| • Rubrik | • Redstor | • Zerto |
| • Druva Phoenix | • Stellar | • Bacula |
| • Acronis Cyber Protect | • Veeam Data Platform | • Enterprise CrashPlan |

- Commvault
- Veritas
- Arcserve
- Cohesity
- Dell Technologies

Benefits of a Functional Security Operations Center (SOC)

A SOC provides numerous benefits to an organization: some of them are listed below:



Source: [Typical SOC Workflow and How DSM Fits in \(Author's Diagram\) | Download Scientific Diagram \(researchgate.net\)](#)

Security Information and Event Management (SIEM) is a security solution that helps organizations recognize and address potential security threats and vulnerabilities before they have a chance to disrupt business operations. SIEM systems help enterprise security teams detect user behavior anomalies and use artificial intelligence (AI) (though every SIEM does not have this yet, but in a year they will have automated services as well) to automate many of the manual processes associated with threat detection and incident response. The primary functions of a SIEM solution are to aggregate, normalize, and correlate security events to provide a holistic view of all the activities that happen in an IT infrastructure. It ingests event data from a wide range of sources (firewalls, routers, switches, endpoints, printers (printers has HDD in it, and doesn't wipe its content automatically, as it saves the files being printed!), servers, applications, other IoT (Internet

of things (IoT)) sensors etc.) across an organization's entire IT infrastructure, including on-premises and cloud environments.


SIEM systems also integrate with third-party threat intelligence feeds to correlate their internal security data against previously recognized threat signatures and profiles. This integration enables teams to block or detect new types of attack signatures. SIEM systems categorize events and map them to a standard, then generate or invoke an incident ticket for the analyst to investigate the severity and take appropriate measures to remedy the event.

Pro-Tip

- The SOC does not make any changes to IT security assets or the infrastructure itself, which is the responsibility of the relevant division. These are informed by tickets. The SOC also takes care that tickets are worked on and closed in a timely manner. If not, the SOC agents will escalate to their supervisor.

As a company expands, so does its infrastructure and capacity. This includes routers, switches, physical servers, applications, gateways, and payment processing systems, which grows exponentially. As a result, you should expect numerous exposed ports, IP addresses, and access systems that require fine-tuning. In most cases, you would want to minimize the attack surface area to mitigate risks. SOC analysts are there to inform you of any visible attack scopes, so you can take appropriate measures, and some of them are:

1. **Continuous Network Monitoring:** Cybercriminals operate round the clock, often performing their attacks after hours or on weekends to maximize their probability of success. A SOC provides 24/7 monitoring of the organization's IT infrastructure and data, ensuring that security analysts and incident responders are always available.
2. **Centralized Visibility:** With the growth of digital transformation initiatives, enterprise networks are becoming more complex. A SOC provides centralized visibility into the network infrastructure and potential attack vectors, enabling an organization to effectively secure a diverse network.
3. **Reduced Cybersecurity Costs:** Maintaining strong corporate cybersecurity can be expensive due to the need for multiple platforms and licenses and obviously the cost of skilled manpower. A centralized SOC enables an organization to reduce these costs by sharing them across the entire organization.

- 
4. **Better Collaboration:** A SOC fosters better collaboration among security professionals, enabling a more coordinated and efficient incident response process.
 5. **Faster Threat Detection and Response:** By using a combination of manual and automated tools, a SOC can more quickly detect and respond to security threats.
 6. **Proactive Defense:** A SOC provides proactive defense against incidents and intrusions, improving security incident detection and reducing incident response times.

24/7 Staffing Requirements for the CSOC Monitoring

A 24/7 Cybersecurity Operations Center (CSOC) requires a well-structured team of security professionals to ensure continuous monitoring and response to security threats. Here are the key roles typically required:

- **CSOC Manager/Director:** This is the person in charge of the entire operations. They oversee the SOC's activities, manage the team, and make critical decisions.
- **Security Analysts:** These are the frontline workers in a CSOC. They monitor security events, analyze alerts, and investigate security incidents. Security analysts are often divided into tiers (Tier 1, Tier 2, etc.) based on their expertise and responsibilities.
- **Incident Responders:** They are responsible for managing and responding to security incidents.
- **Threat Intelligence Analysts:** These analysts gather and analyze information about emerging threats to help the organization stay ahead of potential attacks.
- **Security Engineers:** They are responsible for maintaining and improving the SOC's security infrastructure.

The exact staffing requirements can vary depending on the size and needs of your organization. It's also important to note that staffing a CSOC is not just about the number of personnel, but also about their skills, training, and tools they have at their disposal, and you should have at least n+1 on the critical roles. You should have rotating personnel, on-call status, load balancing with a minimal set of analysts and scaling that based on log ingestion.

So, You Want to be a CISO?

So, you should, let me tell you why. If you are learning your trade in developing computing environment discipline, you should know the path what to do, where to go, job aids that will provide you the necessary tools, learning to reach your goal, therefore, plan early as well. As you can understand that this is not going to happen overnight, and your "Want"



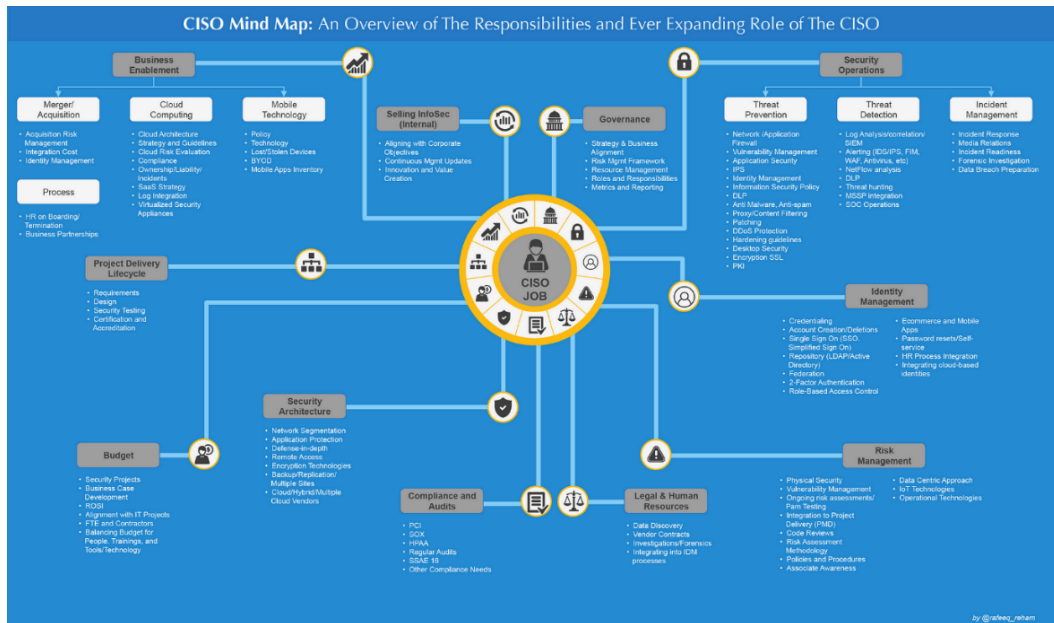
COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

and your "Need" for this will fuel your journey on how badly you want this. Do remember, if you are not doing it, someone else will, and each step you take today, will become the knowledgebase and experience to support you tomorrow, and do spend more than a dollar on yourself, make a monthly plan according to your ability, later on, you will find out that these hard earned knowledge is invaluable throughout your life, that pays *throughout* your life.

Here is some domain knowledge a CISO shall have even though you are starting out as a PC builder and gradually you started integrating networks across the region, and then BAM! You are now in the ocean of information that needs protection services to protect the data. And in the future, you should be able to derive server specs, develop BoQ accordingly with network devices as well.

This picture is derived from Rafeeq Rehman's CISO mind map, represented by Cobalt.io:

1. Rafeeq Rehman's CISO MindMap: [CISO MindMap 2023: What do InfoSec Professionals Really do?Rafeeq Rehman | Cyber | Automation | Digital](#)
2. Cobalt.io: [ciso mindmap - Search Images \(bing.com\)](#)
3. SANS CISO Mindmap: [download \(sans.org\)](#)



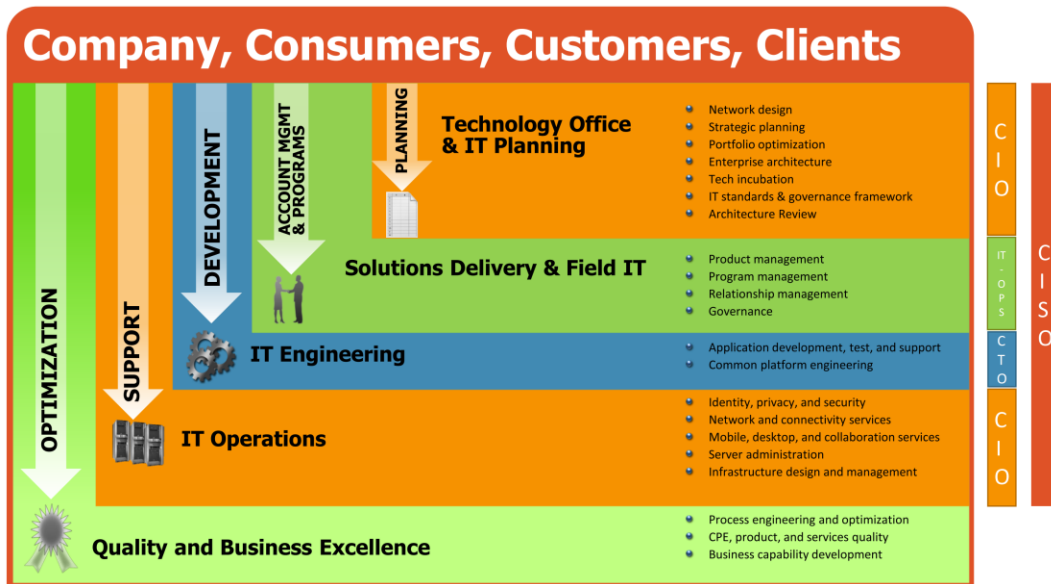
The above illustration clearly defines the responsibilities of a CISO, but somehow, he/she reports to the CIO, maybe I am wrong, but my understanding is that, all of the roles of a CIO (network architect - infrastructure background), CTO (software architect - comes from developer background) roles falls also into the CISO roles.

Pro-Tip

•CISO role also includes 360-degree coverage of the infrastructure, transmission security, networked devices security, application platform, device's configuration security, IoT devices, SCADA (Supervisory Control And Data Acquisition) and PLC device security and much more, and in many cases, CISO role outperforms CIO, CTO roles in many organizational layers. Maybe I am too bold to claim this, but industry will depict and things will change.

In most cases, the technology team is seen as a cost center. Whether the team is developing or producing sellable products or not, developing, implementing, and supporting the whole infrastructure; and the historical journey is taught in that way, and till today management team & CEO's perceived understanding is still smirking in their brain.

My thought – other than the technology personnel, sales & marketing, finance, distribution channels all of these organizational units are the cost centers, as you are paying them a hefty amount of salary (lesser salary for the tech guys, where you are asking to deliver a world for the company, and you lay-off whenever the financial calculation says it's better to have one senior guys and lay-off four and there will be a salary savings! For the organization?), incentives to sell your product (that were created by the technical folks) ...that's how things are, but these perspectives are changing. And yes, we are poor by nature and our extreme capabilities are not intentionally heard by the management at all.



Source: unknown

As we are going to dig deep of how the SOC is formulated and how effectively it's going to help us secure the organizational aspects of their data, access and assets, one thing that tops on all aspects is the mindset of the personnel who would be engaged in the SOC operations, do follow these tips:

1. Ethics rules the game.
2. Document, document and document, and lastly document everything that needs a lineup, layout processes, functions, roles, activities, tasks. Reminder: skills requirements and daily activities are two different things, which never lines up or mentioned in the JD that you have accepted, but now things are changing, but slowly, ask for your daily activities list from the HR or from you line manager.
3. Do not intake any rockstar, tends to deviate from the goal, and affect all the surrounding personnel and their activities, even mind shift takes place. Try to look for an activated brain, juniors are the best, mix different types of blood, who can be taught without any conservation, but do remember seniors are the ones who are playing the mentor role.
4. Rules, processes, functions, activities go for everyone, no exceptions. If the CxO's thinks that these rules don't apply to them then make them accountable for such workarounds

5. Every level of activities needs to be precise; workflow must be in place for L1, L2, L3. Tabletop exercise goes a long way, engrave these processes to the engineers, and always fine tune your activities, lower the engagements on events, known or unknown, reduce analyst burnouts.
6. People will grow to become L2 and L3, let them grow, they are human beings, they also have all the problems of life just like you. Feed them knowledge of how they can become their best self. Give them ways to grow, do remember, salary is never equal to your effort, your knowledge is.

Dunning-Kruger Effect – The Imposter Syndrome

The Dunning-Kruger effect is a type of cognitive bias in which people believe they are smarter and more capable than they are. Essentially, low-ability people do not possess the skills needed to recognize their own incompetence. The combination of poor self-awareness and low cognitive ability leads them to overestimate their capabilities. Incompetent people, the researchers suggested, were not only poor performers but were also unable to accurately assess and recognize the quality of their work. This effect can have a profound impact on what people believe, the decisions they make, and the actions they take.


Another contributing factor is that sometimes a tiny bit of knowledge on a subject can lead people to mistakenly believe that they know all there is to know about it. As the old saying goes, a little bit of knowledge can be a dangerous thing.

Some effects:

- Overestimate their skill levels.
- Fail to recognize the genuine skill and expertise of other people.
- Fail to recognize their own mistakes and lack of skill.

Dunning-Kruger Effect vs. Imposter Syndrome: So, if the incompetent tends to think they are experts, what do genuine experts think of their own abilities? Dunning and Kruger found that those at the high end of the competence spectrum did hold more realistic views of their own knowledge and capabilities. However, these experts tended to underestimate their own abilities relative to how others did.

I really hope that these kinds of personalities are absent in the security industry, and learning from them will prove to be hazardous. The best action is to stay away from them. I have observed some individuals who are somehow with the technical team and learned some scenarios and some acronyms and they started lecturing about the things they are unaware of! Do stay away from such characters, and if you are in a position to



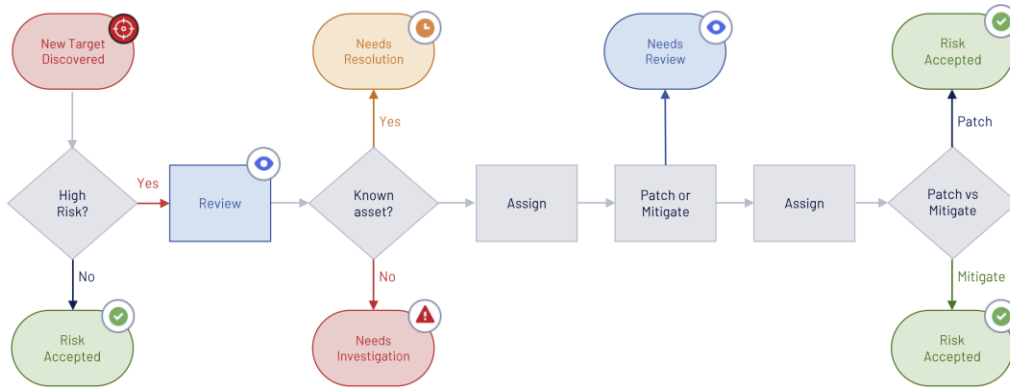
hire someone, do skip them, identify early, and you should be a better judge of a character for selecting your teammates.

Attack Surface Management (ASM)

As business requirements expand and wherever your solution resides either in a collocated datacenter or in the cloud, the ever-growing need for security is endless. The application platform and its portals for different OU's, access to those portals, networked devices, endpoints, servers, firewalls, routers, switches, load balancers etc. these devices needs the benchmarked configurations in place which also needs regular assessment to check for vulnerabilities, as patches takes place and undoubtedly every patch management calls for a recalibration of configurations as it enables more features and a re-assessment is required to know if the patch is enabling something unwanted or unaccounted for. As for a different ASM team regularly performs these operations to gain visibilities on the mentioned devices, since it is critical for the detection team to mitigate of increasing risks, and this functions also reduces SIEM notifications in the first place, where it's also a burden for the SOC analysts. The ASM team's primary function is to identify and notifies the security operations team of any vulnerabilities so they can work with either enterprise affiliates to decommission servers or security affiliates to retire legacy systems that exposes increased vulnerabilities, which are simply unpatchable. Decommissioning of those devices is undertaken by a different team who are the owner or the custodian. Use case of ASM team (Source: [SANS Webcast- Evaluating Attack Surface Management 116765 by Pierre Lidome](#)):

- Identifying external gaps in visibility.
- Discovering unknown assets and shadow IT.
- Attack surface risk management.
- Risk-based vulnerability prioritization.
- Assessing M&A and subsidiary risk.

Operational workflow of the ASM Team



Implement Risk Based Vulnerability Management

Vulnerability management is not just about fixing systems and applications. It involves a comprehensive process that covers patching, alternative controls, network design, isolation, and enhanced security monitoring.

Technology is constantly evolving and so are the vulnerabilities, it's a forever journey. Trying to eliminate them all will take up all your department's time and resources. And your efforts will soon become outdated as new vulnerabilities will emerge. What's more, some systems are simply unpatchable (old systems that simply don't have the latest firmware or capability within the hardware and in the OS, as they went EoL).

The key is to assess the vulnerabilities and the risks they pose to your organization, to prioritize wisely and to look for other solutions besides patching. A risk-based approach to vulnerability management will help you focus on the most important issues and safeguard the business. Minimize the potential risk exposure. Some outline could help you formulate the requirements:

Initiate & describe the project by creating a vulnerability management team and determine how vulnerabilities will be identified through scanners, penetration tests, third-party sources, and incidents that were already took place or that you know of, or the potential exposure of assets. It may sound simple to address but the insights can be:

- a. Develop an SOP for vulnerability assessment & penetration testing.
 - i. Vulnerability tracking.
 - ii. Vulnerability risk assessment.
 - iii. Vulnerability workflow.

- iv. Vulnerability management policy.
 - b. Identify vulnerability sources.
 - c. Triage vulnerabilities and assign priorities.
 - d. Remediate vulnerabilities.
 - e. Measure and formalize.

In the landscape where cyber threats have become very common, traditional vulnerability management may fall short of addressing the most critical risks in the organization. Adopting a risk-based approach allows us to prioritize vulnerabilities based on their potential impact, enabling us to allocate resources efficiently and effectively. Key Components of Risk-based Vulnerability Management

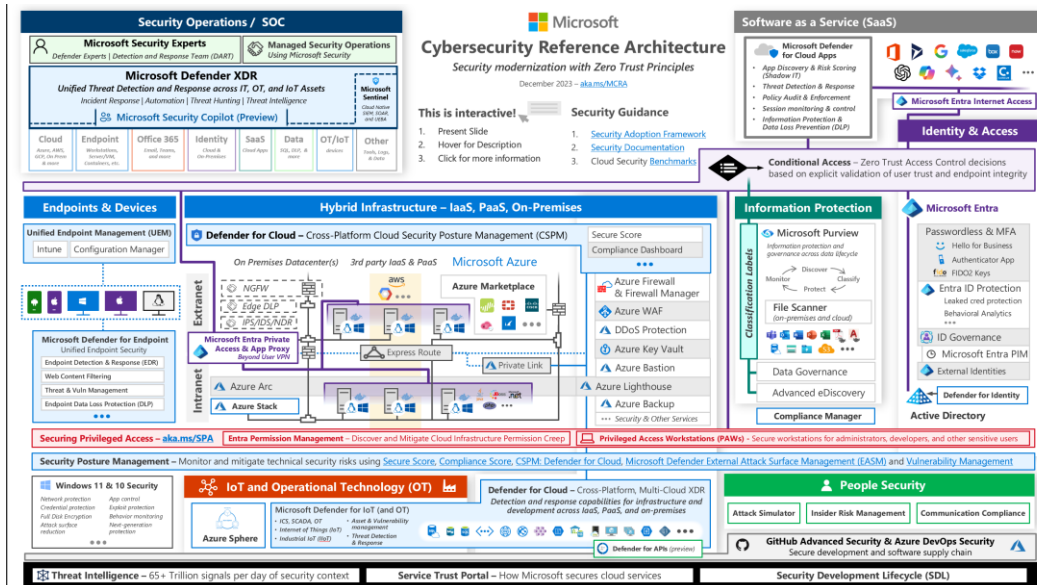
1. **Risk Assessment:** Conduct thorough risk assessments to evaluate vulnerabilities in the context of your specific environment, business processes, and critical assets.
2. **Prioritization:** Prioritize vulnerabilities based on the risk they expose, considering factors like exploitation, potential impact on the operations, and the value of the affected devices.
3. **Continuous Monitoring:** Establish a continuous monitoring system to keep track of emerging threats and promptly respond to new vulnerabilities that may arise.
4. **Mitigation Strategies:** Implementing effective mitigation strategies that address identified vulnerabilities, whether through patches or other proactive measures.

By embracing risk-based vulnerability management, you can enhance your cybersecurity and minimize the impact of security threats.

Cybersecurity Reference Architecture by Microsoft

Reference architectures are crucial since they form the foundation for all systems and integrations. As the saying goes, 'If you think good architecture is expensive, try bad architecture.' We want to avoid bad architecture since it can lead to significant costs over time and cause the organization to suffer. It's important to correct and avoid deploying unconventional methods that may be hazardous.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Source: [Microsoft Cybersecurity Reference Architectures \(MCRA\) - Security documentation | Microsoft Learn](#)

A reference architecture provides detailed description of a company's mission, vision, and strategy. It helps to establish a shared understanding across multiple products, organizations, and disciplines about the current architecture and the future direction. Reference architectures are important because they standardize language and organizational context, making it easier to solve problems by implementing clear guidelines. They also provide resources for designing IT architecture, teams, and solution requirements.

Pro-Tip

• A good architected infrastructure built with security in mind and framework standards are applied, will prove to be stable in time. and there is a picture in the web saying that "If you think good architecture is expensive, try bad architecture". Though its not recommended, do verify with OEM's for the design effectiveness, and transmission capabilities, always try to use validated designs.

If you have built out a SOC where the infrastructure architecture is out of balance, fix those problems first, please. You will go nowhere with those problems attached to your

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



SOC as a dog-tail. Some of the assessments of infrastructure job-aids are shared and you can find the link at the bottom of the book.





CHAPTER 4

SOC Functions

I AM WITH YOU THROUGHOUT THE BOOK AS A FRIEND AND A TECHNICAL ADVISOR, AS THINGS GETS COMPLEX, JUST TRY TO UNDERSTAND THE PURPOSE OF THESE PROCESSES, THEY ARE LAID OUT FOR A REASON, ONCE YOU UNDERSTAND THE 'REASON', YOU CAN GENERATE NEW REASON AS WELL.

The primary functions of a SOC solution are to aggregate, normalize, and correlate security events to provide a holistic view of all the activities that happen in an IT infrastructure. It ingests event data from a wide range of sources across an organization's entire IT infrastructure, including on-premises and cloud environments. Event log data from users, endpoints, applications, data sources, cloud workloads (on-cloud or on-prem), and networks, data from security hardware and software such as firewalls or antivirus software—is collected, correlated, and analyzed in real-time in conjunction with threat intelligence mapping and provided a severity score. These scores

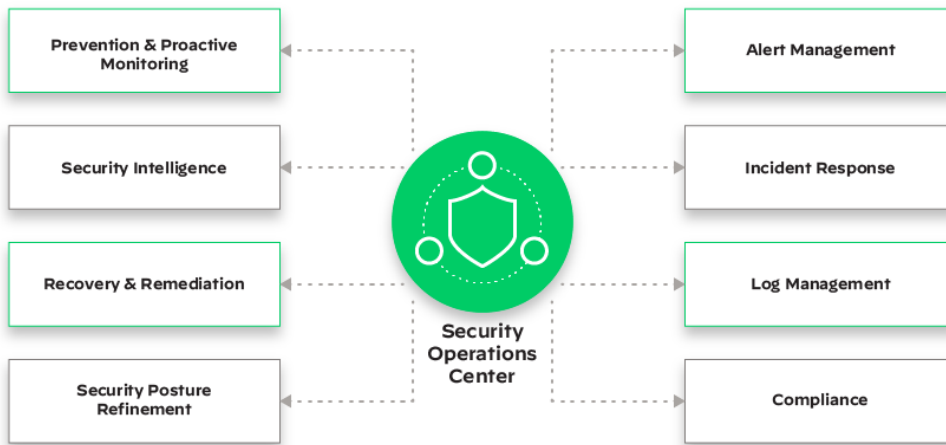


COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

also will be mapped to ISO/IEC 27001, MITRE, PCI-DSS and other standards, if you have a mapping of event to standards, which can correlate with those.

Most of the functions are derived from CISO provided guidelines or can be combined from collected data from experienced SOC personnel, whichever works, a manual or following standards & frameworks (there is none!) on how to do it right at the first time and all the time.

SOC FUNCTIONS



Source: [What Is a Security Operations Center \(SOC\)? - Palo Alto Networks](#)

It is of paramount importance that your perception is limited to your knowledge, not trying to achieve an insulting effect, but it's true to the core, and when you realize this, I can guarantee you that you already know much, and knowledge can be grown, skills can be taught, but look for aptitude that makes us technical people, a highly effective personnel, because of their extreme competencies, and reason why I salute you, my peers. Collaboration is always the key, no matter what you say, how you present, or how many times you have documented, keep doing it, that's the right way, and a peer who knows better, make sure you tag along with those folks, they came to peering as a blessing, not a threat. And ask for help!

That's how a SOC manager should perform, keep learning from each other, fine tune all the processes, try making it shorter, and do share and give back, that's how you grow. Set your ego aside, it's doable.

Open Security Architecture (OSA) Architecture Patterns

OSA can provide benefits to IT service consumers, IT service suppliers and IT vendors, giving the entire IT community an interest in using and improving.

- IT service consumers need to integrate diverse architectures from many suppliers in complex chains. They win using OSA because they can better specify or assess services or products they purchase and improve the quality of products they build. They can reduce knowledge risks from the architecture being in the supplier's control. Additionally, they increase confidence in the ability to integrate services, improve conformance with GRC requirements and reduce audit costs.
- IT service suppliers want to supply services to the maximum number of consumers, minimizing the cost to specify, implement and operate, while ensuring that the services meet the consumers' requirements. They win using OSA as they can provide conformant solutions at the least cost to the largest market.
- IT vendors want to supply products that meet market needs and have a low TCO for the IT service supplier that will operate. They win using OSA as they can build systems with relevant and appropriate controls.

From the landscape you can derive or readily view your perspective on the provided landscapes, a screenshot follows for the "SP-011: Cloud Computing Pattern". Each numbered item is clickable and lands you to the description (and now you have a gold mine for you to map out the business architecture mapping to your cybersecurity architecture and a complete mapping can be generated):

Actor: Architect

- AC-04 Information Flow Enforcement
- SA-04 Acquisitions
- SA-05 Information System Documentation

Actor: Business Mgr

- RA-03 Risk Assessment
- RA-04 Risk Assessment Update
- SA-02 Allocation Of Resources

Architects & Mgrs agree on baseline, map to providers control framework and agree on minimal set of metrics / observables

AC-04 Information Flow Enforcement

Control: The information system enforces assigned authorizations for controlling the flow of information in accordance with applicable policy.

Supplemental Guidance: Information flow control regulates where information is allowed to travel (opposed to who is allowed to access the information) and without explicit regard to subsequent access restrictions that are better expressed as flow control than access control are: keeping external traffic from entering the organization, blocking outside traffic that claims to be from within the organization, and not passing external traffic through proxies. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information (e.g., networks, individuals, devices) within information systems and to control the characteristics of the information and/or the information path. Specific examples of flow control include: proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or engines to filter traffic or provide a packet filtering capability. Related security control: SC-7.

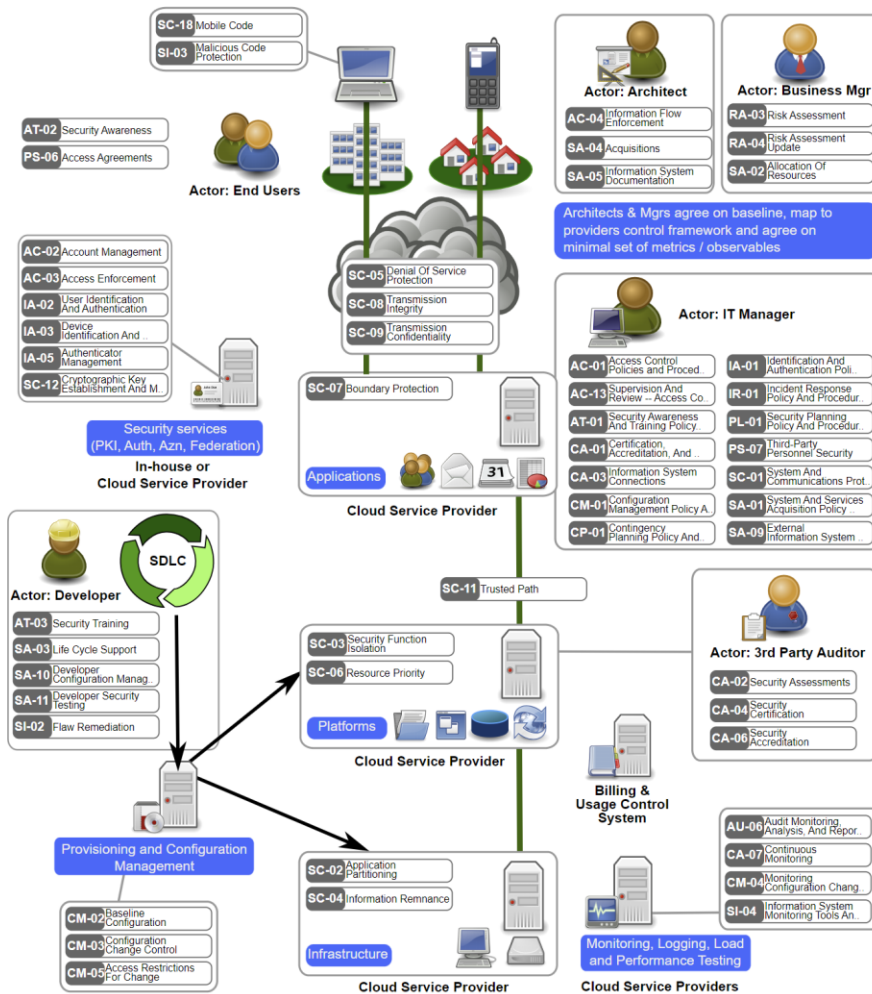
Control Enhancements:

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

- Total Control Catalogue: [Control Catalogue \(opensecurityarchitecture.org\)](https://opensecurityarchitecture.org)
- Patterns Landscape: [Pattern Landscape \(opensecurityarchitecture.org\)](https://opensecurityarchitecture.org)
- Threat Catalogue: [Threat Catalogue \(opensecurityarchitecture.org\)](https://opensecurityarchitecture.org)

SP-011: Cloud Computing Pattern

Diagram:

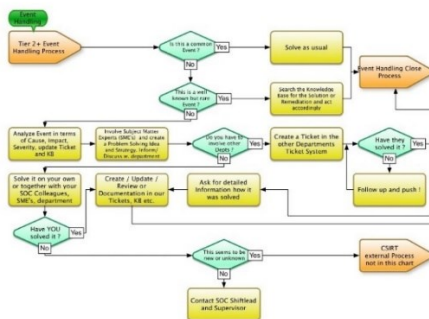
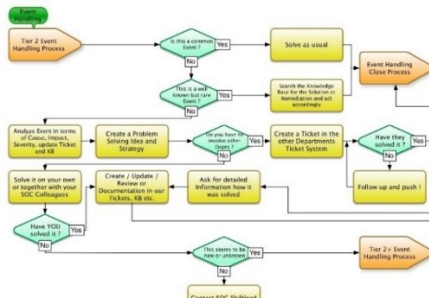
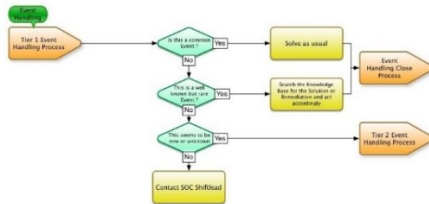
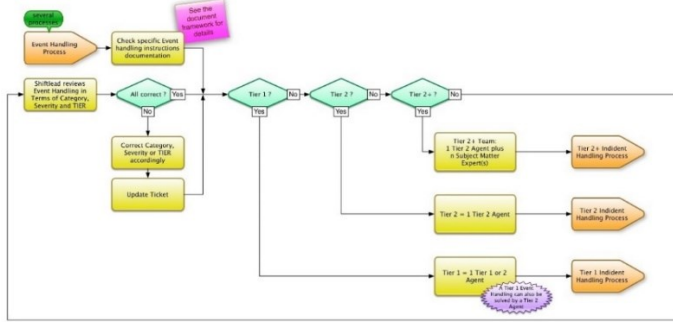


08_02_Pattern_011_15_Cloud_Computing.svg
 OSA is licensed according to Creative Commons Share-alike.
 Please see: <http://www.opensecurityarchitecture.org/cms/community/license-terms>.

Source: [SP-011: Cloud Computing Pattern \(opensecurityarchitecture.org\)](https://www.opensecurityarchitecture.org/patterns/SP-011-Cloud-Computing-Pattern)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

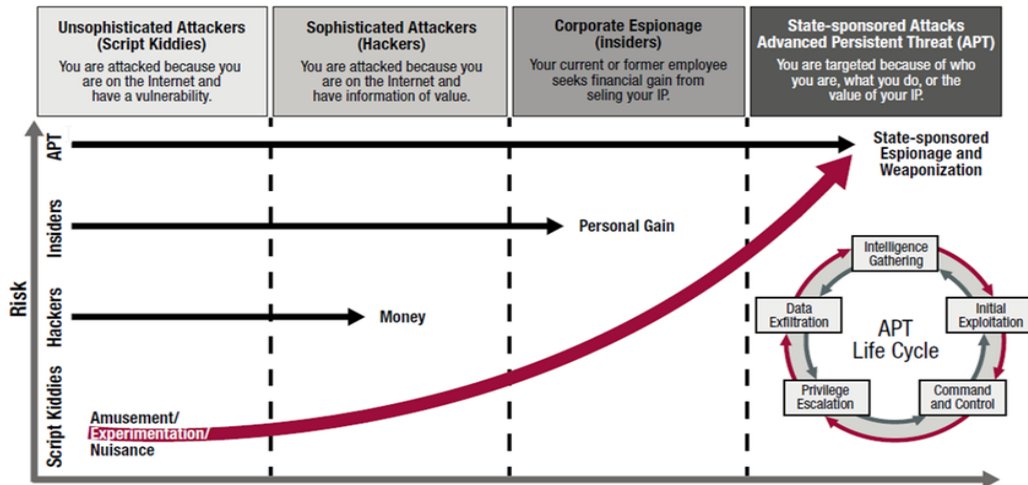
SOC Methodology



Source: [The SOC methodology - SecureGlobal](#)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

In summary, a functional SOC is central to curbing cybersecurity threats that can cost businesses significant amounts in lost revenue and data breaches.



Source: [how threat landscapes have evolved | Download Scientific Diagram \(researchgate.net\)](#)

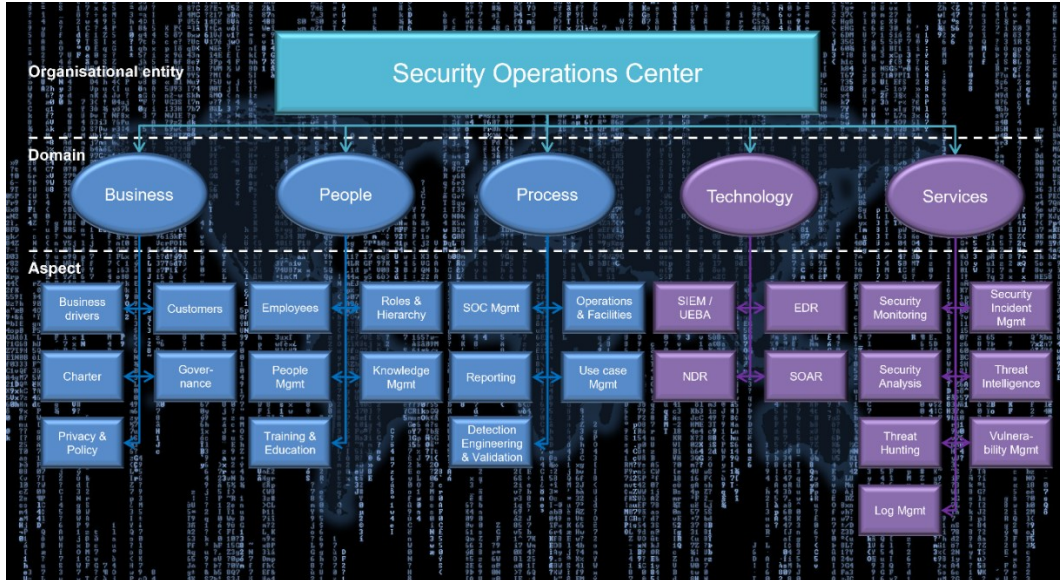
According to a report by Kaspersky ([Cybersecurity in the AI era: How the threat landscape evolved in 2023 | Kaspersky](#)), the use of AI by cybercriminals has become more prevalent in recent years, with AI tools being used to help them in their malicious activities. The report also highlights the potential defensive applications of AI technology. As technology continues to evolve, new vulnerabilities and exploits are discovered, and attackers change their tactics to exploit them. The global threat landscape is in a constant state of flux, with geopolitical instability, newly discovered exploits and vulnerabilities, and constantly evolving tools and shifting targets all contributing to attackers changing their modus operandi. As a result, it is essential for organizations to stay up to date with the latest security trends and technologies to protect themselves from emerging threats.

SOC – Capability Maturity Model (SOC-CMM)

The SOC-CMM model was initially created as a scientific research project to determine characteristics and features of SOCs, such as specific technologies or processes. From that research project, the SOC-CMM has evolved to become the de-facto standard for measuring capability maturity in Security Operations Centers. At the core of the assessment tool lies the SOC-CMM model. This model consists of 5 domains and 26

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

aspects, that are each evaluated using several questions. The domains 'Business', 'People' and 'Process' are evaluated for maturity only (blue color), the domains 'Technology' and 'Services' are evaluated for both maturity and capability (purple color). (Got really lazy here, cited from source SOC-CMM directly)



Source: [SOC-CMM - Measuring capability maturity in security operations centers](#)

You can download all the excel files from here, and its also provided in the job aids: [SOC-CMM - Downloads](#)

Cybersecurity by Bill Ross

A handful of documents available for you to look into, as those guides are invaluable towards my understanding the domain of SOC from architecting to developing SoP, they can be found here:

[Bill Ross | The Catholic University of America - Academia.edu](#)

Some of his very useful contributions are:

1. Cybersecurity Architecture Management System Design CSAMS
2. Cyber Security Frameworks Like the NIST Cyber Security Framework or CSF
3. Cyber Security Architecture Development

4. Security Operations Center (SOC) or Strategic Operating Procedure
5. Cybersecurity Tools

NOC & SOC Visibility Requirement

Every Hardware, Operating Systems, Virtual Machines, Applications must enable the enterprise grade compliance visibility & reporting services which aids for capacity planning & management as per ISO-20000, ISO-27001, ISO-22301, CISESECURITY, ITIL, COBIT, Q4IT, PCI-DSS report generation, which requires data collection from various HW & SW sources (IT Governance). Full Admin (root & admin) access for various agent installations for the following services both for Windows & Linux Systems: (this is not an exhaustive list):

Primary visibility requirements:

1.  People
2.  Processes
3.  Technology
4.  Affiliations
5.  Business
6.  Visibility

And the SOC visibility requirements (a 49 point visibility requirements, change as you see fit, copy the spreadsheet and paste into an excel file):

NOC & SOC Visibility for Infrastructure Monitoring					
SL	Description of the Service Requirement	Modality	App Provisioning in Place?	NW-HW Provisioning in Place?	Adoption Capability
1	Activate and monitor all Networked devices, Linux Systems Audit Services, especially for developer's computers, physical and virtualized servers, AAA services etc.	Outside of the network monitoring	NO	NO	Capable

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



2	Firewall visibility of each service access per resources	Outside of the network monitoring	NO	NO	Capable
3	Cloud Services – CloudFlare (WAF) (CASB)	Outside of the network monitoring	NO	NO	Capable
5	Code Repository Access & Violations Records	Outside of the network monitoring	NO	NO	Capable
6	Linux Software Update & Patch Management	Outside of the network monitoring	NO	NO	Capable
7	Antivirus for Linux servers	Outside of the network monitoring	NO	NO	Capable
8	Monitor Application Services for <ol style="list-style-type: none"> 1. Transaction & Settlement Services 2. Payment Gateways 3. Micro Services 4. Containers, pods etc. 5. Various other services etc. 	Outside of the network monitoring	NO	NO	Capable
9	DAM - Database Activity Monitoring	Outside of the network monitoring	NO	NO	Capable
10	DPM - Database Performance Monitoring	Outside of the network monitoring	NO	NO	Capable
11	Monitor FTP services, where users can send files over the internet	Outside of the network monitoring	NO	NO	Capable
12	Memory Consumptions per Service	Outside of the network monitoring	NO	NO	Capable



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



13	Total hardware resource usage per VM and host OS	Outside of the network monitoring	NO	NO	Capable
14	Data collection for SIEM and internal threat management for Violations Records	Outside of the network monitoring	NO	NO	Capable
15	FIM - Data collection for File Integrity Monitoring	Outside of the network monitoring	NO	NO	Capable
16	Data collection for Access, Change Management	Outside of the network monitoring	NO	NO	Capable
17	SNMP Services for service data Collection	Outside of the network monitoring	NO	NO	Capable
18	Enroll to central Identity and Access Management (SSO-LDAP & IPA)	Outside of the network monitoring	NO	NO	Capable
19	APM - Data collection for Application Performance Management	Outside of the network monitoring	NO	NO	Capable
20	Data collection for Application Security Leakage Management	Outside of the network monitoring	NO	NO	Capable
21	APT - Data collection for Advanced Persistent Threat Management	Outside of the network monitoring	NO	NO	Capable
22	PAM - Data collection for Privilege Access Management	Outside of the network monitoring	NO	NO	Capable
23	ITAM - Data collection for IT Asset Management	Outside of the network monitoring	NO	NO	Capable
24	DRM - Data collection for Digital Rights Management	Outside of the network monitoring	NO	NO	Not Capable



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



25	CASB - Data collection for Cloud Access Security Broker	Outside of the network monitoring	NO	NO	Capable
26	SDWAN - Data collection for Software Defined WAN service Management	Outside of the network monitoring	NO	NO	Not Capable
27	SDDC - Data collection for Software Defined Datacenter Management	Outside of the network monitoring	NO	NO	Not Capable
28	OSINT - Data collection for Open-Source Intelligence to stop software leakage (software can send small chunks of data to cloud storage, stealing code/data)	Outside of the network monitoring	NO	NO	Not Capable
29	UEBA - Data collection for User Entity Behavioral Analytics to stop various types of leakage	Outside of the network monitoring	NO	NO	Not Capable
30	UEM - Data collection for Unified Endpoint Management, to secure and controlling desktop computers, laptops, smartphones and tablets in a connected, cohesive manner	Outside of the network monitoring	NO	NO	Capable
31	EDR - Data collection for EndPoint Detection and Remediation, records, and stores endpoint-system-level behaviors, use various data analytics techniques to detect suspicious system	Outside of the network monitoring	NO	NO	Capable



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



	behavior, provide contextual information, block malicious activity, and provide remediation suggestions to restore affected systems				
32	EMM - Data collection for Enterprise Mobility Management	Outside of the network monitoring	NO	NO	Capable
33	HCI - Data collection for HyperConverged (high density server hosting) Infrastructure	Outside of the network monitoring	NO	NO	Capable
34	ACI - Data collection for Application Centric Infrastructure development	Outside of the network monitoring	NO	NO	Capable
35	SOAR - Data collection for Security Orchestration And Remediation for finding root causes of incidents that cannot be identified for sophisticated attacks	Outside of the network monitoring	NO	NO	Not Capable
36	DLP - Data collection for Data Loss Protection	Outside of the network monitoring	NO	NO	Not Capable
37	DCIM - HW & SW Data collection for Datacenter Infrastructure Management	Outside of the network monitoring	NO	NO	Capable
38	ITIL Services: This is a complete 360 view requirements which is too big to cover in short.	Outside of the network monitoring	NO	NO	Capable





39	IRM - Incident Response & Management	Outside of the network monitoring	NO	NO	Capable
40	Application Software Security	Outside of the network monitoring	NO	NO	Not Capable
41	Data Protection	Outside of the network monitoring	NO	NO	Partial
42	Maintenance, Monitoring and Analysis of Audit Logs and Generate Flags according to Severity	Outside of the network monitoring	NO	NO	Capable
43	Configuration Benchmarks	Outside of the network monitoring	NO	NO	Capable
44	Developer Desktop Enrollment for SSO & Security Audit	Outside of the network monitoring	NO	NO	Capable
45	List of Software Allowed in the Developer's Computers	Outside of the network monitoring	NO	NO	Capable
46	Kubernetes & Container Security Scanner	Outside of the network monitoring	NO	NO	Capable
47	VAPT for External and Internal API	Outside of the network monitoring	NO	NO	Capable
48	Application services, ports, internal API monitoring	Outside of the network monitoring	NO	NO	Capable
49	All Clusters of the Internal Network	Outside of the network monitoring	NO	NO	Capable



Integrated Intelligence for a Threat-informed Defense

A good blend of human intelligence and powerful automation provides real-time visibility into your organization's ability to manage threat exposure. Offensive engagements are

somewhat customized to meet your needs and security posture maturity level and can scale to address even the largest, most complex environment. I would not recommend this offensive approach differently, as the mentality that drives this type of operation always leads to increased incoming threats, as you would be testing hacker's ability to penetrate your defense. But in a government or in a military installation it may be required to withstand and counter-attack your threat sources.

- **IAM (Identity & Access Management):** Please be mindful that in most cases Windows servers needs to be enrolled as a member server of an Active Directory or any popular LDAP (Lightweight Directory Access Protocol) providers, and Linux servers should have identical authentication systems like FreeIPA.
- **HSM servers:** Hardware security modules, where Thales has the most supported appliances which can be used to key or token generations for your applications, meet various FIPS requirements etc.
- **Cloud security:** Ensure a secure, efficient cloud infrastructure through comprehensive assessments.
- **PLC, SCADA, IoT, ICS:** Streamline your design or all the PLC devices, and do not put your devices into a standard networking device. Rather, use industry standard frameworks like IEC 62443-2-1 to reduce the vulnerabilities. Since we are talking about cyber security, it is good practice to have device's configuration checked, once it is updated or reconfigured.
- **Device configurations:** In many ways, IT folks are not used to have benchmarked configurations, they simply configure what needs to be done to achieve a primary functionality leaving the device prone to attacks. You should consult with a practitioner on the benchmark configurations or take professional services, or you can go to the CISEcurity site and download the benchmarked configuration files freely available.
- **Real-IP usage:** In any case, the lower usage also reduces your footprint in the internet. Properly designed secured gateways coupled with WAF or CASB (Cloud Access Security Broker) would provide significant protection. Do remember that every vendor's device can come with infiltration chips that cannot be detected by your firewalls, therefore, it is of paramount importance that the circuit level understanding is a must trait before a solution is derived.


Pro-Tip

• If you have internet facing mobile application or web enabled sites where the back-end has user login portals, its always best to have a contract with your chosen CASB provider, therefore, the first landing or access to your resource would be guarded by your CASB, protecting millions of unwanted hits from the first line of defense, if something still gets through, there should be your routers ACL, and then the firewall, afterwards you can have your packet shapers.

- **Operating system security:** Ensure that a set of instructions is in place for which type of OS is required for which purpose. Constant patch management is also the key to reducing threats.
- **Application security:** Streamline your journey to secure application design beginning with security principles that reduce risk.
- **API Security:** This type of communication method exposes the API whereabouts and without proper transmission protection or SDN capabilities, very little can be ensured.
- **Network security:** Test, evaluate, and improve your network architecture for external, internal, cloud, or hybrid topologies.
- **Threat exposure management:** Continuously discover and eliminate threats to reduce your attack surface over time.
- **IoT and hardware:** Strike the right balance of security and time to market with security testing for systemic vulnerabilities.
- **Red teaming:** Boost your defenses by emulating how an adversary conducts real-world attacks.

An offensive security team performs a variety of functions (not attacking the attackers) to enhance an organization's cybersecurity posture. Here are some key functions:

1. **Security Reviews and Threat Modeling Support:** The team gets involved early in the design phase of a system to provide feedback before code is deployed or operational processes are established.
2. **Security Assessments:** The team conducts hands-on offensive security testing and finds and exploits vulnerabilities for defensive purposes.
3. **Red Team Operations:** The team simulates attacks on the organization's systems to identify vulnerabilities and assess the effectiveness of existing security measures, and in offensive cases, they attack the adversaries as well, either to check their strength or track them if they make any mistake retrying to attack, but the unknown scenario always emerges, as the attacker might start weaponizing with robust and more sophisticated attacks.

- 
4. **Purple Team Operations:** The team works with the defensive security team (Blue Team) to improve the organization's overall security.
 5. **Tabletop Exercises:** The team conducts simulated incident response exercises to test the organization's readiness to handle security incidents.
 6. **Research and Development:** The team stays updated with the latest threats and vulnerabilities and develops new strategies to counter them.
 7. **Predictive Attack Analysis and Incident Response Support:** The team predicts potential attack vectors and provides support during actual security incidents.
 8. **Collaboration with the defensive team:** Working closely with the defensive (blue team) and IT teams to ensure that identified vulnerabilities are promptly addressed and security controls are continuously improved.
 9. **Security Education and Training:** The team helps improve the organization's security culture and overall security posture.
 10. **Gathering Threat Intelligence:** The team collects information about emerging threats and threat actors.
 11. **Informing Risk Management Groups and Leadership:** The team provides valuable input to risk management groups and leadership about the organization's security posture.
 12. **Integration into Engineering Processes:** The team works closely with the engineering team to integrate security into the development process.

The Importance of Having a Data Scientist Team in Cyber Security Operation Center

Cyber security is one of the most critical and challenging domains in the modern world. With the increasing volume and complexity of data, cyber threats, and attacks, it is essential to have a robust and proactive defense system that can protect the systems and data from internal or external risks. Data science, the branch of AI that involves studying and analyzing large volumes of data using various tools and techniques, can play a vital role in enhancing cyber security. In this blog post, we will explore how data science can help cyber security and why having a data scientist team in a cyber security operation center (CSOC) is important.

How Data Science Can Help Cyber Security


Data science can help cyber security in different ways:

- **Detecting anomalies and patterns:** Data science can help identify unusual or suspicious activities or behavioral pattern in the network or system using various methods such as clustering, classification, or regression. For example, data science can help detect malware, phishing, or denial-of-service attacks by analyzing network traffic, email content, or system logs.
- **Predicting vulnerabilities and risks:** Data science can help assess the potential weaknesses or threats in the system or data using various techniques such as forecasting, simulation, or optimization. For example, data science can help predict the likelihood of a breach, the impact of an attack, or the best countermeasures to take, and some specialized tools to implement.
- **Preventing and responding to attacks:** Data science can help prevent or mitigate the damage caused by cyber-attacks using various approaches such as reinforcement learning, natural language processing, or computer vision. For example, data science can help automate the response to an incident, generate alerts or reports, or communicate with the stakeholders.

Why Having a Data Scientist Team in SOC is Important

A SOC is a centralized unit that monitors, analyzes, and responds to cyber security incidents. A SOC typically consists of various roles and functions, such as analysts, engineers, managers, or coordinators. However, having a data scientist team in a SOC can add significant value and benefits, such as:

- **Enhancing the capabilities and performance of the SOC:** A data scientist team can help the SOC leverage the power of data science to improve its efficiency, effectiveness, and accuracy. For example, a data scientist team can help the SOC develop and deploy advanced analytics systems, tools, or models that can automate, optimize, or augment the cyber security processes and tasks.
- **Providing insights and solutions for complex problems:** A data scientist team can help the SOC discover and understand the hidden patterns and insights from the data that can help solve complex or novel cyber security problems. For example, a data scientist team can help the SOC identify the root causes, trends, or correlations of cyber security incidents, or recommend the best actions or strategies to take.
- **Innovating and experimenting with new ideas and technologies:** A data scientist team can help the SOC explore and experiment with new ideas and technologies that can enhance or transform the cyber security domain. For example, a data scientist team can help the SOC apply the latest research or developments in data science, such as deep learning, graph analytics, or quantum computing, to cyber security challenges or opportunities.



Data science and cyber security are two interrelated and complementary disciplines that can benefit from each other. Data science can help cyber security in various ways, such as detecting, predicting, preventing, or responding to cyber-attacks. Having a data scientist team in a SOC can help enhance the capabilities and performance of the SOC, provide insights and solutions for complex problems, and innovate and experiment with new ideas and technologies. Therefore, having a data scientist team in a SOC is important and valuable for any organization that wants to protect its systems and data from cyber risks.


Challenges of Having a Data Scientist Team in CSOC

- **Finding and retaining qualified talent:** Data science is a highly sought-after skill in the market, and there is a shortage of data scientists who have both the technical expertise and the domain knowledge of cyber security. Moreover, data scientists may face high turnover rates due to the competitive nature of the industry and the attractive opportunities elsewhere. Appropriate prioritizing of shifts for security analysts is a must have.
- **Integrating and aligning with the existing SOC functions:** Data science teams need to work closely with other SOC roles and functions, such as analysts, engineers, managers, or coordinators, to ensure that their outputs are relevant, actionable, and consistent. However, this may require overcoming the challenges of communication, collaboration, and coordination across different teams, cultures, and processes.
- **Ensuring data quality, security, and privacy:** Data science teams rely on large volumes and varieties of data to perform their tasks, such as network traffic, system logs, or threat intelligence. However, ensuring that the data is accurate, complete, and up to date can be challenging, especially in a dynamic and complex cyber environment. Moreover, data science teams need to adhere to the strict standards and regulations of data security and privacy, such as encryption, anonymization, or consent, to protect the data from unauthorized access or misuse.

Data Scientist's Data Requirements From a SOC

The data scientist's data requirements from a SOC may vary depending on the specific tasks and goals of the data science team. However, some general data requirements are:


- **Access to relevant and reliable data sources:** Data scientists need to have access to various types of data that are relevant to the cyber security domain,




such as network traffic, system logs, threat intelligence, incident reports, vulnerability scans, etc. These data sources should be reliable, accurate, complete, and up-to-date, and should cover the entire enterprise infrastructure and data assets.


- **Ability to collect, store, and process large volumes and varieties of data:** Data scientists need to have the tools and technologies to collect, store, and process large volumes and varieties of data, such as structured, unstructured, or semi-structured data, in a scalable and efficient manner. These tools and technologies should support data ingestion, integration, transformation, cleansing, and analysis, and should be compatible with the existing SOC functions and systems.
- **Ability to apply appropriate data science methods and techniques:** Data scientists need to have the skills and knowledge to apply appropriate data science methods and techniques to the data, such as descriptive, predictive, or prescriptive analytics, machine learning, deep learning, natural language processing, computer vision, etc. These methods and techniques should be suitable for cyber security problems and objectives and should be validated and evaluated for their performance and accuracy.
- **Ability to communicate and visualize the data and results:** Data scientists need to have the ability to communicate and visualize the data and results in a clear and understandable manner, using various tools and formats, such as dashboards, reports, charts, graphs, etc. These tools and formats should be tailored to the needs and preferences of the different stakeholders, such as analysts, engineers, managers, or coordinators, and should provide actionable insights and recommendations.

Common Data Science Methods and Techniques Used in SOC

- **Descriptive analytics:** This technique involves summarizing and visualizing the data to understand what has happened or is happening in the cyber environment. For example, descriptive analytics can help the SOC create dashboards, reports, charts, or graphs to monitor the network activity, system performance, or threat landscape.
 - **Predictive analytics:** This technique involves applying statistical or machine learning models to the data to forecast what will happen or is likely to happen in the cyber environment. For example, predictive analytics can help the SOC estimate the probability of a cyber-attack, the impact of a vulnerability, or the behavior of an adversary.
- 

- 
- **Prescriptive analytics:** This technique involves using optimization or simulation models to the data to recommend what should be done or is best to be done in the cyber environment. For example, prescriptive analytics can help the SOC determine the optimal allocation of resources, the best response strategy, or the most effective countermeasure.
 - **Anomaly detection:** This technique involves identifying and flagging the data points that deviate from the normal or expected patterns in the data. For example, anomaly detection can help the SOC detect malicious or suspicious activities, such as malware, phishing, or denial-of-service attacks, by analyzing the network traffic, email content, or system logs.
 - **Clustering:** This technique involves grouping the data points that have similar characteristics or features in the data. For example, clustering can help the SOC segment the data into different categories, such as users, devices, or threats, based on their attributes, behaviors, or relationships.
 - **Classification:** This technique involves assigning labels or categories to the data points based on predefined criteria or rules in the data. For example, classification can help the SOC identify the type or severity of a cyber incident, such as malware, phishing, or denial-of-service, based on the features, patterns, or signatures of the data.
 - **Natural language processing:** This technique involves processing and analyzing the textual or spoken data using various methods, such as text classification, named entity recognition, sentiment analysis, topic modeling, machine translation, speech recognition and generation, or text summarization. For example, natural language processing can help the SOC extract information, insights, or emotions from the text or speech data, such as emails, reports, blogs, or podcasts, related to cyber security.

Limitations of Using Data Science in SOC

- 
- **Limited access to data:** Data science requires access to various types of data that are relevant to cyber security, such as network traffic, system logs, threat intelligence, etc. However, these data may not be publicly available or easy to obtain due to privacy, legal, or technical constraints.
 - **Data quality issues:** Data science relies on the quality and reliability of the data to perform accurate and meaningful analysis. However, the data used in SOC may have issues such as missing values, errors, inconsistencies, or noise, which can affect the validity and usefulness of the results.
 - **Bias in data and algorithms:** Data science can be biased due to various factors, such as the way the data is collected, processed, or interpreted, or the way the algorithms are designed, trained, or evaluated. Bias can lead to unfair or

discriminatory outcomes, which can harm the reputation or trustworthiness of the SOC.


- **Lack of skilled staff:** Data science requires a combination of technical skills, domain knowledge, and analytical thinking, which are in high demand and short supply in the market. Finding and retaining qualified data scientists for SOC can be challenging and costly.
- **Lack of integration and alignment:** Data science needs to be integrated and aligned with the existing SOC functions, such as monitoring, analysis, response, and reporting. However, this may require overcoming the barriers of communication, collaboration, and coordination across different teams, cultures, and processes.

Ethical Considerations When Using Data Science in Cyber Security

- **Data privacy and security:** Data science requires access to various types of data that are relevant to cyber security, such as network traffic, system logs, threat intelligence, etc. However, these data may contain sensitive or personal information that needs to be protected from unauthorized access or misuse. Data science teams must respect the users' privacy and data security rights, and adhere to the relevant laws and regulations, such as GDPR or HIPAA.
- **Bias and fairness:** Data science relies on algorithms and models that are trained and tested on data. However, these algorithms and models may be biased due to various factors, such as the way the data is collected, processed, or interpreted, or the way the algorithms are designed, trained, or evaluated. Bias can lead to unfair or discriminatory outcomes, such as false positives or negatives, or misclassification of cyber incidents or threats. Data science teams must ensure that their algorithms and models are unbiased and fair, and that they do not harm or disadvantage any groups or individuals.
- **Transparency and accountability:** Data science involves complex and sophisticated methods and techniques that may not be easily understood or explained by the data science teams or the users. However, these methods and techniques may have significant impacts on cyber security decisions and actions, such as detection, prediction, prevention, or response. Data science teams must ensure that their methods and techniques are transparent and accountable, and that they can provide clear and understandable explanations or justifications for their results and recommendations.

Examples of Unethical Use of Data Science in Cyber Security

- **Data breaches:** Data breaches involve unauthorized access or disclosure of sensitive or personal data by hackers, insiders, or third parties. Data breaches can cause serious harm to the data owners, such as identity theft, fraud, or blackmail. For example, Equifax, one of the largest credit bureaus in the U.S., suffered a massive data breach in 2017 that compromised the personal information of approximately 147 million people.
- **Deepfakes:** Deepfakes are synthetic media that use data science techniques, such as deep learning, to manipulate or generate realistic images, videos, or audio of people or events. Deepfakes can be used for malicious purposes, such as spreading misinformation, impersonating someone, or blackmailing someone. For example, a deepfake video of former U.S. President Barack Obama was created and released on LinkedIn by researchers to demonstrate the potential dangers of this technology.
- **Cyberattacks:** Cyberattacks are deliberate attempts to disrupt, damage, or gain unauthorized access to a computer system or network. Cyberattacks can use data science techniques, such as machine learning, to enhance their effectiveness, stealth, or adaptability. For example, a cyberattack on a Ukrainian power grid in 2016 used machine learning to evade detection which caused a blackout.
- **Malicious AI Models Backdooring Computers:** AI models can be manipulated to perform malicious activities, including backdooring computers. For instance, code uploaded to the AI developer platform Hugging Face was found to covertly install backdoors on end-user machines. This was achieved by exploiting the serialization process, a method used in Python to convert objects and classes into a byte stream. When the malicious model was loaded onto an end-user device, it opened a reverse shell, granting a remote device full control of the user's device. This demonstrates that AI models, like any other software, can pose serious risks if not carefully vetted.
- **AI Making Costly Mistakes:** AI systems can make mistakes that lead to financial losses, wasted time, and even lawsuits. For example, one study estimates that 70% of AI initiatives see no or minimal impact due to factors like lack of expertise, misunderstanding of AI capabilities, and under-budgeting. Missteps in AI implementation can lead to underwhelming results, costing organizations time, money, and energy. Moreover, the misuse of AI in industries like healthcare and insurance has led to a wave of lawsuits.
- **Customer Lawsuits:** As AI technologies become mainstream, so will legal cases involving these systems. There have been numerous lawsuits against companies



for allegedly using AI to infringe on copyrights or to deny claims. For instance, OpenAI, the makers of GPT-4 and DALL·E, are being sued by authors for unlawfully using their work to train its large language models. Similarly, insurers like Humana, Cigna, and UnitedHealthcare are facing class actions for allegedly deploying advanced technology to deny claims.

In summary, while AI has the potential to bring significant benefits, it also comes with risks and challenges. It's crucial for organizations to implement robust security measures, ensure proper use of AI, and stay updated with the legal implications of AI use.

Does Offensive Security Mean to Attack the Attacker?

No, offensive security does not mean attacking the attacker. Offensive security, also known as penetration testing or red teaming, involves authorized professionals simulating cyber-attacks on an organization's systems, networks, and applications. The primary goal is to identify vulnerabilities and weaknesses before malicious attackers can exploit them. The offensive security team works to understand potential entry points, security flaws, and areas where improvements can be made in an organization's cybersecurity defenses.

In offensive security, the activities are conducted ethically and with explicit permission from the organization being tested. The focus is on improving security by identifying and addressing weaknesses, not on attacking external threat actors. The offensive security team operates within legal and ethical boundaries, adhering to a predefined scope and rules of engagement.

In contrast, when we talk about defending against attackers, it falls under the domain of defensive security. Defensive security involves implementing measures to protect systems, networks, and data from unauthorized access, attacks, and other security threats. Defensive security measures include firewalls, intrusion detection systems, antivirus software, access controls, and other safeguards to prevent, detect, and respond to security incidents.

Overall, offensive security and defensive security work hand-in-hand to create a comprehensive and resilient cybersecurity strategy for organizations. The offensive side helps identify weaknesses, while the defensive side focuses on implementing safeguards and responding to potential threats.




CHAPTER 5

Foundational Information Security Principles

MODELS, FRAMEWORKS, ROADMAPS, CONTROL REQUIREMENTS MAPPING IS ALL ABOUT BASIC PRINCIPLES LAID OUT BY BODY OF KNOWLEDGE OR SOME SORT OF GOVERNING BODY; UNDERSTAND THE REQUIREMENTS, YOU DON'T HAVE TO MEMORIZE, FORMULATE AND IMPLEMENT, AND HAVE A DOCUMENT REPOSITORY FOR YOUR FUTURES SAKE, BY NOW, YOU SHOULD BE A PROFESSIONAL.

Core and fundamental principles in cybersecurity provide the foundational knowledge and guidance that all cybersecurity professionals should be familiar with. These





principles help shape effective cybersecurity strategies and practices. Here are key principles in cybersecurity:

Confidentiality: Protecting sensitive information from unauthorized access. This is often achieved through encryption, access controls, and data classification.

Integrity: Ensuring the accuracy and trustworthiness of data. This involves preventing unauthorized alterations, tampering, or corruption of data.

Availability: Ensuring that systems, data, and resources are available when needed. This principle focuses on preventing disruptions, downtime, and service outages.

Authentication: Verifying the identity of users, systems, and devices. Strong authentication methods, such as multi-factor authentication (MFA), enhance security.

Authorization: Granting or restricting access based on a user's or system's permissions. Authorization ensures that users can only access resources they are allowed to and nothing else.

Accountability and Auditing: Monitoring and tracking user activities to hold individuals or systems accountable for their actions. Audit logs help in establishing accountability and incident investigation.

Least Privilege: Providing users and systems with the minimum level of access and permissions required to perform their tasks. This key rule limits potential damage in case of a breach.


Defense in Depth: Employing multiple layers of security controls to protect against various attack vectors. This approach minimizes the likelihood of a single point of failure.

Security by Design: Integrating security into the design and development of systems and applications from the beginning rather than as an afterthought.

Security Awareness and Training: Educating users and staff about security best practices to reduce human-related security risks, such as social engineering.

Patch Management: Regularly updating and patching software and systems to address known vulnerabilities and weaknesses.

Incident Response and Recovery: Developing a plan for responding to security incidents and recovering from them. The goal is to minimize damage and downtime after an incident happens.



Encryption: Process of converting data into a code that is readable only with a key to decode it. Using encryption to protect data in transit and at rest. This helps maintain confidentiality and prevents unauthorized access.

Network Segmentation: Isolating network segments to limit the potential spread of threats and lateral movement by attackers.

Security Policies and Procedures: Documents that define how to protect sensitive data and other assets. Establish clear guidelines and procedures for maintaining security. Policies should be regularly reviewed and updated.

Risk Assessment and Management: Identifying and assessing security risks and taking steps to mitigate or manage them effectively.

Vendor Security Evaluation: Assessing the security of third-party vendors and their products before integration into the organization's environment.

Compliance and Regulation: Adhering to relevant security regulations, standards, and best practices to maintain legal and industry compliance.

User Education and Awareness: Ensuring that users are aware of security threats and their roles in protecting the organization. Regular security training is crucial.

Continuous Monitoring: Ongoing monitoring of systems, networks, and user activities for signs of potential security threats.

Vulnerability Management: Monitoring and mitigating vulnerabilities. Promptly applying security patches and updates to address known vulnerabilities.



Physical Security: Protecting physical access to data centers, server rooms, and other critical infrastructure.

These principles are the building blocks of effective cybersecurity and should guide the development of security policies, procedures, and strategies in organizations. Cybersecurity professionals should have a strong grasp of these principles and apply them in their daily work to protect systems and data effectively.

Source: [CYBERSECURITY LEARNING SATURDAY - Post | LinkedIn](#)

Network Segmentation – A 4-Step Approach

Network segmentation is a security technique that divides a network into smaller, isolated segments, each with its own access and protection policies. This can help limit



the impact of a cyberattack, improve network performance, and simplify management. However, network segmentation can also be challenging to implement, especially in large and complex networks. Therefore, it is important to follow a systematic and gradual approach that focuses on one segment at a time. This article will outline the four steps of network segmentation and provide some tips on how to apply them effectively.

Step 1: Gain Visibility

The first step is to gain visibility into the network traffic and usage patterns of the segment you want to isolate. This will help you understand the communication needs and dependencies of the segment, as well as identify any anomalies or risks. Without visibility, you may end up blocking legitimate traffic or allowing malicious traffic, which can compromise the security and functionality of the segment. To gain visibility, you can use tools such as network monitoring, traffic analysis, and asset discovery.

Step 2: Protect Communications and Resources


The second step is to protect the communications and resources of the segment from both inbound and outbound threats. This means applying security measures such as encryption, authentication, firewall, and intrusion prevention systems to the segment. These measures will help prevent unauthorized access, data leakage, malware infection, and other attacks. Protection is the primary goal of network segmentation, so you should not proceed to the next step until you have achieved a satisfactory level of security for the segment.

Step 3: Implement Granular Controls

The third step is to implement granular controls on the data, users, and assets of the segment. This means enforcing the organization's communication policy and access rules for the segment, based on the principle of least privilege. This will help reduce the attack surface, improve compliance, and support business objectives. To implement granular controls, you can use tools such as network access control, role-based access control, and application control. However, you should be careful not to disrupt the normal operations of the segment, so you should start with a default-allow mode and gradually move to a default-deny mode, using detective and preventive controls.

Step 4: Set a Default Deny on all Inter-Segment Communications

The fourth and final step is to set a default deny policy on all inter-segment communications. This means blocking all traffic between segments, unless explicitly allowed by a specific rule. This will help isolate the segment from the rest of the network and prevent lateral movement of attackers. Only when you have reached this step, you



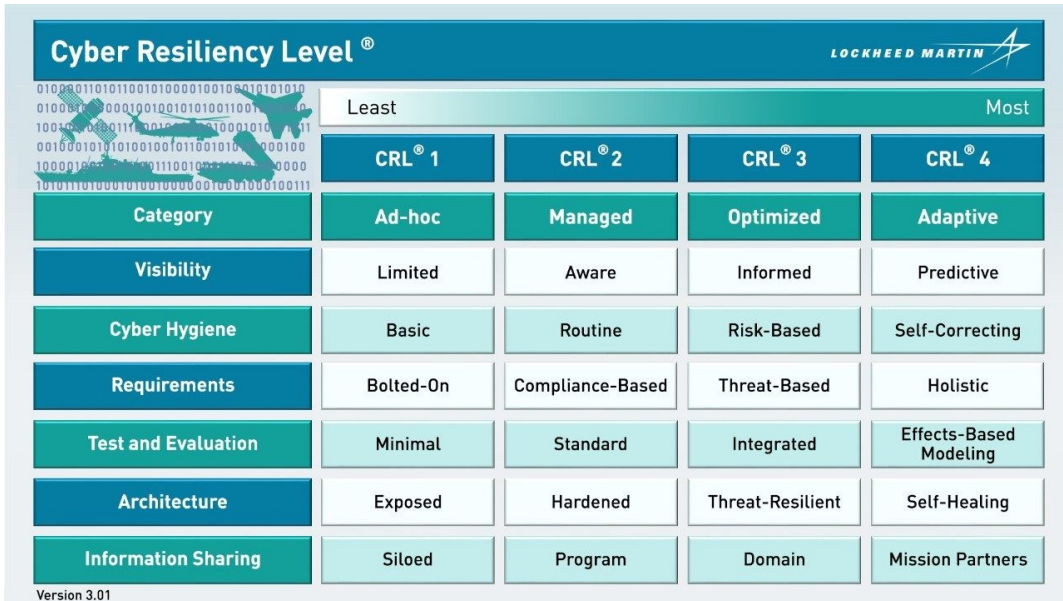
can consider the segment fully segmented and secure. However, you should also monitor and review the segment regularly, as the network conditions and requirements may change over time.

Network segmentation is a powerful and beneficial security technique, but it also requires careful planning and execution. By following the four steps of network segmentation, you can achieve a successful and sustainable segmentation of your network, one segment at a time. However, you should also remember that network segmentation is not a one-time project, but an ongoing process that requires constant adaptation and improvement and a long term planning. As technology evolves and business demands grow, you should be ready to adjust your network segmentation strategy accordingly, and clear up the basic design requirements if it's a first build.

Cyber Resiliency Scoreboard® (CRS®)

Lockheed Martin integrates full-spectrum cyber solutions into everything we do. We introduced the Cyber Resiliency Level® (CRL®) Framework (see Figure 1) in 2019 as the world's first standard method to measure the cyber resiliency *maturity of a weapon system*. In support of the CRL® framework, Lockheed Martin created the Cyber Resiliency Scoreboard® (CRS®) tool to assist customers in making informed decisions in selecting courses of action (CoA) and prioritizing their resources for maximum effect against cyber-attacks:

Source: [CRS_v2.1_Whitepaper_29Aug23_FINAL.pdf \(lockheedmartin.com\)](#)



Cyber Resiliency Level[®] LOCKHEED MARTIN

Least Most

	CRL [®] 1	CRL [®] 2	CRL [®] 3	CRL [®] 4
Category	Ad-hoc	Managed	Optimized	Adaptive
Visibility	Limited	Aware	Informed	Predictive
Cyber Hygiene	Basic	Routine	Risk-Based	Self-Correcting
Requirements	Bolted-On	Compliance-Based	Threat-Based	Holistic
Test and Evaluation	Minimal	Standard	Integrated	Effects-Based Modeling
Architecture	Exposed	Hardened	Threat-Resilient	Self-Healing
Information Sharing	Siloed	Program	Domain	Mission Partners

Version 3.01

Though it's not directly related to our discussion regarding the SOC model, its quoted here as it's a good resource for your KB enrichment.

Threat Driven Modeling in SOC

A methodology that aims to improve the cybersecurity posture of an organization by aligning its security operations with the current and emerging threat landscape. It involves identifying, prioritizing, and mitigating the most relevant and impactful cyberthreats to the organization's assets, data, and business objectives.

Some of the benefits of Threat Driven Modeling in SOC are:

- It helps to focus the resources and efforts of the security team on the most critical and likely threats, rather than on generic or outdated ones.
- It enables a proactive and adaptive approach to cybersecurity, rather than a reactive and static one.
- It fosters collaboration and communication among different stakeholders, such as security analysts, threat intelligence providers, business units, and senior management.

- It supports continuous improvement and learning, as the threat model is regularly updated and refined based on new information and feedback.

Some of the best practices for implementing Threat Driven Modeling in CSOC are:

- Establish a clear and shared understanding of the organization's assets, data, and business objectives, as well as the potential impact of cyberattacks on them.
- Conduct a comprehensive and systematic threat analysis, using both internal and external sources of threat intelligence, to identify the most relevant threat actors, tactics, techniques, and procedures (TTPs) for the organization.
- Prioritize the threats based on their likelihood and severity and map them to the organization's attack surface and vulnerabilities.
- Develop and execute appropriate mitigation strategies and countermeasures, such as patching, hardening, monitoring, alerting, and incident response, to reduce the risk and impact of the threats.
- Monitor and measure the effectiveness of the mitigation strategies and countermeasures and adjust them as needed based on the changing threat landscape and feedback from the security team and other stakeholders.
- Review and update the threat model periodically, or whenever there is a significant change in the organization's environment, assets, data, or business objectives.

Microsoft Threat Modeling Tool STRIDE

The Threat Modeling Tool is a core element of the Microsoft Security Development Lifecycle (MSDL). It allows software architects to identify and mitigate potential security issues early, when they are relatively easy and cost-effective to resolve. As a result, it greatly reduces the total cost of development. Also, we designed the tool with non-security experts in mind, making threat modeling easier for all developers by providing clear guidance on creating and analyzing threat models.

Here are some tooling capabilities and innovations, just to name a few:

- **Automation:** Guidance and feedback in drawing a model
- **STRIDE per Element:** Guided analysis of threats and mitigations
- **Reporting:** Security activities and testing in the verification phase

- **Unique Methodology:** Enables users to better visualize and understand threats
- **Designed for Developers and Centered on Software:** many approaches are centered on assets or attackers. We are focused on software. We build on activities that all software developers and architects are familiar with – such as drawing pictures for their software architecture.
- **Focused on Design Analysis:** The term "threat modeling" can refer to either a requirement or a design analysis technique. Sometimes, it refers to a complex blend of the two. The Microsoft SDL approach to threat modeling is a focused design analysis technique.

STRIDE Model

To better help you formulate the following category, Microsoft invented & uses the STRIDE model, which categorizes different types of threats and simplifies the overall security conversations. There are other threat models like PASTA, TRIKE or VAST, but you can check those out for yourself. We will be focusing on STRIDE model for the sake of the discussion.

Category	Description
<u>S</u> poofing	Involves illegally accessing and then using another user's authentication information, such as username and password
<u>T</u> ampering	Involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet
<u>R</u> epudiation	Associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations. Non-Repudiation refers to the ability of a system to counter repudiation threats. For example, a user who purchases an item might have to sign for the item upon receipt. The vendor can then use the signed receipt as evidence that the user did receive the package
<u>I</u> nformation Disclosure	Involves the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers

<u>D</u>enial of Service	Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability
<u>E</u>levation of Privilege	An unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats include those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed

One of the most popular frameworks for creating threat models is STRIDE, which stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. These are the six categories of threats that can affect a system.

To illustrate how STRIDE works, let's consider a simple web application that allows users to create and share blog posts. The web application has the following components:

- A web server that hosts the application and communicates with the database.
- A database server that stores the user accounts and blog posts.
- A browser that allows the user to interact with the web server.
- Using STRIDE, we can identify the following threats and countermeasures for each component:

Web server:

- **Spoofing:** An attacker could impersonate a legitimate user or the web server itself to gain unauthorized access to the system. To prevent this, the web server should use strong authentication and encryption mechanisms, such as HTTPS and SSL certificates.
- **Tampering:** An attacker could modify the data or code on the web server to compromise its integrity or functionality. To prevent this, the web server should use secure coding practices, input validation, output encoding, and file integrity checks.
- **Repudiation:** An attacker could deny performing an action or claim that an action was performed by someone else. To prevent this, the web server should use logging and auditing mechanisms to record and verify the actions and identities of the users and the web server itself.
- **Information Disclosure:** An attacker could access or leak sensitive information from the web server, such as user credentials, blog posts, or configuration files.

To prevent this, the web server should use encryption, access control, and data minimization techniques to protect the data in transit and at rest.

- **Denial of Service:** An attacker could overload or crash the web server by sending many requests or malicious inputs. To prevent this, the web server should use throttling, caching, and load balancing techniques to handle the traffic and mitigate the impact of malicious requests.
- **Elevation of Privilege:** An attacker could exploit a vulnerability or misconfiguration on the web server to gain higher privileges or access to restricted resources. To prevent this, the web server should use the principle of least privilege, secure configuration, and patch management to limit the permissions and exposure of the web server.

Database server:

- **Spoofing:** An attacker could impersonate the web server or a legitimate user to access or modify the data on the database server. To prevent this, the database server should use strong authentication and encryption mechanisms, such as mutual authentication and database encryption.
- **Tampering:** An attacker could modify the data on the database server to compromise its integrity or functionality. To prevent this, the database server should use secure coding practices, input validation, output encoding, and integrity constraints.
- **Repudiation:** An attacker could deny performing an action or claim that an action was performed by someone else. To prevent this, the database server should use logging and auditing mechanisms to record and verify the actions and identities of the web server and the users.
- **Information Disclosure:** An attacker could access or leak sensitive information from the database server, such as user credentials, blog posts, or database schema. To prevent this, the database server should use encryption, access control, and data minimization techniques to protect the data in transit and at rest.
- **Denial of Service:** An attacker could overload or crash the database server by sending a large number of queries or malicious inputs. To prevent this, the database server should use throttling, caching, and backup techniques to handle the queries and mitigate the impact of malicious inputs.
- **Elevation of Privilege:** An attacker could exploit a vulnerability or misconfiguration on the database server to gain higher privileges or access to restricted data. To prevent this, the database server should use the principle of

least privilege, secure configuration, and patch management to limit the permissions and exposure of the database server.

Browser:

- **Spoofing:** An attacker could impersonate the web server or another user to trick the user into providing sensitive information or performing malicious actions. To prevent this, the browser should use HTTPS and SSL certificates to verify the identity and legitimacy of the web server and display visual indicators to warn the user of potential phishing or spoofing attempts.
- **Tampering:** An attacker could modify the content or behavior of the web application on the browser by injecting malicious code or altering the HTML, CSS, or JavaScript files. To prevent this, the browser should use secure coding practices, input validation, output encoding, and content security policy to prevent cross-site scripting (XSS) and other code injection attacks.
- **Repudiation:** An attacker could deny performing an action or claim that an action was performed by someone else. To prevent this, the browser should use logging and auditing mechanisms to record and verify the actions and identities of the user and the web server.
- **Information Disclosure:** An attacker could access or leak sensitive information from the browser, such as user credentials, blog posts, or browsing history. To prevent this, the browser should use encryption, access control, and data minimization techniques to protect the data in transit and at rest and provide the user with options to clear or manage their data.
- **Denial of Service:** An attacker could overload or crash the browser by sending many requests or malicious inputs. To prevent this, the browser should use throttling, caching, and sandboxing techniques to handle the requests and mitigate the impact of malicious inputs.
- **Elevation of Privilege:** An attacker could exploit a vulnerability or misconfiguration on the browser to gain higher privileges or access to restricted resources. To prevent this, the browser should use the principle of least privilege, secure configuration, and patch management to limit the permissions and exposure of the browser.

Sunburst Visualization of STRIDE-LM to Security Controls

The size of the sector indicates the cumulative number of controls encompassed under that sector. For example, you can see below that the controls are spread evenly across

Threat Modeling Method	Features
STRIDE	<ul style="list-style-type: none"> • Helps identify relevant mitigating techniques • Is the most mature • Is easy to use but is time consuming
PASTA	<ul style="list-style-type: none"> • Helps identify relevant mitigating techniques • Directly contributes to risk management • Encourages collaboration among stakeholders • Contains built-in prioritization of threat mitigation • Is laborious but has rich documentation
LINDDUN	<ul style="list-style-type: none"> • Helps identify relevant mitigation techniques • Contains built-in prioritization of threat mitigation • Can be labor intensive and time consuming
CVSS	<ul style="list-style-type: none"> • Contains built-in prioritization of threat mitigation • Has consistent results when repeated • Has automated components • Has score calculations that are not transparent
Attack Trees	<ul style="list-style-type: none"> • Helps identify relevant mitigation techniques • Has consistent results when repeated • Is easy to use if you already have a thorough understanding of the system
Persona non Grata	<ul style="list-style-type: none"> • Helps identify relevant mitigation techniques • Directly contributes to risk management • Has consistent results when repeated • Tends to detect only some subsets of threats
Security Cards	<ul style="list-style-type: none"> • Encourages collaboration among stakeholders • Targets out-of-the-ordinary threats • Leads to many false positives
hTMM	<ul style="list-style-type: none"> • Contains built-in prioritization of threat mitigation • Encourages collaboration among stakeholders • Has consistent results when repeated
Quantitative TMM	<ul style="list-style-type: none"> • Contains built-in prioritization of threat mitigation • Has automated components • Has consistent results when repeated
Trike	<ul style="list-style-type: none"> • Helps identify relevant mitigation techniques • Directly contributes to risk management • Contains built-in prioritization of threat mitigation • Encourages collaboration among stakeholders • Has automated components • Has vague, insufficient documentation
VAST Modeling	<ul style="list-style-type: none"> • Helps identify relevant mitigation techniques • Directly contributes to risk management • Contains built-in prioritization of threat mitigation • Encourages collaboration among stakeholders • Has consistent results when repeated • Has automated components • Is explicitly designed to be scalable • Has little publicly available documentation
OCTAVE	<ul style="list-style-type: none"> • Helps identify relevant mitigation techniques • Directly contributes to risk management • Contains built-in prioritization of threat mitigation • Encourages collaboration among stakeholders • Has consistent results when repeated • Is explicitly designed to be scalable • Is time consuming and has vague documentation

Source: [Threat Modeling: 12 Available Methods \(cmu.edu\)](https://www.cmu.edu/secure/cybercenter/resources/ThreatModeling12AvailableMethods.html)

Threat modeling should be performed early in the development cycle when potential issues can be caught early and remedied, preventing a much costlier fix down the line. Using threat modeling to think about security requirements can lead to proactive architectural decisions that help reduce threats from the start.

Threat Modeling Using MITRE ATT&CK

The MITRE ATT&CK Framework is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. It's used as a foundation for the development of specific threat models and methodologies in the private sector, government, and the cybersecurity product and service community.

Here's a basic guide on how to use the MITRE ATT&CK Framework for threat modeling:

1. **Understand the Framework:** The MITRE ATT&CK Framework is structured based on common threat actor Tactics, Techniques, and Procedures (TTPs). It provides a methodology for security risk management of those TTPs in the security environment.
2. **Identify Relevant TTPs:** Identify the TTPs that are most relevant to your organization. This could be based on your industry, the types of data you handle, or the specific threats you've encountered in the past.
3. **Map TTPs to Your Environment:** Map the identified TTPs to your existing security controls. This will help you understand which parts of your environment are vulnerable to these TTPs.
4. **Develop and Test Analytics:** Use the mapped TTPs to develop behavioral-based analytic detection capabilities. Then, test these analytics using adversary emulation.
5. **Integrate with Risk Management:** Integrate the results from the ATT&CK framework into your organization's risk management framework. This can help you scale risk reporting up and down the organization, from security operations to senior leadership.
6. **Continual Improvement:** Continually update and refine your threat model as new TTPs are added to the ATT&CK Framework, or as changes occur in your environment.

Remember, the goal of threat modeling with the MITRE ATT&CK Framework is not just to understand the threats you face, but also to improve your defenses by identifying gaps in your security controls.

Threat Modeling with MITRE ATT&CK Framework

Topic is written by By Brad Voris <https://github.com/bvoris/mitreattackthreatmodeling>

This provides a guided step by step walkthrough for threat modeling with MITRE ATT&CK Framework

Links

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

MITRE ATT&CK Website - this is needed to search for threat groups, techniques, and tools used by threat actors

<https://attack.mitre.org/>

ATT&CK Navigator - maps out threat group techniques, allows for developing threat models

<https://mitre-attack.github.io/attack-navigator/>

What are you trying to accomplish?

We are trying to determine the matrices that show known attack techniques of threat groups and develop a model based on those techniques to help anticipate actions of those threat groups and help validate security controls.

What do we need from here?

We need an industry. For this demonstration I've selected HEALTHCARE as the industry.

Lets get started

Go to <https://attack.mitre.org/>

Click the search magnifying glass



Search for "healthcare"

Healthcare ×

Leviathan, MUDCARP, Kryptonite Panda, Gadolinium, BRONZE MOHAWK, TEMP.Jumper, APT40, TEMP.Periscope, Group G0065
... filiated front company.[1] Active since at least 2009, Leviathan has targeted the following sectors: academia, aerospace/aviation, biomedical, defense industrial base, government, **healthcare**, manufacturing, maritime, and transportation across the US, Canada, Europe, the Middle East, and Southeast Asia.[1][2][3] ID: G0065 ⓘ Associated Groups: MUDCARP, Kryptonite Panda, Gadolinu...

APT41, Wicked Panda, Group G0096
... archers have assessed as Chinese state-sponsored espionage group that also conducts financially-motivated operations. Active since at least 2012, APT41 has been observed targeting **healthcare**, telecom, technology, and video game industries in 14 countries. APT41 overlaps at least partially with public reporting on groups including BARIUM and Winni Group.[1][2] ID: G0096 ⓘ Assoc...

Deep Panda, Shell Crew, WebMasters, KungFu Kittens, PinkPanther, Black Vine, Group G0009
... Deep Panda Deep Panda is a suspected Chinese threat group known to target many industries, including government, defense, financial, and telecommunications. [1] The intrusion into **healthcare** company Anthem has been attributed to Deep Panda. [2] This group is also known as Shell Crew, WebMasters, KungFu Kittens, and PinkPanther. [3] Deep Panda also appears to be known as Black V...

Fox Kitten, UNC757, Parisite, Pioneer Kitten, Group G0117
... the Middle East, North Africa, Europe, Australia, and North America. Fox Kitten has targeted multiple industrial verticals including oil and gas, technology, government, defense, **healthcare**, manufacturing, and engineering. [1][2][3][4] ID: G0117 ⓘ Associated Groups: UNC757, Parisite, Pioneer Kitten Version: 1.0 Created: 21 December 2020 Last Modified: 02 June 2022 Version Perma...

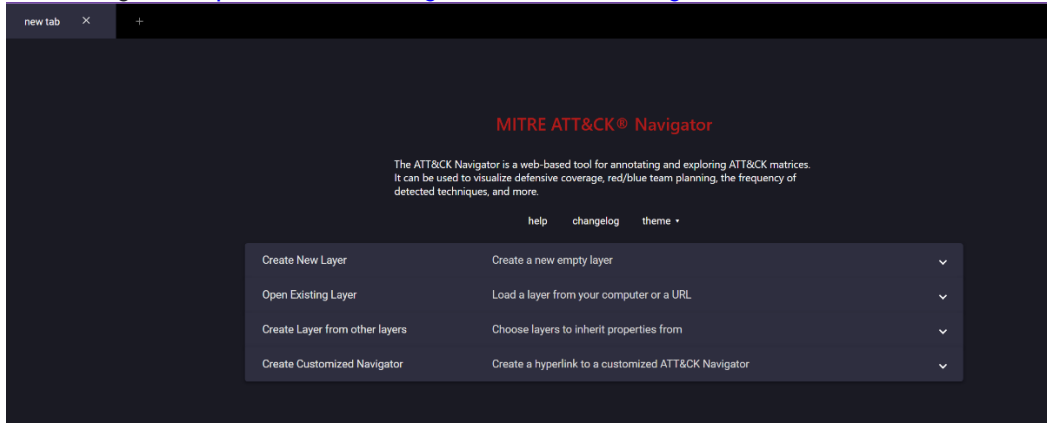
FIN4, Group G0085
FIN4 FIN4 is a financially-motivated threat group that has targeted confidential information related to the public financial market, particularly regarding **healthcare** and pharmaceutical companies, since at least 2013.[1][2] FIN4 is unique in that they do not infect victims with typical persistent malware, but rather they focus on capturing credentials au...

[load more results](#)

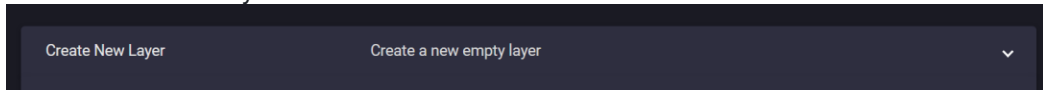
For simplicity we will select two threat groups APT 40/Leviathan and APT 41

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

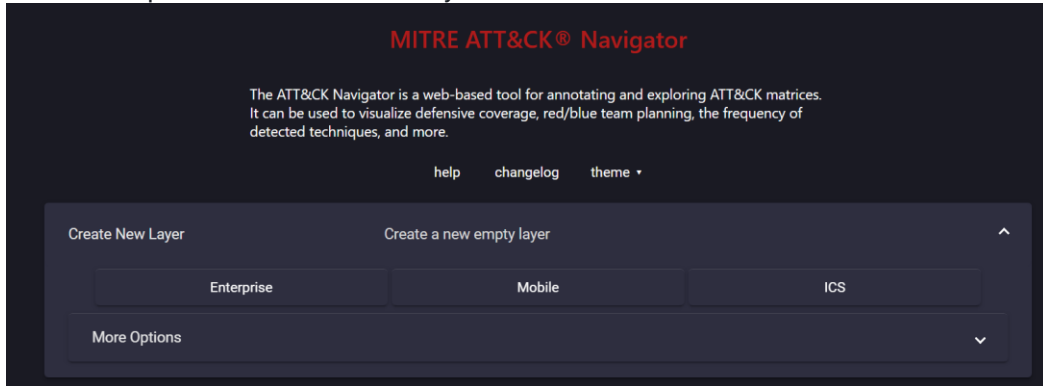
Now lets go to <https://mitre-attack.github.io/attack-navigator/>



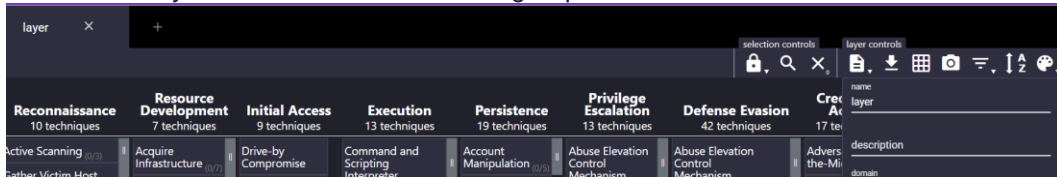
Lets create a new layer



Select Enterprise under create new layer

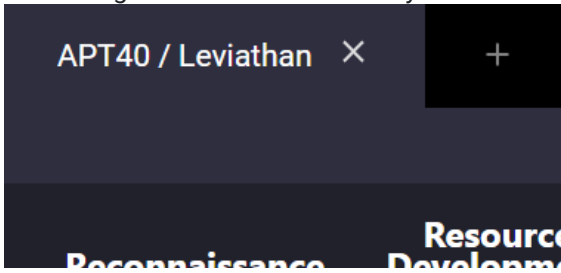


Click on the layer and name it to the threat group

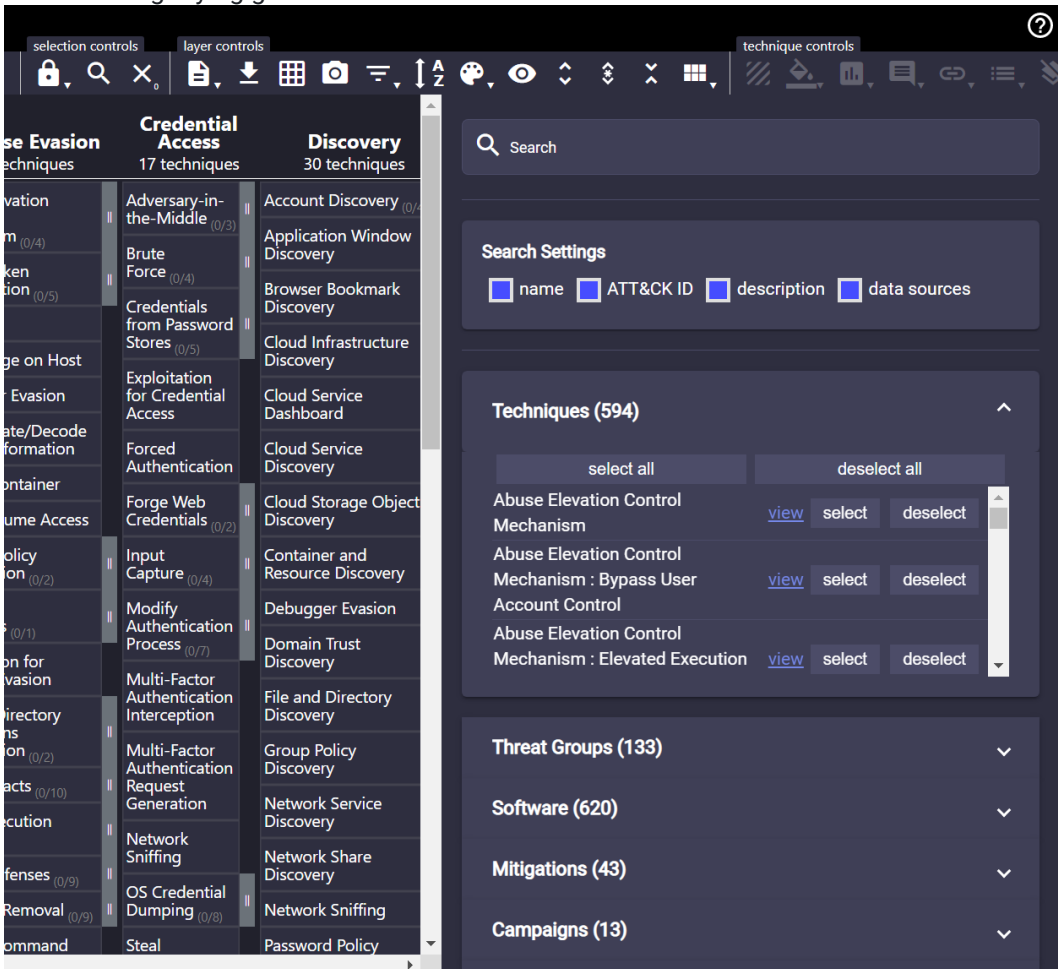


COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

The change will be reflect in the layer name



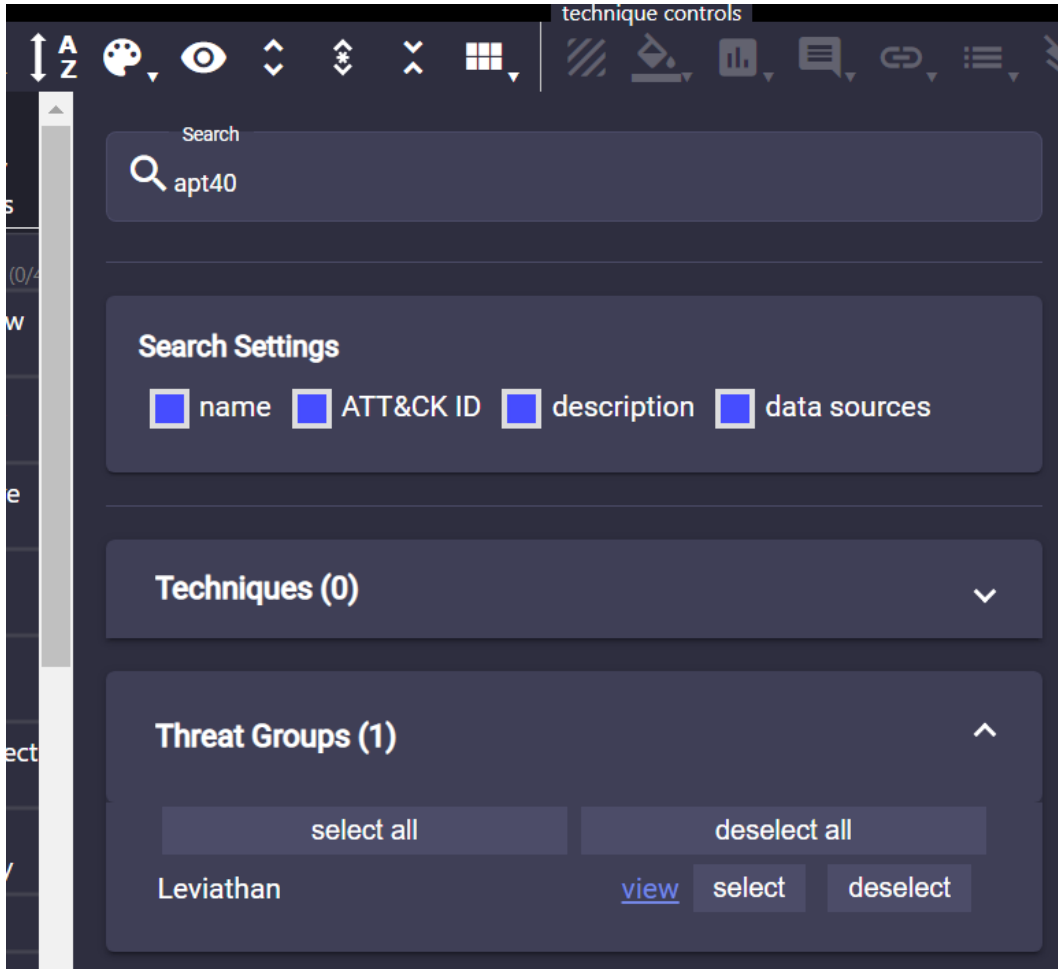
Click the magnifying glass under selection controls



Search for the Threat Group in the search field

The screenshot shows a dark-themed interface with a search bar at the top containing the text 'apt40'. Below the search bar is a 'Search Settings' section with four checkboxes: 'name', 'ATT&CK ID', 'description', and 'data sources', all of which are currently unchecked. Below the settings are two expandable sections: 'Techniques (0)' which is collapsed, and 'Threat Groups (1)' which is expanded. The 'Threat Groups' section contains a table with one entry, 'Leviathan'. Above the table are two buttons: 'select all' and 'deselect all'. To the right of the 'Leviathan' entry are three buttons: 'view', 'select', and 'deselect'. The interface also features a top toolbar with various icons for navigation and actions.

Click select next to the threat group



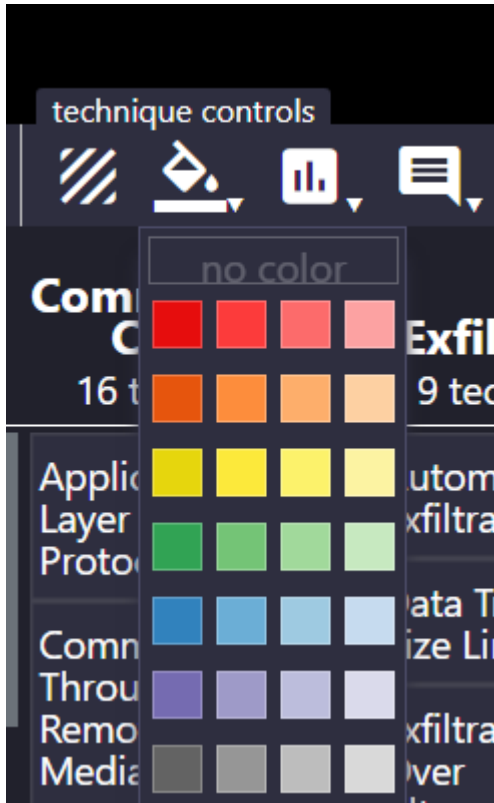
Selected techniques should now appear highlighted

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

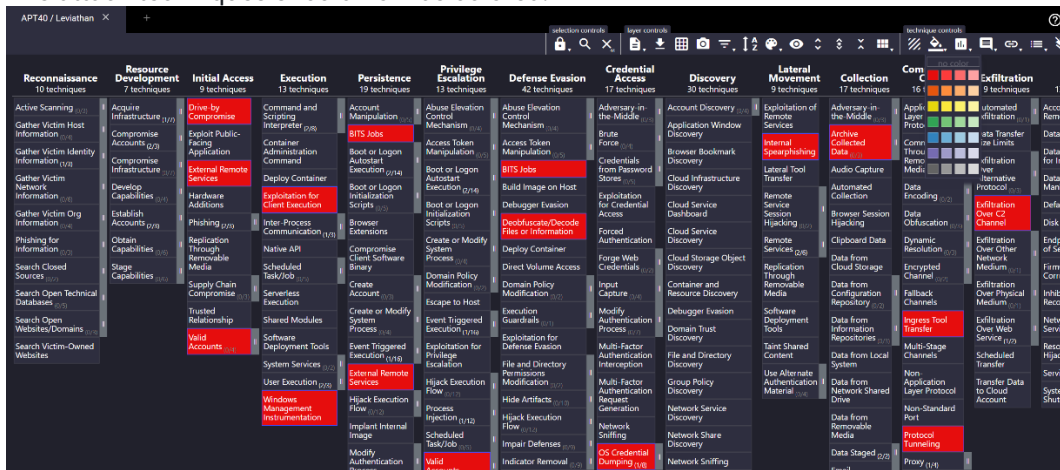


Now we want a bit more visibility in the techniques so we will select a color

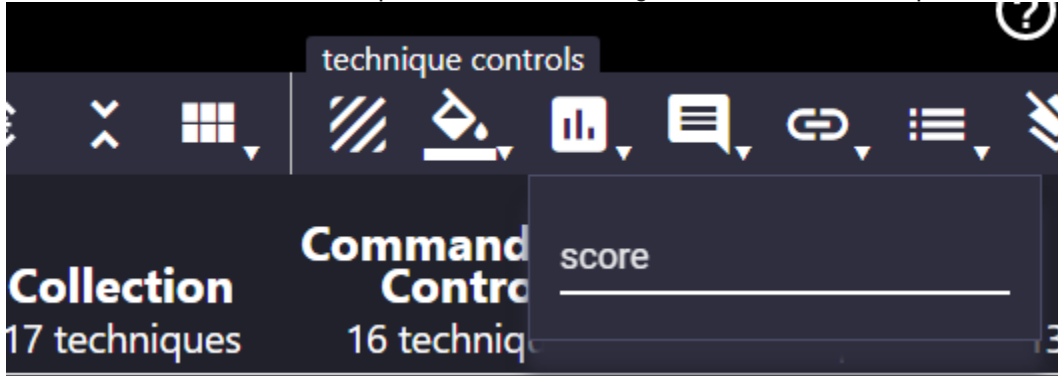
COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



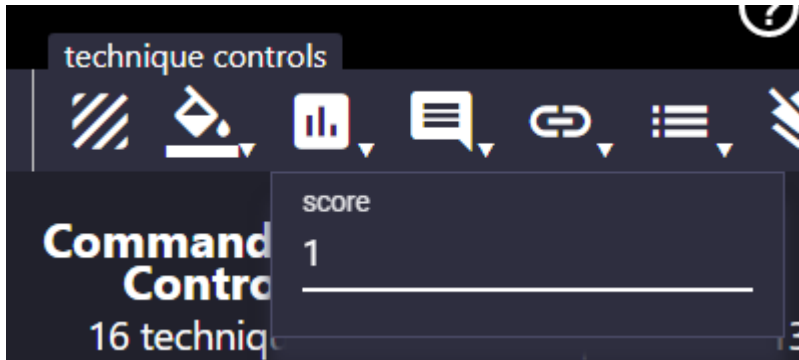
The attack techniques should now be colored.



Now we need to add a score to provide a value or weight to the attack techniques



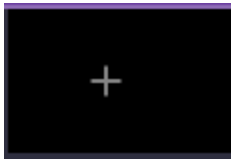
Set the value for score to 1



We've added our first known threat group now we need to add more for the industry we selected.

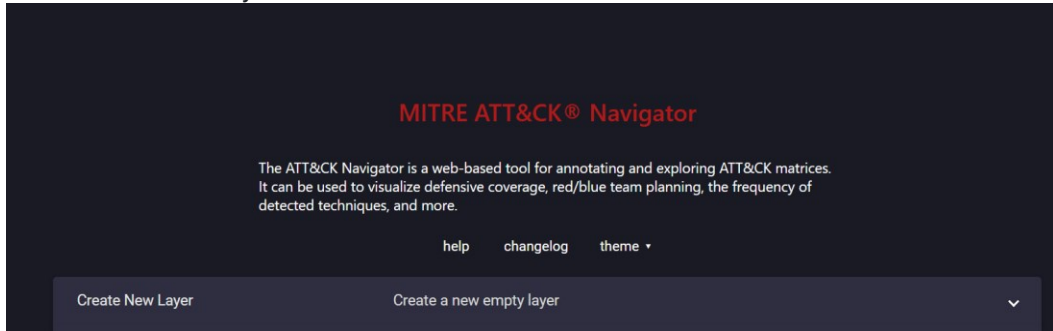
For this exercise we will add one more, but keep in mind you can add as many as you need for your threat model.

Lets add one more by clicking the +

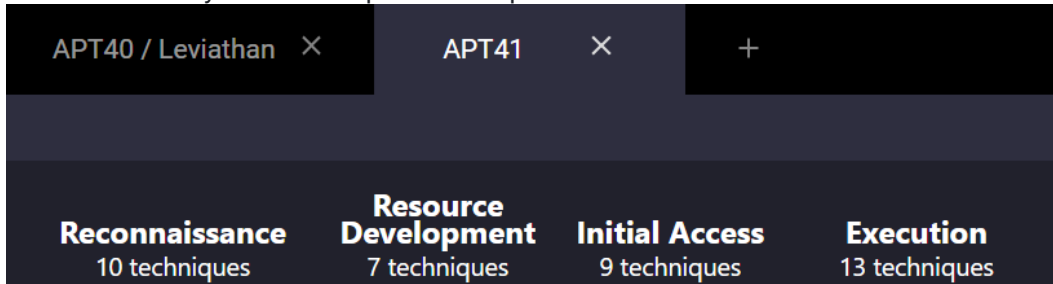




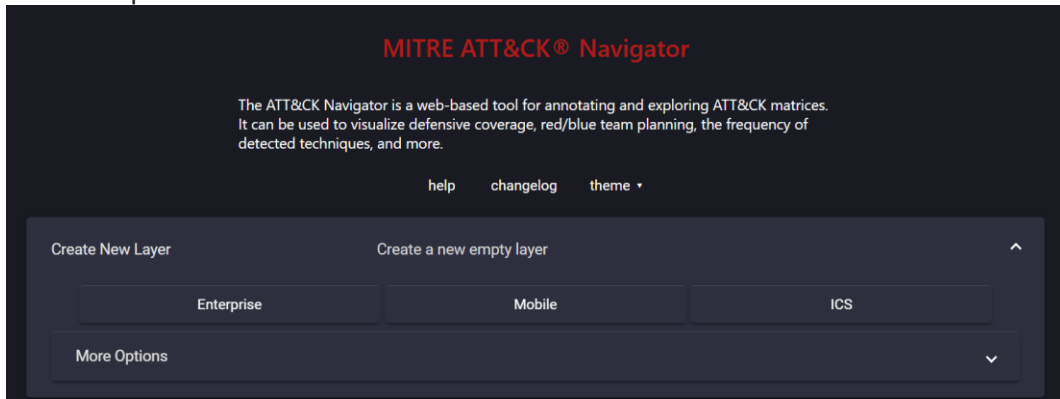
Lets create a new layer



Name the new layer like in the previous steps



Click enterprise



Click Selection Controls magnifying glass and search for the threat group

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

The screenshot displays a Cyber Security Operation Center (CSOC) interface. On the left, a sidebar lists various techniques under three main categories: **Credential Access** (17 techniques), **Discovery** (30 techniques), and **Evolution**. The **Credential Access** techniques include Adversary-in-the-Middle, Brute Force, Credentials from Password Stores, Exploitation for Credential Access, Forced Authentication, Forge Web Credentials, Input Capture, Modify Authentication Process, Multi-Factor Authentication Interception, Multi-Factor Authentication Request Generation, Network Sniffing, and OS Credential Dumping. The **Discovery** techniques include Account Discovery, Application Window Discovery, Browser Bookmark Discovery, Cloud Infrastructure Discovery, Cloud Service Dashboard, Cloud Service Discovery, Cloud Storage Object Discovery, Container and Resource Discovery, Debugger Evasion, Domain Trust Discovery, File and Directory Discovery, Group Policy Discovery, Network Service Discovery, Network Share Discovery, Network Sniffing, and Password Policy.

The main panel on the right shows a search bar with the query "apt41". Below the search bar, there are search settings for "name", "ATT&CK ID", "description", and "data sources". The results are organized into sections: **Techniques (1)** (System Network Configuration Discovery), **Threat Groups (2)** (APT41 and Earth Lusca), **Software (3)**, **Mitigations (0)**, and **Campaigns (1)**. Each threat group entry includes a "view" link and "select" and "deselect" buttons.

Validate that the threat group techniques have been selected

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

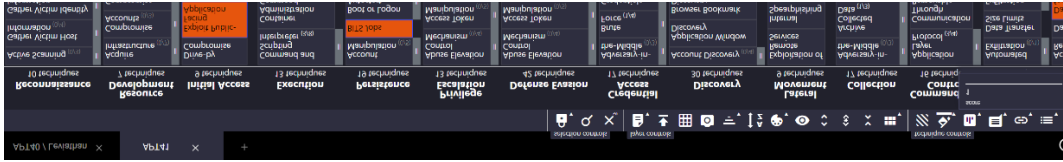
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs	Credentials from Password Stores	Browser Bookmark Discovery
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery
Gather Victim Org Information	Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Debugger Evasion	Forced Authentication	Cloud Service Dashboard
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification	Deploy Container	Forge Web Credentials	Cloud Service Discovery
Search Closed Sources	Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Direct Volume Access	Input Capture	Cloud Storage Object Discovery
Search Open Technical Databases	Trusted Relationship	Serverless Execution	Shared Modules	Create or Modify System Process	Event Triggered Execution	Execution Guardrails	Modify Authentication Process	Container and Resource Discovery
Search Open Websites/Domains	Valid Accounts	Software Deployment Tools	System Services	Event Triggered Execution	External Remote Services	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Debugger Evasion
Search Victim-Owned Websites	Windows Management Instrumentation	User Execution	System Services	External Remote Services	Hijack Execution Flow	File and Directory Permissions Modification	Multi-Factor Authentication Request Generation	Domain Trust Discovery
								File and Directory Discovery
								Group Policy Discovery
								Network Service Discovery
								Network Share Discovery
								Network Sniffing
								OS Credential Dumping
								Network Sniffing

Select the color for threat groups techniques.

The screenshot shows the MITRE ATT&CK framework interface with a search panel open on the right. The search panel includes a search bar with the text "apt41", a color selection grid, and a list of search results. The results are categorized into "Techniques (1)", "Threat Groups (2)", "Software (3)", and "Mitigations (0)". The "Threat Groups (2)" section lists "APT41" and "Earth Lucisa", each with "select" and "deselect" buttons. The "Software (3)" section lists "File and Directory Discovery", "Network Service Discovery", and "Network Share Discovery", each with "select" and "deselect" buttons. The "Techniques (1)" section lists "System Network Configuration Discovery" with "select" and "deselect" buttons.

Set the score for the techniques just as before

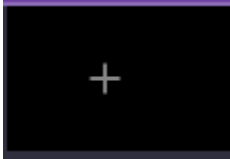
COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



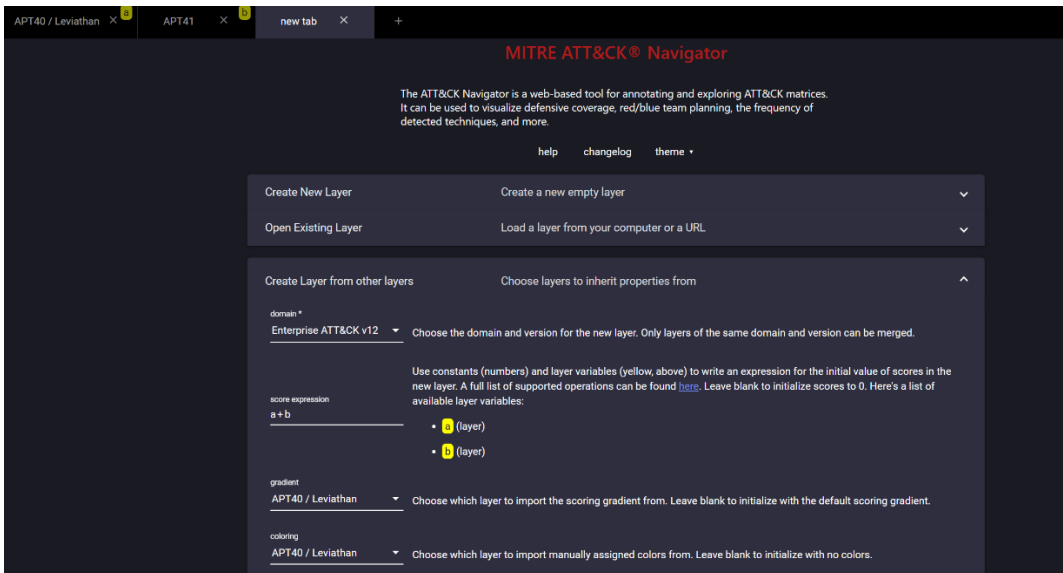
Adding up the layers to show the threat model

Now we want to add all of the layers (if you don't two that fine but you can always do more).

Lets add one more by clicking the +



Click Create Layers from other layers, domain should be Enterprise ATT&CK, Expression should be the layers you have (a+b), gradient & coloring should be your first layer



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

If you've created it correctly you should have a threat model based on the threat groups you selected, color coded with the scores added for a combined score on techniques that overlap.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
Active Scanning (9/2)	Acquire Infrastructure (1/7)	Drive-by Compromise (1/7)	Command and Scripting Interactions (1/13)	Account Manipulation (1/19)	Abuse Elevation Control Mechanism (1/13)	Abuse Elevation Control Mechanism (1/42)	Adversary-in-the-Middle (1/17)	Account Discovery (1/30)	Exploitation of Remote Services (1/9)	Adversary-in-the-Middle (1/17)	Application Layer Protocol (1/16)	Automated Exfiltration (1/9)
Gather Victim Host Information (1/10)	Compromise Accounts (1/7)	External Remote Services (1/9)	Exploit Public-Facing Application (1/13)	Remote Access (1/19)	Access Token Manipulation (1/13)	Access Token Manipulation (1/42)	Brute Force (1/17)	Application Window Discovery (1/30)	Internal Spearphishing (1/9)	Archive Collected Data (1/17)	Data Transfer Size Limits (1/16)	Data Transfer Size Limits (1/9)
Gather Victim Identity Information (1/10)	Compromise Infrastructure (1/7)	External Remote Services (1/9)	Exploit Public-Facing Application (1/13)	Remote Access (1/19)	Access Token Manipulation (1/13)	Access Token Manipulation (1/42)	Credentials from Password Stores (1/17)	Browser Bookmark Discovery (1/30)	Lateral Tool Transfer (1/9)	Audio Capture (1/17)	Communication Through Removable Media (1/16)	Exfiltration Over Alternative Protocol (1/9)
Gather Victim Information (1/10)	Develop Infrastructure (1/7)	External Remote Services (1/9)	Exploit Public-Facing Application (1/13)	Remote Access (1/19)	Access Token Manipulation (1/13)	Access Token Manipulation (1/42)	Exploitation for Credential Access (1/17)	Cloud Infrastructure Discovery (1/30)	Remote Service Session Hijacking (1/9)	Automated Collection (1/17)	Data Encoding (1/16)	Exfiltration Over Alternative Protocol (1/9)
Gather Victim Org Information (1/10)	Establish Accounts (1/7)	External Remote Services (1/9)	Exploit Public-Facing Application (1/13)	Remote Access (1/19)	Access Token Manipulation (1/13)	Access Token Manipulation (1/42)	Exploitation for Credential Access (1/17)	Cloud Service Dashboard (1/30)	Remote Service Session Hijacking (1/9)	Automated Collection (1/17)	Data Encoding (1/16)	Exfiltration Over Alternative Protocol (1/9)
Phishing for Information (1/10)	Obtain Capabilities (1/7)	External Remote Services (1/9)	Exploit Public-Facing Application (1/13)	Remote Access (1/19)	Access Token Manipulation (1/13)	Access Token Manipulation (1/42)	Exploitation for Credential Access (1/17)	Cloud Service Dashboard (1/30)	Remote Service Session Hijacking (1/9)	Automated Collection (1/17)	Data Encoding (1/16)	Exfiltration Over Alternative Protocol (1/9)
Search Closed Sources (1/10)	Stage Capabilities (1/7)	External Remote Services (1/9)	Exploit Public-Facing Application (1/13)	Remote Access (1/19)	Access Token Manipulation (1/13)	Access Token Manipulation (1/42)	Exploitation for Credential Access (1/17)	Cloud Service Dashboard (1/30)	Remote Service Session Hijacking (1/9)	Automated Collection (1/17)	Data Encoding (1/16)	Exfiltration Over Alternative Protocol (1/9)
Search Open Technical Databases (1/10)	Trusted Relationship (1/7)	External Remote Services (1/9)	Exploit Public-Facing Application (1/13)	Remote Access (1/19)	Access Token Manipulation (1/13)	Access Token Manipulation (1/42)	Exploitation for Credential Access (1/17)	Cloud Service Dashboard (1/30)	Remote Service Session Hijacking (1/9)	Automated Collection (1/17)	Data Encoding (1/16)	Exfiltration Over Alternative Protocol (1/9)
Search Open Websites/Domains (1/10)	Valid Accounts (1/7)	External Remote Services (1/9)	Exploit Public-Facing Application (1/13)	Remote Access (1/19)	Access Token Manipulation (1/13)	Access Token Manipulation (1/42)	Exploitation for Credential Access (1/17)	Cloud Service Dashboard (1/30)	Remote Service Session Hijacking (1/9)	Automated Collection (1/17)	Data Encoding (1/16)	Exfiltration Over Alternative Protocol (1/9)
Search Victim-Owned Websites (1/10)	Valid Accounts (1/7)	External Remote Services (1/9)	Exploit Public-Facing Application (1/13)	Remote Access (1/19)	Access Token Manipulation (1/13)	Access Token Manipulation (1/42)	Exploitation for Credential Access (1/17)	Cloud Service Dashboard (1/30)	Remote Service Session Hijacking (1/9)	Automated Collection (1/17)	Data Encoding (1/16)	Exfiltration Over Alternative Protocol (1/9)

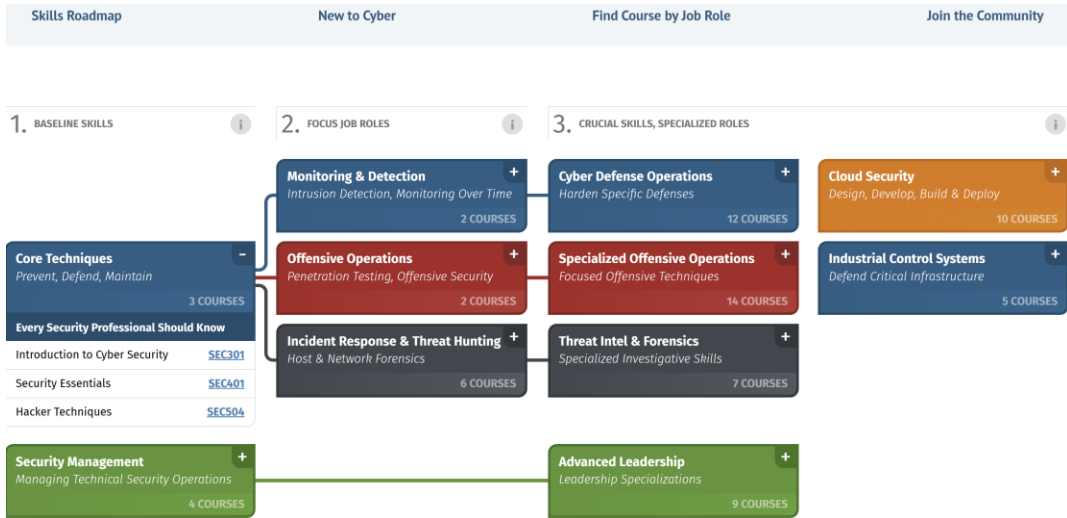
Next Steps

Next steps would be to export your threat model and use this in comparison to your known security controls, if security controls have not been identified then the threat model can provide insight on security controls for your particular use case.

Cyber Security Roadmap

Couple of things to consider that, how a SOC should be developed and what are the skills are required, training requirements for management operations are simplified in this roadmap developed in SANS, have a look at it:

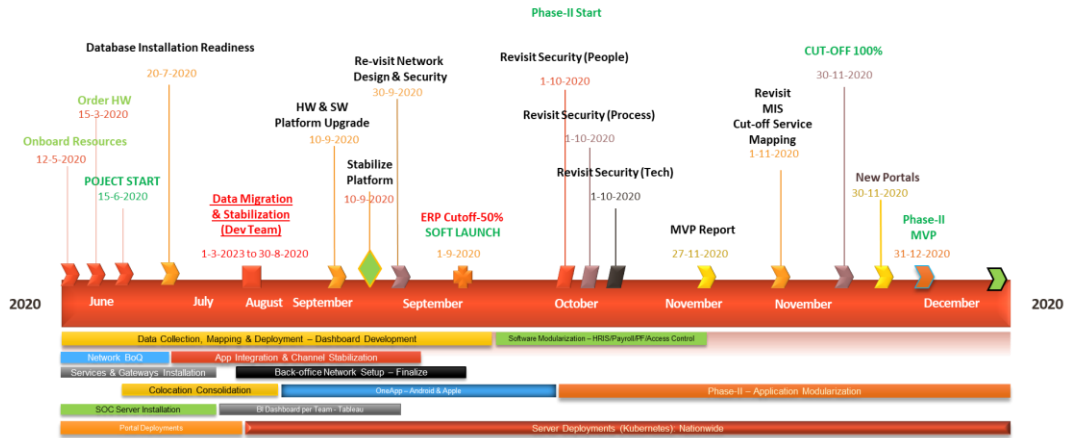
COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Source: [Cyber Security Roadmap | SANS Institute](#)

Here is a template that you can use for your internal development and use (provided as job aids named "Timeline"):

Network - Consolidation Roadmap



This illustration is for board projections (high-level), your own development should be reflected in those line items, also use a timeline generator along with a grant chart in excel for large deployment and breakdown scenario or engage a professional team who would document these for you.

EXAMPLE: Security Operations Center (SOC) in Practice

1. **Proactive Monitoring:** The SOC team gathers information from various resources, including threat intelligence feeds and log files from systems all around the enterprise. They carefully monitor the company's assets, from on-premises servers in data centers to cloud resources. Accurate data collection in monitoring is critical. Excessive and unusable data only prolongs detections engineering and false alarms.
2. **Incident Response and Recovery:** When a potential threat is detected, the SOC coordinates the organization's ability to take the necessary steps to mitigate damage and communicate properly to keep the organization running after an incident. For example, recovery can include activities such as handling acute malware or ransomware incidents.
3. **Remediation Activities:** SOC team members provide data-driven analysis that helps an organization address vulnerability and adjust security monitoring and alerting tools. For example, using information obtained from log files and other sources, a SOC member can recommend a better network segmentation strategy or a better system patching regimen.
4. **Compliance:** The SOC helps ensure that the organization is compliant with important security standards and best practices. This includes conformity to a security policy, as well as external security standards, such as ISO 27001x, the NIST Cybersecurity Framework (CSF), and the General Data Protection Regulation (GDPR).
5. **Coordination and Context:** A SOC team member helps an organization coordinate disparate elements and services and provide visualized, useful information. Part of this coordination is the ability to provide a helpful, useful set of narratives for activities on the network.

In addition to these practices, the SOC performs preventative maintenance such as applying software patches and upgrades, and continually updating firewalls, whitelists and blacklists, and security policies and procedures.

ISO/IEC 27001:2022 Control Requirements

Though this is out of context, these controls are also reflected in the SIEM, that generates compliance report for the ISO/IEC 27001.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

The below list is almost freely provided by Andrey Prozorov in his Patreon site, subscribe to his account for his guidance documents, and you will be able to get together a plan for your company and for your own enrichment. These documents are professionally developed and has a rich content store.

ISO 27001:2022. ISMS Requirements and Information security controls

5. Organizational controls	6. People controls	8. Technological controls
5.1. Policies for information security 5.2. Information security roles and responsibilities 5.3. Segregation of duties 5.4. Management responsibilities 5.5. Contact with authorities 5.6. Contact with special interest groups 5.7. Threat intelligence 5.8. Information security in project management 5.9. Inventory of information and other associated assets 5.10. Acceptable use of information and other associated assets 5.11. Return of assets 5.12. Classification of information 5.13. Labelling of information 5.14. Information transfer 5.15. Access control 5.16. Identity management 5.17. Authentication information 5.18. Access rights 5.19. Information security in supplier relationships 5.20. Addressing information security within supplier agreements 5.21. Managing information security in the ICT supply chain 5.22. Monitoring, review and change management of supplier services 5.23. Information security for use of cloud services 5.24. Information security incident management planning and preparation 5.25. Assessment and decision on information security events 5.26. Response to information security incidents 5.27. Learning from information security incidents 5.28. Collection of evidence 5.29. Information security during disruption 5.30. ICT readiness for business continuity 5.31. Legal, statutory, regulatory and contractual requirements 5.32. Intellectual property rights 5.33. Protection of records 5.34. Privacy and protection of PII 5.35. Independent review of information security 5.36. Compliance with policies, rules and standards for information security 5.37. Documented operating procedures	6.1. Screening 6.2. Terms and conditions of employment 6.3. Information security awareness, education and training 6.4. Disciplinary process 6.5. Responsibilities after termination or change of employment 6.6. Confidentiality or non-disclosure agreements 6.7. Remote working 6.8. Information security event reporting 7. Physical controls 7.1. Physical security perimeter 7.2. Physical entry 7.3. Securing offices, rooms and facilities 7.4. Physical security monitoring 7.5. Protecting against physical and environmental threats 7.6. Working in secure areas 7.7. Clear desk and clear screen 7.8. Equipment siting and protection 7.9. Security of assets off-premises 7.10. Storage media 7.11. Supporting utilities 7.12. Cabling security 7.13. Equipment maintenance 7.14. Secure disposal or re-use of equipment	8.1. User endpoint devices 8.2. Privileged access rights 8.3. Information access restriction 8.4. Access to source code 8.5. Secure authentication 8.6. Capacity management 8.7. Protection against malware 8.8. Management of technical vulnerabilities 8.9. Configuration management 8.10. Information deletion 8.11. Data masking 8.12. Data leakage prevention 8.13. Information backup 8.14. Redundancy of information processing facilities 8.15. Logging 8.16. Monitoring activities 8.17. Clock synchronization 8.18. Use of privileged utility programs 8.19. Installation of software on operational systems 8.20. Network security 8.21. Security of network services 8.22. Segregation of networks 8.23. Web filtering 8.24. Use of cryptography 8.25. Secure development life cycle 8.26. Application security requirements 8.27. Secure system architecture and engineering principles 8.28. Secure coding 8.29. Security testing in development and acceptance 8.30. Outsourced development 8.31. Separation of development, test and production environments 8.32. Change management 8.33. Test information 8.34. Protection of information systems during audit testing *New controls, 2022
ISMS Requirements (ISO 27001) 4. Context of the organization 4.1 Understanding the organization and its context / 4.2 Understanding the needs and expectations of interested parties / 4.3 Determining the scope of the ISMS / 4.4 ISMS 5. Leadership 5.1 Leadership and commitment / 5.2 Policy / 5.3 Organizational roles, responsibilities and authorities 6. Planning 6.1 Assessing risks and opportunities / 6.2 Information security objectives and planning to achieve them / 6.3 Planning of changes 7. Support 7.1 Resources / 7.2 Competence / 7.3 Awareness / 7.4 Communication / 7.5 Documented information 8. Operation 8.1 Operational planning and control / 8.2 Information security risk assessment / 8.3 Information security incident management 9. Performance evaluation 9.1 Monitoring, measurement, analysis and evaluation / 9.2 Internal audit / 9.3 Management review 10. Improvement 10.1 Corrective improvement / 10.2 Nonconformity and corrective action		

by Andrey Prozorov, CISM, CIPP/E, CDPSE, LA 27001 - www.patreon.com/AndreyProzorov

Control: measure that maintains and/or modifies risk

A new 2022 version of the ISO/IEC 27001 has been released and the added controls are marked green. Though it may seem that there are a lot of options to comply with the control pack, only a handful of documents is mandatory for achieving the certification.

For your baseline security requirements, do consult or develop on your own, but do maintain a mapping for the ISO, use the below Minimum Security Baseline (MSB) document:

SL	ICT Security Requirements	Compliance (full, partial)	Remarks (for partial compliance)	Documents Reference
1	ICT Steering Committee formation and periodic meeting	Non-compliant	Planned	After go-live
2	ICT Security Committee and periodic meeting	Non-compliant	Planned	After go-live

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



3	ICT risk management committee formation and periodic meeting	Non-compliant	Planned	After go-live
4	Approved ICT security Policy.	Full Compliant	document ready, to be signed	02 Information Security Program Policy
5	Organogram for ICT departments/divisions. Branch organogram with ICT support unit.	Full Compliant	Approved document ready	
6	Job Description (JD) for ICT personnel.	Full Compliant	document ready, to be signed	
7	Fallback plan for various level of system support personnel.	Full Compliant	document ready, to be signed	
8	Segregation of duties for ICT tasks.	Full Compliant	document ready, to be signed	Roles and Responsibilities for Contingency Planning
9	Operating Procedure for all ICT functional activities (e.g. Backup Management, Database Management, Network Management, Scheduling Processes, System Start-up, Shut-down, Restart and Recovery).	Full Compliant	document ready, to be signed	Operating_Procedures_for_Information_and_Communication_Technology_Final
10	Operating procedure of Core Applications.	Non-compliant	Planned	After go-live
11	Detailed design document for all ICT critical systems/services (e.g. Data Center design, Network design, Power Layout for Data Center, etc.).	Full Compliant		All in documents
12	Documents regarding Standard Certification.	Full Compliant	document ready, to be signed	
13	Insurance/Risk Coverage Fund document. Policy to use risk coverage fund.	Non-compliant	to be obtain, policy remain	01 IT Risk Management Policy, insurance is yet to be funded,



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

				AML-CFT being formulated
14	ICT Risk Management Committee (Formation document, Meeting minutes etc.)	Non-compliant	Planned	After go-live
15	ICT Risk Management Framework.	Full Compliant		05. Risk_Assessment_and_Risk_Treatment_Methodology_Final
16	Documentation about risk management system for any new process a. Assessment of the risk b. Identification of mitigation control c. Remedial plan to reduce the risk	Full Compliant	Risk Policy available	05. Risk_Assessment_and_Risk_Treatment_Methodology_Final
17	Approval of the risk acknowledgement from the owner of the risk (if any)	Full Compliant		05. Risk_Assessment_and_Risk_Treatment_Methodology_Final
18	defining Risk Appetite & Risk Tolerance & board approval.	Full Compliant		No board approval yet
19	Key Risk Indicators (KRIs) documents	Full Compliant	Risk Policy available	08_Appendix_1_Risk_Assessment_Table_Final
20	Information System Risk Assessment procedure document.	Full Compliant	Risk Policy available	08_Appendix_1_Risk_Assessment_Table_Final
21	Change management procedure document for Information Systems	Full Compliant		26 Change Management Policy
22	Incident management framework & Incident log register	Full Compliant		19. Incident procedure 20. Incident Management Process + 21. Incident Log
23	Problem management process.			

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

2 4	ICT Emergency Response Team with role and responsibilities.	Full Compliant	team to be formed	Roles and Responsibilities for Contingency Planning
2 5	ICT incident response plan & process	Full Compliant	team to be formed	19. Incident procedure 20. Incident Management Process + 21. Incident Log
2 6	Incident escalation matrix	Full Compliant	Escalation matrix to be define	19. Incident procedure 20. Incident Management Process + 21. Incident Log
2 7	ICT Asset Management policy/Procedure. Documents related to ICT Asset Classification and Asset custodianship/ownership.	Full Compliant		Information_As set_Inventory
2 8	Inventory of all ICT assets.	Full Compliant		Information_As set_Inventory
2 9	Secure Disposal policy and procedure. Policy to return back organizational assets from employees/external parties upon termination of their employment, contract or agreement.	Full Compliant		16 Information and Media Disposal Policy
3 0	End user device Standardization/Hardening procedure/policy.	Full Compliant		11 Personally Owned Device (BYOD) Security Policy
3 1	Approve list of Software which will only be used in any computer.	Full Compliant	to be list	41.IT Capability Maturity Framework, 20 Access Control Policy
3 2	Domain Controller and Password control policy.	Full Compliant		20 Access Control Policy

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



3 3	Licenses of Software - OS, DB, Anti-Virus, MS Office, MS Exchange Server, Backup Agent, and other standard application (if any).	Full Compliant	Ordered for Microsoft Office365	All are licensed and accounted for
3 4	Bring Your Own Device (BYOD) policy and procedure.	Full Compliant		11 Personally Owned Device (BYOD) Security Policy
3 5	physical Access authorization procedures/policy at data center.	Full Compliant		20 Access Control Policy, 24 Physical Security Policy
3 6	Fire Prevention policy and firefighting team information. Fire drill	Partial Compliant		Not started @ Bulu, Datacenter has FM200
3 7	Baseline standards for Operating Systems, Databases, Network equipment, security equipment	Full Compliant		22 Network Security Management Policy, CISECURITY Benchmarks
3 8	Network design (LAN, WAN) document including protocols and security features. a) Total Bandwidth used b) No of Fiber communication link with vendor name c) Network security devices	Full Compliant		
3 9	Documentation for server OS hardening.	Full Compliant		CISECURITY Benchmarks
4 0	Cryptographic key management policy and procedures.	Full Compliant		31 Encryption and Key Management Policy
4 1	Email and internet usage policy.	Full Compliant		14 Information Exchange Policy
4 2	Cyber Security policy.	Full Compliant		In general all are included in multiple policies, Cybersecurity



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

				Policy, 30 Security Incident Response Policy, 32 Data Breach Response Policy
4 3	Internal and external Penetration Testing and/or Vulnerability Testing report.	Non-compliant	To be done after UAT	Not started yet, will start after all UAT and datacenter readiness achieved
4 4	Patch Management policy.	Full Compliant		27 System Configuration Management Policy
4 5	Security monitoring systems and processes.	Full Compliant		36 Log Management and Monitoring Policy
4 6	Password policy.	Full Compliant		High Level Information security policy
4 7	Privileged Access Management procedure	Full Compliant		Access_Control_Policy
4 8	Business Continuity Plan (BCP).	Full Compliant		34 IT Business Continuity Policy
4 9	Disaster Recovery Plan (DRP) and DR test documentations.	Full Compliant		BCP, plan is ready, not tested yet, will run if after UAT
5 0	Backup & Restore Plan /Policy (BRP). The backup inventory and log sheets.	Full Compliant		33 Backup and Recovery Policy
5 1	Acquisition and Development of Information Systems	Full Compliant		37 Acquiring Information Systems And Services

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

52	ICT Project management framework.	Full Compliant		Roles and Responsibilities for Contingency Planning
53	ICT Asset Procurement Policy. Vendor selection process	Non-compliant		SCM would share their part of the policy
54	List of software with vendor information (Outsourcing and in-house), emergency support contact information	Full Compliant		IT-CMF, 41.IT Capability Maturity Framework
55	Software with user manual & Technical Documentations.	Partial Compliant		Documentations are ongoing
56	Secure Software Development Life Cycle (SDLC) for in-house software.	Full Compliant		Secure software development
57	Secure testing life cycle for in house software	Full Compliant		Secure software development, SQA Test Cases
58	Log management policy	Full Compliant		36 Log Management and Monitoring Policy
59	Data retention policy	Full Compliant		35 Customer Data Privacy Management Policy + 33 Backup and Recovery Policy
60	List of all service providers.	Partial Compliant		SCM will come up with the relevant resources
61	Contingency plan for critical outsourced technologies.	Full Compliant		BCP
62	Support level agreement for the software /hardware	Full Compliant		
63	Confidentiality agreement between vendor and bank.	Full Compliant		
64	Cloud security policy	Full Compliant		10 Cloud Computing Security Policy

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

65	Cross boarder data storing policy	Non-compliant		
66	Cyber security awareness plan	Non-compliant		Planned
67	Customer cyber security awareness plan	Non-compliant		Planned
68	Mobile app security policy , API security & web application security policy	Full Compliant		all minimum baseline documents are outlined
69	Detail audit trail of Database and applications	Full Compliant		Internal Audit plan, team, Procedure (45,46,49,31) + 36 Log Management and Monitoring Policy, Log shipping by default
70	How sensitive data management i.e. balance nid, dob, mother name, mobile number, email address, nominee, passport number	Full Compliant		35 Customer Data Privacy Management Policy
71	Server access with 2FA	Full Compliant		Access_Control_Policy, PEM files
72	Mobile app security with 2FA	Full Compliant		09 Mobile Computing Security Policy, Customer app does not have 2FA
73	Remote access management	Full Compliant		25 Remote Access Security Policy
74	Vendor access management	Full Compliant		17 Third Party Security Policy
75	Work from home policy	Full Compliant		00 High-Level Information Security Policy

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



				+ Remote Working Security Policy
7 6	Source code security	Full Compliant		29 Application Development Security Policy
7 7	Source code leakage prevention	Full Compliant		29 Application Development Security Policy
7 8	Sensitive data leakage prevention	Full Compliant		Application control
7 9	Maker and checker in all action in the application	Full Compliant		Application control
8 0	Email security	Full Compliant		High Level Information Security Policy
8 1	Web security	Full Compliant		MSB
8 2	End point security	Full Compliant		High Level Information Security Policy
8 3	Central log management	Full Compliant		App Control, ELK Stack. 36 Log Management and Monitoring Policy





CHAPTER

6

Processes for a SOC

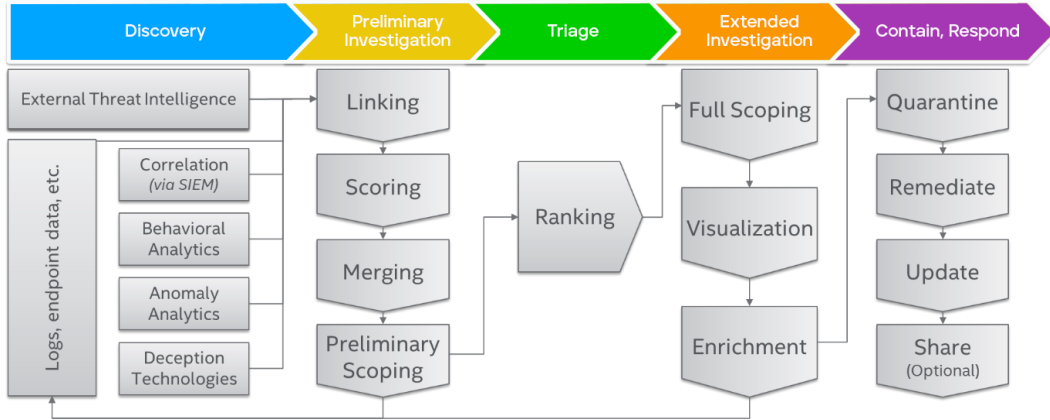
ALONG CAME A SPIDER, DEEPER MAPPING OF ATT&CK FRAMEWORKS ON ENTERPRISE NETWORKS WITH MATRIX AND KPI'S. ALWAYS THINK OF ENTERPRISE GRADE, ALWAYS.

Security operations need to set standards for when manual analysis is needed before an analyst handles alerts. They also need to use alerting strategies to decide what alerts analysts should focus on. Alerting strategies cover the alert's purpose, importance, sources, technical details, validity, and use cases. Palo Alto Networks follows the Alert Detection Strategy (ADS) framework, which aligns with the MITRE ATT&CK Framework. The ATT&CK Framework helps an engineer classify and rank alerts for further investigation. A clear alerting strategy lets analysts watch over relevant alerts and start researching an incident. Automation also helps to make alerts more precise and avoid false alarms.

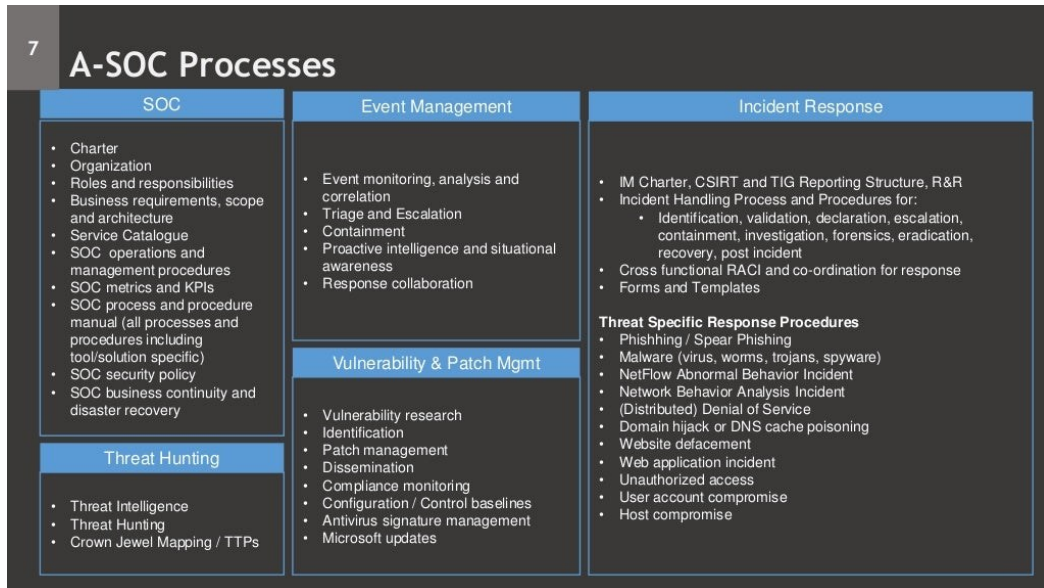


COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER


A security operation center (SOC) is a team of experts that monitor and respond to potential security threats to an organization's IT infrastructure. A SOC typically follows a set of processes to perform its functions, such as:



Source: [What Is a Security Operations Center \(SOC\)? | Trellix](#)



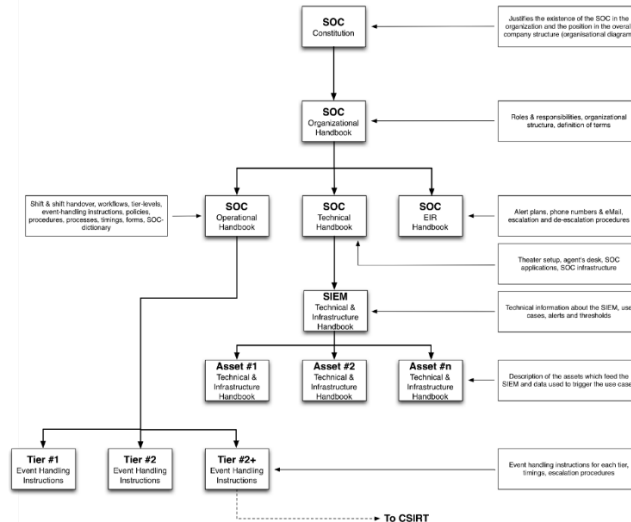
Source: [SOC Architecture \(Tech Stack, Process, Org Structure, People Skills\) | PPT \(slideshare.net\)](#)

- 
- **Event classification and triage:** The process of collecting, filtering, and categorizing security events and alerts from various sources, such as network devices, endpoints, applications, and logs. This process helps to identify and prioritize the most relevant and critical events that require further analysis and action.
 - **Prioritization and analysis:** The process of investigating and validating security events and alerts, using various tools and techniques, such as threat intelligence, correlation, enrichment, and root cause analysis. This process helps to determine the nature, scope, and impact of security incidents, as well as the appropriate remediation steps.
 - **Remediation and recovery:** The process of containing, eradicating, and restoring the normal operations of the affected systems, services, and data, using various tools and techniques, such as isolation, patching, backup, and restore. This process helps to mitigate and resolve security incidents, as well as to prevent or minimize the recurrence of similar incidents.
 - **Assessment and audit:** The process of evaluating and verifying the effectiveness and compliance of the SOC's tools, processes, and performance, using various tools and techniques, such as metrics, indicators, reports, and audits. This process helps to measure and improve the SOC's capabilities and maturity, as well as to comply with relevant regulations and standards.

These are some of the common processes for a SOC, but they may vary depending on the size, scope, and needs of the different types of organization. I hope this helps you understand what processes are to be established for a SOC.



Documentation Framework for a Security Operation Center



Source: [The SOC methodology - SecureGlobal](#)

Creating a documentation framework for your security operation center (SOC) would be a very complex and challenging task that requires careful planning, research, and execution. However, it can also be rewarding and beneficial for your organization's security posture and performance, as your SOC maturity levels increase. In a year or two your SOC would have a plethora of case files, rules 'fine-tuned' to 'an excellence', ingestion rules and all.

Case documentation is a complete record of what happened during an incident response. It helps SOC teams use their previous knowledge and insights to handle incidents better in the future. It also makes it easier for team members and stakeholders to work together, communicate clearly, and improve their processes and security operations. By keeping case documentation precise and thorough, SOC teams can boost their incident response skills and defend organizations from emerging cyberthreats.

Here are some general steps that you can follow to create a documentation framework for your SOC:

1. **Define the scope and objectives** of your SOC. What are the main functions, processes, roles, and technologies that your SOC will perform and use? What are

the expected outcomes and benefits of your SOC? How will you measure and report them?

2. **Review the existing documentation frameworks** and standards for SOCs. You can use them as references and sources of best practices for your own framework. Some examples are OWASP (Open Web Application Security Project) SOC - Security Operations Centre Framework Project, NIST SP 800-61 Revision 2 - Computer Security Incident Handling Guide, and ISO/IEC 27035:2016 - Information technology - Security techniques - Information security incident management.
3. **Design and document your SOC framework** based on your scope and objectives. You should cover the key functions of your SOC, such as threat intelligence, security monitoring, incident management, and quality assurance. You should also define the roles and responsibilities of your SOC staff, the tools and technologies that they will use, and the methodologies and procedures that they will follow.
4. **Implement and test your SOC framework.** You should deploy and configure your SOC tools and technologies, train and onboard your SOC staff, and establish and practice your SOC processes and procedures. You should also conduct regular tests and drills to evaluate and improve your SOC framework.

Traditional Tools

- **Security Information and Event Management (SIEM)**
- Governance, risk and compliance (GRC) systems
- Vulnerability scanners and penetration testing tools
- Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and wireless intrusion prevention
- Firewalls, Next-Generation Firewalls (NGFW) which can function as an IPS, and Web Application Firewalls (WAF)
- Log management systems (commonly as part of the SIEM)
- Cyber threat intelligence feeds and databases

Next-Gen Tools

- **Next-generation SIEMs** which are built on big data platform and includes machine learning and advanced behavioral analytics, threat hunting, built-in incident response and SOC automation
- Network Traffic Analysis (NTA) and Application Performance Monitoring (APM) tools
- Endpoint Detection and Response (EDR), which helps detect and mitigate suspicious activities on hosts and user devices
- User and Entity Behavior Analytics (UEBA), which uses machine learning to identify suspicious behavioral patterns

Source: [SOC vs. SIEM: Understanding The Role of SIEM Solutions in the SOC \(exabeam.com\)](https://www.exabeam.com/blog/soc-vs-siem-understanding-the-role-of-siem-solutions-in-the-soc)

5. **Monitor and review your SOC framework.** You should collect and analyze data and feedback from your SOC operations, such as security events, alerts, incidents, metrics, and indicators. You should also conduct periodic audits and reviews to assess and verify your SOC framework's effectiveness and compliance.
6. **Update and improve your SOC framework.** You should identify and address any gaps, issues, or challenges that arise from your SOC operations, such as new or emerging threats, vulnerabilities, or risks. You should also incorporate any changes, enhancements, or innovations that can improve your SOC framework's efficiency and agility.

Escalation Process

The business and security operations teams require a clear set of guidelines to enhance an organization's awareness of potential issues and to obtain the essential support for mitigation. When a lower-severity alert requires escalation, it should be prioritized and receive the necessary escalation as needed. Escalation can take place either within SecOps staff tiers or between affiliating teams.

Within security operations, escalation can happen among staff tiers when an alert falls beyond the scope of what an analyst can manage. These escalations serve as valuable learning opportunities for analysts. As organizations increasingly automate security operations, the necessity for escalation diminishes, granting tier-3 analysts additional time to concentrate on projects aimed at producing higher-fidelity alerts.


At times, an alert may necessitate additional information from an affiliating team. Interface agreements should be established between affiliating teams and the security operations team, defining expectations during an escalation. These agreements should specify the severity level at which increased awareness from the business becomes necessary. They should also outline documentation parameters and clearly state communication expectations for all stakeholders. Impactful interface agreements document an escalation matrix, highlighting specific scenarios and associated escalation steps. Regular updates and reviews of these agreements are crucial to maintain accuracy, including provisions for backup contacts and procedures to address unresponsiveness.

Incident Distribution

By giving analysts' the duty to deal with various kinds of alerts, they not only gain more knowledge and skills, but also learn how to handle different scenarios.

Analysts are always learning new things and becoming more versatile in their field when they face different alert types. Sharing incidents among analysts makes sure that they know how to use the available tools and prevents them from only working on familiar alerts. This way of working promotes a proactive attitude, which helps analysts to manage any alert with more speed, efficiency, and effectiveness. In addition, dealing with diverse alert types trains analysts. By interacting with different alerts regularly, analysts acquire the ability to quickly evaluate the urgency and importance of each case, then assign and use resources wisely.

This exposure to diverse alert types sharpens their skills to spot patterns, detect anomalies, and notice key signs, which helps them to act fast and make smart decisions. In summary, the deliberate distribution of diverse alerts to analysts encourages constant



improvement, which enables them to broaden their skills, stay flexible, and keep up with changing threats. It builds a dynamic environment that fosters continual learning, improves problem-solving abilities, and boosts the overall performance of the security operations team.

Investigation

Analysts collect background information in the initial research phase, but they look for the evidence in the investigation phase to better comprehend the incident. An analyst should act like a detective during the investigation. It's a hands-on process that reveals the who, what, when, where, why and how (5W1H) of an incident.

In the investigation phase, all the important information is collected and any missing pieces from the initial research are filled. This involves finding out the IT assets and business services that are affected and checking how well the existing containment measures work, which guide the next steps of mitigation. The main aim is to get a complete picture of the security incident, including how much damage it can cause, what the attacker wants and how well different containment measures can stop them. With this vital information, the analysts can choose the best containment and mitigation plan.

The investigation process is very important for verifying the reality of an incident, enabling analysts to tell apart true incidents and false positives with certainty. When a false positive occurs, giving feedback to content engineers or the security engineering team is necessary for adjusting alerts or changing controls, depending on the case. This feedback loop guarantees continuous enhancement and refinement of the SOC's detection and response skills.

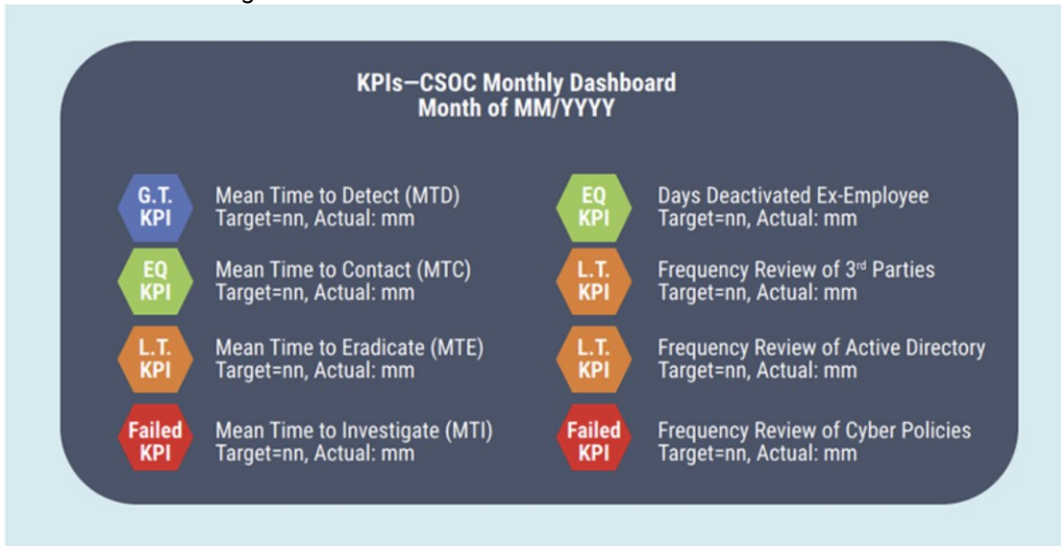
By doing careful investigations, the SOC improves its skill to deal with security incidents, reduce the harm of threats and boost overall incident management. The SOC can also keep improving its methods and increase its skill to find and handle future incidents with precision and speed.

Challenges for SOC Development

Developing a Security Operations Center (SOC) can be a complex task with challenges all over the SOC system. Here are some common one's:

1. **Staffing and Skills:** Finding and retaining skilled cybersecurity professionals can be difficult due to the global shortage of such professionals.
2. **Budget Constraints:** Establishing and maintaining a SOC can be expensive. It requires investment in technology, infrastructure, and personnel.

3. **Keeping Up with Evolving Threats:** Cyber threats are constantly evolving, and SOC's must continually update their knowledge and tools to keep up.
4. **False Positives:** SOC's often deal with a high volume of alerts, many of which are false positives. This can lead to alert fatigue and overlooked threats.
5. **Integration of Tools:** SOC's use a variety of tools, and integrating these tools can be a challenge.




6. Source: [Best Practices for Setting Up a Cybersecurity Operations Center \(isaca.org\)](https://www.isaca.org)
7. **Regulatory Compliance:** SOC's must ensure that they are compliant with various regulatory standards, which can be complex and time-consuming.
8. **Measuring Effectiveness:** It can be difficult to measure the effectiveness of a SOC. Key performance indicators (KPIs) need to be defined and tracked.
9. **Continuous Improvement:** SOC's need to continuously improve their processes and skills to stay effective.


These challenges can be addressed through careful planning, ongoing training, use of automation and AI, and regular review of SOC processes and procedures.

Cyber Resiliency Scoring and Metrics

Cyber resiliency scoring methods and metrics are tailorable resources to aid systems engineers, program managers, and others supporting risk management for systems or programs in which cyber resiliency is a concern. A scoring system and a set of metrics



are only meaningful in the context of programmatic and engineering decisions, under risk framing assumptions (in particular, assumptions about cyber threats, as well as assumptions about operating conditions). Scores and metrics are produced in the course of analysis activities, guide subsequent analysis activities, and support decisions regarding the need for and selection of alternative solutions.



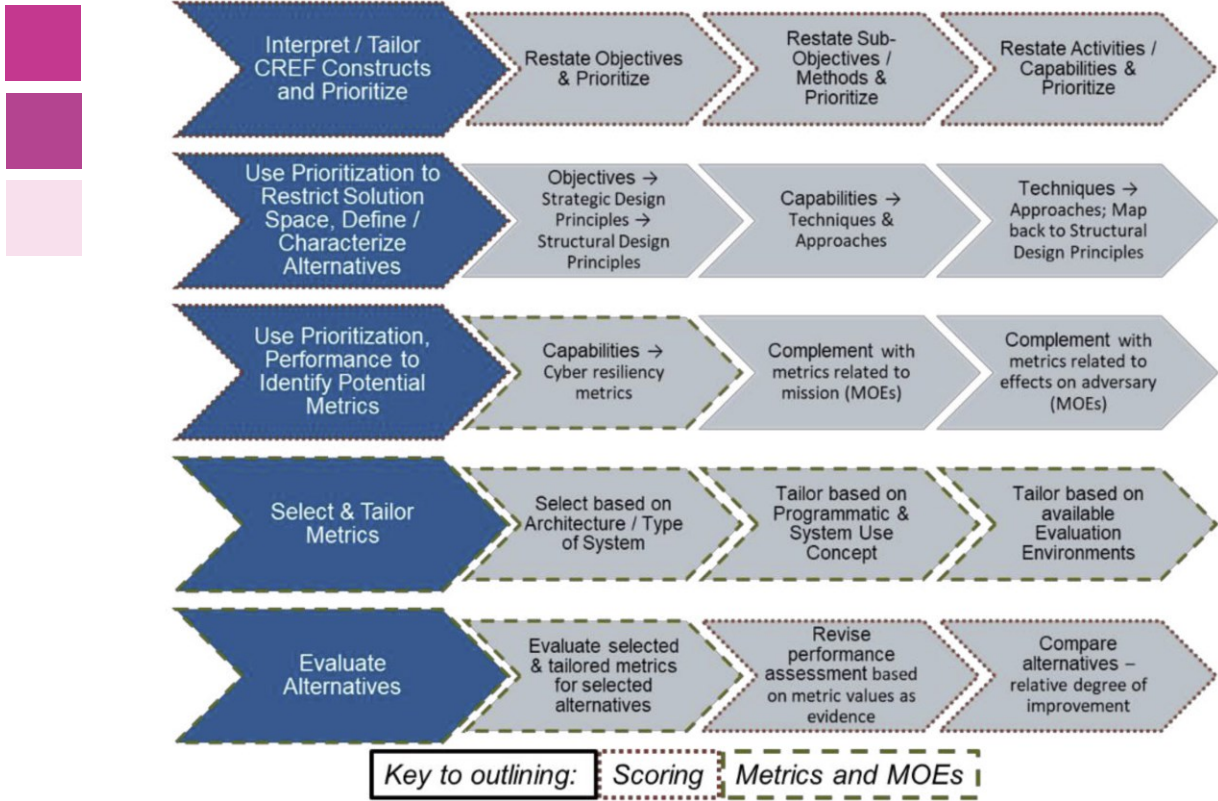
Below picture illustrates the overall concept of use for the cyber resiliency scoring methodology and metrics catalog described in this paper. The process uses the Cyber Resiliency Engineering Framework (CREF), Systems engineering tasks in which the scoring methodology is used are outlined in red; those which use the catalog are outlined in green.

The scoring methodology is used in the first two steps, as the relative priorities of cyber resiliency objectives, subobjectives, and capabilities are assessed and used to restrict the solution space. The scoring methodology is also used in the third step, as a bridge to the catalog.

Source: MITRE, check the job aid folder for the file named “prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf”



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



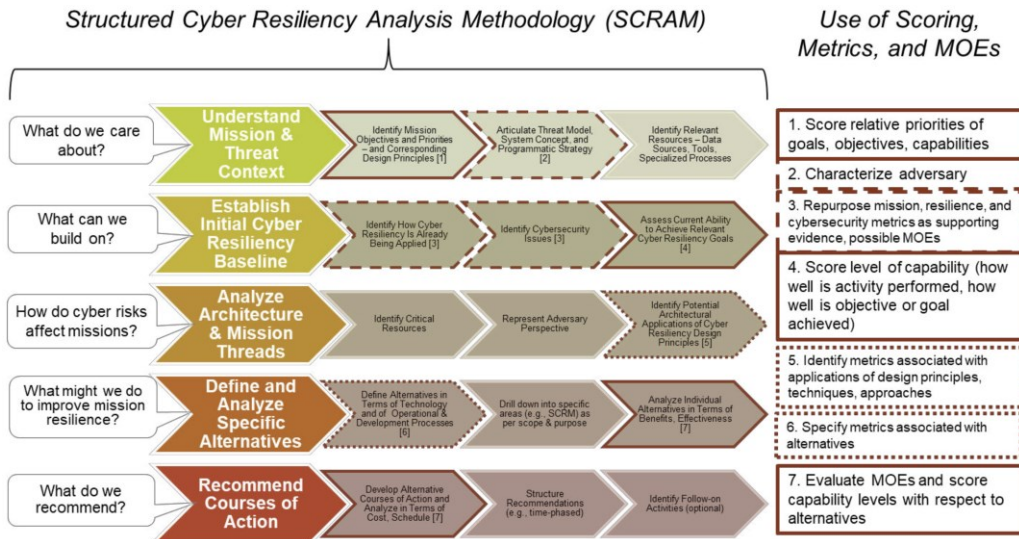
The below figure indicates how this concept fits into the Structured Cyber Resiliency Analysis Methodology (SCRAM). Tailoring and prioritizing objectives, sub-objectives, and capabilities.

- (1) in the context of a defined threat model, system concept, and programmatic strategy.
- (2) are an outcome of the first step in © 2018 The MITRE Corporation. 2 SCRAM, Understand the mission and threat context. The second step includes identifying how cyber resiliency is already being applied and any cybersecurity issues. Identifying these can indicate existing metrics which could be repurposed for cyber resiliency.
- (3). The results of the identification are used in the initial baseline assessment.
- (4) or scoring, the final task in the second step of SCRAM. In the third step, potential applications of cyber resiliency design principles, techniques, and implementation approaches are identified; metrics associated with these can be identified.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

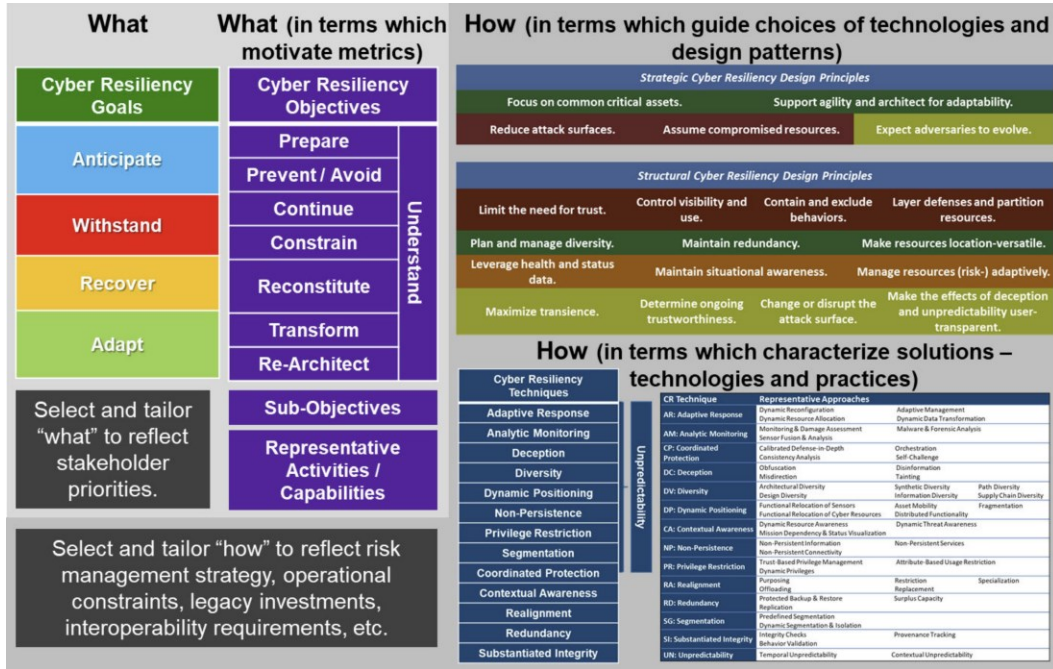
(5) from the metrics catalog. Alternatives are identified in the fourth step, enabling the metrics from the catalog and the metrics identified earlier (3) to be specified in enough detail that they can be evaluated to support comparisons.

(6). MOEs (Measures of Effectiveness) and metrics, and scores which are informed by these, are evaluated at the end of the fourth step and revisited at the start of the fifth and final step of SCRAM (7).



Source: MITRE, check the job aid folder for the file named “prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf”

CREF At-a-glance



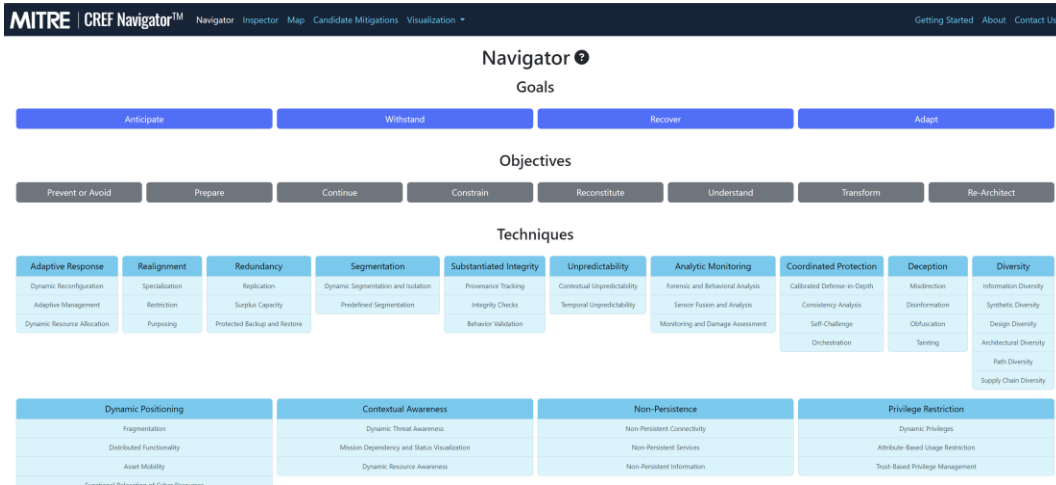
CREF Objectives (The Purple Column)

- **Prevent** or **avoid** – Preclude the successful execution of an attack or the realization of adverse conditions.
- **Prepare** – Accept that adversity will occur and maintain a set of realistic responses to address anticipated adversity.
- **Continue** – Maximize the duration and viability of essential mission or business functions during adversity.
- **Constrain** – Limit damage from adversity inflicted on high-value assets, such as those that store or process sensitive information or support mission-essential capabilities.
- **Reconstitute** – Restore as much mission or business functionality as possible after adversity, while ensuring that the restored resources are trustworthy.
- **Understand** – Maintain useful representations of mission and business dependencies and the status of resources with respect to possible adversity. (Note that this objective supports all the others.)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

- **Transform** – Modify mission or business functions and their supporting processes to better handle adversity. This can include tactical changes to procedures or configurations, as well as broader modifications like restructuring governance responsibilities or operational processes.
- **Re-architect** – Modify system, mission and supporting architectures to handle adversity more effectively.

MITRE's CREF Navigator



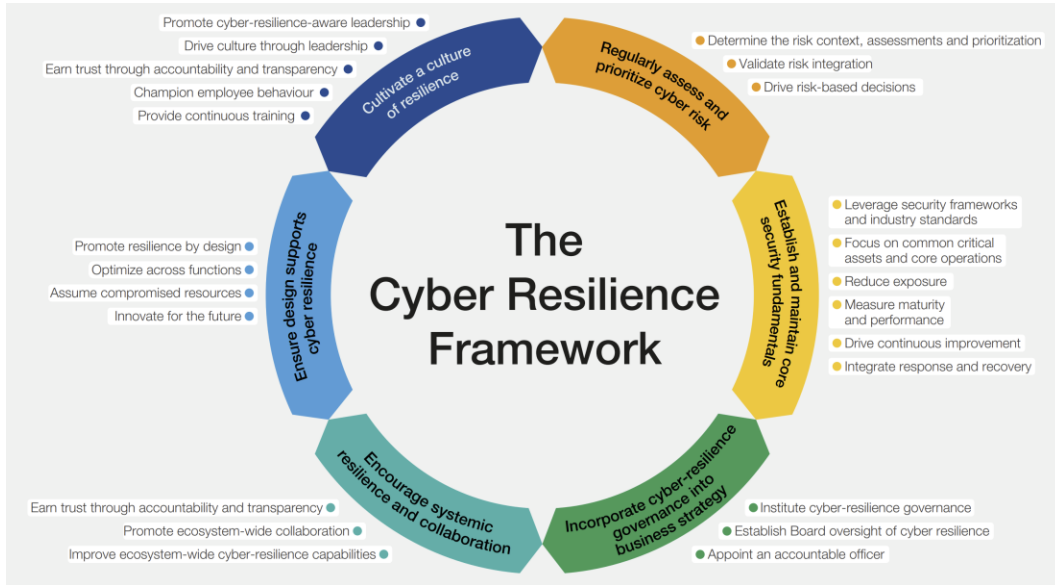
Source: [CREF Navigator \(mitre.org\)](https://mitre.org)

The CREF Navigator is a web-based relational tool developed by MITRE. It distills complex concepts and relationships from NIST SP 800-160 Volume 2 (Rev 1) into useful cyber resiliency terms, tables, and relationship visualizations. This tool enables architectural and engineering analysis for improving cyber resiliency. The principles of the CREF framework follow four guiding pillars:

- **Anticipate:** Maintain a state of informed preparedness to forestall compromises of mission/business functions from adversary attacks.
- **Withstand:** Continue essential mission/business functions despite successful execution of an attack by an adversary.
- **Recover:** Restore mission/business functions to the maximum extent possible after successful execution of an attack by an adversary.
- **Adapt:** Change mission/business functions and/or supporting cyber capabilities to minimize adverse impacts from actual or predicted adversary attacks.

Cyber Resilience Framework (World Economic Forum & Accenture)

Each of the CRF principles is accompanied by a set of practices and sub-practices to further enable cyber leaders to develop and assess their cyber resilience (JobAids – filename “WEF_Cyber_Resilience_Index_2022.pdf”):



Source: World Economic Forum and Accenture

In that document you will find all the metrics aligned and explained in a broader scope with fully expanded Cyber Resilience Framework’s key principles, associated practices and sub-practices in greater detail, Mapping of the Cyber Resilience Framework against other international frameworks, and the taxonomy of the Cyber Resilience Index.

Visibility Tuning

After an incident and its investigation, security staff will make changes to the alerting system, called visibility tuning. This important step helps reduce false positives and low-quality alerts within the SOC. During a security incident, an analyst may find ways to improve incident detection and visibility through centralized log monitoring. As a result, the analyst will fine-tune the tuning process to enhance visibility for future incidents. The tuning process is based on metrics gathered from SOC systems and involves removing alerts that are old or ineffective. The tuning process will determine:

- Who or what causes visibility insertion or triggered the event to show up in the SIEM
- Limits for alert causes, put a threshold limit if frequency is getting high

After a breach case is closed, a review process for current alerts is advised that security staff check alerts every three months, with a monthly check of alert metrics.

Content Engineering

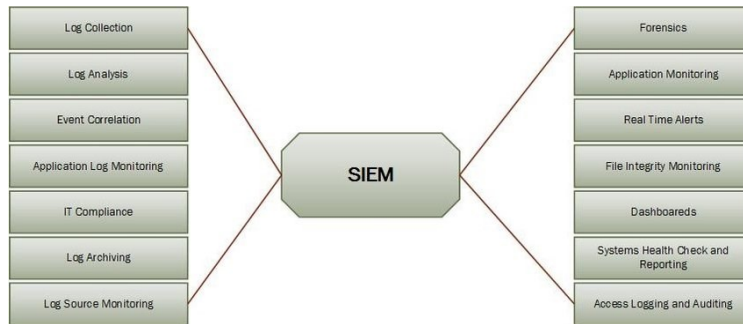
To find new triggers for analysts to review, a content engineer will check the available tools, infrastructure capabilities and current alerts. A content engineer needs to know the visibility required for incident response, but they should not be part of the incident response team to avoid bias in the review. There should also be a standard rollout process for every alert created. The interface agreement between SecOps and the content engineering team should specify how often updates are made, how alerts are vetted and how feedback is given. It should also show how staff members can ask for new or changed alerts. Alerts that are set up properly help to rank events by severity.

How a SOC is Typically Operated

A Security Operations Center (SOC) is a centralized function or team responsible for improving an organization's cybersecurity posture and preventing, detecting, and responding to threats. Here's how a SOC is typically operated:

1. **Asset and Tool Inventory:** The SOC needs visibility into the assets that it protects and insight into the tools it uses to defend the organization. This means accounting for all the databases, cloud services, identities, applications, and endpoints across on-premises and multiple clouds. Consistent protection across the network, cloud and endpoints.
2. **Reducing the Attack Surface:** A key responsibility of the SOC is reducing the organization's attack surface. The SOC does this by maintaining an inventory of all workloads and assets, applying security patches to software and firewalls, identifying misconfigurations, and adding new assets as they come online. ML-curated alerts to identify attackers in minutes, this is a must have. Correlation of low-confidence alerts to produce high-confidence alerting.
3. **Continuous Monitoring:** Using security analytics solutions like a security information enterprise management (SIEM) solution, a security orchestration, automation, and response (SOAR) solution, or an extended detection and response (XDR) solution, SOC teams monitor the entire environment—on-premises, clouds, applications, networks, and devices—all day, every day, to uncover abnormalities or suspicious behavior. Automated threat prevention for updates to security controls in minutes.

4. **Threat Intelligence:** The SOC also uses data analytics, external feeds, and product threat reports to gain insight into attacker behavior, infrastructure, and motives. This intelligence provides a big picture view of what's happening across the internet and helps teams understand how groups operate. Documented roles and responsibilities to clearly define who owns each element of security operations. Processes designed to ease the adoption of automation while accommodating manual response activities.



Source: [Typical Log Sources in Enterprise Networks | Download Scientific Diagram \(researchgate.net\)](#)

Security Operations Mindmap



Source: [SoC Mind Map \(cm-alliance.com\)](#)

Please understand that the above picture is for your reference only, this is not an exhaustive list, and certainly is not an operational overview, only a high level summary, and not nearly complete.

SOC Workstation Security Requirements

Workstation security requirements are the specifications and guidelines that ensure the security and integrity of the workstations used by the SOC staff. Some of the common requirements are:

- Reminder – Zero Trust Applies to All! (ZT applies to what the business can and will support. If it isn't economically feasible for the business to adopt they will downgrade ZT to their own version of ZT)
- Hardened operating systems.
- Use of strong passwords and multifactor authentication, organization must provide the mobile phones that's configured to receive SMS/text or an RSA key generation. These phones and the workstations must not go out of the SOC premises.
- Encryption of hard drives.
- Must not have any remote apps installed.
- Removable media must not be enabled, all USB ports must be disabled.
- Limit software usage, git usage, tools usage and must be pre-approved and pre-installed. New tools installations requirements must also be approved and protected by app-locking utilities.
- Installation of antivirus, firewall, and other security monitoring software that hardened the operating systems. Firewall must be properly configured in a way to severely minimized to withstand attacks, and itself cannot be made a bot.
- Regular patching and updating of operating systems and applications from a central repository, not from the OEM's.
- Restriction of access to sensitive data and systems.
- Logging and monitoring of workstation activities.
- Compliance with enterprise policies and standards enforced.

These requirements may vary depending on the size, nature, and maturity of the enterprise and the CSOC. Some enterprises may choose to outsource their CSOC functions to a managed security service provider (MSSP), while others may prefer to have an in-house CSOC. In either case, the CSOC workstation security requirements should be clearly defined, documented, and enforced to protect the enterprise from cyberattacks.



CHAPTER 7


SOC Organogram

RED MUST KNOW HOW BLUE IS DETECTING RED'S EVASIVE TECHNIQUES, AND BLUE MUST KNOW HOW RED IS USING WHICH TECHNIQUE TO ATTACK! AND BLUE SHOULD HAVE ADEQUATE VISIBILITIES OVER NETWORKED DEVICES. AND THE PURPLE WILL SEE TO IT THAT EACH TEAM IS WELL EQUIPPED AND UNDERSTANDS EACH OTHER'S GOALS TO MINIMIZE RISKS OF THE ORGANIZATION, QUIT PLAYING, TIME TO BE SERIOUS.

The primary diagram describes the team's hierarchy. You can play with it as you see fit for your organizational requirements allows you. As you can see, in the organogram, the Purple, Blue and the Red team is under the SOC manager. In your case you could have the SOC manager as the purple team and let him function as a Purple team player.

But the SOC manager has his own duties as reflected in this study, or where you are forming your JD shown in the NICCS pathway tool. This will create some levels of



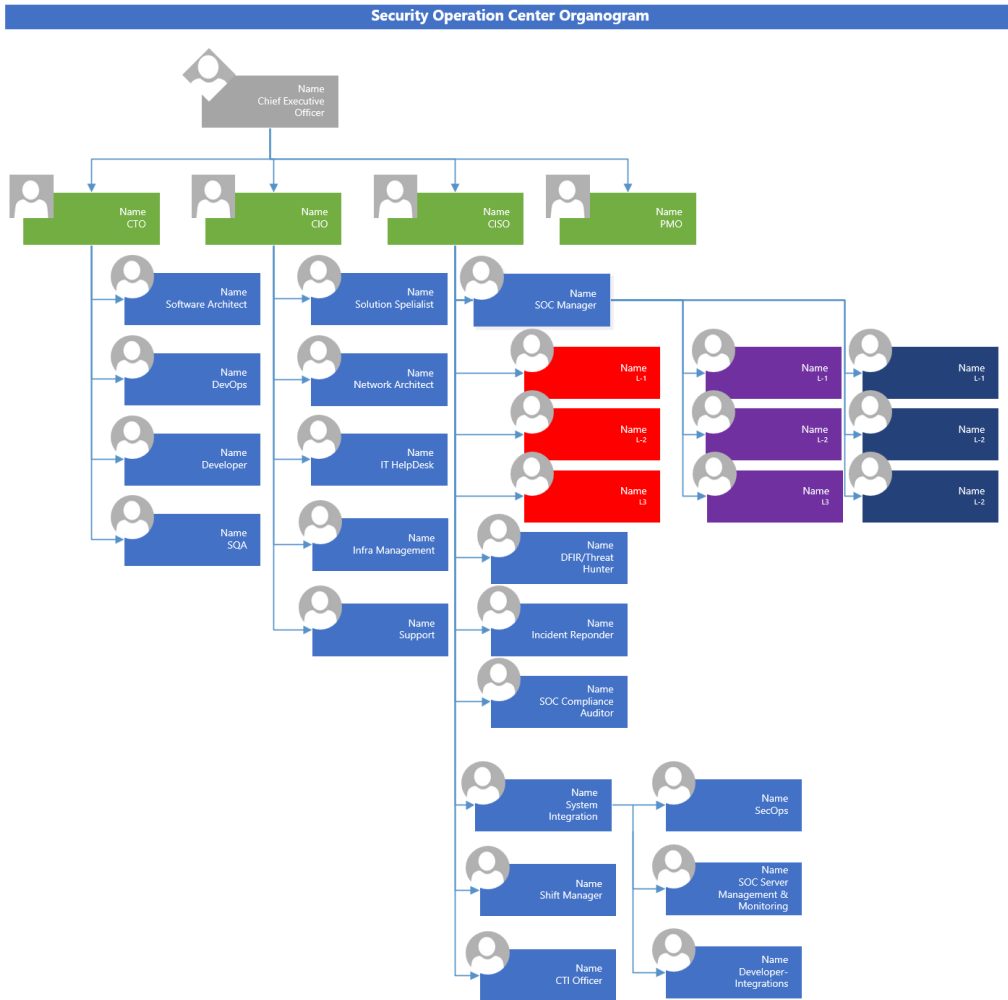


ambiguity as layers of skills and activities will overlap. But sooner or later you will need to make the hiring manager understand the requirements and job roles are unique to their skills.

It is imperative that the infrastructure administrators of the CIO team must not manage the SOC servers, and similarly, the developers of the CTO's team members should not deploy any applications, this must be done by either the DevOps from the CISO's team or from the developers who are in the CISO's team. For a large operational model of SOC, you will need developers in your SOC team to properly operate, integrate, and develop better dashboards to independently operate. But the CTO and CIO's team members can help and will help, and their collaboration is also required for the SOC to perform their duties properly. Since the endpoints are managed by the CIO's team, network infrastructure is managed by CIO's team, maybe the physical and the VM's are also managed by the CIO's team, CTO is managing the ERP or its components, and CTO's team is developing your platform service requirements etc. and the PMO will always play a vital role reporting all the requirements, completion of integrations, and make the CxO's happy!



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Source: the Visio file is provided in the job aids folder named "SOC Organogram"

I have not provided proper focus on the organogram on the CIO, CTO's part, just the parts that's required and has overlapping activities. This is just for your understanding of the roles and responsibilities, as you can see that the DFIR is placed in conjunction with threat hunting, you can separate them if you want them to. The SOC Director also plays a vital role in SOC's operational activities, which is also not mentioned in the organogram.

Cybersecurity Teams: Red, Blue & Purple

Red, blue, and purple teams are cybersecurity teams that have different roles and responsibilities in an organization's cybersecurity strategy. Here is a brief overview of each team:

- **Red team:** The red team is responsible for **discovering** security vulnerabilities through vulnerability assessment & penetration testing. They simulate cyberattacks against an organization's network or systems to identify weaknesses and vulnerabilities. Once they discover these vulnerabilities, they may even try to attack them to test the reaction of the organization's security controls. They'll launch realistic attacks by mimicking the techniques, tactics, and tools real threat actors use. When the red team completes their testing, they'll generate a report detailing the methods they used to discover vulnerabilities and how those vulnerabilities can be exploited by threat actors.

Pro-Tip

• Never test your infrastructure devices in real-time unless absolutely necessary, but do run assessment tests on all networked devices and application, but where applicable or scope is there, do run all tests in VM's or replicated (P2V- physical to virtual) VM, and run all tests in it.

It's very important to understand that Red team member's mindset needs to be like a hacker, assessing 360°degrees of the threat findings on all networked services, and predominantly, they think like threat actors (ethical) and simulate cyberattacks against an organization's network or systems. Their goal is to find vulnerabilities in the organization's defenses that could be exploited by real-world attackers. Skill sets for red teams include:

- Penetration testing
- White, black, and gray box testing
- Ethical hacking

Red Team Exercises are Typically Conducted in Three Phases

- **Planning Phase** – In this phase, the Red Team develops a plan of attack and determines how they will attempt to identify or exploit the organization's vulnerabilities.
- **Execution Phase** – In this phase, the Red Team executes the plan and attempts to exploit the organization's vulnerabilities.
- **Evaluation Phase** – In this phase, the Red Team evaluates their success and provides documented evidence as feedback to the organization, where the blue

team can take measures to remedy each of the vulnerabilities found from the assessment.

Benefits of Red Teaming

Now that we understand how Red Team Exercises help CISOs validate the security controls effectively, let's look at the benefits of Red Teaming:



Source: [How do Red Team Exercises help CISO to Validate the Security Controls Effectively? - Security Boulevard](#)

Top Red Team Frameworks: TIBER, AASE & CBEST

Just like any other cybersecurity framework, red teaming frameworks prescribe a set of tried and tested standard processes and procedures that should be followed by organizations. A red teaming framework has the following components:

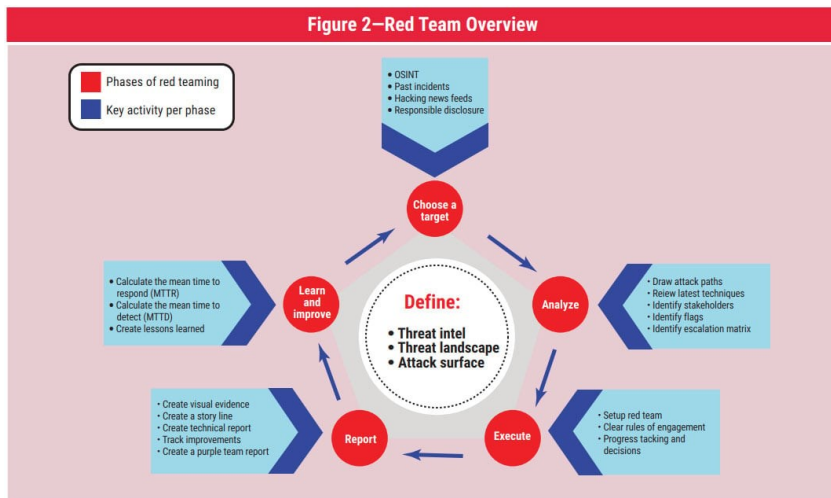
- Defining the scope of a red teaming exercise and risk tolerance level of the organization
- Gathering threat intelligence data
- Conducting red team exercises
- Analyzing results and preparing a remediation plan
- Presentation before the senior management/board

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Whether following a particular red teaming framework is mandatory depends on the industry an organization is working in and the authority that has prescribed the framework. Some of the well-known red teaming frameworks include:

- [TIBER-EU](#) (Threat Intelligence-Based Ethical Red Teaming Framework – European Union)
- [UK's CBEST](#)
- [Hongkong's iCAST](#) (Intelligence-led Cyber Attack Simulation Testing)
- [Saudi Arabia's FEER](#) (Financial Entities Ethical Red Teaming)
- [Singapore's AASE](#) (Adversarial Attack Simulation Exercises)
- [Mitre's ATT&CK](#) framework

Another framework for red team from ISACA



Source: [Red Teaming for Cybersecurity \(isaca.org\)](https://www.isaca.org/cybersecurity/red-teaming-for-cybersecurity)

A few challenges common in security teams include:

- Keeping analysts challenged and satisfied with their position.
- Finding the right talent to fill security roles.
- Continuously monitoring and adjusting analyst staffing to align with the SOC's.
- Business objectives and operational efficiency.
- Enabling analysts to engage in self-development and growth activities, including.
- Dedicated time for threat hunting and intelligence research.
- Chasing false positives.

Differences Between Red Teaming and Penetration Testing

Penetration Testing is a process aimed at discovering potential weaknesses in an information system that could be manipulated by unauthorized individuals. It mimics the behavior of a harmful intruder attempting to access the system's resources.

Conversely, Red Teaming is a strategy employed by organizations to uncover their own vulnerabilities and assess the effectiveness of their security measures against potential threats. Red Teams typically consist of seasoned professionals with extensive knowledge of exploiting weaknesses and circumventing security measures.

In essence, while Red Teaming concentrates on uncovering an organization's vulnerabilities, Penetration Testing is primarily concerned with discovering vulnerabilities that could be leveraged by an unauthorized individual.

A Better Choice Between the In-house Red Team and Outsourced Red Team

- There are several factors to consider when making the decision between in-house and outsourced Red Team.



Source: [How do Red Team Exercises help CISO to Validate the Security Controls Effectively? - Security Boulevard](#)

- **Cost** – The first factor is cost. In-house Red Teams are typically more expensive than outsourced Red Teams because they require dedicated resources (e.g. employees, tools, etc.). Whereas, outsourced Red Teams are typically less expensive because they leverage the resources of the service provider. The difference in quality for in house, versus external will always be there as the internal team would have much extended visibility on the infrastructure.
- **Time** – The second factor is time. In-house Red Teams require more time to set up and manage than outsourced Red Teams. Outsourced Red Teams are ready to go right away and do not require any additional setup time.
- **Skills** – The third factor is skills. In-house Red Teams require employees who have the necessary skills to carry out a Red Team exercise. Outsourced Red

Teams typically have employees who are skilled in penetration testing and red teaming.

- **Experience** – The fourth factor is experience. In-house Red Teams typically have more experience than outsourced Red Teams. This is because outsourced Red Teams are typically composed of employees from multiple organizations, where they don't insights of the internal network and its architectures.
- **Organizational Requirements** – The fifth factor is organizational requirements. In-house Red Teams are typically better suited for organizations that have the necessary resources (e.g. employees, tools, etc.). Outsourced Red Teams are typically better suited for organizations that do not have the necessary resources.
- **Organizational Risk Appetite**– The In-house Red Teams are better suited for organizations that are willing to take on more risk. Whereas the outsource Red Teams are better suited for organizations that want to mitigate their risk.

Therefore, the right choice is to outsource Red Team if the company has a lack of resources and wants to mitigate its risk. However, if the company is willing to take on more risk, then the right choice is to develop the in-house Red Team, since every patch update requires re-testing and this is proven to be very expensive in the long run.

- **Blue team:** The blue team is responsible for **defending** against real threat actors, as well as members of the red team. They monitor for suspicious activity and implement security controls, reduces attack surface areas that are pointed out by the Red teamers which effectively prevents security incidents. Blue teams take a proactive approach to cybersecurity and leverage Security Information and Event Management (SIEM) platforms to monitor network traffic and investigate security events. They have their own tools to identify threats and notify proper authority to remedy the problems.

Pro-Tip

• Red and Blue team must work together, and in terms, they must be the best friends as they are the 2 sides of a single coin. Before a device is put into production (while all patches and firmware is updated), it must be tested for vulnerabilities, and after only satisfactory results generated, this can be put into production, as these live devices cannot be tested for penetration during live operations, unless you have plenty of routes or redundancy available

Blue team drills are structured to evaluate an organization's proficiency in identifying, averting, and reacting to cyberattacks. As the defensive faction, Blue teams are

responsible for network surveillance, detection of Red team operations, and response to the emulated assault. The skillsets of a Blue team encompass:

- Security Operations Center (SOC)
- Incident management
- Security of operations
- Threat pursuit
- Digital investigation

Additionally, Blue teams formulate new detection protocols for their security apparatus in response to threats identified by the Red team. This could encompass new identifiers for intrusion detection systems or bespoke queries for log analysis tools.

The blue team will detect and neutralize the more sophisticated attacks and closely monitor current and emerging threats to preemptively defend the organization.

The Blue team's Objectives and Duties


- Understanding every phase of an incident and responding appropriately.
- Noticing suspicious traffic patterns and identifying indicators of compromise.
- Rapidly shutting down any form of compromise.
- Identifying the red team/threat actors' command and control (C&C or C2) servers and blocking their connectivity to the target.
- Undertaking analysis and forensic testing on the different operating systems their organization runs, including use of third-party systems.

The Blue Team's Methods

- Reviewing and analyzing log data.
- Utilizing a security information and event management (SIEM) platform for visibility and detection of live intrusions and to triage alarms in real-time.
- Gathering new threat intelligence information and prioritizing appropriate actions in context with the risks.
- Performing traffic and data flow analysis.

Content+Cloud operates a cutting-edge Security Operations Centre and can act as your blue team.

- **Purple team:** The purple team is a collaborative effort, bringing members of the red and blue teams together. The purple team focuses on collaboration between the red and blue teams to strengthen an organization's overall security. The red



team members help the team in understanding the threat actor's tactics, techniques and procedures, and blue team members on the basis of the information given by red team configures and improve its detection and response capabilities. Purple teams rely on collaboration between the red and blue teams, which makes communication essential to success. With the traditional two-team methodology, the red team only alerts the blue team after completing their testing. This leaves the blue team in a reactionary state with a long list of cybersecurity findings to address. With a purple team, however, the blue team is notified when the red team begins testing and simulating real-world tactics used by Advanced Persistent Threat (APT) groups.

The Purple Team's Maturity Model is a framework that encourages the creation of a permanent team with shared goals and objectives. The model measures the team's maturity through threat understanding and detection understanding. The framework helps in understanding deployment, integration, and creation.

The Purple Team Model Has Three Levels of Maturity

1. **L1-Deployment:** In this level, teams deploy tools developed by someone else, such as vendor platforms or open-source projects.
2. **L-2-Integration:** In this level, teams pair the tools and resources together to achieve better results.
3. **L-3-Creation:** In this final level, teams add tools to the capabilities developed in previous levels.

The Purple Team's Objectives and Duties Include

- Working alongside the red and blue teams, analyzing how they work together and recommending any necessary adjustments to the current exercise, or noting them for future.
- Seeing the big picture and assuming the mindset and responsibilities of both teams. For example, a purple team member will work with the blue team to review how events are being detected. The team member will then shift to the red team to address how the blue team's detection capabilities can be subverted.
- Analyzing the results and overseeing necessary remedial actions, e.g. patching vulnerabilities, implementing employee awareness training.
- Ultimately deriving maximum value from the exercise by applying learning and ensuring stronger defenses.

Purple Team Exercises Usually Follow Four Steps

1. **Planning:** First, the red and blue teams collaborate to plan the exercise, which includes defining the scope of the exercise, identifying the business critical systems within the infrastructure & the data to be tested, and determining the types of attacks to be simulated.
2. **Simulation:** Second, the red team conducts simulated attacks on the organization's systems and infrastructure, using tactics and techniques like those used by real-world attackers. The blue team monitors and defends against these attacks, using their knowledge of the organization's security defenses and incident response procedures.
3. **Debrief:** Third, after the simulation, the red and blue teams meet to discuss the exercise results. They review the effectiveness of the organization's security defenses, identify areas of weakness, and develop strategies for improving the organization's overall security posture.
4. **Implementation:** Lastly, based on the exercise results, the purple team develops and implements strategies to address the weaknesses and vulnerabilities identified during the simulation. This may involve improving security policies and procedures, upgrading security technologies, or providing additional employee training.

In a purple team exercise, various tools and techniques are used to simulate attacks and test an organization's security defenses. Some of the critical tools and techniques used in purple team exercises include:

- **Threat emulation software:** This type of software is designed to simulate real-world threats and attacks, allowing organizations to test their security defenses in a controlled environment. Threat emulation software may include tools for penetration testing, vulnerability scanning, and other security testing activities.
- **Collaboration platforms:** Purple team exercises rely heavily on collaboration between the red and blue teams, and collaboration platforms can be used to facilitate communication and information sharing between the teams. Platforms like Slack, Microsoft Teams, or Jira can be used to coordinate tasks, share information, and discuss findings.
- **Incident response platforms:** These platforms are used to manage and coordinate an organization's response to a simulated attack. These platforms help the purple team to develop and test incident response procedures, as well as to track and manage the progress of the response.
- **SIEM:** The purple team uses the SIEM to monitor and analyze the effectiveness of an organization's security defenses during a simulated attack.

- **EDR:** Purple teams use EDR tools to identify and respond to potential threats and attacks in real time.
- **Threat intelligence platforms:** Threat intelligence platforms are used to gather and analyze information about potential threats and attacks. The purple team can use this information to better understand the TTPs used by real-world attackers and to develop more effective security strategies.

Security analysts can act quickly and without extra approvals when they follow the parameters and guidelines of a pre-approved mitigation scenario. This method balances the need for fast and flexible responses to security incidents with the potential effects on the organization's risk level. By giving analysts the authority to make decisions within set boundaries, pre-approved mitigation improves the organization's capacity to stop and resolve cyberthreats. The incident response team should have a written list of pre-approved scenarios that the analysts can apply to mitigate incidents. Some examples of pre-approved mitigation scenarios are stopping a process, locking a system or isolating a device. Another example is to set up a dynamic process to block a specific Indicator of Compromise (IoC), such as known malicious URLs, domains or IP addresses, without needing a security commit to initiate a change request.

Purple Team Exercise Tools

The below list is a compilation of purple team tools that are most widely used in purple teaming exercises.

- [APTSimulator](#)
- [Atomic Red Team](#)
- [AutoTTP](#)
- [Blue Team Training Toolkit](#)
- [CALDERA](#)
- [InfectionMonkey](#)
- [DumpsterFire](#)
- [Invoke-Adversary](#)
- [NSA Unfetter](#)
- [Office 365 Attack Simulator](#)
- [Purple Team Automation](#)
- [Red Team Automation \(RTA\)](#)
- [Uber Metta](#)

Some other commercial tools are:

- [AttackIQ](#)
- [Cymulate](#)
- [ReliaQuest](#)
- [SafeBreach](#)
- [SCYTHE](#)
- [Verodin](#)
- [XM-Cyber](#)

Purple Team Tactics

To improve the security of your organization's infrastructure, you need to implement some purple teaming strategies, some of the important ones that you need to keep in your mind are following:

1. Understand organizations culture.
2. Operationalize the MITRE framework.
3. Understand your team's strengths and weakness.
4. Create a good and healthy environment for communication.
5. Have a strategy implementation for 24/7 testing.

Steps for Building a Successful Purple Team

Building a successful purple team that boosts your organization's security requires following a good plan that are explained in following steps:

1. **Develop a Plan:** Using MITRE ATTACK framework, create a comprehensive purple team plan. Developing a plan helps you set up your organization for success.
2. **Leverage Automation:** Automation tools have become an integral part of the purple teaming methodology. Automation provides continuous testing and evaluation and ensure no security gaps left behind. Automation also provides your security team with real time data tracking.
3. **Set Goals:** Without setting your goals, it's difficult for a team to complete their mission. Give the team details of the objectives to help them find the problem and develop solutions.
4. **Execute your Plan:** Following a structured plan helps teams manage all security incidents effectively and ensures that they are on the right track to achieving their goals and objectives.
5. **Measure Exercise Results:** On completion of the purple team exercise, document all the results so that it helps your team identify what the organization needs now and in the future.

It is essential to understand that the more devices, applications or networked devices you have, the attack surface area increases exponentially, and depending on the size, geo locations, volumes of network transmission really make the transmission in a nightmare situation, and there is no 1-click solution to such problems, and remediations on all domains of the cybersecurity monitoring makes it absolutely impossible.



Pro-Tip

• An approach to layered security is still the best practice. You can have a look at the basic design at the end of this document that, zones were designed in a way where ACL's were put in for transmission, is only allowed to communicate to the recipients and no other. Also, internet facing web server should be frontended with a CASB provider, and on the backend, your device should only communicates to the CASB, and your web server must have WAF in front of them. Where possible, cloud services should be avoided, they are still not matured enough.





CHAPTER

8

Setting up a SOC

SO HOW DO YOU FIT INTO ANY OF THE SOC ROLES? HOW BEST TO OUTLINE YOUR JD/SKILLS/ACTIVITIES WHICH CAN BE MAPPED TO SOC MATRIX? SOC OPERATION RELIES ON THE EFFECTIVENESS OF YOUR ROLES AND RESPONSIBILITIES. ARCHITECTING, INTEGRATION IS NOT THE WHOLE STORY, OPERATIONALIZE THE SOC WITH YOUR SKILLS, NOT WEAPONIZING IT.

Since we have discussed the requirements of developing a SOC including the standards, frameworks, enterprise architecture, attack surface management, models, processes, organogram and those were in context as required to understand the pre-requisites for developing a SOC. This is not the end of the discussion and as we progress and deep dive into the abyss, I will guide you with the right context every time its required from a different perspective.

This calls for a stakeholder engagement for you which involves several steps:

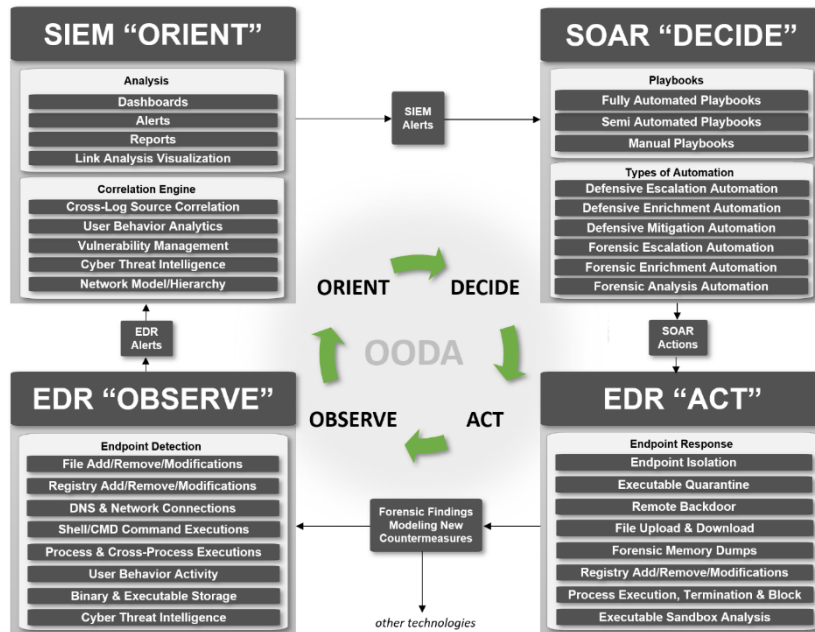
1. **Identify Your Objectives and Capabilities:** Understand your business objectives and the capabilities of your organization. This will help you focus your SOC project and control costs.



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



2. **Develop Your SOC Strategy:** Define the scope of your SOC, including the types of threats you need to protect against and the assets you need to protect.
3. **Design Your SOC Solution:** This includes deciding whether to have an in-house SOC, outsource it, or use a hybrid model. You also need to decide on the size of your team and the skills they need.
4. **Create Processes, Procedures, and Training:** Develop standard operating procedures for your SOC team. This includes processes for incident response, threat hunting, and reporting.
5. **Prepare Your Environment:** This involves setting up the physical or virtual space for your SOC. You also need to ensure you have the necessary hardware and software.
6. **Implement Your Solution:** Deploy the technologies you've chosen for your SOC. This includes security information and event management (SIEM) systems, intrusion detection systems (IDS), and other security tools.
7. **Deploy End-to-End Use Cases:** Start deploying a few use cases that focus on end-to-end threat detection and response.
8. **Maintain and Evolve Your Solution:** Cyber threats are constantly evolving, so your SOC needs to evolve too. Regularly review and update your processes, train your team on new threats, and update your tools.



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Source: [An OODA-driven SOC Strategy using: SIEM, SOAR and EDR \(correlatedsecurity.com\)](https://www.correlatedsecurity.com)

Remember, building a SOC is a major undertaking that requires careful planning and coordination of people, processes, and technologies (PPT, always comes down to PPT). It's well worth it when configured properly to provide adequate security for your enterprise.

Pro-Tip

• You should develop a SOC strategy document that must be mapped to the business requirements of the organization that must include if its feasible to develop one with in-house resources or to outsource as a virtual SOC. Develop actionable steps to setup your strongest protection against cybercrime.

How a Security Operations Center (SOC) Works in Practice



Source: [What is a Security Operations Center \(SOC\)? \(Ultimate Guide\) - SOCRadar® Cyber Intelligence Inc.](#)

1. **Proactive Monitoring:** The SOC team gathers information from various resources, including threat intelligence feeds and log files from systems all around the enterprise. They carefully monitor the company's assets, from on-premises servers in data centers to cloud resources. Accurate monitoring is critical.
2. **Incident Response and Recovery:** When a potential threat is detected, the SOC coordinates the organization's ability to take the necessary steps to mitigate damage and communicate properly to keep the organization running after an incident. For example, recovery can include activities such as handling acute malware or ransomware incidents.
3. **Remediation Activities:** SOC team members provide data-driven analysis that helps an organization address vulnerability and adjust security monitoring and alerting tools. For example, using information obtained from log files and other sources, a SOC member can recommend a better network segmentation strategy or a better system patching regimen.
4. **Compliance:** The SOC helps ensure that the organization is compliant with important security standards and best practices. This includes conformity to a security policy, as well as external security standards, such as ISO 27001x, the NIST Cybersecurity Framework (CSF), and the General Data Protection Regulation (GDPR).
5. **Coordination and Context:** A SOC team member helps an organization coordinate disparate elements and services and provide visualized, useful information. Part of this coordination is the ability to provide a helpful, useful set of narratives for activities on the network.

In addition to the above-mentioned points, the SOC performs preventative maintenance such as applying software patches and upgrades, and continually updating firewalls, whitelists and blacklists, and security policies and procedures.

This is a broad example and the specific workings can and may vary based on the organization's needs and resource requirements.

Functions of the Sigma Rules in SOC

Sigma rules are textual signatures written in YAML (Yet Another Markup Language) that are used in Security Operation Centers (SOCs) to detect anomalies and identify suspicious activity in log events. Here are some of their key functions:

1. **Anomaly Detection:** Sigma rules monitor log events for signs of suspicious activity and cyber threats.
2. **Cross-Platform Compatibility:** Sigma rules are cross-platform and work across different Security Information and Event Management (SIEM) products. This allows defenders to share detection rules with each other, independent of their security arsenal.
3. **Conversion to SIEM-Specific Language:** Sigma rules can be converted by SIEM products into their distinct, SIEM-specific language, while retaining the logic conveyed by the Sigma rule.
4. **Incident Response:** Incident response professionals can use Sigma rules to specify detection criteria. Any log entries matching this rule will trigger an alarm.
5. **Advanced Monitoring:** Sigma rules allow for advanced monitoring of log events and entries.

Sigma rules standardize detection rule formats across all SIEM and log management platforms, enabling more effective collaboration among security analysts. They also provide flexibility, allowing companies to evolve their cybersecurity technology stack in a way that makes sense for them.

Released by Florian Roth in 2017, Sigma ([The Generic Signature Format for SIEM Systems](#)) has paved the way for platform-agnostic search. With Sigma, defenders can harness the community's power to react promptly to critical threats and new adversary tradecraft. You get a fixed-language specification for the generic rule format, a tool for converting Sigma rules into various query formats and a repository of over one thousand rules for several attack techniques.

Like YARA, or Snort Rules, Sigma is a tool for the open sharing and crowdsourcing of threat intelligence, it focuses on SIEM instead of files or network traffic. What Snort is to network traffic, and YARA is to files, Sigma is to logs.

Most attacks on IT systems and networks manifest themselves in event logs stored in the SIEM systems or other log storage and analysis solutions. This makes SIEM a crucial tool to detect and alert against intruders. SIEM detection rulesets existed in the vendor or platform-specific databases in the earlier days. The growing demand for up-to-date detections and analytics to be secure today requires sharing detection intelligence between different stakeholders and vendors. Sigma solves this challenge to make the queries and rulesets platform-agnostic.

Sigma Allows Defenders to Share Detections in a Common Language

Sigma satisfies various use cases:

- Sigma has become an agnostic way of sharing detections between Researchers and Intelligence who identify new adversary behaviors.
- Security teams can avoid vendor-lock-in, i.e. by defining rules in Sigma; we can more easily move between platforms.
- Sigma can be utilized to crowdsource detection methods and make them usable instantly for everyone.
- Using Sigma to share the signature with other threat intel communities.

Sigma rules can be converted into a search query specific to your SIEM solution and supports various solutions:

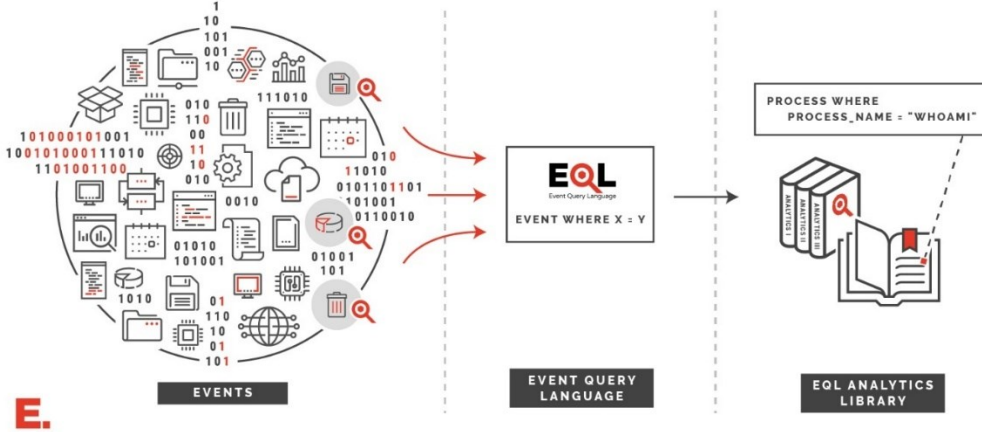
- Splunk
- ElasticSearch Query Strings and DSL
- Kibana
- Microsoft Defender Advanced Threat Protection (MDATP)
- Azure Sentinel
- IBM QRadar
- LogPoint
- Qualys
- RSA NetWitness
- LimaCharlie
- ArcSight
- PowerShell and Grep

Source: [A deep dive into Sigma rules and how to write your own threat detection rules - FourCore](#)

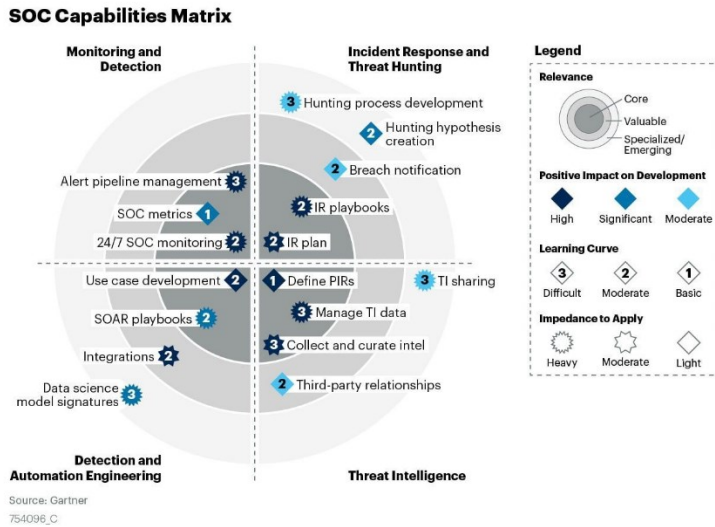
EQL Analytics Library

eqllib is a library of event based analytics, written in [EQL](#) (Event Query Language) to detect adversary behaviors identified in MITRE [ATT&CK®](#).

WHAT DOES THE EVENT QUERY LANGUAGE DO?



SOC Capabilities Matrix – Gartner



Gartner

May now you can see that the garner’s capability matrix is what we have addressed throughout the book. Interestingly, they have “Data Science Model” included, but not AI.

SOC Roles & Responsibilities



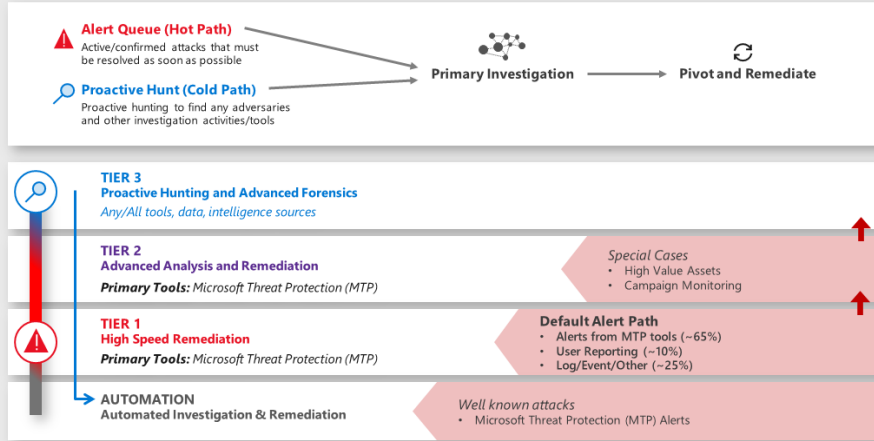
Source: [Next-Gen SOC - CyRadar](#)

SOC analysts are organized into four tiers. First, SIEM alerts flow to Tier 1 analysts who monitor, prioritize, and investigate them. Real threats are passed to a Tier 2 analyst with deeper security experience, who conducts further analysis and decides on a strategy for containment.

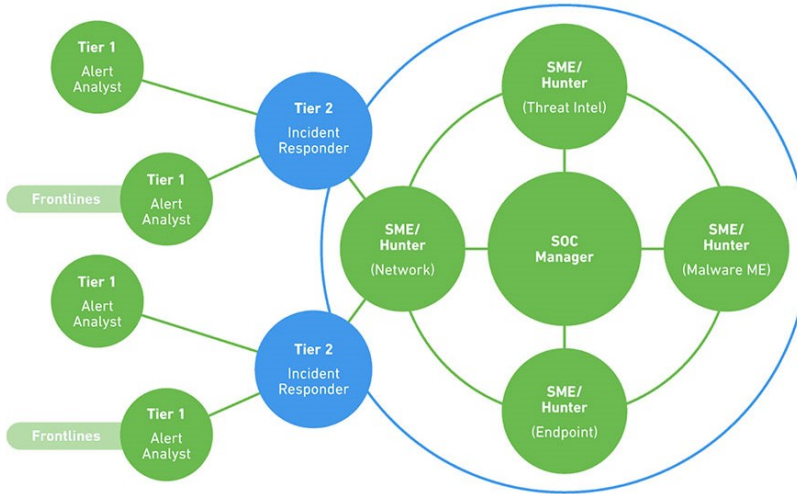
Critical breaches are moved up to a Tier 3 senior analyst, who manages the incident and is responsible for actively hunting for threats continuously. The Tier 4 analyst is the SOC manager, responsible for recruitment, strategy, priorities, and the direct management of SOC staff when major security incidents occur.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Microsoft's Corporate IT SOC – Tiers and Tools



Source: [CISO Series: Lessons learned from the Microsoft SOC—Part 2a: Organizing people](#)



The table below explains each SOC role in more detail.

Role	Qualifications	Duties
------	----------------	--------

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



<p>Tier 1 Analyst Alert Investigator</p>	<p>System administration skills; web programming languages, such as Python, Ruby, PHP; scripting languages; security certifications such as CISSP or SANS SEC401</p>	<p>Monitors SIEM alerts, manages and configures security monitoring tools. Prioritizes and triages alerts or issues to determine whether a real security incident is taking place.</p>
<p>Tier 2 Analyst Incident Responder</p>	<p>Similar to Tier 1 analyst, but with more experience including incident response. Advanced forensics, malware assessment, threat intelligence. Ethical hacker certification or training is a major advantage.</p>	<p>Receives incidents and performs deep analysis; correlates with threat intelligence to identify the threat actor, nature of the attack, and systems or data affected. Defines and executes on strategy for containment, remediation, and recovery.</p>
<p>Tier 3 Analyst Subject Matter Expert/Threat Hunter</p>	<p>Similar to Tier 2 analyst but with even more experience, including high-level incidents. Experience with penetration testing tools and cross-organization data visualization. Malware reverse engineering, experience identifying and developing responses to new threats and attack patterns.</p>	<p>Day-to-day, conducts vulnerability assessments and penetration tests, and reviews alerts, industry news, threat intelligence, and security data. Actively hunts for threats that have made their way into the network, as well as unknown vulnerabilities and security gaps. When a major incident occurs, teams with the Tier 2 Analyst in responding to and containing it.</p>
<p>Tier 4 SOC Manager Commander</p>	<p>Similar to Tier 3 analyst, including project management skills, incident response management training, and strong communication skills.</p>	<p>Like the commander of a military unit, responsible for hiring and training SOC staff, in charge of defensive and offensive strategy. Manages resources, priorities and projects, and manages the team directly when responding to business-critical security incidents. The organization's point of contact for security incidents, compliance, and other security-related issues.</p>
<p>Security Engineer Support and Infrastructure</p>	<p>Degree in computer science, computer engineering or information assurance, typically combined with certifications like CISSP.</p>	<p>A software or hardware specialist who focuses on security aspects in the design of information systems. Creates solutions and tools that help organizations deal robustly with</p>



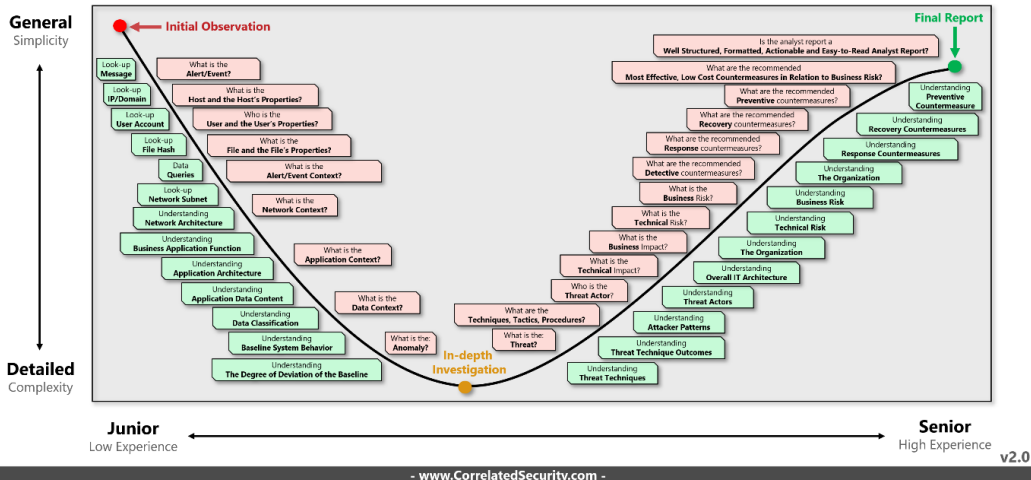
disruption of operations or malicious attacks. Sometimes employed within the SOC, and sometimes supports the SOC as part of development or operations teams.

Source: [What is Security Operations Center - SOC: Roles & Responsibilities - Exabeam](#)

A Cyber Security Analyst Maturity Curve

Cyber Security Analyst Maturity Curve

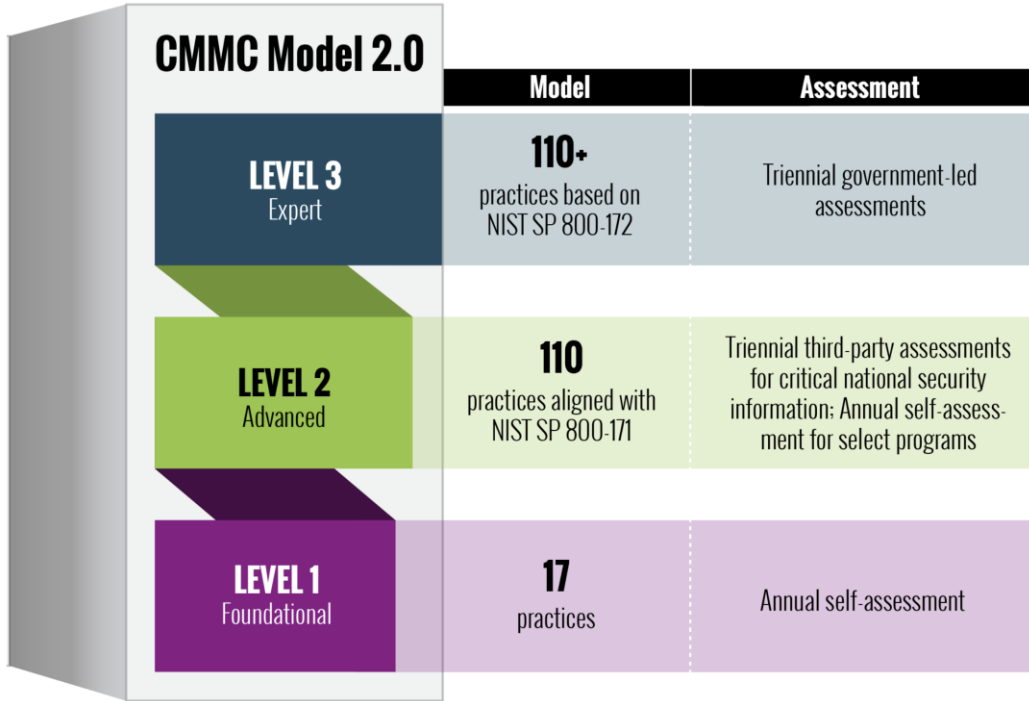
"A senior cyber security analyst should be able to reach the **simplicity at the far side of complexity** and to be able to communicate the cyber security risks, threats and related countermeasures **simply, effectively and actionable.**"



Source: [Cyber Security Analyst Maturity Curve \(correlatedsecurity.com\)](#)

CMMC Maturity Model 2.0

The CMMC levels and associated sets of practices across domains are cumulative. More specifically, for an organization to achieve a specific CMMC level, it must also demonstrate achievement of the preceding lower levels. For the case in which an organization does not meet its targeted level, it will be certified at the highest level for which it has achieved all applicable practices.



Full documentation can be downloaded from this link: [CMMC Documentation \(defense.gov\)](https://www.defense.gov/cmmc/)



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Deriving Your Job Description or Resume

NICCS®

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

Education & Training

Workforce Development

Cybersecurity & Career Resources

Workforce Development > Cyber Career Pathways Tool

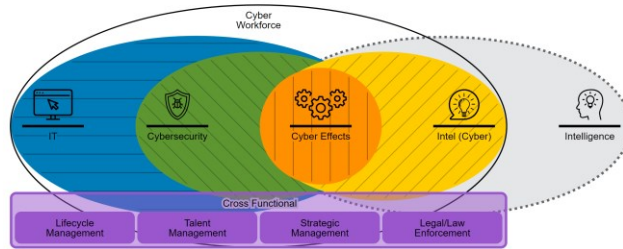
Cyber Career Pathways Tool

Open the User Guide

This tool presents a new and interactive way to explore work roles within the Workforce Framework for Cybersecurity (NICE Framework). It depicts the Cyber Workforce according to five distinct, yet complementary, skill communities. It also highlights core attributes among each of the 52 work roles and offers actionable insights for employers, professionals, and those considering a career in Cyber. To start, select a work role below, or enter keywords in the search bar.

As a new feature within Cyber Career Pathways Tool, the micro-challenges (TTCyber IT) consist of hands-on experiences that allow users to complete several core cybersecurity workforce tasks. The following cybersecurity workforce roles have available challenges: [Technical Support Specialist](#), [System Administrator](#), [Network Operations Specialist](#), [System Security Analyst](#), [Database Administrator](#), [Data Analyst](#), [Cyber Defense Analyst](#), [Cyber Defense Incident Responder](#), [Vulnerability Assessment Analyst](#), and [Law Enforcement/Counterintelligence Forensics Analyst](#).

Explore the micro-challenges using the Tool below!

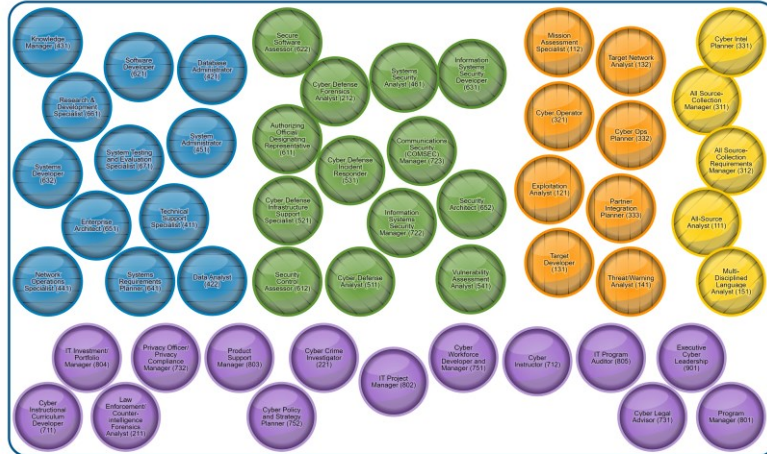


Select a Work Role

Go to the Career Pathway Roadmap page

Hide Diagram

Begin typing to search work role names. Or [search job titles](#).



Relationship filters:

Selected KSATs

Compared KSATs

All

Federal Core

All

Federal Core

KSATs

On Ramps


Off Ramps

Secondary Work Roles

Select a relationship filter button to change the relationships/roles shown in the galaxy. With a role selected, the galaxy will also change when you view that data in the info panel, unless you have locked the filter.

Source: [Cyber Career Pathways Tool | NICCS \(cisa.gov\)](#)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



NICCS[®]
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

Education & Training Workforce Development Cybersecurity & Career Resources

Workforce Development > Career Pathway Roadmap

Career Pathway Roadmap

Welcome to the Cyber Career Roadmap (Multi-Pathway Tool)!

This digital tool offers an interactive way for working professionals (cyber and non-cyber), employers, students, and recent grads to explore and build their own career roadmap across the 52 different NICE Framework work roles. The start of your next cyber journey is only a few clicks away.

Users can select up to five work roles to learn more about their shared skillsets, alignment to the Cyber Skill Communities, or related specialization and functions. The Cyber Career Roadmap highlights the mobility between these connection points to help you and others determine the next steps in your career progression and skillset development. The tool also offers recommended on/off-ramps (i.e. steppingstones) and secondary work roles to consider and pursue in your career roadmap.

No matter where you are in your cyber career, the Cyber Career Roadmap provides a starting point in career planning.

To get started, select from three to five work roles of interest, or use the search bar.

Select a Work Role

Begin typing to search work role names.

The Cyber Career Pathways Tool is developed and maintained in partnership with the [Federal Cyber Workforce Management and Coordination Working Group](#).

This tool is based on the NICE Cybersecurity Workforce Framework ([NIST Special Publication 800-181](#) ¹, August 2017) and revisions published in late 2020 renaming the framework as the Workforce Framework for Cybersecurity (NIST Special Publication 800-181 Rev. 1, November 2020). Please visit the [NICE Framework Resource Center](#) ² for more information, as well as the [latest updates](#) ³.

Other Useful Links

- [The Cyber Career Pathways Tool User Guide](#)
- [NICCS Education and Training Catalog](#)
- [Workforce Framework for Cybersecurity \(NICE Framework\)](#)
- [NICCS Cybersecurity Resources](#)


Last Published Date: January 6, 2022

[Return to top](#)


Sitemap NICCS Policy Plain Writing ¹ About NICCS

NICCS[®]
NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES

Contact NICCS
NICCS@hq.dhs.gov



CISA.gov
An official website of the Cybersecurity and Infrastructure Security Agency ¹



National Terrorism Advisory System
NTAS
NATIONAL TERRORISM ADVISORY SYSTEM OF DHS
NO CURRENT ADVISORIES
[Put this widget on your web page](#)

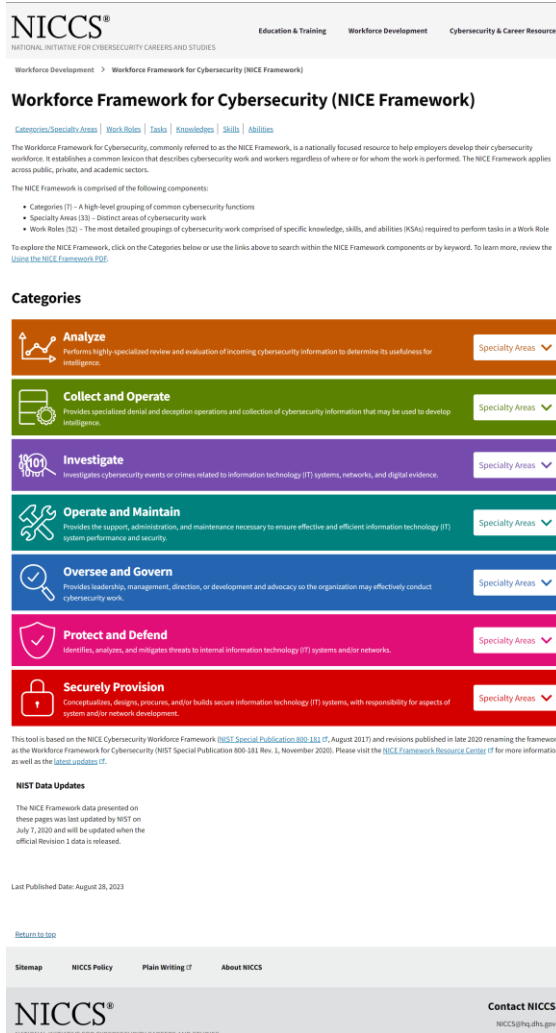
[About CISA](#) ¹ [Accessibility](#) ¹ [Budget and Performance](#) ¹ [FOIA Requests](#) ¹
[No FEAR Act](#) ¹ [Office of Inspector General](#) ¹ [Privacy Policy](#) ¹

Looking for U.S. government information and services? [Visit USA.gov](#) ¹

Source: [Career Pathway Roadmap | NICCS \(cisa.gov\)](#)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Here is a git repo for you to find out how the cybersecurity JD's are formulated: [GitHub - rezaduty/cybersecurity-career-path: Cybersecurity Career Path](#)



The screenshot shows the NICCS (National Initiative for Cybersecurity Careers and Studies) website page for the Workforce Framework for Cybersecurity (NICE Framework). The page is titled "Workforce Framework for Cybersecurity (NICE Framework)" and includes navigation links for "Categories", "Specialty Areas", "Work Roles", "Tasks", "Knowledge", "Skills", and "Abilities".

The page describes the NICE Framework as a nationally focused resource to help employers develop their cybersecurity workforce. It is composed of the following components:

- Categories (7) – A high-level grouping of common cybersecurity functions
- Specialty Areas (33) – Distinct areas of cybersecurity work
- Work Roles (52) – The most detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities (KSAs) required to perform tasks in a Work Role

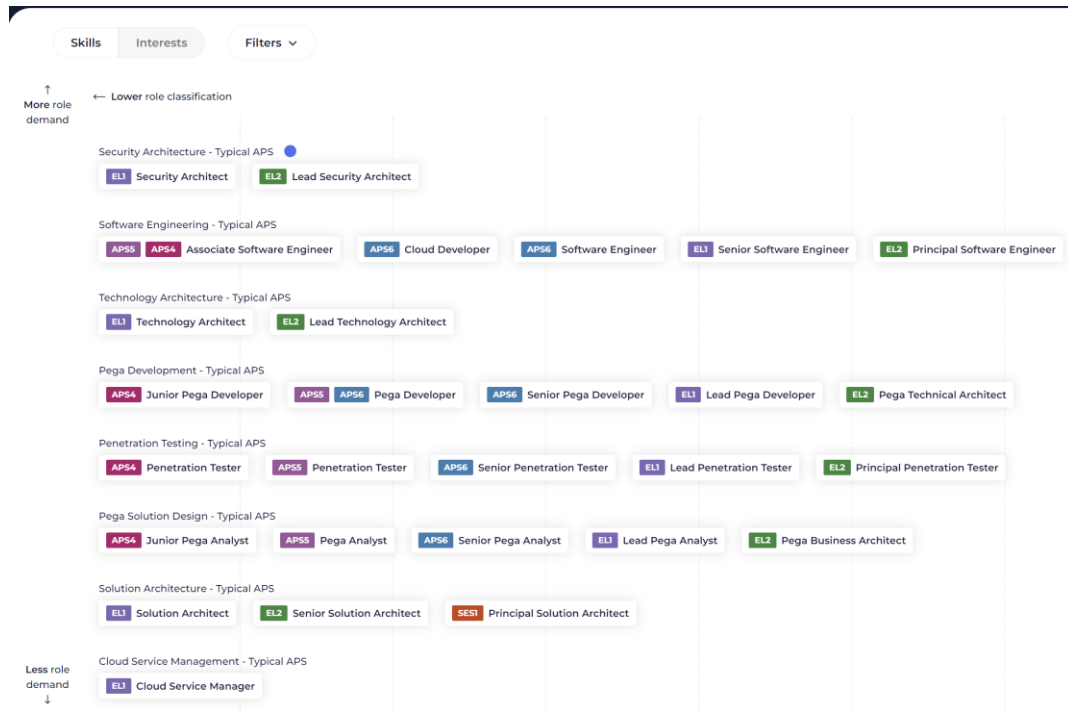
The page lists seven categories, each with a description and a "Specialty Areas" dropdown menu:

- Analyze**: Performs highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.
- Collect and Operate**: Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
- Investigate**: Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.
- Operate and Maintain**: Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
- Oversee and Govern**: Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
- Protect and Defend**: Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
- Securely Provision**: Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development.

At the bottom of the page, there is a "NIST Data Updates" section and a "Return to top" link. The footer includes a "Site map" with links to "NICCS Policy", "Plain Writing 17", and "About NICCS", along with the "Contact NICCS" information: NICCS@hq.dhs.gov.

Source: [Workforce Framework for Cybersecurity \(NICE Framework\) | NICCS \(cisa.gov\)](#)

And here is another one to map your career which is supported and designed by SFIA v8.0 which is mapped to their KB requirements (this is particularly developed for Australian technology people):



Source: [Career Pathfinder \(digitalprofession.gov.au\)](https://digitalprofession.gov.au)

Security Triage in Cybersecurity

Triage is a critical incident response process that allows security teams to sort through a torrent of alerts and potential threats to identify the most pressing issues. It involves immediately analyzing and prioritizing security events based on severity so that resources can be allocated accordingly.

The purpose of cybersecurity triage is to speed up the response to detected or actively unfolding IT incidents. Triage enables security analysts to jump on the most dangerous threats right away before they get out of control.

Analysts can initiate containment and mitigation steps on severe incidents while addressing less serious issues to the back of the queue for later handling.

Importance of Triage in Incident Response

Triage is essential for managing the overflow of security alerts faced by modern SOC's. Without triage, analysts could easily become overwhelmed and fail to identify and escalate critical incidents quickly enough. Triage allows them to cut through the noise faster and efficiently.

Security Triage Analysis Process

When a security alert or event comes in, the triage process kicks off with some initial detection and validation steps. Analysts will look to confirm whether a real incident has taken place or if an alert is just a false positive. Here are the triage analysis process steps:

- **Detection** – Validate security alert or event as a real incident vs. false positive
- **Scoping** – Quickly investigate incident to surface attack details, affected assets, related indicators, etc.
- **Severity Classification** – Assign severity level (low/medium/high) based on potential impact and damage.
- **Escalation** – Report the incident to appropriate parties based on the severity threshold.
- **Containment** – Initiate containment of high/critical incidents to isolate and limit damage.
- **Queuing** – Add lower severity incidents to the queue for future response based on resources.
- **Eradication** – For severe events, execute steps to eliminate threats from the environment.
- **Recovery** – For severe events, start restoration of impacted systems and data
- **Circle Back** – Continuously analyze and Triage new security alerts as they come in.

DevSecOps At A Glance

Since the folks who would be responsible for operationalizing the SOC as a whole, are the people often misunderstood for their role, its time that's changed. Their deployments are the SOC outcome, and these folks are integrating every component what makes a SOC. In most cases, they are experts in integration on both Windows and Linux platforms, write the queries and perfected it over time, and provides actionable outcomes to the analysts, or they gradually train the analysts on how to efficiently do these tasks and activities.

SecOps consists of six elements including: Business (goals and outcomes) People (who will perform the work) Interfaces (external functions to help achieve goals) Visibility

(information needed to accomplish goals) Technology (capabilities needed to provide visibility and enable people) Processes (tactical steps needed to execute on goals).

Security Operations Center processes used to be completely isolated from other parts of the organization. Developers would build systems, IT operations would run them, and security were responsible for securing them. Today it is understood that joining these three functions into one organization—with joint responsibility over security—can improve security and create major operational efficiencies.


Application security is a reactive process after deployment, where DevSecOps is proactive and controls security before deployments. The team is responsible for notifying security operations of any potential false positives and then making the appropriate exceptions so they are not inundated with false positive alerts when the application is launched. DevSecOps also notifies security operations of any data loss prevention (DLP) concerns.

When new vulnerabilities are found, application security (AppSec) validates that systems are updated and patched. Otherwise, the security team is notified that changes are required, and SecOps will need to be notified of vulnerabilities and IoCs in order to monitor systems.

Application security teams communicate frequently with the content engineering team to create new alerts, advise threat intelligence of new IoCs and gather feedback from the threat hunting team about hunts conducted on new use cases.

The Transition from a Siloed SOC to DevSecOps

Before SecOps	After SecOps	Towards DevSecOps
In the past, operations and security teams had conflicting goals. Operations was responsible for setting up systems to achieve uptime and performance goals. Security was responsible for verifying a checklist of regulatory or compliance requirements, closing security holes and putting defenses in place. In this environment, security	SecOps combines operations and security teams into one organization. Security is “shifting left”—instead of coming in at the end of the process, it is present at the beginning, when requirements are stated and systems are designed. Instead of having ops set up a system, then having security come in to secure it, systems are built from the get-go with security in mind.	SecOps has additional implications in organizations which practice DevOps—joining development and operations teams into one group with shared responsibility for IT systems. In this environment, SecOps involves even broader cooperation—between security, ops and



was a burden—perceived as something that slows down operations and creates overhead. But in reality, security is part of the requirements of every IT system, just like uptime, performance or basic functionality.

software development teams. This is known as DevSecOps. It shifts security even further left—baking security into systems from the first iteration of development.

Source: [SOC Processes and Best Practices in a DevSecOps World - Exabeam](#)

Key Components of a DevSecOps Approach

- **Analysis of code:** deliver code in small pieces so the team can quickly identify vulnerabilities.
- **Submitting changes:** permit anyone to submit changes, this can increase efficiency and speed. Afterward, observe if the change is successful or not or make changes to the provided system.
- **Monitor compliance:** be prepared for an audit at all times, which means always being in a state of compliance. They are the one's normally assigned to generate the ISMS, GDPR, Privacy policy enforcements, change management and so on.
- **Investigate threats:** identify possible threats each time the team updates code so they can respond quickly.
- **Assess vulnerability:** identify vulnerabilities with code analysis and ensure the team quickly attends to them.
- **Train security:** train software and IT engineers and provide them with instructions for set procedures.
- **Development:** deploys and maintains the CI/CD pipelines as well as the
- **Computational storage:** if CEPH or Kubernetes based applications are in use.
- **Develop a distributed SOC with DevOps:** members of a department familiar with DevOps can assist with incident response as they have an in-depth understanding of IT systems and can gain knowledge of vulnerabilities and threats from security staff.
- **Partner threat hunters with DevOps team:** threat hunters can communicate directly with dev or ops teams to address security gaps at their core, rather than isolating a threat and reporting it to management.
- **Creating superior security centers:** the SOC can work with specific dev and operation groups to put in place security best practices. They can convey these positive results to the entire organization to encourage DevSecOps practices.
- **Make the SOC available for advice and guidance:** everyone working with security should be able to easily contact the SOC and liaise with the top security experts of the organization.

Lastly, the DevOps and the SecOps both performs overlapping functions, and usually they are combined in a form to perform as a DevSecFinOps, and these personnel are the ones who are supporting and keeping the SOC infrastructure alive.

Functions of a SOC Analyst (L1, L2, L3)

Security Operations Center (SOC) analysts play a crucial role in maintaining an organization's cybersecurity. Here are some of their key responsibilities:

1. **Monitoring and Protecting:** SOC analysts monitor and protect the organization's assets, including personnel data, brand integrity, intellectual property, and operation systems.
2. **Triage Specialist (Tier 1 Analyst):** Tier 1 analysts collect raw data, review alarms and alerts, confirm or adjust the criticality of alerts, and enrich them with relevant data. They also manage and configure the monitoring tools.
3. **Incident Responder (Tier 2 Analyst):** Tier 2 analysts review higher-priority security incidents escalated by Tier 1 analysts and perform a more in-depth assessment using threat intelligence. They design and implement strategies to contain and recover from an incident.
4. **Threat Hunter (Tier 3 Analyst):** Tier 3 analysts handle major incidents escalated by Tier 2 analysts. They proactively identify possible threats, security gaps, and vulnerabilities.



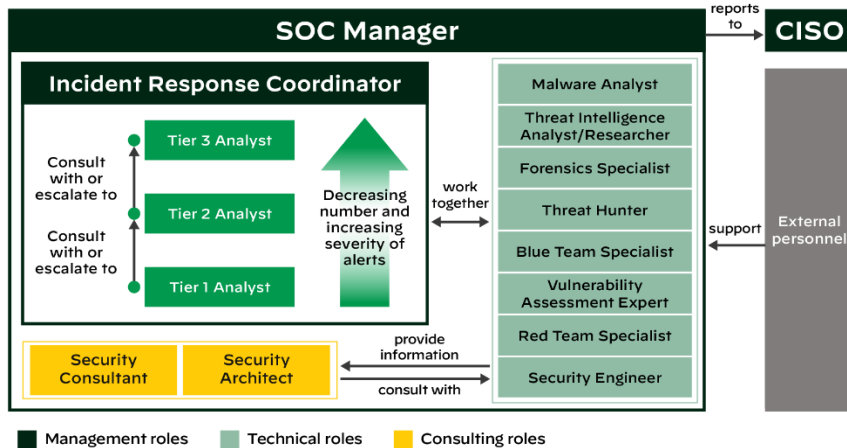
Source: [SOC Analyst Career Path: Certification, Role, Salary, and More - KINGSLAND UNIVERSITY](#)

5. **Collaboration:** SOC analysts work with other departments of the company, such as human resources or sales, to ensure that their systems are secure.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

- 6. Tool Management:** SOC analysts use various tools to monitor and analyze network traffic. They monitor firewall, email, web, and DNS logs to identify and mitigate intrusion attempts.
- 7. Reporting:** SOC analysts are responsible for documenting cyber incidents and implementing incident response plans.

These roles and responsibilities may vary depending on the organization's size, industry, and cybersecurity maturity.



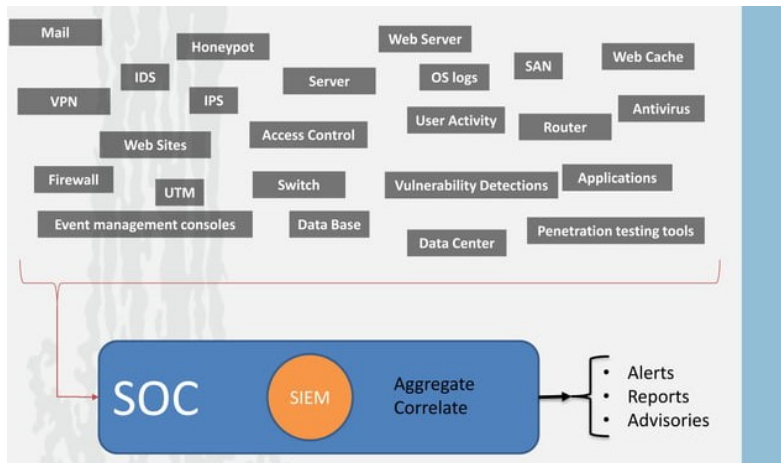
Source: Security Operations Center: A Systematic Study and Open Challenges

Source: [Security Operations Center \(SOC\) Roles and Responsibilities - Palo Alto Networks](#)

Functions of a Triage Specialist (Tier 1 Analyst), in a SOC

A Triage Specialist, also known as a Tier 1 Analyst, in a Security Operations Center (SOC) has several key responsibilities:

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Source: [An introduction to SOC \(Security Operation Center\) | PPT \(slideshare.net\)](#) by Ahmad Haghghi

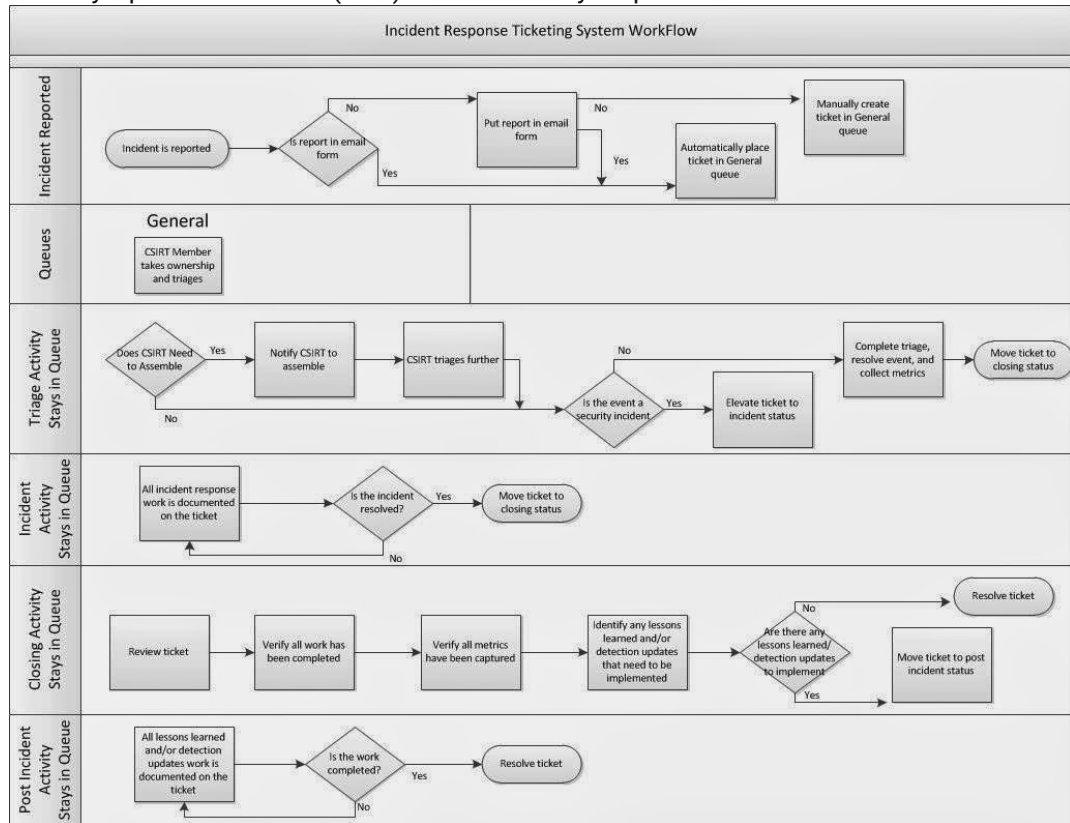
Some of the components that a SOC has visibility and alerts on

1. **Reviewing Alerts and Incident Reports:** They review alarms, alerts, and incident reports.
2. **Triage and Prioritize Alerts:** They confirm, determine, or adjust the criticality of alerts and enrich them with relevant data.
3. **Conducting Initial Research:** They conduct initial research to gather more information about the incident.
4. **Documenting Activities:** They document all activities, including initial assessments, steps taken, and recommendations for further action.
5. **Identifying High-Risk Events:** They identify other high-risk events and potential incidents.
6. **Managing Monitoring Tools:** They often manage and configure the monitoring tools.
7. **Escalation:** If problems occurring cannot be solved at this level, they have to be escalated to tier 2 analysts.


These responsibilities are crucial for maintaining the security posture of an organization. They provide the **first line** of defense against cyber threats.

Functions of an Incident Responder (Tier 2 Analyst), in a SOC

Tier 2 Analyst in a SOC is an Incident Responder, also known as a Tier 2 Analyst, in a Security Operations Center (SOC) has several key responsibilities:



1. **Reviewing Incidents:** They review the higher-priority security incidents escalated by Tier 1 analysts.
2. **In-Depth Assessment:** They perform a more in-depth assessment using threat intelligence, such as indicators of compromise and updated rules.
3. **Understanding the Scope:** They need to understand the scope of an attack and be aware of the affected systems.
4. **Transforming Data:** The raw attack telemetry data collected at Tier 1 is transformed into actionable threat intelligence at this second tier.

- 
5. **Incident Response:** Incident responders are responsible for designing and implementing strategies to contain and recover from an incident.
 6. **Escalation:** If a Tier 2 analyst faces major issues with identifying or mitigating an attack, additional Tier 2 analysts are consulted, or the incident is escalated to Tier 3.
 7. **Investigating Security Incidents:** They investigate security incidents and determine the root cause of the incident.
 8. **Detailed Incident Reports:** They provide detailed incident reports and recommendations for remediation.
 9. **Responding to Escalated Alerts:** They respond to escalated alerts, notifications, communications, and provide incident response activities such as tracking the incident, communication with stakeholders, remediation and recovery actions, and reporting.

These responsibilities are crucial for maintaining the security posture of an organization. They provide the **second line** of defense against cyber threats.

Functions of A Threat Hunter (Tier 3 Analyst) in a SOC

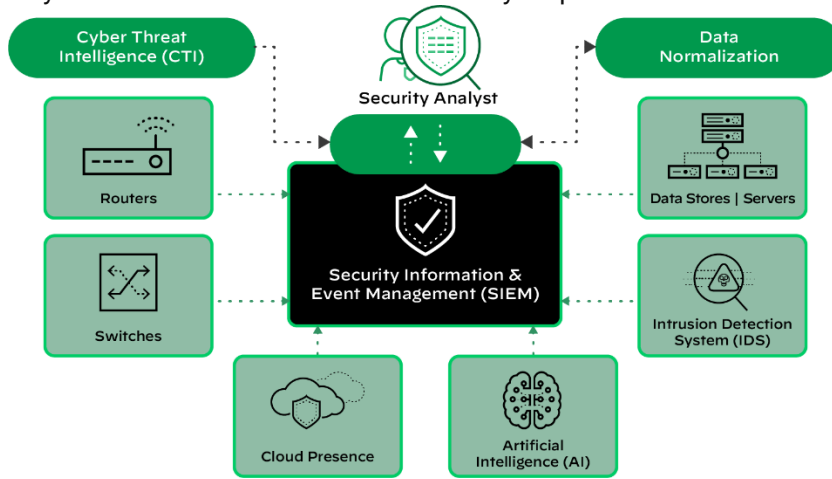
In a Security Operations Center (SOC) has several key responsibilities:

1. **Handling Major Incidents:** They handle major incidents escalated to them by the incident responders.
2. **Vulnerability Assessments and Penetration Tests:** They perform or at least supervise vulnerability assessments and penetration tests to identify possible attack vectors.
3. **Proactive Threat Identification:** Their most important responsibility is to proactively identify possible threats, security gaps, and vulnerabilities that might be unknown.
4. **Advanced Asset Protection:** They use internal and external threat intelligence to search for anomalous behavior, test security controls, and perform advanced asset protection.
5. **Regular Reviews of Security Controls:** They perform regular reviews of security controls.
6. **Closing Security Gaps:** They review industry news and threat intelligence to identify new vulnerabilities, close security gaps, and make the SOC team more efficient in general.

These responsibilities are crucial for maintaining the security posture of an organization. They provide the **third line** of defense against cyber threats.

Functions of a Cyber Threat Intelligence (CTI) Manager

Cyber Threat Intelligence (CTI) Manager plays a crucial role in an organization's cybersecurity framework. Here are some of their key responsibilities:




Source: [Security Operations Center \(SOC\) Roles and Responsibilities - Palo Alto Networks](#)

SECURITY OPERATION CENTER ROLES



Source: [What Is a Security Operations Center \(SOC\)? - Palo Alto Networks](#)


Planning: They plan the collection, processing, analysis, and dissemination of information about threats against applications, systems, or industries.

- 
1. **Collecting and Analyzing Threat Data:** CTI Managers collect and analyze current and potential threat data.
 2. **Understanding Attack Behavior and Motives:** They understand a cyber attacker's attack behavior and motives, and predict the attackers' next attack targets.
 3. **Risk Mitigation:** They use the intelligence to prioritize the SOC team's day-to-day response and remediation activities, helping to mitigate the risks of new cyber threats.
 4. **Promoting Proactive Cybersecurity Measures:** They promote proactive cybersecurity measures for fighting cyberattacks rather than reactive cybersecurity, where security mechanisms trigger only after an incident is identified.
 5. **Informing Practices and Use Cases:** Threat intel informs practices and use cases like vulnerability management, risk management, incident response and incident management, and overall security operations.
 6. **Empowering Organizations:** They empower organizations to make better informed, faster, and data-driven decisions on cybersecurity.
 7. **Supporting Threat Detection and Incident Response:** They feed the detection, prevention, response cycle, and support threat detection and incident response.

These responsibilities help organizations avoid financial losses and reputational damages due to data breaches. They also enable organizations to cut down unnecessary costs.

Functions of a 'SOC Manager' in a SOC

A SOC (Security Operations Center) Manager plays a crucial role in an organization's cybersecurity framework. Here are some of their key responsibilities:

- **Team Management:** They direct SOC operations and are responsible for syncing between analysts and engineers. They oversee the SOC team, ensuring everyone is trained, motivated, and effectively working together.
 - **Hiring and Training:** They are responsible for hiring new staff members and providing regular training sessions and mentorship opportunities to facilitate knowledge-sharing within the team.
 - **Developing and Implementing Security Policies:** SOC Managers play a key role in creating and enforcing security policies. They develop security policies by reviewing industry standards and working closely with other departments to understand their security needs.
 - **Establishing SOC Performance Goals and Priorities:** They establish performance goals and priorities for the SOC.
- 

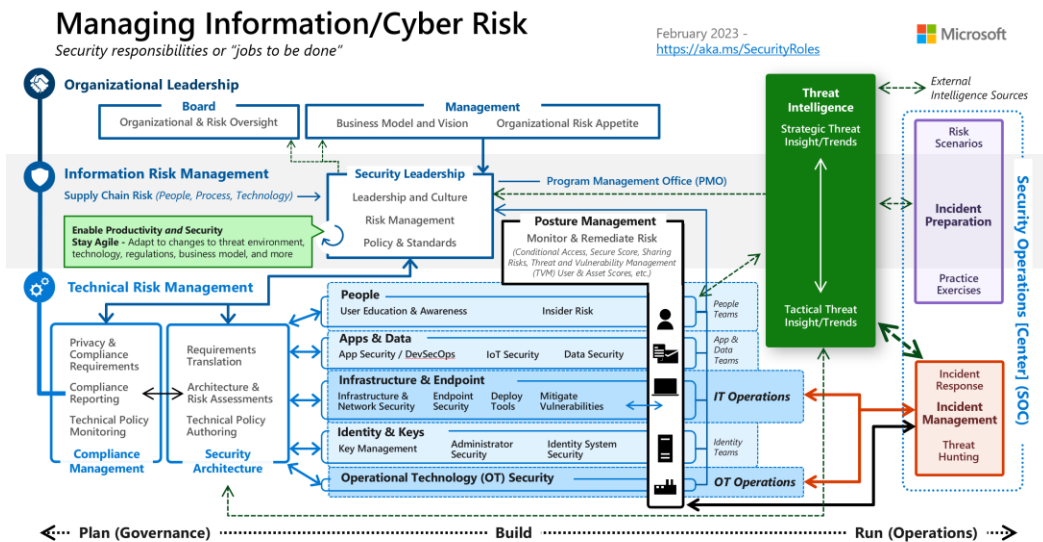
COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

- **Reporting:** They provide regular updates on the SOC's activities and performance and any notable incidents or threats that have been detected. They also report to the Chief Information Security Officer (CISO) about security operations.
- **Cybersecurity Strategy:** They are responsible for creating and executing the organization's cybersecurity strategy.
- **Responding to Major Security Threats:** They direct and orchestrate the company's response to major security threats.

These responsibilities help organizations avoid financial losses and reputational damage due to data breaches. They also enable organizations to cut down unnecessary costs.


Functions of a Security Architect in a SOC

A Security Architect in a Security Operations Center (SOC) plays a crucial role in maintaining an organization's cybersecurity. Here are some of their key responsibilities:



Source: [Microsoft Cybersecurity Reference Architectures \(MCRA\) - Security documentation | Microsoft Learn](#)

1. **Designing and Tuning Security Detections:** They work directly with customers and security tools to design and tune security detections.

- 
2. **Planning:** They plan, research, and design a robust security infrastructure within the company. Architects develop standards, and frameworks for blueprints that engineers and analysts use to deploy secure systems.
 3. **Conducting Regular System and Vulnerability Tests:** They conduct regular system and vulnerability tests. Vulnerability Management teams (engineers and analysts) conducts these tests.
 4. **Implementing Enhancements:** They implement or supervise the implementation of enhancements.
 5. **Collaborating with SOC Analysts:** They collaborate with SOC analysts to investigate security incidents raised by security tools.

These responsibilities help organizations avoid financial losses and reputational damage due to data breaches. They also enable organizations to cut down unnecessary costs.





CHAPTER

9

Zero Trust Security

NOTIFY EACH RISK TYPES WITH CORRELATED DATA, THE MOMENT YOU HAVE NOTIFIED THIS, NOW IT'S THE SERVER ADMIN'S TASK TO UPDATE THE SERVICE OR PATCH IT OR HAVE A WORKAROUND IN PLACE. YOUR PRIMARY JOB IS TO IDENTIFY RISKS AND REDUCE THE ATTACK SURFACE AREA, YES, THAT'S HOW YOU BECOME A CISO.


Your foundation starts with it. Previously it was like “Trust everyone, but do monitor”, and since our human activities came out to be destructive, the motto changed to “Trust no one, monitor everyone!”

Benefits of The Principle of The Least Privileged (PoLP)

The principle of least privilege (POLP) is a security concept that limits user access rights to only the necessary resources and privileges required for performing their task, which also reduces your infrastructures attack surface area. The benefits of POLP include:

- **Minimizing attack surface.** Fewer and more controlled privileges limit the paths by which a malicious actor can enter your network and exploit the assets within.



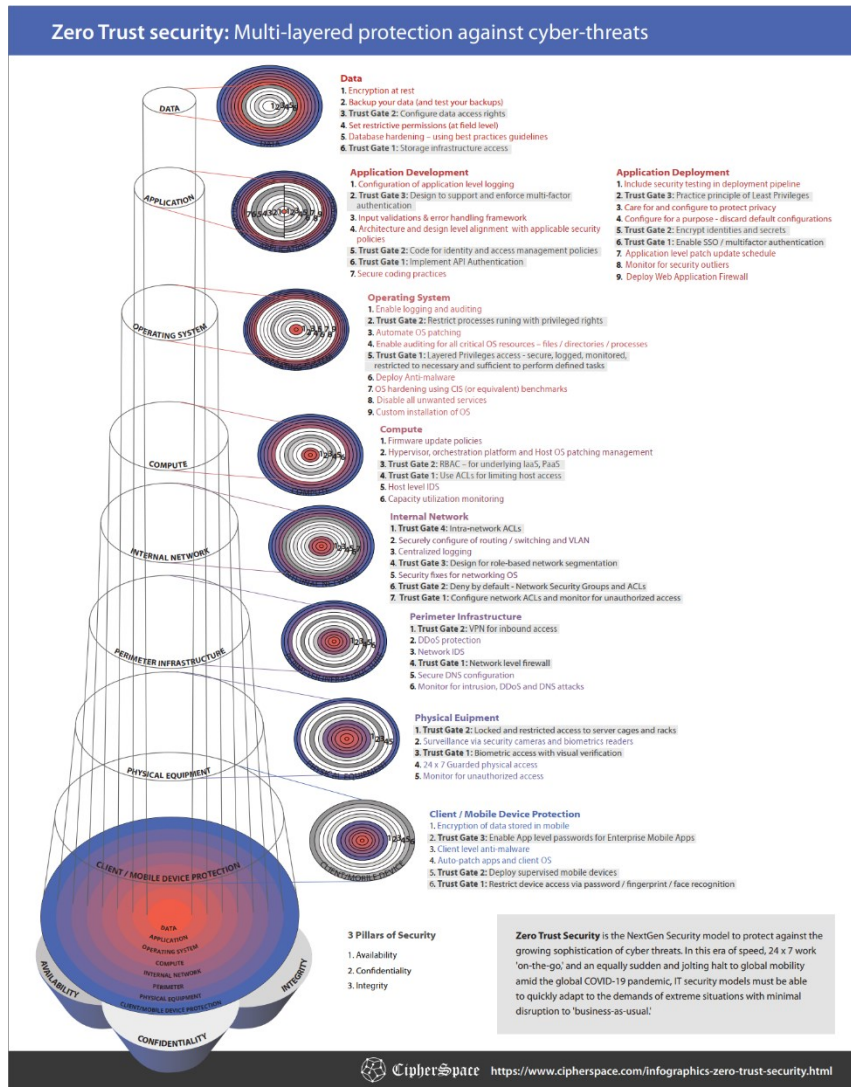


Using least privilege policies can help you prevent, find, and defend against harmful activity.

- **Limiting the spread of malware.** If an organization grants too much access, malware can quickly spread once it accesses a device. Granular controls confine malware to the place it first enters.
- **Improving overall operations.** Limiting the risks associated with a breach also means limiting the amount of downtime and work involved in resolving the problem.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

- Meeting regulatory guidelines.** If you operate in a regulated industry, you may be subject to certain regulatory guidelines for cybersecurity. Implementing a principle of least privilege policy can support the audit process related to regulatory compliance, as it can provide audit trails of activity in your network. For



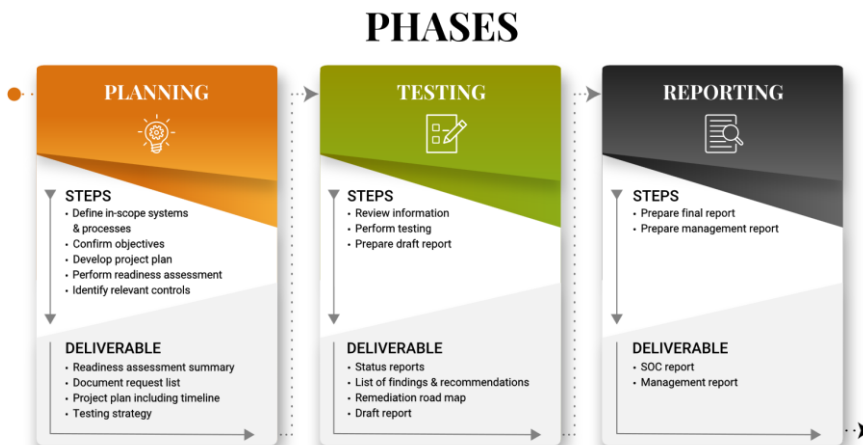
example, if your organization must comply with General Data Protection Regulation (GDPR), you may be audited to ensure compliance. With the right

solutions, you can record and monitor activity, users, and devices to meet GDPR compliance while also ensuring your organization's and users' security.

- **Guarding against human error or malice.** Human users can inadvertently or purposely cause harm to an organization if proper safeguards aren't in place. If someone decides to install malicious code or simply makes an error when typing a command, least privilege controls can help limit the damage.
- **Cost savings.** Downtime caused by a malicious attack can be costly for your organization. Investing in access management software can centralize and automate the approval and denial process to defend against future attacks and quickly resolve attacks if and when they occur.


Functions of a SOC Compliance Auditor in a SOC

A SOC (Service Organization Control) Compliance Auditor in a Security Operations Center (SOC) plays a crucial role in maintaining an organization's cybersecurity. Here are some of their key responsibilities:



Source: [SOC Audit & SOC Compliance | Armanino](#)

1. **Evaluating Controls:** The auditor checks the internal controls in place at third-party service providers. These controls are necessary to protect client data, financial information, and intellectual property.
2. **Preparing SOC Reports:** The auditor compiles a detailed report, which includes a description of the company's system, its services, and the specific controls in place. The report also contains the auditor's opinion on the effectiveness of the controls.

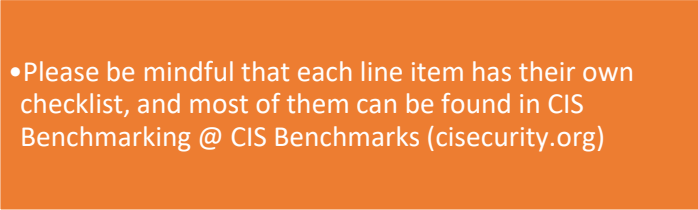
- 
3. **Ensuring Compliance with AICPA Guidelines:** As a representative of the AICPA, the SOC auditor ensures that service organizations adhere to the requirements of the selected SOC audit type (either SOC 1, SOC 2, or SOC 3). These are for **Service Operational Controls**.
 4. **Assessing Security, Availability, Processing Integrity, Confidentiality, and Privacy:** A SOC audit is an assessment of a service organization's internal controls related to the security, availability, processing integrity, confidentiality, and privacy of their systems.
 5. **Building Trust and Confidence:** Companies often use SOC audits to build trust and confidence with their customers.

These responsibilities help organizations avoid financial losses and reputational damage due to data breaches. They also enable organizations to cut down unnecessary costs.

Knowledge Area (not an exhaustive list)

Below is the list of items that provides insights into the high level requirements of the security benchmarking of your networked devices (firewall, router, switches, printers, servers), operating systems, applications, IoT, SCADA systems, client nodes with Windows or Linux distributions etc.

Pro-Tip

- 
- Please be mindful that each line item has their own checklist, and most of them can be found in CIS Benchmarking @ CIS Benchmarks (cisecurity.org)

Your 1-Stop Point for all Benchmark Checklists from CISECURITY

Cloud Providers

- Alibaba Cloud
- Amazon Web Services
- Google Cloud Computing Platform
- Google Workspace
- IBM Cloud Foundations
- Microsoft 365
- Microsoft Azure

- Microsoft Dynamics 365 Power Platform
- Oracle Cloud Infrastructure

Desktop Software

- Microsoft Exchange Server
- Microsoft Office
- Zoom
- Google Chrome
- Microsoft Web Browser
- Mozilla Firefox

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

- Safari Browser
- DevSecOps Tools**
- Software Supply Chain Security
- Mobile Devices**
- Apple iOS
 - Google Android
- Multi Function Print Devices**
- Print Devices
- Network Devices**
- Check Point Firewall
 - Cisco
 - F5
 - Fortinet
 - Juniper
 - Palo Alto Networks
 - pfSense Firewall
 - Sophos
- Operating Systems**
- IBM i
 - IBM Z System
 - Aliyun Linux
 - AlmaLinux OS
 - Amazon Linux
 - Bottlerocket
 - CentOS Linux
 - Debian Family Linux
 - Debian Linux
 - Distribution Independent Linux
 - Fedora Family Linux
 - LXD
 - Oracle Linux
 - Red Hat Enterprise Linux
 - Robot Operating System (ROS)
 - Rocky Linux
 - SUSE Linux Enterprise Server
 - Ubuntu Linux
 - Microsoft Intune for Windows
 - Microsoft Windows Desktop
 - Microsoft Windows Server
 - Apple macOS
 - IBM AIX
 - Oracle Solaris
- Server Software**
- MIT Kerberos
 - Microsoft SharePoint
 - Apache Cassandra
 - IBM Db2
 - MariaDB
 - Microsoft SQL Server
 - MongoDB
 - Oracle Database
 - Oracle MySQL
 - PostgreSQL
 - BIND
 - Docker
 - Kubernetes
 - VMware
 - Apache HTTP Server
 - Apache Tomcat
 - IBM WebSphere
 - Microsoft IIS
 - NGINX

Source: [CIS Benchmarks \(cisecurity.org\)](https://www.cisecurity.org)

If you have downloaded any of the above-mentioned benchmark documents, you will find the checklist at the end of each of the documents provided by CIS benchmark controls.

Pro-Tip

• These are extensive checklists per product, and can be daunting to achieve 6 on a scale of 10, but still that doesn't mean that you will be secured, nothing is 100% secured despite your best efforts.

Classified as	Solution Description
IT Support (Enterprise) (Managed Services)	Branch IT Support (IT under an SLA)
	Laptop OS Image Deployment
	Desktop OS Image Deployment
	Network Troubleshooting
	Threat Monitoring by Branch, managed services
	Network uptime management
	Device Standardization Across the Organization
	Firmware Update Per Device
	Patch Update Per Device
	Printer Management by SSO-ID Card
	Internet/Access: Router & Switch Mgmt.
	CCTV-Camera & NVR Management
	Antivirus/Ransomware Management Per Device
	Hardware Management & Reporting Services
	Servers
	Routers
	Switches
	CCTV Camera with NVR
	MFP Printers
	ECM Scanners (Enterprise Content Management)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



	Laptops
	Desktops
	UPS & Battery
	Rack PDU Management (Power Distribution Unit)
	Cables - Cat6A, Cat-7A, USB Cables etc.
	Automated Print Support
	MFP Printer Installations
	Integration with Active Directory SSO
	ID Card Based Printing & Authentication
	Automated Print Queue Management
	Monthly Usage Reporting
	SLA Bindings (Service Level Agreement)
	System Integration
	Various Server & Client Based Software Installation
	3rd Party Software Installation
	Middleware Installation – RPA (Robotic Process Automation)
	Monitoring Service Implementation
	Network & Application Performance Tuning
Industrial Systems	SCADA Sensor Deployment (Supervisory Control And Data Acquisition)
	PLC Development (Programmable Logic Controller)
	Vulnerability Assessment
	Penetration Testing



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Cyber Security	Cyber Security Gap Analysis
	Cyber Security Resilience Review
	Vulnerability Assessment
	Penetration Testing
	Incident Response
Enterprise Network Design	Application SSO (Single Sign-on)
	Network Design Review
	Vulnerability Assessment
	Penetration Testing
	Application Centric Infrastructure
	Cisco DNA, SDN Infrastructure
	ITIL Process Deployment
	NMS Deployment & Alert Reporting or Managed Services
Application Development & Integration	Gap Analysis
	Enterprise Resource Planning
	Customer Relationship Management
	Finance & Accounting Management
	Customized Application Development
	Domain hosting, parking
	SSL Certificate Deployment
	Web Site & Application Development
	Bulk SMS Services
	Bulk Email Services



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



	DIAL Group DID Numbers
	Payment Gateway Integration
IT-CMF	Gap Analysis
	IT Capability Maturity Matrix Development for the Tech Folks
	ITIL - IT Information Library Process Management
	COBIT- Process Implementation
ISO/IEC Compliance	Gap Analysis
	27001 - Information Security Management System Development
	27001 - Certification
	PCI-DSS - Payment Card Industry Data Security Standard
	22301 - Business Continuity Planning
	22301 - Certification
Microsoft Deployment Services	Gap Analysis
	Active Directory (SSO)
	Exchange Email Server
	SharePoint Collaboration Server
	ECM - Enterprise Content Management
	DMS - Data Management Services
	LMS - Learning Management Services
	Skype for Business Server
	Dynamics Development & Integrations
	SQL Server Deployment



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



	System Center Datacenter
	SCCM - Configuration Manager
	SCEP - Endpoint Protection
	SCOM - Operation Manager
	SCDPM - Data Protection Manager
	SCSM - Service Manager
	SCVMM - Virtual Machine Manager
	Sentinel & SIEM Deployment
	BI Analytics & Dashboard Development
	Privileged Access Management
Application & API Security Testing	Gap Analysis
	Any Application
	Core Banking Software
	Banks Internally Built Application
	Web Application Security Testing
Datacenter Design	Datacenter Managed Services & Reporting
	EIA/TIA-942 Certification
	Design and Deployment
	Environment Monitoring
	DCIM - Datacenter Infrastructure Management
Contact Center (IPTSP)	On-prem or Managed Services
	Design & Deployment
	Custom Solution with IVR Systems



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



	Customized Dashboards
	Reporting Services
SOC Development	SOC Design & Development
	JD Development for L1, L2, L3 Analyst
	Gap Analysis
	1.SIEM - Security Information & Event Management
	2.IAM - Identity & Access Management
	3.PAM - Privilege Access Management
	4.ACI - Application Centric Infrastructure
	5.APM - Application Performance Monitoring
	6.DRM - Data Rights Management
	7.BPM - Business Process Management
	8.DAM - Database Activity Monitoring
	9.LMS - Learning Management System
	10.RMM - Remote Monitoring & Management
	11.SDWAN - Software Defined WAN
	12.SDN - Software Defined Network
	13.SDDC - Software Defined Data Center
	14.SOC - Service Organizational Controls
	15.SOC - Security Operation Center
	16.OSINT – Open-Source Intelligence
	17.SPF - Security Policy Framework
18.RPA - Robotic Process Automation	
19.UEBA - User Entity Behavior Analytics	
20.MDR - Managed Detection And Response	



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



21.EDR - Endpoint Detection & Remediation/Response
22.DFIR - Digital Forensics Incident Response
23.EMM - Enterprise Mobile Management
24.HCI - Hyper Converged Infrastructure
25.SOAR - Security Orchestration, Automation and Response
26.DLP - Integrated Data Loss Prevention (Host & Network)
27.ISAC - Information Sharing and Analysis Centers
28.DNS – Domain Name Service Protection
29.DCIM - Datacenter Infrastructure Management
30.EMS - Environmental Monitoring Services
31.ZTNA - Zero Trust Network Architecture
32.ECM - Enterprise Content Management
33.CASB - Cloud Access Security Broker
34.CWPP - Cloud Workload Protection Platforms
35.CSPM - Cloud Security Posture Management
36.SSE - Security Service Edge
37.SWG - Secure Web Gateway
38.WAF - Web Application Firewall
39.SASE - Secure Access Service Edge
40.CIEM - Cloud Infrastructure Entitlement Management
41.CIG - Cloud Identity Governance
42.TVM - Threat and Vulnerability Management
43.CTEM - Continuous Threat Exposure Management
44.RBVM – Risk based Vulnerability Management
45.VMDR – Vulnerability Management, Detection & Response (Under RBVM)



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Compliance Implementation	Gap Analysis
	SWIFT CSP Consultancy & Assessment
	ITIL Implementation
	GRC Program Development with a 3years Perspective Plan
	ISO 27001, 22301 Documentation Development & Implementation
	Networked Device Hardening
	Application Hardening: Web Based & Custom
	Security Program Development & Implementation
	IT Quality Implementation on ISMS, HelpDesk, API Integrations etc.
	CISECURITY Cyber Security Control Implementation
Broadcast Multimedia	Design & Integration Services
	MCR Development
	Gallery Implementations
	ENG Equipment
	Video Conferencing Equipment
	Video on Demand Setup for TV, Mobile
	RF Equipment
	Sound Proofing Systems
Smart City Initiatives	Power Generation - Wind & Solar
	Camera Grid Systems
	GIS - Drone Based underwater landscape mapping
	GIS - Drone Based landscape mapping



	AI Based - Face recognition & car number plate mapping
	Railway/Train WiFi

Copy and paste the spreadsheet into an excel file, make your own roadmap. Use the 3yrs planning tool as well as this worksheet.

Malware Sandbox Tools for Analysis

Malware sandbox tools are automated analysis tools that help with triage during incident response and forensic investigations. They provide an overview of the specimen's capabilities, so that analysts can decide where to focus their follow-up efforts. Sandboxes can be software applications, virtual machines, embedded software, or browser plug-ins. Some examples of free, hosted services that perform automated malware analysis are **AMAAaS**, **Any.run**, **Binary Guard**, **True Bare Metal**, **Intezer Analyze**, **IRIS-H**, and **CAPE Sandbox**.


Two good solutions for daily use are ANY.RUN and Joe Sandbox. On the other hand paid versions like Kaspersky's threat intelligence portal shows promising results like the below screenshot of the malware named "RemcosRAT". It readily shows IoCs, execution map, payload delivery, activities, MITRE ATT&CK matrix. You can checkout the MITRE Attack Flow v2.1.0 from the following link

[Attack Flow v2.1.0 – Attack Flow v2.1.0 documentation \(center-for-threat-informed-defense.github.io\)](#)

And there is a but as well, not all sandbox produces directly related results, its not fully automated, as the KB needs to be feed into the search engine, where it is impossible to have all of the malwares dissected, and how it works results incorporated into one giant KB.

Once the analysis is complete, Kaspersky's Research Sandbox provides a detailed report on the behavior and functionality of the analyzed sample, allowing you to define the appropriate response procedures:

1. **Summary** – general information about a file's execution/URL browsing results.
2. **Sandbox** detection names – a list of detections (both AV and behavioral) that were registered during the file execution.
3. **Triggered** network rules – a list of network SNORT rules that were triggered during analysis of traffic from the executed object.

- 
4. **Execution** map – a graphically represented sequence of object activities (actions taken on files, processes and the registry, and network activity) and the relationship between them. The root node of the tree represents the executed object.
 5. **Suspicious** activities – a list of registered suspicious activities.
 6. **Screenshots** – a set of screenshots that were taken during the file execution/URL browsing.
 7. **Loaded** PE images – a list of loaded PE images that were detected during the file execution/URL browsing.
 8. **File** operations – a list of file operations that were registered during the file execution/URL browsing.
 9. **Registry** operations – a list of operations performed on the OS registry that were detected during the file execution/URL browsing.
 10. **Process** operations – a list of interactions of the file with various processes that were registered during the file execution.
 11. **Synchronize** operations – a list of operations of created synchronization objects (mutex, event, semaphore) that were registered during the file execution/URL browsing.
 12. **Downloaded** files – a list of files that were extracted from network traffic during the file execution/URL browsing.
 13. **Dropped** files – a list of files that were saved (created or modified) by the executed file.
 14. **HTTPS/HTTP/DNS/IP/TCP/UDP** and etc. – network sessions/requests details that were registered during the file execution/URL browsing
 15. **Network** traffic dump (PCAP) – network activity can be exported in PCAP format.
 16. **MITRE ATT&CK** matrix – all identified process activities recorded during emulation are presented in the form of a MITRE ATT&CK matrix.

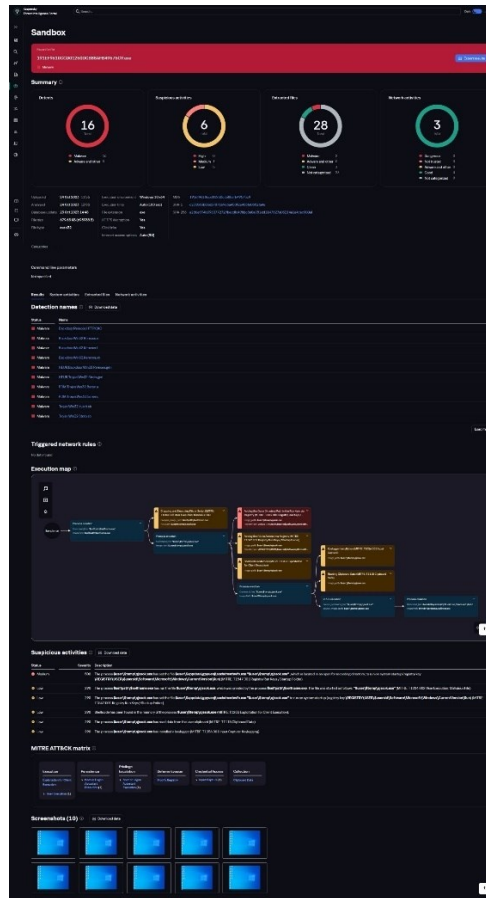
Source: Kaspersky Research Sandbox Datasheet (screenshot provided below): [Advanced Automated Malware Analysis – Kaspersky Research Sandbox | Kaspersky](#)

Moreover, further tools can be found here for your daily need:

1. [Malware Analysis Tools | 25 Best Malware Analysis Tools and Techniques \(educba.com\)](#)
 2. [13 Best Malware Analysis Tools Of 2024 - RankRed](#)
- 


Pro-Tip

- You should know that sandboxes should be run in a containerized environment, therefore, if you are testing malware or any other types of malicious codes, you would be protected from the harm it can cause



Indicators of Compromise (IoC)

Indicators of Compromise (IoC) are pieces of information (aka misconfigurations that left a whole in the device/application exploitable and the digital signature or footprint left by



the attackers) that indicate a potential security breach or cyberattack can or did occur exploiting those misconfigurations.

Cybersecurity professionals use them to identify and respond to threats effectively. IoCs can be a file, IP address, domain name, registry key, or any other evidence of malicious activity. They can help organizations locate and confirm the presence of malicious software on a device or network. Indicators of Compromise (IoCs) are evidence left behind by an attacker or malicious software that can be used to identify a security incident.

Learning how to identify IoCs is a job handled almost exclusively by trained infosec professionals. Often these individuals leverage advanced technology to scan and analyze tremendous amounts of network traffic, as well as isolate suspicious activity. The most effective cybersecurity strategies blend human resources with advanced technological solutions, such as AI, ML and other forms of intelligent automation to better detect anomalous activity and increase response and remediation time.

Some common Indicators of Compromise (IoCs) are:

1. Unusual traffic patterns between internal systems
2. Unusual usage patterns for privileged accounts
3. Administrative access to your network from unsuspected geographical locations
4. A spike in database read volume
5. A high rate of authentication attempts and failures
6. Unusual configuration changes

These are some of the signs that a system or network may have been breached by a cyber threat. IoCs can help cybersecurity professionals identify and respond to malicious activity effectively.

TTP (Tactics, Techniques, Procedures)

TTPs stands for tactics, techniques, and procedures. This is the term used by cybersecurity professionals to describe the behaviors, processes, actions, and strategies used by a threat actor to develop threats and engage in cyberattacks. TTPs can help security teams detect and mitigate attacks by understanding the way threat actors operate and the tools they use. There are several frameworks and initiatives that can help security teams identify and address TTPs, such as MITRE ATT&CK, OWASP. TTPs can also be discovered by analyzing the artifacts, tools, and infrastructure changes that lead up to any anomalous networking incident.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Map of Attack Scenarios to TTP (Sample)

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
T100: Drive-by-Download T101: Exploitation of Public-Facing Services T102: Phishing T103: Spear Phishing T104: Watermark T105: Malicious File T106: Malicious Link T107: Malicious Email T108: Malicious Document T109: Malicious PDF T110: Malicious Image T111: Malicious Video T112: Malicious Audio T113: Malicious Script T114: Malicious Java T115: Malicious JavaScript T116: Malicious CSS T117: Malicious XML T118: Malicious JSON T119: Malicious YAML T120: Malicious Dockerfile T121: Malicious Kubernetes Manifest T122: Malicious Helm Chart T123: Malicious Terraform Script T124: Malicious Ansible Playbook T125: Malicious Puppet Manifest T126: Malicious Chef Cookbook T127: Malicious Salt Pillar T128: Malicious Nix Flake T129: Malicious Docker Compose T130: Malicious Kubernetes Deployment T131: Malicious Kubernetes Service T132: Malicious Kubernetes Ingress T133: Malicious Kubernetes ConfigMap T134: Malicious Kubernetes Secret T135: Malicious Kubernetes PersistentVolumeClaim T136: Malicious Kubernetes StorageClass T137: Malicious Kubernetes StatefulSet T138: Malicious Kubernetes CronJob T139: Malicious Kubernetes Job T140: Malicious Kubernetes PodDisruptionBudget T141: Malicious Kubernetes NetworkPolicy T142: Malicious Kubernetes ResourceQuota T143: Malicious Kubernetes LimitRange T144: Malicious Kubernetes PodSecurityPolicy T145: Malicious Kubernetes PodSecurityRestriction T146: Malicious Kubernetes PodSecurityStandard T147: Malicious Kubernetes PodSecurityPolicyException T148: Malicious Kubernetes PodSecurityRestrictionException T149: Malicious Kubernetes PodSecurityStandardException T150: Malicious Kubernetes PodSecurityPolicyExceptionException T151: Malicious Kubernetes PodSecurityRestrictionExceptionException T152: Malicious Kubernetes PodSecurityStandardExceptionException T153: Malicious Kubernetes PodSecurityPolicyExceptionExceptionException T154: Malicious Kubernetes PodSecurityRestrictionExceptionExceptionException T155: Malicious Kubernetes PodSecurityStandardExceptionExceptionException T156: Malicious Kubernetes PodSecurityPolicyExceptionExceptionExceptionException T157: Malicious Kubernetes PodSecurityRestrictionExceptionExceptionExceptionException T158: Malicious Kubernetes PodSecurityStandardExceptionExceptionExceptionException T159: Malicious Kubernetes PodSecurityPolicyExceptionExceptionExceptionExceptionException T160: Malicious Kubernetes PodSecurityRestrictionExceptionExceptionExceptionExceptionException T161: Malicious Kubernetes PodSecurityStandardExceptionExceptionExceptionExceptionException T162: Malicious Kubernetes PodSecurityPolicyExceptionExceptionExceptionExceptionExceptionException T163: Malicious Kubernetes PodSecurityRestrictionExceptionExceptionExceptionExceptionExceptionException T164: Malicious Kubernetes PodSecurityStandardExceptionExceptionExceptionExceptionExceptionException T165: Malicious Kubernetes PodSecurityPolicyExceptionExceptionExceptionExceptionExceptionExceptionException T166: Malicious Kubernetes PodSecurityRestrictionExceptionExceptionExceptionExceptionExceptionExceptionException T167: Malicious Kubernetes PodSecurityStandardExceptionExceptionExceptionExceptionExceptionExceptionException T168: Malicious Kubernetes PodSecurityPolicyExceptionExceptionExceptionExceptionExceptionExceptionExceptionException T169: Malicious Kubernetes PodSecurityRestrictionExceptionExceptionExceptionExceptionExceptionExceptionExceptionException T170: Malicious Kubernetes PodSecurityStandardExceptionExceptionExceptionExceptionExceptionExceptionExceptionException T171: Malicious Kubernetes PodSecurityPolicyExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionException T172: Malicious Kubernetes PodSecurityRestrictionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionException T173: Malicious Kubernetes PodSecurityStandardExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionException T174: Malicious Kubernetes PodSecurityPolicyExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionException T175: Malicious Kubernetes PodSecurityRestrictionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionException T176: Malicious Kubernetes PodSecurityStandardExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionException T177: Malicious Kubernetes PodSecurityPolicyExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionException T178: Malicious Kubernetes PodSecurityRestrictionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionException T179: Malicious Kubernetes PodSecurityStandardExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionException T180: Malicious Kubernetes PodSecurityPolicyExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionExceptionException	T101: Execution T102: Command and Control T103: Persistence T104: Privilege Escalation T105: Defense Evasion T106: Credential Access T107: Discovery T108: Lateral Movement T109: Collection T110: Command and Control T111: Exfiltration T112: Impact	T101: Execution T102: Command and Control T103: Persistence T104: Privilege Escalation T105: Defense Evasion T106: Credential Access T107: Discovery T108: Lateral Movement T109: Collection T110: Command and Control T111: Exfiltration T112: Impact	T101: Execution T102: Command and Control T103: Persistence T104: Privilege Escalation T105: Defense Evasion T106: Credential Access T107: Discovery T108: Lateral Movement T109: Collection T110: Command and Control T111: Exfiltration T112: Impact	T101: Execution T102: Command and Control T103: Persistence T104: Privilege Escalation T105: Defense Evasion T106: Credential Access T107: Discovery T108: Lateral Movement T109: Collection T110: Command and Control T111: Exfiltration T112: Impact	T101: Execution T102: Command and Control T103: Persistence T104: Privilege Escalation T105: Defense Evasion T106: Credential Access T107: Discovery T108: Lateral Movement T109: Collection T110: Command and Control T111: Exfiltration T112: Impact	T101: Execution T102: Command and Control T103: Persistence T104: Privilege Escalation T105: Defense Evasion T106: Credential Access T107: Discovery T108: Lateral Movement T109: Collection T110: Command and Control T111: Exfiltration T112: Impact	T101: Execution T102: Command and Control T103: Persistence T104: Privilege Escalation T105: Defense Evasion T106: Credential Access T107: Discovery T108: Lateral Movement T109: Collection T110: Command and Control T111: Exfiltration T112: Impact	T101: Execution T102: Command and Control T103: Persistence T104: Privilege Escalation T105: Defense Evasion T106: Credential Access T107: Discovery T108: Lateral Movement T109: Collection T110: Command and Control T111: Exfiltration T112: Impact	T101: Execution T102: Command and Control T103: Persistence T104: Privilege Escalation T105: Defense Evasion T106: Credential Access T107: Discovery T108: Lateral Movement T109: Collection T110: Command and Control T111: Exfiltration T112: Impact	T101: Execution T102: Command and Control T103: Persistence T104: Privilege Escalation T105: Defense Evasion T106: Credential Access T107: Discovery T108: Lateral Movement T109: Collection T110: Command and Control T111: Exfiltration T112: Impact	T101: Execution T102: Command and Control T103: Persistence T104: Privilege Escalation T105: Defense Evasion T106: Credential Access T107: Discovery T108: Lateral Movement T109: Collection T110: Command and Control T111: Exfiltration T112: Impact

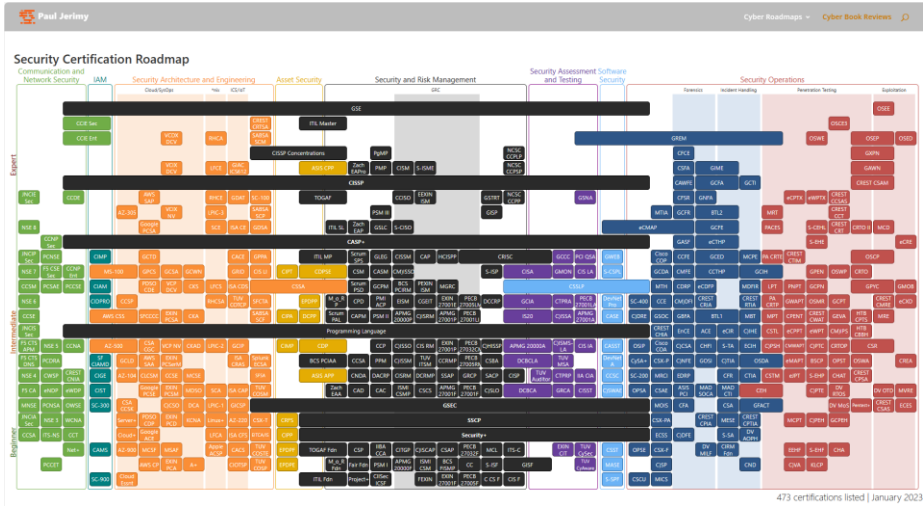
Legend of displayed Detection Capabilities:

- Green: Password Spray
- Blue: Consent Grant
- Yellow: Service Principals in Azure DevOps Pipelines
- Pink: Azure AD Connect Sync Service Account
- Orange: Replay of Primary Refresh (PRT) and other issued tokens
- Purple: Multiple Attack Scenarios on same TTP

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Source: [GitHub - Cloud-Architekt/AzureAD-Attack-Defense](#): This publication is a collection of various common attack scenarios on Azure Active Directory and how they can be mitigated or detected.

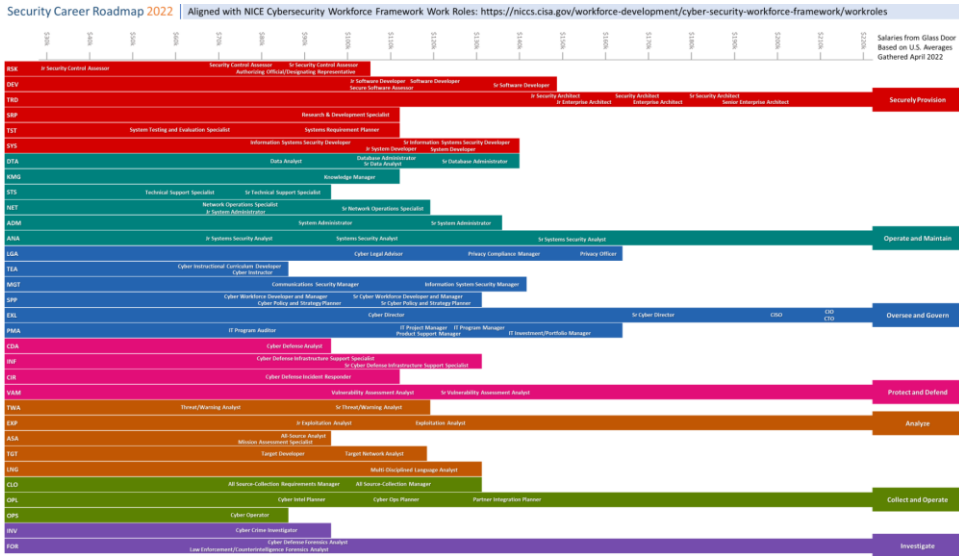
Certification & Knowledge Mapping



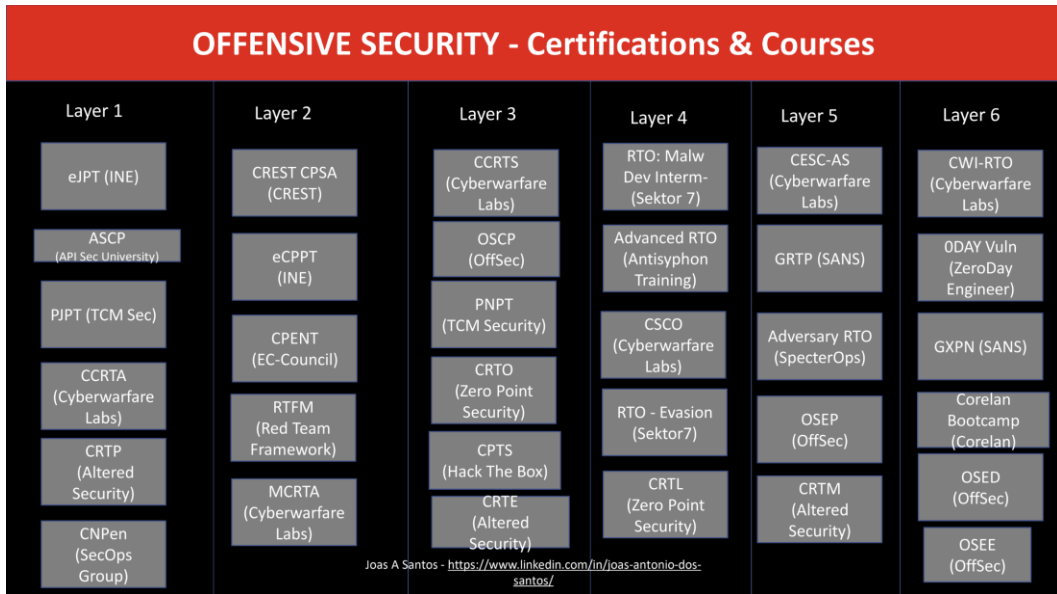
Source: [Security Certification Roadmap - Paul Jerimy Media](#)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Security Career Roadmap



Source: [IT Career Roadmap - Paul Jerimy Media](#)



Source: Brad Voris ([bvoris/CollectiveWorks: Complete written works by Brad Voris \(github.com\)](https://github.com/bvoris/CollectiveWorks))

The excel file can be found in the job aids named "Security_Analyst_Job_Research_Brad_Voris.xlsx". This excel file outlines the jobs, skills, educational, certification and experience in one worksheet. Use it for your understanding of each role which can be mapped to your future goal. Do look out for new versions in his Git.




CHAPTER

10

Incident Response

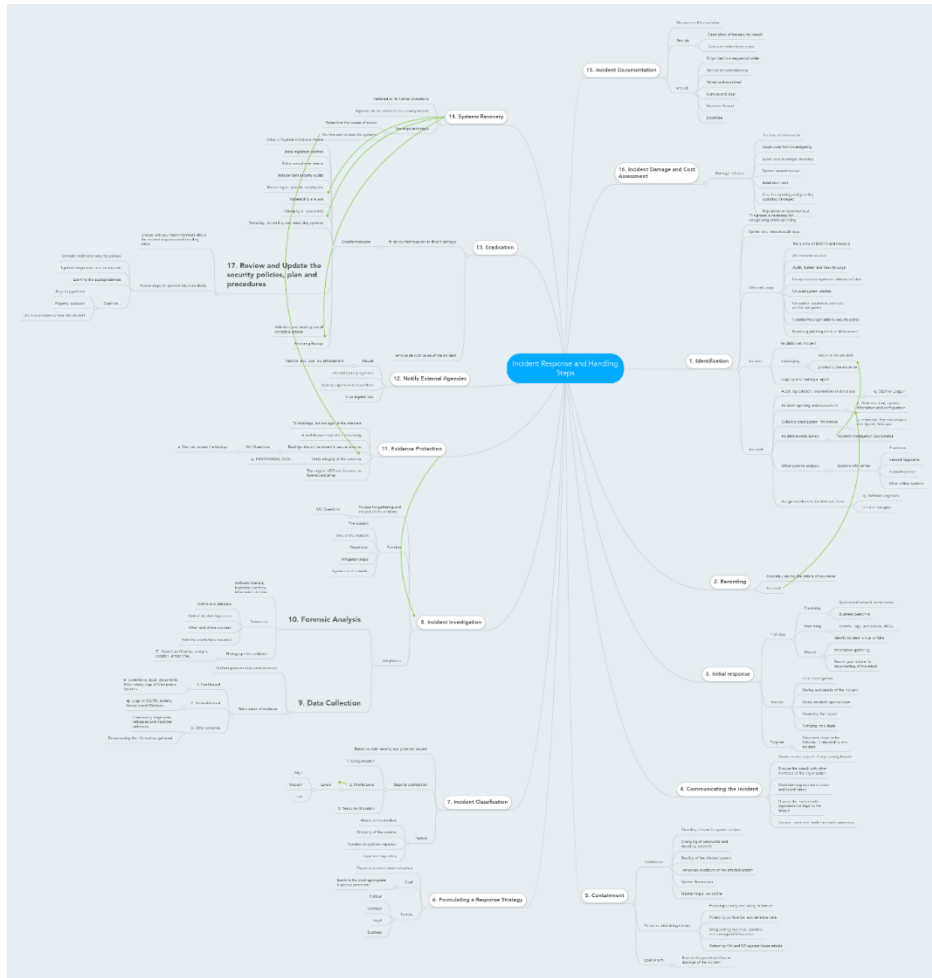
YOUR KNOWLEDGE MAPPING IS THE FIRST MILESTONE A SOC CAN HAVE WHO CAN DESCRIBE CLEARLY, WHAT'S HAPPENED, HOW THINGS GOT COMPROMISED AND WHAT ACTION HAS BEEN TAKEN FOR FUTURE? REMEMBER, SOC FORMS WITH YOU, NOT WITHOUT YOU. YOU ARE IMPORTANT! WITH YOUR MINDSET, KNOWLEDGE, DISCIPLINED AND PASSIONATE.



There are different frameworks and methodologies available in the web for incident response, but they generally share some common steps:

- **Preparation:** This step involves preparing the resources, tools, policies, and personnel needed to handle incidents effectively. It also includes training, awareness, and prevention measures to reduce the likelihood and impact of incidents.
- **Detection and Analysis:** This step involves identifying and verifying the occurrence, scope, and severity of an incident, as well as collecting and analyzing relevant data and evidence. It also includes reporting and escalating the incident to the appropriate stakeholders and authorities.
- **Containment, Eradication, and Recovery:** This step involves isolating and removing the threat from the affected systems and networks, as well as restoring normal operations and functionality. It also includes verifying the effectiveness of the containment and eradication measures and applying patches and updates to prevent recurrence.

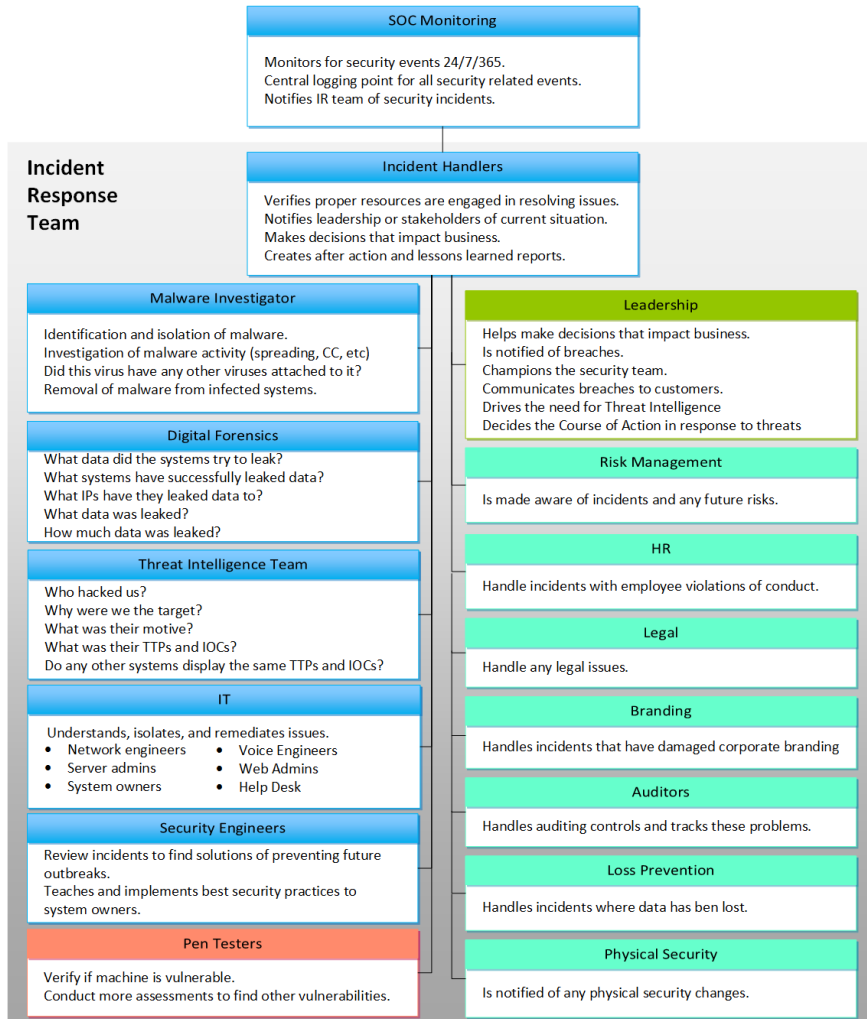
COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Source: [Incident Response and Handling Steps - MindMeister Mind Map](#)

- **Post-Incident Activity:** This step involves reviewing and evaluating the incident response process and outcomes, as well as identifying and implementing lessons learned and best practices. It also includes documenting and reporting the incident details, findings, and recommendations, as well as conducting audits and follow-ups to ensure compliance and improvement.

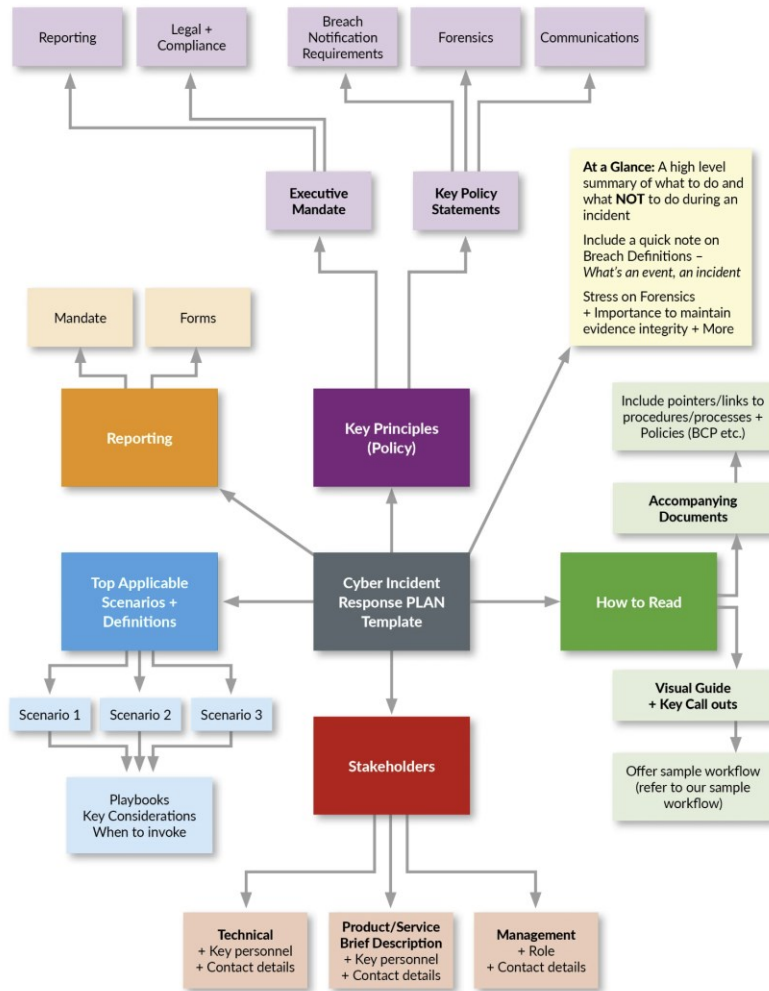
Incident Response Roles



Source: [Computer incident response team roles and responsibilities \(rolesresponsibility.netlify.app\)](https://www.netlify.com/blog/2016/07/27/computer-incident-response-team-roles-and-responsibilities/)

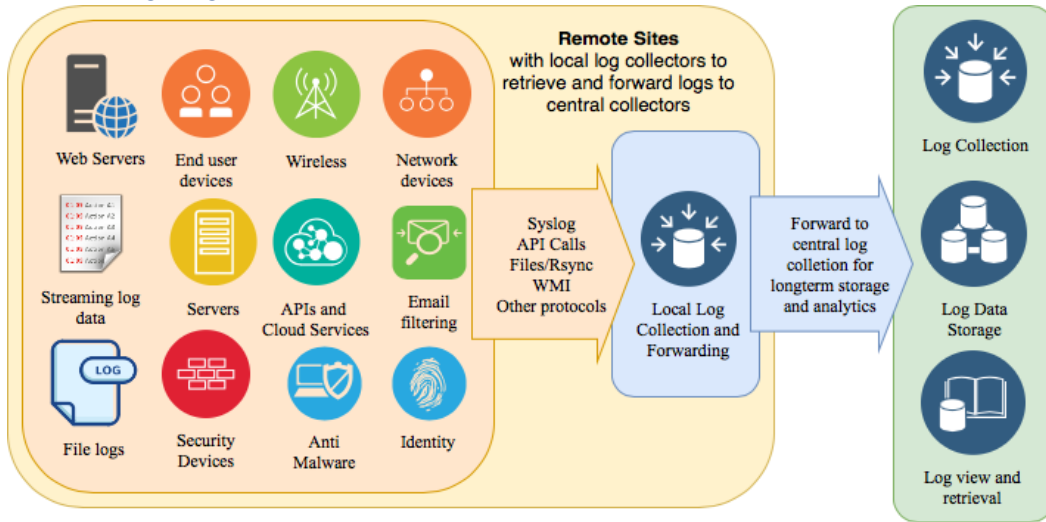
Generic Incident Response Playbook

Download the freely provided and a useful template from CM-Alliance: [Cybersecurity Incident Response Plan Template and Example UK - Cyber Management Alliance \(cm-alliance.com\)](https://www.cm-alliance.com)

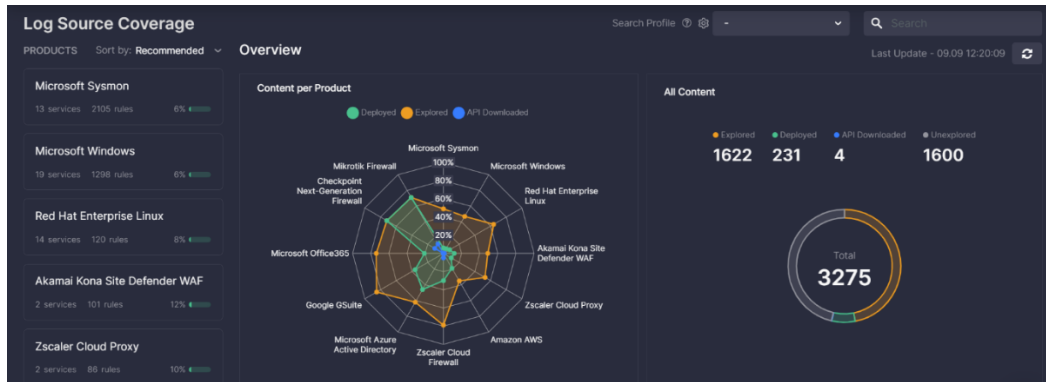


COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Prioritizing Log Sources




Source: [Security Operations Center \(SOC\): Prioritizing Log Sources Rafeeq Rehman | Cyber | Automation | Digital](#)



Source: [SOC Prime's Innovation for Collaborative Cyber Defense - SOC Prime](#)

There are several factors to consider when it comes to prioritizing log sources for a Security Information and Event Management (SIEM) system. One approach is to focus on logs coming from security devices such as firewalls, IDS, content filtering and proxy servers, identity management systems, proxies, VPN concentrators, end-point detection and response systems, etc. Another approach is to evaluate the relevance of each log source to your organization's security goals. Focus on log sources that provide



information about potential threats or vulnerabilities that align with your security goals. Consider legal and compliance requirements specific to your industry. For organizations with compliance requirements, compliance frameworks offer a good starting point. It is also important to consider the potential impact and severity of each log source. By prioritizing log sources based on their relevance and potential impact, organizations can allocate resources effectively and focus on the most important security risks.

Windows Event Logs Artifact

The artifact contains Event Logs in Windows operating systems. The details you can view include:

1. **Level** - Event log level/type. This can be information, warning, error, success/failure audit.
2. **Channel** - Event log channel or category. Security, Application, System etc.
3. **Computer** - Local system name.
4. **Event ID** - Event identification number. By filtering according to ID we can get the important events.
5. **Keywords** - They are used to group the event with other similar events based on the usage of the events.
6. **Opcode** - The activity or a point within an activity that the application was performing when it raised the event.
7. **Provider GUID** - The unique GUID for the provider. It is useful when performing research or operations on a specific provider.
8. **Provider Name** - Name of event provider.
9. **Security User ID** - It is used to uniquely identify a security principal or security group.
10. **Task** - Identifies the type of recorded event log. Application developers can define custom task categories for providing additional details.
11. **Event Record Order** - Order of the event in the main event category.
12. **Located At** - File offset location of the specific event.
13. **Event Record ID** - Event record identification number in the main category.
14. **XML** - XML view of the event,
15. **Record Length** - Length of the event.

Windows Reports – What to look for?

As a security-conscious administrator, you want to keep an eye on a number of events such as:

1. Successful or failed login attempts to the Windows network, domain controller or member servers.
2. Successful or failed attempts of remote desktop sessions.
3. Password lockouts after repeated login attempts.
4. Successful or failed login attempts outside business hours.
5. Adding, deleting, or modifying local or domain user accounts or groups.
6. Adding users to privileged local or active directory groups.
7. Clearing event logs in domain controllers or member servers.
8. Changing local audit policies and group policies.
9. Changing or disabling Windows firewall or firewall rules.
10. Adding new services, stopping or deleting existing services.
11. Changing registry settings.
12. Changing critical files or directories.

Common Windows Log Events Used in Security Investigations

Here are a few common event codes on Windows 7/Vista/8/10 and Windows Server 2008/2012R2/2016/2019 (previous versions of Windows have different codes), commonly used in security investigations:

Event ID	What it means
4624	Successful log on
4625	Failed log on
4634	Account log off
4648	Log on attempt with explicit credentials
4719	System audit policy change
4964	Special group assigned to new log on attempt
1102	Audit log cleared
4720	New user account created
4722	User account enabled
4723	Attempt to change password
4725	User account disabled
4728	User added to privileged global group
4732	User added to privileged local group
4756	User was added to privileged universal group
4738	Change to user account
4740	User locked out of an account
4767	User account unlocked
4735	Change to privileged local group
4737	Change to privileged global group
4755	Change to universal group

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

4772	Failed request for Kerberos ticket
4777	Domain controller failed to validate credentials
4782	Account password hash accessed
4616	System time changed
4657	Change to registry value
4697	Service install attempt
4946	Rule added to Windows Firewall exception
4947	Rule modified in Windows Firewall exception
4950	Windows Firewall settings change
4954	Change to Windows Firewall Group Policy
5025	Windows Firewall service stopped
5031	Application blocked by Windows Firewall from accepting traffic
5155	Windows Filtering Platform blocked a service from listening on a port

Source: [Event Log: Leveraging Events and Endpoint Logs for Security \(exabeam.com\)](#)

Furthermore, the following table contents also will be helpful for SOC feed for Network Traffic Analysis:

Log Item - What it is - Why it's Important		
Source IP Address	Where the traffic originates.	Tracking the source of attacks or suspicious activities.
Destination IP Address	Target of the traffic.	Determining potential internal targets and external threat sources.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Source Port	Port on the source IP initiating the connection.	Identifying specific applications or services being used.
Destination Port	Port being accessed on the destination IP.	Detecting unusual access patterns or services being targeted.
Timestamps	Exact time of events.	Correlating events across different systems for incident response.
Protocol (TCP/UDP/ICMP, etc.)	Communication protocol used.	Understanding the nature and purpose of the traffic.
Packet Size	Size of packets.	Indicating malicious activities through large or unusually sized packets.
TCP Flags (SYN, ACK, FIN, etc.)	State of TCP connections.	Identifying different stages of network communication and potential scanning activities.
DNS Queries and Responses	Domain name resolutions.	Detecting malicious domain communications.
HTTP Methods (GET, POST, etc.)	Types of HTTP requests.	Monitoring web applications and identifying potential web-based attacks.
URLs Accessed	The URLs requested.	Identifying access to malicious or



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



		inappropriate websites.
HTTP Status Codes (200, 404, 503, etc.)	Response status.	Spotting errors, server issues, or high rates of specific responses.
SSL/TLS Handshakes	Encrypted communication initiation.	Ensuring secure communications and detecting anomalies.
VPN Logins and Logouts	VPN access monitoring.	Ensuring only authorized remote access.
Email Logs (Sender, Receiver, Subject)	Email traffic monitoring.	Detecting phishing attempts and email based threats.
File Transfers (FTP/SFTP)	Tracking file uploads and downloads.	Preventing data loss and spotting unauthorized transfers.
Authentication Logs (Success/Failure)	Records login attempts.	Detecting brute-force attacks and unauthorized access.
IDS/IPS Alerts	Intrusion detection/prevention alerts.	Early detection of potential threats and intrusions.
Bandwidth Usage	Amount of data transferred.	Signaling data exfiltration or denial-of service attacks.
NetFlow Data	Information about network traffic flow.	Network behavior analysis and anomaly detection.



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Firewall Allow/Deny Logs	Allowed and blocked traffic records.	Security policy enforcement and detecting breaches.
DHCP Leases	IP address assignments.	Tracking devices and identifying rogue devices.
ARP Traffic	Address Resolution Protocol traffic.	Detecting ARP poisoning and MitM attacks.
Geolocation of IP Addresses	Geographical location of IP addresses.	Identifying traffic from unusual or high-risk locations.
Wi-Fi Connection Logs	Wireless network connections tracking.	Securing wireless networks and detecting unauthorized access.
ARP Requests and Responses	Monitors ARP protocol traffic.	Mapping network addresses and detecting spoofing.
SNMP Traps	Alerts from network devices.	Identifying events or issues on network devices.
SMTP Traffic	Monitors Simple Mail Transfer Protocol activities.	Tracking email delivery and detecting spam or malicious emails.
ICMP Traffic	Monitors Internet Control Message Protocol.	Error message analysis and operational network information.
SIP Traffic	Monitors Session Initiation Protocol in VoIP.	Managing VoIP communications and identifying potential abuses.
NTP Traffic	Monitors Network Time Protocol.	Ensuring time synchronization and detecting man-in-the-middle attacks.



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



DHCP	Monitors the DHCP process.	Tracking IP address allocation and identifying rogue DHCP servers.
Discover/Offer/Request/Acknowledge		
LDAP Queries	Monitors Lightweight Directory Access Protocol.	Accessing directory services and detecting unauthorized queries.
SQL Queries	Monitors Structured Query Language traffic.	Database interaction monitoring and detecting SQL injection attacks.
RADIUS Authentication Logs	Monitors RADIUS protocol.	Authentication and authorization process tracking.
Kerberos Authentication Attempts	Monitors Kerberos protocol.	Network authentication security analysis.
Syslog Messages	Collects and analyzes system logs.	Gathering crucial information from various network devices.
SSL Certificate Information	Monitors SSL certificates in communications.	Ensuring secure communications and detecting certificate issues.
IPv6 Traffic	Monitors IPv6 protocol traffic.	Future-proofing network monitoring as IPv6 adoption increases.
Traceroute Information	Monitors packet paths through a network.	Network path analysis and troubleshooting.
Wireshark Captures	Analyzes detailed packet captures.	In-depth network analysis and issue identification.
DDoS Attack Indicators	Monitors for signs of DDoS attacks.	Early detection and mitigation of DDoS attacks.



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Tor Traffic	Monitors Tor network usage.	Detecting anonymous communication potentially used for malicious activities.
Malware Callbacks	Monitors for compromised system communications.	Identifying systems communicating with command and control servers.
Zero-Day Attack Indicators	Monitors for unknown attack patterns.	Detecting new, potentially unpatched vulnerabilities.
Mobile Device Management (MDM) Logs	Monitors mobile device activities.	Managing and securing mobile device usage within the network.
Cloud Service Access Logs	Monitors access to cloud based services.	Securing cloud services and detecting unauthorized access.
VPN Tunnel Status	Monitors the status of VPN tunnels.	Ensuring the health and security of VPN connections.
VoIP Call Logs	Monitors Voice over IP call details.	Tracking VoIP communications for abuse or data leakage.
Data Leakage Indicators	Monitors for unauthorized data transmission.	Preventing sensitive data from leaving the network.

Source: LinkedIn Shares – Credit- Writer’s name was not found

Windows Events: Valuable, but Expensive

These are Windows event codes that can be prohibitively expensive to log, as they can generate hundreds of events in a short period of time. However they provide a great level of insight into an environment, so if disk space – or log ingestion into a SIEM – allows for these to be collected, I encourage them to be logged.

Event Code	Description	Why?
4657	A registry value was changed	A loud event code, this is still very valuable to detect suspicious registry value changes, as another common foothold for persistence is for attackers to alter or add a registry key. There





		are some key areas in the Windows registry that these footholds would be placed to be most effective – startup registry keys “run” and “run once” – so you can narrow your scope to just these registry paths if needed. See section below, “4657 Registry Keys to Monitor”
4688	New process was created	This will allow you to see any and all new processes that are run in the environment. If that sounds incredibly noisy, it is – however it provides an amazing insight into an endpoint. Additionally you can enable it to include process command line arguments, which allows for endpoint visibility not usually seen without a paid-for tool. If your disk space – or license if ingesting into a SIEM platform – allows for this event code with command line to be ingested, I do suggest it, however it is extremely loud.
4697	An attempt was made to install a service	This event code would be very loud to monitor across all areas, so we want to ensure it’s monitored on critical or otherwise sensitive systems. Service installations should be planned and there are services that attackers would want to install on a high value system. The service type field should be monitored to determine the access level of this new service, while the service start type field should be monitored for how the service is set to run.

Registry Keys to Monitor

Below are some very solid registry keys to monitor, all of which cover the persistence methods discussed above. Rather than log all registry changes, instead focus on these locations to best detect suspicious registry behavior. Credit goes to MITRE ATT&CK for these paths below – <https://attack.mitre.org/techniques/T1547/001/>

Run at startup keys:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

Startup folder items:



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

Automatic service startups:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices

Policy-driven startup programs:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

User Logon Program Launch – within “load” value:

- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Autocheck launch – within BootExecute value

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager
 - This last one is interesting as it's the path of the automatic disk checking service Microsoft employs upon abnormal shutdowns. Since it's an automatic function, attackers realized they can adjust this value to also add that same automatic run functionality to their program/process for persistence. It's pretty cool!

Source: [Windows Security Event Logs – What to Monitor? - Critical Start](#)

Which Are The Most Critical Linux Logs to Monitor?

- `/var/log/syslog` or `/var/log/messages` – stores all activity data across the Linux system.
- `/var/log/auth.log` or `/var/log/secure` – stores authentication logs
- `/var/log/boot.log` – messages logged during startup
- `/var/log/maillog` or `var/log/mail.log` – events related to email servers
- `/var/log/kern` – Kernel logs
- `/var/log/dmesg` – device driver logs
- `/var/log/faillog` – failed login attempts
- `/var/log/cron` – events related to cron jobs or the cron daemon
- `/var/log/yum.log` – events related to installation of yum packages
- `/var/log/httpd/` – HTTP errors and access logs containing all HTTP requests
- `/var/log/mysql.log` or `/var/log/mysql.log` – MySQL log files

Using Linux Event Logs for Security

The Linux operating system stores a timeline of events related to the server, kernel, and running applications. The main log categories are:

- Application logs
- Event logs
- Service logs
- System logs

There are several ways to view logs in Linux:

- Access the directory `cd/var/log`. Specific log types are stored in subfolders under the log folder, for example, `var/log/syslog`.
- Use the `dmseg` command to browse through all system logs
- Use the `tail` command, which displays the last lines written to a certain log file, where problems are usually found. For example `tail -f /var/log/syslog` prints the next line written to the file, letting you follow changes to the syslog file as they happen.

Following are commonly used Linux log files:



- **/var/log/syslog or /var/log/messages** – general system activity logs. Used to detect problems that may occur during startup or to isolate application service errors. RedHat-based systems store information in the messages folder while Debian-based systems store them in the syslog folder.
- **/var/log/auth.log or /var/log/secure** – all authentication and authorization logs. Used to investigate failed login attempts. RedHat-based systems store these in the auth.log folder while Debian-based systems store them in the secure folder.
- **/var/log/kern.log** – kernel activity logs, including custom kernels.
- **/var/log/faillog** – failed login attempts.
- **/var/log/maillog or var/log/mail.log** – logs related to mail servers. Used to track issues like emails tagged as spam, and suspicious use of postfix or smtpd.

Common Log Sources for Cloud Services

Cloud Threat Hunting					
Scenario	M365	Azure	AWS	GCP	GWS
Cloud ENUM	UAL	Activity Logs	CloudTrail	System Event Logs	Service Logs
Password Spray	UAL	Sign-in Logs	CloudTrail	Login Audit Logs	User Log Events
Storage Canaries	UAL	Storage Logs	CloudTrail	Storage Logs	Drive Log Events
Lateral Movement	UAL	Activity Logs	CloudTrail	System Event Logs	User Log Events
Exposed Keys	UAL	Activity Logs	CloudTrail	System Event Logs	OAuth Log Events

Elli Shlomo

Determine the Best Log Data Sources

Below picture lists some common data sources in a suggested order of priority, starting with identity and access management (IAM) logs and primary security controls, and then the other categories as your program matures:





Order	Data Source	Logs to Collect/Monitor
Tackle first	IAM	<ul style="list-style-type: none"> • Single sign-on (SSO) • Multifactor authentication (MFA) • Host-based collection (e.g., Windows servers)
	Security controls	<ul style="list-style-type: none"> • IDS • Endpoint security (anti-virus, anti-malware, etc.) • Data loss prevention (DLP) • Virtual private network (VPN) concentrators • Web filters • Honeypots • Firewalls
Tackle second	Network infrastructure	<ul style="list-style-type: none"> • Routers • Switches • Domain controllers • Wireless access points • Application servers • Databases • Intranet applications
Tackle third	Non-log infrastructure information	<ul style="list-style-type: none"> • Configuration • Locations • Owners • Network maps • Vulnerability reports • Software inventory
	Non-log business information	<ul style="list-style-type: none"> • Business process mappings • Points of contact • Partner information

Logs to Avoid

There are also categories of data you should not consider logging, such as:

- Data from test environments that are not an essential part of your software delivery pipeline (CI/CD). These data would confuse your SIEM, and will produce undesired results, culminating a huge number of incident record to pop-up, cleaning it up would increase the man-hour and Analyst burn-outs.
- Data that could adversely impact compliance. For example, data associated with users who enable do-not-track settings should not be logged. Similarly, try to avoid logging highly sensitive data, such as credit card numbers, unless you are certain your logging and storage processes meet the security requirements for that data (PCI-DSS).

Best Practices for MacOS Logging & Monitoring

Source: [SOC Logging and Monitoring Best Practices | IANS Research](#)

Organizations can pull the right logs to manage MacOS platforms in a variety of ways, including using endpoint detection and response (EDR) tools, integrating within Active Directory (AD) or leveraging a Mac management platform like Jamf. From there, it's a matter of specifying the logs you want and sending them to your SIEM. This piece details



the options and shows you how to build an optimal MacOS logging and monitoring capability.

Challenges of MacOS Logging

Local system logging in the MacOS world is a challenging endeavor due to a variety of reasons.

First, Microsoft is still the center of the enterprise computing landscape, and most organizations either don't allow Macs or turn a blind eye to their use.

Second, Apple has typically been consumer-focused, so in cases like this, its solutions don't quite fit the needs of the enterprise. That said, MacOS is an excellent operating system, and getting what you need is usually possible.

Choosing a MacOS Logging Method

A few years back, Apple rewrote the entire logging engine on its MacOS platform and retitled it unified logging. Unified logging normalizes the log engines across Apple's iOS and MacOS platforms. This caused changes to every aspect of logging, including creating logs, storing logs and using logs.

One key change is that Mac converted all its log storage to a format called `.tracev3`, which is a compressed binary format. This means you must use native tools to get the logs back out. Also, you can't write simple scripts to just copy certain log files off the underlying Unix file system.

There are a few different approaches to consider when trying to figure out how to get the appropriate logs to monitor:

EDR: The first, and perhaps easiest approach is to look at the capabilities of your EDR tools. Tools such as CylanceOPTICS and CrowdStrike have extensive cross-platform telemetry monitoring and logging capabilities that may be able to get most of this data quite easily. Those systems will often already be integrated with your SIEM solutions, easing the implementation burden.

AD: Another option is to explore integrating your Mac population into AD, so you can log any network logon events by default through the standard AD integration.

Mac management platforms: These provide another option for gathering and shipping log data from your fleet of systems. Jamf (aka Casper) is the de facto standard here, and it includes features similar to Microsoft System Center Configuration Manager (SCCM).

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Jamf offers an enterprise log management framework for shipping logs to your SIEM. You must define specific predicates (i.e., queries) to filter down the stream of events to ship. (Beware shipping all events, because there is an extraordinary amount of logs with no apparent value.)

Choose What to Monitor in MacOS

Once you've got a solution to actually get the logs out, try to identify the specific logs you care about seeing. Consider a dedicated work effort with your Mac management team to pinpoint exactly the logs to search for.

Specific logs can be loosely attributed to a few different key items (see Table 1).

Logging Topic	Mac Considerations
System integrity	Monitor for local user account creations through native logging, Filevault 2 failures.
Security state change	This depends on what is meant by state change, but it would ideally be monitored by EDR (ensuring no uninstalls of security tools, for example).
Logon	Do a native logs search for "AuthenticationAllowed" and "Success," or rely on an AD domain join (see Figure 1). As you can see, Mac now does not even record usernames to show who logged in. Instead it's redacted with <code>*private*</code>, unless you create a special profile to retrieve it.
Logoff	Do a native logs search for "point of no return" or rely on an AD domain join.
Registry	Mac doesn't use registry in the same way, but it has a distributed file format tied to each application called a .plist file. These are not centrally managed like the Windows registry. To monitor for change, you'll need to identify critical applications to monitor first.
Sensitive privilege use	Search for <code>process=sudo</code> to get user permission escalation events. You can also use "AuthenticationAllowed completed"
User account management	Look for password changes "PasswordChangeAllowed" and user account creations.

Figure 1: Native Log Search Results for "AuthenticationAllowed"

The screenshot shows a macOS Console window with a search filter applied: `eventMessage CONTAINS AuthenticationAllowed AND eventMessage CONTAINS Success`. The search results show three log entries, all with redacted usernames (`*private*`).

```
["show", "--predicate", "eventMessage CONTAINS \\(AuthenticationAllowed\\) AND eventMessage CONTAINS \\(Success\\)", "--style", "syslog", "--last", "1d"]
```

Timestamp	(process)[PID]	Message
2020-07-13 18:08:12.917851-0400	localhost opendirectoryd[156]: (AccountPolicy) [com.apple.AccountPolicy:Framework]	AuthenticationAllowed: Evaluation result for record *private*, record type *private*: Success
2020-07-13 18:08:47.627264-0400	localhost opendirectoryd[156]: (AccountPolicy) [com.apple.AccountPolicy:Framework]	AuthenticationAllowed: Evaluation result for record *private*, record type *private*: Success
2020-07-13 18:08:56.288897-0400	localhost opendirectoryd[156]: (AccountPolicy) [com.apple.AccountPolicy:Framework]	AuthenticationAllowed: Evaluation result for record *private*, record type *private*: Success

Source: IANS, 2020

Identifying the logs you want to track can be done with a log viewer like Consolation 3 (shown in Figure 1). Use its user interface (UI) to define search criteria and review and tune the results. Then, take the “predicate” generated at the bottom and use that in your log shipping solution to pluck those logs from the log stream and send them to your logging solution.

Logging Solution for MacOS

There is no dedicated, one-size-fits-all logging solution for MacOS that directly correlates to traditional Windows logging. To get a workable solution in place:

Be systematic: Apple has highly verbose logs, but they can be culled down through a dedicated process.

Realize you can’t set it and forget it: Apple’s logging standards should be considered subject to change as they don’t typically have the longevity of Windows logs. Expect logging standard to change and also anticipate maintenance with each OS upgrade.

Common Ports Monitored by The SOC Analysts

Port Number	Use	Cyber Risk
20, 21	FTP (File Transfer Protocol)	Unencrypted, susceptible to sniffing, spoofing, and brute force attacks.
22	SSH (Secure Shell)	Target for brute force attacks; vulnerable if weak credentials are used.
23	Telnet	Unencrypted, prone to eavesdropping, hijacking, and credential theft.
25	SMTP (Simple Mail Transfer Protocol)	Can be exploited for spamming and relay attacks.
53	DNS (Domain Name System)	Vulnerable to DNS spoofing and DDoS attacks.
80	HTTP (Hypertext Transfer Protocol)	Unencrypted, susceptible to interception and manipulation.
110	POP3 (Post Office Protocol version 3)	Unencrypted, vulnerable to eavesdropping if not secured.
119	NNTP (Network News Transfer Protocol)	Can be exploited in distributing malicious content.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

123	NTP (Network Time Protocol)	Can be misused for DDoS attacks.
137-139	NetBIOS	Vulnerable to unauthorized access and spreading malware.
143	IMAP (Internet Message Access Protocol)	Unencrypted, potential for credential theft.
161, 162	SNMP (Simple Network Management Protocol)	Vulnerable to unauthorized access and information disclosure.
443	HTTPS (HTTP Secure)	Can be targeted by SSL stripping or MiTM attacks, though less risky than HTTP.
445	SMB (Server Message Block)	Known for vulnerabilities like EternalBlue, used in ransomware attacks like WannaCry.
993	IMAPS (Internet Message Access Protocol over SSL)	While encrypted, it can be a vector for targeted attacks if credentials are compromised.
135	Microsoft RPC	Can be exploited for unauthorized remote procedure calls.
139	NetBIOS Session Service	Vulnerable to unauthorized access and attacks on Windows networks.
143	IMAP (Internet Message Access Protocol)	Susceptible to interception, especially if unencrypted.
389	LDAP (Lightweight Directory Access Protocol)	Can be exploited in injection attacks and unauthorized access.
443	HTTPS (Hypertext Transfer Protocol Secure)	Potential for SSL/TLS vulnerabilities, MiTM attacks.
445	Microsoft-DS (Active Directory, Windows shares)	Known for SMB vulnerabilities, like EternalBlue.
465	SMTPTS (Secure SMTP)	Can be targeted for spam and phishing attacks, even though encrypted.
587	SMTP with TLS/SSL	Secure, but can be targeted in mail-based attacks.
636	LDAPS (LDAP over SSL)	Encrypted, but vulnerable to specific SSL/TLS attacks.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

993	IMAPS (IMAP over SSL)	Encrypted, but susceptible to targeted email attacks.
995	POP3S (POP3 over SSL)	Encrypted, but vulnerable to targeted email attacks.
1723	PPTP (Point-to-Point Tunneling Protocol)	Known vulnerabilities in VPN connections.
3306	MySQL Database Service	Vulnerable to SQL injection and unauthorized access.
3389	RDP (Remote Desktop Protocol)	Target for brute force and credential stuffing attacks.
5900	VNC (Virtual Network Computing)	Vulnerable to eavesdropping and remote control if unsecured.
69	TFTP (Trivial File Transfer Protocol)	Unsecured, vulnerable to interception and unauthorized access.
88	Kerberos	Can be targeted for authentication attacks.
109	POP2 (Post Office Protocol version 2)	Unencrypted, susceptible to eavesdropping.
156	SQL Service	Vulnerable to SQL injection and unauthorized access.
194	IRC (Internet Relay Chat)	Can be used for communication in botnets, susceptible to eavesdropping.
220	IMAP3 (Internet Message Access Protocol version 3)	Prone to the same risks as IMAP.
389	LDAP (Lightweight Directory Access Protocol)	Susceptible to directory traversal and unauthorized access.
427	SLP (Service Location Protocol)	Vulnerable to spoofing and DoS attacks.
546, 547	DHCPv6 (Dynamic Host Configuration Protocol for IPv6)	Vulnerable to unauthorized DHCP servers and MITM attacks.
554	RTSP (Real Time Streaming Protocol)	Can be exploited in streaming and DoS attacks.
631	IPP (Internet Printing Protocol)	Vulnerable to interception and unauthorized printing/access.

989, 990	FTPS (FTP over SSL)	More secure than FTP, but still can be targeted for data interception.
1194	OpenVPN	Can be targeted in VPN bypass and DoS attacks.
1433, 1434	Microsoft SQL Server	Vulnerable to SQL injection and unauthorized access.
1701	L2TP (Layer 2 Tunneling Protocol)	Vulnerable in unencrypted implementations.
1812, 1813	RADIUS (Remote Authentication Dial-In User Service)	Vulnerable to credential theft and replay attacks.
2049	NFS (Network File System)	Vulnerable to unauthorized file access and interception.
2082, 2083	cPanel	Can be targeted for web hosting control panel attacks.
2483, 2484	Oracle Database	Vulnerable to SQL injection and unauthorized access.
5060, 5061	SIP (Session Initiation Protocol)	Vulnerable to VoIP spam, eavesdropping, and hijacking.

Common Tools Used by SOC

Security Operations Centers (SOCs) use a variety of tools to monitor, detect, and respond to security incidents. Here are some of the common tools used by SOC:


Most used tools:

- [100 Best Free Red Team Tools in 2023 - Cyber Security News](#)
- [A-poc/RedTeam-Tools: Tools and Techniques for Red Team / Penetration Testing \(github.com\)](#)
- [A-poc/BlueTeam-Tools: Tools and Techniques for Blue Team / Incident Response \(github.com\)](#)
- [bigb0sss/RedTeam-OffensiveSecurity: Tools & Interesting Things for RedTeam Ops \(github.com\)](#)

Best Linux Distros for Cybersecurity

1. **Kodachi:** Kodachi uses a customized Xfce desktop and aims to give users access to a wide variety of security and privacy tools.

2. **Qubes OS:** Qubes has established itself as arguably the most popular security-centric distro. It works on the principle of compartmentalization, isolating different tasks into separate virtual machines for enhanced security.
3. **ParrotOS:** Based on Debian, ParrotOS provides a cloud-friendly environment with online anonymity and an encrypted system. It's suitable for penetration testers and security enthusiasts.
4. **BlackArch:** Built on Arch Linux, BlackArch offers a repository containing thousands of security tools organized into various groups. It's specialized for penetration testing.
5. **Tails (The Amnesic Incognito Live System):** Tails is designed for privacy-conscious users. It routes internet traffic through the Tor network and leaves no trace on the host system.
6. **Kali Linux:** Kali Linux, formerly known as BackTrack, distribution of the Linux operating system was developed by Offensive Security and is derived from the Debian distribution of Linux.
7. **Node Zero:** NodeZero was built around the Ubuntu distribution of the original Linux software as a complete system designed with penetration testing in mind.
8. **CAINE Linux:** An Ubuntu-based variation of the Linux software, the Computer-Aided Investigative Environment (CAINE). CAINE was created as part of a project for digital forensics software, organizing cyber forensic tools with a user-friendly graphical interface
9. **BackBox:** BackBox is an Ubuntu based open-source Operating System that offers a penetration test and security assessment facility. This system also provides a network analysis toolkit for security in the IT environment.
10. **Fedora Security Lab:** Fedora Security environment enables you to work on security auditing, forensics, and hacking. It comes with a clean and fast desktop environment.
11. **Dracos Linux:** Dracos Linux is an open-source OS that is packed with a wide range of tools, like forensics, information gathering, malware analysis, and more.
12. **Samurai Web Testing Framework:** Samurai Web Testing Framework is a virtual machine that is supported on VMWare (cloud computing software) VirtualBox (virtualization product). This live Linux environment is configured to perform web pen-testing. It contains various tools for attacking websites.
13. **Network Security Toolkit (NST):** Network Security Toolkit (NST) is a Linux-based Live USB/DVD flash drive. It offers free and open-source network and computer security tools that can be used for hacking. This distribution is used by hackers to perform routine security and network traffic monitoring task.
14. **ArchStrike:** ArchStrike is an OS that can be used for security professionals and researchers. It follows Arch Linux OS standards to maintain packages properly. This environment can be used for pen testing and security layer.



Each distribution of the Linux operating software was developed by individuals or by a community who want to custom tailor it to what they feel is the best version for cybersecurity purposes. Each one will have different advantages and shortcomings. If you are unsure about which Linux distribution will best suit you, the best detail is that you can try them all out without a penalty since they are all open-source and will not cost you a dime. However, if reviews are any indication, Kali Linux appears to be the top contender. Choose the one that aligns best with your needs and expertise!





CHAPTER 11

SOC Reference Architecture

TRY TO GRAB THE KNOWLEDGE OF FINDING AND STUDYING REFERENCE ARCHITECTURES AS MUCH AS POSSIBLE, THE PROVIDED RA LINKS ARE GOOD FOR A FRESH START, BUT THAT'S NOT THE END, AS YOU WILL SEE DIFFERENT PERSPECTIVES ARE ADDED TO DIFFERENT ARCHITECTURE THAT CAN BE STANDALONE, CLUSTERED (OS OR SERVICES), WITH OR WITHOUT HA.

A well-structured SOC is crucial for effective cybersecurity management. Here are some insights:

1. **SOC Conceptual Architecture:**

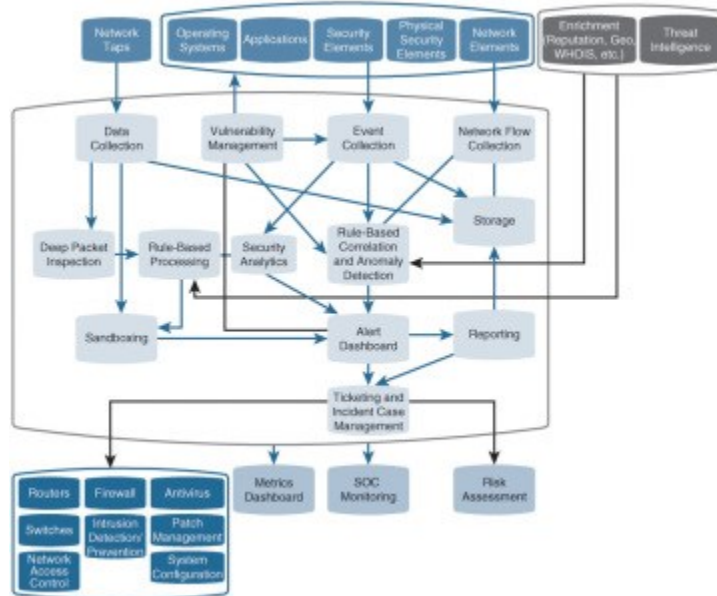
- To optimize your investment, it's essential to operate various SOC technologies within a cohesive architecture.
- The proposed reference conceptual architecture formalizes several key aspects:



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

- **Input Sources:** These are categorized data sources that feed information into the SOC.
- **Output:** The SOC generates alerts and takes necessary actions based on the analyzed data.
- **Technologies:** The suite of tools and technologies employed within the SOC.
- **Relationships:** How these technologies interact and collaborate.
- **Measurement Points:** Areas where data can be collected (e.g., type, value, frequency).

- Refer to below picture for an illustration of this conceptual architecture.



Source: [SOC Conceptual Architecture > Overview of Security Operations Center Technologies | Cisco Press](#)

2. Managed Threat Defense Services:

- Additionally, consider an alternative architecture where SOC responsibilities are outsourced to a managed service provider.
- Cisco's architecture for managed threat defense services caters to customers seeking to outsource some or all of their SOC functions. See the below picture:



Source: [SOC Conceptual Architecture > Overview of Security Operations Center Technologies | Cisco Press](#)

Microsoft Reference Architecture for Security Operations

Modern Security Operations (SecOps) reduces organizational risk from active attacks by rapidly detecting and remediating them

While a highly technical discipline, SecOps is first a human-centric function that empowers people with technology (rather than trying to replace people). Modern security operations technology helps extend **human** skills & expertise across today's 'hybrid of everything' technical environments to meet the threats posed by adaptable **human** attackers (who often use automated tools).

Because serious cyberattacks are often driven in near-real time by human attack operators, success metrics for security operations (SecOps / SOCs) should focus heavily on the **time** attackers have in the environment and helping defenders reduce attacker dwell time (measured in **Mean Time to Remediate or MTTR**). This reduces attacker ability to inflict damage on the organization.

Raw Data and Classic SecOps

Historically, security operations focused on collecting as much activity/event data from the environment as they could in a Security Incident & Event Management (SIEM). While collection is an important foundational step, this often led to a *'collection is not detection'* problem where very few actionable insights were actually gleaned from the data collected.

Queries authored by human analysts sometimes help detect anomalies that were malicious attacks, but these static queries often generated many false positive detections because of the continuously changing attacks, organizational assets, user behavior patterns, and data source scenarios. These false positives (false alarms) waste precious human analyst time and attention, taking them away from managing real attacks and increasing analyst fatigue/burnout.

Automation (SOAR) and Integration

Another key element for empowering security operations comes from the adoption of Security Orchestration, Automation, and Remediation (**SOAR**) technologies and **integration** of toolsets together (natively or by providing APIs).

SOAR/Automation and Integration:

- **Reduce manual work** for analysts and other roles with seamless experiences. Manual steps take time away from meaningful work and erode analyst morale, they would rather be fighting the bad guys than copy/pasting between tools and switching consoles
- **Speed Up** response time because the automation happens at machine speed rather than human speed.
- **Increase Scale** of security operations to meet the growing volume of attacks and increased scope/complexity of modern multi-cloud hybrid enterprises.

Microsoft focuses on automation and integration by

- **Embedding SOAR** technologies throughout our tools (AutoIR in Defender XDR, Azure Logic Apps in Microsoft Sentinel)
- **Single Microsoft 365 Defender console** to integrate experience for endpoint, email, SaaS
- **Natively integrating** Microsoft tools together (SIEM and XDR) to simplify SecOps workflows
- **Creating APIs** to connect with existing 3rd party tools

Microsoft Sentinel and SIEM Modernization

The need for SIEM technology has not gone away with the advent of XDR, but has shifted to the cases where it's needed most - creating custom detections (not duplicating XDR common detections) and analyzing multiple different data sources (including existing 3rd party security tools).

Microsoft Sentinel is a cloud-native SIEM that complements XDR tooling by providing analytics to create custom detections and hunt for threats across arbitrary log/data sources from any platform, cloud, application, or device.

Microsoft Sentinel alerts and workflows are integrated into Microsoft Defender XDR to streamline the analyst experience and minimize the need to change console/interfaces during time-sensitive incidents.

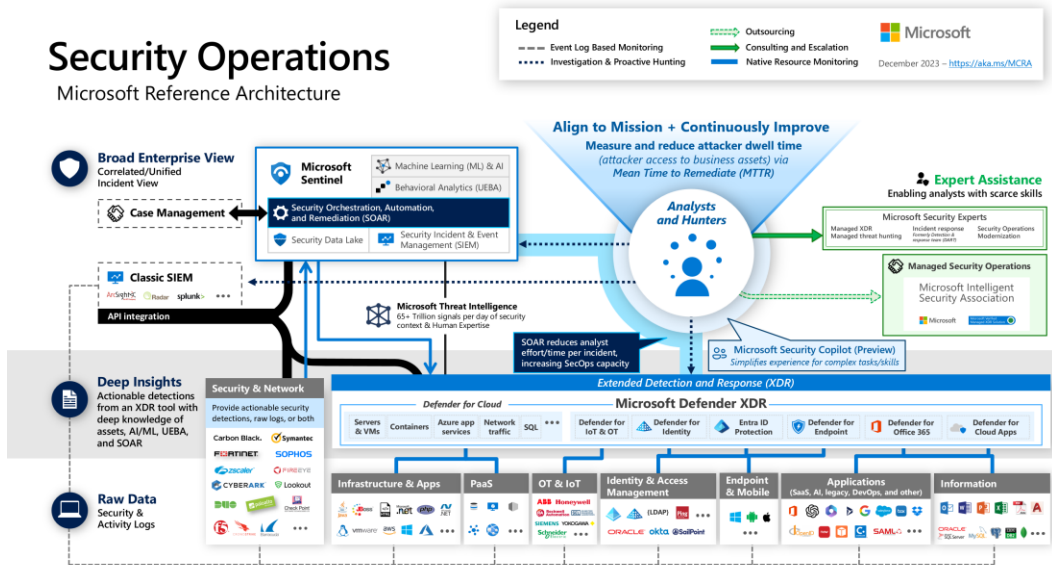
Notes:

- In addition to traditional SIEM functionality of static analysis of event logs, Microsoft Sentinel incorporates SOAR, ML, UEBA, Jupyter Notebooks, Threat Intelligence, and Security Data Lake approaches to refine threat detection, investigation, and threat hunting processes. Microsoft Sentinel also supports lower cost archival storage for large volumes of data.
- Microsoft Sentinel also offers many playbooks and other features to streamline investigation & remediation of critically important assets like SAP® applications and Operational Technology (OT) and Industrial internet of things (IIoT) [also known as Industrial Control Systems (ICS) / Supervisory Control and Data Acquisition (SCADA)].

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Security Operations

Microsoft Reference Architecture



Source: [Microsoft MCRA \(December 2023 Edition\)](https://aka.ms/MCRA)

1. **Security Information and Event Management (SIEM):** SIEM tools aggregate log data from various sources, examine it for possible attack patterns, and raise an alert if a threat is found.
2. **Log Collection and Management Tool:** These tools automate the process of log collection, parsing, and analysis.
3. **Vulnerability Management Tools:** These tools scan and monitor the organization's network periodically for any vulnerabilities.
4. **Endpoint Detection and Response (EDR):** EDR tools continuously monitor various endpoints, collect data from them, and analyze the information for any suspicious activities and attack patterns.
5. **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):** These systems monitor network traffic for suspicious activity and issue alerts when such activity is discovered.
6. **Firewalls and Next-Generation Firewalls (NGFW):** These tools monitor and control incoming and outgoing network traffic based on predetermined security rules.
7. **Governance, Risk, and Compliance (GRC) Systems:** These tools help organizations to strategically align IT with business objectives, while effectively managing risk and meeting compliance requirements.
8. **Investigation Tools:** These tools are used to investigate security incidents.

9. **Vulnerabilities Feeds and Databases:** These tools provide information about the latest vulnerabilities.

These tools help SOCs to protect the organization's information assets by providing real-time analysis of security alerts generated by applications and network hardware.

Demonstrating Privacy Accountability (NYMITY)

Source: [PMAF Poster - January 2017 \(vvena.nl\)](#)

Providing complete overview of the framework, delving deeper into the 13 core Privacy Management Activities (PMAs) may be helpful to you:

1. Governance:

- Establish a privacy steering committee.
- Appoint a data protection officer (DPO).
- Develop and implement a privacy policy.
- Conduct regular privacy risk assessments.
- Train employees on privacy policies and procedures.

2. Risk Management:

- Identify and assess privacy risks for all data processing activities.
- Implement appropriate controls to mitigate identified risks.
- Conduct regular reviews of data security measures.
- Respond to and report data breaches promptly.

3. Data Mapping:

- Create a complete inventory of all personal data collected, stored, and processed.
- Map data flows to understand how personal data moves throughout the organization.
- Implement data classification procedures to identify sensitive information.

4. Data Subject Rights:

- Establish clear processes for individuals to exercise their data subject rights, such as access, rectification, and erasure.
- Provide easily accessible information on how individuals can contact the organization regarding their data rights.
- Train employees on handling data subject rights requests.

5. Third-Party Risk Management:

- Conduct due diligence on third-party vendors that handle personal data.
- Implement contractual clauses to ensure third-party compliance with data privacy regulations.
- Monitor third-party data security practices and conduct audits as needed.

6. Data Security:

- Implement appropriate technical and organizational security measures to protect personal data.
- Conduct regular penetration testing and vulnerability assessments.
- Encrypt sensitive data at rest and in transit.

7. Incident Response:

- Develop and document an incident response plan for data breaches and other privacy incidents.
- Train employees on identifying and reporting privacy incidents.
- Conduct regular incident response drills and exercises.

8. Privacy Impact Assessments:

- Conduct PIAs for any new projects or technologies that involve personal data.
- Identify and mitigate potential privacy risks associated with the project or technology.
- Document the PIA findings and incorporate them into the project design.

9. Training and Awareness:

- Provide regular training for all employees on data privacy policies, procedures, and regulations.
- Conduct targeted training for employees with access to sensitive data.

- Raise awareness of data privacy throughout the organization.

10. Transparency and Reporting:

- Publish a clear and accessible privacy policy on the organization's website.
- Disclose personal data breaches and other privacy incidents promptly.
- Prepare and submit data protection reports as required by applicable regulations.

11. Cross-Border Data Flows:

- Implement appropriate safeguards for transferring personal data outside the organization's jurisdiction.
- Conduct risk assessments and comply with relevant data transfer mechanisms.
- Train employees on cross-border data transfer procedures.

12. Privacy by Design:

- Integrate privacy considerations into the design of new products, services, and processes.
- Minimize data collection and retention.
- Implement data-minimization principles throughout the data lifecycle.

13. Data Retention and Disposal:

- Define and document data retention periods for different types of personal data.
- Implement secure disposal procedures for data that is no longer needed.
- Train employees on proper data retention and disposal practices.

Please note that this is a high-level overview of the 13 core PMAs within the Nymity PAMF. Each PMA can be further broken down into even more specific tasks and actions, providing organizations with a detailed roadmap for implementing a comprehensive data privacy program.

Penetration Testing ROI Template by risk3sixty

Penetration Testing ROI Template by risk3sixty

Testing Scope		Estimated Costs		Estimated Benefits		
Description	Count	Cost Type	Amount	Benefit Type	Value	Notes
Systems	240	Penetration Test	\$ 50,000	Reduction in Breach Cost Exposure	\$ 229,600	28% reduction in exposure
Web Applications	2	Cost Per Record Breached	\$ 364	Revenue Generation	\$ 100,000	2% of revenue
Cloud Instances	1	Average Loss Expectancy (ALE)	\$ 820,000	Increased Valuation	\$ 240,000	1% of current valuation
Networks	10			TOTAL:	\$ 569,600	
PII Data Records	10,000					
Current Annual Revenue	\$ 5,000,000					
Current Valuation	\$ 24,000,000					
Number of Expected Breaches Per Year	1					
ROI	10.39	<- \$10.39 return for every dollar spent on penetration testing				
Payback Period	0.09	<- Expressed in years				
Cost-benefit Ratio	11.39	<- \$11.39 benefit for every dollar spent on penetration testing				

NOTES:

1. Enter values in YELLOW cells.
2. Do not modify gray or blue cells.
3. This calculator only assumes the cost of a breach related to PII records. It does not include calculations for ransomware payments, loss of intellectual property, or other financial impacts. To calculate with additional impacts, recalculate your ALE and update that field.

ASSUMPTIONS:

1. Standard data used in calculations can be found in the 2022 IBM Security and Ponemon Institute Cost of a Data Breach Report
2. Reduction in Breach Cost Exposure = ((PII data records) * .5) * \$164 * (Number of Expected Incidents Per Year) * .28 | Assumes 50% of records breached
3. Additional Revenue Generation is an estimate based on industry data
4. Increased valuation is an estimate based on industry data
5. ROI = (Monetary Value of Benefits - Cost of Penetration Testing) / Cost of Penetration Testing
6. Payback Period = Cost of Penetration Testing / Estimated Annual Monetary Value of Benefits
7. Cost-Benefit Ratio = Estimated Monetary Value of Benefits / Cost of Penetration Testing
8. ALE = (Number of incidents per Year) X (Potential Loss per Incident)

Source: [Penetration Testing ROI Calculator - risk3sixty](#)

Automated Penetration Testing

There are number of platforms that has their own developed platforms which has automated testing services both for your on-premise and cloud platforms. It's important to note that while automated tools can speed up the testing process and provide valuable insights, they should be complemented with manual testing and a comprehensive security program to ensure a thorough evaluation of the overall security posture.

Automated penetration testing can help organizations identify and address security weaknesses before malicious actors can exploit them. Here are some key aspects of automated penetration testing:

1. Tools and Frameworks:

- **Open Source Tools:** Tools like Metasploit, OWASP ZAP, Nikto, and Nmap are commonly used in automated penetration testing. These tools provide a wide range of functionalities for vulnerability scanning, exploitation, and post-exploitation activities.
- **Commercial Solutions:** There are also commercial penetration testing tools and platforms available, such as Rapid7's Nexpose, Qualys, and Burp Suite, Evolve:PT Professional. These tools often provide additional features and support, which can be proven very useful.

2. Vulnerability Scanning:

- Automated penetration testing tools typically start with vulnerability scanning to identify potential weaknesses in a system. This involves scanning the target for known vulnerabilities in software, configurations, or network infrastructure.

3. Exploitation:

- Once vulnerabilities are identified, automated tools may attempt to exploit them to gain unauthorized access or escalate privileges. This step helps assess the severity and impact of the vulnerabilities.

4. Post-Exploitation:

- Some automated penetration testing tools include post-exploitation modules to simulate what an attacker could do after gaining access. This may involve extracting sensitive information, lateral movement within the network, or establishing persistence.

5. Reporting:


- After the automated penetration testing is complete, a detailed report is generated. This report includes information about the vulnerabilities discovered, their severity, and recommendations for remediation. The report is crucial for organizations to understand their security posture and prioritize remediation efforts.

Pro-Tip

- These reports can be compared with other known frameworks (NIST, CIS, 27001 etc.) and how it affects the organizational structure as well.

6. Continuous Testing:

- Automated penetration testing can be integrated into a continuous testing and deployment pipeline. This allows organizations to identify and address security issues early in the development process, reducing the overall risk.



Pro-Tip

- As the devices firmware's, application patches take place, which also calls for VA/PT over and over again.

7. Challenges:

- While automated penetration testing is a valuable tool, it has limitations. It may not identify certain complex vulnerabilities that require manual testing or advanced understanding of the application's logic. False positives and negatives are also potential challenges that need to be considered.

8. Compliance:

- Automated penetration testing is often used to meet compliance requirements in various industries. Organizations may be required to conduct regular penetration tests to demonstrate the security of their existing systems.

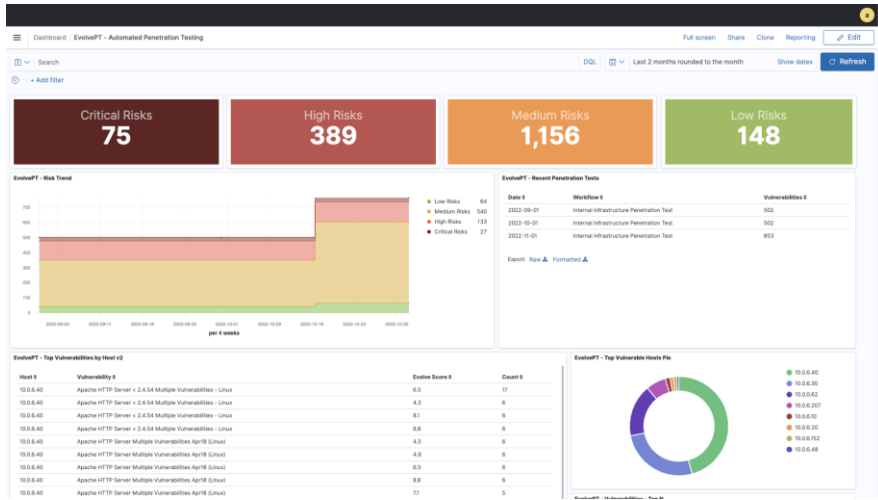


Pro-Tip

- Personally, I would go for engaging a human being in manual testing for specific testing on a specific target and would try to receive valuable insights, that didn't get identified in the automated scenario.

Though at times it could be costly, but on a holistic view and with a shorter amount of time, this option could really come in handy. One of the Automated-PT service providers I have seen is from EVOLVE-PT with insights (in your case things may not be the same as it depends on the complexity of your network infrastructure, integrations of various components and their provided visibility will affect the outcome of the below picture):

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Source: [EvolvePT - The Most Comprehensive Penetration Testing Tool \(threatintelligence.com\)](https://threatintelligence.com)



CHAPTER

12

Frameworks Used by SOC

DIFFERENT FRAMEWORKS ARE APPLIED TO THE SOC INFRASTRUCTURE, REASON WHY ITS IMPERATIVE THAT YOU SHOULD HAVE GOOD KNOWLEDGE ON THE REFERENCE ARCHITECTURES, SERVICES INTEGRATED, MAPPED TO DIFFERENT VISIBILITY REQUIREMENTS, PLAYBOOKS AND DIFFERENT TYPES OF OPERATIONAL ACTIVITIES.

Security Operations Centers (SOCs) use various frameworks to standardize their defense strategies, manage cybersecurity risks, and improve operations. Here are some of the common frameworks used by SOC (Major & high level shown only):



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER




Source: [Cyber Kill Chain® | Lockheed Martin](#)

The Cyber Kill Chain is a concept developed by Lockheed Martin to describe the various stages of a cyber-attack, from initial reconnaissance to achieving the attacker's objectives. Understanding and utilizing the Cyber Kill Chain is crucial in the field of cybersecurity for several reasons:

Early Detection and Prevention: The Cyber Kill Chain allows organizations to detect and prevent cyber-attacks at an early stage. By breaking down the attack lifecycle into stages, security teams can identify indicators of compromise, recognize patterns, and intervene before an attack progresses.





Attack Visualization and Understanding: It provides a visual representation of the different stages an attacker goes through, helping security professionals understand the attack process. This visualization aids in creating effective defense strategies and responses tailored to each stage.

Risk Mitigation: Understanding the Cyber Kill Chain enables organizations to implement targeted security measures at each stage, mitigating risks effectively. By focusing on vulnerable points in the chain, security controls can be optimized to disrupt the attack before it reaches its final objective.

Incident Response Planning: The Cyber Kill Chain is a valuable tool in incident response planning. It allows organizations to create and refine incident response plans based on a clear understanding of the stages an attacker must go through. This proactive approach improves the organization's resilience against potential threats.

Threat Intelligence Integration: The Kill Chain framework integrates well with threat intelligence. Security teams can map threat intelligence data to specific stages of the Kill Chain, providing context and relevance to potential threats. This integration enhances the organization's ability to respond to real-world, targeted attacks.

Continuous Improvement: By analyzing successful and attempted attacks through the lens of the Kill Chain, organizations can continuously improve their cybersecurity strategies. Lessons learned from previous incidents can be used to enhance security controls, update policies, and adapt defenses to evolving threats.

Efficient Resource Allocation: The Kill Chain helps organizations allocate resources more efficiently by identifying critical stages in the attack lifecycle. This strategic allocation ensures that security measures are concentrated where they are most needed, optimizing the use of resources.

Communication and Collaboration: The Cyber Kill Chain provides a common language for cybersecurity professionals. It facilitates better communication and collaboration within security teams and between different organizations. This shared understanding is essential in addressing and mitigating threats collectively.

Advanced Threat Detection: The Kill Chain enables the development and deployment of advanced threat detection mechanisms. By understanding the tactics, techniques, and procedures (TTPs) employed by attackers at each stage, organizations can design and implement more sophisticated detection and monitoring systems.

Adapting to Evolving Threats: The Kill Chain framework is dynamic and adaptable. As cyber threats evolve, security professionals can update and refine their defense

strategies based on the changing tactics of attackers. This adaptability ensures that cybersecurity measures remain effective over time.

The Famous Non-Controlling Body - NIST

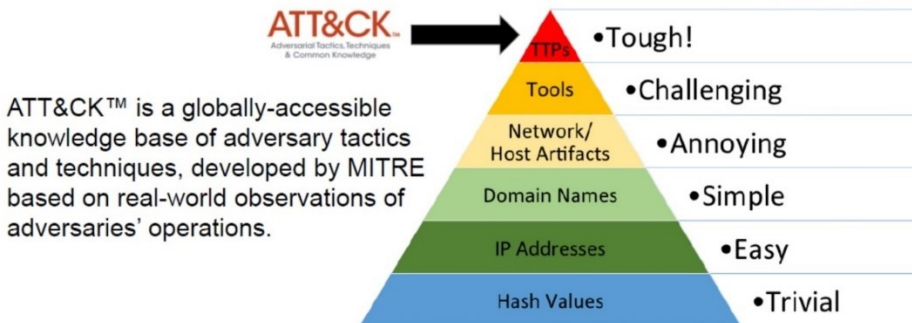
- NIST Cybersecurity Framework (CSF):** The NIST CSF includes threat lifecycle management standards, best practices, and guidelines. It helps organizations protect critical infrastructure by increasing security in various ways. The five core functions of the NIST CSF are (in short IPDRR, now "G" is added for Governance):
 - **Identify:** Learn how to better manage cybersecurity risks to various components like assets, systems, and data.
 - **Protect:** Implement safeguards to protect critical infrastructure services.
 - **Detect:** Define what constitutes a cybersecurity event.
 - **Respond:** Specify actions performed in response to a detected cybersecurity event.
 - **Recover:** Identify services to focus on for resilience, and outline the required restore capabilities of impaired services.
- MITRE ATT&CK Framework:** The MITRE ATT&CK framework provides observable adversarial behaviors to help intelligently identify tactics occurring after an attack has started. It helps inform threat intelligence, threat detection, and analysis, red teaming and adversary emulation, as well as engineering and assessment. ([Matrix - Enterprise | MITRE ATT&CK®](#))

© 2019 SPLUNK INC.

MITRE ATT&CK

Overview on Attacker Techniques and Attack Phases

attack.mitre.org



ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques, developed by MITRE based on real-world observations of adversaries' operations.

Source: David Bianco
<https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>
TTPs = Tactics, Techniques, and Procedures

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

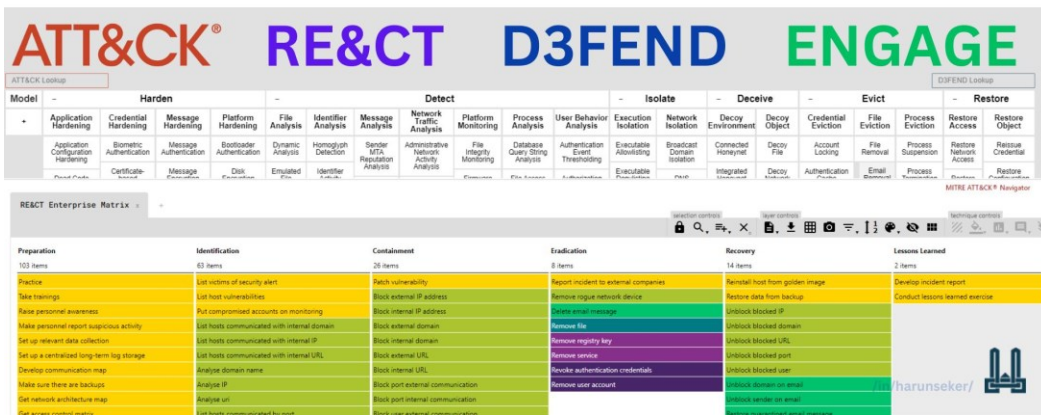
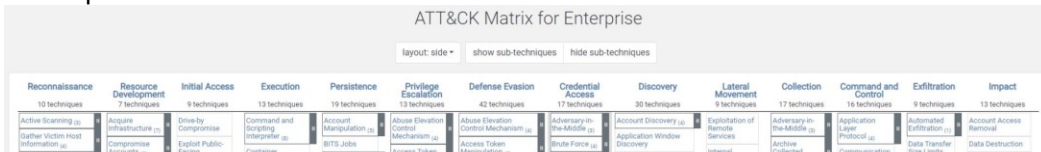
Source: [Q&A Follow-Up: So nutzt Datev MITRE ATT&CK & Splunk im SOC | Splunk](#)


3. **Cyber Kill Chain Framework:** This framework is used to understand and prevent intrusions into the network.
4. **Unified Kill Chain Framework:** This framework is an extension of the Cyber Kill Chain and is used to analyze threats from all vectors.
5. **ISO 27XXX series:** these series are prepared for certification and covers some areas of working domains. The problem with these series are, they overlap, and require multiple certifications to achieve domain coverage on information security, cybersecurity and for privacy protection.

MITRE has developed several frameworks to help organizations defend against cyber attacks:

MITRE ATT&CK framework is to help organizations and security professionals improve their cyber defense by identifying and understanding the methods and techniques used by attackers. It is used to identify and categorize tactics, techniques, and procedures (TTPs) used by cyber attackers to compromise systems.

MITRE D3FEND framework is a knowledge base, but more specifically a knowledge graph, of cybersecurity countermeasure techniques. In the simplest sense, it is a catalog of defensive cybersecurity techniques and their relationships to offensive/adversary techniques.





MITRE RE&CT Framework is designed for accumulating, describing and categorizing actionable Incident Response techniques. RE&CT's philosophy is based on the MITRE's ATT&CK framework, which comes with a navigator too.

MITRE Engage combines several active defense types, including basic cyber defensive actions alongside adversary engagement and cyber deception operations. Together, these defenses enable organizations to counter attacks while also obtaining additional information about the adversary.

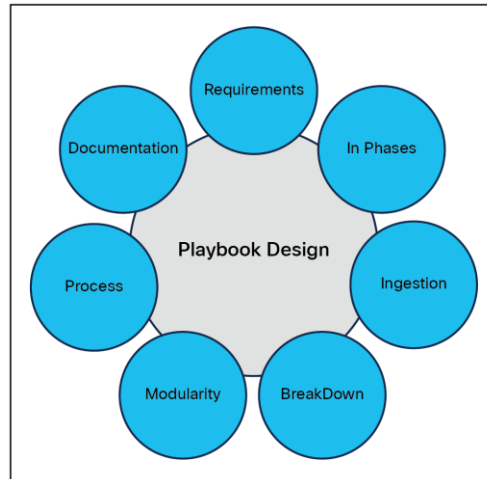
ATT&CK Framework and Navigator : <http://attack.mitre.org/>
D3FEND Framework and Navigator : <https://d3fend.mitre.org/>
RE&CT Framework : <https://lnkd.in/edCj2qh7>
RE&CT Navigator: <https://lnkd.in/ekYsfV-c>
ENGAGE Navigator: <https://lnkd.in/ev4S3vdb>

A plethora of certifications on information security, cybersecurity and for privacy protection @iso.org: [ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection](https://www.iso.org/standard/62454.html)

These frameworks help SOCs to protect the organization's information assets by providing real-time analysis of security alerts generated by applications and network hardware.

Building an Effective Security Operations Center (SOC) Playbook

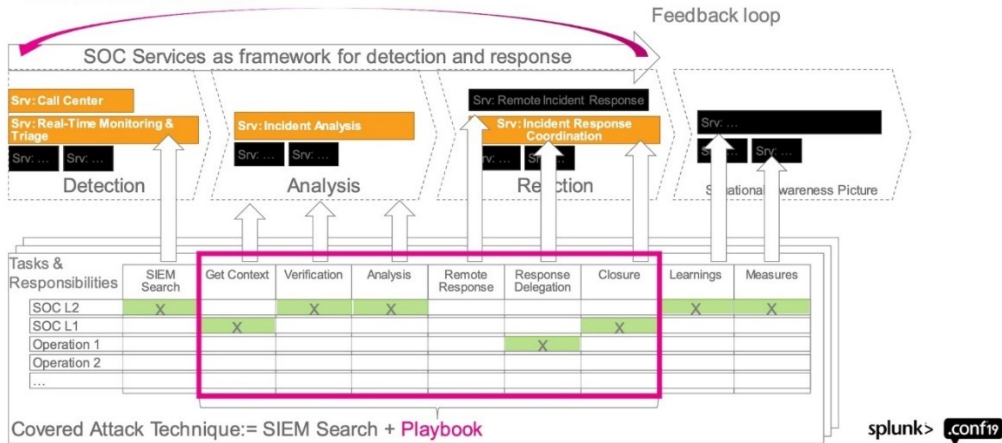
Developing a playbook involves several steps:



1. **Understand your Environment:** Get a clear picture of your IT infrastructure, including the IP addresses, endpoints, firewalls, and other elements.
2. **Identify Threat Vectors:** Understand the common cyber threats that your organization is likely to face. This could include phishing emails, ransomware attacks, and more.
3. **Define Roles and Responsibilities:** Clearly outline who is responsible for what during an incident response process. This includes the security team, response teams, stakeholders, and others involved.
4. **Outline the Procedures:** Provide step-by-step procedures for different incidents. This should include everything from identification, triage, escalation, remediation, and follow-up steps.
5. **Integrate Tools:** Mention the tools that will be used during the incident response process such as SIEM, EDR, sandbox, etc.
6. **Test the Playbook:** Once the playbook is created, it needs to be tested and refined based on the results. Some good playbook links are shared in the reference section.

SOC-Services, Playbooks, Responsibilities

Who does when what?



Source: [soc services playbooks & responsibilities in splunk - Search Images \(bing.com\)](https://www.splunk.com/en_us/blog/2018/05/soc-services-playbooks-responsibilities.html)

SOC Services, Playbooks and Responsibilities

The SOC provides various services, utilizes playbooks, and assigns specific responsibilities to ensure effective cybersecurity operations. Here's an overview of SOC services, playbooks, and responsibilities:

Services:

- **Continuous Monitoring:**
 - **Service Description:** The SOC continuously monitors the organization's networks, systems, applications, and data for any signs of security incidents or anomalies.
 - **Objective:** Early detection of potential threats and vulnerabilities to minimize the impact of Security incidents.
- **Incident Detection and Analysis:**
 - **Service Description:** Rapid detection and analysis of security incidents, including suspicious activities, anomalies, and potential breaches.
 - **Objective:** Identify and understand the nature and scope of security incidents.
- **Incident Response:**

- Service Description: Immediate response to confirmed security incidents, including containment, eradication, and recovery efforts.
- Objective: Minimize the impact of security incidents and restore normal operations swiftly.
- Threat Intelligence Integration:
 - Service Description: Integration of threat intelligence feeds to enhance the SOC's understanding of current and emerging threats.
 - Objective: Stay informed about the threat landscape to proactively defend against potential attacks.
- Vulnerability Management:
 - Service Description: Identification, assessment, and management of vulnerabilities in the organization's infrastructure.
 - Objective: Mitigate vulnerabilities before they can be exploited by attackers.
- Log Management and Analysis:
 - Service Description: Collection, storage, and analysis of logs and events from various sources to identify security incidents.
 - Objective: Detect anomalous activities and track potential indicators of compromise.
- Security Awareness and Training:
 - Service Description: Providing security awareness training for employees to recognize and report potential security threats.
 - Objective: Create a security-aware culture within the organization to reduce the likelihood of human error leading to security incidents.

Playbooks:

- Incident Detection and Response Playbook:
 - Description: Step-by-step procedures for detecting, analyzing, and responding to security incidents.
 - Use Case: Provides a structured approach for SOC analysts to follow when responding to alerts or incidents.
- Phishing Response Playbook:
 - Description: Guidelines for identifying, analyzing, and responding to phishing attacks.
 - Use Case: Helps SOC analysts and incident responders effectively handle phishing incidents, protecting against social engineering threats.
- Malware Analysis Playbook:

- Description: Procedures for analyzing and responding to malware incidents.
- Use Case: Enables the SOC team to identify the type and impact of malware and initiate appropriate response measures.
- Data Breach Response Playbook:
 - Description: Outlines steps to follow when responding to a data breach, including legal, communication, and technical aspects.
 - Use Case: Ensures a coordinated and effective response to data breaches, minimizing reputational damage.
- Patch Management Playbook:
 - Description: Procedures for managing and applying patches to address vulnerabilities.
 - Use Case: Ensures a systematic approach to patching to mitigate potential security risks.

Responsibilities:

- SOC Analysts:
 - Responsibilities: Monitor alerts, investigate incidents, and execute response procedures based on playbooks.
- Incident Responders:
 - Responsibilities: Lead the response to confirmed security incidents, coordinate containment and recovery efforts, and collaborate with relevant stakeholders.
- Threat Intelligence Analysts:
 - Responsibilities: Analyze threat intelligence, identify potential threats, and provide actionable insights to enhance security measures.
- Security Engineers:
 - Responsibilities: Implement and maintain security technologies, conduct vulnerability assessments, and contribute to the development of playbooks.
- Security Awareness Trainers:
 - Responsibilities: Develop and deliver security awareness training programs to educate employees on security best practices.
- SOC Manager:
 - Responsibilities: Oversee SOC operations, set strategic goals, collaborate with leadership, and ensure the SOC's effectiveness in addressing security threats.
- Security Operations Director:

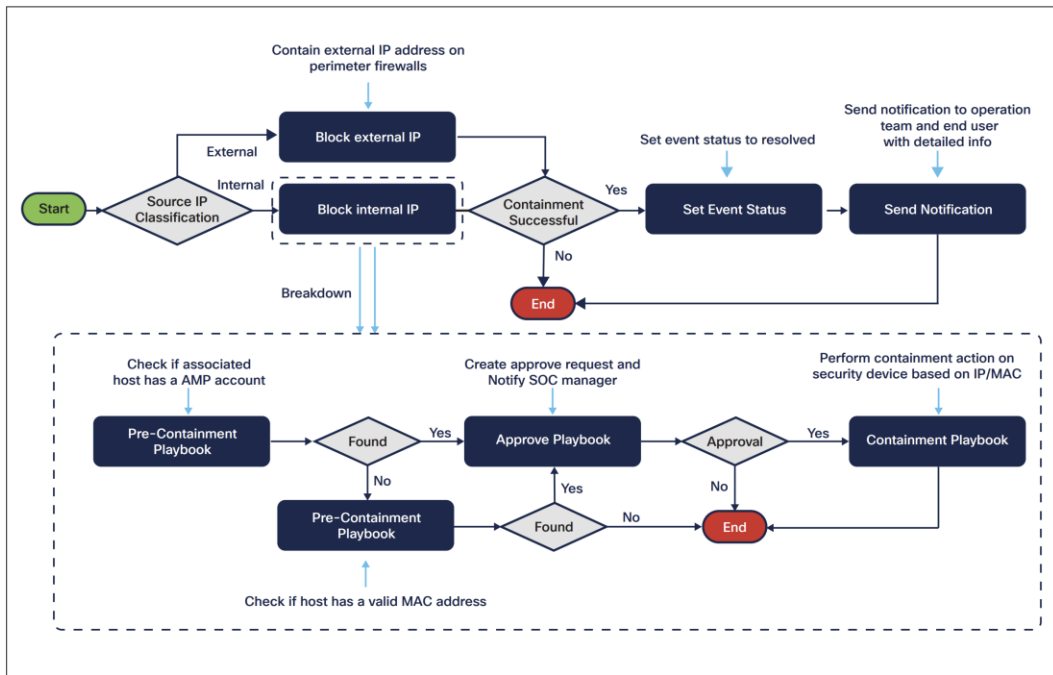
COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

- Responsibilities: Provide leadership and strategic direction for the overall security operations, aligning with organizational goals and objectives.

The screenshot displays a comprehensive incident response playbook for a DDoS attack. The interface is organized into a grid of cards, each representing a different phase of the incident response process. The phases include Preparation, Identification, Containment, Remediation, Recovery, and Aftermath. Each phase contains specific objectives, actions, and analysis steps. For example, in the Containment phase, the objective is to 'Mitigate the attack's effects on the targeted environment', and actions include blocking DDoS traffic and disabling affected features. The Remediation phase focuses on 'Stop the DDoS' and 'Technical remediation actions'. The Recovery phase involves 'Assess the end of the DDoS incident' and 'Rollback the mitigation measures'. The Aftermath phase includes 'Debrief' and 'Assess the effectiveness of your DDoS incident process'.

Source: [Cyber Security Incident management system using Flexible Evolving Playbooks \(flexibleir.com\)](https://flexibleir.com)

Below is part of the containment playbook workflow for showing the high-level and breakdown process for the internal IP/MAC address block:



Source: [Designing Security Automation Playbooks - Sharing Lessons Learned with Practitioners White Paper \(cisco.com\)](#)

Playbook Battle Cards: [gsvsoc_cirt-playbook-battle-cards/GSPBC-1000 - Impact - Data Encrypted For Impact - Ransomware.pdf at master · guardsight/gsvsoc_cirt-playbook-battle-cards \(github.com\)](#)

Remember, creating an event specific SOC playbook is an ever-ending process. It needs to be updated regularly as new threats emerge and changes occur in the IT environment. Incorporating tools like Tufin can greatly enhance the effectiveness of your SOC playbook.

Designing Security Automation Playbooks

Designing security automation playbooks is a crucial aspect of a well-structured Security Operations Center (SOC). Playbooks are step-by-step guides that define the processes and actions to be taken in response to specific security incidents or events. Here's a comprehensive guide on designing security automation playbooks:

1. Identify Common Security Incidents:

- **Objective:** Understand the types of security incidents your organization is likely to encounter.
- **Action:**
 - Conduct a thorough risk assessment.
 - Analyze historical incident data.
 - Collaborate with threat intelligence sources.

2. Define Playbook Objectives:

- **Objective:** Clearly outline the goals and objectives of each playbook.
- **Action:**
 - Identify the specific security incidents or scenarios the playbook will address.
 - Define the desired outcomes and response objectives.

3. Document Playbook Steps:

- **Objective:** Clearly document the sequence of steps to be followed during an incident.
- **Action:**
 - Break down the incident response process into actionable steps.
 - Provide detailed instructions for each step.

4. Automate Repetitive Tasks:

- **Objective:** Automate routine and repetitive tasks to increase efficiency.
- **Action:**
 - Identify tasks that can be automated, such as log analysis or threat intelligence correlation.
 - Integrate automation scripts or tools into the playbook.

5. Integrate with Security Tools:

- **Objective:** Ensure seamless integration with existing security tools.
- **Action:**
 - Identify the security tools used in your environment.
 - Develop integrations or connectors to facilitate automated actions.

6. Include Decision Points:

- **Objective:** Build flexibility into playbooks by incorporating decision points.
- **Action:**
 - Identify decision criteria based on incident characteristics.
 - Provide guidance for analysts to make informed decisions.

7. Consider Playbook Dependencies:

- **Objective:** Ensure that playbooks are designed to account for dependencies on other processes or teams.
- **Action:**
 - Clearly outline any dependencies, such as involving legal or communication teams.
 - Provide escalation paths when needed.

8. Define Trigger Conditions:

- **Objective:** Clearly define the conditions that trigger the execution of a playbook.
- **Action:**
 - Identify specific indicators or events that initiate the playbook.
 - Set threshold conditions for triggering the playbook.

9. Incorporate Threat Intelligence:

- **Objective:** Enhance playbooks with real-time threat intelligence.
- **Action:**
 - Integrate threat intelligence feeds to enrich incident context.
 - Define actions based on threat intelligence indicators.

10. Continuous Improvement:

- **Objective:** Facilitate ongoing refinement and improvement of playbooks.

- **Action:** - Establish a feedback loop for analysts to provide input. - Regularly review and update playbooks based on lessons learned and changes in the threat landscape.

11. Training and Documentation:

- **Objective:** Ensure that analysts are well-trained on playbook usage.

- **Action:** - Develop comprehensive documentation for each playbook. - Conduct regular training sessions for SOC analysts.

12. Test Playbooks Regularly:

- **Objective:** Validate the effectiveness of playbooks through regular testing.

- **Action:** - Conduct tabletop exercises to simulate real-world scenarios. - Evaluate the efficiency of playbooks and identify areas for improvement.

13. Compliance and Reporting:

- **Objective:** Incorporate compliance requirements into playbooks.

- **Action:** - Ensure that playbooks adhere to regulatory and compliance standards. - Implement reporting mechanisms for audit trails.

14. Cross-Functional Collaboration:

- **Objective:** Encourage collaboration between different teams within the organization.

- **Action:** - Include communication and collaboration steps within playbooks. - Foster a culture of information sharing and teamwork.

15. Regular Review and Update:

- **Objective:** Keep playbooks up-to-date with evolving threats and technologies.

- **Action:** - Establish a periodic review process for playbooks. - Update playbooks based on changes in the threat landscape or organizational structure.

By following these steps, with the SOC manager's help, team players can develop playbooks that enhance the efficiency of their incident response processes and contribute to a more resilient cybersecurity posture.

Security Automation


To improve the incident response process, the security automation team implements automation opportunities using automation tools that they own and maintain. The security automation function needs to know the incident response process well and figure out where automation can make the response more accurate and faster overall.

Before investing in automation, the return on investment (ROI) is always important. The ongoing cost of maintenance and support should be carefully considered when doing a ROI analysis. Use cases that can be automated more often should be given priority during automation development. This improvement will pay up for a long time, and in 3 to 5 years' time, the SOC maturity will be higher and from detection to incident response time will be much decreased, and over a year these savings will be very significant. In most cases, the DevSecOps team will be doing the automations.

How SOC Handles an Ongoing Attack

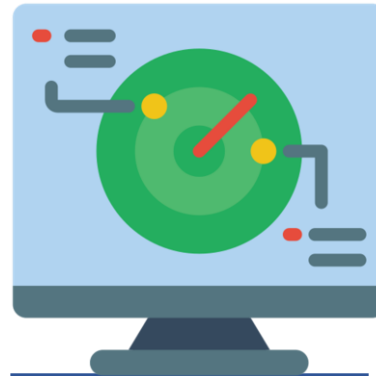
A Security Operations Center (SOC) follows a structured process to handle an ongoing attack. Here are the typical steps involved:

1. **Incident Identification:** The SOC identifies the incident by monitoring systems and analyzing alerts.

- 
2. **Incident Triage:** SOC analysts determine the severity of the incident and prioritize it accordingly.
 3. **Incident Investigation:** The SOC team investigates the incident to understand its nature and scope. This could involve analyzing logs, network traffic, and other relevant data.
 4. **Containment:** The SOC team works to contain the incident to prevent further damage. This could involve isolating affected systems or blocking malicious IP addresses.
 5. **Eradication and Recovery:** The SOC team eradicates the threat from the system and recovers the affected systems. This could involve removing malware, patching vulnerabilities, and restoring systems from backups. But if your backups contain malware inside of them, then a sad scenario emerges.
 6. **Post-Incident Analysis:** After the incident has been resolved, the SOC team conducts a post-incident analysis to understand what happened, why it happened, and how similar incidents can be prevented in the future.
 7. **Communication:** Throughout the incident response process, the SOC team communicates with relevant stakeholders, including management, employees, and possibly customers.

These steps help ensure that incidents are handled effectively and efficiently, minimizing the impact on the organization.





CHAPTER

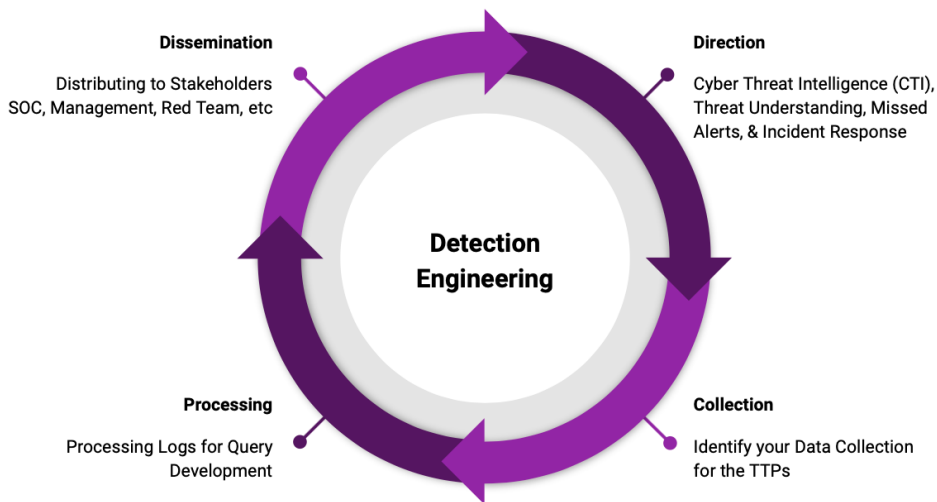
13

Process of Detection Engineering

AGAIN, COMES THE REFERENCE ARCHITECTURE THAT'S PRE-FABRICATED TO ESTABLISH SUPPORTABILITY, INDEXING, PARSING, SEARCH CONCURRENCY ETC.

Detection Engineering (DE) is a crucial aspect of a Security Operations Center (SOC). It involves designing, developing, testing, and maintaining threat detection logic. This threat detection logic can be a rule, a pattern, or even a textual description. The scope of DE is wide and works in multiple dimensions, from risk management to threat intelligence.





Source: [Purple Teaming and Threat-Informed Detection Engineering | SANS Blog](#)

At first the data is collected and correlated by types by SIEM, and SIEM provides the case data to the event management services. All TTPs and IoC data collected and provided within the case. Red team then looks out for actual telemetry data, maps the hash to relevant data sources and confirms the event which can then move to the blue team or to the IR team. In most cases, the internal system flaw that detected the vulnerability, sent out to the server or the application management admin team for resolving the detected issue.

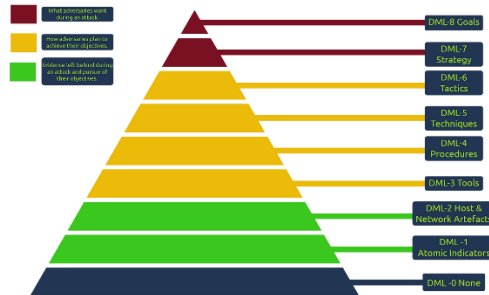
In most cases false positives are minimized by fine tuning the playbooks or the runbooks as they are well known by the team. By letting SIEM know that these data should not be generated in the future. But the catch is, 2/3 out of a 100 events, these may be the RCA for a cause that they are continuously been flagged, and if they come across continuously, these events then be looked into seriously.



Source: [TryHackMe – Intro to Detection Engineering – Walkthrough | by Hamza Anjum | Medium](#)

Detection Maturity Level Model

The DML model comprises nine dedicated maturity levels, numbered from 0 to 8, with the lowest value representing technical aspects of an attack and the highest level representing abstract and intelligence-based aspects of an attack. The image from the THM platform describes at which level we achieve what kind of detection.

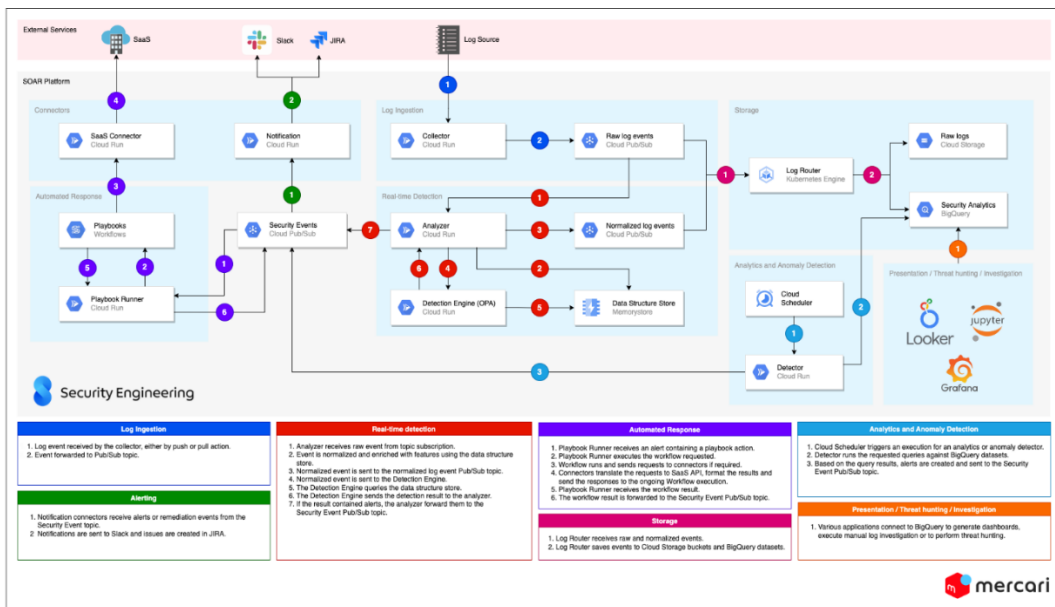


COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Source: [TryHackMe – Intro to Detection Engineering – Walkthrough | by Hamza Anjum | Medium](#)

The goal of detection engineering is to create an automated system of threat detection which is customizable, flexible, repeatable, and produces high-quality alerts for security teams to act upon. It's about developing an environment inside an organization where several teams collaborate to address risks and target potential threats better.


One of the important concepts of detection engineering is Detection-as-Code (DaC). Essentially, DaC means that detection will involve the best implementation practices of software engineering by using the modern agile CI/CD (continuous integration and continuous delivery) pipeline.



Source: [Detection Engineering and SOAR at Mercari | Mercari Engineering](#)

Benefits of Detection Engineering

- **Dynamic threat identification:** Advanced techniques and tactics help detection engineers to identify risks at an early stage of the attack lifecycle. It discovers dynamic and sophisticated threats in real time.
- **Improved incident response:** Activities related to incident response are made easier by automation and adaptability employed in detection engineering.



Quicker response times are made possible by automated systems that can quickly analyze and prioritize security events.


In a SOC, the first tier is SOC-I Engineers. They are responsible for detecting, identifying, and troubleshooting security events that come in. Their main functions are detection, classification, and escalation of attacks. Thus, detection engineering plays a vital role in the functioning of a SOC. It helps in the early detection of threats, thereby enabling the SOC to respond effectively and efficiently to security incidents.

Detection Engineering vs Threat Hunting

Detection engineering is not a new concept, as it has been used for a long time with systems like Intrusion Detection Systems (IDS). To create detection signatures, analysts, engineers, and researchers would spend a lot of resources on analyzing logs and network traffic. However, Detection engineering has evolved over time. In addition to automated detections for atomic indicators, such as IP addresses and domains, modern detection engineering also uses indicators based on the tools and behaviors of threat actors (TTPs).

Detections go through several stages before they result in signals of malicious activity, also known as rules or alerts. These efforts focus on known indicators or behavior and aim to generate signals that will capture malicious activity. The detection engineering process is different from threat hunting. Let's look at some of the aspects of this process. One of the most crucial and time-consuming tasks in detection engineering is handling false positives. False positives can be overwhelming, so some compromises must be made. Another important task is evaluating the current state of detections and adjusting existing rules based on their performance. This could mean lowering the priority of a rule if needed. In this way, Detection engineering has a more structured process. Similar to the development process, rules go through a testing and development phase before they are deployed.

Key Differences:

1. **Threat Awareness:** Detection Engineering focuses on known threats, while Threat Hunting targets unknown threats.
 2. **Use of Infrastructure:** Both use existing security tools, but Detection Engineering enhances detection mechanisms, while Threat Hunting leverages the tools to seek hidden threats.
 3. **Focus:** Detection Engineering centers on detecting specific artifacts or meta-characteristics, whereas Threat Hunting focuses on suspicious behaviors.
- 

4. **Process:** Detection Engineers work on balancing detection with minimizing false positives. Threat Hunting content, however, is written to accommodate non-malicious results that may show suspicious behaviors.
5. **Automation:** Detection content is designed for automation, while Threat Hunting content requires careful interpretation by skilled threat hunters.

Source (Differences): [Detection Engineering vs Threat Hunting: What Are They, Really? \(cyborgsecurity.com\)](https://cyborgsecurity.com/detection-engineering-vs-threat-hunting-what-are-they-really/)

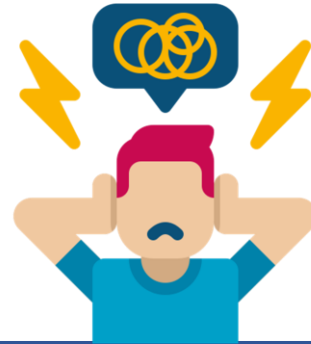
Pro-Tip

•Bad Queue & Timing problem of the SIEM from detection to generating an alert is an ongoing problem, simply put, the timestamps logs and a timestamp of the local time zones will have a bliss all together, have the detection engine configured in either with UTC or GMT, this will affect your detection rules, if a new one is added. Time stamp on events must be placed automatically.

Evasive Techniques

Attackers use evasive techniques to bypass intrusion detection systems (IDSs). These techniques include (not an exhaustive list):

- Flooding.
- Fragmentation.
- Encryption.
- Obfuscation.
- Packet fragmentation.
- Source routing.
- Source port manipulation.



CHAPTER

14

OSINT Tools and Their Usage

THIS IS WHERE YOUR FOCUS NEEDS MORE ATTENTION AS DATA IS COLLECTED FROM VARIOUS WEB SOURCES WHO PROVIDES THESE DATA, SOMETIMES UNVERIFIED. EVERYONE NEEDS HELP, ASK FOR ONE!

OSINT tools are designed to collect and aggregate important information about a target from various online platforms. These tools are openly accessible and can be used by anyone, but they are primarily used by hackers and security professionals who rely heavily on this information. OSINT, short for Open-Source Intelligence, is the practice of gathering intelligence from publicly available sources and data. Unlike classified information that requires specific access, OSINT relies on accessible data that can be legally obtained without constraints. This includes data from the internet, public records, and news sources.

While our focus has been on OSINT tools within the context of our security operations center (SOC), these techniques and tools have diverse applications across various



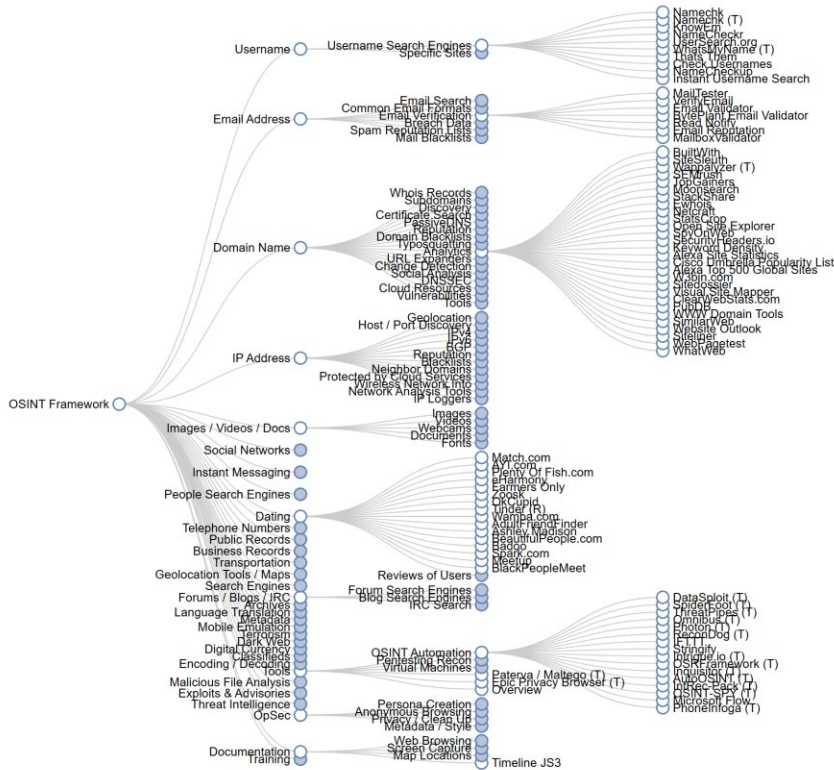
COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

functions. Penetration testers and bug bounty hunters use them to gather public intelligence on organizations, aiding in prioritizing testing based on exposed technologies and vulnerabilities.

OSINT tools are adaptable for both offensive and defensive purposes, contingent on the user's objectives. Security professionals find great value in OSINT tools for simplifying otherwise laborious tasks. Within SOCs, OSINT tools and methodologies are leveraged to fortify security stance. Common applications of OSINT in cybersecurity encompass external threat analysis, mapping the attack surface, surveying infrastructure, identifying network vulnerabilities, and more.

OSINT Framework

i.e. this mindmap is not fully expanded: click on the link to see the expanded view



Source: [OSINT Framework](#)

OSINT is Primary Used for Different Visibilities

1. **Threat Intelligence** – OSINT empowers us to explore the latest hacking methodologies, emerging threats, real-world vulnerabilities, and exploits. This external threat intelligence assists us in enhancing infrastructure security against contemporary attack vectors.
2. **Incident Response** – OSINT aids in swiftly gathering context during security incidents surrounding suspicious indicators such as IP addresses, domains, and file hashes potentially involved in an attack. This expedites incident investigation and response efforts.
3. **Attack Surface Mapping** – Through OSINT utilization, we unveil exposed systems, open ports, utilized technologies, subdomains, and other outward-facing assets. This process enables us to map potential attack surfaces and mitigate associated risks.
4. **Infrastructure Mapping** – OSINT tools provide comprehensive visualization of our entire online infrastructure footprint encompassing cloud providers, domains, networks, and services. Such holistic visibility of assets significantly bolsters security measures.
5. **Breach Assessment** – In scenarios of suspected compromise, OSINT techniques assist in assessing the impact by scouring for organizational data on sale within dark web markets and other public sources.


Most Commonly Used OSINT's

1. Recon-NG
2. Maltego
3. URL Scan
4. SpiderFoot
5. FOCA
6. theHarvester
7. Google Dorks
8. Creepy
9. TweetDeck
10. Mitaka
11. Spysc
12. BuiltWith
13. Intelligence X
14. DarkSearch.io
15. Grep.app
16. Shodan
17. Metagoofil
18. Searchcode
19. Babel X

Differences between open-source intelligence (OSINT) and classified intelligence:

1. **Nature and Accessibility:**
 - **Open-Source Intelligence (OSINT):**

- **Classified Intelligence:**
 - **Nature:** OSINT refers to information collected from publicly available sources. These sources include news articles, social media, websites, academic papers, and other openly accessible data.
 - **Accessibility:** OSINT is openly available to anyone without the need for special clearances or permissions.
- **Classified Intelligence:**
 - **Nature:** Classified intelligence involves sensitive information that is not publicly accessible. It includes data related to national security, military operations, and other confidential matters.
 - **Accessibility:** Classified intelligence is restricted and accessible only to authorized personnel with appropriate security clearances.
- 2. **Collection Methods:**
 - **OSINT:**
 - Collected from open sources such as websites, social media platforms, and public records.
 - Techniques include web scraping, data mining, and analysis of publicly available information.
 - **Classified Intelligence:**
 - Gathered through specialized channels, covert operations, and classified sources.
 - Requires specialized training and access to secure databases.
- 3. **Purpose and Use:**
 - **OSINT:**
 - Used for situational awareness, threat assessment, and understanding public sentiment.
 - Supports decision-making in various domains, including business, law enforcement, and cybersecurity.
 - **Classified Intelligence:**
 - Supports national security, military operations, and strategic planning.
 - Provides insights into adversary capabilities, intentions, and vulnerabilities.
- 4. **Handling and Security:**
 - **OSINT:**
 - Generally unclassified and does not require strict handling procedures.
 - However, ethical considerations are essential to avoid privacy violations.
 - **Classified Intelligence:**
 - Requires rigorous security protocols.

- 
- Classified information is compartmentalized, encrypted, and protected to prevent unauthorized access.
 - 5. **Examples:**
 - **OSINT:**
 - Monitoring social media trends during a crisis.
 - Analyzing news articles to track geopolitical developments.
 - **Classified Intelligence:**
 - Intercepted communications between foreign entities.
 - Satellite imagery revealing military installations.





CHAPTER

15

SOC and CSIRT, Better Together

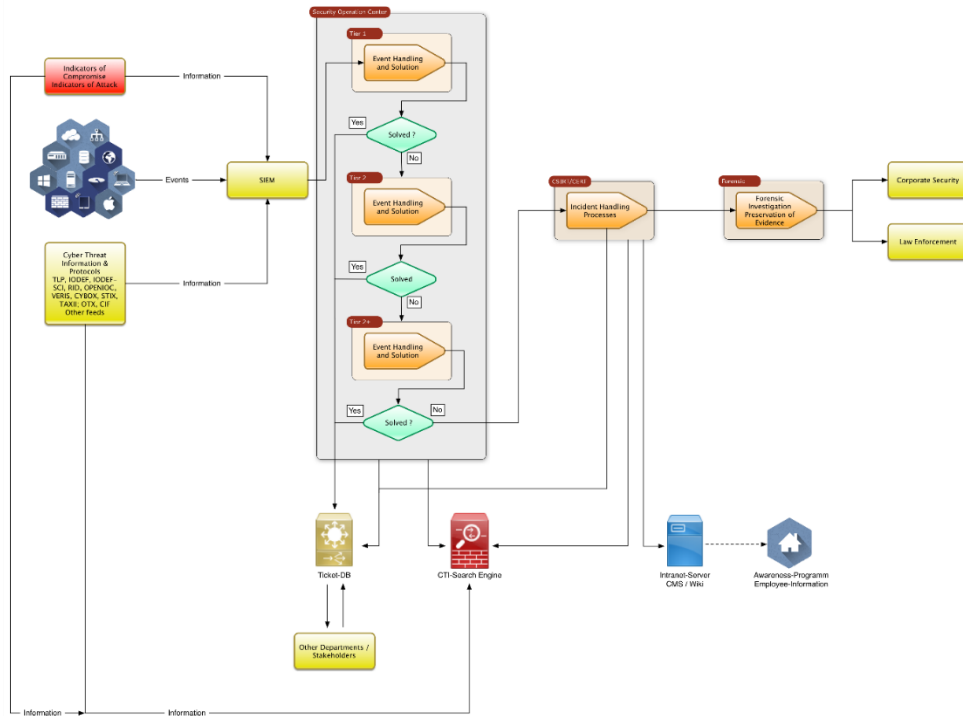
A SIEM IS BETTER COUPLED TOGETHER WITH SOAR, THAT WE HAVE COVERED FOR BETTER DATA COMPOSITION & CASE MANAGEMENT, AND CSIRT FULFILLS INCIDENT RESPONSE MANAGEMENT TO THE RESPONDER, WITH INTEGRATED OSINT.

A Security Operations Center (SOC) and a Computer Security Incident Response Team (CSIRT) are two key components of an organization's cybersecurity infrastructure. They work together to ensure the security of the organization's information systems.

The SOC is responsible for the detection and prevention of cyberattacks on an organization. It is a centralized function that actively monitors the organization's networks, servers, and other IT structures for potential threats. When a security incident is detected, the SOC performs initial analysis and passes the incident to the CSIRT.



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Source: [SOC-CSIRT Workflow - SecureGlobal](#)

The CSIRT, on the other hand, is a multi-functional team that responds to security incidents. It can be an ad hoc group that comes together when a security incident occurs, or it can be a more established group with a recognized membership that immediately knows its responsibilities when an incident occurs. The CSIRT is activated if the SOC requires help with additional analysis.

There are also documents available on how to develop and integrate CSIRT in your SOC by ENISA @ [How to set up CSIRT and SOC – ENISA \(europa.eu\)](#) and their assessment maturity level for CSIRT is located @ [SIM3v2i self-assessment tool – ENISA \(europa.eu\)](#). other sites for CSIRT:

- insights.sei.cmu.edu

FIRST Services Framework – Typical CSIRT Services

SERVICE AREAS



INFORMATION SECURITY INCIDENT MANAGEMENT

- Information Security Incident Report Acceptance
- **Information Security Incident Analysis**
- **Artifact and Forensic Evidence Analysis**
- Mitigation and recovery
- **Information Security Incident Coordination**
- Crisis management Support



VULNERABILITY MANAGEMENT

- Vulnerability Discovery/Research
- Vulnerability Report intake
- Vulnerability Analysis
- **Vulnerability Coordination**
- Vulnerability Disclosure
- Vulnerability Response



SITUATIONAL AWARENESS

- Data Acquisition
- Analysis and Synthesis
- Communication



KNOWLEDGE TRANSFER

- **Awareness Building**
- Training and Education
- Exercises
- Technical and Policy Advisory



INFORMATION SECURITY EVENT MANAGEMENT

- Monitoring and Detection
- Event Analysis

Source: [How to set up CSIRT and SOC – ENISA \(europa.eu\)](http://europa.eu)

Another good resource center for CSIRT: [Resources for Creating a CSIRT \(cmu.edu\)](http://cmu.edu)

Current Maturity Level

Info-table view: This table is updated in real-time. You can click on any ID to navigate to it in the web version, link provided above ([SIM3v2i self-assessment tool – ENISA \(europa.eu\)](#)).

ID	Title	Maturity	Relative to Basic	Basic	Intermediate	Advanced
0-1	Mandate	0	Improvement needed	3	4	4
0-2	Constituency	0	Improvement needed	3	4	4
0-3	Authority	0	Improvement needed	3	4	4
0-4	Responsibility	0	Improvement needed	3	4	4
0-5	Service Description	0	Improvement needed	3	4	4

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



0-6	Public Media Policy	0	Improvement needed	2	3	4
0-7	Service Level Description	0	Improvement needed	3	4	4
0-8	Incident Classification	0	Improvement needed	2	3	3
0-9	Participation in CSIRT Systems	0	Improvement needed	3	4	4
10	Organisational Framework	0	Improvement needed	3	3	3
11	Security Policy	0	Improvement needed	2	3	4
11	Code of Conduct/Practice/Ethics	0	Improvement needed	2	3	3
12	Staff Resilience	0	Improvement needed	2	3	4
13	Skillset Description	0	Improvement needed	2	2	3
14	Staff Development	0	Improvement needed	2	3	4
15	Technical Training	0	Improvement needed	1	2	3
16	Soft Skills Training	0	Improvement needed	1	2	3
17	External Networking	0	Improvement needed	2	3	3
18	IT Assets & Configuration	0	Improvement needed	1	2	3
19	Information Sources List	0	Improvement needed	2	3	4
20	Consolidated Messaging System(s)	0	Improvement needed	2	3	3
21	Incident Tracking System	0	Improvement needed	2	3	3
22	Resilient Voice Calls	0	Improvement needed	2	3	3



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



T-6	Resilient Messaging	0	Improvement needed	2	3	3
T-7	Resilient Internet Access	0	Improvement needed	2	3	3
T-8	Incident Prevention Toolset	0	Improvement needed	2	2	3
T-9	Incident Detection Toolset	0	Improvement needed	2	3	3
T-10	Incident Resolution Toolset	0	Improvement needed	2	3	3
P-1	Escalation to Governance Level	0	Improvement needed	3	4	4
P-2	Escalation to Press Function	0	Improvement needed	2	3	3
P-3	Escalation to Legal Function	0	Improvement needed	2	3	3
P-4	Incident Prevention Process	0	Improvement needed	2	3	4
P-5	Incident Detection Process	0	Improvement needed	2	3	4
P-6	Incident Resolution Process	0	Improvement needed	2	3	4
P-7	Specific Incident Processes	0	Improvement needed	2	3	4
P-8	Audit & Feedback Process	0	Improvement needed	3	4	4
P-9	Emergency Reachability Process	0	Improvement needed	2	3	3
P-10	Best Practice Internet Presence	0	Improvement needed	2	3	3
P-11	Secure Information Handling Process	0	Improvement needed	2	3	3
P-12	Information Sources Process	0	Improvement needed	2	3	4
P-13	Outreach Process	0	Improvement needed	2	3	4





P-14	Governance Reporting Process	0	Improvement needed	3	4	4
P-15	Constituency Reporting Process	0	Improvement needed	2	3	3
P-16	Meeting Process	0	Improvement needed	2	2	3
P-17	Peers Collaboration Process	0	Improvement needed	2	3	4

The CSIRT performs three main tasks:

1. Receives information on a security breach.
2. Analyzes it.
3. Responds to the sender.

In addition to these tasks, CSIRTs may also support SOC's by:

- Reviewing standard security arrangements.
- Managing audits and training for new threats.
- Investigating new vulnerabilities and sharing the latest industry-level responses.
- Liaising with different internal and external stakeholders when an incident occurs.
- Managing remotely-stored critical information (passwords, network configs, etc.) in an emergency.
- A CSIRT consists of 5 pillars, which represent the basic activities.



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

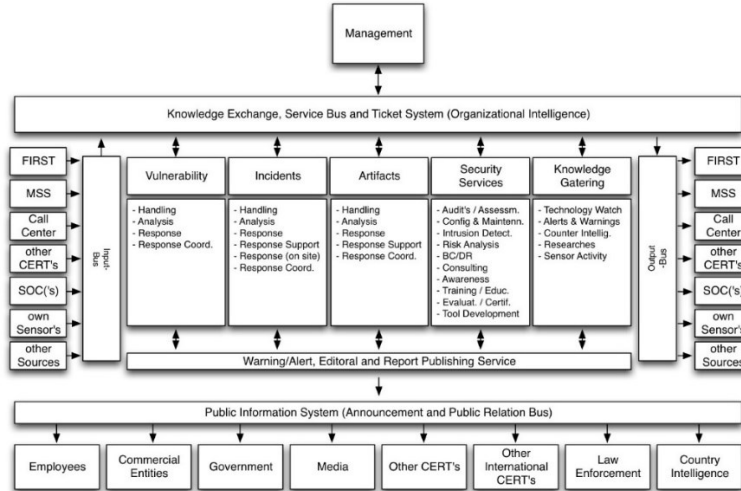


Basisaktivität (Säule)	Services
Vulnerability	<ul style="list-style-type: none"> - Handling - Analysis - Response - Response Coordination
Incident	<ul style="list-style-type: none"> - Handling - Analysis - Response Support - Response (On-Site) - Response Coordination
<u>Artifact</u>	<ul style="list-style-type: none"> - Handling - Analysis - Response - Response Support - Response Coordination
Security Services	<ul style="list-style-type: none"> - Audits and Assessments - Configuration & Management - Intrusion Detection - Risk Analysis - Business Continuity, Disaster Recovery - Consulting - Awareness - Training / Education - Evaluation / Certification - Tool Development
Knowledge Gathering	<ul style="list-style-type: none"> - Technology Watch - Alerts & Warnings - Counter Intelligence - Researches - Sensor Activity



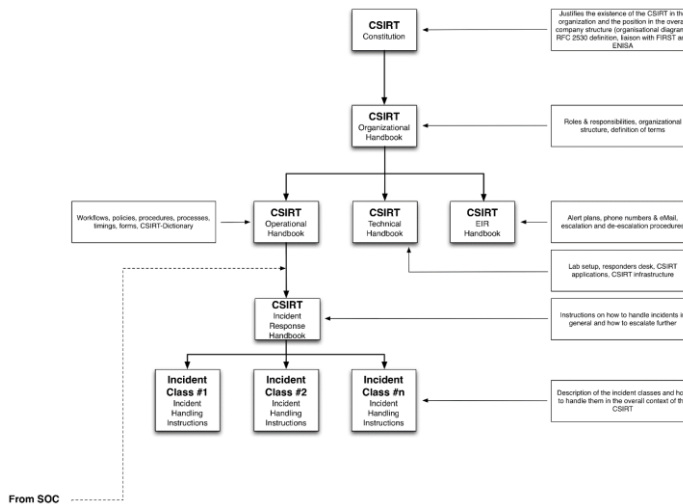
COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

5 CSIRT Pillars



Source: [The CSIRT methodology - SecureGlobal](#)

CSIRT Documentation Framework



Source: [The CSIRT methodology - SecureGlobal](#)

In essence, while the SOC is focused on proactive monitoring and detection, the CSIRT is reactive, responding to incidents as they occur. Both teams work closely together, with the SOC acting as a front end for the CSIRT. This collaboration ensures a comprehensive approach to cybersecurity, enhancing the organization's ability to prevent, detect, and respond to cyber threats.



CHAPTER


16

Digital Forensics and Incident Response (DFIR)

TRACING BACK WHAT HAPPENED DURING A BREACH, OR AN EARLY DETECTION OF BREACH IS WHAT YOU ARE GETTING TRAINED FOR IN YOUR DOMAIN AND IN YOUR SPACE. YOUR FINDINGS WILL BE ULTIMATUM TO THE ABUSER AS ELECTRONIC EVIDENCE ARE PRODUCED.

DFIR stands for Digital Forensics and Incident Response. It is a field within cybersecurity that focuses on the identification, investigation, and remediation of cyberattacks. DFIR has two main components: Digital Forensics and Incident Response. Digital Forensics is a subset of forensic science that examines system data, user activity, and other pieces of digital evidence to determine if an attack is in progress and who may be behind the

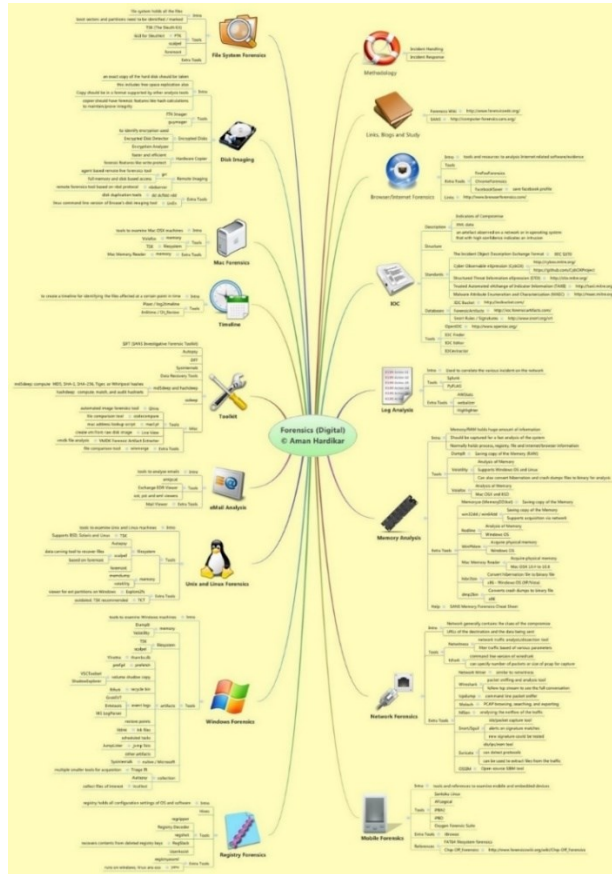




activity. Incident Response is the overarching process that an organization will follow in order to prepare for, detect, contain, and recover from a data breach. DFIR has become a central capability within the organization's security strategy and threat hunting capabilities due to the proliferation of endpoints and an escalation of cybersecurity attacks in general. The shift to the cloud, as well as the acceleration of remote-based work, has further heightened the need for organizations to ensure protection from a wide variety of threats across all devices that are connected to the network. Though DFIR is traditionally a reactive security function, sophisticated tooling and advanced technology, such as artificial intelligence (AI) and machine learning (ML), have enabled some organizations to leverage DFIR activity to influence and inform preventative measures. In such cases, DFIR can also be considered a component within the proactive security strategy.

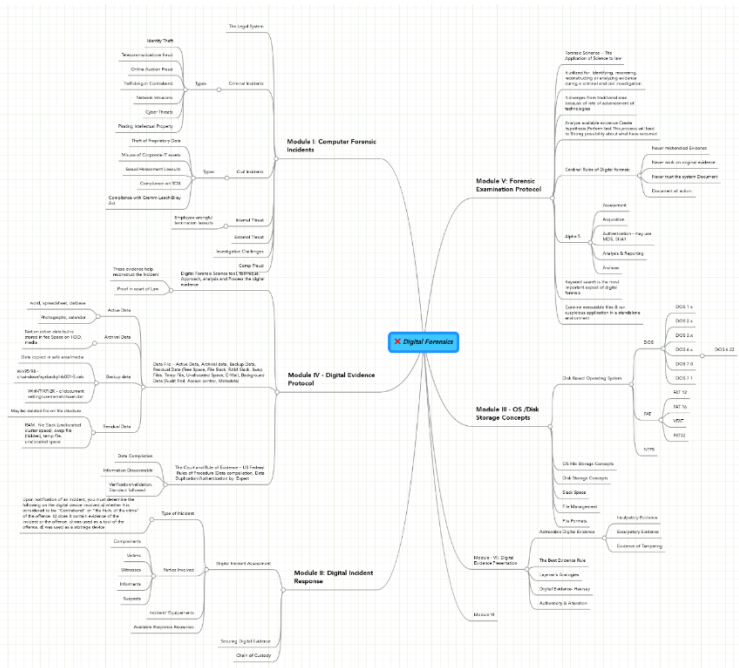


Digital Forensic Mindmap



Source: (scoop.it)

Another Mindmap of DFIR



Source: [Digital Forensics - MindMeister Mind Map](#)

How is Digital Forensics Used in the Incident Response Plan

Digital forensics provides the necessary information and evidence that the computer emergency response team (CERT) or computer security incident response team (CSIRT) needs to respond to a security incident.

Digital forensics may include:

- **File System Forensics:** Analyzing file systems within the endpoint for signs of compromise.
- **Memory Forensics:** Analyzing memory for attack indicators that may not appear within the file system.
- **Network Forensics:** Reviewing network activity, including emailing, messaging and web browsing, to identify an attack, understand the cybercriminal's attack techniques and gauge the scope of the incident.

- **Log Analysis:** Reviewing and interpreting activity records or logs to identify suspicious activity or anomalous events.

The Value of Integrated Digital Forensics and Incident Response (DFIR)


While digital forensics and incident response are two distinct functions, they are closely related and, in some ways, interdependent. Taking an integrated approach to DFIR provides organizations with several important advantages, including the ability to:

- **Respond** to incidents with speed and precision
- **Follow** a consistent process when investigating and evaluating incidents
- **Minimize** data loss or theft, as well as reputational harm, as a result of a cybersecurity attack
- **Strengthen** existing security protocols and procedures through a more complete understanding of the threat landscape and existing risks
- **Recover** from security events more quickly and with limited disruption to business operations
- **Assist** in the prosecution of the threat actor through evidence and documentation

Source: [Digital Forensics and Incident Response \(DFIR\) - CrowdStrike](#)

Types of Forensics

- **File system forensics:** File system forensics is a subset of digital forensics. The process allows us to analyze machines on the data storage level, which usually includes remote devices.
- **Memory forensics:** Memory forensics helps analyze volatile forms of evidence like system memory and detect signs of malware, even when traditional protection mechanisms like an antivirus don't find anything.
- **Network forensics:** Network forensics is the process of investigating what happens in a digital network. Did an infection originate from an email or link? Understanding this process can be helpful, as it's one that digital forensics experts encounter regularly.
- **Malware triage:** The malware triage service is designed to help DFIR teams identify particular malware strains and better address the damage it causes.
- **Log analysis:** Log analysis is a valuable skill for identifying abnormal activity happening on a system. Automating this task saves time, but you'll want to ensure that your log analysis software is reliable and accurate.

- 
- **Software development:** Software development and technology change rapidly, so staying up to date with trends is essential for DFIR teams. Being able to code and script can be a huge asset.
 - **Communication:** How you communicate with team members, other organizations, and management can often determine how successful an incident response is.
 - **Analytical thinking:** Analytical thinking is a challenging but essential skill for DFIRs. It takes focus to gather relevant information and challenge your assumptions before testing them out. Even if you're three steps ahead, it's worth slowing down to reflect on analytical thinking.
 - **Teamwork:** It's important to remember that incident response is a high-stakes experience, and team members must know how to work together as a cohesive unit. It takes commitment, communication, and responsibility to succeed.

DFIR Timeline Generator

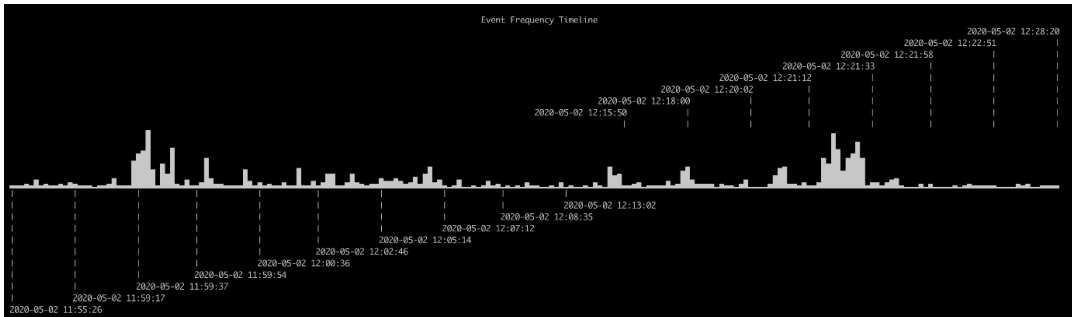
A Free Threat Hunting Tool and Fast Forensics Timeline Generator.

Timeline analysis involves reviewing events over some time to construct the story of events to look for potential attacks and uncover hidden threats.

It allows us to differentiate routine events from suspicious ones by considering the context and timing of each action.

Hayabusa is a sigma-based threat hunting and fast forensics timeline generator for Windows event logs, developed by Yamato Security group:

- Cross-platform: Works on Windows, Linux, macOS.
- Simplified forensic timelines.
- Converts Sigma rules to Hayabusa rules.
- MITRE ATT&CK tactics mapping.
- Evtx record carving from slack space.
- Parses and extracts from PowerShell classic logs.
- Multi-threaded for up to 5x speed boost.



Source: [GitHub - Yamato-Security/hayabusa](https://github.com/Yamato-Security/hayabusa): Hayabusa (隼) is a sigma-based threat hunting and fast forensics timeline generator for Windows event logs.

CVE, CVSS, NVD, KEV

CVE (Common Vulnerabilities and Exposure) is the largest repository which enlists product-wise vulnerabilities which are publicly disclosed, and each vulnerability is allotted a unique alphanumeric number that corresponds to the product's identified vulnerability. Later on, these CVE numbers are cataloged per product.


You should also know that CVE is sponsored by the U.S. Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Security Agency (CISA)

Historically MITRE hosted the CVE site <https://cve.mitre.org/> and the registered owner of the CVE list and the CVE logo, which were the originally popular amongst security analysts, and now the new site (<https://www.cve.org/>) has been launched, where you still can search of CVE's for products.

Operating under the authority of the CVE Program, "CNAs" (CVE Numbering Authorities) are organizations that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed upon scope, for inclusion in first-time public announcements of new vulnerabilities. These CVE IDs are provided to researchers, vulnerability discoverers or reporters, and information technology vendors.

The CVSS specifications are owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help computer security incident response teams across the world. The official CVSS documentation can be found at <https://www.first.org/cvss/>

NVD (National Vulnerability Database): The NVD ([NVD - Home \(nist.gov\)](https://nvd.nist.gov/)) is the U.S. government repository of standards-based vulnerability management data represented



using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, product names, and impact metrics. You should know that this is not updated to the same frequency as CVSS or CVE.

CVEShield provides additional insights, such as:

- **V-Score:** Estimates the likelihood of a vulnerability being exploited by threat actors. By incorporating a range of open-source data sources including NVD, MITRE, CISA KEV (Known Exploited Vulnerability), and social media.
- **E-Score:** Evaluates the probability of a software vulnerability being exploited in the wild.
- **CVSS Score:** A standardized vulnerability severity rating
- **Description:** A brief summary of each vulnerability for quick insight.

You can check it out from the link: [CVEShield](#)



CHAPTER

17

Continuous Threat Exposure Management - CTEM

SCENARIO DEMANDS FOR EARLY NOTIFICATIONS FROM SOC, AS VULNERABILITIES CHANGES STATES TO DIFFERENT DEVICE CONFIGURATIONS. SOC ALSO MONITORS COMPROMISED TYPES AND LOCATES SOURCES, MERGES DATA FROM OSINT, DETECTION ENGINEERING DATA, ALONG WITH YOUR DFIR DATA INTO A ONE GIANT CASE FILE FOR 1 SINGLE EVENT.

Continuous Threat Exposure Management (CTEM) is a cybersecurity process that leverages attack simulations to identify and mitigate threats to an organization's



networks and systems. This allows organizations to test their security posture and identify vulnerabilities before they are exploited by real attackers.

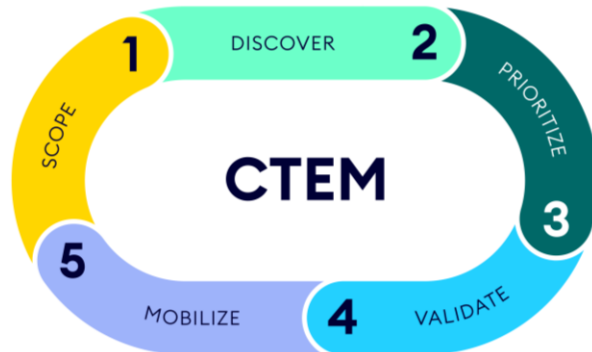
CTEM consists of five stages: scoping, discovery, prioritization, validation, and remediation. The goal of CTEM is to establish well-defined security and risk management strategies that align with business objectives and reduce the attack surface of the enterprise.

CTEM is a forward-thinking framework that goes beyond traditional vulnerability management methods by actively and regularly identifying, assessing, monitoring, and reducing security weaknesses in an organization's infrastructure. CTEM also promotes collaboration among all stakeholders, including IT operations, governance, risk, compliance, and asset owners.

In another perspective from XM Cyber (very detailed explanation from them – click on the picture source link to see details), their perspective is as follows, only change observed for the number 5 and that's to "Mobilize" in reference to Gartner:


Source: [CTEM | XM Cyber](#)

How is CTEM Different from Cloud Security Posture Management (CSPM)?



CTEM and CSPM are both cloud security technologies that help organizations identify and mitigate risks in their cloud environments. However, they focus on different aspects of cloud security:

- CTEM is mainly concerned with **attack simulations** that test the security posture and resilience of the cloud infrastructure against various threat scenarios. CTEM helps organizations find and fix vulnerabilities before they are exploited by real attackers.
- CSPM is mainly concerned with **configuration management** that monitors and assesses the compliance and risk of various cloud services and settings. CSPM



helps organizations detect and remediate misconfigurations that expose cloud resources to potential breaches.

Both CTEM and CSPM complement each other by addressing different attack surfaces and providing different insights into the cloud security posture. Some of the key benefits of using both CTEM and CSPM are:

- Improved visibility and control over cloud assets and services
- Enhanced detection and prevention of cloud-based attacks
- Reduced attack surface and exposure to threats
- Increased compliance with security standards and regulations
- Optimized cloud security performance and efficiency

Security and risk management leaders should aim for visibility into exposures and attract the interest of other senior leaders byctem highlighting the issues with the most potential impact on an organization’s critical operations. They should define a narrower scope for CTEM, aligned with business objectives, using familiar language, and explaining the impact on the business, not technology.


As part of a CTEM plan, security leaders should expand communication with other department heads, asset owners and third parties to have clear paths to mobilize responses and remediations. They should also get traction with business departments and asset owners by clearly articulating and discussing the residual risk associated with the postponement of remediation efforts, offering short-term and long-term options to reduce or eliminate exposure.

If you want to learn more about CTEM and CSPM, you can check out these articles:

- [CSPM Vs. CIEM: Demystifying Two Popular Cloud Security Acronyms](#)
- [CIEM vs CSPM: Which is Better for Reducing Public Cloud Risk?](#)
- [CIEM vs CSPM](#)
- [Real Life Use Cases CIEM vs CWPP vs CSPM](#)
- [CIEM vs CSPM: Which Is the Right Solution for Your Cloud?](#)

Readiness Requirements to Implement CTEM and CSPM

Implementing CTEM and CSPM in your organization requires a strategic and collaborative approach that involves various stakeholders, tools, and processes. Here are some general steps that you can follow to get started:

- 
- Define your scope and objectives: Identify your business-critical assets, services, and settings that need to be protected and monitored in the cloud. Align your security goals with your business priorities and compliance requirements.
 - Choose your tools and platforms: Select the appropriate CTEM and CSPM solutions that suit your cloud environment and security needs. You can use a combination of tools that provide different functionalities, such as attack simulation, configuration monitoring, vulnerability scanning, risk assessment, and remediation automation.
 - Establish your workflows and policies: Define your roles and responsibilities, communication channels, reporting mechanisms, and escalation procedures for managing and responding to cloud security issues. Establish clear and consistent policies and standards for configuring and securing your cloud resources and services.
 - Execute and monitor your CTEM and CSPM programs: Run regular and continuous tests and scans to identify and prioritize your cloud security exposures. Validate and verify the effectiveness and accuracy of your findings and recommendations. Remediate and resolve the identified issues as soon as possible, following the best practices and guidelines.
 - Review and improve your CTEM and CSPM programs: Analyze and measure your cloud security performance and progress over time. Identify and address any gaps, challenges, or opportunities for improvement. Update and refine your scope, objectives, tools, workflows, and policies as needed.

Threat Intelligence Platform for SOC Security

A Threat Intelligence Platform (TIP) is a crucial tool for Security Operations Centers (SOCs). It allows SOC teams to collect, collate, and parse threat data in real-time, enabling security teams to identify and prevent attacks even before they occur. TIPs help security teams better understand the threat landscape as they accumulate and analyze information from various sources.

Here are a few examples of Threat Intelligence Platforms for SOCs:

1. ThreatConnect
2. **SOCRadar® Digital Risk Protection Platform:** This product combines External Attack Surface Management, Digital Risk Protection, and Cyber Threat Intelligence modules to improve your security posture. It provides visibility and context regarding the severity of unknown external-facing digital assets with automated continuous monitoring. It also offers actionable intelligence alerts with instant phishing domain identification, compromised credential and credit card detection.
3. **Recorded Future Intelligence Cloud:** This tool provides real-time intelligence on a wide range of topics, including cybersecurity, geopolitical events, and financial

markets. The platform is user-friendly and easy to navigate with intuitive visualizations that allow users to quickly identify trends and patterns.

4. **ThreatQuotient™ ThreatQ v5:** This platform supports the SOC of the future, where data is the foundation. ThreatQ's newest features include a unique DataLinq Engine for connecting disparate systems and sources to enable extended detection and response (XDR), Smart Collections for driving automation, and an enhanced ThreatQ Data Exchange for bi-directional sharing of data, context, and threat intelligence.



SOC Policies & Processes

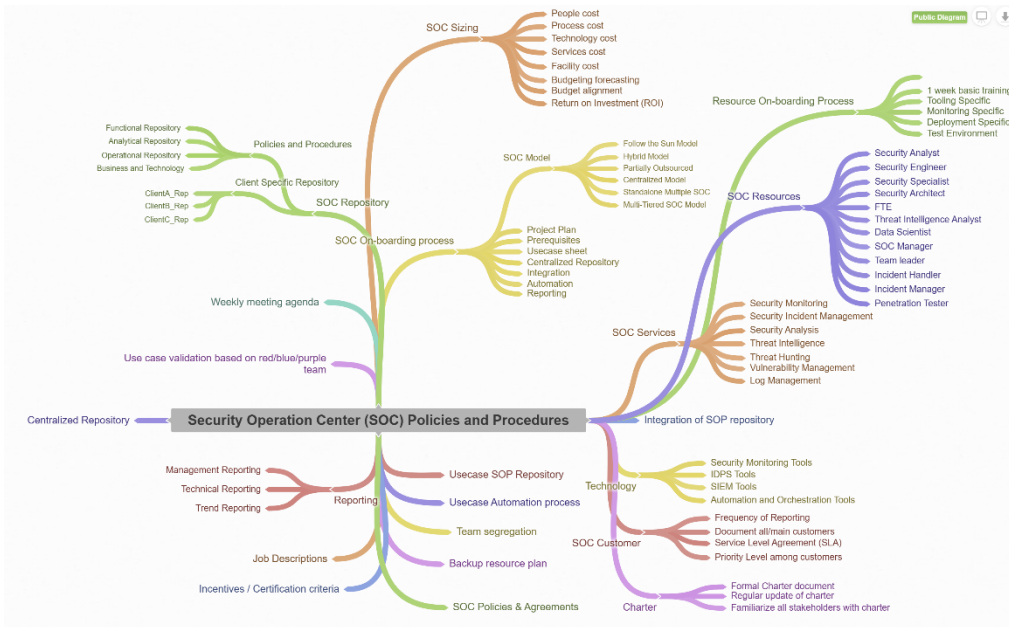
SOME GUIDANCE DOCUMENTATION IS REQUIRED AND MADE A DE-FACTO TO OPERATE THE SOC IN A DESIRED LEVEL OF FUNCTIONALITY. AS HEAVILY INVESTED INTO A SOC, IT IS EXPECTED THAT THE OUTCOME MUST BE PRODUCED IN AN ORDERLY FASHION WITH A RISK MANAGEMENT SCENARIO TO PROTECT AGAINST ANY TYPE OF THREATS.

These are some of the policies, processes and procedures to follow. At some times, security analysts can be seen reacting to these policies as they are already overburdened with too many things to follow these outlines, but it can be slowly injected into the SOC processes, you would want to be creative in applying these controls into the SOC formation, the art of it is that your analysts will become more effective and professional, the downside of this, they will move out even faster. But it's a job nonetheless that you will need to carry out.



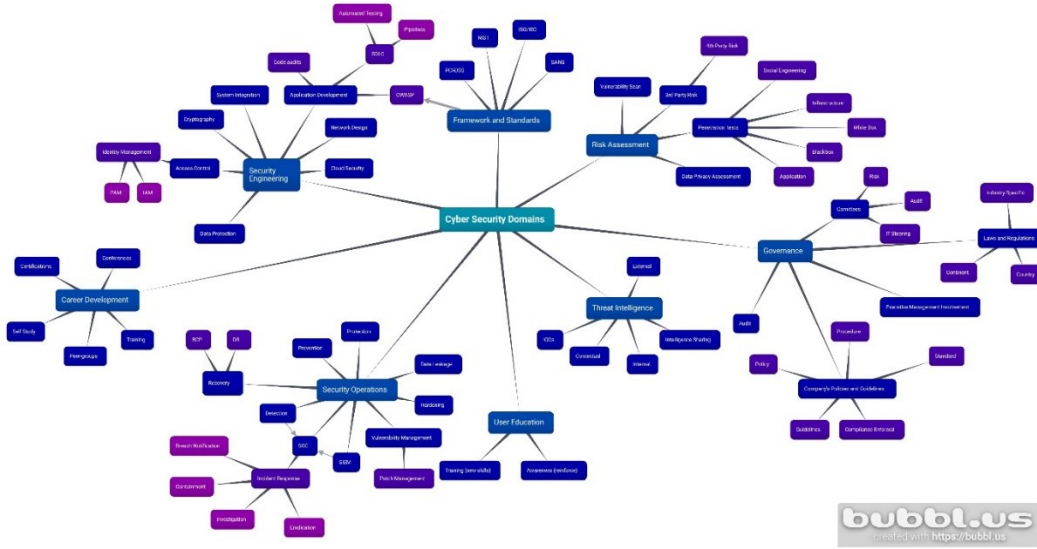
COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

The below CSIAC document also outlines some of the best designed governance matrices for a countries cybersecurity governance framework. Each of the boxes are clickable and will land you on a linked page to that respective framework and which has links to relevant resources. This can be too much as well since too many frameworks, processes, policies are interrelated, and tracing those to a map is nearly impossible. But the knowledgebase is worth browsing it, when you require it, for a specific tasks, events, activities or guidelines are needed.



Source: [Security Operation Center \(SOC\) Policies and Procedures \(coggle.it\)](#)

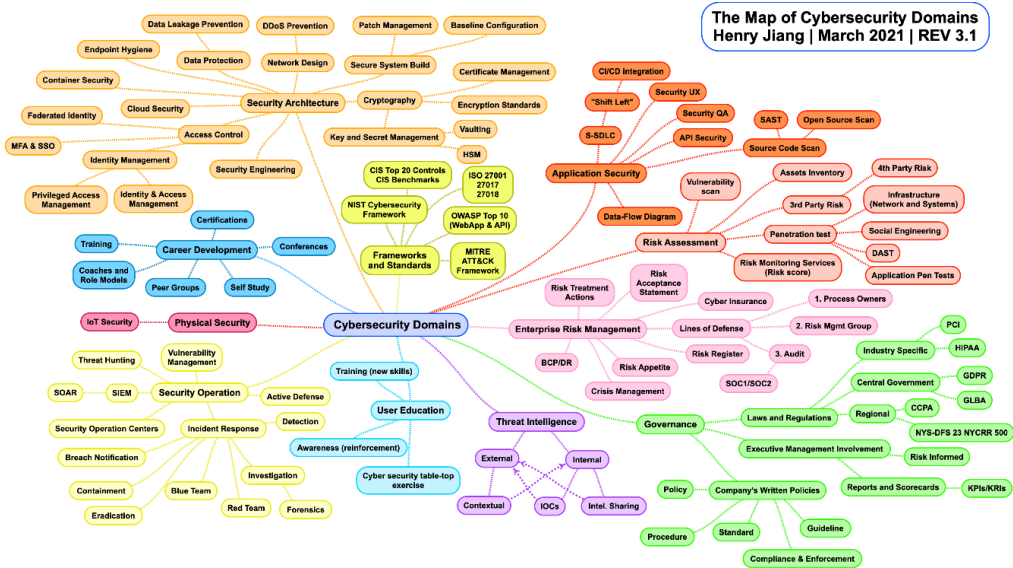
Cyber Security Domains



Source: [Bubbl.us - Cyber Security Domains](https://bubbl.us)

Another good mind map here from Henry Jiang:

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Source: [LinkedIn Share | Powered by Box](#)

But these are not nearly complete, as you may feel that there are lot of domain missing from the above two pictures. There is also another mindmap you can explore and here is the link: [Cyber Security | MindMeister Mind Map](#)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Cybersecurity & Data Privacy by Design Principles

C|P 2023.4
SCF | **SECURE CONTROLS FRAMEWORK**

- Cybersecurity & Data Protection Governance (GOV)**
Execute a documented, risk-based program that supports business objectives while encompassing appropriate cybersecurity & data protection principles that addresses applicable statutory, regulatory and contractual obligations.
- Artificial Intelligence and Autonomous Technology (AAT)**
Ensure trustworthy and resilient Artificial Intelligence (AI) and autonomous technologies to achieve a beneficial impact by informing, advising or simplifying tasks, while minimizing emergent properties or unintended consequences.
- Asset Management (AST)**
Manage all technology assets from purchase through disposition, both physical and virtual, to ensure secured use, regardless of the asset's location.
- Business Continuity & Disaster Recovery (BCD)**
Maintain a resilient capability to sustain business-critical functions while successfully responding to and recovering from incidents through well-documented and exercised processes.
- Capacity & Performance Planning (CAP)**
Govern the current and future capacities and performance of technology assets.
- Change Management (CHG)**
Manage change in a sustainable and ongoing manner that involves active participation from both technology and business stakeholders to ensure that only authorized changes occur.
- Cloud Security (CLD)**
Govern cloud instances as an extension of on-premise technologies with equal or greater security protections than the organization's own internal cybersecurity & data privacy controls.
- Compliance (CPL)**
Oversee the execution of cybersecurity & data privacy controls to ensure appropriate evidence required due care and due diligence exists to meet compliance with applicable statutory, regulatory and contractual obligations.
- Configuration Management (CFG)**
Enforce secure configurations according to vendor-recommended and industry-recognized secure practices that enforce the concepts of "least privilege" and "least functionality" for all systems, applications and services.
- Continuous Monitoring (MCH)**
Maintain situational awareness of security-related events through the centralized collection and analysis of event logs from systems, applications and services.
- Cryptographic Protections (CRY)**
Utilize appropriate cryptographic solutions and industry-recognized key management practices to protect the confidentiality and integrity of sensitive/regulatory data both at rest and in transit.
- Data Classification & Handling (DCH)**
Enforce a standardized data classification methodology to objectively determine the sensitivity and criticality of all data and technology assets so that proper handling and disposal requirements can be followed.
- Embedded Technology (EMB)**
Provide additional scrutiny to reduce the risks associated with embedded technology, based on the potential damages posed from malicious use of the technology.
- Endpoint Security (END)**
Harden endpoint devices to protect against resolvable threats to those devices and the data those devices store, transmit and process.
- Human Resources Security (HRS)**
Execute sound hiring practices and ongoing personnel management to cultivate a cybersecurity & data privacy-minded workforce.
- Identification & Authentication (IAC)**
Enforce the concept of "least privilege" consistently across all systems, applications and services for individual, group and service accounts through a documented and standardized Identity and Access Management (IAM) capability.
- Incident Response (IRO)**
Maintain a viable incident response capability that trains personnel on how to recognize and report suspicious activities so that trained incident responders can take the appropriate steps to handle incidents, in accordance with a documented Incident Response Plan (IRP).
- Information Assurance (IAC)**
Execute an impartial assessment process to validate the existence and functionality of appropriate cybersecurity & data privacy controls, prior to a system, application or service being used in a production environment.
- Maintenance (MNT)**
Proactively maintain technology assets, according to current vendor recommendations for configurations and updates, including those supported or hosted by third-parties.
- Mobile Device Management (MDM)**
Implement measures to restrict mobile device connectivity with critical infrastructure and sensitive/regulatory data that limit the attack surface and potential data exposure from mobile device usage.
- Network Security (NET)**
Architect and implement a secure and resilient defense-in-depth methodology that enforces the concept of "least functionality" through restricting network access to systems, applications and services.
- Physical & Environmental Security (PES)**
Protect physical environments through layers of physical security and environmental controls that work together to protect both physical and digital assets from theft and damage.
- Data Privacy (PRD)**
Align data privacy practices with industry-recognized data privacy principles to implement appropriate administrative, technical and physical controls to protect regulated personal data throughout the lifecycle of systems, applications and services.
- Project & Resource Management (PRM)**
Operationalize a viable strategy to achieve cybersecurity & data privacy objectives that establishes cybersecurity as a key stakeholder within project management practices to ensure the delivery of resilient and secure solutions.
- Risk Management (RSK)**
Proactively identify, assess, prioritize and remediate risk through alignment with industry-recognized risk management principles to ensure risk decisions adhere to the organization's risk threshold.
- Secure Engineering & Architecture (SEA)**
Utilize industry-recognized secure engineering and architecture principles to deliver secure and resilient systems, applications and services.
- Security Operations (OPS)**
Execute the delivery of cybersecurity & data privacy operations to provide quality services and secure systems, applications and services that meet the organization's business needs.
- Security Awareness & Training (SAT)**
Foster a cybersecurity & data privacy-oriented workforce through ongoing user education about evolving threats, compliance obligations and secure workplace practices.
- Technology Development & Acquisition (TDA)**
Develop and/or acquire systems, applications and services according to a Secure Software Development Framework (SSDF) to reduce the potential impact of undetected or unaddressed vulnerabilities and design flaws.
- Third-Party Management (TPM)**
Execute Supply Chain Risk Management (SCRM) practices so that only trustworthy third-parties are used for products and/or service delivery.
- Threat Management (THR)**
Proactively identify and assess technology-related threats, to both assets and business processes, to determine the applicable risk and necessary corrective action.
- Vulnerability & Patch Management (VPM)**
Leverage industry-recognized Attack Surface Management (ASM) practices to strengthen the security and resilience systems, applications and services against evolving and sophisticated attack vectors.
- Web Security (WEB)**
Ensure the security and resilience of internet-facing technologies through secure configuration management practices and monitoring for anomalous activity.

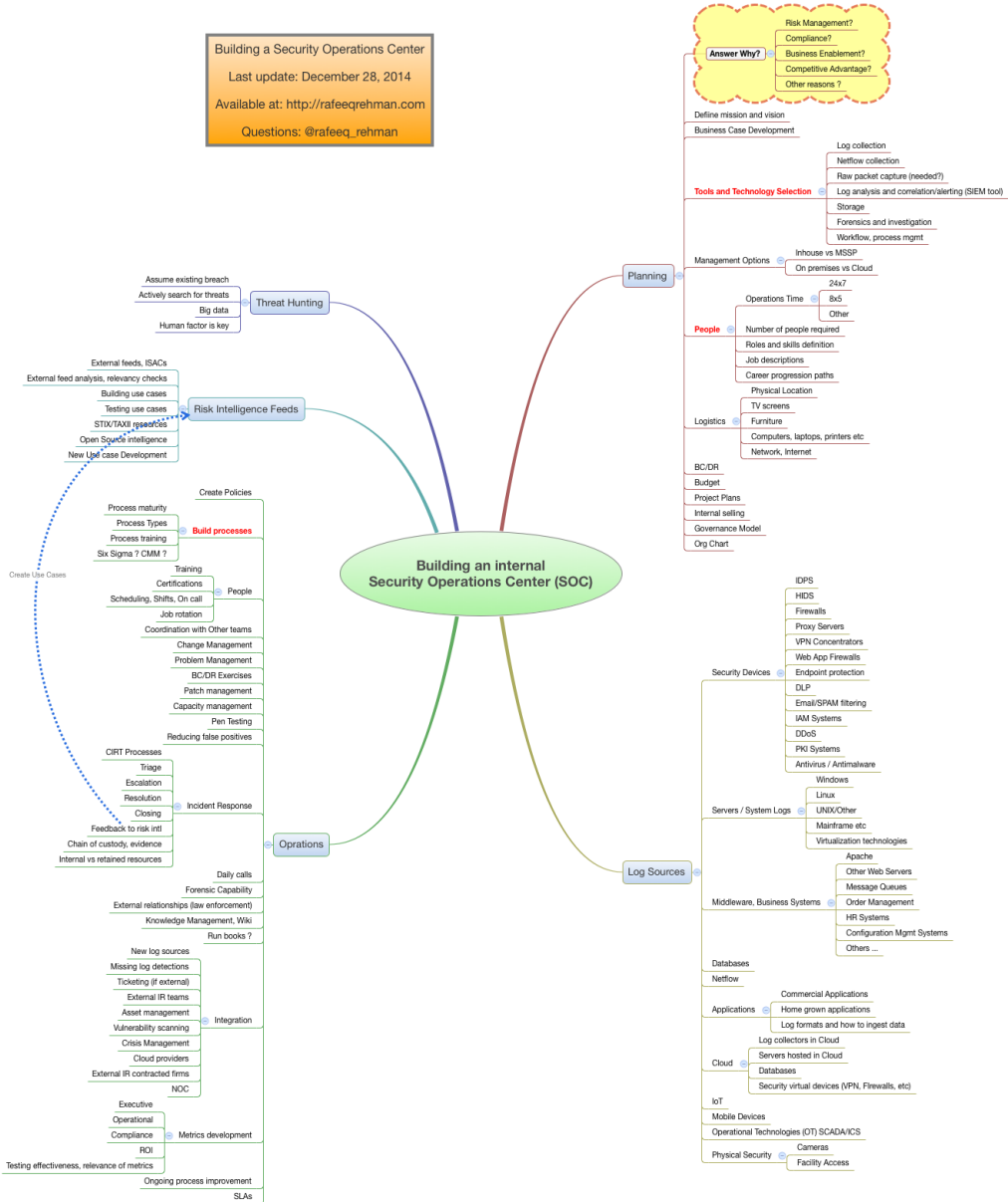
Copyright © 2023 by Secure Controls Framework Council, LLC (SCF Council). All rights reserved.

As you can see there is no shortage of available frameworks, and it is very easy to get lost around all of them frameworks. But you should know what your infrastructure security level is, what's required, and what are the things to fix. The SCF also aligned some of the critical design principles as well (33 line items, breakdowns you can download from their site, its freely available with an excel worksheet). These are the things for you to know and to figure out how best to fit it in your infrastructure management and therefore, choose a method on how to fix it, by following a framework.


COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Building a SOC by Rafeeq Rehman

Building a Security Operations Center
Last update: December 28, 2014
Available at: <http://rafeeqrehman.com>
Questions: @rafeeq_rehman



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



The above picture has the most mentioned domains in one picture, other pictures may be out there, but I haven't come across those yet, but tried to add most mindmaps and shared in the job aids folder as images or mindmeister files.

Rafeeq Rehman also has a CISO mindmap which could be very useful if you are willing to step up your career and want to understand these domains and enrich your understanding, you can download it from here: [Rafeeq Rehman | Cyber | Automation | Digital - Rafeeq Rehman - Personal](#)





CHAPTER

19

Generating and Consuming SOC Reports

THIS IS WHERE THE CLARITY OF THE CASE FILES MEETS THE CLOSURE, IF IT'S A FALSE ALARM, IF NOT, THEN THE RCA GETS INTO ACCOUNT, LATER ON REMEDIATED AND THE CASE GETS CLOSED WITH A WEALTH OF INCORPORATED DATA.

Security Operation Center (SOC) reports are documents that provide information and insights on the activities and performance of a SOC, such as the number, type, and severity of security incidents, the time and resources spent on detection and response, and the effectiveness and efficiency of the SOC's tools and processes. SOC reports can help SOC managers and stakeholders to evaluate and improve the SOC's capabilities and maturity, as well as to communicate and demonstrate the value and impact of the SOC to the organization.



Some of the best practices in generating and consuming SOC reports are:

- For SOC managers:
 - Define the purpose, scope, and audience of the SOC report. What are the main objectives and questions that the SOC report aims to address? What are the key metrics and indicators that the SOC report will use to measure and demonstrate the SOC's performance and value? Who are the intended recipients and users of the SOC report, and what are their expectations and needs?
 - Collect and analyze the relevant data and information from the SOC's tools and processes. Use various sources and methods, such as logs, alerts, incidents, tickets, surveys, feedback, and audits, to gather and validate the data and information that will support the SOC report's findings and conclusions. Use appropriate tools and techniques, such as dashboards, charts, graphs, and tables, to visualize and summarize the data and information in a clear and concise manner.
 - Write and format the SOC report in a professional and consistent way. Use a standard template and structure, such as executive summary, introduction, methodology, results, discussion, recommendations, and appendix, to organize and present the SOC report's content and layout. Use clear and concise language, avoid jargon and acronyms, and proofread and edit the SOC report for accuracy, completeness, and readability.
 - Distribute and share the SOC report with the relevant stakeholders and users. Use secure and appropriate channels and formats, such as email, web, or print, to deliver and disseminate the SOC report to the intended recipients and users. Obtain feedback and comments from the stakeholders and users, and address any questions, concerns, or issues that may arise from the SOC report.
- For SOC stakeholders and users:
 - Review and understand the SOC report's purpose, scope, and audience. What are the main objectives and questions that the SOC report aims to address? What are the key metrics and indicators that the SOC report uses to measure and demonstrate the SOC's performance and value? Who are the intended recipients and users of the SOC report, and what are their expectations and needs?
 - Evaluate and verify the SOC report's data and information. How reliable and valid are the data and information that support the SOC report's findings and conclusions? How well do the data and information reflect the actual activities and performance of the SOC? How relevant and

useful are the data and information for the SOC report's purpose and scope?

- Interpret and apply the SOC report's findings and conclusions. What are the main strengths and weaknesses of the SOC's capabilities and maturity? What are the main opportunities and challenges for the SOC's improvement and development? What are the main recommendations and actions that the SOC report suggests for the SOC and the organization?
- Communicate and collaborate with the SOC manager and other stakeholders and users. Provide feedback and comments on the SOC report, and ask questions, raise concerns, or suggest issues that may need further clarification or investigation. Share and discuss the SOC report's findings and conclusions with other stakeholders and users, and align and coordinate the implementation and follow-up of the SOC report's recommendations and actions.


Case Documentation

Case documentation is a complete record of incident response actions, which helps SOC teams use previous experiences and lessons learned to handle incidents better in the future. It also helps team members and stakeholders work together, communicate clearly, and improve continuously by finding areas for process improvement and boosting security operations. By keeping precise and thorough case documentation, SOC teams can improve their incident response skills and defend organizations better from changing cyberthreats by tuning the visibility requirements. Some of the process relations and group activity follows:

Pro-Tip

•when a breach is detected and showing up in the SIEM, DO NOT panic (also shows your fear, and it will spread across your peers), this is what you have been trained for, help out to facilitate, do not engage every available personnel for the incident response

1. Breach detection & alert notification.
2. Red & purple teams' engagement is mostly required in this case.
3. Blue teams' engagement on fine tuning the notification time, visibility increment requirement outline generated, further protection requirements generated and share with the SOC manager.
4. Associated TTP's & IoC's are generated and integrated.

- 
5. Investigation results accumulation.
 6. Investigation research accumulation.
 7. Pre-approved mitigation criteria.
 8. Threat intelligence accumulation & data validation.
 9. Severity triage, affected systems, parties, people, data analytics.
 10. Review quality of the case documentation.
 11. SOC manager – breach response & reporting to the stakeholders.
 12. Preventative measures, lessons learned, store KB for future use, possibility of automation for such investigation and remediation process.
 13. Document everything, sign-off for closure.

Difference Between TTP and IoC

Though mentioned earlier, TTP stands for **Tactics, Techniques, and Procedures**, which are the strategies and methods used by threat actors to conduct cyberattacks. TTPs focus on the overall behavior and patterns of the attackers, rather than specific artifacts or evidence.


IoC stands for **Indicators of Compromise**, which are observable and verifiable signs that a security incident has occurred or is occurring. IoCs are often derived from specific events or data points observed during an attack or intrusion, such as file hashes, IP addresses, domain names, or network traffic.

The main difference between TTP and IoC is that TTP is a **proactive** approach that tries to understand and anticipate the attacker's intentions and capabilities, while IoC is a **reactive** approach that tries to identify and analyze the current or previous threats based on specific evidence. TTPs can help organizations develop more effective and comprehensive defense strategies, while IoCs can help organizations detect and respond to threats faster and more accurately, as time passes, these KBs can be used for future and for faster and easier understanding of a threat, if that threat is previously observed and the mitigation playbook can be associated and updated, and the immediate resolution can be drawn, and the case will be closed if no remediation needs to be taken or any process is in place for automatic remediation or cleanup.

KPI's for a Security Operation Center

Key Performance Indicators (KPIs) are a way of measuring the success or failure of a business goal, function, or objective, and they provide actionable information on which decisions can be based. Here are some commonly used KPIs for a Security Operations Center (SOC):



- 
1. **Ingress:** Risk assessment for systems conveyed to SOC, and number of devices log shipped to SOC.
 2. **Occurrence:** Incident occurrence due to known vs. unknown vulnerability.
 3. **Threat Level:** Threat actor attribution (using threat intelligence). Thoroughness and accuracy of enterprise sweeping (check all information systems for indicators of compromise)
 4. **Incident Response Time:** These measures how quickly the SOC responds to a security incident.
 5. **Threat Detection Rate:** These measures how effectively the SOC is identifying threats. Time from detection to containment to eradication.
 6. **False Positive Rates:** This measures the accuracy of threat detection.
 7. **Mean Time to Resolve (MTTR):** These measures show how fast the organization can identify a security incident and provide a complete resolution. Number of incidents closed in one shift. Thoroughness of eradication (no recurrence of original or similar compromise).
 8. **Mean Time to Detect (MTTD):** This measures the time it takes for the organization to detect a security incident.
 9. **Impact:** Time to discover all impacted assets and users. Downtime for workers or duration of business outage per incident.
 10. **Number of Incidents Handled or Resolved:** This measures the effectiveness of the SOC's incident response and remediation efforts.
 11. **Avoidability** of incident (could the incident have been avoided with common security practices in place?). Monetary cost per incident. Losses accrued vs. losses prevented.

These are for your standard KPI's in a SOC, but you are not limited to anything, add as many KPI's as per your requirement, and as per your team constructions. Overdoing it will also have a negative impact, as your analysts will have faster burnouts.

Remember, the most effective way to develop meaningful KPIs is to start by identifying which security operations goals or functions are the most critical to the security operations program, and who is assigned for particular jobs. Suppose a number of analysts are assigned for inside threat events, and another team is for outside. Inside team can be divided into running 2 major tasks or activities for Windows systems and one for Linux based systems, but it also depends on your requirements, and availability of analysts. Also, these KPIs should be regularly reviewed and updated to ensure they continue to align with the organization's goals and the evolving threat landscape.

Benefits of SOC KPI's

While security operations may have similar goals, most security operations goals are less finite. Most security operations goals are more focused on positive or negative trends





over time than achieving a specific target. Let's discuss why KPIs are important, how to choose the best KPIs for a given organization, and how many KPIs are appropriate. Quality KPI's serve as a security program enabler and driver for continuous improvement. The threat landscape is a dynamic and ever-changing environment, and effective security operations programs require actionable information on which decisive action can be based. KPIs help ensure that a security operations program continues to remain effective and that any process or technology gaps are addressed appropriately. Most common KPI's are based on the following criteria:

- Analysts Skills.
- Process Success.
- Detection Success.
- Key Risk Findings.
- Workloads & its Distributions to L1, L2, L3.
- Mitigation Success.

The following list is intended to be used as a primer to inspire ideas to identify the most important KPIs for an organization:

PI	Why Do We Care?	Possible Measurements	Assessment of:
Number of devices being monitored	How many devices are being monitored? Is the number increasing or decreasing? Why?	Number of devices Number of devices / analyst	Workload
Total number of events	How many events are being handling? Is the number increasing or decreasing? Why? Are the current staffing levels adequate?	Number of events / hour (/ analyst) Number of events / day (/ analyst) Number of events / month (/ analyst) Number of events / year (/ analyst) Number of events / event type	Cost to value Key risks Workload
Number of events per device or host	How many events are received for each device or host?	Number of events per device or host / day	Detection success Key risks





	<p>Are there certain devices or hosts which are more prone to security issues, causing increased risk? Why?</p> <p>Are there certain devices or hosts which are more prone to false positive events? Why?</p>	<p>Number of events per device or host / month</p> <p>Number of events per device or host / year</p> <p>Number of events / device or host type</p> <p>Number of events / operating system type</p>	
Number of events per service or application	<p>How many events are received for each service or application?</p> <p>Are there certain services or applications which are more prone to security issues, causing increased risk? Why?</p> <p>Are there certain services or applications which are more prone to false positive events? Why?</p>	<p>Number of events / service</p> <p>Number of events / application</p>	<p>Detection success Key risks</p>
Number of events per account	<p>How many events are received for account?</p> <p>Are there certain accounts (users) which are more likely to perform risky behavior, leading to security events and increased risk? Why?</p>	<p>Number of events / account</p> <p>Number of events / user</p>	<p>Detection success Key risks</p>
Number of events per location	<p>How many events are received per geographic location, office, etc.?</p> <p>Are certain locations more prone to security events? Why?</p>	<p>Number of events / department</p> <p>Number of events / office</p> <p>Number of events / region</p>	<p>Key risks</p>



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



<p>Number of false positive alerts</p>	<p>How many false positive events are received? Is this acceptable? Can the number of false positive events be reduced? How?</p>	<p>Number of false positives / hour Number of false positives / day Number of false positives / month Number of false positives / year Percentage of events that are false positives</p>	<p>Detection success</p>
<p>Time to detection</p>	<p>How long is it taking your organization to detect a security event? Is this acceptable? Are there ways this time to detection can be reduced? How?</p>	<p>Measured in minutes, hours or days... Average time to detection Average time to detection / technology Average time to detection / event type Outliers</p>	<p>Detection success Process success</p>
<p>Time to resolution</p>	<p>How long is it taking your organization to resolve an actual security event? Is this acceptable? Are there process or technology improvements that can be made to reduce this time? What are they? Are additional staff or training required? How many staff or what additional training is required?</p>	<p>Measured in minutes, hours or days... Average time to resolution Average time to resolution / event type</p>	<p>Mitigation success Process success</p>



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



		Average time to resolution / resolution strategy Outliers	
Time to identify event as false positive	How long is it taking your organization to determine that an event is a false positive? Is this acceptable?	Measured in minutes, hours or days...	Analyst skills
	Are analysts spending too much time investigating false positives? Why?	Average time to identify	Process success
	Is additional training required? What kind?	Average time to identify / technology Average time to identify / event type Outliers	
Number of analysts assigned	How many analysts are being assigned to each event? Is it the proper number?	Average number of analysts / event	Analyst skills
	Are too many analysts being assigned to one event meaning that they are not available to respond to other events?	Average number of analysts / event type	Cost to value
	Why?	Average number of analysts (per level) / event	Workload
Escalation level	Are too few analysts being assigned to an event due to staff shortages?	Average number of analysts (per level) / event type	
	How many events are being escalated and to what level?	Average number of events / level	Analyst skills
	Are events being escalated too quickly or not soon enough? Why?	Average number of events / level / (time period)	Cost to value



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



	<p>Are there improvements to the escalation process that can make event handling more efficient? What are they?</p> <p>Is the training for each level sufficient to produce the desired skill level? If not, what additional training is required?</p>	<p>Escalation level / event type</p> <p>Escalation level / technology</p> <p>Average time (min or hours) to escalate</p>	<p>Process success</p>
Event source	<p>Are certain detection technologies more or less effective at detecting security events? Why?</p> <p>Are certain detection technologies more prone to false positives? Why?</p> <p>How often are users or analysts manually detecting an event before it is detected by a detection technology? Why?</p>	<p>Total number of events / technology</p> <p>Total number of events / technology / (time period)</p> <p>Total number of false positives / technology</p>	<p>Detection success Key risks</p>

Source: [SOAR-KPIs.pdf \(acadiatech.com\)](https://www.acadiatech.com/soar-kpis.pdf)

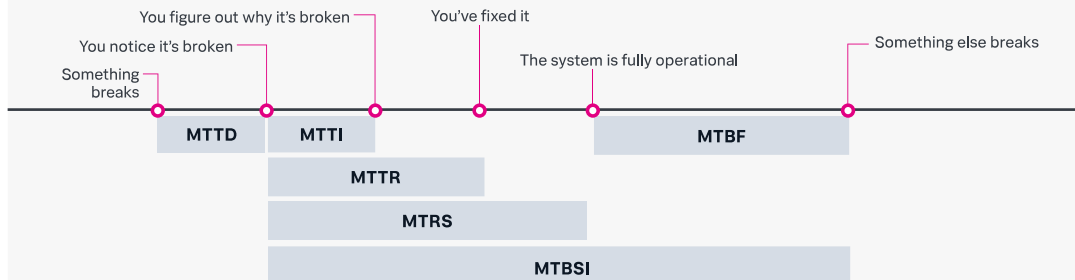
You will be doomed if your SIEM dashboard is not grouped based on locations, devices, infrastructures etc.



Failure Metrics Timeline

Failure Metrics Timeline

Common failure metrics measure various segments of the function-fail-repair-function cycle. Not depicted below are failure rate (average number of failures over a given period of time) and mean time to failure, or MTTF (estimated life of a system/component, generally for maintenance purposes).



Source: [SOC Metrics: Security Metrics & KPIs for Measuring SOC Success | Splunk](#)

- MTTI: Mean time to identify or investigate.
- MTRS: Mean time to restore service.
- MTBSI: Mean time to between system incidents.
- MTBF: Mean time before failure.
- MTTF: Mean time to failure.

Defining Success for Your Ideal Reporting Model

Source, a great article from Cyril Simonnet: [The Optimal Reporting Structure for Your SOC: Enabling Effective Security Operations | LinkedIn](#)

The "right" reporting structure for your SOC depends on your unique risk profile, corporate politics, leadership, and culture. But across any model, the hallmarks of success remain the same:

- The SOC has adequate resources and budget to meet operational demands. No skimping on what they need to get the job done!
- Security operations and detection content remain properly focused based on likely threats. Stay on target and ignore distractions!
- Visibility exists in the SOC's capabilities and gaps.

- The SOC retains autonomy over core technical functions while adhering to corporate standards.
- Collaboration between the SOC and CISO is fostered to create security alignment.
- Executive management has trust and confidence in the SOC's competence.

Rather than get distracted by abstract debates over organizational boxes and lines, focus on these tangible outcomes that demonstrate SOC effectiveness.



CHAPTER

20

Cybersecurity Tabletop Exercises

CONTINUOUS EXERCISING YOUR ACTIVITY WITHIN THE SOC HIERARCHY ENABLES DEPENDENCIES ON YOUR PEERS DATA COLLECTION REQUIREMENTS, MATERIALS PREPAREDNESS, COORDINATED EFFORT FOR CASE MANAGEMENT ETC. YOU ARE NOT MEANT TO DO EVERYTHING, TRUST YOUR PEERS, AND THEY WILL TRUST YOU AS WELL, WELL, DEFINITELY, IN TIME.

Conducting cybersecurity tabletop exercises is a valuable practice for organizations to test their incident response plans, enhance team collaboration, and improve overall cybersecurity preparedness. Here's a comprehensive guide on how to prepare for and conduct tabletop exercises, along with the desired results and awareness you want to achieve:



How to Prepare for Cybersecurity Tabletop Exercises

1. Define Objectives:

- Clearly outline the objectives of the tabletop exercise. Common objectives include testing incident response procedures, evaluating communication channels, and assessing team coordination.

2. Identify Scenarios:

- Select realistic and relevant scenarios based on potential cybersecurity threats and risks to your organization. Consider incidents such as ransomware attacks, data breaches, or phishing campaigns.

3. Build a Scenario Script:

- Develop a detailed scenario script that outlines the progression of the incident. Include information on how the incident is discovered, who is involved, and the potential impacts on the organization.

4. Engage Stakeholders:

- Identify key stakeholders who should participate in the exercise, including representatives from IT, security, legal, communications, and executive leadership.

5. Establish Ground Rules:

- Define the rules and parameters of the tabletop exercise, including whether it will be a full simulation or a discussion-based exercise. Clarify the roles and responsibilities of participants.

6. Prepare Materials:

- Gather all necessary materials, including the scenario script, communication templates, incident response plans, and any relevant documentation. Distribute these materials to participants in advance.

7. Schedule and Coordinate:

- Set a date and time for the tabletop exercise, ensuring that key participants can attend. Coordinate with facilitators and participants to ensure everyone is aware of their roles.



8. Facilitator Training:

- Train facilitators who will guide the exercise. Facilitators should understand the scenario, objectives, and expected outcomes, as well as how to manage the flow of the discussion or simulation.

How to Conduct Cybersecurity Tabletop Exercises

1. Introduction:

- Begin the exercise with an introduction, outlining the objectives, ground rules, and the scenario participants will be addressing.

2. Scenario Presentation:

- Present the scenario to participants, detailing the incident's unfolding events. Encourage participants to react as they would in a real-world situation.

3. Discussion and Decision-Making:

- Facilitate a discussion among participants as they make decisions and respond to the evolving scenario. Encourage open communication and collaboration.

4. Injects and Surprises:

- Introduce injects or surprises into the scenario to simulate unexpected developments or new information. This challenges participants to adapt their response strategies.

5. Documentation:

- Require participants to document their decisions, actions taken, and any lessons learned during the exercise. This documentation is valuable for post-exercise analysis.

6. Debrief Session:

- Conclude the exercise with a debrief session. Discuss what went well, areas for improvement, and lessons learned. Encourage participants to share insights and feedback.

7. Post-Exercise Analysis:

- Conduct a thorough analysis of the exercise outcomes. Evaluate the effectiveness of communication, decision-making, and coordination. Identify areas for improvement in processes, documentation, or team dynamics.

8. Actionable Recommendations:

- Generate actionable recommendations based on the lessons learned from the exercise. These recommendations should drive improvements in incident response plans, communication protocols, and overall cybersecurity posture.

Desired Results and Awareness

1. Improved Incident Response Planning:

- Identify gaps or weaknesses in the incident response plan and make necessary improvements.

2. Enhanced Communication and Coordination:

- Strengthen communication channels and coordination among different teams involved in incident response.

3. Increased Situational Awareness:

- Improve participants' ability to assess and respond to evolving situations by enhancing their situational awareness.

4. Team Building and Collaboration:

- Foster a collaborative and cohesive incident response team by providing opportunities for team members to work together effectively.

5. Adaptability and Flexibility:

- Test the team's ability to adapt to unexpected developments and demonstrate flexibility in response strategies.

6. Identifying Improvement Areas:

- Identify specific areas for improvement in processes, procedures, and technical capabilities.

7. Crisis Communication Skills:

- Enhance the organization's crisis communication skills by practicing communication during a simulated incident.

8. Executive Leadership Awareness:

- Increase awareness among executive leadership about the organization's cybersecurity preparedness and potential challenges.

9. Compliance Testing:

- Evaluate the organization's ability to comply with regulatory requirements and industry standards during a cybersecurity incident.

10. Continuous Improvement Culture:

- Instill a culture of continuous improvement by regularly conducting tabletop exercises and incorporating lessons learned into cybersecurity practices.

These exercises contribute to a more resilient cybersecurity posture and help teams refine their incident response capabilities.

Outcome of the Cybersecurity Tabletop Exercise

The outcome of a cybersecurity tabletop exercise is multi-faceted and serves several critical purposes in enhancing an organization's cybersecurity resilience. Here are key outcomes that organizations can expect from conducting cybersecurity tabletop exercises:

1. Identification of Weaknesses and Gaps:

- One of the primary outcomes is the identification of weaknesses and gaps in the organization's cybersecurity posture. This includes weaknesses in incident response plans, communication protocols, technical controls, and overall preparedness.

2. Improved Incident Response Planning:

- The exercise highlights areas for improvement in the incident response plan. Organizations can refine and update their plans based on the insights gained during the exercise, ensuring that they are better equipped to handle real-world incidents.

3. Enhanced Communication and Collaboration:

- Tabletop exercises facilitate improved communication and collaboration among different teams involved in incident response. Participants learn to share information effectively, coordinate actions, and work together cohesively during a simulated incident.

4. **Increased Situational Awareness:**

- Participants develop a heightened sense of situational awareness, learning to assess and respond to evolving scenarios. This outcome is crucial for effective decision-making and response in the face of a real cybersecurity incident.

5. **Team Building and Collaboration Skills:**

- The exercise serves as a team-building opportunity, allowing participants to work together, understand each other's roles, and build trust. This collaborative experience contributes to a more effective and resilient incident response team.

6. **Adaptability and Flexibility Testing:**

- Tabletop exercises test the team's ability to adapt to unexpected developments and demonstrate flexibility in response strategies. This outcome ensures that the organization's incident response capabilities can handle dynamic and evolving cyber threats.

7. **Identification of Improvement Areas:**

- The exercise identifies specific areas for improvement, not only in processes and procedures but also in technical capabilities. This outcome helps organizations prioritize and address weaknesses in their cybersecurity infrastructure.

8. **Crisis Communication Skills Enhancement:**

- Organizations enhance their crisis communication skills by practicing communication during a simulated incident. This includes communicating internally within the organization and externally with stakeholders, regulatory bodies, and the public.

9. **Executive Leadership Awareness:**

- Tabletop exercises increase awareness among executive leadership about the organization's cybersecurity preparedness and potential challenges. This heightened awareness can lead to better-informed decision-making and resource allocation.

10. Compliance Testing and Validation:

- The exercise serves as a test of the organization's ability to comply with regulatory requirements and industry standards during a cybersecurity incident. This outcome is crucial for maintaining compliance and avoiding potential legal and regulatory consequences.

11. Continuous Improvement Culture:

- Through regular tabletop exercises, organizations foster a culture of continuous improvement. Lessons learned from each exercise are used to refine and enhance cybersecurity practices, ensuring that the organization stays resilient in the face of evolving cyber threats.

12. Actionable Recommendations:

- Following the exercise, organizations generate actionable recommendations based on the lessons learned. These recommendations drive improvements in incident response plans, communication protocols, and overall cybersecurity posture.

In summary, it empowers SOC members to identify and address weaknesses, enhance collaboration, and continuously improve their cybersecurity defenses to effectively mitigate and respond to cyber threats.

If you look at the big picture, the collaboration I am talking about is to have triangular synergy with the CIO, CTO & the CISO. If the ego comes in the play and professionalism is absent in either of the three, the SOC goes nowhere, even if powerful team members are present.

There are some exercises available for you to checkout, the most prominent ones are:

1. [CTEP Package Documents | CISA](#)
2. [Cybersecurity Tabletop Exercise Examples, Best Practices, and Considerations | RSI Security](#)
3. [Tabletop Exercises \(TTX\) \(cisecurity.org\)](#)
4. [Implementing Your First Cybersecurity Tabletop Exercise - JumpCloud](#)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER





CHAPTER


21

Artificial Intelligence in Cybersecurity Operation Center

AN AI BASED SYSTEM CAN DO BOTH, INFILTRATE BY SCANNING AND IDENTIFYING BREAKS IN YOUR NETWORK, AND AS WELL THE OTHER SIDE, CAN LAY OUT HONEYPOTS TO TRAP AND TRACE THE SAME FUNCTIONS, AND REPORT TO SOC PROCESSES FOR INTERVENTION.

AI is a powerful tool that can enhance the capabilities and efficiency of security teams, but it also poses new challenges and risks. Therefore, it is important to design, deploy, and use AI securely, and to be aware of the potential threats that AI can enable or amplify, such as adversarial attacks, deepfakes, or automated exploits.






Increase in AI adoption and expansion, many organizations are evaluating whether artificial intelligence can help improve business operations that normally require human intelligence, such as analyzing vast amounts of data, managing the increasing complexity of environments, and as a powerful tool for implementing cybersecurity strategies to protect business-critical elements like customer data and other sensitive information and in future analytics for threat hunting, threat engineering, detection engineering etc.

While the full extent and implications of AI capabilities within the cybersecurity industry are not yet understood, here is a simplified overview of common problem areas in which AI-powered systems could show promising results:

1. Increase efficiency.
2. Improve accuracy.
3. Improve threat detection.
4. Improve scalability.
5. Improve integration capabilities which produces actionable results.
6. Effective location identification of threats bounced or generated from.
7. OTC cost of the AI reduces overall costs for data mapping.
8. Automated responses to security threats.
9. Accelerate incident investigation.
10. Provide predictive threat prevention.
11. Determine root cause.
12. Data & input validation of the data from different sources.
13. Combining OSINT data into one glass view of the treat vectors.

Security Teams Need AI to Help Them Find Threats

AI can help security teams detect threats by using sophisticated algorithms and predictive intelligence to analyze data, identify patterns and anomalies, and find and stop attacks before they cause damage. AI can also help security teams manage their workload, reduce false positives, and learn from past incidents. Some examples of how AI can help security teams detect threats are:

- AI can hunt down malware by comparing files and traffic against known malicious signatures or behaviors, or by using machine learning to classify new or unknown malware based on its features.
 - AI can run pattern recognition to detect phishing schemes, ransomware, credential stuffing, and domain hijacking by looking for indicators of compromise, such as suspicious URLs, attachments, or login attempts.
- 

- AI can find and thwart attacks by using anomaly detection to spot deviations from normal network or user activity, such as unusual data transfers, connections, or commands.
- AI can prevent future threats by learning from past incidents and identifying patterns in data that may indicate a potential attack before it happens, such as correlations, trends, or outliers.

Limitations of AI in SOC

Some of the limitations of AI in SOC that need to be addressed by SOC managers, analysts, and developers, as well as other stakeholders such as governments, businesses, researchers, and civil society. AI is a powerful and evolving technology that can offer many benefits and challenges for SOC, and it requires constant monitoring, evaluation, and improvement.

AI in SOC (Security Operations Center) is a valuable tool for detecting and responding to cyber threats, but it also has some limitations that need to be addressed. Some of the limitations of AI in SOC are:

- **Data quality and availability:** AI relies on large and diverse data sets to learn and improve its performance, but data quality and availability may vary depending on the source, format, and context of the data. Poor or insufficient data can lead to inaccurate or biased results or reduce the effectiveness of AI models.
- **Human factors:** AI cannot replace human judgment, expertise, and intervention in SOC, but rather complement and augment them. However, human factors such as trust, communication, collaboration, and ethics may affect how AI is perceived, used, and supervised by SOC analysts and managers. For example, human operators may over-trust or under-trust AI, fail to understand or explain AI outputs, or misuse or abuse AI for malicious purposes.
- **Adversarial attacks:** AI may be targeted by malicious actors who seek to compromise, manipulate, or deceive AI systems or their users. For example, attackers may use adversarial examples, deepfakes, or poisoning attacks to fool or corrupt AI models, or exploit their vulnerabilities or weaknesses.
- **Regulatory and ethical challenges:** AI may pose regulatory and ethical challenges for SOC, such as privacy, security, accountability, fairness, and transparency. For example, AI may collect, process, or share sensitive or personal data without proper consent, security, or governance, or produce outcomes that are unfair or discriminatory to certain groups or individuals.

Ensure the Transparency and Explainability of AI Outputs in SOC

AI outputs in CSOC (cybersecurity operations center) are the results or decisions produced by AI systems that are used to detect and respond to cyber threats.

Transparency and explainability of AI outputs in SOC are important for building trust, accountability, and compliance among various stakeholders, such as SOC analysts, managers, customers, regulators, and auditors. Some of the ways to ensure the transparency and explainability of AI outputs in SOC are:

- **Data governance:** This involves establishing clear policies and procedures for data collection, processing, storage, and sharing, and ensuring compliance with relevant laws and regulations. Data governance can help ensure that the data used by AI systems is accurate, fair, and representative, and that the data sources, quality, and limitations are disclosed and documented.
- **Algorithmic transparency:** This involves making the AI systems and their outcomes understandable and explainable to users, regulators, and developers, and allowing for scrutiny and challenge. Algorithmic transparency can help ensure that the AI systems are designed and developed with ethical and social considerations, and that the functioning mechanisms, assumptions, and limitations are disclosed and documented.
- **User control:** This involves giving users the ability to access, correct, delete, or withdraw their data, and obtaining their informed consent for data use. User control can help ensure that the users have the right to know, understand, and influence how their data is used by AI systems, and that the users can opt out or appeal the AI outputs if they disagree or are dissatisfied.
- **Human oversight:** This involves ensuring that human judgment, expertise, and intervention are involved in the development, deployment, and use of AI systems. Human oversight can help ensure that the AI systems are aligned with human values and goals, and that the human operators can monitor, evaluate, and correct the AI outputs if needed.
- **Plain language explanations:** This involves providing clear and concise explanations of how the AI systems work, why they produce certain outputs, and what the implications and consequences are. Plain language explanations can help ensure that the AI outputs are understandable and interpretable by users, regardless of their technical expertise, and that the users can make informed and rational decisions based on the AI outputs.

Possibilities of Implementing AI in SOC

Implementing AI for your organization's security can be a complex and challenging task, but also a rewarding one. AI can help you enhance your security posture, detect and prevent threats, and automate tedious tasks. Here are some steps you can take to implement AI for your organization's security:

- Align AI strategy with business and security objectives. Before embarking on AI implementation, you should define your goals, scope, and expected outcomes. You should also identify the key use cases and scenarios where AI can add value to your security operations.
- Invest in skilled AI talent. AI requires specialized skills and expertise, such as data science, machine learning, and security engineering. You should either hire or train your staff to acquire these skills, or partner with external vendors or consultants who can provide them.
- Thoroughly evaluate AI solutions. There are many AI solutions available in the market, but not all of them are suitable for your needs. You should conduct a thorough assessment of the features, capabilities, performance, and reliability of the AI solutions you are considering. You should also test them in your environment and compare them with your existing tools and processes.
- Establish a robust data governance framework. Data is the fuel for AI, and you need to ensure that you have enough, high-quality, and relevant data to feed your AI systems. You should also ensure that your data is secure, compliant, and ethical. You should establish clear policies and procedures for data collection, storage, access, sharing, and deletion.
- Implement strong security measures for AI infrastructure. AI systems are not immune to cyberattacks, and you need to protect them from malicious actors. You should implement strong security measures for your AI infrastructure, such as encryption, authentication, authorization, monitoring, and auditing. You should also update your AI systems regularly and patch any vulnerabilities.

Challenges of Using AI in SOC

AI in cybersecurity can offer many benefits, such as automating threat detection and response, improving risk assessment and compliance, and enhancing cost management. However, AI also poses some challenges and risks, such as:

- **Lack of transparency and explainability:** AI systems often operate as black boxes, making it difficult to understand how they reach their decisions or outcomes. This can lead to trust issues, ethical dilemmas, and legal liabilities.
- **Overreliance on AI:** AI systems are not infallible, and they may make mistakes or fail to account for all possible scenarios. Relying too much on AI can reduce human vigilance, expertise, and intervention, and create a false sense of security.
- **Bias and discrimination:** AI systems may reflect or amplify the biases and prejudices of their data, developers, or users. This can result in unfair or inaccurate outcomes, such as misidentifying or discriminating against certain groups or individuals.
- **Vulnerability to attacks:** AI systems may be targeted by malicious actors who seek to compromise, manipulate, or deceive them. For example, attackers may use adversarial examples, deepfakes, or poisoning attacks to fool or corrupt AI systems.
- **Lack of human oversight:** AI systems may act autonomously or unpredictably, without sufficient human supervision or control. This can raise ethical, legal, and social issues, such as accountability, responsibility, and consent.
- **High cost:** AI systems may require significant resources, such as data, computing power, and talent, to develop, deploy, and maintain. This can create barriers to entry, widen the digital divide, and increase the risk of cyberattacks.
- **Privacy concerns:** AI systems may collect, process, and share large amounts of personal or sensitive data, without proper consent, security, or governance. This can expose individuals or organizations to data breaches, identity theft, or surveillance.

Common Pitfalls of AI Performance Optimization

AI performance optimization is the process of improving the efficiency, accuracy, and reliability of AI systems. However, it can also involve some challenges and pitfalls that can hinder the desired outcomes. Some of the common pitfalls of AI performance optimization are:

- **Poor architecture choices:** Choosing the wrong architecture for your AI system can lead to poor performance, scalability, and manageability. You should consider the complexity, accuracy, interpretability, scalability, and robustness of


the available architectures, and select the one that matches your problem characteristics and performance criteria.

- **Inaccurate or insufficient training data:** The quality and quantity of your training data will determine the quality and accuracy of your AI system. You should ensure that your data is clean, relevant, and representative of your problem domain. You should also perform data cleaning, preprocessing, and augmentation to remove noise, outliers, missing values, and biases from your data.
- **Lack of AI explainability:** AI systems can be difficult to understand and interpret, especially when they use complex or black-box models. This can lead to a lack of trust, accountability, and transparency in your AI system. You should use methods and tools that can provide explanations for your AI system's decisions, such as feature importance, saliency maps, or counterfactual examples.
- **Difficulty in reproducing results:** AI systems can be sensitive to changes in data, parameters, or environments, which can cause inconsistencies or discrepancies in the results. This can make it hard to validate, verify, or compare your AI system's performance. You should use rigorous methods and standards to document, share, and reproduce your AI system's results, such as code versioning, data provenance, or reproducibility frameworks.
- **Ethical and social challenges:** AI systems can have ethical and social implications, such as privacy, fairness, bias, or human dignity. These can affect the acceptance, adoption, and impact of your AI system. You should consider the ethical and social aspects of your AI system and follow the principles and guidelines that can ensure the responsible and beneficial use of AI, such as human values, human agency, or human oversight.

Ensure the Fairness of the AI System


Ensuring the fairness of your AI system is a complex and important task that requires careful consideration of the data, models, algorithms, and outcomes of your AI system. Fairness is not only a legal and ethical obligation, but also a business and social benefit, as it can enhance the trust, acceptance, and impact of your AI system. Here are some general steps that you can take to ensure the fairness of your AI system:

- Define what fairness means for your AI system and its stakeholders. Fairness is a context-dependent and multi-dimensional concept that can have different interpretations and implications depending on the problem domain, the data



sources, the target groups, and the intended outcomes of your AI system. You should consult with your stakeholders, including your customers, employees, regulators, and the public, to understand their expectations, needs, and values, and to define the fairness criteria and metrics that are relevant and appropriate for your AI system.


- Assess the potential sources and impacts of bias and discrimination in your AI system. Bias and discrimination can arise at any stage of the AI lifecycle, from data collection and processing to model development and deployment, to outcome evaluation and feedback. You should identify and analyze the potential sources and impacts of bias and discrimination in your AI system, such as data quality, representativeness, and diversity, model complexity, accuracy, and explainability, algorithmic assumptions, parameters, and objectives, and outcome fairness, accountability, and transparency. You should also consider the potential direct and indirect harm that your AI system could cause to individuals or groups, such as privacy violations, dignity infringements, or opportunity losses.
- Implement appropriate measures and techniques to mitigate bias and discrimination in your AI system. There are various measures and techniques that you can use to mitigate bias and discrimination in your AI system, depending on the type, level, and severity of the bias and discrimination, and the trade-offs and constraints that you face. Some of the common measures and techniques are:
 - Data preprocessing: This involves applying methods and tools to clean, augment, balance, or anonymize your data before feeding it to your AI system, to reduce noise, outliers, missing values, or biases in your data.
 - Model regularization: This involves applying methods and tools to constrain, simplify, or regularize your model during the training process, to reduce overfitting, underfitting, or complexity in your model.
 - Algorithmic debiasing: This involves applying methods and tools to modify, adjust, or optimize your algorithm during or after the training process, to reduce unfairness, discrimination, or bias in your algorithm.
 - Outcome postprocessing: This involves applying methods and tools to evaluate, correct, or explain your outcomes after the inference process, to reduce unfairness, discrimination, or bias in your outcomes.

- 
- Monitor and evaluate the fairness of your AI system regularly and continuously. Fairness is not a static or one-time property, but a dynamic and ongoing process that requires constant monitoring and evaluation. You should collect and analyze feedback and data from your AI system deployment and use them to measure and evaluate the fairness of your AI system, using the criteria and metrics that you defined. You should also identify and address any issues, errors, or changes that may affect the fairness of your AI system, such as data drift, concept drift, or model degradation. You should update your AI system with new data, features, or algorithms to keep it fair and accurate.

Examples of AI Bias and Discrimination in SOC

SOC stands for Cybersecurity Operations Center, which is a centralized unit that monitors, detects, and responds to cyber threats and incidents. AI systems can be used to enhance the capabilities and efficiency of SOC, such as by automating tasks, analyzing data, or providing insights. However, AI systems can also introduce bias and discrimination in SOC, which can affect the security and privacy of users, as well as the trust and accountability of SOC. Here are some examples of AI bias and discrimination in SOC from different domains and applications:

- **Incident response:** AI systems can be used to assist SOC analysts in responding to cyber incidents, such as by providing recommendations, actions, or solutions. However, if the data or algorithms are biased, they can lead to inaccurate or inappropriate incident response that affects the recovery and resilience of users. For example, a study found that an AI system used to prioritize cyber incidents was biased against certain types of incidents, such as phishing or ransomware, as it used features that were more common in other types of incidents, such as denial-of-service or malware.
- **Threat intelligence:** AI systems can be used to collect, analyze, and share information about cyber threats, such as their sources, methods, or targets. However, if the data or algorithms are biased, they can lead to incomplete or misleading threat intelligence that affects the awareness and preparedness of users. For example, a report found that an AI system used to generate threat reports was biased against certain regions, such as Africa or Asia, as it used sources that were more focused on other regions, such as Europe or North America.
- **User behavior analytics:** AI systems can be used to monitor and analyze the behavior of users on networks, devices, or applications, and detect anomalies, risks, or violations. However, if the data or algorithms are biased, they can lead to



unfair or intrusive user behavior analytics that affect the access and usability of users. For example, a study found that an AI system used to identify insider threats was biased against certain user groups, such as contractors or remote workers, as it used features that were more common in regular employees, such as working hours or location.

To prevent or mitigate AI bias and discrimination in SOC, it is important to ensure that the data, algorithms, and objectives of AI systems are fair, transparent, and accountable, and that the stakeholders, including the developers, analysts, and users, are involved and informed in the AI development and deployment process.


Algorithmic Debiasing

Algorithmic debiasing is the process of reducing or eliminating unfairness, discrimination, or bias in AI algorithms, models, or outcomes. There are many tools available for algorithmic debiasing, but one of the most comprehensive and extensible ones is the AI Fairness 360 (AIF360) toolkit by IBM. AIF360 is an open-source library that contains techniques developed by the research community to help detect and mitigate bias in machine learning models throughout the AI application lifecycle. AIF360 is available in both Python and R, and supports various types of bias mitigation methods, such as data preprocessing, model regularization, algorithmic debiasing, and outcome postprocessing. AIF360 also provides interactive web demos, tutorials, notebooks, and videos to help users learn and apply the toolkit. You can find more information and resources about AIF360 on its website or GitHub repository. [AI Fairness 360 \(ibm.com\)](https://aif360.github.io/)

Mitigate the Risks of AI in SOC

There are several strategies and measures that we can take to mitigate the risks of AI in cybersecurity, such as:

- **Data governance:** We can use effective data governance to help ensure that data is properly classified, protected, and managed throughout its life cycle. This can help prevent model poisoning attacks, protect data security, maintain data hygiene, and ensure accurate outputs.
- **Threat-modelling:** We can use threat-modelling techniques to identify and prioritize the potential threats and vulnerabilities of AI systems, and design appropriate countermeasures and controls.
- **Access controls:** We can use access controls to limit who can access, modify or influence the AI systems, data and outputs, and monitor and audit the activities of authorized users.

- 
- **Encryption and steganography:** We can use encryption and steganography to protect the confidentiality and integrity of data and models and prevent unauthorized access or tampering.
 - **End-point security, or user and entity behavior analytics:** We can use end-point security or user and entity behavior analytics to detect and respond to anomalous or malicious behaviors of users or devices that interact with AI systems.
 - **Vulnerability management:** We can use vulnerability management tools to scan, test and patch the AI systems and components, and reduce the exposure to known or unknown exploits.
 - **Security awareness:** We can use security awareness programs to educate and train the users and developers of AI systems on the best practices and ethical principles of AI security and foster a culture of responsibility and accountability.

Emerging Trends in AI Security

Some emerging trends in AI security are:



- **AI-based threat detection:** This involves using machine learning algorithms to analyze large amounts of data and identify patterns that may indicate a potential threat. For example, AI can hunt down malware, detect phishing schemes, and find and thwart attacks by using anomaly detection.
- **Behavioral analytics:** This involves using AI to monitor and understand the behavior of users, devices, and networks, and detect any deviations or anomalies that may signal a compromise or an attack. For example, AI can run pattern recognition to spot credential stuffing, domain hijacking, or insider threats.
- **Cybersecurity automation:** This involves using AI to automate and streamline various cybersecurity tasks, such as threat hunting, incident response, vulnerability management, and risk assessment. For example, AI can provide autonomous remediation, behavioral analysis, real-time forensics, and predictive intelligence.
- **AI-powered authentication:** This involves using AI to enhance the security and convenience of authentication methods, such as biometrics, multi-factor authentication, and behavioral authentication. For example, AI can use facial recognition, voice recognition, or keystroke dynamics to verify the identity of users.

- **Adversarial machine learning:** This involves using AI to attack or defend against other AI systems, by exploiting their weaknesses or enhancing their strengths. For example, attackers may use adversarial examples, deepfakes, or poisoning attacks to fool or corrupt AI systems, while defenders may use robustness testing, encryption, or steganography to protect or hide AI systems.
- **AI in IoT security:** This involves using AI to secure the growing number of connected devices, such as smart home gadgets, industrial sensors, and wearable devices, that form the Internet of Things (IoT). For example, AI can provide network monitoring, device management, data protection, and threat prevention for IoT devices.
- **Cyber threat intelligence:** This involves using AI to collect, analyze, and share information about current or emerging cyber threats, such as threat actors, attack vectors, indicators of compromise, and mitigation strategies. For example, AI can provide contextualized and actionable intelligence, such as threat profiles, attack trends, or risk scores.


Examples of AI solutions for the SOC

AI solutions for the SOC are applications or systems that use artificial intelligence to enhance the capabilities and efficiency of the cybersecurity operations center. Some examples of AI solutions for the SOC are:

- **AI-powered threat detection and response:** These solutions use AI techniques, such as machine learning, natural language processing, or computer vision, to monitor, analyze, and respond to cyberthreats and incidents in real time. They can help SOC analysts to identify and prioritize the most critical alerts, automate tasks, and provide recommendations or solutions. For example, [IBM QRadar Advisor with Watson](#) is an AI solution that uses cognitive reasoning to investigate security incidents and provide actionable insights.
- **AI-powered threat intelligence and analytics:** These solutions use AI techniques, such as data mining, statistical analysis, or deep learning, to collect, process, and share information about cyberthreats, such as their sources, methods, or targets. They can help SOC analysts to gain situational awareness, understand the threat landscape, and anticipate future attacks. For example, [Recorded Future](#) is an AI solution that uses natural language processing and machine learning to provide threat intelligence from various sources, such as the web, social media, or dark web.

- 
- 
- **AI-powered user behavior analytics and insider threat detection:** These solutions use AI techniques, such as anomaly detection, behavioral modeling, or biometrics, to monitor and analyze the behavior of users on networks, devices, or applications, and detect anomalies, risks, or violations. They can help SOC analysts to prevent or mitigate insider threats, such as data leakage, sabotage, or fraud. For example, Securonix is an AI solution that uses machine learning and big data analytics to provide user behavior analytics and insider threat detection.

There are many AI-based security products that can help organizations protect their data and systems from cyber threats. Some of them are:

- **Darktrace:** A versatile platform that uses self-learning AI to neutralize novel threats, such as ransomware, insider attacks, and IoT breaches.
 - **CrowdStrike:** A cloud-native platform that uses AI to monitor user endpoint behavior and prevent sophisticated attacks, such as nation-state intrusions, supply chain compromises, and zero-day exploits.
 - **SentinelOne:** A platform that uses AI to provide advanced threat-hunting and incident response capabilities, such as autonomous remediation, behavioral analysis, and real-time forensics.
 - **Check Point Software:** A platform that uses AI to provide network monitoring and security, such as firewall, VPN, threat prevention, and cloud security.
 - **Fortinet:** A platform that uses AI to prevent zero-day threats, such as malware, botnets, and phishing, by using deep learning and sandboxing technologies.
 - **Zscaler:** A platform that uses AI to provide data loss prevention, such as encryption, policy enforcement, and anomaly detection, for cloud-based applications and services.
 - **Trellix:** A platform that uses AI to provide continuous monitoring and security for complex IT environments, such as data centers, edge computing, and IoT devices.
 - **Vectra AI:** A platform that uses AI to provide hybrid attack detection, investigation, and response, such as network traffic analysis, threat intelligence, and automated response.
- 

- **Cybereason:** A platform that uses AI to defend against MalOps, which are coordinated and malicious operations that target multiple endpoints, users, and networks.
- **Tessian:** A platform that uses AI to protect against email-based threats, such as phishing, spear phishing, and business email compromise, by analyzing human behavior and communication patterns.

Ethical Use of AI in SOC

The ethical use of AI in SOC is the use of AI systems that respect the values, rights, and interests of the stakeholders involved in or affected by the cybersecurity operations center, such as the developers, analysts, users, and the public. To ensure the ethical use of AI in SOC, we can follow some general steps, such as:

- Establish clear and transparent policies and guidelines for the development, deployment, and evaluation of AI systems in SOC, based on the principles and standards of ethical AI, such as fairness, accountability, transparency, and human dignity.
- Involve and consult with the stakeholders in the design, implementation, and oversight of AI systems in SOC, and ensure that they are informed and empowered to participate in the decision-making and feedback processes.
- Monitor and audit the performance and impact of AI systems in SOC, and identify and address any issues, errors, or risks that may arise, such as bias, discrimination, privacy, security, or reliability.
- Review and update the AI systems in SOC regularly and continuously, and incorporate new data, features, or algorithms to improve their accuracy, efficiency, and fairness.

Offensive AI Tools

Artificial intelligence driven offensive tools are used to automate or enhance cyberattacks, such as generating phishing emails, exploiting vulnerabilities, or even creating deepfakes.

SOC can benefit from AI-driven offensive tools in several ways, such as:

- **Simulating attacks:** SOC can use AI-driven offensive tools to test the security posture of their own network and systems and identify potential weaknesses or

gaps. This can help them improve their own defenses and resilience against real attacks and gain real visibility.

- **Gaining intelligence:** SOC can use AI-driven offensive tools to gather information about their adversaries as well, such as their capabilities, intentions, strategies, and targets. This can help SOC anticipate and counter adversary movement, and gain advantage in the cyber domain.
- **Conducting operations:** SOC can use AI-driven offensive tools to launch or support cyber operations against their adversaries, such as disrupting, degrading, or destroying their assets, networks, or data. This can help them achieve their objectives and deter future attacks if so wanted intentionally, although this type mentality is dangerous for the team, and should be avoided. If you are in a position where you are a part of state sponsored activities, and offensive tools are developed or used, then you should rethink your future.

SOC need to ensure the ethical use of AI-driven offensive tools by following best practices, such as:

- **Establishing clear guidelines and policies:** SOC should define the scope, purpose, and principles of using AI-driven offensive tools, and communicate them to all relevant stakeholders. They should also monitor and audit the compliance and effectiveness of these guidelines and policies and update them as needed. One misunderstood steps or exposed identities, or origination country exposure could ruin very cautiously built relationship with countries.
- **Ensuring accountability and transparency:** SOC should be able to explain the rationale, methods, and outcomes of using AI-driven offensive tools, and provide evidence of their validity and reliability. They should also be able to identify and report any errors, risks, or harm that may arise from their use, and take corrective actions accordingly.
- **Respecting human rights and values:** SOC should respect the dignity, privacy, and autonomy of the individuals and groups that may be affected by their use of AI-driven offensive tools, and avoid any discrimination, exploitation, or harm. They should also consider the social and ethical implications of their use, and balance them with the security and strategic objectives.
- **Seeking external input and feedback:** SOC should consult with experts, peers, and stakeholders from different disciplines, sectors, and backgrounds, to gain diverse perspectives and insights on the ethical use of AI-driven offensive tools. They should also solicit feedback from the users and beneficiaries of their use and incorporate their views and preferences.

Privacy and Confidentiality of Data Used by AI Systems

Privacy and confidentiality of data used by AI systems are important issues that require careful attention and solutions. Some of the possible ways to ensure them are:

- **Data governance:** This involves establishing clear policies and procedures for data collection, processing, storage, and sharing, and ensuring compliance with relevant laws and regulations.
- **Data hygiene:** This involves collecting only the data types necessary to create the AI, keeping the data secure, and maintaining the data only for as long as needed.
- **Data sets:** This involves building AI using accurate, fair, and representative data sets, and avoiding or correcting any biases or errors in the data. Do validate inputs before using it.
- **User control:** This involves giving users the ability to access, correct, delete, or withdraw their data, and obtaining their informed consent for data use.
- **Algorithmic transparency:** This involves making the AI systems and their outcomes understandable and explainable to users, regulators, and developers, and allowing for scrutiny and challenge.
- **Encryption and steganography:** This involves protecting the confidentiality and integrity of data and models, and preventing unauthorized access or tampering.
- **Access controls:** This involves limiting who can access, modify, or influence the AI systems, data, and outputs, and monitoring and auditing the activities of authorized users.
- **Vulnerability management:** This involves scanning, testing, and patching the AI systems and components, and reducing the exposure to known or unknown exploits.
- **Security awareness:** This involves educating and training the users and developers of AI systems on the best practices and ethical principles of AI security and fostering a culture of responsibility and accountability.

Legal and Regulatory Frameworks for AI Security

AI security is a complex and evolving field that requires coordination and cooperation among various stakeholders, such as governments, businesses, researchers, and civil society. There are different legal and regulatory frameworks for AI security in different

regions and countries, each reflecting their own values, priorities, and challenges. Some of the examples are:

- **The EU Artificial Intelligence Act:** This is a comprehensive and risk-based regulation that aims to ensure that AI systems are trustworthy, safe, and respect fundamental rights and values. The act proposes to ban or limit certain high-risk applications of AI, such as mass surveillance, social scoring, or biometric identification, and to impose obligations on providers and users of AI systems, such as transparency, human oversight, and quality assurance.
- **The US AI Bill of Rights:** This is a set of principles and guidelines that seeks to promote the ethical and responsible development and use of AI in the US. The bill of rights covers topics such as privacy, security, accountability, fairness, and human dignity, and calls for the establishment of a national AI commission to oversee and regulate AI activities.
- **The UK AI Strategy:** This is a framework that aims to establish the UK as an “AI superpower” by fostering innovation, growth, and public trust in AI. The strategy focuses on four pillars: research and development, skills and talent, adoption and transformation, and governance and ethics. The strategy also proposes to create a new AI regulatory body to ensure compliance with existing and future laws.
- **The Singapore Model AI Governance Framework:** This is a voluntary and non-binding framework that provides practical guidance and best practices for organizations to implement AI governance and ethics. The framework covers aspects such as human involvement, explainability, data quality, security, and accountability, and encourages organizations to conduct self-assessments and disclose their AI policies to stakeholders.
- **The China Administrative Measures for Generative Artificial Intelligence Services:** This is a draft regulation that aims to ensure that content created by generative AI is consistent with social order and morals, avoids discrimination, is accurate, and respects intellectual property. The regulation requires providers and users of generative AI services to obtain licenses, conduct audits, and label the content as AI-generated.

These are some of the legal and regulatory frameworks for AI security that are currently in place or under development in different regions and countries. However, there are many more initiatives and proposals that address different aspects of AI security, such as data protection, consumer protection, cybersecurity, human rights, and international

cooperation. AI security is a dynamic and evolving field, and it requires constant monitoring, evaluation, and improvement.

Measure ROI of AI in SOC

Measuring the ROI of AI in security can be a challenging task, as it involves quantifying the benefits and costs of AI solutions in a complex and dynamic environment. However, it is also an important task, as it can help you justify your AI investments, optimize your AI performance, and align your AI strategy with your business and security objectives.

There are different methods and metrics that you can use to measure the ROI of AI in security, depending on your specific use cases and goals. Some of the common methods and metrics are:

- **Hard ROI:** This is the traditional financial ratio of the net gain or loss from AI investments relative to their total cost. It can be calculated by subtracting the total cost of AI (including development, deployment, maintenance, and operational costs) from the total value of AI (including revenue increase, cost savings, productivity gains, and risk reduction) and dividing the result by the total cost of AI. Hard ROI can help you evaluate the profitability and efficiency of your AI solutions, but it may not capture the full range of benefits and costs that AI can bring to your security operations.
- **Soft ROI:** This is a broader measure of the qualitative and intangible benefits and costs of AI, such as customer satisfaction, employee engagement, brand reputation, innovation, and ethics. Soft ROI can be assessed by using surveys, feedback, ratings, reviews, or other indicators of stakeholder perception and satisfaction. Soft ROI can help you understand the impact of AI on your security culture, values, and relationships, but it may not be easily quantified or compared across different AI solutions.
- **Balanced scorecard:** This is a strategic management tool that combines both hard and soft ROI metrics into a comprehensive and balanced framework. It can help you align your AI objectives with your security vision, mission, and strategy, and track your AI performance across four key dimensions: financial, customer, internal, and learning and growth. Balanced scorecard can help you measure and communicate the value of AI in security from multiple perspectives, but it may require a lot of data collection and analysis, as well as stakeholder involvement and alignment.


To measure the ROI of AI in security effectively, you should follow some best practices, such as:

- Define your AI goals and expectations clearly and realistically, align them with your security and business objectives.
- Choose the most appropriate method and metrics for your AI use cases and goals and use a combination of hard and soft ROI metrics to capture the full value of AI.
- Collect and analyze relevant and reliable data to measure your AI outcomes and impacts and use benchmarks and baselines to compare your AI performance with your current state or industry standards.
- Monitor and evaluate your AI results and progress regularly and use feedback and insights to improve your AI solutions and strategy.
- Communicate and report your AI ROI clearly and transparently to your stakeholders and use stories and examples to illustrate the value of AI in security.

Optimize AI Performance for Better ROI

Optimizing your AI performance for better ROI is a key goal for any AI project. There are many factors that can affect your AI performance, such as data quality, model selection, parameter tuning, deployment strategy, and monitoring and feedback. Here are some general tips and techniques that can help you optimize your AI performance for better ROI:

- Ensure that your data is clean, relevant, and representative of your problem domain. Data is the foundation of AI, and the quality of your data will determine the quality of your AI solutions. You should perform data cleaning, preprocessing, and augmentation to remove noise, outliers, missing values, and biases from your data. You should also use appropriate data sources, formats, and splits to ensure that your data covers the range and diversity of your use cases and scenarios.
- Choose the right model and algorithm for your problem and objective. There are many AI models and algorithms available, but not all of them are suitable for your needs. You should consider the complexity, accuracy, interpretability, scalability, and robustness of the models and algorithms, and select the ones that match your problem characteristics and performance criteria. You should also compare



and evaluate different models and algorithms using appropriate metrics and validation methods.

- Fine-tune your model parameters and hyperparameters to optimize your model performance. Model parameters and hyperparameters are the settings that control the behavior and learning of your model. You should adjust and optimize these settings to improve your model performance and avoid overfitting or underfitting. You can use various methods, such as grid search, random search, or Bayesian optimization, to find the optimal values for your parameters and hyperparameters.
- Deploy your model in a suitable environment and platform that can support your AI requirements and goals. You should consider the availability, reliability, security, and scalability of your deployment environment and platform, and ensure that they can handle your AI workload and demand. You should also choose the right deployment mode, such as batch, online, or hybrid, depending on your use case and latency requirements.
- Monitor and update your model regularly to maintain and improve your model performance and ROI. You should collect and analyze feedback and data from your model deployment and use them to measure and evaluate your model performance and ROI. You should also identify and address any issues, errors, or changes that may affect your model performance and ROI, such as data drift, concept drift, or model degradation. You should update your model with new data, features, or algorithms to keep it relevant and accurate.

Can AI Replace Human Analysts in SOC?

AI can replace some of the tasks that human analysts perform in SOC, such as data collection, processing, analysis, and visualization, but it cannot replace the human judgment, creativity, and intuition that are essential for effective cybersecurity operations.

AI can augment and assist human analysts in SOC, by providing them with faster, smarter, and more accurate tools and insights, but it cannot replace the human skills and values, such as critical thinking, problem-solving, communication, collaboration, and ethics, that are required for cybersecurity decision-making and response. Therefore, AI can be seen as a partner, not a competitor, for human analysts in SOC, and the future of SOC will depend on the synergy and collaboration between AI and human analysts.



CHAPTER

22

Open-Source SOC

Developing an **open-source-based Security Operations Center (SOC)** involves several key steps. Let's break it down:

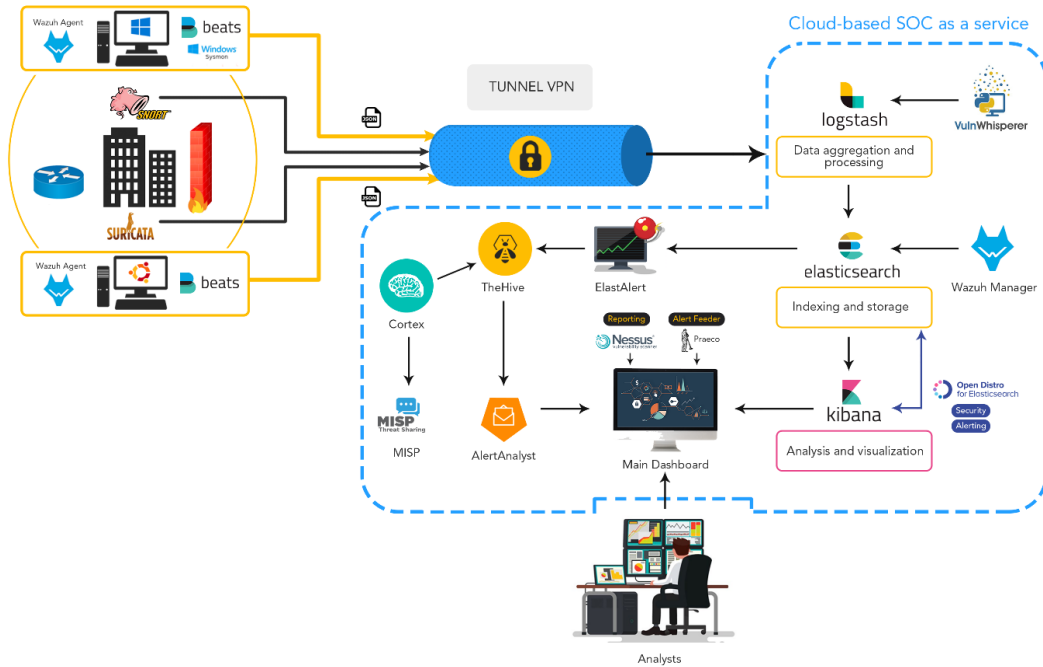
1. **Human Resources:**
 - Start by training your existing staff or hiring individuals with skills and experience in monitoring, incident management, threat hunting, intrusion detection, reverse engineering, and malware analysis.
 - Consider combining internal and external resources to build a strong SOC team.
2. **Processes:**
 - Establish clear workflows for incident management. Define roles, responsibilities, and documented processes.
 - Ensure that each team member understands their position and tasks within the SOC.
3. **Technology Stack:**



- Assemble a comprehensive set of open-source tools to support your SOC's visibility and response capabilities:
 - **SIEM (Security Information and Event Management):** Combines security information management (SIM) and security event management (SEM) functions into a single framework.
 - **Incident Tracking and Management System:** Helps organize and track incidents.
 - **Intrusion Detection and Prevention Systems (IDS/IPS/IDPS):** Monitor network traffic for signs of malicious activity.
 - **Threat Intelligence (CTI) Platform:** Enriches data with indicators of compromise (IOCs).
 - **Packet Capture and Analysis Tools:** Investigate network traffic.
 - **Automation Tools:** Automate routine tasks to free up analysts' time.
 - **Malware analysis tools:** investigate any malware's workflows within a sandboxed environment like ANY.RUN which lets your DFIR teams to analyze sophisticated ransomware or malware in a Linux environment.
- 4. **Network Monitoring:**
 - Use tools to monitor network traffic and detect anomalies.
 - Implement behavioral monitoring and data loss prevention mechanisms.
- 5. **Endpoint Management:**
 - Securely manage endpoints (devices) within your network.
- 6. **Asset Discovery:**
 - Identify and track assets (servers, workstations, devices) on your network.
- 7. **Incident Response:**
 - Develop incident response playbooks and procedures.
 - Implement ticketing systems for efficient case management.

Remember that open-source solutions offer flexibility, adaptability, and mostly cost-effectiveness that cannot be beaten. But do leverage the community support and customize your SOC to fit your organization's needs!

Designing the Open-source SOC



- Source: [archanchoudhury/SOC-OpenSource: This is a Project Designed for Security Analysts and all SOC audiences who wants to play with implementation and explore the Modern SOC architecture. \(github.com\)](https://github.com/archanchoudhury/SOC-OpenSource)
- [Deploying of infrastructure and technologies for a SOC as a Service \(SOCaaS\) | by Ibrahim Ayadhi | Medium](https://medium.com/@ibrahimayadhi/deploying-of-infrastructure-and-technologies-for-a-soc-as-a-service-socass-1234567890)

Designing an Open-Source Cybersecurity Operations Center (CSOC) using Wazuh, an impressive open-source security platform. Wazuh provides a comprehensive toolkit for threat detection, investigation, and response. Here's how you can architect your CSOC with Wazuh:

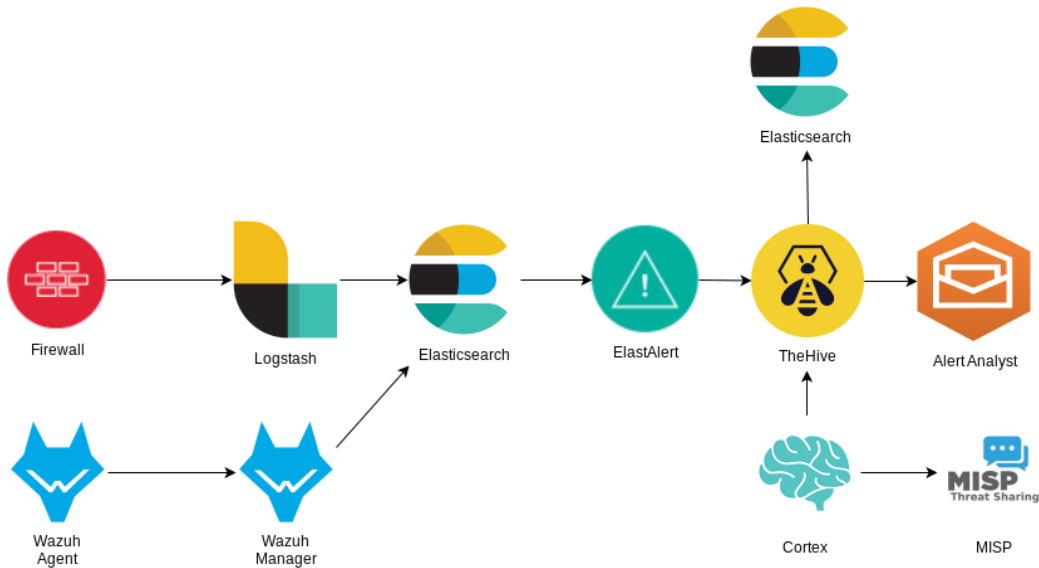
1. Understanding Wazuh:

- **Wazuh** is more than just a **SIEM (Security Information and Event Management)** solution. It goes beyond simple log aggregation and analysis.
- Key capabilities include:

- **Endpoint Detection and Response (EDR):** Monitors endpoints for suspicious activity, detects malware, and enables incident response actions.
 - **File Integrity Monitoring (FIM):** Watches critical files and systems for unauthorized changes.
 - **Vulnerability Assessment and Scoring (VAS):** Proactively identifies vulnerabilities and prioritizes them.
 - **Threat Hunting and Investigation:** Empowers SOC analysts to uncover hidden threats and investigate incidents.
 - **Cloud Security Monitoring:** Seamlessly integrates with AWS, Azure, or GCP for cloud deployments.
2. **Open-Source Advantage:**
- **Cost-Effectiveness:** Wazuh is budget-friendly, making it ideal for organizations conscious of costs.
 - **Customization:** The open-source code allows tailoring Wazuh to specific needs and seamless integration with existing security tools.
 - **Transparency and Security:** Community-driven development ensures continuous improvement and reliability.
3. **Wazuh Architecture:**
- The architecture consists of:
 - **Wazuh Server:** Central component for managing agents, rules, and alerts.
 - **Elastic Stack:** Used for log storage, analysis, and visualization.
 - **Wazuh Agents:** Deployed on endpoints for data collection.
 - Clustering options provide **load balancing** and **high availability**.
4. **Deployment Steps:**
- **Install Wazuh:** Set up the Wazuh server and deploy agents on endpoints.
 - **Configure Rules:** Customize rules to match your organization's security policies.
 - **Integrate with Elastic Stack:** Use Elasticsearch, Logstash, and Kibana for log analysis and visualization.
 - **Threat Hunting:** Empower analysts to proactively hunt for threats.
 - **Incident Response:** Define actions for detected incidents.
 - **Cloud Integration:** Extend monitoring to cloud environments.
5. **Why Choose Wazuh?**
- **Versatility:** Whether you're a seasoned SOC warrior or just starting, Wazuh fits all sizes.
 - **Affordability:** No vendor lock-in, no license costs.
 - **Community Support:** Trusted by thousands of enterprise users.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Wazuh's open-source nature, powerful features, and cost-effectiveness make it an excellent choice for designing your CSOC. Arm your digital kingdom with vigilant guards and invisible shields!



Source: [Using Elasticsearch and TheHive to Build an Open-Source Security Emergency Response Platform. thehive csdn-CSDN Blog](#) (Translate to English)

I am going to provide you with the total solution design picture gradually, including the specifications, the sizing guides, the network BoQ, the firewall BoQ for better understanding the open-source based SOC design. Also, the following 2 network designs have a 1500 user base and another has a 350,000 user base, which can adequately provide the insights desired by the SOC.

Products used in conjunction for developing the open source-based SOC:

1. Wazuh: [Wazuh - Open Source XDR. Open Source SIEM.](#)
2. Suricata: [Home - Suricata](#)
3. Snort: [Snort - Network Intrusion Detection & Prevention System](#)
4. Windows Sysmon: [Sysmon - Sysinternals | Microsoft Learn](#)
5. ELK Stack: [Elasticsearch Platform – Find real-time answers at scale | Elastic](#)
6. Cortex: [TheHive-Project/Cortex: Cortex: a Powerful Observable Analysis and Active Response Engine \(github.com\)](#)

7. TheHive: [TheHive Project \(thehive-project.org\)](https://thehive-project.org)
8. Filebeat: [Filebeat: Lightweight Log Analysis & Elasticsearch | Elastic | elastic/beats:tropical_fish: Beats - Lightweight shippers for Elasticsearch & Logstash \(github.com\)](https://www.elastic.co/guide/en/elastic/elastic-beats:7.x/tropical_fish:Beats-Lightweight-shippers-for-Elasticsearch-&Logstash.html)
9. Praeco: [johnsusek/praeco: Elasticsearch alerting made simple. \(github.com\)](https://github.com/johnsusek/praeco)
10. Vulnwhisperer: [HASecuritySolutions/VulnWhisperer: Create actionable data from your Vulnerability Scans \(github.com\)](https://github.com/HASecuritySolutions/VulnWhisperer)
11. MISP: [MISP/MISP: MISP \(core software\) - Open Source Threat Intelligence and Sharing Platform \(github.com\)](https://github.com/MISP/MISP)
12. checkMK
13. Open UBA
14. Open-XDR

Wazuh and Associated Components Integrations

The integration links are provided below that can be used to integrate each services mentioned above.

- [Deploying Wazuh agents using Windows Group Policy Objects \(GPO\) | Wazuh](#)

At some point, it may seem that the above integrations could be an easy way to develop your open source-based SOC. but my team still has challenges because in most cases, these are community supported, and lots of other things can happen using free software's, they are not actually free. Also, I have the understanding that nothing is for free, and those software's can come with its internal challenges of data infiltration as well. Some cons:

1. Not fully interactable.
2. Services stopped running without any cause.
3. Data transfers can generate errors.
4. Individual model breaks.
5. Reinstallation takes place.
6. DB cannot be retrieved.
7. OS patches destroyed some applications.

Here are some insights for your SOC's hardware specification for an enterprise network, not to be taken seriously, but for discussion purpose and configuration management purpose, these designs are here to help you to specify the BoQ in total.

Pro-Tip

• Nothing is actually free, you need to look out for the transmissions of your software services that getting out of your network, block them! imagine a printer is sending out gigabytes of data to the outside of your network, it shouldn't have right? you are right.

Create a New Detection Rule in CSOC

Creating a new detection rule in a Cybersecurity Operations Center (CSOC) involves defining patterns, behaviors, or indicators of compromise (IoCs) that are associated with known threats. These rules are designed to trigger alerts when the logic returns True during log monitoring. Here's a general process to create a new detection rule:

1. **Identify the Threat:** Understand the threat you want to detect. This could be a specific type of malware, an attack pattern, or any suspicious behavior.
2. **Define the Rule:** Based on the threat, define a rule that can detect it. This usually involves specifying patterns or behaviors that are indicative of the threat.
3. **Implement the Rule in the SIEM System:** The Security Information and Event Management (SIEM) system is where these rules live. It's a tool used to aggregate and analyze log data from various sources. Implement your rules in this system.
4. **Test the Rule:** Once the rule is implemented, it's important to test it to ensure it's working as expected and not generating false positives.

For example, if you're a Security Engineer tasked with writing a Detection Rule to trigger whenever a log comes through alerting that a user authenticated successfully to AWS without using MFA, you would follow these steps.

The exact process can vary depending on the specific CSOC and the tools they use. It's always best to refer to your organization's specific guidelines or procedures for creating detection rules. If you're using a specific tool or platform and need more detailed instructions, please let me know!

An Example of a Detection Rule

Here are a couple of examples of detection rules:

1. **Monitoring Email Logs for Specific Domains:** This rule monitors email logs of user-sent emails and includes a filter criteria that checks for external recipient email address domain. It excludes a list of users (like the marketing team) who are known to send emails to external addresses.
2. **Brute-force Attack Detection:** This rule detects instances of brute-force attacks by looking for a large number of failed login attempts from the same IP address within a short period of time. The rule is defined as follows in Sigma format:

```
title: Brute-force attack detected
description: This rule detects instances of brute-force attacks
by looking for a large number of failed login attempts from the
same IP address within a short period of time.

author: John Doe
tags: brute-force, password guessing, security
index: audit
detection:
  selection:
    event_id: 4625
    log_name: security
  condition: selection: failed_login_count > 10 duration < 30m
ip_address = *
```

3. **Snort Rule for Win.Trojan.Doublepulsar Variant:** Network Intrusion Prevention Systems (NIPS) like Snort can block threats by leveraging rule-based detection. For example, the Snort rule Sid 1-42329 is able to detect the Win.Trojan.Doublepulsar variant.

The exact syntax and parameters can vary depending on the specific detection system or tool you are using.

Custom rule creation in Snort

Creating a custom rule in Snort involves defining the protocol, direction, source and destination IP addresses and ports, and rule options. Here's a step-by-step guide:

1. **Define the Protocol:** Specify the protocol you want to match. This can be ICMP, TCP, UDP, or other protocols.
2. **Determine the Direction:** Determine the direction of the traffic you want to match.

3. **Determine the Source and Destination IP Addresses and Ports:** Specify the source and destination IP addresses and ports.
4. **Define the Rule Options:** Specify the rule options.

For example, if you had a `malware.rules` file in the same directory as your Lua configuration file, you could include that rules file like so:

Lua

```
ips = { include = 'malware.rules' }
```

If you want to include multiple `.rules` files, then you can do so like:

Lua

```
ips = { rules = [[ include /path/to/rulesfile1.rules include  
/path/to/rulesfile2.rules ]] }
```

Alternatively, a single rules file or a path to a rules directory can be passed directly to Snort on the command line. This is done either with the `-R` option for a single rules file or the `--rule-path` option to pass in a whole directory of rules files.

For example, the below command will run all the rules present in `malware.rules` against the traffic in `bad.pcap`:

```
$ snort -c $my_path/lu/snort.lua -R malware.rules -r bad.pcap
```

It's always best to refer to your organization's specific guidelines or procedures for creating detection rules, they may already be laid out or standardized for your specific platform.

Testing Your Custom Rules to Ensure They Work as Expected

Here's a general process you can follow:

1. **Load the Rules:** First, make sure that your rules are loaded correctly. You can do this by running Snort with the `-T` option, which validates the configuration.

```
$ snort -c /path/to/snort.conf -T
```

2. **Run Snort with a PCAP File:** You can test your rules against a pcap file using the `-r` option. This allows you to see if your rules trigger any alerts with the given network traffic.

```
$ snort -c /path/to/snort.conf -R /path/to/rulesfile.rules -r /path/to/test.pcap
```

3. **Check the Alerts:** Snort provides several “alert mode” options that can be set on the command line to tweak the way alerts are displayed. These modes include `cmg` which displays alerts alongside a hexdump of the alerting packet(s), as well as a few different `alert_*` modes.

```
$ snort -c /path/to/snort.conf -q -r /path/to/test.pcap -R /path/to/rulesfile.rules -A cmg
```


Generate a Detection Rule for APT-41

APT41 is a prolific Chinese cyber threat group that carries out state-sponsored espionage activity in parallel with financially motivated operations. They are known to adapt quickly to changes and detections within victim environments, often recompiling malware within hours of incident responder activity.

Here’s an example of a Snort rule that could be used to detect APT41 activity based on the information available:

```
alert tcp any any -> $HOME_NET any (msg:"APT41 activity detected"; flow:established,to_server; content:"|00 01 00 00 00 01 00 00 00 00 00 00|"; depth:12; reference:url,mandiant.com/resources/blog/game-over-detecting-and-stopping-an-apt41-operation; classtype:trojan-activity; sid:1000001; rev:1;)
```

This rule will trigger an alert whenever it detects a TCP packet from any IP address and port to your home network (replace `$HOME_NET` with your network range) that contains the specific content pattern associated with APT41.



Please note that this is a simplified example and real-world detection rules might need to be more complex to accurately detect APT41 activity and reduce false positives. The exact content pattern, source, and destination you should use depend on the specific characteristics of APT41 that you want to detect.

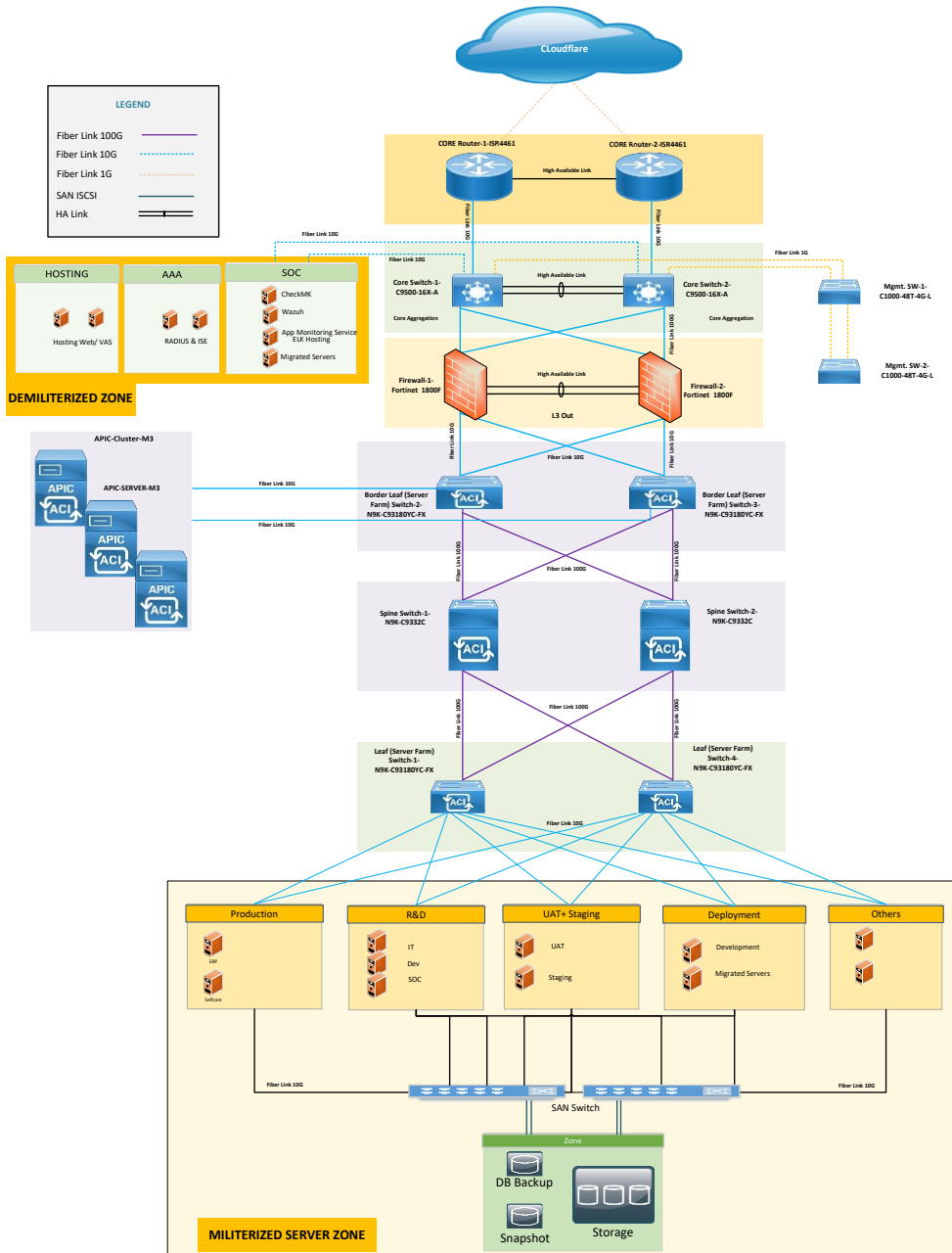
Also, keep in mind that APT41 is known for its ability to adapt quickly to changes and detections within victim environments. Therefore, it's important to continuously update your detection rules to keep up with any new tactics, techniques, and procedures (TTPs) used by APT41.

The Network Design

Please be mindful that all the SOC traffic should not be fed into the Firewall, but the SOC should be placed outside of the firewall, just like the design, but you are free to put it into the zones and collect all the data from within. In the below design, I will share the BoQ of each device, that might help you understand how to generate device specifications for your SOC. Though the BoQ's are shared in this study, the SOC is above the firewall, residing in the DMZ. You can separate them through a firewall as well, not shown in the design.



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

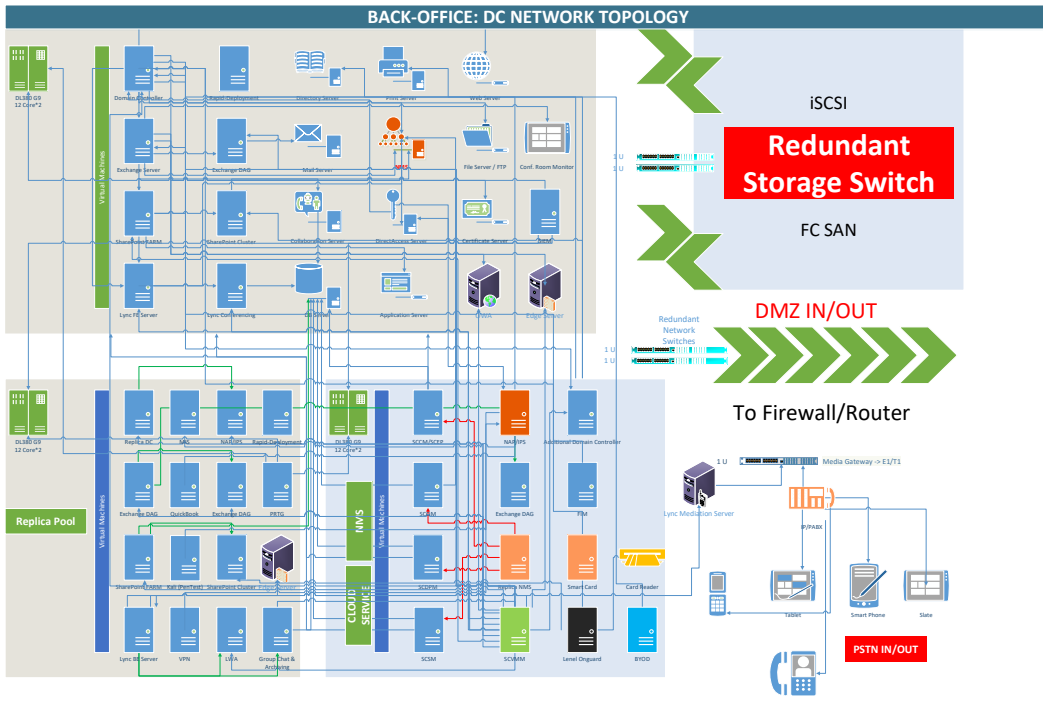


COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Back-office Network Design (1500 Users)

In summary, you should have the following items in your back-office (on-prem (3* HP DL380 G9 in total physical servers) and without HA for DR) (the Visio file is also provided in the job aids for your future use):

1. Active Directory or any LDAP or any RADIUS or any type of ID provider.
2. Email server: Exchange, SendMail, Postfix, cPanel based Squirrel Mail etc.
3. SharePoint or Private Cloud Services like OwnCloud or something similar.
4. Communication Stack: IM, CHAT, Conferencing like Lync/Teams.
5. System Center: SCCM, SCSM, SCDPM, SCOM, SCO, SCVMM etc.
6. Laptop Image Storage for image backup for rapid deployment.
7. IP Telephony, PSTN gateway.
8. File integrity monitoring (FIM).
9. Office door control and access control management.
10. Paessler PRTG or MRTG monitoring for data graph.
11. Storage backup for replication, snapshots etc.

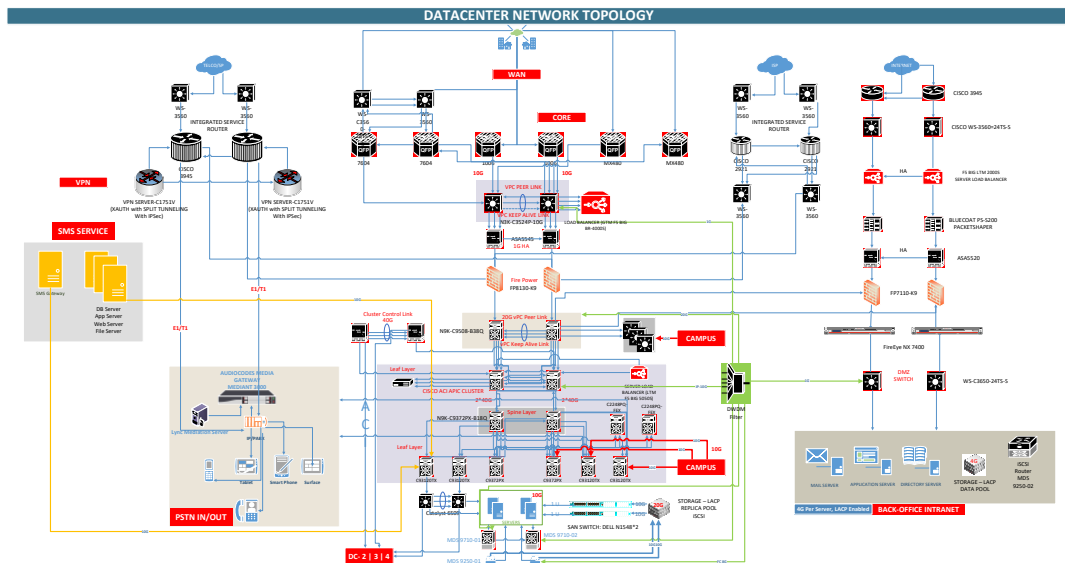


COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

These designs, connectivity and integration ensure optimal network transmission for a small business with up-to 1500++ personnel. Make no mistake, the better the architecture, the better results, and integrations service it would provide for SOC data collection, monitoring and remediations.

Back-office Network Design (350K Users)

You should have your own design devised either by your team of architects or from a hired gun! But in any situation, you will need to specify what are the workflows, business requirements, and then map it out to the service requirements. Here campus means that there is a distribution network and connectivity requirements as well accommodating more than 350,000 user bases. Network capacity building is also an art, you can build whatever you want, but there is an “if”, whether you want to learn the transmission requirements as well, then you dive into these designs as time passes, and you are growing to become a race-horse, never stop, and don't give up.



The above network is designed for providing the following services in addition to the back-office network, all in-house applications, monitoring, and management and then some more (the Visio file is also provided in the job aids for your future use):

1. Mass mailer service
2. Mass SMS service
3. ERP level developments

4. Integrated payment gateways etc.

VM List for Open-Source SOC Deployment

SL	Category	VM Name	Name	Purpose	IP Address
1	Syslog Server	FHSYSLOG (Syslog Server)	Syslog Server	Collect All Syslog from All devices	
2	Wazuh Cluster	FHWAINDEXER02{Wazuh Indexer (Elasticsearch)}	Wazuh Indexer01	Wazuh Master Node	
3		FHWAINDEXER01{Wazuh Indexer (Elasticsearch)}	Wazuh Indexer02	Wazuh Worker Node	
4		FHWASERVER (Wazuh Manager Server Master node)	Wazuh Server	Wazuh Server	
5		FHWALB01(Wazuh Load Balancer)	Loadbalancer01	Wazuh server LB	
6		FHWALB02(Wazuh Load Balancer)	Loadbalancer02	Wazuh server LB	
7		FHWADASHBOARD(Wazuh dashboard)	Wazuh Dashboard	Wazuh Dashboard	
8	ELK	FHELKAPM(APM)	Elastic Search	ELK with APM	
9		FHKIBANA(ELK Dashboard, Logstash)	APM with Kibana	ELK with APM	
10	IDS	FHSURICATA(IPS IDS)	Suricata	IDS & IPS	
11	IR	FHSOCTHEHIVE(MISP to TheHive)	Thehive	Case Management & Incident Responder	
12	Threat Intel	FHCORTEX (Threat Intel-Cortex)	Cortex		
13	Misp	FHSOCMISP(Malware Information Sharing Platform)	MISP		

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

14	OpnC TI Stack	FHTIOPENCTI01(Threat Intel(OpenCTI) for docker Swarm)	Stack Master	Docker swarm master	
15		FHTIOPENCTI02(Threat Intel(OpenCTI) for docker Swarm)	Stack worker	Docker swarm worker	

Physical Server BoQ (DELL): 2 Servers Required

Option	Selection	SKU / Product Code	Quantity
Base	PowerEdge R550 Server	[210-AZEG] / G8S6JX7	1
Motherboard	PowerEdge R550 Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM	[329-BGIB] / GQLSN36	1
Trusted Platform Module	No Trusted Platform Module	[461-AADZ] / GMHJL5Y	1
Chassis	2.5" Chassis with up to 16 Hard Drives (SAS/SATA), 2 CPU	[321-BGSK] / G1PZL09	1
Fans	Standard Fan Cold Swap 2U,V2 x5	[750-ADIN] / G2ZA0YM	1
Shipping	PowerEdge R550 Shipping	[340-CVKM] / GDE6JS2	1
Shipping Material	PowerEdge R550 Shipping Material	[343-BBRT] / GEUHQ4M	1
Regulatory	PowerEdge 2U CCC Marking, No BIS or CE Marking	[389-DYHB][389-DYMO] / GWVOG2D	1
OEM Regulatory	None		
Processor	Intel® Xeon® Silver 4316 2.3G, 20C/40T, 10.4GT/s, 30M Cache, Turbo, HT (150W) DDR4-2666	[338-CBWL] / GF0RKH9	1
Additional Processor	Intel® Xeon® Silver 4316 2.3G, 20C/40T, 10.4GT/s, 30M Cache,	[338-CBWL][379-BDCO] / G6AS94T	1

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

	Turbo, HT (150W) DDR4-2666		
Processor Thermal Configuration	Standard Heatsink for 2 CPU configuration	[412-AAVU][412-AAVU] / GF2HDPU	1
Memory DIMM Type and Speed	3200MT/s RDIMMs	[370-AEVR] / GR3CFNV	1
Memory Configuration Type	Performance Optimized	[370-AAIP] / GH9QB EI	1
Memory	64GB RDIMM, 3200MT/s, Dual Rank, 16Gb	[370-AEVP] / GQC5KJW	8
RAID	C1, No RAID for HDDs/SSDs (Mixed Drive Types Allowed)	[780-BCDI] / G8510ID	1
RAID/Internal Storage Controllers	Front HBA355i Rear Load	[405-AAXY][750-ACFQ] / GXR V4JM	1
Internal Optical Drive	No Internal Optical Drive	[429-AAIQ] / GZP2ROB	1
Storage	960GB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug AG Drive, 1 DWPD	[400-AXSW] / GA16FX3	8
Boot Optimized Storage Cards	No BOSS Card	[403-BCID] / GIEP1Z6	1
Operating System	No Operating System	[611-BBBF] / G78MU35	1
OS Media Kits	No Media Required	[605-BBFN] / GKH7AZI	1
Embedded Systems Management	iDRAC9 Datacenter 15G	[528-CRVW] / G6CD90H	1
Group Manager	iDRAC Group Manager, Enabled	[379-BCQV] / GTC0D81	1
Password	iDRAC, Factory Generated Password	[379-BCSF] / G2T768J	1
IDRAC Service Module	None		
OCP 3.0 Network Adapters	Broadcom 57412 Dual Port 10GbE SFP+, OCP NIC 3.0	[540-BCNT] / G81KH5Z	1
IDSDM Card Reader	None		
Internal SD Module	None		

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Power Supply	Dual, Hot-Plug, Power Supply Fault Tolerant Redundant (1+1), 1100W MM (100-240Vac) Titanium, NAF	[450-AKLF] / GWT5F27	1
Power Cords	C13 to C14, PDU Style, 12 AMP, 6.5 Feet (2m) Power Cord, North America	[492-BBDI] / GC1DFVJ	4
Bezel	PowerEdge 2U LCD Bezel	[325-BEBV][350-BCFM] / G98L4KP	1
Quick Sync	No Quick Sync	[350-BCER] / GLUIZE1	1
BIOS and Advanced System Configuration Settings	Performance BIOS Setting	[384-BBBL] / GJO594B	1
Advanced System Configurations	UEFI BIOS Boot Mode with GPT Partition	[800-BBDM] / GSFTG4Y	1
Rack Rails	ReadyRails Static Rails for 2/4-post Racks	[770-BDZN] / GW0EL38	1
System Documentation	OpenManage DVD Kit, PowerEdge R550	[631-ADDZ] / GPO85GA	1
Secondary OS	None		
Enabled Virtualization	None		
Microsoft SQL Server	None		
Web Tracking	None		
OCONUS	None		
GSA Purchase Order	None		
SERVICES & SUPPORT			
Option	Selection	SKU / Product Code	Quantity
Protect your purchase - View Support offers below	Basic Next Business Day 36 Months, 36 Month(s)	[709-BBFL] / G32DMTS	1
Extended Services	NO WARRANTY UPGRADE SELECTED, 36 Month(s)	[883-BBBD] / GKQE3CR	1
Keep Your Hard Drive for Enterprise Services	None		
Keep Your Component for Enterprise Services	None		

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Partner Operations Support	None		
Services: On-site Diagnosis Service	None		
Configuration Services Asset Report	None		
Enterprise Deployment Services	No Installation	[900-9997] / NOINSTL	1

Networking Device BoQ

Line Number	Part Number	Description	Service Duration (Months)	Estimated Lead Time (Days)	Qty
1.0	ISR4461/K9 (CORE Router)	Cisco ISR 4461 Router (2x10GE+4x1GE,3NIM,3SM,8G FLASH,4G DRAM)	---	70	2
1.0.	CON-SNT-ISR44619	SNTC-8X5XNBD Cisco ISR 4461 (4GE,3NIM,3SM,8G FLASH,4G	60	N/A	2
1.1	SL-44-IPB-K9	IP Base License for Cisco ISR 4400 Series	---	28	2
1.2	PWR-4460-650-AC	650W AC Power Supply for Cisco ISR 4461	---	28	2
1.3	PWR-4460-650-AC2	Redundant 650W AC Power Supply for Cisco ISR 4461	---	28	2
1.4	CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	---	35	4
1.5	ACS-4460-FANASSY	Cisco ISR 4460 Fan Assembly	---	28	2
1.6	SM-F-BLANK	Fixed faceplate for SM slot on Cisco 4461 ISR	---	28	2
1.7	MEM-4460-DP-4G	4G DRAM for Cisco ISR 4460 Data Plane	---	28	2
1.8	POE-COVER-4450	Cover for empty POE slot on Cisco ISR 4450	---	28	4

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

1.9	NIM-BLANK	Blank faceplate for NIM slot on Cisco ISR 4400	---	28	2
1.10	SM-S-BLANK	Removable faceplate for SM slot on Cisco 2900,3900,4400 ISR	---	28	6
1.11	CAB-CONSOLE-RJ45	Console Cable 6ft with RJ45 and DB9F	---	14	2
1.12	CAB-CONSOLE-USB	Console Cable 6ft with USB Type A and mini-B	---	14	2
1.13	SISR44V2UK9173	Cisco ISR 4400 Series IOS XE Universal	---	28	2
1.14	SL-44-SEC-K9	Security License for Cisco ISR 4400 Series	---	28	2
1.15	SL-44-APP-K9	AppX License for Cisco ISR 4400 Series	---	28	2
1.16	FL-44-HSEC-K9	U.S. Export Restriction Compliance license for 4400 series	---	28	2
1.17	FL-4460-PERF-K9	Performance on Demand License for 4460 Series	---	28	2
1.18	MEM-4460-32G	32G DRAM (1 DIMM) for Cisco ISR 4460	---	28	2
1.19	MEM-FLSH-8GU32G	8G to 32G Flash Memory Upgrade for Cisco ISR 4460	---	28	2
1.20	NIM-ES2-8	8-port Layer 2 GE Switch Network Interface Module	---	70	2
1.21	NIM-SSD	NIM Carrier Card for SSD Drives	---	28	2
1.22	SSD-SATA-400G	400 GB, SATA Solid State Disk	---	28	2
Server Farm Switch					
2.0	N9K-C93180YC-FX (Core Switch)	Nexus 9300 with 48p 1/10/25G, 6p 40/100G, MACsec	---	70	4
2.0.1	CON-SNT-N93YCFX	SNTC-8X5XNBD Nexus 9300 with 48p	60	N/A	4
2.1	NXK-AF-PI	Dummy PID for Airflow Selection Port-side Intake	---	14	4
2.2	NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	---	14	4

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

2.3	CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	---	70	8
2.4	NXA-PAC-500W-PI	Nexus NEBs AC 500W PSU - Port Side Intake	---	14	8
2.5	NXA-FAN-30CFM-B	Nexus Fan, 30CFM, port side intake airflow	---	7	1 6
2.6	C1E1TN9300 XF-5Y	Data Center Networking Essentials Term N9300 XF, 5Y	---	3	4
2.7	SVS-B-N9K-ESS-XF	EMBEDDED SOLN SUPPORT SWSS FOR ACI NEXUS 9K	---	3	4
2.8	MODE-ACI-LEAF	Dummy PID for mode selection	---	14	4
2.9	ACI-N9KDK9-16.0	Nexus 9500 or 9300 ACI Base Software NX-OS Rel 16.0	---	14	4
Management Switch					
3.0	C1000-48T-4G-L	Catalyst 1000 48port GE, 4x1G SFP	---	126	2
3.0.1	CON-SNT-C10T48GL	SNTC-8X5XNBD Catalyst 1000 48port GE, 4x1G SFP, LANBa	60	N/A	2
3.1	CAB-C15-CBN	Cabinet Jumper Power Cord, 250 VAC 13A, C14-C15 Connectors	---	14	2
3.2	PWR-CLP	Power Retainer Clip For 3560-C, 2960-L & C1000 Switches	---	14	2
CORE Aggregator Switch					
4.0	C9500-16X-A	Catalyst 9500 16-port 10Gig switch, Advantage	---	70	2
4.0.1	CON-SNT-C95K16XA	SNTC-8X5XNBD Catalyst 9500 16-por	60	N/A	2
4.1	CAB-C15-CBN	Cabinet Jumper Power Cord, 250 VAC 13A, C14-C15 Connectors	---	14	4
4.2	PWR-C4-950WAC-R	950W AC Config 4 Power Supply front to back cooling	---	14	2
4.3	PWR-C4-950WAC-R/2	950W AC Config 4 Power Supply front to back cooling	---	14	2
4.4	C9500-NW-A	C9500 Network Stack, Advantage	---	14	2

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

4.5	S9500UK9-179	Cisco Catalyst 9500 XE 17.9 UNIVERSAL	---	14	2
4.6	C9500-NM-8X	Cisco Catalyst 9500 8 x 10GE Network Module	---	14	2
4.7	C9500-DNA-16X-A	C9500 DNA Advantage, Term licenses	---	14	2
4.7.0.1	C9500-DNA-L-A-5Y	DNA Advantage 5 Year License	60	N/A	2
4.8	PI-LFAS-T	Prime Infrastructure Lifecycle & Assurance Term - Smart Lic	---	14	6
4.8.0.1	PI-LFAS-AP-T-5Y	PI Dev Lic for Lifecycle & Assurance Term 5Y	60	N/A	6
4.9	NETWORK-PNP-LIC	Network Plug-n-Play Connect for zero-touch device deployment	---	3	2
Cisco 10G Fiber Module					
5.0	SFP-10G-SR=	10GBASE-SR SFP Module	---	14	70
6.0					
Spine Switch - N9K-C9332C					
6.0.1	CON-SNT-N9KC9332	SNTC-8X5XNBD Nexus 9K ACI NX-OS Spine, 32p 40/100G	60	N/A	2
6.1	MODE-ACI-SPINE	Dummy PID for mode selection	---	14	2
6.2	NXK-AF-PI	Dummy PID for Airflow Selection Port-side Intake	---	14	2
6.3	ACI-N9KDK9-16.0	Nexus 9500 or 9300 ACI Base Software NX-OS Rel 16.0	---	14	2
6.4	NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	---	14	2
6.5	NXA-PAC-750W-PI	Nexus AC 750W PSU - Port Side Intake	---	14	4
6.6	NXA-FAN-35CFM-PI	Nexus Fan, 35CFM, port side intake airflow	---	70	10
6.7	CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	---	70	4
7.0	APIC-CLUSTER-M3	APIC Cluster - Medium Configurations (Up to 1200 Edge Ports)	---	14	1
7.0.1	CON-L1NBD-APICCLM3	CX LEVEL 1 8X5XNBD APIC Cluster Medium	60	N/A	1

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

7.1	APIC-SERVER-M3	APIC Appliance - Medium Configuration (up to 1200 Edge Ports)	---	14	1
7.2	APIC-DK9-5.2	APIC Base Software Release 5.2	---	14	1
7.3	APIC-PCIE-C25Q-04	Cisco APIC VIC 1455 Quad Port 10/25G SFP28 CNA PCIE	---	14	1
7.4	APIC-PSU1-770W	770W power supply for USC C-Series	---	14	2
7.5	APIC-TPM2-002	Trusted Platform Module 2.0 for UCS servers	---	14	1
7.6	APIC-RAID-M5	Cisco 12G Modular RAID controller with 2GB cache	---	14	1
7.7	APIC-HD1T7K12N	1 TB 12G SAS 7.2K RPM SFF HDD	---	14	2
7.8	APIC-CPU-3106	1.7 GHz 3106/85W 8C/11MB Cache/DDR4 2133MHz	---	14	2
7.9	APIC-SD800GK3X-EP	800GB 2.5in Enterprise Performance 12G SAS SSD (3X endurance)	---	14	1
7.10	APIC-MSTOR-SD	Mini Storage Carrier for SD (holds up to 2)	---	14	1
7.11	APIC-SD-32G-S	32GB SD Card for UCS servers	---	14	1
7.12	APIC-MR-X16G1RW	16GB RDIMM SRx4 3200 (8Gb)	---	14	6
7.13	APIC-SERVER-M3	APIC Appliance - Medium Configuration (up to 1200 Edge Ports)	---	14	1
7.14	APIC-DK9-5.2	APIC Base Software Release 5.2	---	14	1
7.15	APIC-PCIE-C25Q-04	Cisco APIC VIC 1455 Quad Port 10/25G SFP28 CNA PCIE	---	14	1
7.16	APIC-PSU1-770W	770W power supply for USC C-Series	---	14	2
7.17	APIC-TPM2-002	Trusted Platform Module 2.0 for UCS servers	---	14	1
7.18	APIC-RAID-M5	Cisco 12G Modular RAID controller with 2GB cache	---	14	1
7.19	APIC-HD1T7K12N	1 TB 12G SAS 7.2K RPM SFF HDD	---	14	2
7.20	APIC-CPU-3106	1.7 GHz 3106/85W 8C/11MB Cache/DDR4 2133MHz	---	14	2

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

7.21	APIC-SD800GK3X-EP	800GB 2.5in Enterprise Performance 12G SAS SSD (3X endurance)	---	14	1
7.22	APIC-MSTOR-SD	Mini Storage Carrier for SD (holds up to 2)	---	14	1
7.23	APIC-SD-32G-S	32GB SD Card for UCS servers	---	14	1
7.24	APIC-MR-X16G1RW	16GB RDIMM SRx4 3200 (8Gb)	---	14	6
7.25	APIC-SERVER-M3	APIC Appliance - Medium Configuration (Up to 1200 Edge Ports)	---	14	1
7.26	APIC-DK9-5.2	APIC Base Software Release 5.2	---	14	1
7.27	APIC-PCIE-C25Q-04	Cisco APIC VIC 1455 Quad Port 10/25G SFP28 CNA PCIE	---	14	1
7.28	APIC-PSU1-770W	770W power supply for USC C-Series	---	14	2
7.29	APIC-TPM2-002	Trusted Platform Module 2.0 for UCS servers	---	14	1
7.30	APIC-RAID-M5	Cisco 12G Modular RAID controller with 2GB cache	---	14	1
7.31	APIC-HD1T7K12N	1 TB 12G SAS 7.2K RPM SFF HDD	---	14	2
7.32	APIC-CPU-3106	1.7 GHz 3106/85W 8C/11MB Cache/DDR4 2133MHz	---	14	2
7.33	APIC-SD800GK3X-EP	800GB 2.5in Enterprise Performance 12G SAS SSD (3X endurance)	---	14	1
7.34	APIC-MSTOR-SD	Mini Storage Carrier for SD (holds up to 2)	---	14	1
7.35	APIC-SD-32G-S	32GB SD Card for UCS servers	---	14	1
7.36	APIC-MR-X16G1RW	16GB RDIMM SRx4 3200 (8Gb)	---	14	6
7.37	CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	---	70	2
7.38	CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	---	70	2
7.39	CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	---	70	2

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER


8.0	SFP-10G-SR=	10GBASE-SR SFP Module	---	14	1
9.0	QSFP-100G-SR4-S=	100GBASE SR4 QSFP Transceiver, MPO, 100m over OM4 MMF	---	14	1
10.0	GLC-TE=	1000BASE-T SFP transceiver module for Category 5 copper wire	---	14	4
11.0	GLC-SX-MMD=	1000BASE-SX SFP transceiver module, MMF, 850nm, DOM	---	14	8

Fortinet Firewall BoQ

Item	SKU	Description	Qty
FortiGate-1800F	FG-1800F	4 x 40GE QSFP+ slots, 12 x 25GE SFP28 /10GE SFP+ slots, 2x10GE SFP+ HA slots, 8 x GE SFP slots, 18 x GE RJ45 ports. SPU NP7 and CP9 accelerated, dual AC power supplies	2
	FC-10-F18HF-928-02-60	FortiGate-1800F 5 Year Advanced Threat Protection (IPS, Advanced Malware Protection Service, Application Control, and FortiCare Premium)	2
	FC-10-F18HF-204-02-60	Upgrade FortiCare Premium to Elite (Require FortiCare Premium)-Five years	2
	FN-TRAN-SFP+SR	10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots	8
			14

There is a lot more to it than meets the eye for developing a functional SOC. It is not like any off-the-shelf software deployment that will end up working and providing services that's it supposed to. A SOC can be very tiresome to develop with in-house resources or buying a complete solution; though there is no complete solution yet, not even close. SOC frameworks and compliance requirements are aligning to its core requirements, but above functions under PPTD (people, process, technology, data) are still scarce, even though SIEM, CTI, IoC's OSINT, Cyber Counterintelligence (CCI) are playing their part, and yet Artificial Intelligence is now used to develop malicious codes.

But open-source solutions have ways to integrate to a much efficient SOC, but you will end up managing a large number of integrations and a blunder likely to occur when



upgrades or patches comes in. Moreover, you will need an army of team members to manage all the software components, tuning it precisely what you want out of it, producing actionable results.

This document is a broad example for developing your own SOC, at times, information overflow can be a daunting task to shape the documentation correctly, and the specific workings can vary based on the organization's size, needs and resources requirements.





BONUS CHAPTER

1

Project Management

THE SOC CANNOT BE DERIVED FROM A SINGULAR PERSON'S VIEW, IT REQUIRES BUSINESS (BPM) TO TECHNOLOGY MAPPING WHICH MUST HAVE INTEGRATION CAPABILITIES THROUGHOUT THE INFRASTRUCTURE, THAT'S WHERE ITS BEST TO LEAVE THE PROJECT MANAGEMENT TO THE RIGHT PERSONNEL. EVENTUALLY, YOU WILL END UP DERIVING BITS AND PIECES OF INFORMATION AND PUT TOGETHER, YOU WILL BECOME A PROJECT MANAGER AS WELL.

The below process groups reflect on how a project should be managed according to the PMI, assuming that you have a PMO in place to track project performance and relevant activities. Though this is a PMI standard, you are to initiate what works, doesn't have to be by the book, making it overly simplified, or overly complex, either of them is going to



land you with undesired results, and you have to be creative about how to place to your PMO and achieve your goal.

Project Management by PMI Terms

Knowledge Areas	Project Management Process Groups				
	Initiating Process Group	Planning Process Group	Executing Process Group	Monitoring and Controlling Process Group	Closing Process Group
4. Project Integration Management	4.1 Develop Project Charter	4.2 Develop Project Management Plan	4.3 Direct and Manage Project Work 4.4 Manage Project Knowledge	4.5 Monitor and Control Project Work 4.6 Perform Integrated Change Control	4.7 Close Project or Phase
5. Project Scope Management		5.1 Plan Scope Management 5.2 Collect Requirements 5.3 Define Scope 5.4 Create WBS		5.5 Validate Scope 5.6 Control Scope	
6. Project Schedule Management		6.1 Plan Schedule Management 6.2 Define Activities 6.3 Sequence Activities 6.4 Estimate Activity Durations 6.5 Develop Schedule		6.6 Control Schedule	
7. Project Cost Management		7.1 Plan Cost Management 7.2 Estimate Costs 7.3 Determine Budget		7.4 Control Costs	
8. Project Quality Management		8.1 Plan Quality Management	8.2 Manage Quality	8.3 Control Quality	
9. Project Resource Management		9.1 Plan Resource Management 9.2 Estimate Activity Resources	9.3 Acquire Resources 9.4 Develop Team 9.5 Manage Team	9.6 Control Resources	
10. Project Communications Management		10.1 Plan Communications Management	10.2 Manage Communications	10.3 Monitor Communications	
11. Project Risk Management		11.1 Plan Risk Management 11.2 Identify Risks 11.3 Perform Qualitative Risk Analysis 11.4 Perform Quantitative Risk Analysis 11.5 Plan Risk Responses	11.6 Implement Risk Responses	11.7 Monitor Risks	
12. Project Procurement Management		12.1 Plan Procurement Management	12.2 Conduct Procurements	12.3 Control Procurements	
13. Project Stakeholder Management	13.1 Identify Stakeholders	13.2 Plan Stakeholder Engagement	13.3 Manage Stakeholder Engagement	13.4 Monitor Stakeholder Engagement	

Table 1-4 (Guide). Project Management Process Group and Knowledge Area Mapping

A Guide to the Project Management Body of Knowledge (PMBOK® Guide) – Sixth Edition. ©2017 Project Management Institute, Inc. All rights reserved.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

The following project charter directly corresponds to the above BoQ, and the network design provided. You can take advantage of the format for your primary requirements. But do make changes as you see fit.

A very good starter kit can be found from the below link (combine and tailor to your need) for your all types of PM requirements, but make sure you use what's required, overly complicating things will not be understood by business personnel, which in turn, will complicate achieving your target, eyes on the ball!

Download the PM files from here: [850+ FREE Project Management Templates in Excel and Word \(engineeringmanagement.info\)](https://www.engineeringmanagement.info)

Project Charter

Project Charter: Back-office Infrastructure Modernization		
General Project Information		
Project Name	Back-office Infrastructure Modernization	Extra Notes: Most Importantly, this is initiated by the board member as the value presentation is provided multiple times. Securing and segmenting the core ERP system needs to be segmented as the network broadcast hits the ERP system infrastructure, and from security perspective, this infrastructure will be placed in a safe zone. Reason why the separation is required to secure the ERP and its associated services. This initiative is undertaken as the previous MIS went through a surgery and it's
Project Sponsor	CEO	
Project Manager	xxxxxxxxxxxxxxxxxxx	
Email Address		
Phone Number	xxxxxxxxxxxxxxxxxxx	
Organizational Unit	Information Security, I&I	
Process Impacted	M365, MIS, Server Re-allocations, VM's, according to the design etc.	
Expected Start Date	1st August 2023 (Assumed all HW Received)	
Expected Completion Date	27 Working Days	
Expected Savings (if any)	N/A	
Estimated Costs (BDT)	N/A	
Green Belts Assigned	N/A	



<p>Black Belts Assigned</p>	<p>N/A</p>	<p>architecture were out of time and the old design flaws were making the application ineffective, thus the initiation of the TechStack needs to be in place to take the old MIS to a new ERP based architectural design. In order to do that, the platform needed to be upgraded to the latest build for speed, HA and monitoring purposes, microservices and latest technological advancement were introduced.</p>
------------------------------------	------------	--

Describe the Problem or Issue, Goals, Objectives, and Deliverables of this Project

<p>Problem or Issue</p>	<p>Performance information related to the current MIS is not there and is not reliable and accurate as reported in the discussion groups. Processes are poorly defined, inconsistent, and prone to high error rates each month. Incidents were recorded of high severity, which led us to develop components, integrate new movements, and a complete makeover was required in order for the MIS to be functional. As the MIS is the heart of company's daily networked operations, its is of utmost interest that the back-office network is separated for the following primary reasons:</p> <ol style="list-style-type: none"> 1. Separate office-network and its resources from the distribution network & retail network 2. Provide NGFW type firewall to provide secure access to the militarized zone 3. Block DDoS attacks on the ERP, M365 4. Block distribution network's unusual broadcasts, stop hits to the back-office network devices 5. Block unusual IP hits on the back-office networked, application, servers etc. 6. Enablement of application performance delivery and monitoring etc.
--------------------------------	---





<p>Purpose of Project</p>	<p>This project identifies root causes behind distortions with actual problems of the AD, ADC, AD-Azure Sync Servers, Synology backup servers and implement solutions to in capturing and reporting business losses accordingly, while finalizing a new ERP and redevelop the complete platform</p>
<p>Business Case</p>	<p>Critical business decisions regarding IT investments depend upon reliable and accurate cost information. The current process needs upgradation and there are development distortions in the reporting of actual costs for IT projects within the Project Management System. This project will attempt to fix this broken process and give management the correct information needed for properly managing multi-million-dollar investments in information technology for future readiness in an automated scalable and robust system. The main benefit of this project has to do with improving the integrity of the critical business application, data and the corresponding decision-making processes surrounding this data, security, access control, server-side monitoring, application monitoring such as the Monthly Performance Reports.</p>
<p>Goals / Metrics</p>	<p>Design and develop a complete set of solutions to address root causes behind the impairment of actual cost data in the Project Management System for the uncontrolled downtime of the platform, placed in the current datacenter. At the highest level, this involves two data streams, determine the full extent of the problem through data analysis, micromodule development, and other tests regarding the current platform establishment. Develop solutions for improving all the application and network processes and monitor the results of the implemented solutions with the CISO staff. Server VM migration study is not included here, this will be announced as per movement of server migration plan.</p>
<p>Expected Deliverables</p>	<p>Project Charter, newly developed network design, implementation plan, control Plans, and Project Summary Close Out</p>

Define the Project Scope and Schedule



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Within Scope	This project is limited to only the project that are considered "developmental" since these project components must report development phases on the Azure DevOps. IS team will devise the transformation & movement checklist to transfer OLD-DC devices to the new DC Servers, which is mentioned in the plan & WBS document.			
Outside of Scope	Projects not using the Project Management System will not be reviewed. Additionally, this project will not develop detailed system requirements for the Project Management System. The focus will be on the process itself and how the process relates to source systems for data, and other than the new network design, device installation, everything else is out of scope			
Tentative Schedule (27 working days)		Key Milestone	Start	Complete
		Form Project Team / Preliminary Review / Scope	TBA	TBA
		Finalize Project Plan / Charter / Kick Off	TBA	TBA
		Define Phase	TBA	TBA
		Deploy IaaS and provision all physical servers	TBA	TBA
		Measurement Phase	TBA	TBA
		Analysis Phase	TBA	TBA
		Improvement Phase	TBA	TBA
		Control Phase	TBA	TBA
		Project Summary Report and Close Out	TBA	TBA
Define the Project Resources and Costs				
Project Team	Shahab Al Yamin Chawdhury. In addition to the ten (10) core team members, System Administrative support & deliverables is understood for the life cycle of the project.			



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Support Resources	Project Management Office staff will provide some administrative help. Projects that are reviewed may get tasked to help with data gathering and collection, HW movement etc.			
Special Needs	At least two of the core team members will need network access to the Project Management System (Imran & Uzzal). The project will also need programming support to extract data from two other systems: All NMS and AppPlat NMS for IS Configuration & Verification.			
Cost Type	Vendor / Labor Names	Rate-BDT	Qty	Amount-BDT
Labor	In House Developer Team	0	0	0
Colocation Addition (Monthly recurring chargeable items)	Rack (2) Power (2) Internet (40mbps)	0	0	0
3rd Party Channel Movement	3rd Party channel availability without having more than 3 HOP (source><DC><destination)	0	0	0
HW & SW Configuration	Cisco, Fortinet, DELL Storage, DELL Server, EMS & DC Accessories (Please see individual BoQ on different sheets)	0	0	0
Logistics	In House - Admin Team	0	0	0
VA/PT	In House - CSOC Team	0	0	0
Partner Support	Relevant partners for HW	0	0	0
Sanitization	In House - IS Team	0	0	0
Food & Hotel Cost	Support for In-house team members (Strategy Session)	0	0	0
		Total Cost		0

Define the Project Benefits and Customers



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Process Owner	CISO owns the overall process over this movement reporting for the new application development (ERP), IT Hardware installation to the DC. Each Project Manager must make sure they follow a set of procedures for capturing and reporting actual costs correctly. The Project Management Office provides oversight and support for the processes and completion reporting of activities.	
Key Stakeholders	All personnel assigned to IT Developmental Projects, including Project Managers, Project Analyst, Project Planners, Project Schedulers, and Budget Managers. All personnel who provide leadership support above the project level, including the Chief Information Security Officer, the CISO Staff, Directors and Senior Managers within the IT Department.	
Final Customer	Chief Information Security Officer and Chief Technology Officer	
Expected Benefits	Sustainable AppPlat, which now supports the ground for improvement, in terms of architectural superiority	
Tasks	Descriptions	Percentile
Power	Consistency of sustainable power and precision air conditioners in DC	99
Internet	Network & internet availability	99.99
Channel	3rd Party channel availability without having more than 3 HOP (source><DC><destination)	97
MNO	All MNO Connectivity with Fiber Backbone	97
3 Datacenter Links	Lambda ring network connectivity for DC, NDC, DR	98
Lambda speed	PDC to NDC or FDC is 2ms< PDC & NDC to FDR 3ms<	98
Maintenance on DC	Manned maintenance	99
Monitoring	Network monitoring services (TBA)	98
Goal	DC Service Uptime Assurance to 98.00%	98
Application Platform Development	Clusters will be Installed into multiple physical servers	98



Describe Project Risks, Constraints, and Assumptions

<p>Risks</p>	<ol style="list-style-type: none"> 1. Changes to Project Scope - Project needs to stay focused on root causes behind the source data and not expand the project into developing system requirements for problems with various applications. 2. Bad Data - The availability of cost data within the Project Management System may be so poor that even a basic level of performance cannot be established. 3. Implementation of Solutions - This project will most likely require changes in how Project Managers currently capture and process DB data. In some cases, Project Managers may resist and refuse to adopt these new procedures and recommendations. Thus, the problem with bad data will continue. 4. The understanding of the stakeholder on ERP is somewhat limited, where reluctance to in-house delivery is not understood and intention to purchase 3rd party software & integrations can be continuous, even though the value of the MIS 2.0 may not be understood properly, as the stakeholders limited understanding on adding ad-hoc based solution could lead to an uncontrollable situation on cost, CR, access issues, access rights etc.
<p>Constraints</p>	<ol style="list-style-type: none"> 1. Resources will be constrained to four full-time personnel + 1 System Administrator. IS team does not have adequate manpower to allocate any additional resources for this project. 2. The project team will have direct access to PMP or Six Sigma Black Belts, but the project will be constrained by the fact that a Certified Black Belt is not assigned full time to this project. 3. Programming support will be limited for the project and pulling extracts of data from source systems could be slow since a System Request must be submitted if canned extracts or queries are not adequately available.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

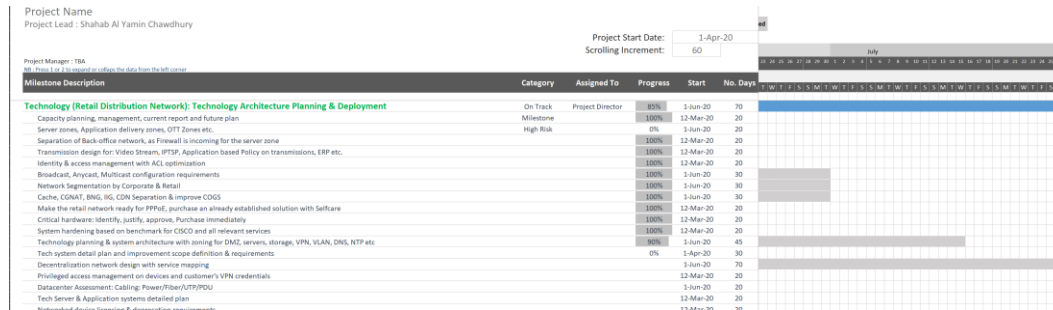
Assumptions

1. The project is following a Six Sigma DMAIC approach. The organization has limited personnel who are experienced in doing projects according to this methodology. This project assumes that all stakeholders will understand and accept the six sigma related work products and deliverables.
2. This project has support from the CEO & MD and the PMO. This project assumes that this sponsorship and support is sufficient to push successful implementation of solutions that result from this project.

Prepared by: **Shahab Al Yamin Chawdhury** Date: **May 1, 2023**

Project WBS

A sample project WBS could look like the following picture (the Gantt chart is provided in the job aids):



Virtual Machine Allocation Plan

The excel worksheet below is for your design and tracking purposes of how the VM's were deployed, and what resources are taken up from the physical server, due to the size of the worksheet, only a screenshot is provided, which I trust you can easily recreate. (also provided in the job aids)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Current Server Allocation										Host										IP										Zone									
Order Name	Model	SN Name	Rank	Proc Qty	Proc Core	Proc GHz	RAM GB	RAM Qty	RAM GB	SSD Qty	SSD GB	Storage GB	OS	Agent IP	Local IP	Sub	NSAID	Public IP	Zone	Platform	Type	App	OS	VM															
Stack Servers (2000)																																							
VM00	VMware	VMware	1	2	40		60	4	16384	4	5	13784 GB								Private																			
VM01	VMware	VMware																		Private																			
VM02	VMware	VMware																		Private																			
VM03	VMware	VMware																		Private																			
VM04	VMware	VMware																		Private																			
VM05	VMware	VMware																		Private																			
VM06	VMware	VMware																		Private																			
VM07	VMware	VMware																		Private																			
VM08	VMware	VMware																		Private																			
VM09	VMware	VMware																		Private																			
VM10	VMware	VMware																		Private																			
VM11	VMware	VMware																		Private																			
VM12	VMware	VMware																		Private																			
Stack Servers (2000)																																							
VM13	VMware	VMware	2	2	40		60	2	16384	4	5	13784 GB								Private																			
VM14	VMware	VMware																		Private																			
VM15	VMware	VMware																		Private																			
VM16	VMware	VMware																		Private																			
VM17	VMware	VMware																		Private																			
VM18	VMware	VMware																		Private																			
VM19	VMware	VMware																		Private																			
VM20	VMware	VMware																		Private																			
VM21	VMware	VMware																		Private																			
VM22	VMware	VMware																		Private																			
Stack Servers (2000)																																							
VM23	VMware	VMware	1	2	40		60	2	16384	4	5	13784 GB								Private																			
VM24	VMware	VMware																		Private																			
VM25	VMware	VMware																		Private																			
VM26	VMware	VMware																		Private																			
VM27	VMware	VMware																		Private																			
VM28	VMware	VMware																		Private																			
VM29	VMware	VMware																		Private																			
VM30	VMware	VMware																		Private																			
VM31	VMware	VMware																		Private																			
VM32	VMware	VMware																		Private																			



BONUS CHAPTER

2

VA/PT Plan

A PLAN FOR THE VULNERABILITY ASSESSMENT AND PENETRATION TESTING NEEDS TO BE DERIVED IF YOU ARE UPGRADING CERTAIN INFRASTRUCTURE DEVICES OR ADDING A NEW SOC. THE FOLLOWING PLAN WAS DERIVED LONG BACK AND COULD HELP YOU GET STARTED.

Plan Document

Purpose

Complexity of systems is increasing day by day. This leads to more and more vulnerabilities in Systems. Attackers use these vulnerabilities to exploit the victim's system. It is better to find out these vulnerabilities in advance before the attacker do. The



power of Vulnerability assessment is usually underestimated. While Vulnerability Assessment and Penetration Testing can be used as a cyber-defense technology to provide proactive cyber defense with an enclosed proposal where we are fundamentally approving Vulnerability Assessment and Penetration Testing (VAPT) as a Cyber defense technology on our most critical systems. We will describe the complete life cycle of Vulnerability Assessment and Penetration Testing on systems or networks and afterwards proactive action will be taken to resolve that vulnerability and stop possible attacks in our systems.

We will describe complete process flow on how to use Vulnerability Assessment and Penetration Testing as a powerful Cyber Defense Technology and will authorize a PenTester (internal or hired) for conducting such testing on our critical systems. Primary focus areas for deploying an effective cyber security measure are:

- a. Detection of network and all systems vulnerabilities
- b. Initiate a Perimeter for Securing Internal Application Services
- c. Limit and Monitor Access to Internal Network
- d. Secure Application & Data Access within the network
- e. Intrusion Detection & Prevention
- f. Minimize Network Crawlers, Ransomwares, Zero Day Exploits
- g. Layer-7 Intelligence and Granular Visibility
- h. Prevention against Unknown Attacks
- i. Threat Intelligence, Context, Granular Visibility on Modern Attacks

Scope of the Project

- **Hardware.** In particular, the servers that are used for hosting multiple critical services like applications, databases housed within virtual machines to be secured should be considered. Virtual Machines and their IP Addresses (155 VM's in total):

SL	Device Type	Quantity	DC/DR
1	Network Switch	11	DC and DR
2	Router	5	DC and DR
3	Firewall	3	DC and DR
4	Load Balancer/WAF	3	DC and DR
5	Blade Server	14	DC and DR
6	Rack Server	7	DC and DR
7	SAN Switch	4	DC and DR
8	Fabric Switch	4	DC and DR

	Total	51	
--	--------------	-----------	--


This is not limited to the following (not an exhaustive list):

SL	Task Description	Modality
1	Information gathering	
2	Requirement analysis	
3	Network diagram review	
4	Vulnerability scan from external	
5	Vulnerability scan from internal	
6	Vulnerability assessment for external	
7	Vulnerability assessment for internal	
8	Attack simulate	
9	Bruit force for SSH	
10	SQL injection	
11	execute exploit based on vulnerability	
12	DoS attack for web application	
13	Segmentation Test	
14	Configuration review	
15	Physical Site visit	
16	Follow up with team to resolve issues	
17	Generate Remediation Report Per Device	

Description of VAPT Services

A vulnerability is a weakness in the application which can be an implementation bug or a design flaw that allows an attacker to cause harm to the user of the application and get extra privilege. Vulnerability is the potential risk for the system. Attacker uses these vulnerabilities to exploit the system and get unauthorized and elevated access and information.

Vulnerabilities are a big flaw in system security and Information assurance. A vulnerability free system can provide more Information Assurance and system security. Though it is almost impossible to have a 100% vulnerability free system, but by removing as many vulnerabilities as possible, we can increase system security. The need of



Vulnerability Assessment and Penetration Testing is usually underestimated till now. It is just considered as a formal activity and use by very less people. By using regular and efficient Vulnerability Assessment, we can reduce the substantial amount of risk to be attacked and have more secured systems.

In this plan, we will describe Vulnerability Assessment and Penetration Testing as an important Cyber Defense Technology. By using VAPT as a Cyber Defense Technology, we can gradually remove vulnerabilities from our system and reduce the possibility of cyber-attack and harden each system. We will describe the complete life cycle of a VAPT for proactive defense. This will also provide a complete process on how to use VAPT as a cyber-defense strategy.


Vulnerability Assessment and Penetration Testing

Vulnerability assessment is the process of scanning the system or software or a network to find out the weakness and loophole in that. These loopholes can provide backdoor to attacker to attack the victimized device or an application platform. A system may have access control vulnerability, Boundary condition vulnerability, Input validation vulnerability, Authentication Vulnerabilities, Configuration Weakness Vulnerabilities, and Exception Handling Vulnerabilities etc.

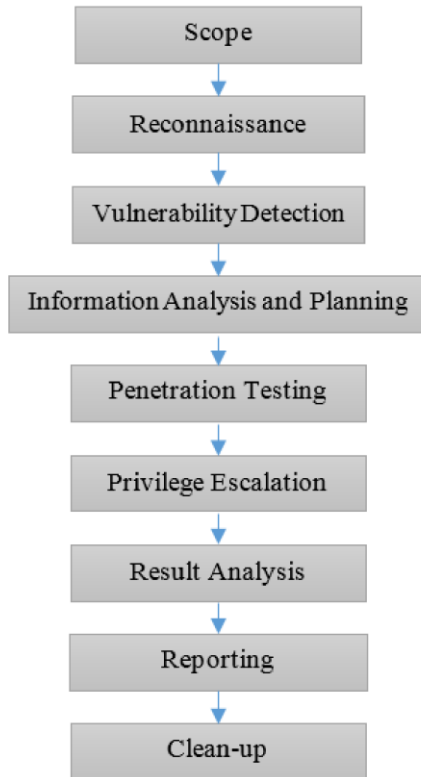
Penetration testing is the next step after vulnerability assessment. Penetration testing is to try to exploit the system in authorized manner to find out the possible exploits in the system. In penetration testing, the tester will have authority to do penetration testing and he intently exploits the system and find out possible exploits. We will provide replica VM's for testing, no live system will be tested, or no configuration will be changed to perform the VA & the PT.

Lifecycle of VAPT

Vulnerability Assessment and Penetration Testing is a total 9 step process. These steps are shown in the below figure. First, the tester has to decide the scope of the assignment (Black/grey/white box). After deciding the scope, the tester gets information about the operating system, network, and IP address in reconnaissance step. After this tester will use various vulnerability assessment technique (explained further) on the testing object to find out vulnerabilities. Then the tester analyses the found vulnerability and make plan for penetration testing. The tester uses this plan to penetrate the victim's system. After penetrating the system, the tester increases the privilege in the system. In result analysis



step, tester analyses all the results and devise recommendation to resolve the vulnerability from the system. All these activities are documented and sent to management to take suitable action. It is crucial to understand that IT Admins will be present during the penetration testing, and no systems will be internally touched / take control of the system / exploit its vulnerabilities and such activities will not take place, even no system or OS level components will not be altered at any point of time.



Vulnerability Assessment & penetration testing techniques

In this section, we will describe some popular VAPT techniques which will be used to conduct in our previously mentioned proposed systems.

Vulnerability Assessment technique

Static analysis

In this technique we do not execute any test case or exploit. We analyze the code structure and contents of the system. With this technique we can find out about all types of vulnerabilities. In this technique we do not exploit the system, so there would be no bad effect of this testing on the system. One of the big disadvantages of this technique is that it is quite slow and require many man-hours to perform.

Manual Testing

In this technique, we do not require any tool or any software to find out vulnerabilities. In this test the pentester uses his own knowledge and experience to find out the vulnerabilities in the system. This testing can be performed with prepared test plan (Systematic manual testing) or without any test plan (Exploratory manual testing). This technique costs higher compared to other techniques, because we do not need to buy any vulnerability assessment tool for this technique, but experience of the pentester is also very costly.

Automated Testing

In automated testing technique the pentester will use automated vulnerability testing tools to find out vulnerabilities in the system. These tools execute all the test cases to find out vulnerabilities. This reduces the man-hours and time required to perform testing. Because of tool repeated testing can also be performed very easily.

Automated testing provides better accuracy than what other techniques provide. It takes very less time and same test cases can be used for future operations over again. But tools increase cost of testing. A single tool is not capable to find out all type of vulnerabilities. So, this increases the total cost to perform vulnerability assessment.

Fuzz Testing

In this test the pentester will try to get response from the system. To check if the system returns or responds or the system crashes or completely gets unresponsive. This is like robustness testing. This technique can be applied with very less human interaction. This technique also can be used to find out zero-day vulnerability.

Penetration Testing Techniques

Black Box Testing

In this technique, the tester does not have any prior knowledge of the network architecture or systems of the testing network. Usually, black box testing is performed from external

network to internal network. A tester have to use his expertise and skills to perform this testing.

Grey Box Testing

In this technique, the tester has some partial knowledge of the testing network. Tester do not have knowledge of complete network architecture, but he will know some basic information of testing network and system configuration. In actuality, Grey box testing is the combination of both the other techniques. This can be performed from internal or external network.

White Box Testing

Testers have complete knowledge of the network configuration of the testing network and the system configuration of the testing network/system. Usually, this testing is performed from the internal network. White box testing requires deep understanding of the testing network or system and provides better results.

Vulnerability Assessment and Penetration Testing Tools

There are many open sources or premium VAPT tools available in the market. Every tool has its expertise and limitations. In Table 1 we have listed Top 15 VAPT tools, their usage and the operating systems on which they are compatible. These make VAPT process fast and more accurate to assess and detect vulnerability in a given system.

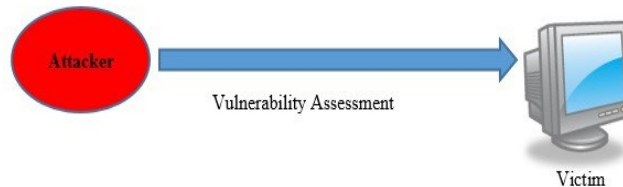
Table: Top 15 VAPT tools.

NO	Name	License	Type	Operating System
1	Metasploit	Proprietary	Vulnerability scanner and exploit	Cross-platform
2	Nessus	Proprietary	Vulnerability scanner	Cross-platform
3	Kali Linux	GPL	Collection of various tools	Linux
4	Burp Suite	Proprietary	web vulnerability scanner	Cross-platform
5	w3af	GPL	web vulnerability scanner	Cross-platform
6	OpenVAS	GPL	Vulnerability scanner	Cross-platform
7	Paros proxy	GPL	web vulnerability scanner	Cross-platform
8	Core Impact	Proprietary	Vulnerability scanner and exploit	Windows
9	Nexpose	Proprietary	Entire vulnerability management lifecycle	Linux, Windows
10	GFI LanGuard	Proprietary	Vulnerability scanner	Windows

11	Acunetix WVS	Proprietary	web vulnerability scanner	Windows
12	QualysGuard	Proprietary	Vulnerability scanner	Cross-platform
13	MBSA	Freeware	Vulnerability scanner	Windows
14	AppScan	Proprietary	web vulnerability scanner	Windows
15	Canvas	Proprietary	Vulnerability scanner and exploit	Cross-platform

VA/PT As A Cyber Defense Technology

In this section we will show how we can consider vulnerability analysis as a cyber-defense technology. What usually attacker do is he reconnaissance the victim's network and get information about victim's network. After receiving system information, attacker performs vulnerability assessment on the victim's network/system and generate a vulnerability list. This is shown in the below picture.



After getting the vulnerability list of the victim, the attacker plans for the possible attack layer by layer. With that list enriches gradually, the attacker exploits the victim's network or system and compromises his system security and information. This is shown in the below picture. But if Victim removes majority of the vulnerabilities from his system, the attacker would not be able to exploit the victim's network/system. By applying VAPT technique user can find out the vulnerabilities those can result in various severe attacks like – Zero-day exploits, DDoS attack, RA flooding, ARP poisoning etc. After finding out the vulnerabilities, a user can apply countermeasures against them. To fix the system from known vulnerabilities, Administrator should find out vulnerabilities in his own system/network. The administrator should apply complete vulnerability and penetration testing cycle on the system/network. When the administrator gets the list of available vulnerability in his system, he should remove those vulnerabilities. To remove the vulnerabilities, the administrator should apply the necessary patches, updates, install

necessary software's and other requisites. In this way an administrator should remove all vulnerabilities from his system/network.



Figure 1 Attacker exploiting victim's system

Now, if the attacker would run a vulnerability assessment of the victim's system/network, he would not find any known open vulnerability in the victim's system/network. In the absence of open vulnerabilities in the system, the attacker would not be able to exploit victim's system/network. Therefore, by using Vulnerability Assessment and Penetration Testing as a cyber- defense, technology administrators can be able to save his resources and critical information and can achieve proactive cyber defense.

Conclusion and Future Work

In this plan, we have explained how Vulnerability Assessment and Penetration Testing can be used as an effective cyber defense technology. We have also described why VAPT should be made a compulsory activity for cyber defense in a periodic manner. This document clearly explains the necessity to increase use of VAPT for complete system security and would be able to withstand open and known system vulnerabilities, and can stop major cyber-attacks and would be able to provide hardened system security.

Point of Contact

Communicating points of contact for all phases of a project is vital in order to ensure stakeholders understand who can address questions or concerns related to various aspects of the project. This is especially true for implementation and migration of applications as this may be an extremely fluid part of the project, and the responsibility may be shifting from one IT Group to another.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

The VAPT Testing Project spans several different levels of operations of the company is an extremely fluid in technical projects. As such, it is important to understand the points of contact for the various aspects of this project. The chart below provides all stakeholders with points of contact should any urgent questions or concerns arise. All stakeholders should ensure their communications are compliant with the VAPT Testing Plan.

Name	Role	Contact Information
TBA	Project Sponsor	
TBA	Independent Director	
Shahab Al Yamin Chawdhury	CISO	
	IT Admin	
	IT Admin	
TBA	Project Manager	

Project Manager Nomination

I/We hereby undersigned nominate the following person to be the “**Project Director**” for the deployment of “**VA/PT Testing**”:

Name	Title	Date
Nomination Accepted by		
SHAHAB AL YAMIN CHAWDHURY	CISO	

Computer Forensic & Cyber Security Tools, Open-Source)

Disk Tools & Data Capture

Name	From	Description
Arsenal Image Mounter	Arsenal Recon	Mounts disk images as complete disks in Windows, giving access to Volume Shadow Copies, etc.
DumpIt	MoonSols	Generates physical memory dump of Windows machines, 32 bits 64 bit. Can run from a USB flash drive.
EnCase Forensic Imager	Guidance Software	Create EnCase evidence files and EnCase logical evidence files [direct download link]
Encrypted Disk Detector	Magnet Forensics	Checks local physical drives on a system for TrueCrypt, PGP, or Bitlocker encrypted volumes.
FAT32 Format	Ridgecrop	Enables large capacity disks to be formatted as FAT32.
Forensics Acquisition of Websites	Web Content Protection Association	Browser designed to forensically capture web pages.
FTK Imager	AccessData	Imaging tool, disk viewer and image mounter.
Guymager	vogu00	Multi-threaded GUI imager under running under Linux.
Live RAM Capturer	Belkasoft	Extracts RAM dump including that protected by an anti-debugging or anti-dumping system. 32 and 64 bit builds
NetworkMiner	Hjelmvik	Network analysis tool. Detects OS, hostname and open ports of network hosts through packet sniffing/PCAP parsing.
Nmap	Nmap	Utility for network discovery and security auditing.
Magnet RAM Capture	Magnet Forensics	Captures physical memory of a suspect's computer. Windows XP to Windows 10, and 2003, 2008, 2012. 32 & 64 bit.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

OSFClone	Passmark Software	Boot utility for CD/DVD or USB flash drives to create dd or AFF images/clones.
OSFMount	Passmark Software	Mounts a wide range of disk images. Also allows creation of RAM disks.

Email Analysis

Name	From	Description
EDB Viewer	Lepide Software	Open and view (not export) Outlook EDB files without an Exchange server.
Mail Viewer	MiTeC	Viewer for Outlook Express, Windows Mail/Windows Live Mail, Mozilla Thunderbird message databases and single EML files.
MBOX Viewer	SysTools	View MBOX emails and attachments.
OST Viewer	Lepide Software	Open and view (not export) Outlook OST files without connecting to an Exchange server.
PST Viewer	Lepide Software	Open and view (not export) Outlook PST files without needing Outlook.

General Tools

Name	From	Description
Agent Ransack	Mythicsoft	Search multiple files using Boolean operators and Perl Regex.
Computer Forensic Reference Data Sets	NIST	Collated forensic images for training, practice and validation.
EvidenceMover	Nuix	Copies data between locations, with file comparison, verification, logging.
FastCopy	Shirouzu Hiroaki	Self labelled 'fastest' copy/delete Windows software. Can verify with SHA-1, etc.
File Signatures	Gary Kessler	Table of file signatures.
HexBrowser	Peter Fiskstrand	Identifies over 1000 file types by examining their signatures.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

HashMyFiles	Nirsoft	Calculate MD5 and SHA1 hashes.
MobaLiveCD	Mobatek	Run Linux live CDs from their ISO image without having to boot to them.
Mouse Jiggler	Arkane Systems	Automatically moves mouse pointer stopping screen saver, hibernation etc..
Notepad ++	Notepad ++	Advanced Notepad replacement.
NSRL	NIST	Hash sets of 'known' (ignorable) files.
Quick Hash	Ted Technology	A Linux & Windows GUI for individual and recursive SHA1 hashing of files.
USB Write Blocker	DSi	Enables software write-blocking of USB ports.
Volix	FH Aachen	Application that simplifies the use of the Volatility Framework.
Windows Forensic Environment	Troy Larson	Guide by Brett Shavers to creating and working with a Windows boot CD.

File and Data Analysis

Name	From	Description
Advanced Prefetch Analyser	Allan Hay	Reads Windows XP,Vista and Windows 7 prefetch files.
analyzeMFT	David Kovar	Parses the MFT from an NTFS file system allowing results to be analysed with other tools.
bstrings	Eric Zimmerman	Find strings in binary data, including regular expression searching.
CapAnalysis	Evolka	PCAP viewer.
Crowd Response	CrowdStike	Windows console application to aid gathering of system information for incident response and security engagements.
Crowd Inspect	CrowdStrike	Details network processes, listing binaries associated with each process. Queries VirusTotal, other malware repositories & reputation services to produce "at-a-glance" state of the system.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

DCode	Digital Detective	Converts various data types to date/time values.
Defraser	Various	Detects full and partial multimedia files in unallocated space.
eCryptfs Parser	Ted Technology	Recursively parses headers of every eCryptfs file in selected directory. Outputs encryption algorithm used, original file size, signature used, etc.
Encryption Analyzer	Passware	Scans a computer for password-protected & encrypted files, reports encryption complexity and decryption options for each file.
ExifTool	Phil Harvey	Read, write and edit Exif data in a large number of file types.
File Identifier	Toolsley.com	Drag and drop web-browser JavaScript tool for identification of over 2000 file types.
Forensic Image Viewer	Sanderson Forensics	View various picture formats, image enhancer, extraction of embedded Exif, GPS data.
Ghiro	Alessandro Tanasi	In-depth analysis of image (picture) files.
Highlighter	Mandiant	Examine log files using text, graphic or histogram views.
Link Parser	4Discovery	Recursively parses folders extracting 30+ attributes from Windows .lnk (shortcut) files.
LiveContactsView	Nirsoft	View and export Windows Live Messenger contact details.
PECmd	Eric Zimmerman	Prefetch Explorer.
RSA Netwitness Investigator	EMC	Network packet capture and analysis.

Mac OS Tools

Name	From	Description
Audit	Twocanoes Software	Audit Preference Pane and Log Reader for OS X.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Disk Arbitrator	Aaron Burghardt	Blocks the mounting of file systems, complimenting a write blocker in disabling disk arbitration.
Epoch Converter	Blackbag Technologies	Converts epoch times to local time and UTC.
FTK Imager CLI for Mac OS	AccessData	Command line Mac OS version of AccessData's FTK Imager.
IORegInfo	Blackbag Technologies	Lists items connected to the computer (e.g., SATA, USB and FireWire Drives, software RAID sets). Can locate partition information, including sizes, types, and the bus to which the device is connected.
mac_apt	Yogesh Khatri, Champlain College	Mac OS triage tool, works usable against E01, DD, DMG and mounted images
Volafox	Kyeongsik Lee	Memory forensic toolkit for Mac OS X

Mobile Devices

Name	From	Description
iPBA2	Mario Piccinelli	Explore iOS backups.
iPhone Analyzer	Leo Crawford, Mat Proud	Explore the internal file structure of Pad, iPod and iPhones.
ivMeta	CSI Tech	Extracts phone model and software version and created date and GPS data from iPhone videos.
SAFT	SignalSEC Corp	Obtain SMS Messages, call logs and contacts from Android devices.

Data Analysis Suites

Name	From	Description
Autopsy	Brian Carrier	Graphical interface to the command line digital investigation analysis tools in The Sleuth Kit (see below).

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Backtrack	Backtrack	Penetration testing and security audit with forensic boot capability.
Caine	Nanni Bassetti	Linux based live CD, featuring a number of analysis tools.
Digital Forensics Framework	ArxSys	Analyses volumes, file systems, user and applications data, extracting metadata, deleted and hidden items.
Forensic Scanner	Harlan Carvey	Automates 'repetitive tasks of data collection'. Fuller description here.
Kali Linux	Offensive Security	Comprehensive penetration testing platform
Paladin	Sumuri	Ubuntu based live boot CD for imaging and analysis.
SIFT	SANS	VMware Appliance pre-configured with multiple tools allowing digital forensic examinations.
The Sleuth Kit	Brian Carrier	Collection of UNIX-based command line file and volume system forensic analysis tools.
Volatility Framework	Volatile Systems	Collection of tools for the extraction of artefacts from RAM.

File Viewers

Name	From	Description
BKF Viewer	SysTools	https://www.systoolsgroup.com/lotus-dxl-viewer.html
DXL Viewer	SysTools	View (not save or export) Lotus Notes DXL file emails and attachments.
E01 Viewer	SysTools	View (not save or export from) E01 files & view messages within EDB, PST & OST files.
MDF Viewer	SysTools	View (not save or export) MS SQL MDF files.
MSG Viewer	SysTools	View (not save or export) MSG file emails and attachments.
OLM Viewer	SysTools	View (not save or export) OLM file emails and attachments.

Internet Analysis

Name	From	Description
Browser History Capturer	Foxtton Software	Captures history from Firefox, Chrome, Internet Explorer and Edge web browsers running on Windows computers.
Browser History Viewer	Foxtton Software	Extract, view and analyse internet history from Firefox, Chrome, Internet Explorer and Edge web browsers.
Chrome Session Parser	CCL Forensics	Python module for performing off-line parsing of Chrome session files (“Current Session”, “Last Session”, “Current Tabs”, “Last Tabs”).
ChromeCacheView	Nirsoft	Reads the cache folder of Google Chrome Web browser, and displays the list of all files currently stored in the cache.
Cookie Cutter	Mike’s Forensic Tools	Extracts embedded data held within Google Analytics cookies. Shows search terms used as well as dates of and the number of visits.
Dumpzilla	Busindre	Runs in Python 3.x, extracting forensic information from Firefox, Iceweasel and Seamonkey browsers. See manual for more information.
Facebook Profile Saver	Belkasoft	Captures information publicly available in Facebook profiles.
IECookiesView	Nirsoft	Extracts various details of Internet Explorer cookies.
IEPassView	Nirsoft	Extract stored passwords from Internet Explorer versions 4 to 8.
MozillaCacheView	Nirsoft	Reads the cache folder of Firefox/Mozilla/Netscape Web browsers.
MozillaCookieView	Nirsoft	Parses the cookie folder of Firefox/Mozilla/Netscape Web browsers.
MozillaHistoryView	Nirsoft	Reads the history.dat of Firefox/Mozilla/Netscape Web browsers, and displays the list of all visited Web page.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



MyLastSearch	Nirsoft	Extracts search queries made with popular search engines (Google, Yahoo and MSN) and social networking sites (Twitter, Facebook, MySpace).
PasswordFox	Nirsoft	Extracts the user names and passwords stored by Mozilla Firefox Web browser.
OperaCacheView	Nirsoft	Reads the cache folder of Opera Web browser, and displays the list of all files currently stored in the cache.
OperaPassView	Nirsoft	Decrypts the content of the Opera Web browser password file, wand.dat
Web Historian	Mandiant	Reviews list of URLs stored in the history files of the most commonly used browsers.
Web Page Saver	Magnet Forensics	Captures how web pages look at a specific point in time

Registry Analysis

Name	From	Description
AppCompatCache Parser	Eric Zimmerman	Dumps list of shimcache entries showing which executables were run and their modification dates. Further details.
ForensicUserInfo	Woanware	Extracts user information from the SAM, SOFTWARE and SYSTEM hives files and decrypts the LM/NT hashes from the SAM file.
Process Monitor	Microsoft	Examine Windows processes and registry threads in real time.
RECcmd	Eric Zimmerman	Command line access to offline Registry hives. Supports simple & regular expression searches as well as searching by last write timestamp. Further details.
Registry Decoder	US National Institute of Justice, Digital Forensics Solutions	For the acquisition, analysis, and reporting of registry contents.



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Registry Explorer	Eric Zimmerman	Offline Registry viewer. Provides deleted artefact recovery, value slack support, and robust searching. Further details.
RegRipper	Harlan Carvey	Registry data extraction and correlation tool.
Regshot	Regshot	Takes snapshots of the registry allowing comparisons e.g., show registry changes after installing software.
ShellBags Explorer	Eric Zimmerman	Presents visual representation of what a user's directory structure looked like. Additionally exposes various timestamps (e.g., first explored, last explored for a given folder. Further details.
USB Device Forensics	Woanware	Details previously attached USB devices on exported registry hives.
USB Historian	4Discovery	Displays 20+ attributes relating to USB device use on Windows systems.
USBDeview	Nirsoft	Details previously attached USB devices.
PasswordFox	Nirsoft	Extracts the user names and passwords stored by Mozilla Firefox Web browser.
UserAssist	Didier Stevens	Displays list of programs run, with run count and last run date and time.
Windows Registry Recovery	MiTec	Extracts configuration settings and other information from the Registry.

Application Analysis

Name	From	Description
DFIR	Magnet Forensics	Various Tools
Google Maps Tile Investigator	Magnet Forensics	Takes x,y,z coordinates found in a tile filename and downloads surrounding tiles providing more context.
KaZAlyser	Sanderson Forensics	Extracts various data from the KaZaA application.
LiveContactsView	Nirsoft	View and export Windows Live Messenger contact details.
SkypeLogView	Nirsoft	View Skype calls and chats.

For Reference

Name	From	Description
HotSwap	Kazuyuki Nakayama	Safely remove SATA disks similar to the “Safely Remove Hardware” icon in the notification area.
IEHistoryView	Nirsoft	Extracts recently visited Internet Explorer URLs.
LiveView	CERT	Allows examiner to boot dd images in VMware.
Ubuntu guide	How-To Geek	Guide to using an Ubuntu live disk to recover partitions, carve files, etc.
WhatsApp Forensics	Zena Forensics	Extract WhatsApp messages from iOS and Android backups.
iPhone Backup Browser	Rene Devichi	View unencrypted backups of iPad, iPod and iPhones.

Password Protection

Name	From	Description
Password Strength Test	How Secure Is My Password	Enter your password and see how long it will take for a computer to crack it
Secure Password Check	Kaspersky	Check how secure a password is
Password Manager	LastPass	Password storer with AES-256 bit encryption with PBKDF2 SHA-256 and salted hashes.
Password Manager	StickyPassword	Password Manager using AES-256 encryption

Password Hacking Protection

Name	From	Description
------	------	-------------

HavelBeenPwnd

[haveibeenpwned](#)

Check if you have an account that has been compromised in a data breach

Browsing Security

Name	From	Description
No Script	NoScript	NoScript Firefox extension provides extra protection for Firefox, Seamonkey and other mozilla-based browsers
Comodo Dragon	Comodo Cybersecurity	A Chromium technology-based Web Browser that offers you all of Chrome's features PLUS the unparalleled level of security and privacy
TOR	TOR Project	Experience real private browsing without tracking, surveillance, or censorship.
Disconnect	Disconnect	Get greater transparency and control over the personal information you share online

Redirect Checkers

Name	From	Description
Where Goes	Where Goes	takes a URL and shows you the entire path of redirects and meta-refreshes that leads to the final destination.
Redirect Detective	Redirect Detective	Redirect Detective is a free URL redirection checker that allows you to see the complete path a redirected URL goes through.
Redirect Check	Redirect Check	This site is used to chase the redirection of URLs.

Website URL Checkers

Name	From	Description
------	------	-------------

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



VirusTotal	Virus Total	Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community
ScanURL	Scan URL	See if a website has been reported for phishing, hosting malware/viruses, or poor reputation. We check with reputable 3rd-party services, such as Google Safe Browsing Diagnostic, PhishTank, and Web of Trust (WOT).
Site Safety Center	TrendMicro	can check the safety of a particular URL that might seem suspicious
Zulu	Zscaler	Zulu is a dynamic risk scoring engine for web based content

Data Removal

Name	From	Description
Eraser	Heidi	Completely remove sensitive data from your hard drive





BONUS CHAPTER

3

IT Service Strategy Planning

SINCE YOUR HELPDESK WILL BE THE EPICENTER OF ALERTS OF SERVICE CALLS AND GENERATION OF TICKET, ITS ALWAYS BENEFICIAL TO INTEGRATE THE SERVICE OR SUPPORT OR YOUR CALL CENTER TO THE SAME CAUSE. YOU ARE ALSO FREE TO HAVE A SEPARATE SOC CALL CENTER AS WELL IF YOU HAVE THE EXTRA BUDGET.

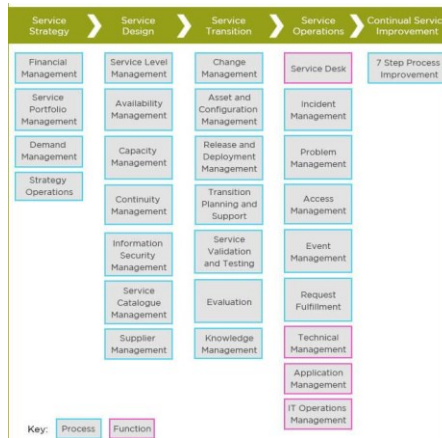
Service Strategy deals with the strategic analysis, planning, positioning, and implementation relating to IT service models, strategies, and objectives. It provides guidance on leveraging service management capabilities to effectively deliver value to customers and illustrates value for service providers. In short:



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Process & Functions



The following people, process and products combine to make this a functional operating unit with IT:

- People
 - Service Definition Manager



- Service Research Manager
- Financial Analysis Manager
- Service Marketing Manager
- Service Forecast Manager
- Process
 - Portfolio Management
 - Financial Management
 - Demand Management
- Products
 - Service Request & Planning Tools
 - Service Knowledge & Configuration Management Tools

IT Service Design – Modeling the IT Services

Service Design translates strategic plans and objectives and creates the designs and specifications for execution through service transition and operations.

- People
 - Enterprise Architect: Network, NOC, SOC
 - Application Architect
 - Security Engineering Manager
 - Desktop Engineering Manager
 - Network Engineering Manager
 - Systems, Servers & Storage Engineering Manager
 - Applications Engineering Manager
- Process
 - Service Catalogue Management
 - Service Level Management
 - Capacity Management
 - Availability Management
 - Continuity Management
 - Information Security Management
 - Supplier Management
- Products
 - Service Catalogue Tools
 - Service Level Management Tools
 - Capacity Planning Tools
 - Service Modeling Tools
 - Service Knowledge & Configuration Management Tools

IT Service Transition - Implementing the IT Services

Service Transition provides guidance on the service design and implementation, ensuring that the service delivers the intended strategy and can be operated and maintained effectively.

People

- Security Asset Manager
- Desktop Asset Manager
- Network Asset Manager
- Systems, Servers & Storage Asset Manager
- Applications Asset Manager

Process

- Support & Transition Management
- Change Management
- Asset & Configuration Management
- Release & Deploy Management
- Validation Management
- Evaluation Management
- Knowledge Management

Products

- Asset Management Tool
- Service provision Tool
- Run Book Task Automation Tools
- Service Knowledge & Configuration Management Tools

IT Service Operation – Managing the IT Services

Service Operation provides guidance on managing a service through its day-to-day production life. It also provides guidance on supporting operations by means of new models and architectures such as shared services, utility computing, web services, and mobile commerce.

People

- Security Operation Manager
- Desktop Operations Manager
- Network Operations Manager
- Systems, Server & Storage Operations Manager
- Applications Operations Manager

Process

- Event Management
- Incident Management
- Problem Management
- Fulfillment Management
- Access Management
- Service Desk Function Management
- Service Operations Function Management
- Technical Operations Function Management
- Application Operations Function Management

Products

- Service Desk with Incident Management Tool
- Problem Management Tool
- Event Management Tool
- Run Book Technology Troubleshooting Tool
- Run Book Application Troubleshooting Tool
- Service Knowledge & Configuration Management Tools

IT Continual Service Improvement – Measuring the IT Services

Continual Service Improvement provides guidance on measuring service performance through the service life cycle, suggesting improvements in service quality, operational efficiency and business continuity.

People

- Service Measurement Manager
- Quality Measurement Manager

- Compliance Measurement Manager
- Security Measurement Manager
- Resource Measurement Manager

Process

- IT Governance Management (using COBIT best practices)
- IT Resource Management (using PMI methods)
- IT Quality Management (using Six Sigma methods)
- IT Security Management (using ISO standards)

Products

- Compliance Management & Measurement Tools
- Service Knowledge & Configuration Management Tools

Standardize the IT Service Desk

Standardizing the IT Service Desk or HelpDesk to improve the quality and consistency of IT support services. It involves defining and implementing best practices, policies, and procedures for handling IT incidents and requests. By standardizing the IT Service Desk or HelpDesk, you can achieve the following benefits:

- Increase customer satisfaction and loyalty by providing timely and reliable IT support.
- Reduce costs and risks by minimizing errors, rework, and escalations.
- Improve efficiency and productivity by streamlining workflows and automating tasks.
- Enhance collaboration and communication by aligning IT teams and stakeholders.
- Foster continuous improvement and innovation by measuring and reporting on performance and outcomes.

IT Governance & Management Principles

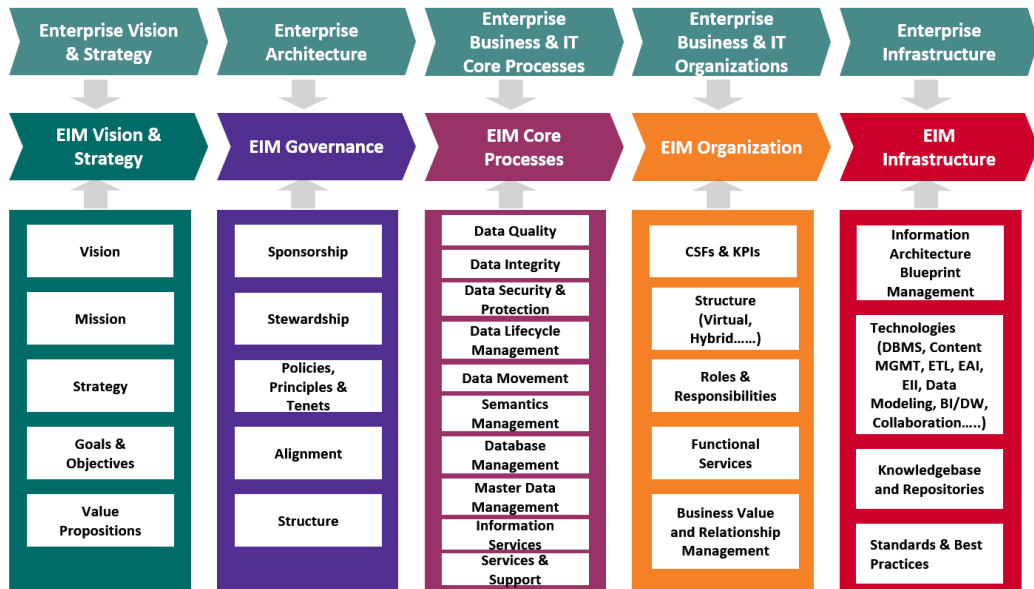
Source: [Enterprise Information Management Framework - Xtensible Solutions](#)

Like many data-driven organizations, utilities often become involved with maintaining numerous data silos underlying the systems used to manage their business. Often the focus becomes managing the data silos rather than leveraging the systems to the benefit of the enterprise.

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

To correct or avoid this situation, enterprises must establish a strategy that includes best practices around people, processes, and technologies to facilitate agile and adaptable information management solutions.

This strategy, called Enterprise Information Management (EIM), encompasses five key components: Vision and Strategy, Governance, Core Processes, Organization, and Infrastructure.




EIM Vision and Strategy

EIM vision and strategy focuses on developing a comprehensive framework and effective road map for iterative and incremental implementation of an enterprise approach to information management. This approach will lead to accurate, consistent, secure, and transparent access to data that flows seamlessly and continuously throughout the enterprise. EIM vision and strategy promotes consensus among business and IT on the meaning of EIM, what problems EIM will address and the value it will bring to the enterprise.

EIM Governance

EIM governance is required to achieve alignment between business and IT as well as to establish respective roles and responsibilities for data and information management



across the enterprise. The governance structure addresses the development, maintenance, communication and enforcement of data management policies and procedures, in addition to the data quality, services, tools and technologies needed to move to an enterprise-wide data management and services culture. EIM governance is critical to ensuring that stakeholders feel confident in leading the charge toward realizing EIM vision and strategy.

EIM Core Processes

EIM includes the definition of core information management processes that support EIM governance and services as well as integration of the processes at user, business and data levels. These core processes target increased accountability and transparency of information across the enterprise and define metadata and master data strategies. Semantic formalization of information is added to the EIM through the development, management and use of an Enterprise Semantic Model (ESM). An ESM provides consistent design and implementation of data and information services across transactional and analytical systems.

EIM Organization

A complete EIM strategy addresses the organization required to ensure a successful EIM initiative. It provides a formal mechanism for developing required EIM core competencies and enables the realization of EIM's value by both IT and business. EIM organization considers key performance indicators and critical success factors as well as roles and responsibilities, structure, and deployment using a logical, incremental approach for resourcing.

EIM Infrastructure

EIM infrastructure provides the definition of a standards-based open platform that consists of data, metadata management, semantic reconciliation and closed-loop information flows for master data and converged content. Decisions to make when establishing the EIM infrastructure include:

- Selecting standards and best practices using existing or new tools and technologies to implement information services.
- Procuring tools that allow data assets to be more widely available.
- Acquiring resources that enable business intelligence and near real time dashboards for more effective and intelligent business operations.

Most Used Frameworks

COBIT: Published by ISACA, COBIT is a comprehensive framework of “globally accepted practices, analytical tools and models” (PDF) designed for governance and management of enterprise IT. With its roots in IT auditing, ISACA expanded COBIT’s scope over the years to fully support IT governance. The latest version is COBIT 5, which is widely used by organizations focused on risk management and mitigation.

ITIL: Formerly an acronym for Information Technology Infrastructure Library, ITIL focuses on IT service management. It aims to ensure that IT services support core processes of the business. ITIL comprises five sets of management best practices for service strategy, design, transition (such as change management), operation and continual service improvement.

COSO: This model for evaluating internal controls is from the Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO’s focus is less IT-specific than the other frameworks, concentrating more on business aspects like enterprise risk management (ERM) and fraud deterrence.

CMMI: The Capability Maturity Model Integration method, developed by the Software Engineering Institute, is an approach to performance improvement. CMMI uses a scale of 1 to 5 to gauge an organization’s performance, quality and profitability maturity level. According to Calatayud, “allowing for mixed mode and objective measurements to be inserted is critical in measuring risks that are qualitative in nature.”

FAIR: Factor Analysis of Information Risk (FAIR) is a relatively new model that helps organizations quantify risk. The focus is on cyber security and operational risk, with the goal of making more well-informed decisions. Although it’s newer than other frameworks mentioned here, Calatayud points out that it’s already gained a lot of traction with Fortune 500 companies.

COBIT Framework v5

Control Objectives for Information and Related Technology (COBIT) is a framework created by ISACA for information technology (IT) management and smart IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues, and business risks.

COBIT 5 Process Reference Model

COBIT 5 contains a process reference model which consists of 37 generic processes required for the governance and management of enterprise IT. These processes are organized in 5 groups:

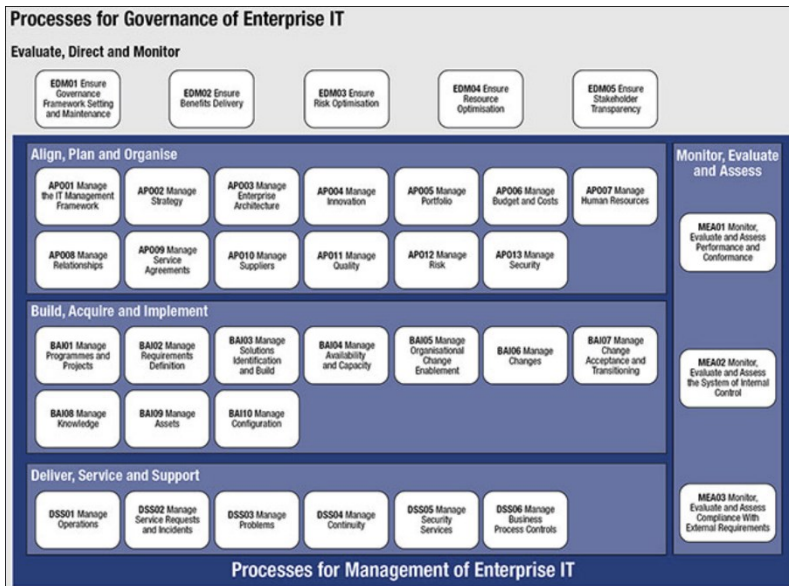
COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

- Evaluate Direct and Monitor (EDM)
- Align, Plan and Organize (APO)
- Build, Acquire and Implement (BAI)
- Deliver, Service and Support (DSS)
- Monitor, Evaluate and Assess (MEA)

These processes are described in detail in *COBIT 5: Enabling Processes*. The COBIT 5 process reference model subdivides the IT-related practices and activities of the enterprise into 2 main areas—governance and management—with management further divided into domains of processes:

The governance domain contains 5 governance processes. Within each process, Evaluate, Direct and Monitor (EDM) practices are defined.

The management domains are in line with the responsibility areas of Plan, Build, Run and Monitor (PBRM).



Source: [Portfolio, Program and Project Management Using COBIT 5 \(isaca.org\)](http://Portfolio, Program and Project Management Using COBIT 5 (isaca.org))

Common Service Desk Challenges

- Low business satisfaction

- Disconnected to SOC services where a critical vulnerability is reported yet it's not conveyed to the SOC team. The tool is not provide by SOC and not monitored, independently operating.
- Users are unable to get assistance with IT services quickly.
- Users go to their favorite technician instead of using the service desk.
- Service desk managers struggle to set and meet service-level expectations, which further compromises end-user satisfaction.
- High cost to resolve
 - Connected SOC tools are inadequate and the helpdesk manager got multiple portals to support.
 - Tier 2 and tier 3 resolve issues that should be resolved at tier 1.
 - Tier 2 and tier 3 often interrupt projects to focus on service support.
 - Specialists would rather work on projects than provide service support.
- Unresolved issues
 - Tickets are not created for all incidents.
 - Tickets are lost or escalated to the wrong technicians.
 - Poor data (input validation is not maintained) impedes root-cause analysis of incidents.
- Poor planning
 - Lack of data for effective trend analysis leads to poor demand planning.
 - Lack of data leads to lost opportunities for templating and automation.
 - The Service Desk lacks processes and workflows to provide consistent service.
- Lost resources or accountability
 - Lack of cross-training and knowledge sharing.
 - Lack of skills coverage for critical applications and services.
 - Time wasted troubleshooting recurring issues. o Reports unavailable due to lack of data and ineffective categorization.

Ways That the Service Desk Handles Cybersecurity

- The service desk follows the best practices and guidelines for IT service management, such as the ITIL framework, which covers various aspects of IT security, such as security incident management, security policy, and security awareness.
- The service desk uses the right software and tools to monitor, manage, and secure the IT environment, such as antivirus software, firewalls, backups, automation, and encryption. The service desk also keeps the devices and applications updated and patched to prevent vulnerabilities and exploits.

- The service desk trains its staff and end users on how to identify and prevent cybersecurity risks, such as phishing, malware, ransomware, and social engineering and report to SOC with collected or recorded data. The service desk also educates them on how to follow the security policies and procedures, such as using strong passwords, avoiding public Wi-Fi, and reporting suspicious activities.
- The service desk collaborates and communicates with other IT teams and stakeholders, such as the InfoSec team, the IT governance team, and the business units, to ensure a coordinated and consistent approach to cybersecurity. The service desk also reports and analyzes security incidents and requests and provides feedback and recommendations for improvement.

If your service desk is not up to the mark, try starting from the start, again. By checking on the following:

12. Assess current state. Time, resource and quality of manpower. Input validation by the T1, T2, T3 and train properly for problem inputs.
13. Communication & implementation roadmap, documented processes and process performance.
14. Assurance: Service desk SoP. Integrated remote support options.
15. Maturity assessment & current model analysis, if the SOC requirements are addressed in the model or not.
16. Incident and ticket generation workflows with integrated data collection and video recording methods.
17. Review ticket handling procedures (chat, walk-ins, web portal, phone, email etc.) (this portal should have ID provider integration for better visibility and lesser typing) (application-based notifications or SMS based or web based apps were used).
18. Identify metrics and reports, mapped to RACI.
19. Import incident escalation management workflows from SOC. Service level response and resolution (SLOR&R) time.
20. Revisit ticket category-wise service list, and update as required with integrated KB generations.

Pro-Tip

• IT & SOC must not use different ticketing system, otherwise there will be a workflow conflict. most of the ITSM softwares are now equipped with AI as well, take advantage of that feature.



BONUS CHAPTER

4

Jurisdiction Assignment Matrix

THIS IS THE BUSINESS AND OPERATIONAL REQUIREMENTS WHERE IT'S OUTLINED ON WHO WILL DO WHAT BY MARKING THEIR LIMIT TO AUTHORITATIVE TASKS AND ACTIVITIES. THIS PERSPECTIVE ALSO DEFINES WORK ROLES PERFORMED BY CERTAIN INDIVIDUALS, AND THEIR ROLES ARE AUTHORIZED AND UNDERSTOOD BY THE STAKEHOLDERS AND APPROVED. DO CHANGE AS REQUIRED.

The file is provided in the Job-aid folder named "Technology Responsibility and Jurisdiction Assignment Matrix_V3.1.xlsx"



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Technology Responsibility & Jurisdiction Assignment Matrix									
Operational & Organizational Risk Management									
Partial Fulfillment for ISO/IEC 27001, ER(Risk & Resource)M, BCP, DRP									
Document Number: XX/ISMS/TRJAM/01 Version: 3.1 Submitted Date: 6th July 2022 Last Review Date: 25th January 2024									
R-Responsible A-Accountable C-Consulted I-Informed									
SL	Task Head	Task Sub-head	Current Status	Progress	RACI	Owner	Submit to	Audit	Description
	Board Reporting	Policy Development	N/A		RA	IS	Board	I	Board will periodically review process and security measure requirement analysis and take necessary improvement requirements
		Direct Board Reporting	N/A		RA	IS, Audit, PMO	Board	I	Security team, Audit, PMO
		Organizational Risk Management	N/A		RA	IS	Board	I	Board will periodically review process and security measure requirement analysis directly related to business, and take necessary improvement requirements
	IT, IS Governance Program	Identity & Access Management	N/A		RA	I (IS)	IC (IS)	I	All networked devices access management including VPN access will be managed and maintained by IS team
		Enterprise Risk Management (ERM)	N/A		RA	I (IS)	Board	I	Whole networked device assessment according to the NIST / CISECURITY standard and provide actionable guidance to the stakeholders and to the Board
		Policy & process development	N/A		RA	I (IS)	Board	I	Will be vetted by IS team

You can also add different roles and their profiles into this worksheet as well for the SOC manager, L1/L2/L3 analysts tasks and roles explicitly carried out on a daily basis, and the accompanied RACI will enable them jurisdictions to perform certain tasks, so that no one questions their authority over certain aspects of their job functions, roles and responsibilities, tasks, and activities.



References

1. [What is a security operations center \(SOC\)? | Microsoft Security](#)
2. [The Importance of the Security Operations Center \(SOC\) - Check Point Software](#)
3. [What is Security Operations Center \(SOC\)? Working Structure and Benefits | by Ismail Tasdelen | DataBulls | Medium](#)
4. [What is a Security Operations Center \(SOC\)? | StackScale](#)
5. [What Is a Security Operations Center | Cybersecurity | CompTIA](#)
6. [What is Security Operations Center \(SOC\)? | IBM](#)
7. [Security Operations Center \(SOC\) Best Practices - Check Point Software](#)
8. [What Is a Security Operations Center? Complete Guide \(exabeam.com\)](#)
9. [A Small Business Guide to the Security Operations Center \(fool.com\)](#)
10. [7 Steps to Building A Security Operations Center \(SOC\) | LogRhythm](#)
11. [How to Build a Security Operations Center \(SOC\): Peoples, Processes, and Technologies \(digitalguardian.com\)](#)
12. [Cybersecurity Career Master Plan \(packt-cdn.com\) | by Dr. Gerald Auger](#)
13. [Sigma rules explained: When and how to use them to log events | CSO Online](#)
14. [The Ultimate Guide to Sigma Rules \(graylog.org\)](#)
15. [Career Scope as a SOC Professional - InfosecTrain](#)
16. [Security Operations Center \(SOC\) Roles and Responsibilities - Palo Alto Networks](#)
17. [What Is an SOC Analyst? \(Background, Skills, & Requirements\) \(springboard.com\)](#)
18. [What is Tier 1, 2, 3 Incident Response? A Cybersecurity Expert Explains - Cyber Insight](#)
19. [SOC Analyst Types Explained: Tier 1, 2 & 3 | Legends of Tech Blog](#)
20. [What Is a Security Operations Center \(SOC\)? - Palo Alto Networks](#)
21. [Tier 3 Advanced Security Analyst or Threat Hunter - Trilight Security](#)
22. [What is a SOC-as-a-Service \(SOCaaS\)? - CrowdStrike](#)
23. [Kickstart Your Cybersecurity Career as a SOC Analyst | Infosec \(infosecinstitute.com\)](#)
24. [What is Cyberthreat Intelligence \(CTI\)? - Palo Alto Networks](#)
25. [Cyber Threat Intelligence \(CTI\): A Beginner's Guide | Splunk](#)
26. [A day in the life of a SOC architect - Hurricane Labs](#)
27. [Security Operations Center \(SOC\) Roles and Responsibilities - Check Point Software](#)
28. [How to Coordinate CTI and Vulnerability Management | IANS Research](#)
29. [Security Operations Center \(SOC\) tools and technologies | ManageEngine Log360](#)
30. [SOC Tools | AT&T Cybersecurity \(att.com\)](#)
31. [CISO_mindmap_2020_recommendations.pdf \(rafeeqrehman.com\)](#)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

32. [SOC vs. SIEM: Understanding The Role of SIEM Solutions in the SOC \(exabeam.com\)](https://exabeam.com)
33. [4 Security Operations Center Frameworks You Should Know \(bluevoyant.com\)](https://bluevoyant.com)
34. [What is SOC \(checkpoint.com\)](https://checkpoint.com)
35. [What Is a Security Operations Center \(SOC\)? \(bluevoyant.com\)](https://bluevoyant.com)
36. [Supercharge Your SOC With an Automated Approach to Incident Response - SentinelOne](https://sentinelone.com)
37. [8 Steps to Improving Your SOC's Incident Detection & Response \(cyberproof.com\)](https://cyberproof.com)
38. [What Is a SOC? 10 Core Functions and 6 Key Challenges \(cynet.com\)](https://cynet.com)
39. [SecurityOperationsCenter_eBook.pdf \(bluesec.pl\)](https://bluesec.pl)
40. [Best Practices for Setting Up a Cybersecurity Operations Center \(isaca.org\)](https://isaca.org)
41. [OWASP SOC Project](https://owasp.org)
42. [7 Steps to Build a SOC with Limited Resources | PPT \(slideshare.net\)](https://slideshare.net)
43. [CrowdStrike-Services-SOC-Assessment-Data-Sheet.pdf](https://crowdstrike.com)
44. [SOAR-KPIs.pdf \(acadiatech.com\)](https://acadiatech.com)
45. [Top SOC Metrics and KPI 2023: Mastering Security Operations \(blueteamresources.in\)](https://blueteamresources.in)
46. [SOC Metrics: Security Metrics & KPIs for Measuring SOC Success | Splunk](https://splunk.com)
47. [The SOC methodology - SecureGlobal](https://secureglobal.com)
48. [What is a secure enterprise architecture roadmap? | PPT \(slideshare.net\)](https://slideshare.net)
49. [Microsoft Word - Threat-Driven Approach whitepaper v3.03a.docx \(lockheedmartin.com\)](https://lockheedmartin.com)
50. [Cyber Kill Chain@ | Lockheed Martin](https://lockheedmartin.com)
51. [The Cyber Kill Chain: The Seven Steps of a Cyberattack \(eccouncil.org\)](https://eccouncil.org)
52. [Gaining the Advantage Cyber Kill Chain.pdf \(lockheedmartin.com\)](https://lockheedmartin.com)
53. [Building an Effective SOC Playbook | Tufin](https://tufin.com)
54. [Incident response playbooks | Microsoft Learn](https://microsoft.com)
55. [Incident response planning | Microsoft Learn](https://microsoft.com)
56. [LDR551: Building, Leading, & Managing \(SOC\) Security Operations Center | SANS Institute](https://sansinstitute.org)
57. [The Fundamental Guide to Building a Better Security Operations Center \(SOC\) \(splunk.com\)](https://splunk.com)
58. [DetailedPhishingV01 - \(flexibleir.com\)](https://flexibleir.com)
59. [Cyber Security Incident management system using Flexible Evolving Playbooks \(flexibleir.com\)](https://flexibleir.com)
60. [SOC Operations: 6 Vital Lessons & Pitfalls \(darkreading.com\)](https://darkreading.com)
61. [Toreon | News | 4 pitfalls to avoid when building a CSOC](https://toreon.com)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

62. [SOC Processes, Operations, Challenges, and Best Practices - Sapphire.net](#)
63. [OODA loop - Wikipedia](#)
64. [SOC Processes | AT&T Cybersecurity \(att.com\)](#)
65. [CSIRT vs SOC: What Are the Differences? \(ryadel.com\)](#)
66. [What Is a Security Operations Center? Complete Guide \(exabeam.com\)](#)
67. [What is Security Operations Center - SOC: Roles & Responsibilities - Exabeam](#)
68. [Top 36 Threat Intelligence Providers for SOC Teams - Maltego](#)
69. [Purple Teaming and Threat-Informed Detection Engineering | SANS Blog](#)
70. [What Is Detection Engineering? | Detection Engineering Explained \(uptycs.com\)](#)
71. [Detection Engineering is Painful – and It Shouldn't Be \(Part 1\) | by Anton Chuvakin | Anton on Security | Medium](#)
72. [How to Build a Security Operations Center \(SOC Guide\) - 2023 \(gbhackers.com\)](#)
73. [What Is A Security Operations Center \(SOC\)? \(A Complete Guide For 2023\) - Cybersecurity For Me](#)
74. [Chief Information Security Officer \(CISO\) Workshop - Security documentation | Microsoft Learn](#)
75. [Download Security Compliance Toolkit and Baselines from Official Microsoft Download Center](#)
76. <https://www.microsoft.com/en-us/security/blog/2019/02/21/lessons-learned-from-the-microsoft-soc-part-1-organization/>
77. [Microsoft Cybersecurity Reference Architectures \(MCRA\) - Security documentation | Microsoft Learn](#)
78. [Top Open Source Solutions for Building Security Operations Center II \(socradar.io\)](#)
79. [SOC Open Source, ELK- TheHive- Cortex- MISP Complete Setup Guide, Part 1 - YouTube](#)
80. [SOC Open Source, Build own SOAR with Shuffle, ELK-TheHive-Cortex-Teams Full Automation, Part 2 - YouTube](#)
81. [archanchoudhury/SOC-OpenSource: This is a Project Designed for Security Analysts and all SOC audiences who wants to play with implementation and explore the Modern SOC architecture. \(github.com\)](#)
82. [andreafortuna/autotimeliner: Automagically extract forensic timeline from volatile memory dump \(github.com\)](#)
83. [Eric Zimmerman's tools](#)
84. [Welcome to the Plaso documentation – Plaso \(log2timeline\) 20230717 documentation](#)
85. [SANS Digital Forensics and Incident Response Blog | Digital Forensic SIFTing: Colorized Super Timeline Template for Log2timeline Output Files | SANS Institute](#)

86. [Helping CTI Analysts Approach and Report on Emerging Technology Threats and Trends | SANS](#)
87. [Linux Incident Response - Introduction to Rootkits | SANS](#)
88. [Linux Incident Response - Using ss for Network Analysis | SANS](#)
89. [Linux Incident Response - A Guide to syslog-ng | SANS](#)
90. [Timeline Analysis in DFIR, Full Process Explained - YouTube](#)
91. [SOC-Community/Awesome-SOC: A collection of sources of documentation and best practices to build and run a SOC \(github.com\)](#)
92. [How To Build A SIEM with Suricata and Elastic Stack on Rocky Linux 8 | DigitalOcean](#)
93. [SoC Mind Map \(cm-alliance.com\)](#)
94. [DoD CIO Library \(defense.gov\)](#)
95. [Playbook for DDOS Security Response - All Articles - CISO Platform](#)
96. [gvsoc_cirt-playbook-battle-cards/GSPBC-1000 - Impact - Data Encrypted For Impact - Ransomware.pdf at master · guardsight/gvsoc_cirt-playbook-battle-cards \(github.com\)](#)
97. [How to Build a Great SOC \(isaca.org\)](#)
98. [Event Log: Leveraging Events and Endpoint Logs for Security \(exabeam.com\)](#)
99. [SIEM Tools: Top 6 SIEM Platforms, Features, Use Cases and TCO \(exabeam.com\)](#)
100. [DDoS Quick Guide \(cisa.gov\)](#)
101. [Protect Your Business Assets With a Roadmap for a Maturing Cybersecurity Program \(gartner.com\)](#)
102. [GitHub - cisagov/ScubaGear: Automation to assess the state of your M365 tenant against CISA's baselines](#)
103. [Cyber Security Toolkit for Boards - NCSC.GOV.UK](#)
104. [Cyber risk modelling and quantification \(kpmg.com\)](#)
105. [CMMC Documentation \(defense.gov\)](#)
106. [What are Indicators of Compromise \(IoCs\)? \(packetlabs.net\)](#)
107. [Indicators of Compromise \(IOCs\) | Fortinet](#)
108. [What are Indicators of Compromise? IOC Explained - CrowdStrike](#)
109. [CRMP | Cyber Risk Management | Interactive Framework](#)
110. [Getting Started with the NICE Framework | NIST](#)
111. [Publications | CSRC \(nist.gov\)](#)
112. [Cyber Security Posters | SANS Institute](#)
113. [7 Key Enterprise Architecture Metrics - Simplicable](#)
114. [Enterprise Architecture Guide - Simplicable](#)
115. [Three Diagrams Architects Can't Live Without | by Susannah Plaisted | Salesforce Architects | Medium](#)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

116. [Yara Toolkit \(securitybreak.io\)](https://securitybreak.io)
117. [Digital Forensics and Incident Response \(DFIR\) - CrowdStrike](#)
118. [What is Digital Forensics and Incident Response \(DFIR\)? \(bluevoyant.com\)](https://bluevoyant.com)
119. [Cyber Security Tools | SANS Institute](#)
120. [Digital Forensics & Incident Response Framework for Embedded Systems \(mandiant.com\)](#)
121. [macOS and iOS Forensic Analysis | SANS Institute](#)
122. [Digital Forensics and Incident Response \(DFIR\) Framework for Operational Technology \(OT\) | NIST](#)
123. [DFIR Cheatsheet Booklet | SANS](#)
124. [Common Secure Security Operations Centre - UNICC](#)
125. [Security Operation Center - Design & Build | PPT \(slideshare.net\)](#)
126. [DTS Solution - Building a SOC \(Security Operations Center\) | PPT \(slideshare.net\)](#)
127. [Full Library | RSA Conference](#)
128. [Cyber Security Posters | SANS Institute](#)
129. [Russell Reynolds - Cyber Security: The CISO Assessment Level Model CALM | AESC](#)
130. [ciso-radar-2023-wavestone-uai-2880x1908.png \(2880x1908\)](#)
131. [Demos, Templates, Charts and Maps on Dragon1](#)
132. [About the Authors | Red Team Development and Operations](#)
133. [Cybersecurity Red Team Guide. My first blog was on the Blue Team side... | by Joshua Speshock | Medium](#)
134. [Cybersecurity Red Team Guide. My first blog was on the Blue Team side... | by Joshua Speshock | Medium](#)
135. [Red Team | The GitLab Handbook](#)
136. [Handbooks, Guides and Articles | US Army Combined Arms Center](#)
137. [Red Teaming Handbook - GOV.UK \(www.gov.uk\)](#)
138. [What Is Red Teaming and How Does It Work? | Synopsis](#)
139. [Top 3 Red Teaming Frameworks \(TIBER,AASE,CBEST\) - BreachLock](#)
140. [Red Teaming as a Service | BreachLock](#)
141. [Red Teaming for Cybersecurity \(isaca.org\)](#)
142. [RT_Handbook_v6.pdf \(army.mil\)](#)
143. [Comparing open source attack simulation platforms for red teams \(redcanary.com\)](#)
144. [GitHub - praetorian-inc/purple-team-attack-automation: Praetorian's public release of our Metasploit automation of MITRE ATT&CK™ TTPs](#)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

145. [TIBER-EU FRAMEWORK – How to implement the European framework for Threat Intelligence-based Ethical Red Teaming \(europa.eu\)](#)
146. [Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions \(bis.org\)](#)
147. [What is Red Teaming? Methodology & Tools \(varonis.com\)](#)
148. [What is a Security Operations Center \(SOC\)? \(varonis.com\)](#)
149. [Red Team Framework | PPT \(slideshare.net\)](#)
150. [Building an InfoSec RedTeam | PPT \(slideshare.net\)](#)
151. [Red Team vs. Blue Team | PPT \(slideshare.net\)](#)
152. [Red team and blue team in ethical hacking | PPT \(slideshare.net\)](#)
153. [GitHub - infosecn1nja/Red-Teaming-Toolkit: This repository contains cutting-edge open-source security tools \(OST\) for a red teamer and threat hunter.](#)
154. [5 Best C2 Framework for Red Teaming - The Sec Master](#)
155. [What is Red Team? How Red Teaming is Different Than Penetration Testing? - The Sec Master](#)
156. [The roles of red, blue and purple teams - Content+Cloud \(contentandcloud.com\)](#)
157. [Red, Blue, and Purple Teams in Cybersecurity: Understanding the Roles and Tools \(todyl.com\)](#)
158. [How do Red Team Exercises help CISO to Validate the Security Controls Effectively? - Security Boulevard](#)
159. [What Should Influence Your SOC Strategy in 2023? \(sightgain.com\)](#)
160. [SOC Metrics: PowerPoint Presentation \(first.org\)](#)
161. [Incident Response Plan: Frameworks and Steps - CrowdStrike](#)
162. [Computer Security Incident Handling Guide - NIST](#)
163. [6 Incident Response Steps to Take After a Security Event - Exabeam](#)
164. [Step-By-Step Guide To An Effective Incident Response Plan](#)
165. [The complete 6-step incident response lifecycle | incident.io](#)
166. [OWASP Security Operations Centre Framework Project OWASP](#)
167. [How to: Setup Powershell Logging for SIEM | by Secprentice | Medium](#)
168. [Windows+Sysmon+Logging+Cheat+Sheet_Aug_2019.pdf \(squarespace.com\)](#)
169. [Module 11 Logs and Event Analysis.pdf \(cemca.org\)](#)
170. [Windows_Event_Log_Analysis_IR_Guide.pdf \(0ut3r.space\)](#)
171. [PROTECT - Windows Event Logging and Forwarding \(October 2021\).pdf \(cyber.gov.au\)](#)
172. [How to: Setup Powershell Logging for SIEM | by Secprentice | Medium](#)
173. [Security Operation Center - Design & Build | PPT \(slideshare.net\)](#)
174. [SEC's new cyber disclosure rule: PwC](#)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

175. [Enterprise Cybersecurity Architecture \(jamesfisher.org\)](https://www.jamesfisher.org/)
176. [Cybersecurity roadmap : Global healthcare security architecture | PPT \(slideshare.net\)](#)
177. [Building a Next-Generation Security Operation Center Based on IBM QRadar and Security Intelligence Concepts | PPT \(slideshare.net\)](#)
178. [From SIEM to SOC: Crossing the Cybersecurity Chasm | PPT \(slideshare.net\)](#)
179. [Security operations center-SOC Presentation-مركز عمليات امنيت | PPT \(slideshare.net\)](#)
180. [Building Security Operation Center | PPT \(slideshare.net\)](#)
181. [redteam-plan/README.md at master · magoo/redteam-plan · GitHub](#)
182. [Red Team Guides | Red Team Development and Operations](#)
183. [GitHub - J0hnbX/RedTeam-Resources](#)
184. [Microsoft Word - Threat-Driven Approach whitepaper v3.03a.docx \(lockheedmartin.com\)](#)
185. [Cyber Resiliency Level: CRL_v3.01_Whitepaper_29Aug23_FINAL.pdf \(lockheedmartin.com\)](#)
186. [Threats - Microsoft Threat Modeling Tool - Azure | Microsoft Learn](#)
187. [Microsoft Threat Modeling Tool overview - Azure | Microsoft Learn](#)
188. [Threat Modeling Process | OWASP Foundation](#)
189. [What is STRIDE Threat Model? \(practical-devsecops.com\)](#)
190. [STRIDE-LM Threat Model - CSF Tools](#)
191. [Using the STRIDE-LM Threat Model to Drive Security Control Selection - CSF Tools](#)
192. [Microsoft Word - Threat-Driven Approach whitepaper v3.03a.docx \(lockheedmartin.com\)](#)
193. [Security Quality Requirements Engineering \(SQUARE\) Methodology \(cmu.edu\)](#)
194. [Security Modeling and Threat Modeling Resources - Cybersecurity Memo \(51sec.org\)](#)
195. [Security Modeling and Threat Modeling Resources - Cybersecurity Memo \(51sec.org\)](#)
196. [A Threat Modeling Process to Improve Resiliency of Cybersecurity ProgramRafeeq Rehman | Cyber | Automation | Digital](#)
197. [Research Publications | CSA \(cloudsecurityalliance.org\)](#)
198. [ITIL 4 Introduction- ITIL 4 Certification Scheme & ITIL 4 Framework \(knowledgehut.com\)](#)
199. [What is ITIL®? | YaSM Service Management Wiki](#)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

200. [EQL search in Elastic SIEM Detection rules | LinkedIn](#)
201. [Analytics – EQL Analytics Library documentation \(eqllib.readthedocs.io\)](#)
202. [A deep dive into Sigma rules and how to write your own threat detection rules - FourCore](#)
203. [GitHub - SigmaHQ/sigma: Main Sigma Rule Repository](#)
204. [Uncoder AI: Active Threat-Informed Defense | Sigma Rules & ATT&CK](#)
205. [Analytics – EQL Analytics Library documentation \(eqllib.readthedocs.io\)](#)
206. [The No Hassle Guide to Event Query Language \(EQL\) for Threat Hunting \(varonis.com\)](#)
207. [EQL syntax reference | Elasticsearch Guide \[8.12\] | Elastic](#)
208. [A Mind Map on the Use of Information and Communication Technology ICT in Educational Assessment.jpg \(2048x1463\)](#)
209. [CSIRT Framework Development SIG \(first.org\)](#)
210. [How Purple Team Can Use Continuous Adversary Simulation | SANS Institute](#)
211. [Adversary Emulation Library - MITRE Engenuity \(mitre-engenuity.org\)](#)
212. [The Center for Threat-Informed Defense - GitHub](#)
213. [The First 100 Days Of An Enterprise Architect \(gartner.com\)](#)
214. [OVAL - Documents \(mitre.org\)](#)
215. [HIDS A Guide To Host Based Intrusion Detection Systems \(bulletproof.co.uk\)](#)
216. [A Guide to Network Intrusion Detection Systems \(bulletproof.co.uk\)](#)
217. [CWE - Common Weakness Enumeration \(mitre.org\)](#)
218. [Policy Mapping Poster with US Cyber Centers Map | Behance :: Behance](#)
219. [OMG Standards Introduction | Object Management Group](#)
220. [It governance and management framework \(management-club.com\)](#)
221. [IT Management Framework - Information Professionals \(informpros.com.au\)](#)
222. [ISO/IEC 38500:2015 - Information technology – Governance of IT for the organization](#)
223. [SOC Operations: 6 Vital Lessons & Pitfalls \(darkreading.com\)](#)
224. [Building a Modern CSOC - A Complete Guide for SOC Analysts \(cybersecuritynews.com\)](#)
225. [The VERIS Framework](#)
226. [Publications | Offensive AI Lab \(offensive-ai-lab.github.io\)](#)
227. [Counter-AI Offensive Tools and Techniques – CSIAC](#)
228. [Preparing for AI-enabled cyberattacks | MIT Technology Review](#)

229. [Full article: The Emerging Threat of Ai-driven Cyber Attacks: A Review \(tandfonline.com\)](#)
230. [Risk Modeling: Quantify Cyber Insights for Effective Risk Management – Series \(brighttalk.com\)](#)
231. [What is Attack Tree Model: A Comprehensive Cyber Security Tool? - Cyber Insight](#)
232. [NIST CSF & FAIR - Part 1 \(fairinstitute.org\)](#)
233. [Selecting the Right Cyber Risk Quantification Model \(cybersaint.io\)](#)
234. [Cybersecurity Tabletop Exercise Examples, Best Practices, and Considerations | RSI Security](#)
235. [Cyber Attack Incident Response Tabletop Exercise | Scenarios & Process \(zcybersecurity.com\)](#)
236. [How to Build an Effective Cyber Tabletop Exercise \(freecodecamp.org\)](#)
237. [The Complete Guide to Running a Cybersecurity Tabletop Exercise - Red Goat \(red-goat.com\)](#)
238. [Tabletop Exercises: Real Life Scenarios and Best Practices \(threatintelligence.com\)](#)
239. [Top 5 ICS Incident Response Tabletops and How to Run Them | SANS Institute](#)
240. [Tabletop exercises explained: Definition, examples, and objectives | CSO Online](#)
241. [Cybersecurity Incident Response Exercise Guidance \(isaca.org\)](#)
242. [Tabletop Simulations for Security Programs | Red Canary](#)
243. [Implementing Your First Cybersecurity Tabletop Exercise - JumpCloud](#)
244. [Everything You Need to Know about Cyber Crisis Tabletop Exercises | Tripwire](#)
245. [Tabletop Exercise: Pretty Much Everything You Need to Know | RedLegg](#)
246. [Cyber Resiliency Engineering Framework | MITRE](#)
247. [How to Write an Actionable Alert - Catscrd|](#)
248. [Writing Practical Splunk Detection Rules – Part 1 | by Vit Bukac | Medium](#)

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Body of Knowledge & Control Frameworks

BoK for the Cybersecurity and essentially the enterprise risk management

1. **Zachman:** [About the Zachman Framework - Zachman International - FEAC Institute \(zachman-feac.com\)](#)
2. **Dragon1:** [Dragon1 Software for Managing Risk, Projects, Strategy, Data](#)
3. **TOGAF & IT4IT:** The Open Group Architecture Framework
4. **Q4IT:** [DCMM, IT Quality Index \(q4it.eu\)](#)
5. **OSA:** [Open Security Architecture](#)
6. **DoD Reference Architecture:** [DoD Cybersecurity Reference Architecture \(defense.gov\)](#)
7. **DoD Architecture Framework 2.02:** [DODAF - DOD Architecture Framework Version 2.02 - DOD Deputy Chief Information Officer \(defense.gov\)](#)
8. **DoD Library:** [DoD CIO Library \(defense.gov\)](#)
9. **FedRAMP:** [Search For Any FedRAMP Policy or Guidance Resource | FedRAMP.gov](#)
10. **CMMC:** [CMMC Documentation \(defense.gov\)](#)
11. **DAMA:** [DMBoK - Data Management Body of Knowledge \(dama.org\)](#)
12. **FAIR:** [The Importance and Effectiveness of Cyber Risk Quantification \(fairinstitute.org\)](#)
13. **SCF – Secure Controls Framework:** [Secure Controls Framework \(SCF\) Download](#)
14. **ENISA:** [Publications – ENISA \(europa.eu\)](#)
15. **APQC's Process Classification Framework (PCF):** [Process Frameworks | APQC](#)
16. The DoD Cybersecurity Policy Chart: [The DoD Cybersecurity Policy Chart – CSIAC](#)
17. The IIA: [Internal Audit Competency Framework \(theiia.org\)](#)
18. The Chartered Institute of IT: [Security / data / privacy | BCS](#)
19. **BCI - Business Continuity Institute:** [Introduction to Business Continuity | The Business Continuity Institute \(BCI\) | BCI \(thebci.org\)](#)
20. **IAPP:** [International Association of Privacy Professionals \(iapp.org\)](#)
21. **IEEE - IEEE Cybersecurity – Home of the IEEE Cybersecurity Initiative**
22. **SANS - Cyber Security**
23. **IRM - Institute of Risk Management:** [Special Interest Groups \(SIGs\) \(theirm.org\)](#)
24. **IASA - An Association for All IT Architects** [Btabok - BTABoK \(iasaglobal.org\)](#)
25. **CIISec - Chartered Institute of Information Security** [Resource Centre - CIISec](#)
26. **SABSA – Enterprise Security Architecture** [SABSA Executive Summary - The SABSA Institute](#)
27. **ICTTF - International Cyber Security Task Force**
28. **CyBOK - Cyber Security Body of Knowledge**

29. **BABOK**: [Business Analysis | The Global Standard | IIBA®](#)
30. **SWEBOK**: [Software Engineering Body of Knowledge SWEBOK- Version 3 \(computer.org\)](#)
31. **SIA** - [Center of Excellence - Security Industry Association](#)
32. **SFIA** - Skills Framework for the Information Age: [SFIAv9 Levels of responsibility and generic attributes – English \(sfia-online.org\)](#)
33. **IVI Institute** - IT Capability Maturity Framework: [IT-CMF - Innovation Value Institute \(ivi.ie\)](#)
34. **ADCG** - Association for Data & Cyber Governance: [Benefits – ADCG](#)
35. **SCF** - Secure Controls Framework: [Secure Controls Framework](#)
36. **CGI** - Corporate Governance Institute: [Corporate Governance Courses for Directors and Non-Executive Directors \(thecorporategovernanceinstitute.com\)](#)
37. **COSO** - Enterprise Risk Management: [COSO ERM Framework | COSO](#)
38. **DORA** – [Digital Operational Resilience Act \(DORA\) - Regulation \(EU\) 2022/2554 \(digital-operational-resilience-act.com\)](#)
39. **NIST CSF**: [Cybersecurity Framework | NIST](#)
40. **NIS-2**: [The NIS2 Directive: A high common level of cybersecurity in the EU | Think Tank | European Parliament \(europa.eu\)](#)
41. PMI BoK - [PMBOK Guide | Project Management Institute \(pmi.org\)](#)
42. Global Cyber Alliance: [Actionable Cybersecurity Tools \(globalcyberalliance.org\)](#)
43. **NCSC UK**: [10 Steps to Cyber Security - NCSC.GOV.UK](#)
44. **OSA**: [Pattern Landscape \(opensecurityarchitecture.org\)](#)
45. **ISA**: [International Society of Automation \(ISA\)](#)
46. **DRJ**: [Disaster Recovery Journal \(drj.com\)](#)
47. **NYMITY**: [Charts_Cover_Final.ai \(oasis-open.org\)](#)
48. **NYMITY**: [Privacy Management Accountability Framework - Hong Kong.ai \(pcpd.org.hk\)](#)
49. **NYMITY**: [PMAF Poster - January 2017 \(vvena.nl\)](#)
50. [The Ultimate Guide to Privacy Management | Blog | OneTrust](#)
51. [Information and Privacy Commission New South Wales \(nsw.gov.au\)](#)
52. [SME Guides | SBS SME \(sbs-sme.eu\)](#)
53. [About Cyber Essentials - NCSC.GOV.UK](#)
54. [Cyber Essentials Toolkits | CISA](#)
55. [CISA Cyber Essentials Starter Kit | CISA](#)
56. [Home Page - CREST \(crest-approved.org\)](#)
57. [CERT Resilience Management Model \(CERT-RMM\) Collection: CERT Resilience Management Model \(CERT-RMM\) Collection \(cmu.edu\)](#)

- 58. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2): [cybersecurity-capability-maturity-model-february-2014 \(energy.gov\)](#)
- 59. [NICE Framework Resource Center | NIST](#)
- 60. CSA Cloud Control Matrix: [CSA \(cloudsecurityalliance.org\)](#)
- 61. [White Papers \(insaonline.org\)](#)

Acronyms

Access Control List (ACL), 66	Business Continuity Plan (BCP), 26, 46, 65, 83, 156, 157	Cloud Workload Protection Platforms (CWPP), 232
Advanced Persistent Threat (APT), 108, 187	Business Continuity Planning (BCP), 26	Command & Control (C2), 68
Advanced Threat Protection (ATP), 197	Business Process Management (BPM), 55, 56, 63, 231, 405, 474	Computer Security Incident Response Team (CSIRT), 309, 310, 311, 312, 314, 316, 317, 321, 454, 459
Alert Detection Strategy (ADS), 160	Business Support System (BSS), 50	Continuous Threat Exposure Management (CTEM), 63, 232, 326, 327, 328, 329
Align, Plan and Organize (APO), 447	Capability Maturity Model (CMM), 104, 105	Control Objectives for Information and Related Technologies (COBIT), 68, 106, 229, 443, 446, 447
Application Centric Infrastructure (ACI), 66, 110, 228, 231	Center for Internet Security (CIS), 225	Could Access Security Broker (CASB), 232
Application Performance Monitoring (APM), 231	Cloud Access Security Broker (CASB), 63, 64, 107, 109, 112, 232	Courses of Action (CoA), 126
Architecture Development Method (ADM), 50	Cloud Identity Governance (CIG), 232	Cyber Intelligence Operation Center (CIOC), 70
Artificial Intelligence (AI), 86	Cloud Infrastructure Entitlement Management (CIEM), 232	Cyber Open-Source Intelligence (COSI), 70
Automatic Call Distribution (ACD), 66	Cloud Security Posture Management (CSPM), 232	Cyber Resiliency Engineering Framework
Bring Your Own Device (BYOD), 72, 154, 155		
Build, Acquire and Implement (BAI), 447		

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

(CREF), 169
Cyber Threat Intelligence (CTI), 216, 217, 380, 403, 452, 455
Cybersecurity Framework (CSF), 150, 195
cybersecurity operations center (CSOC), 24
Cybersecurity Operations Center (CSOC), 24

Data Loss Prevention (DLP), 232
Data Loss Protection (DLP), 63, 71, 110, 209, 232
Data Management Services (DMS), 229
Data Rights Management (DRM), 231
Database Activity Monitoring (DAM), 231
Datacenter Infrastructure Management (DCIM), 230
Deliver, Service and Support (DSS), 447
Denial of Service (DoS), 65, 130, 265, 266, 418
Department of Defense Architecture Framework (DoDAF), 69
Detection as Code (DaC), 301
Digital Forensics and Incident Response (DFIR), 63, 180, 232, 318, 319, 321, 322, 323, 326, 380, 455, 456
Digital Forensics Incident Response (DFIR), 232
Disaster Recovery Plan (DRP), 26, 46, 65, 83, 156
Disaster Recovery Planning (DRP), 26
Distributed Denial of Service (DDoS), 65
DNS Security (DNSSec), 66
Domain Name Service (DNS), 232

End of Life (EoL), 94
Endpoint Detection & Remediation (EDR), 232
Endpoint Detection & Response (EDR), 63, 66, 109, 189, 194, 232, 260, 261, 274, 288, 382
Enterprise Content Management (ECM), 226
Enterprise Information Management (EIM), 444, 445
Enterprise Mobile Management (EMM), 232
Enterprise Risk Management (ERM), 26, 46, 83, 446, 463, 475
Enterprise Security Risk Management (ESRM), 61
Enterprise Semantic Model (ESM), 445
Environmental Monitoring Services (EMS), 232
Evaluate Direct and Monitor (EDM), 447
Event Query Language (EQL), 197
Extended Detection and Response (XDR), 175

General Data Protection Regulation (GDPR), 195

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Hardware Security Module (HSM), 67, 112	Learning Management Services (LMS), 229	Next Generation Firewall (NGFW), 274, 408
Host-based Intrusion Detection System (HIDS), 67	Lightweight Directory Access Protocol (LDAP), 66, 112	Open Source Intelligence (OSINT), 65
Hyper Converged Infrastructure (HCI), 232	Lightweight Directory Access Protocol (LDAP), 63, 66, 108, 112, 254, 264, 265, 391	Open Web Application Security Project (OWASP), 164, 237, 278, 453, 457, 458
Identity & Access Management (IAM), 112, 231	Line of Business (LoB), 50	Open-Source Intelligence (OSINT), 70, 109, 231, 304
Information Sharing and Analysis Centers (ISAC), 232	Managed Detection And Response (MDR), 231	Operation Support System (OSS), 50
Internet of things (IoT), 87	Managed Security service provider (MSSP), 177	Payment Card Industry Data Security Standard (PCI-DSS), 68, 99, 106, 229, 260
Intrusion Detection and Prevention System (IPS), 67	Microsoft Security Development Lifecycle (MSDL), 128	People, Process & Technology (PPT), 194
Intrusion Detection System (IDS), 67	Monitor, Evaluate and Assess (MEA), 447	Power Distribution Unit (PDU), 227
IT Information Library (ITIL), 229	Multi-factor Authentication (MFA), 123	Privilege Access Management (PAM), 108, 231
key performance indicator (KPI), 25	National Vulnerability Database (NVD), 324	Project Management Office (PMO), 45, 67, 179, 405, 406, 414
Key Performance Indicator (KPI), 25	Network Time Protocol (NTP), 66	
Known Exploited Vulnerability (KEV), 325		

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

Recovery Point Objective (RPO), 85	(SDL), 128	(SSE), 232
Recovery Time Objective (RTO), 85	Security Information & Event Management (SIEM), 231	Service Level Agreement (SLA), 227
Recovery Time Objective (RTO), 85	Security Information and Event Management (SIEM), 26, 63, 65, 70, 78, 79, 80, 81, 82, 83, 86, 87, 93, 108, 150, 165, 175, 185, 186, 188, 193, 194, 196, 197, 199, 201, 230, 231, 247, 255, 256, 260, 261, 262, 272, 273, 274, 288, 299, 309, 380, 381, 383, 403, 453, 455, 457, 458, 459	Service level response and resolution (SLOR&R), 449
Remote Authentication Dial-In User Service (RADIUS), 66	Security Operation Center SOC, 22	Service Organization Control (SOC), 223
Remote Monitoring & Management (RMM), 231	Security Orchestration, Automation and Response (SOAR), 232	Software Defined Data Center (SDDC), 231
Responsible, Accountable, Contacted, Informed (RACI), 72, 449, 451	Security Orchestration, Automation, and Response (SOAR), 26, 63, 78, 79, 80, 81, 82, 83, 110, 175, 194, 232, 272, 273, 301, 309, 348, 453, 454	Software Defined Network (SDN), 66, 231
Risk Based Vulnerability Management (RBVM), 232	Security Policy Framework (SPF), 231	Software Defined WAN (SDWAN), 231
Robotic Process Automation (RPA), 227, 231	Security Service Edge	Software Development Life Cycle (SLDC), 64
Secure Access Service Edge (SASE), 232		Standard Operating Procedure (SOP), 94, 105, 449, 476
Secure Web Gateway (SWG), 232		Structured Cyber Resiliency Analysis Methodology (SCRAM), 170, 171
Security Content Automation Protocol (SCAP). (SCAP), 325		Supervisory Control And Data Acquisition (SCADA), 227
Security Development Lifecycle		Threat and Vulnerability Management (TVM), 232
		Total Cost of Ownership (TCO), 100, 455

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Unified Threat Management (UTM), 67
User Entity Behavior Analytics (UEBA), 231



Web Application Firewall (WAF), 66, 67, 107, 112, 232, 417
who, what, when, where, why and how (5W1H), 46, 167

Yet Another Markup Language (YAML), 195
Zero Trust Network Architecture (ZTNA), 232



COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER



Author Brief




Thank you for downloading this book, I hope it helped you gain some insights on how to break into cybersecurity and its domain knowledge requirements and essentially help build your SOC.

This book is my 10th book, the other nine were not this extensive in their nature but had different views and insights in it. I wanted to see if I could be up for it and I was collecting information's that's reflected throughout the book, which are quite old, like 10yrs old and from more than 600+ documents combined. My family supported my time away from them, and

because of their sacrifices, this book came to completion.

While I was in junior high, I used to make guitar amplifier and sell it to the store back in the young days for the guitar players, local players bought those amps and it was a good hit for me as the money started to pour in, and I've used those earnings to train myself in different things, like bikes and car engine reconstructions 😊. I borrowed some money from my dad for a side business and started a CD duplication station with 12 Sony SCSI drives, had 4 towers producing 48 CDs approximately in 6 minutes at 12x write speed with Padus DiskJuggler software equipped with Adaptec UW-39320 Dual Channel SCSI controllers, one channel holding 6 SCSI drives. Fish breeding was also one of my hobbies, having trillions of babies! from Angel, Black Moors, and for huge number of aquariums I've made a custom water heater as those available in the market were too expensive.

At the the beginning of my career I have enrolled myself into learning dBase and Lotus123 in the year 1993, and later moved gradually to software development in the year 2005 with FoxPro 2.6 with SQL Personal Edition, later closely worked with Visual Studio and TFS. Side by side, I started using the Linux Slackware and SCO Unix for banking app installations throughout 2005 (on an individual contributor capacity). I have been observing that Banking and local enterprises do not want to use Linux as its too complex to manage and dependency lies with the administrators and those folks are in limited supply, and Windows Administrators are flooding the country with their deployment expertise, and I started losing the battles but not the war. Therefore, organizations started to move to Microsoft Windows systems, and then I started using IBM PC-DOS v2.1, and the last usage of MS-DOS was v6.22. Meanwhile, I started to work on NT v3.51(PDC & BDC deployments) in the year 1998 approximately, and gradually went up to



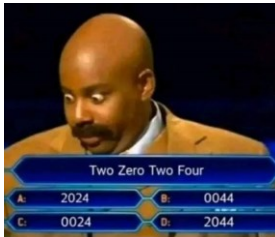
it till date with all of Microsoft Services (AD, Exchange, SharePoint, Lync & Communication Server, ISA Server, System Center Components like SCCM, SCOM, SCDPM, SCVMM, SCO, SCSM etc.), and occasionally Linux for SOC purposes.

I also have tried different things in the past and failed miserably and wasted a lifetime of money in learning things my way, as when it comes to knowledge, I've found out that everything people shared with me confidently, are 20%-30% correct and the rest is just plain made-up lies. But still at that time, I came in late for frameworks, certifications, and achieved the MCP since 2002, and never looked back of what I didn't achieve, but competing against my peers and myself for enriching my knowledge day after day, planned of the things that I wanted to go for, and astonishingly, at that time, Bangladesh were not in the internet era. I had some friends who were rich enough to buy USRobotics Modem (Sportster 14.4K) and I've bunked at their office at night and used their lines all day long (weekends) creating an email address, subscribing to news of gadgets and technology roadmaps, market share of the top players and things of that sort. Side by side I've spent handsomely for my training like repairing TV & Radio's, started a small HAM-Radio project, amplifier builds using STK IC with cassette player, guitar amplifier, hobby electronics, NLE video editing, started to learn 3D Studio Max v4, guitar lessons! Web site development training, power generator calibration, Datacenter development, TV Broadcasting with MCR design, Audio Booth design, etc.

Side by side, my enormous hunger for knowledge and to know the "why" and the "how" lead me to different paths all together. While I was deploying country's largest network that resides in the Government of Bangladesh, the Ministry of Finance to be exact, led me explore and learn at a fast pace, as devices were coming in like a waterfall, and I felt like "I am doomed", as I didn't have the knowledge to configure a Cisco Router, a Cisco Switch, Cisco ASA, but I have acquired those skills in a matter of a month, and configured them properly, and later on got CCNA certified in 2008. That's not the end, "properly" has a different meaning all together back in the days in 2005. At that time, someone from my team changed something into the router, and then I learned to harden these systems, activating log, and harder passwords employed. But my mentality changed, as the network went down, and I got the blame onto me, though I have found out who changed the configurations. Since then, every networked device got deployed, developed the first checklist of configurations to set forth.

Side by side, I have been supporting offices, individuals to integrate their PC's, build their PC's, connecting multiple PC's into a network, provide a shared printer etc. that were done using Microsoft Windows for Workgroups 3.11 in the year 1998-2000. Amazingly, I received a task offer from my connections, to establish a 20-computer network within the National Parliament Library, and did it within a month with Compaq Servers (AD


developed with PDC only), which were equipped with Pentium-pro processors, that was the first time I got to see the Pentium-pro processors. And some laptop purchased from a US manufacturer, I forgot the name, but the processors were made by Transmeta Efficion! Weird, but true, never heard their names but worked well alongside of Cyrix. Later, I got to work with Cyrix Processors from IBM as well. In those times, I bought myself a bike, small but fearsome, a Honda MBX-125F. Once it's time to change the piston, bored a bigger housing and replaced the piston with a Yamaha DT-200 piston 😊 it was a radiator cooled 6-gear engine, imagine the thrust, but broke the engine in 6 months' time. And since I got a ride for myself, my engagement with customers exploded, I've received orders to set networks, sell PC's like 40 PC's a month, and with that money I've got myself into electronic courses, camera operation courses, soundproofing for recording room courses, BetaCAM-SP operation and export courses etc.



Afterwards, I really got tired of having to support 64 districts network operations, though there were nine personnel in my team to support the vast network from 64 regional government offices. Applied for a SysAdmin job in BBC, and finally landed the job after six interviews, the last one was terrifying for me, I am one small me, having a meeting with the BBC-UK's technology team lead with a bunch of other folks, and I was just

like the picture on the left side 😊. But acquired my strength, and on my last interview meeting, the country manager finalized me on the spot after one and a half hours of rigorous technical discussion. Landed on another candy land, with so many broadcasts equipment to get my hands on, my dream started again, heart pumped like a race-horse and acquired so many hands on knowledge, and lastly got trained in the BBC-UK's Wood Norton for the broadcast system deployments, BBC Bush House @ Strand for datacenter storage management services, connecting satellites & broadcast live streams, soundproofing a room, deployed gallery and recording systems with Final-cut Pro with Mac systems etc.

From BBC, I have received a lead to join Microsoft, since I was working on with AD, Exchange 2003, MS-SQL Server 2000, SMS Server and with lot other components from Microsoft (I have made great use of these documents from MoF, IPD etc.) it was an easy win for me to land the job. But a surprise was waiting for me again. Whatever I did, was not enough! And I was totally stoked to get my hands into those literatures on the Microsoft's central encyclopedia. And as a country's technical lead for Bangladesh & Nepal I've got so many companies to look out for their enterprise grade deployments, and I got engaged with so many different types of network deployments, opened so many doors....and that was the fastest learning time of my life...what a rush! My head literally



got bombarded with frameworks like MoF (Microsoft's Operational Framework), technical guides, deployment guides, system tuning guides, architecture design and things of these sort from the TechNet and from TechNet-Gallery as well, what a candy land for me 😊 and during my stay at Microsoft, I've had the life changing experience to discipline myself and to embrace larger perspectives and to roll with the trends, never thought of my limitations, and thanks to all my friends who never helped me and just because of those guys, I have learned to do things myself, hands-on, head on.

As my forum grew, I took on mentees and always gave them everything they ever could have asked for, and they grew to be such fierce competitors, and those friends warned that never to create any competitor so I would lose the competitive edge, but turned out, it was totally opposite, we as a team, an IT governance team, a SOC team, a Developer team, a DevOps team, we could go to war!

In those times, I was able to mature and capture an opportunity to develop an MFS (mobile financial service) organization. A battle took place for the MFS application, whether to develop with in-house resources or buy one? in-house won the debate as a monumental cost saving took place and granted to develop and deploy the service. Business requirements (BPM) mapped to SRS, IT requirements mapped and purchase of the equipment started momentarily. Completely new MFS platform developed with an eighty three FTE's (IT, & Dev, SOC) worked day and night with Kubernetes and Blockchain services, which is the 1st ever MFS application built in the country, and it's a massive application architected with microservices, mobile app UX developed and released publicly both for Android & Apple, two collocated datacenter deployed as DC & DR, and we did it within 9 months since its inception to production for the whole MFS deployment services.

I have always tried to engage myself to create new doors of new opportunities from my connections, as wanted to explore for gaining different knowledge. Joined the largest nationwide ISP in Bangladesh, and enriched myself with their networking topology, scanned thousands of devices for vulnerabilities, how to detect configurations mishaps, how to detect network anomalies, benchmarking everything, documenting everything, breach & incident response, re-architected a gigantic ERP with 50+ core functional modules that controls different Router hardware for activating and deactivating clients automatically, various external & internal portals, revenue generating services, ERP portals, BI dashboards, payment gateway integrations, DDoS threat remediation techniques etc. and we did it with a fifty three personnel team (IT, Dev, SOC, & IPT).

I consider myself lucky, though I am not from a wealthy family, as I had many opportunities to choose from as they presented to me, and I eagerly explored different

COMPLETE GUIDE TO CYBER SECURITY OPERATION CENTER

- ERP - planning & software development
- Policy, standards, processes & procedure development
- Architecting integration solutions & middleware
- ERM risk reporting
- Risk management strategy
- Risk analysis
- Control framework deployment
- Vulnerability assessment & penetration testing
- Database security architecture
- System security architecture
- Cloud security architecture
- Awareness training
- Business process development
- Database security architecture
- Operations Management
- Team Management
- Coaching/Mentoring
- Application security architecture
- SoP development
- Information protection, processes & procedures
- Plans (IR, BC, DR)
- Major frameworks: NIST, CISEcurity, ITIL, ISMS, TOGAF, SFIA, CMMC, SCF


I know this is too much to claim for, but in Bangladesh, the JD comes through in the Job Boards, they are horrible, and they wanted everything in a single person, I mean who writes these JD's? but somehow tried to do whatever I can that enriched my understanding a hundred fold, and evidential documentations, project documentations are the things that made what I came to be.

Industry: ISP, Bank & NBFI, MFS (Mobile Financial Service), System Integrator (SI), Broadcast & Terrestrial etc.

Certifications: Microsoft Cybersecurity Architect Expert, CISM, CISA, CDPSE, CRISC, CGEIT, PCCS-CCIP (Datacenter), PMP, CCNA, MCT*10, MCSE*4, Prince2, MCSA, MCITP, ITILv3, MCTS, MSBS.

You can reach out to me in different ways:

- My blog site: [MOBS Bangladesh \(mobs-bd.org\)](http://MOBS Bangladesh (mobs-bd.org))
- Download this FREE eBook (pdf) from the "Article" Section: [Articles | MOBS Bangladesh \(mobs-bd.org\)](http://Articles | MOBS Bangladesh (mobs-bd.org))
- Join Discord: Please message me on LinkedIn
- Connect with me in LinkedIn: Shahab Al Yamin Chawdhury | LinkedIn
- Job aids – download documentation: Book-SOC Job Aids



I am aware that, I have been able to successfully confused you throughout the book, but as you grow, you will see that it was not intentional, it's just what things are right now, maybe in 20 years' time, everything will be automated and integrated to a platform sized solution, management plane, data plane and control or console plane will have synergies all together and in a better way to sharing things to the monitoring services, devices firmware's will have better API's prepared to share data instantly, management and AI based detection and protection techniques will reach an astounding level, and attackers will be highly sophisticated as well adopting to AI services to do human-less works for them.

Lastly, if you want to connect, please drop me a line on LinkedIn, and for the eBook, if you want the DOCX version, I will send out the link to download the editable version of the book. If you need consultation or strategy development, or seeking any type of help, you can always contact me on LinkedIn as well.

Please be mindful that I get a lot of messages from my peers, don't get offended if I cannot reply to you all for attending your queries.

Good luck on your journey, I hope that you succeed on every step you take in your lifetime, and your path will shine brighter every day in the coming years.

Let's grow together and share knowledge, as they are meant to be free.

Regards | Shahab

