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 CHAWDHURY
MSc | Enterprise Architect
4th April 2024, Version: 6.2

This Book is Dedicated to:

My Daughter - Aairah

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*

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

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, metrices, 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.

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								
	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.

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

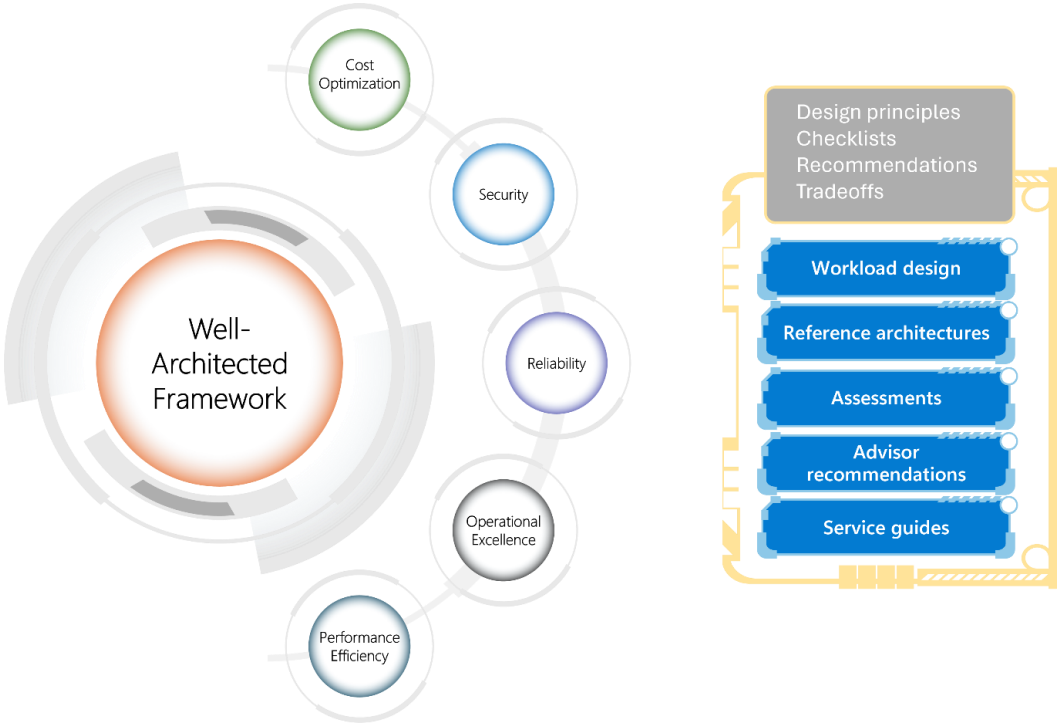
The **Azure Well-Architected Framework (WAF)** encompasses five essential tenets that guide solution architects in building robust and efficient workloads on **Microsoft Azure**:

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.

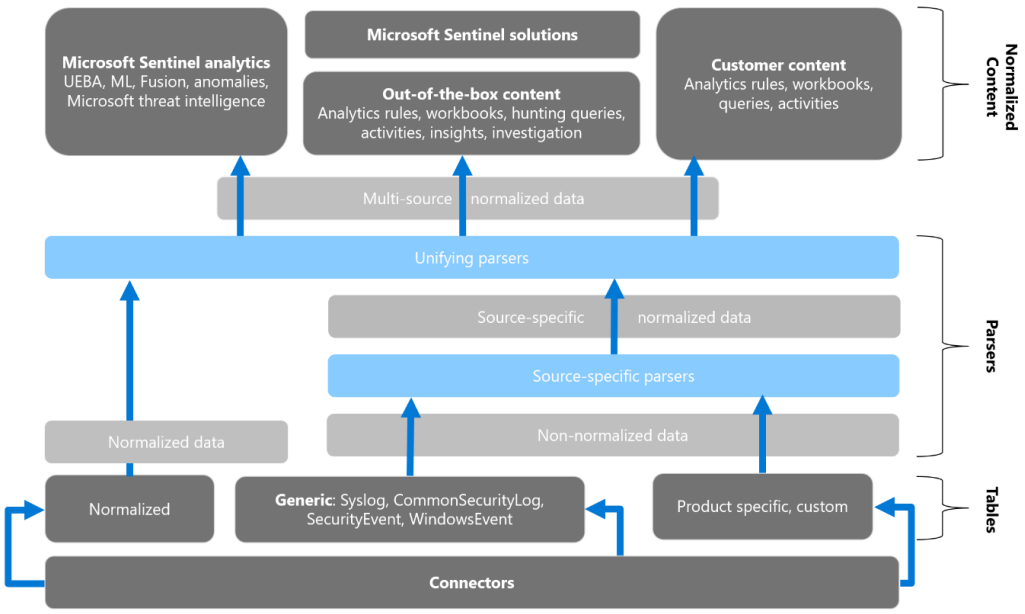
ASIM and the Open Source Security Events Metadata (OSSEM)

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.



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

ASIM includes the following components:

Normalized Schemas

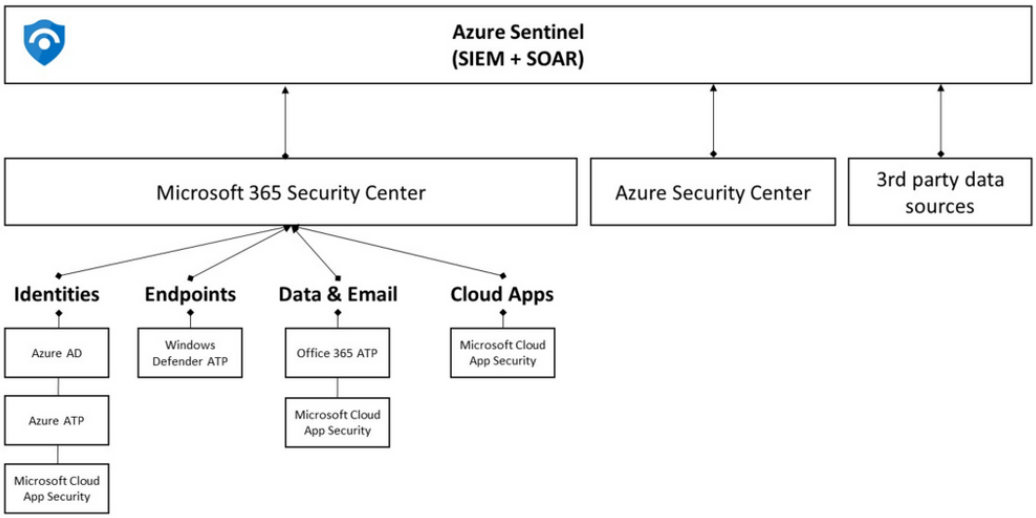
Normalized schemas cover standard sets of predictable event types that you can use when building unified capabilities. Each schema defines the fields that represent an event, a normalized column naming convention, and a standard format for the field values.

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

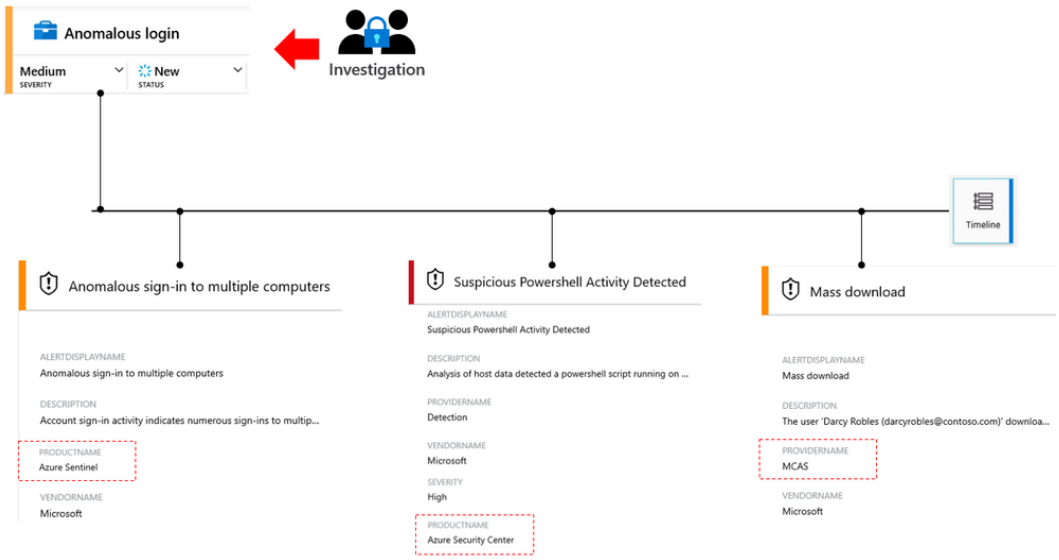
Azure Sentinel in other hand is a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) tool. Azure Sentinel's role is to ingest data from different data sources and perform data correlation across these data sources. On top of that, 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:



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.

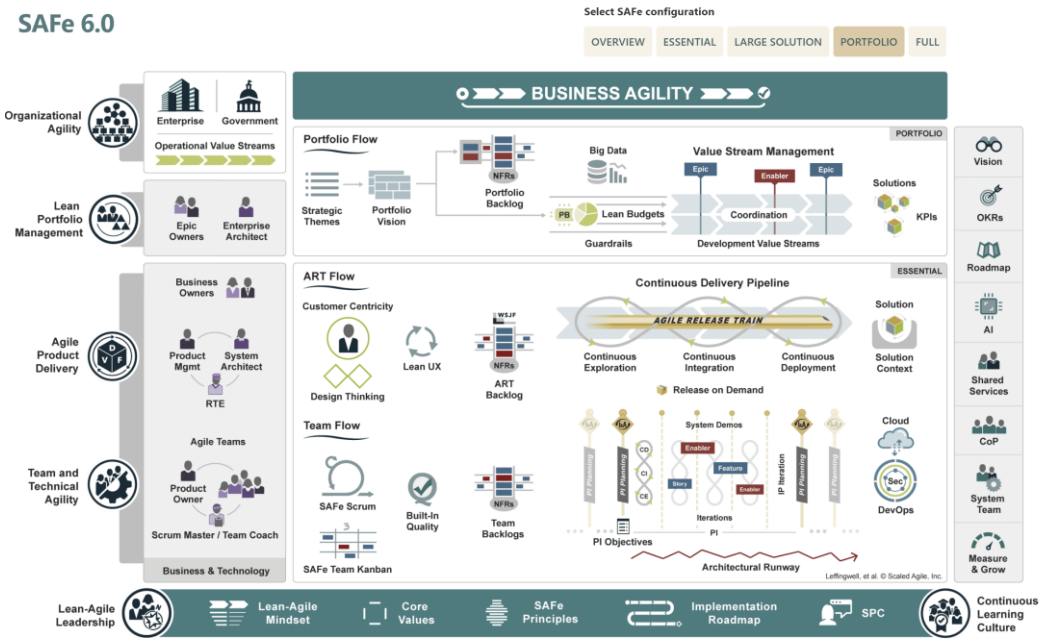
Key System Design Fundamentals

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

- 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]



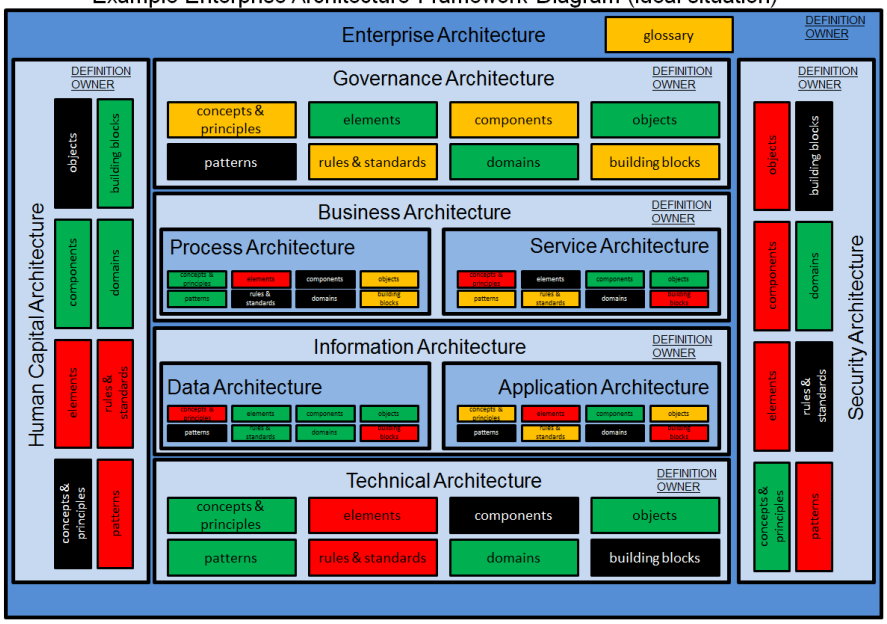
Source: [SAFe 6.0 (scaledagileframework.com)]

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:

Example Enterprise Architecture Framework Diagram (ideal situation)



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:

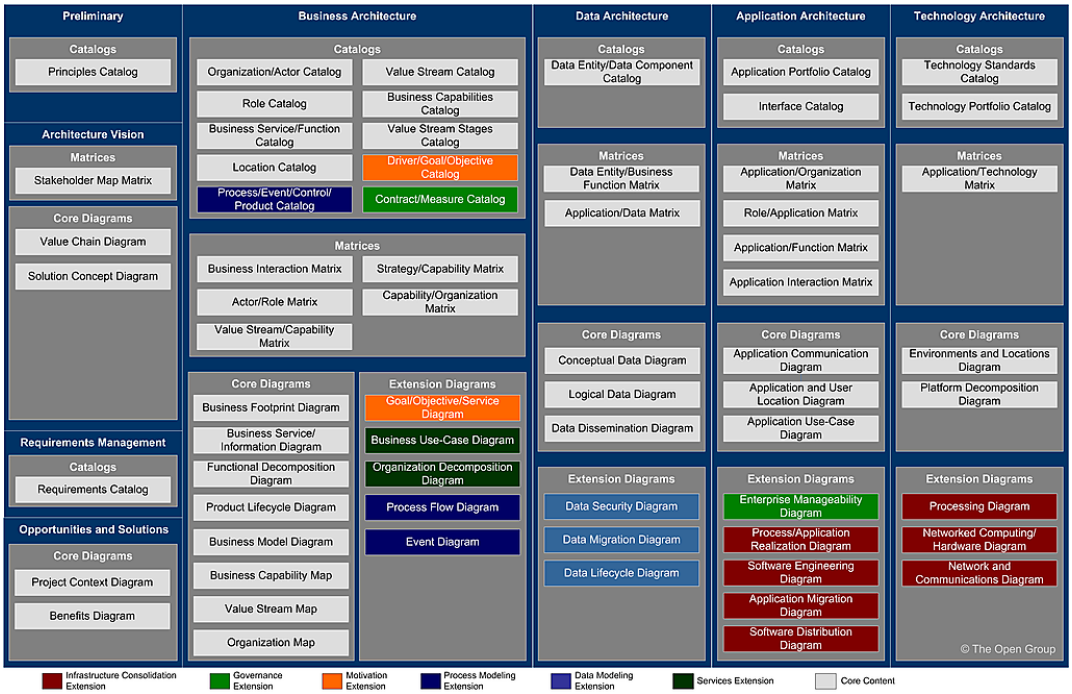
1. **Business architects** would choose key business challenges with business architecture model.
2. **Business operators** are responsible for: processes, data, infrastructure.
3. **Business unit leads** are responsible for: sending out their requirements to the business architect where the BA folks 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.

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)]



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:

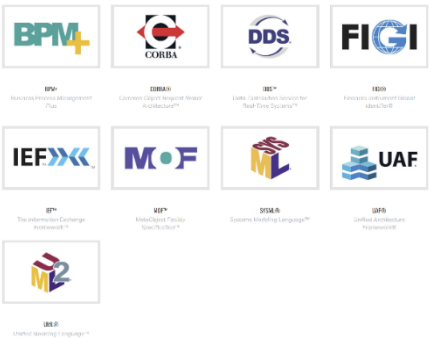
- *Scenario:* A healthcare organization integrates electronic health records, billing systems, and diagnostic services.

- *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:

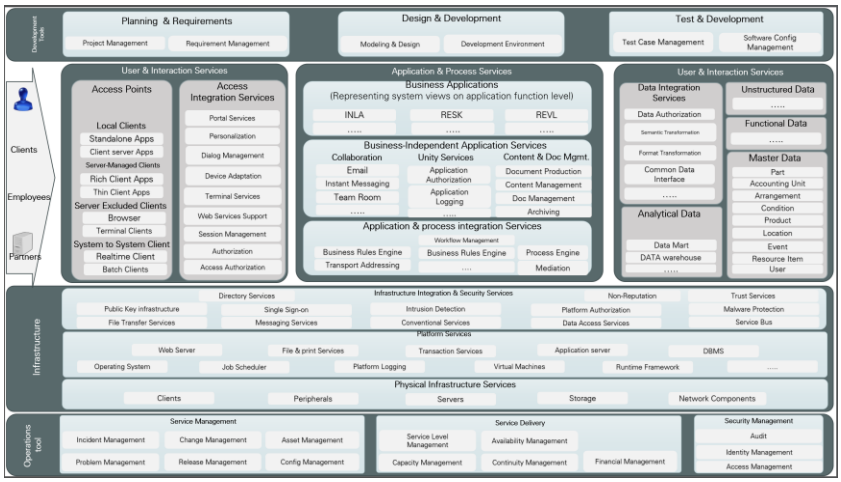


Source: [OMG Standards Introduction | Object Management Group]

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:

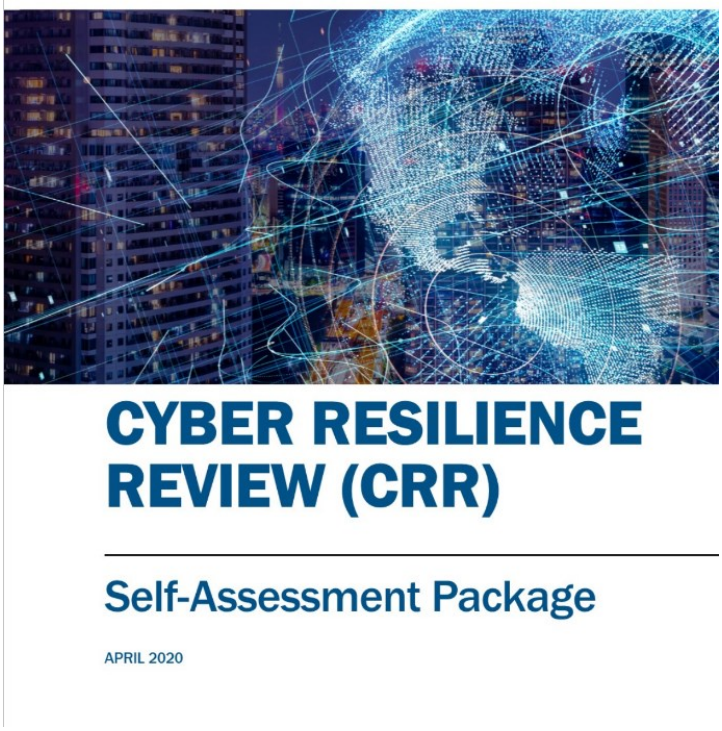


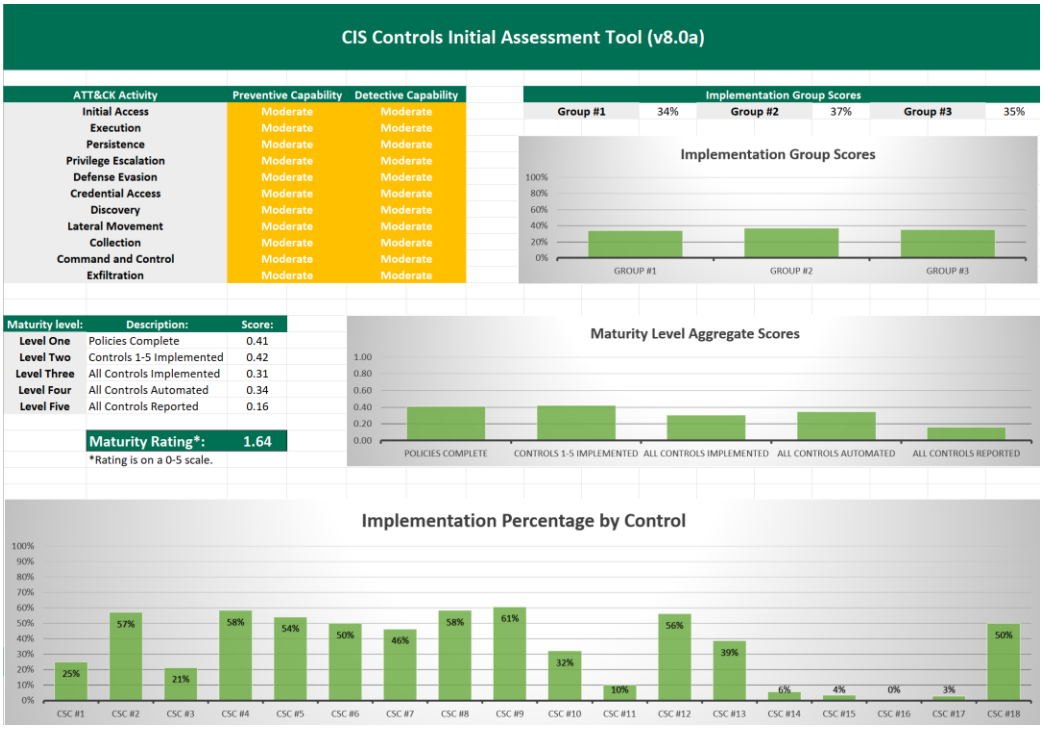
Before you jump into developing your own SOC program, I would strongly recommend that you assess the current infrastructure either using NIST, CISECURITY, or Homeland Security's CRR framework (Developed by Carnegie Melon University, shared from CISA's site) (also provided in the job aids folder named "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”):





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

operations team about the increased attack surface when new networks are set up or devices are replaced with newer lines or their firmware's 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

Figure 1—Foundation of a CSOC

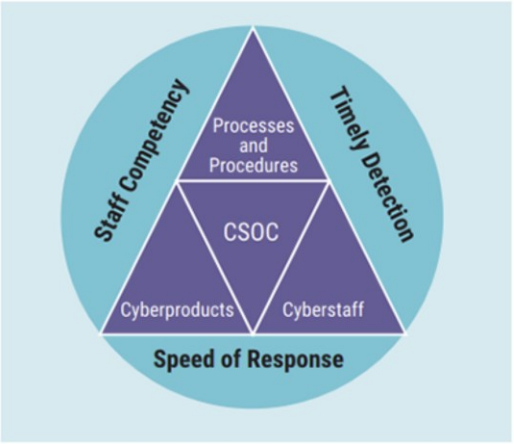
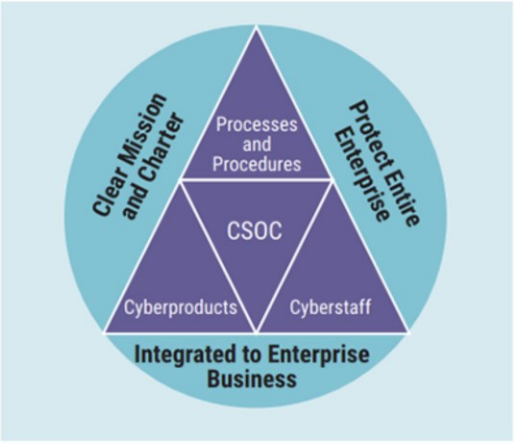


Figure 2—Critical Enablers of a CSOC

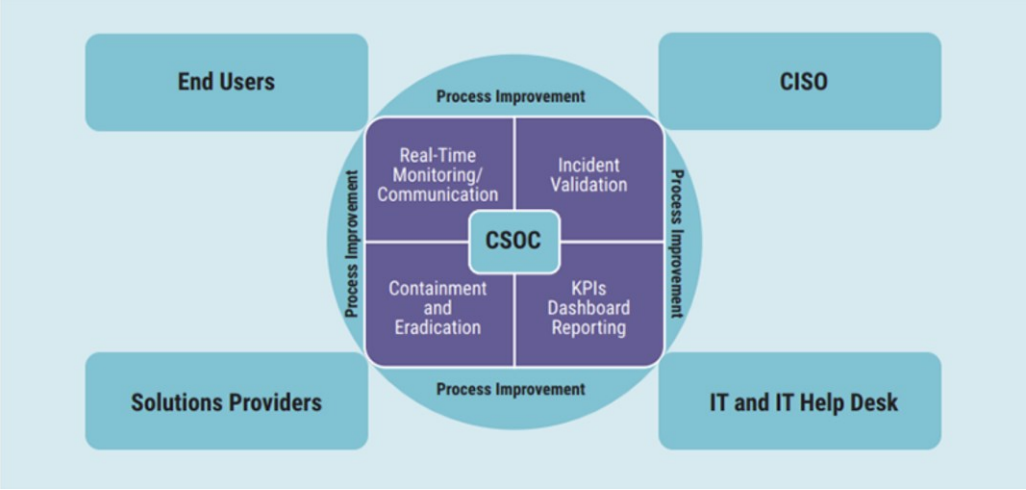


Source: [Best Practices for Setting Up a Cybersecurity Operations Center (isaca.org)]

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.

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)



Source: Best Practices for Setting Up a Cybersecurity Operations Center (isaca.org)

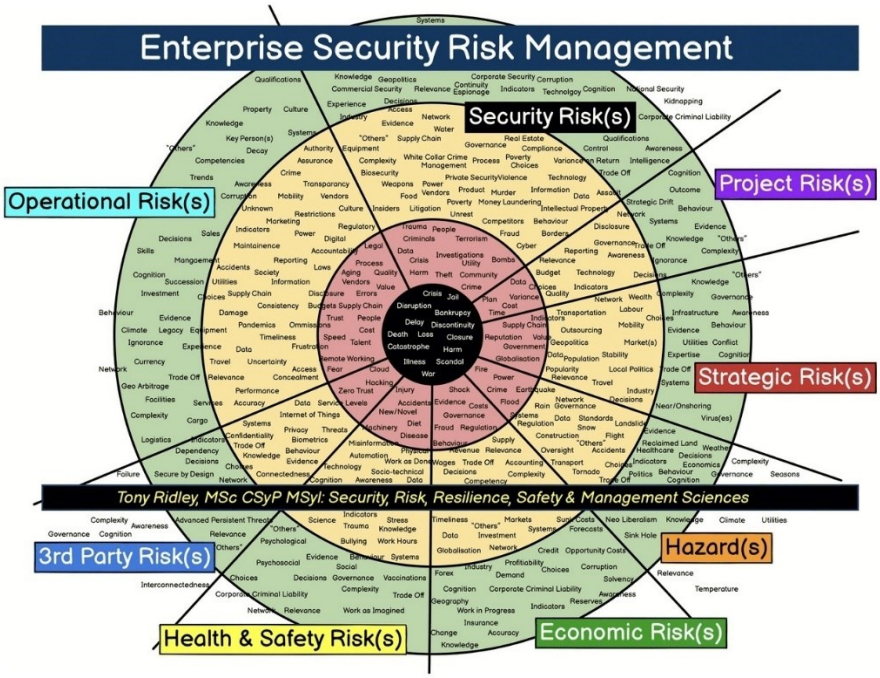
The sad part of the cybersecurity is that the activity domains are not clear, lack of frameworks, the knowledgebase is not clear, scarcity of the mentor is not available to follow, or people are not open to things they know, where appropriate tools are not grouped together for performing a set of activities 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:



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

1	Organizational Development	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.
	Enterprise Architecture	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.
	Application Architecture Design	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

	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.
Code Repositories	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.

Database	Most popular one's like MS-SQL, Oracle, PostgreSQL, MongoBD 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, 3rd 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

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.
- Mange 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 repose 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 breech. Let legal and marketing work the customer notification obligations.

- 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	Recce
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**	**Recce**
1: Inventory of Authorized and Unauthorized Devices	X	X	X	X	X	X	

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

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	

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.

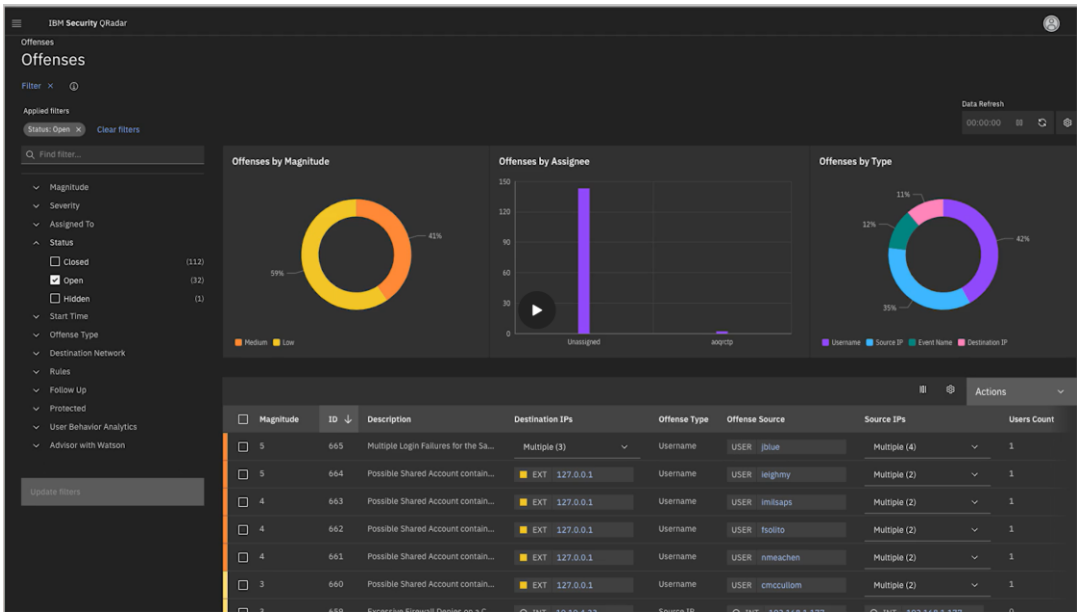
Some of the benefits of integrating SIEM and SOAR are:

- **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]

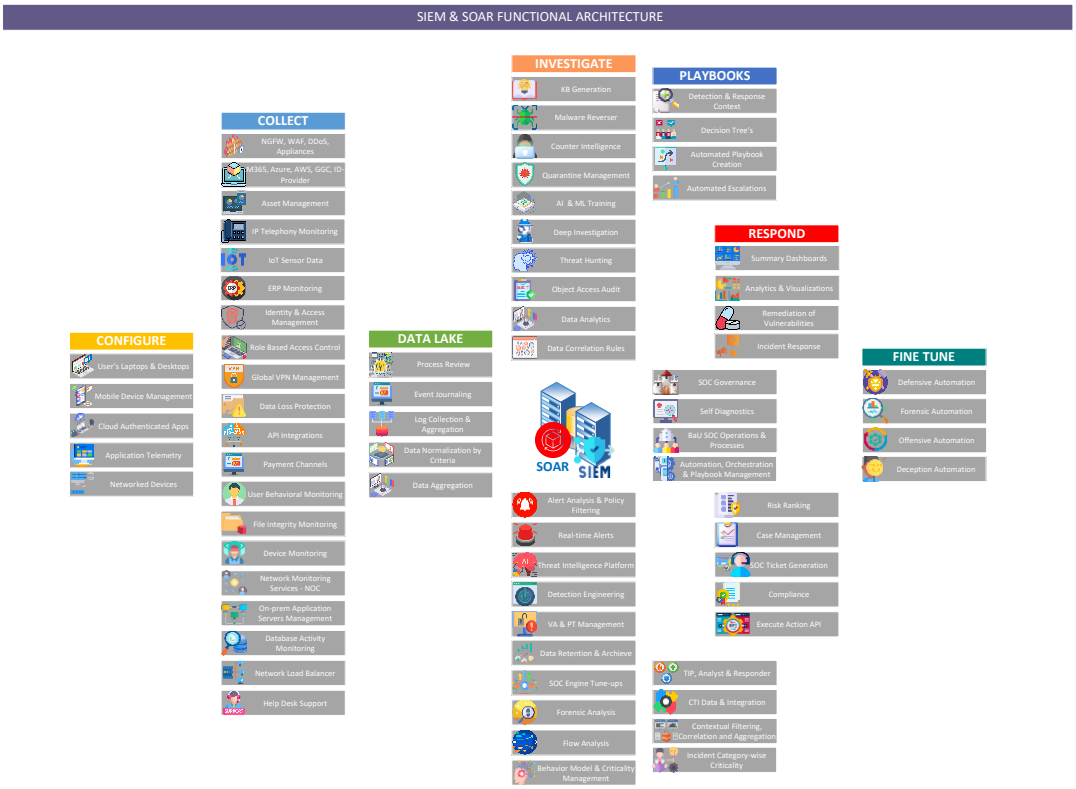


SIEM & SOAR Architecture

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.



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.

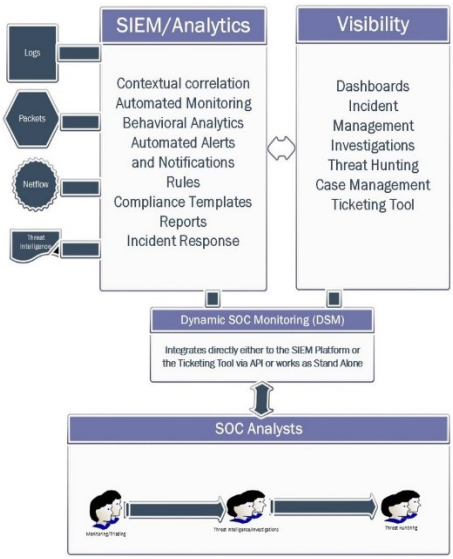
Some of the best ones are:

- Rubrik
- Druva Phoenix
- Acronis Cyber Protect
- Redstor
- Stellar
- Veeam Data Platform
- Zerto
- Bacula 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?

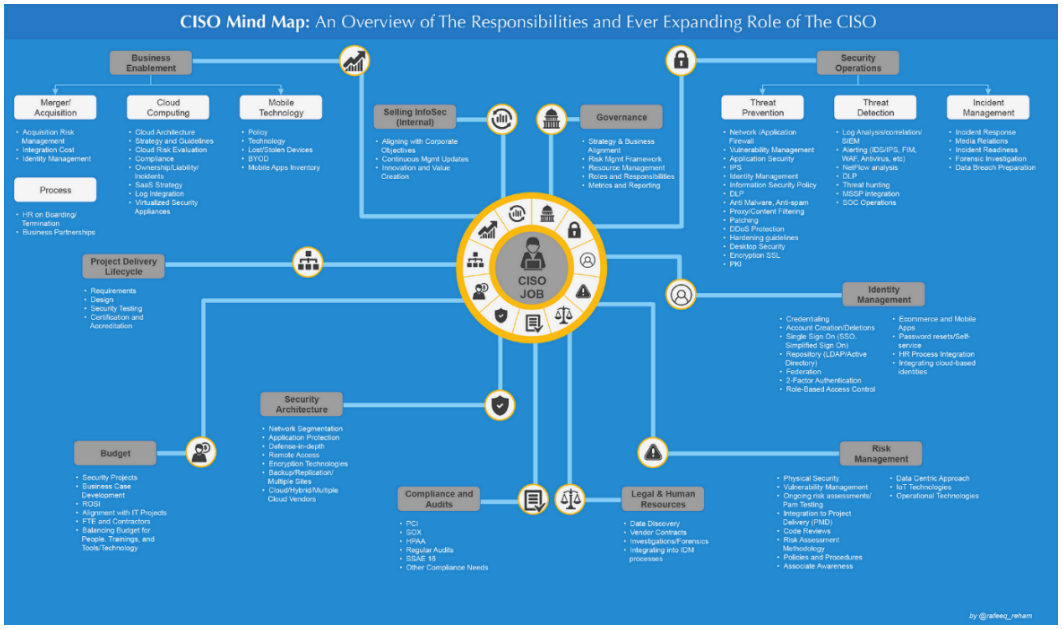
So, you should, let me tell you why. If you are learning your trade in developing computing environment discipline, you should know the path what to do, where to go, job aids that will provide you the necessary tools, learning to reach your goal, therefore, plan early as well. As you can understand that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

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)



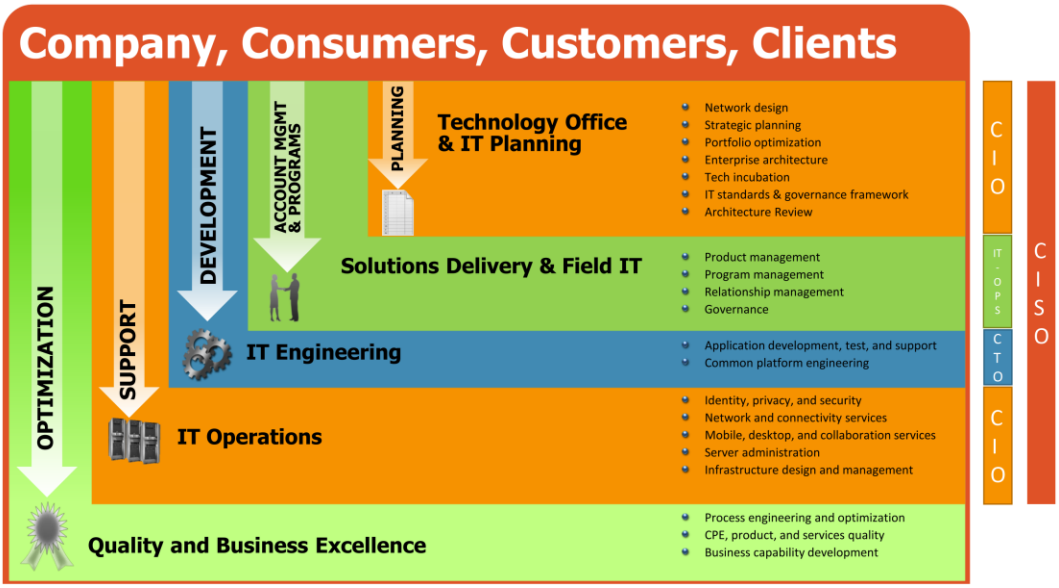
The above illustration clearly defines the responsibilities of a CISO, but somehow, he/she reports to the CIO, maybe I am wrong, but my understanding is that, all of the roles of a CIO (network architect - infrastructure background), CTO (software architect - comes from developer background) roles falls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

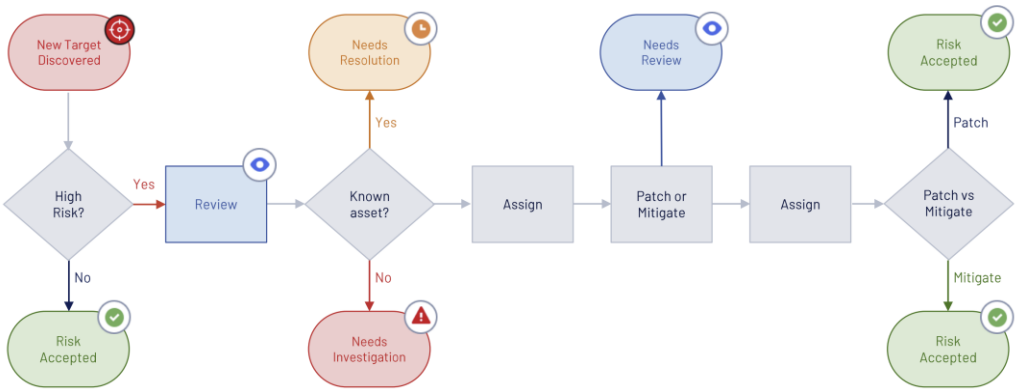
hire someone, do skip them, identify early, and you should be a better judge of a character for selecting your teammates.

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.

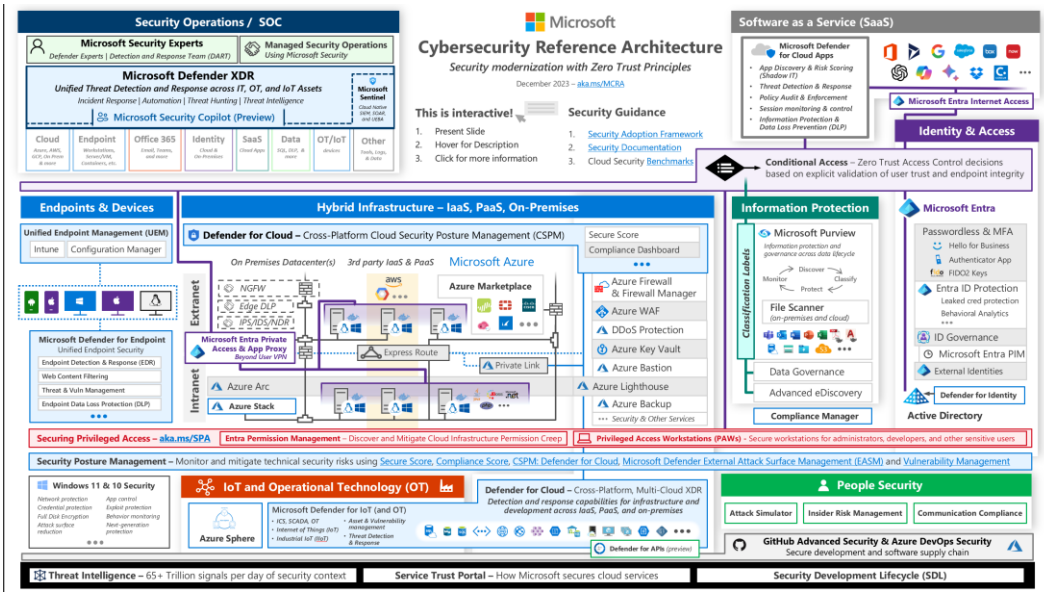
In the landscape where cyber threats have become very common, traditional vulnerability management may fall short of addressing the most critical risks in the organization. Adopting a risk-based approach allows us to prioritize vulnerabilities based on their potential impact, enabling us to allocate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



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

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

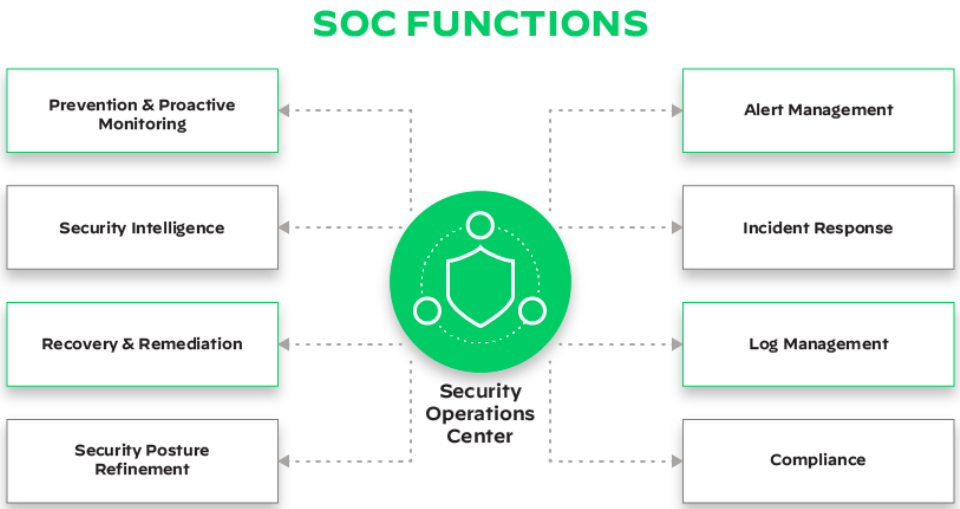
SOC Functions

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

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.



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!

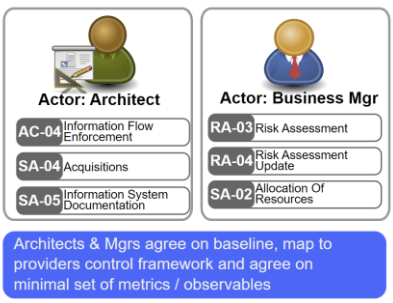
That's how a SOC manager should perform, keep learning from each other, fine tune all the processes, try making it shorter, and do share and give back, that's how you grow. Set your ego aside, it's doable.

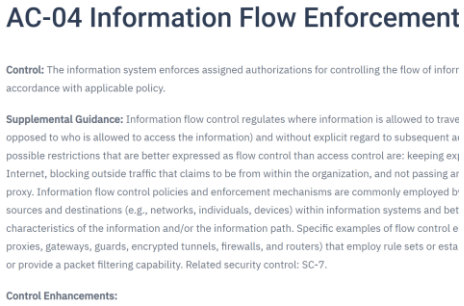
Open Security Architecture (OSA) Architecture Patterns

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):

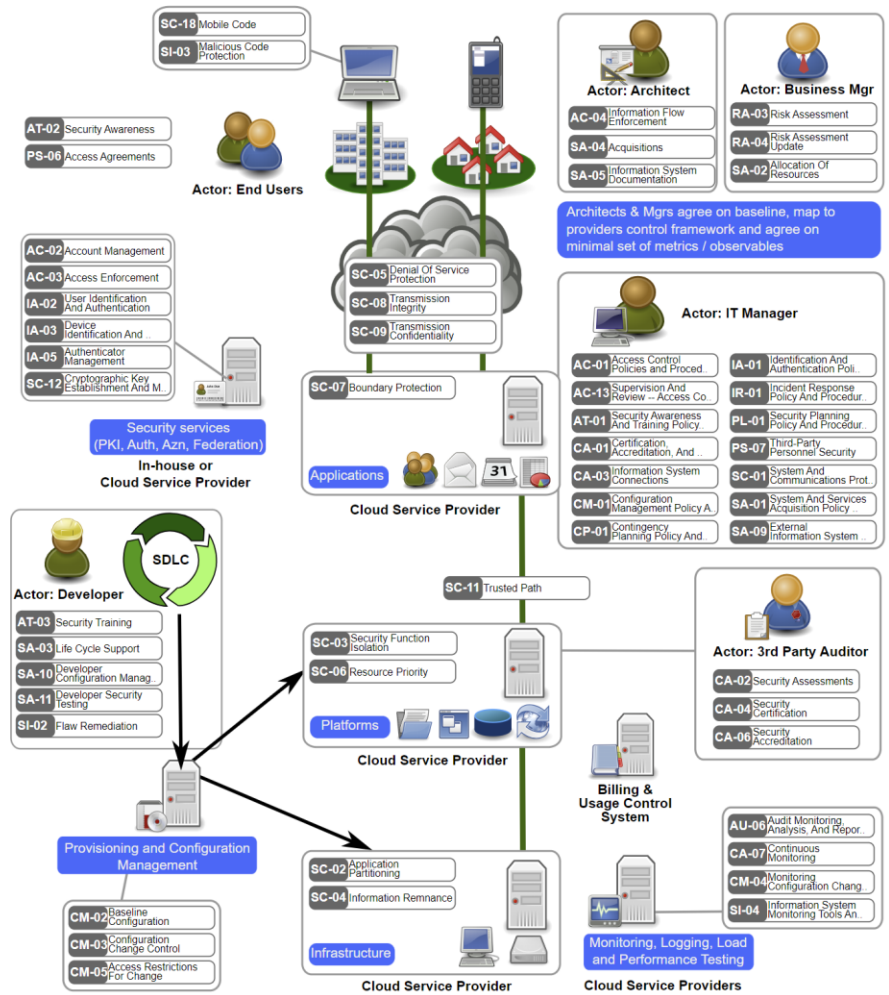




- Total Control Catalogue: Control Catalogue (opensecurityarchitecture.org)
- Patterns Landscape: Pattern Landscape (opensecurityarchitecture.org)
- Threat Catalogue: Threat Catalogue (opensecurityarchitecture.org)

SP-011: Cloud Computing Pattern

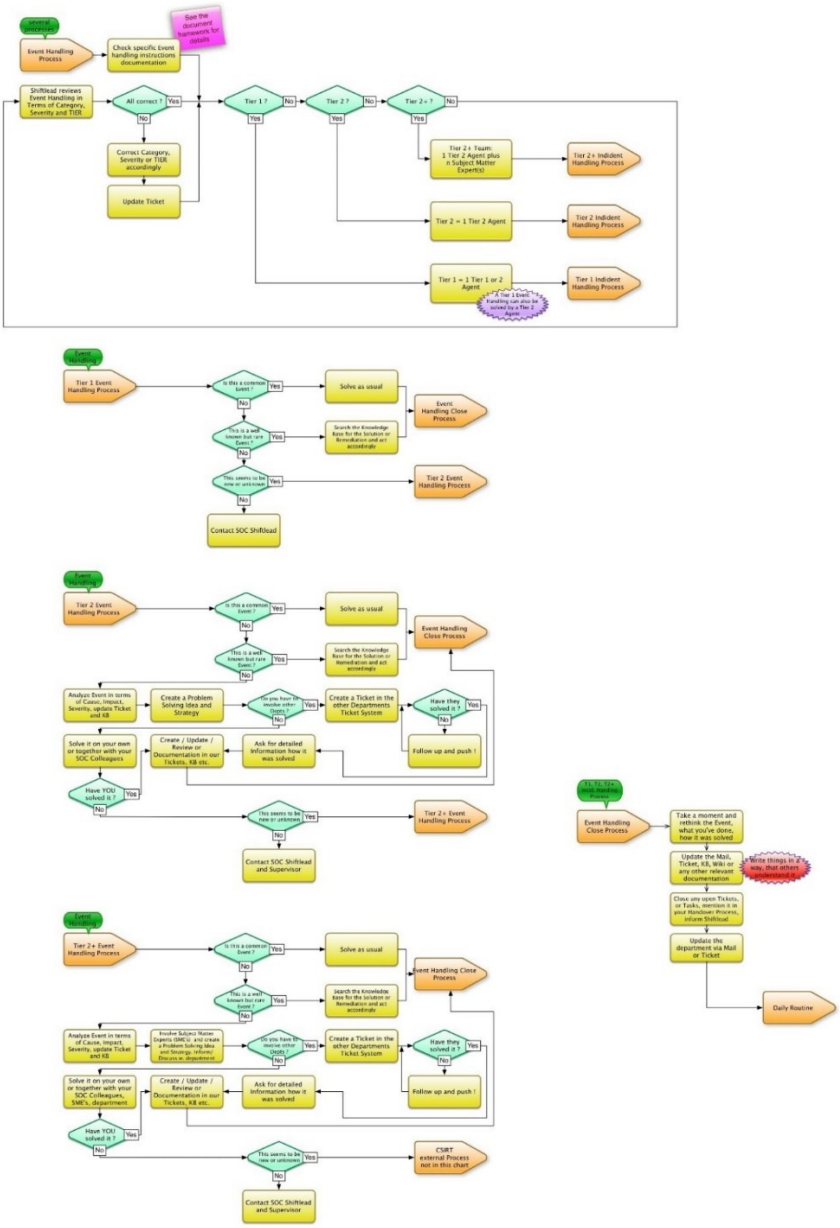
Diagram:



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.

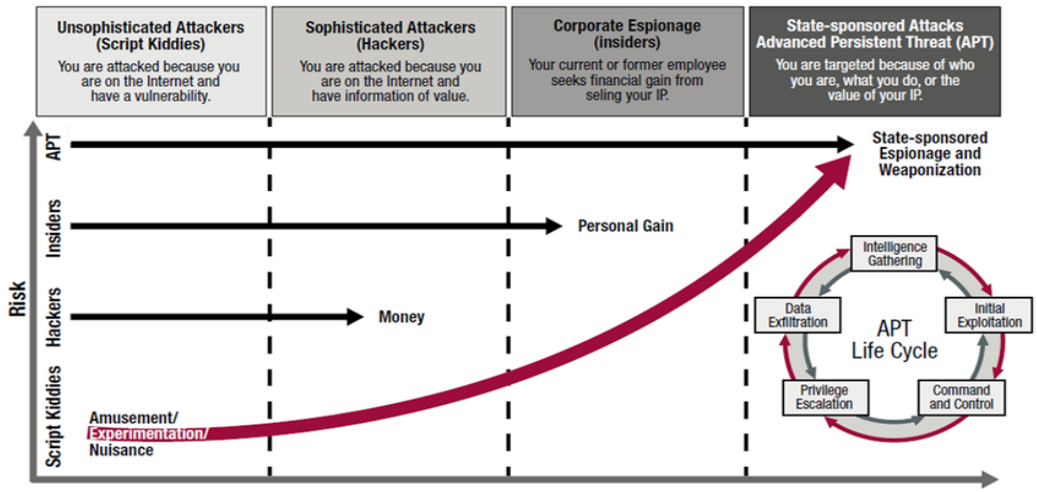
Source: SP-011: Cloud Computing Pattern (opensecurityarchitecture.org)

SOC Methodology



Source: [The SOC methodology - SecureGlobal]

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



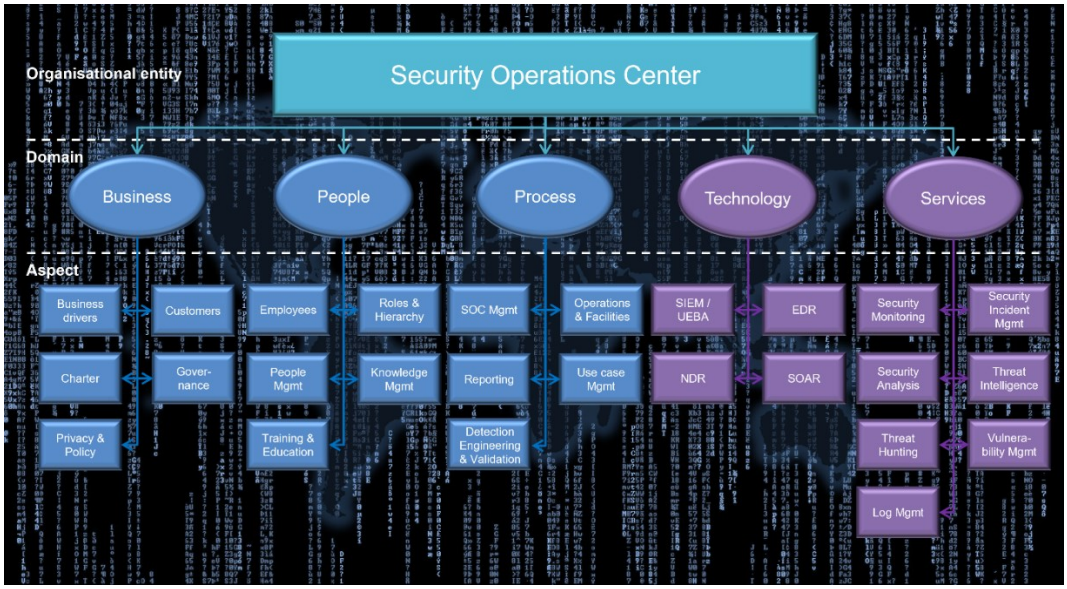
Source: [how threat landscapes have evolved | Download Scientific Diagram (researchgate.net)]

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

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, CISECURITY, 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

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 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

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

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

	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

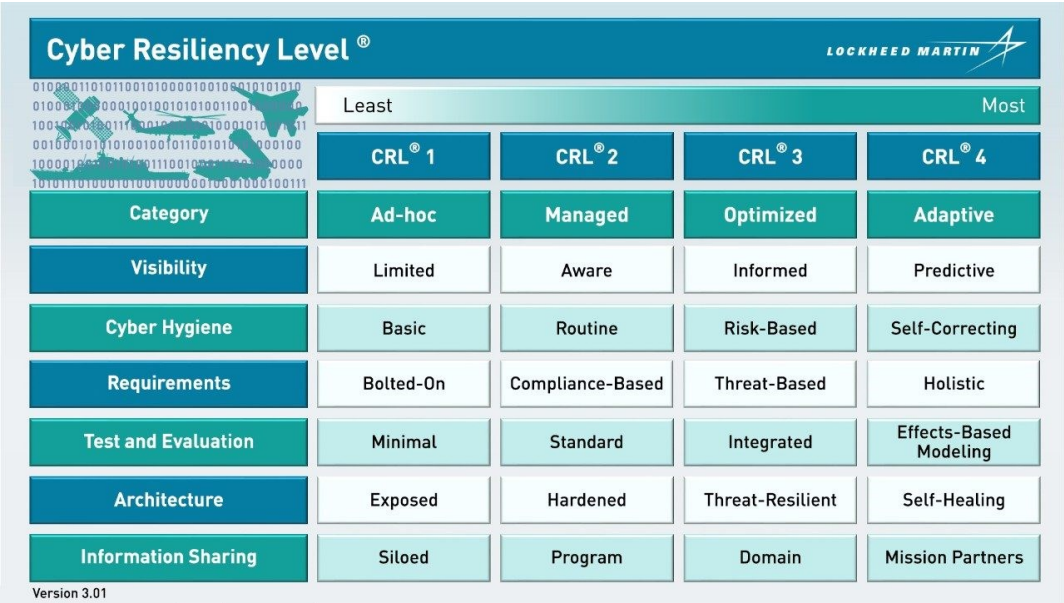
can consider the segment fully segmented and secure. However, you should also monitor and review the segment regularly, as the network conditions and requirements may change over time.

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)



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
Spoofing	Involves illegally accessing and then using another user's authentication information, such as username and password
Tampering	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
Repudiation	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
Information 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

Denial 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
Elevation 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.

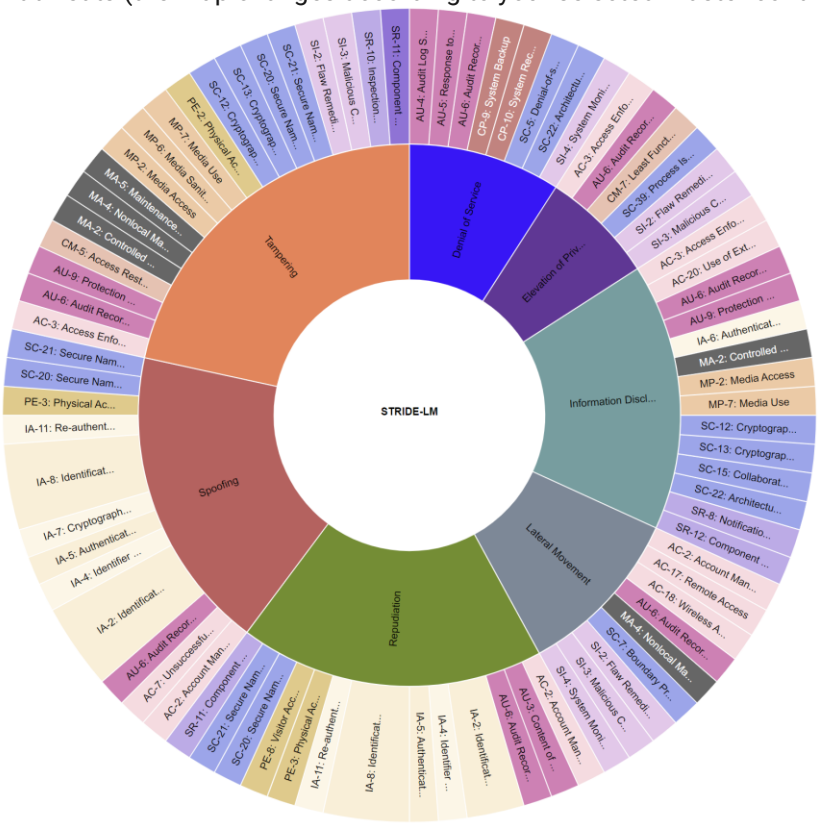
Browser:

- **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

the different threats (the map changes according to your selected master control points):



Source: [Sunburst Visualization of STRIDE-LM to Security Controls - CSF Tools]

Threat Modeling: 12 Available Methods

Threat-modeling methods are used to create:

- an abstraction of the system.
- profiles of potential attackers, including their goals and methods.
- a catalog of potential threats that may arise.

Threat Modeling Method	Features
STRIDE	• Helps identify relevant mitigating techniques • Is the most mature • Is easy to use but is time consuming
PASTA	• 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	• Helps identify relevant mitigation techniques • Contains built-in prioritization of threat mitigation • Can be labor intensive and time consuming
CVSS	• Contains built-in prioritization of threat mitigation • Has consistent results when repeated • Has automated components • Has score calculations that are not transparent
Attack Trees	• 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	• 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	• Encourages collaboration among stakeholders • Targets out-of-the-ordinary threats • Leads to many false positives
hTMM	• Contains built-in prioritization of threat mitigation • Encourages collaboration among stakeholders • Has consistent results when repeated
Quantitative TMM	• Contains built-in prioritization of threat mitigation • Has automated components • Has consistent results when repeated
Trike	• 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	• 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	• 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)]

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

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?

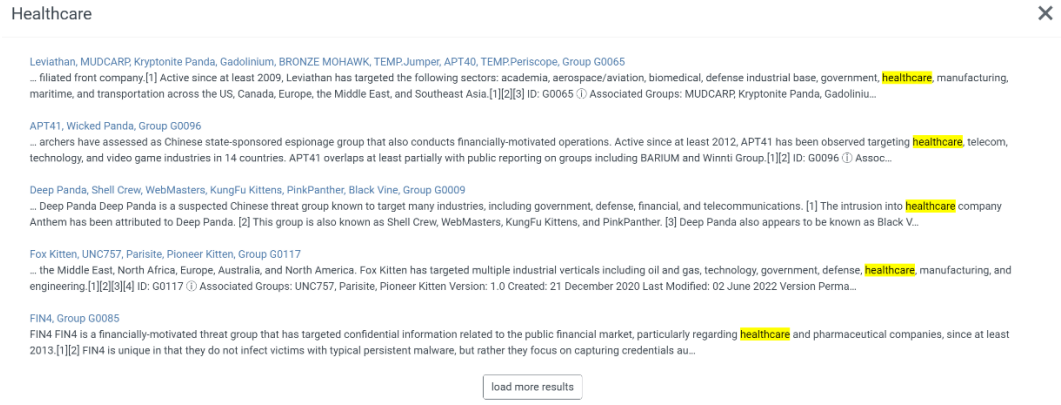
We need an industry. For this demonstration I've selected HEALTHCARE as the industry.

Lets get started

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

Click the search magnifying glass

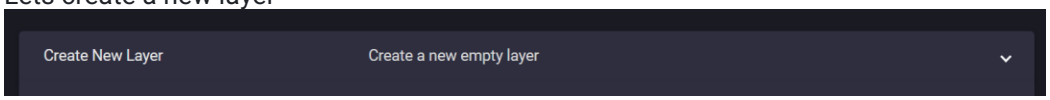
Search for "healthcare"



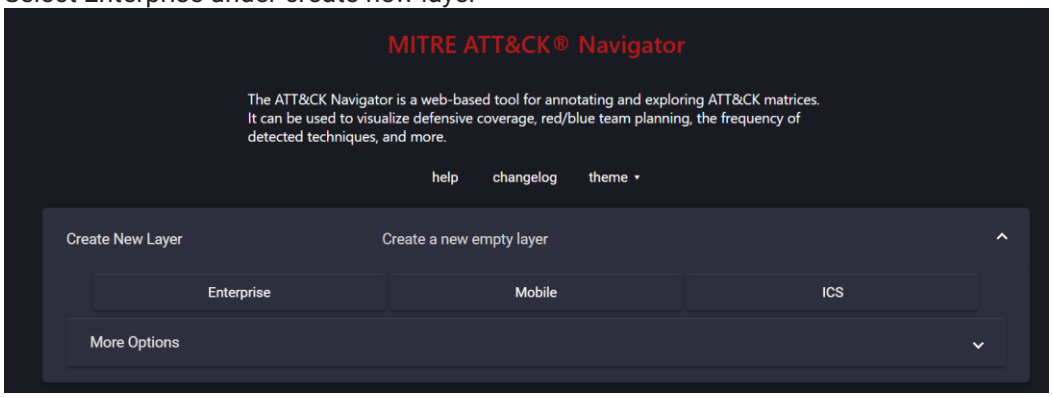
For simplicity we will select two threat groups APT 40/Leviathan and APT 41

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

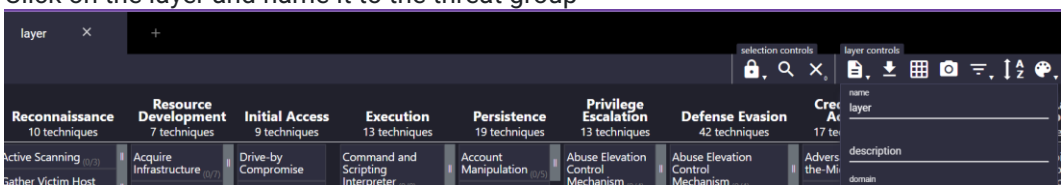
Lets create a new layer



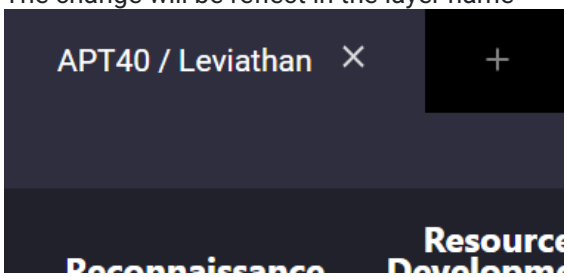
Select Enterprise under create new layer



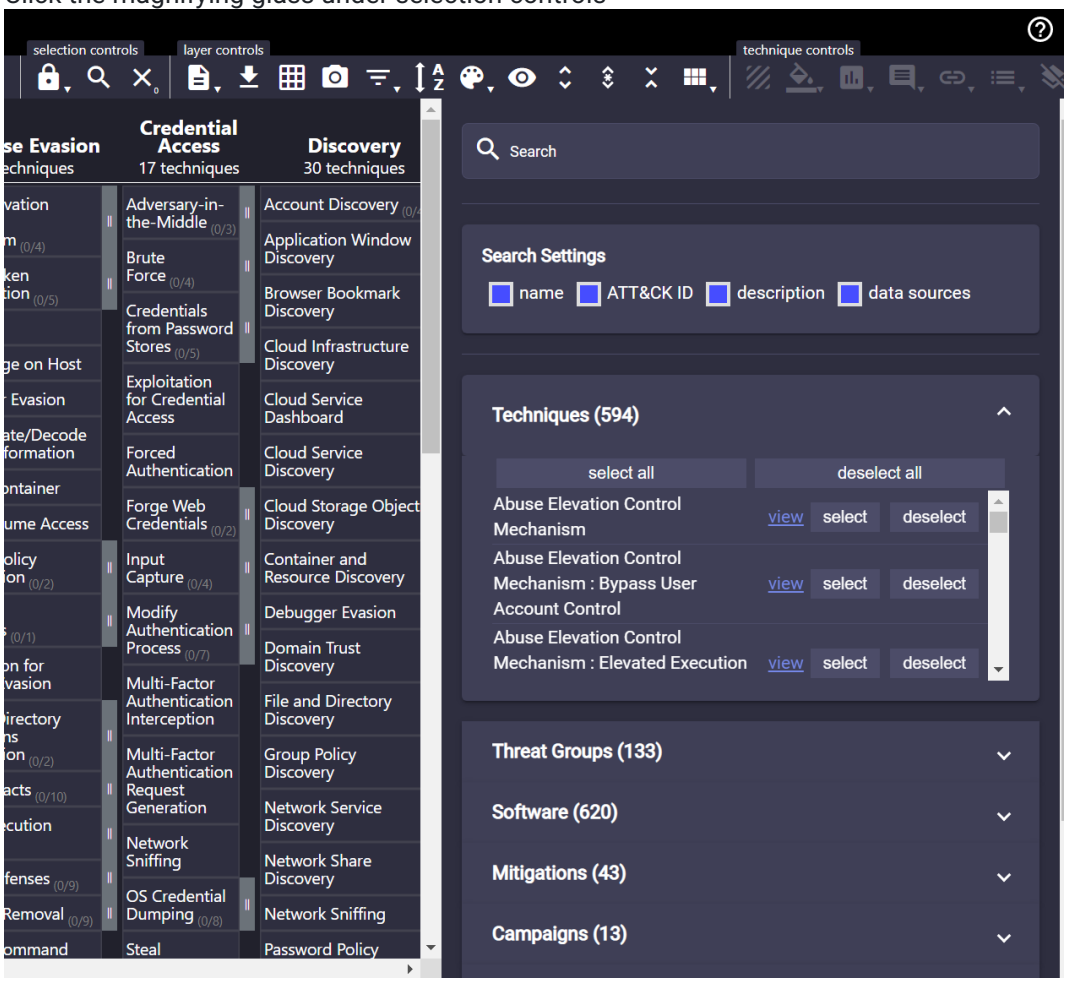
Click on the layer and name it to the threat group



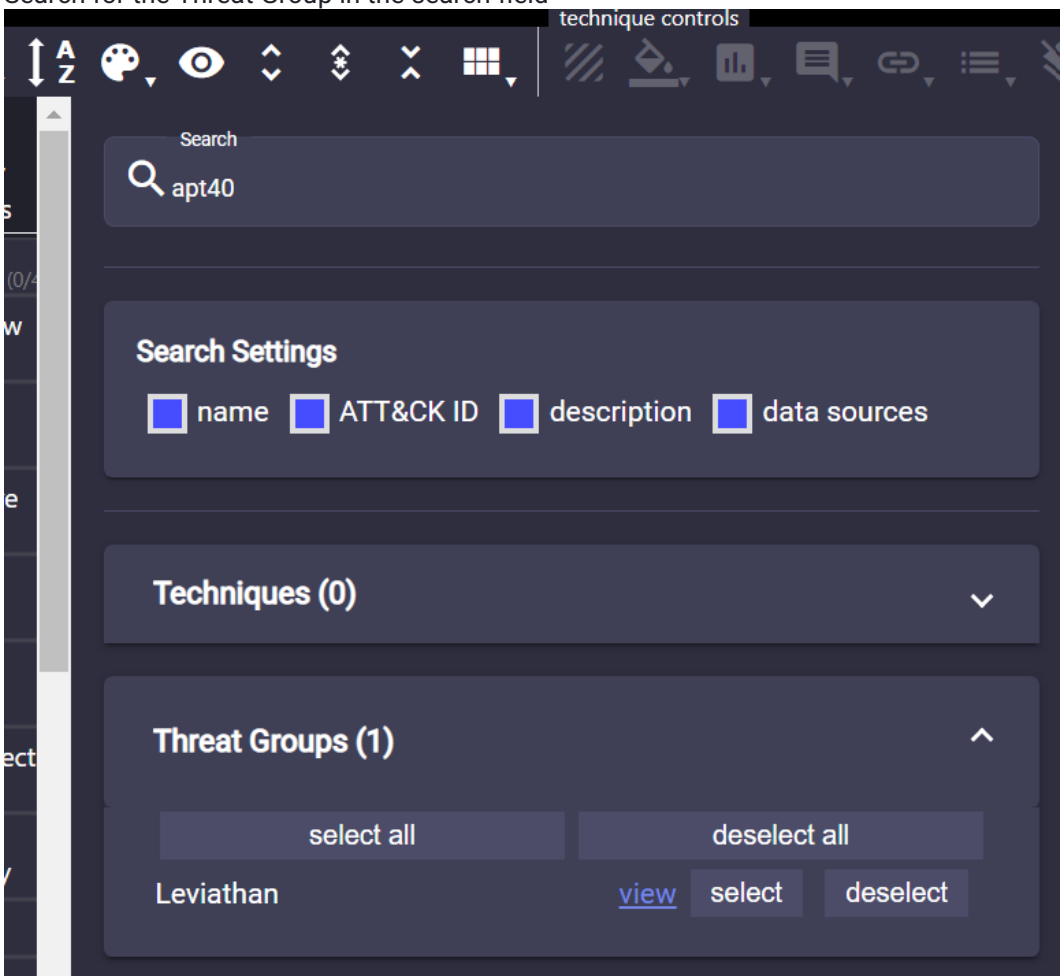
The change will be reflect in the layer name



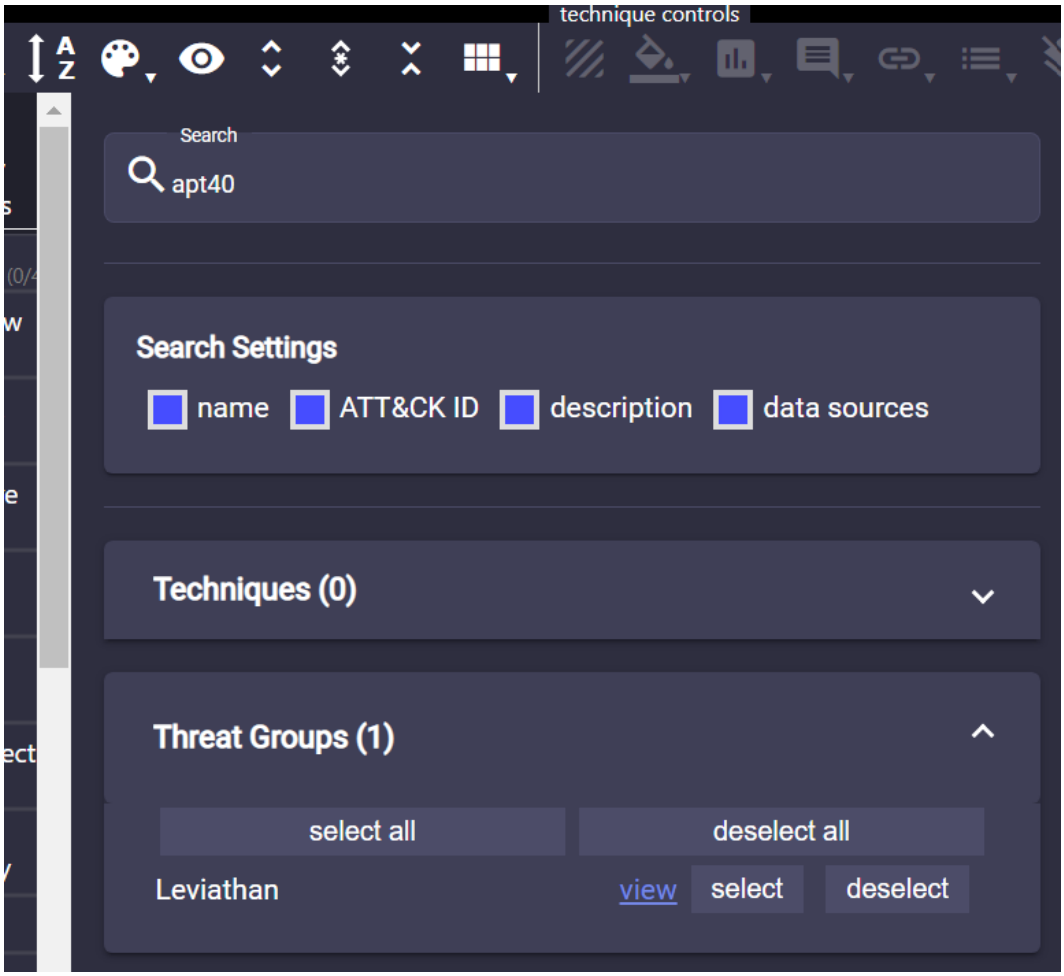
Click the magnifying glass under selection controls



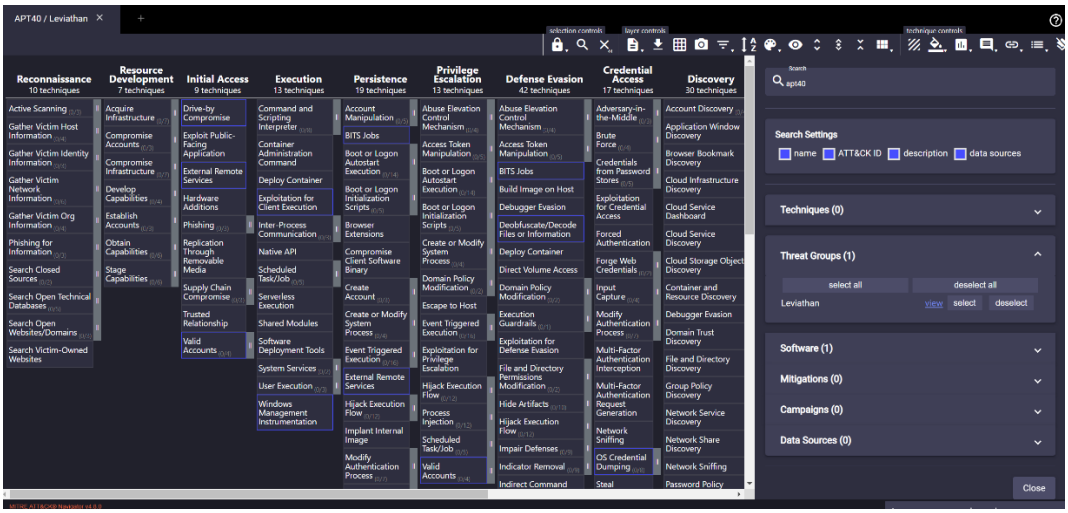
Search for the Threat Group in the search field



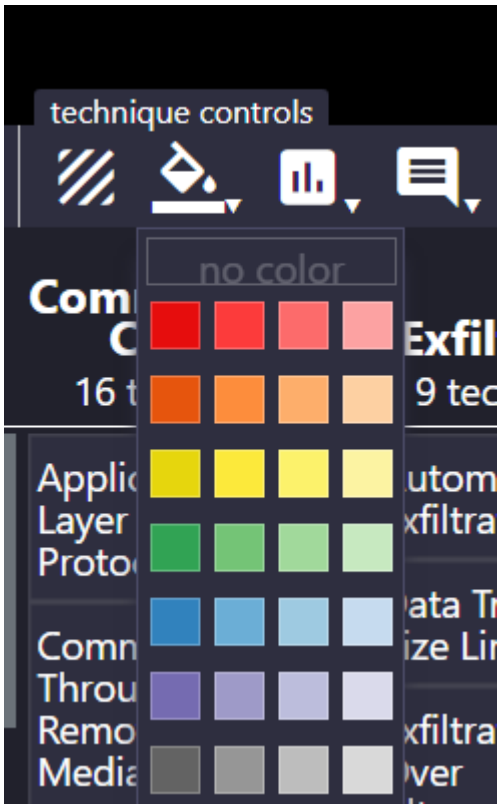
Click select next to the threat group



Selected techniques should now appear highlighted

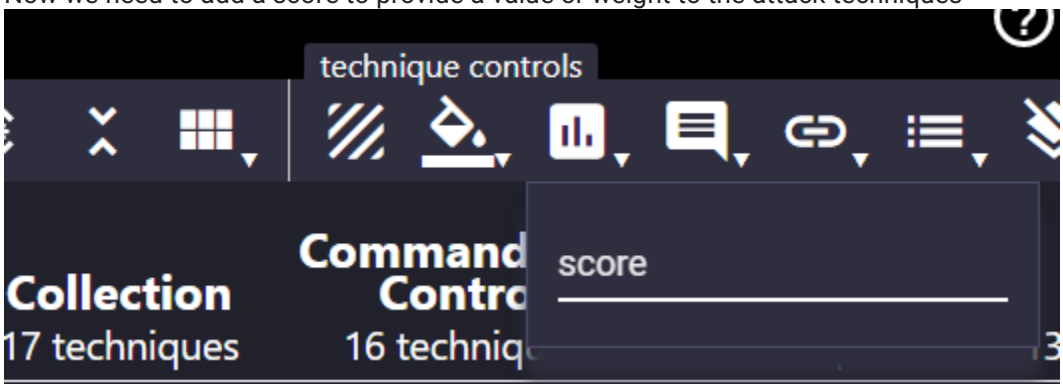


Now we want a bit more visibility in the techniques so we will select a color

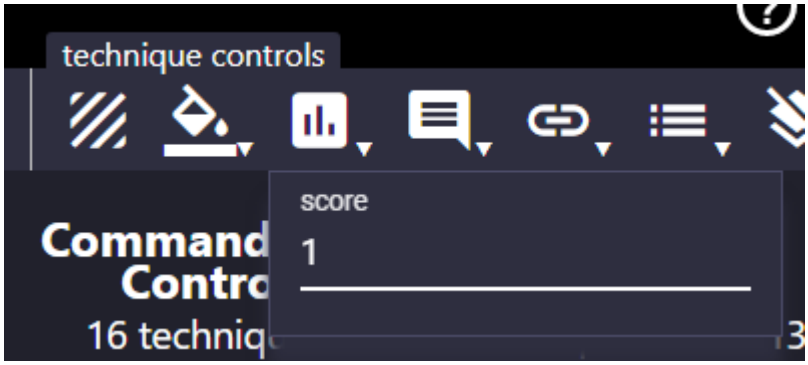


The attack techniques should now be colored.

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



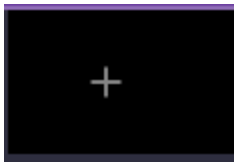
Set the value for score to 1



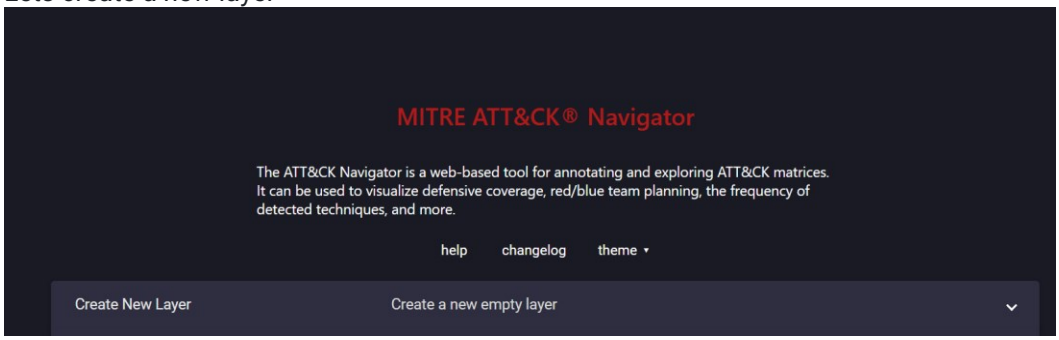
We've added our first known threat group now we need to add more for the industry we selected.

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

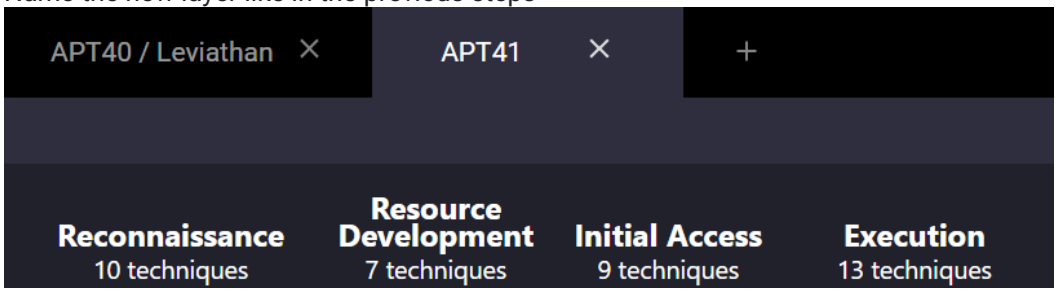
Lets add one more by clicking the +



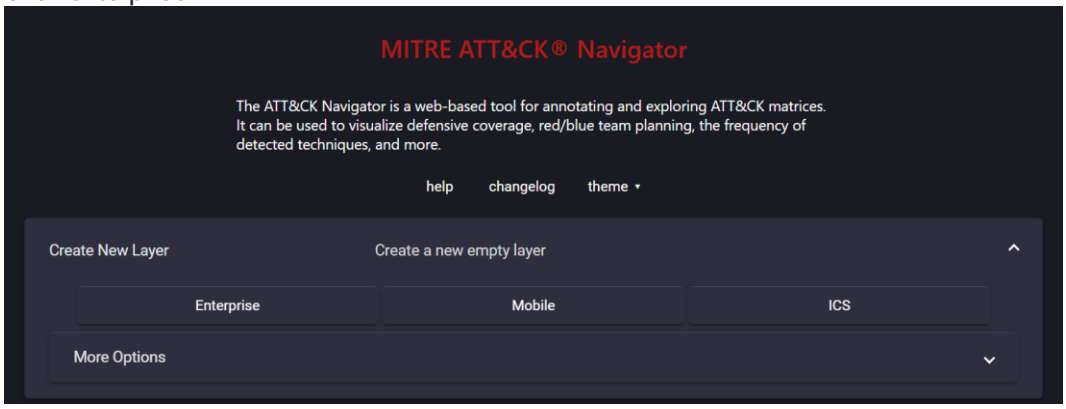
Lets create a new layer



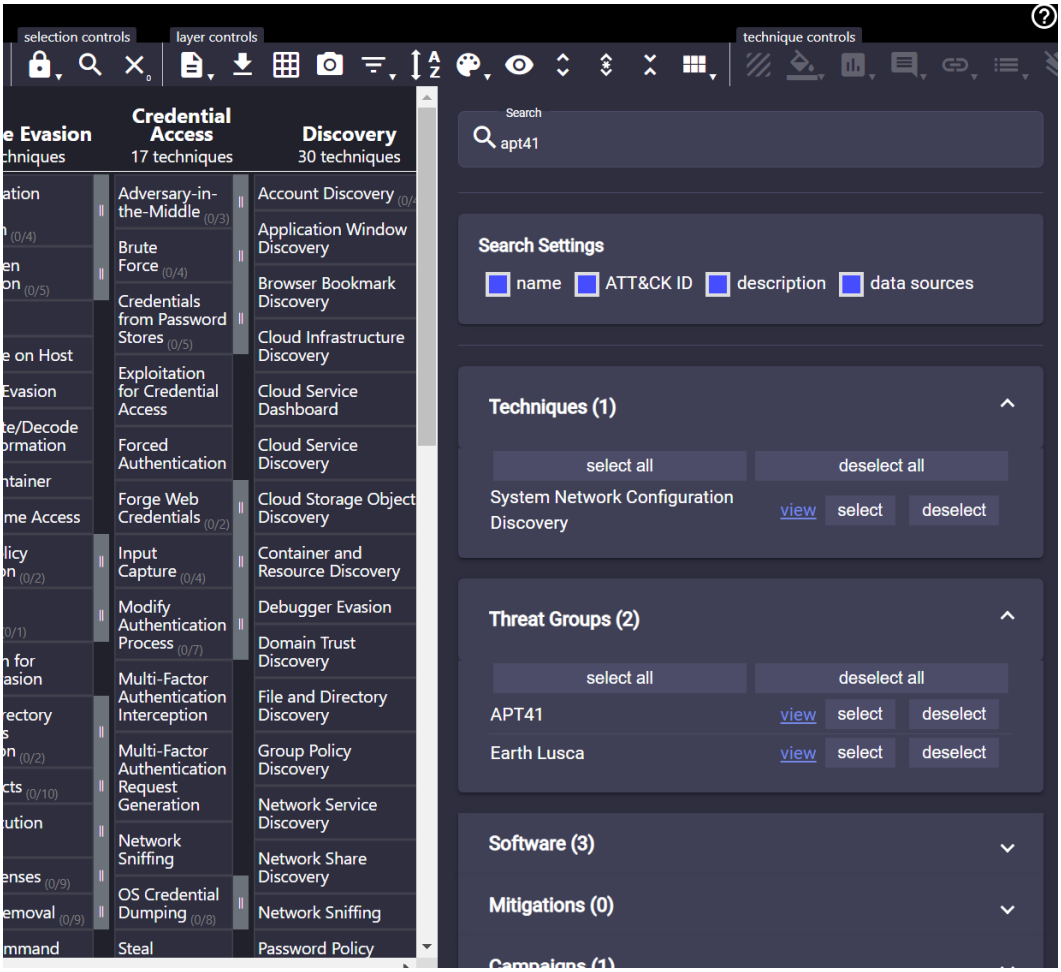
Name the new layer like in the previous steps



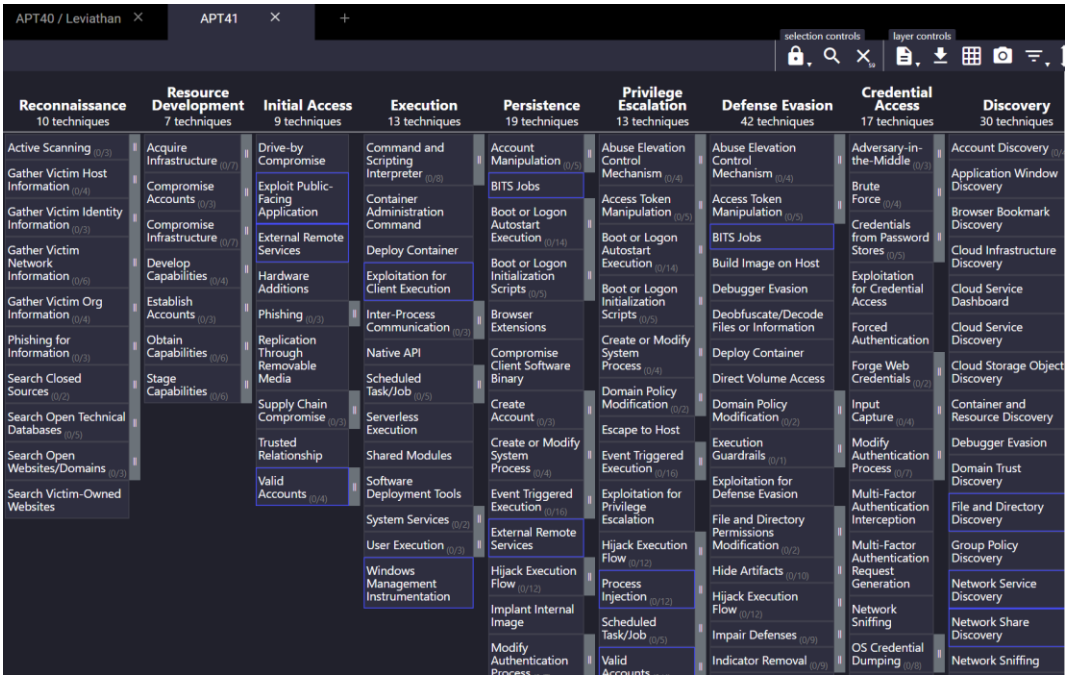
Click enterprise



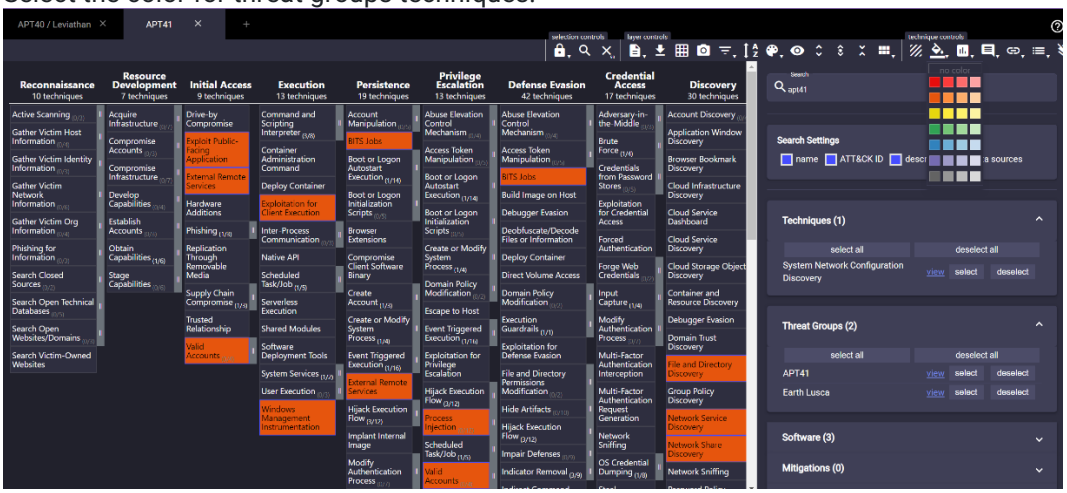
Click Selection Controls magnifying glass and search for the threat group



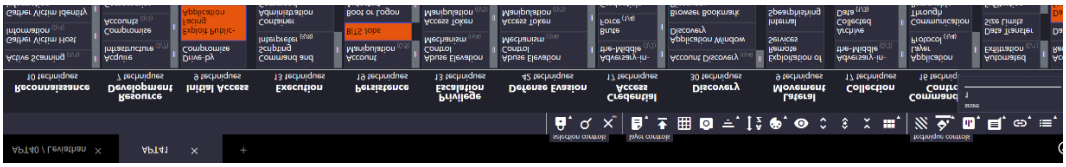
Validate that the threat group techniques have been selected



Select the color for threat groups techniques.

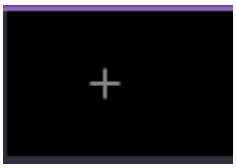


Set the score for the techniques just as before

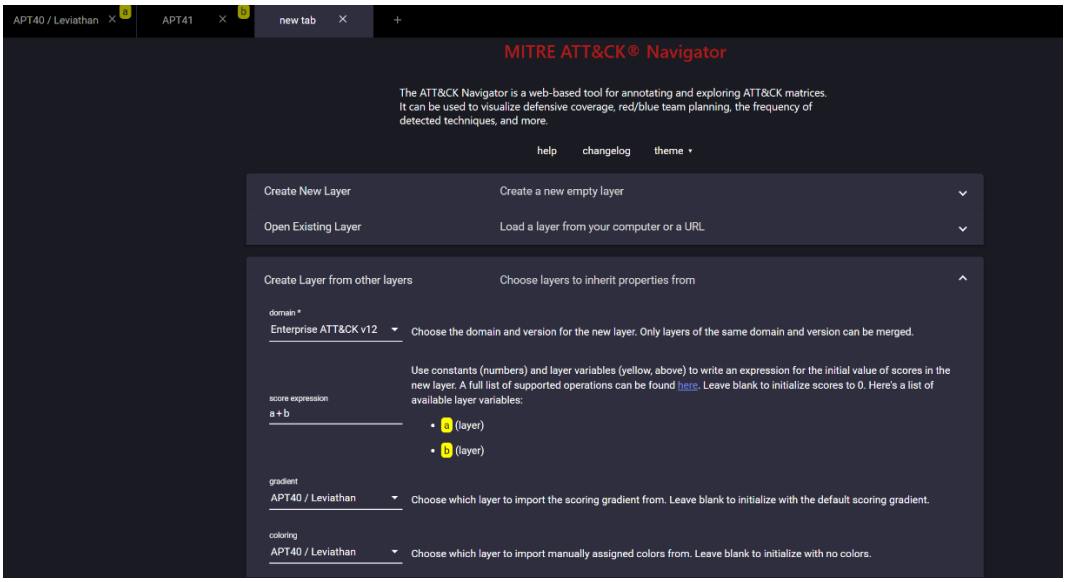


Adding up the layers to show the threat model

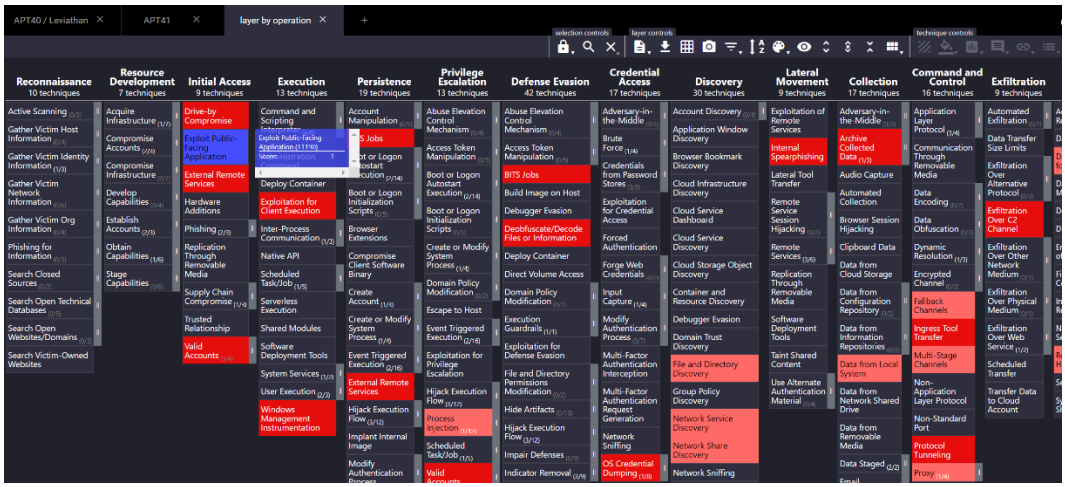
Now we want to add all of the layers (if you don't two thats fine but you can always do more).
Lets add one more by clicking the +



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



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.

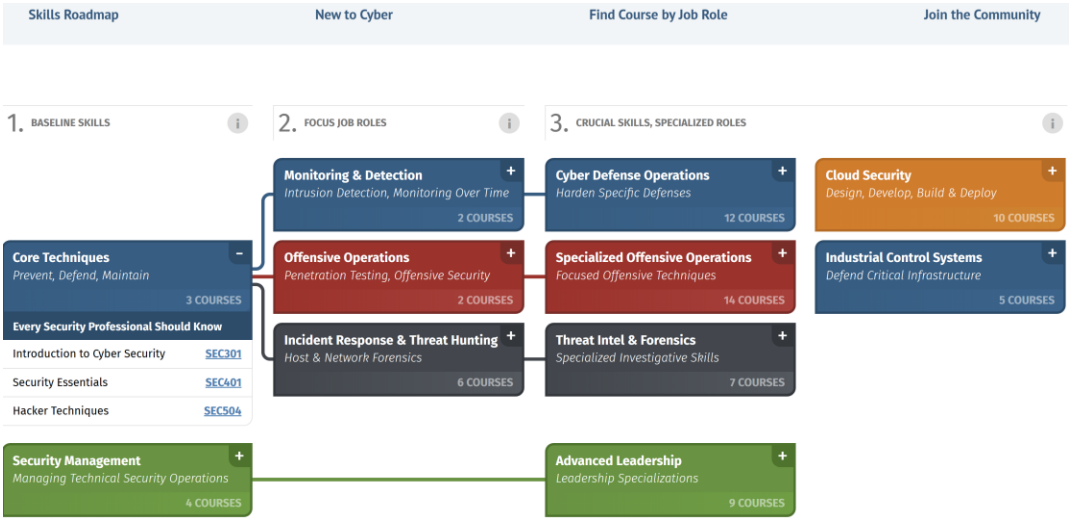


Next Steps

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.

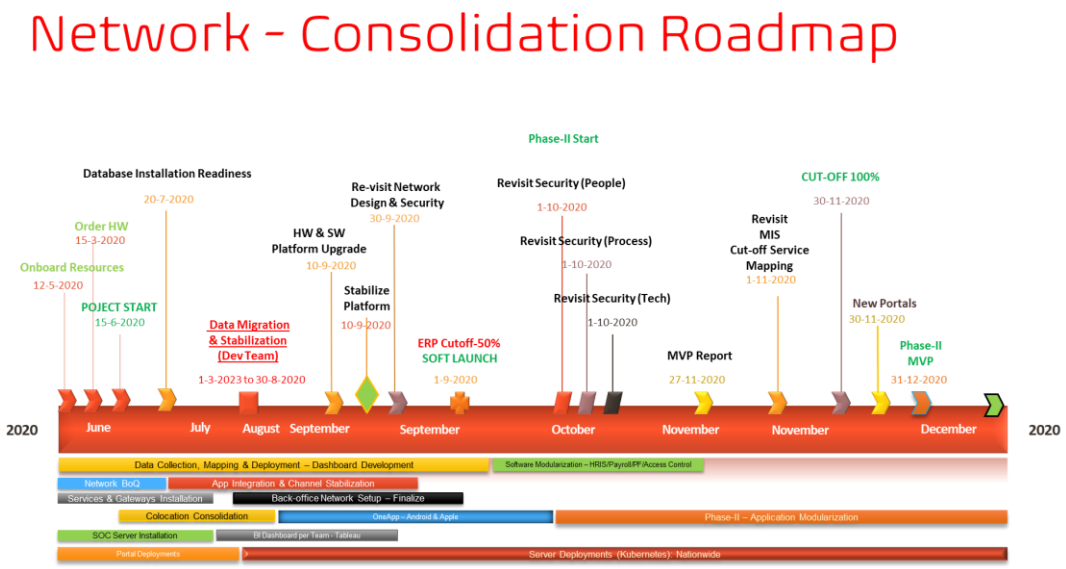
Cyber Security Roadmap

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:



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”):



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

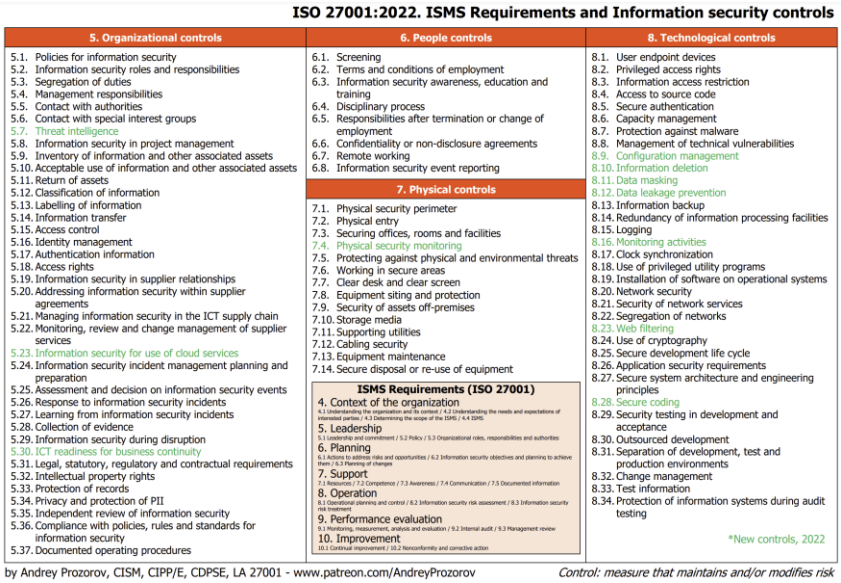
1. **Proactive Monitoring**: The SOC team gathers information from various resources, including threat intelligence feeds and log files from systems all around the enterprise. They carefully monitor the company's assets, from on-premises servers in data centers to cloud resources. Accurate data collection 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.

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

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. People controls

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

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 Actions to address 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 risk treatment
9. Performance evaluation
9.1 Monitoring, measurement, analysis and evaluation / 9.2 Internal audit / 9.3 Management review
10. Improvement
10.1 Continual improvement / 10.2 Nonconformity and corrective action

8. Technological controls

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

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

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,

				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 avaiable	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.			

24	ICT Emergency Response Team with role and responsibilities.	Full Compliant	team to be formed	Roles and Responsibilities for Contingency Planning
25	ICT incident response plan & process	Full Compliant	team to be formed	19. Incident procedure 20. Incident Management Process + 21. Incident Log
26	Incident escalation matrix	Full Compliant	Escalation matrix to be define	19. Incident procedure 20. Incident Management Process + 21. Incident Log
27	ICT Asset Management policy/Procedure. Documents related to ICT Asset Classification and Asset custodianship/ownership.	Full Compliant		Information_Asset_Inventory
28	Inventory of all ICT assets.	Full Compliant		Information_Asset_Inventory
29	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
30	End user device Standardization/Hardening procedure/policy.	Full Compliant		11 Personally Owned Device (BYOD) Security Policy
31	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
32	Domain Controller and Password control policy.	Full Compliant		20 Access Control Policy

33	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
34	Bring Your Own Device (BYOD) policy and procedure.	Full Compliant		11 Personally Owned Device (BYOD) Security Policy
35	physical Access authorization procedures/policy at data center.	Full Compliant		20 Access Control Policy, 24 Physical Security Policy
36	Fire Prevention policy and firefighting team information. Fire drill	Partial Compliant		Not started @ Bulu, Datacenter has FM200
37	Baseline standards for Operating Systems, Databases, Network equipment, security equipment	Full Compliant		22 Network Security Management Policy, CISECURITY Benchmarks
38	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		
39	Documentation for server OS hardening.	Full Compliant		CISECURITY Benchmarks
40	Cryptographic key management policy and procedures.	Full Compliant		31 Encryption and Key Management Policy
41	Email and internet usage policy.	Full Compliant		14 Information Exchange Policy
42	Cyber Security policy.	Full Compliant		In general all are included in multiple policies, Cybersecurity

				Policy, 30 Security Incident Response Policy, 32 Data Breach Response Policy
43	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
44	Patch Management policy.	Full Compliant		27 System Configuration Management Policy
45	Security monitoring systems and processes.	Full Compliant		36 Log Management and Monitoring Policy
46	Password policy.	Full Compliant		High Level Information security policy
47	Privileged Access Management procedure	Full Compliant		Access_Control_Policy
48	Business Continuity Plan (BCP).	Full Compliant		34 IT Business Continuity Policy
49	Disaster Recovery Plan (DRP) and DR test documentations.	Full Compliant		BCP, plan is ready, not tested yet, will run if after UAT
50	Backup & Restore Plan /Policy (BRP). The backup inventory and log sheets.	Full Compliant		33 Backup and Recovery Policy
51	Acquisition and Development of Information Systems	Full Compliant		37 Acquiring Information Systems And Services

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

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

				+ Remote Working Security Policy
76	Source code security	Full Compliant		29 Application Development Security Policy
77	Source code leakage prevention	Full Compliant		29 Application Development Security Policy
78	Sensitive data leakage prevention	Full Compliant		Application control
79	Maker and checker in all action in the application	Full Compliant		Application control
80	Email security	Full Compliant		High Level Information Security Policy
81	Web security	Full Compliant		MSB
82	End point security	Full Compliant		High Level Information Security Policy
83	Central log management	Full Compliant		App Control, ELK Stack. 36 Log Management and Monitoring Policy

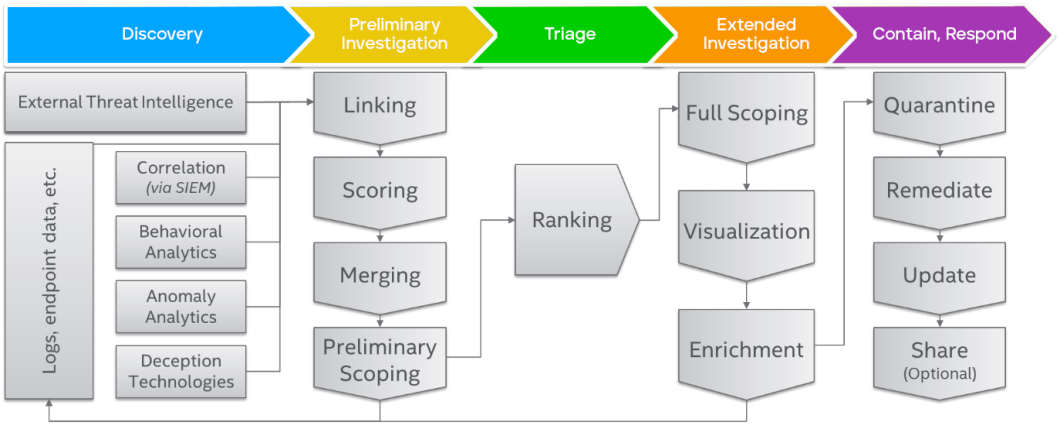
CHAPTER 6

Processes for a SOC

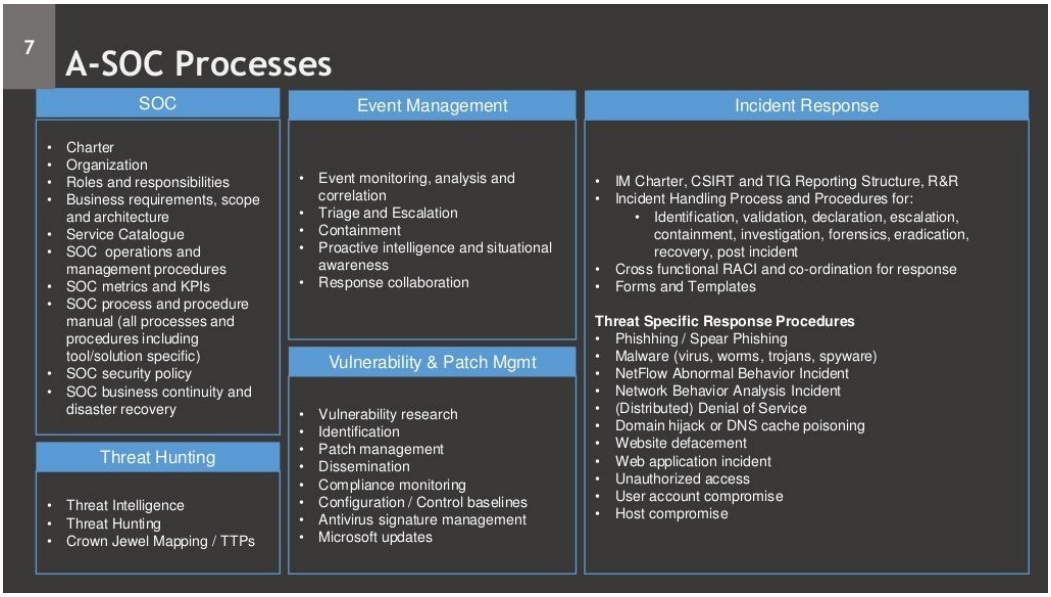
ALONG CAME A SPIDER, DEEPER MAPPING OF ATT&CK FRAMEWORKS ON ENTERPRISE NETWORKS WITH MATRIX AND KPI'S. ALWAYS THINK OF ENTERPRISE GRADE, ALWAYS.

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.

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]

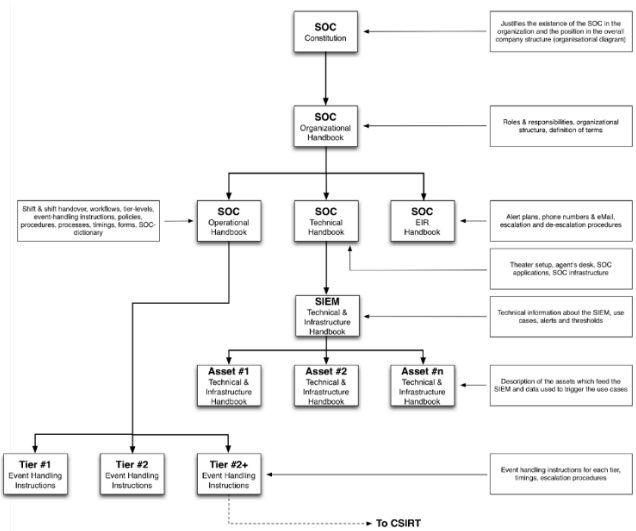


Source: [SOC Architecture (Tech Stack, Process, Org Structure, People Skills) | PPT (slideshare.net)]

- 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)]

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.

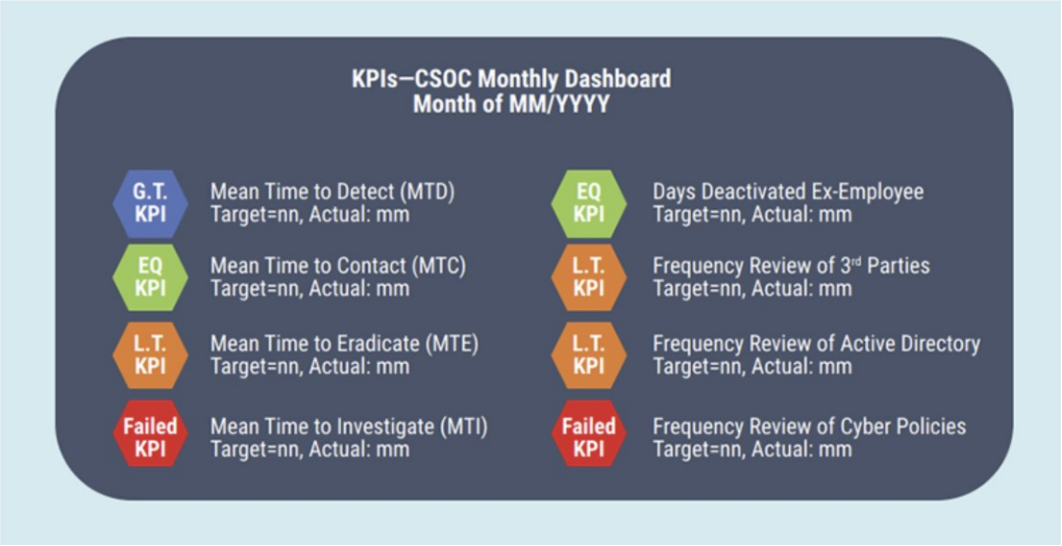
By doing careful investigations, the SOC improves its skill to deal with security incidents, reduce the harm of threats and boost overall incident management. The SOC can also keep improving its methods and increase its skill to find and handle future incidents with precision and speed.

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 SOCs must continually update their knowledge and tools to keep up.
4. **False Positives**: SOCs 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**: SOCs 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)]

7. **Regulatory Compliance**: SOCs 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**: SOCs 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

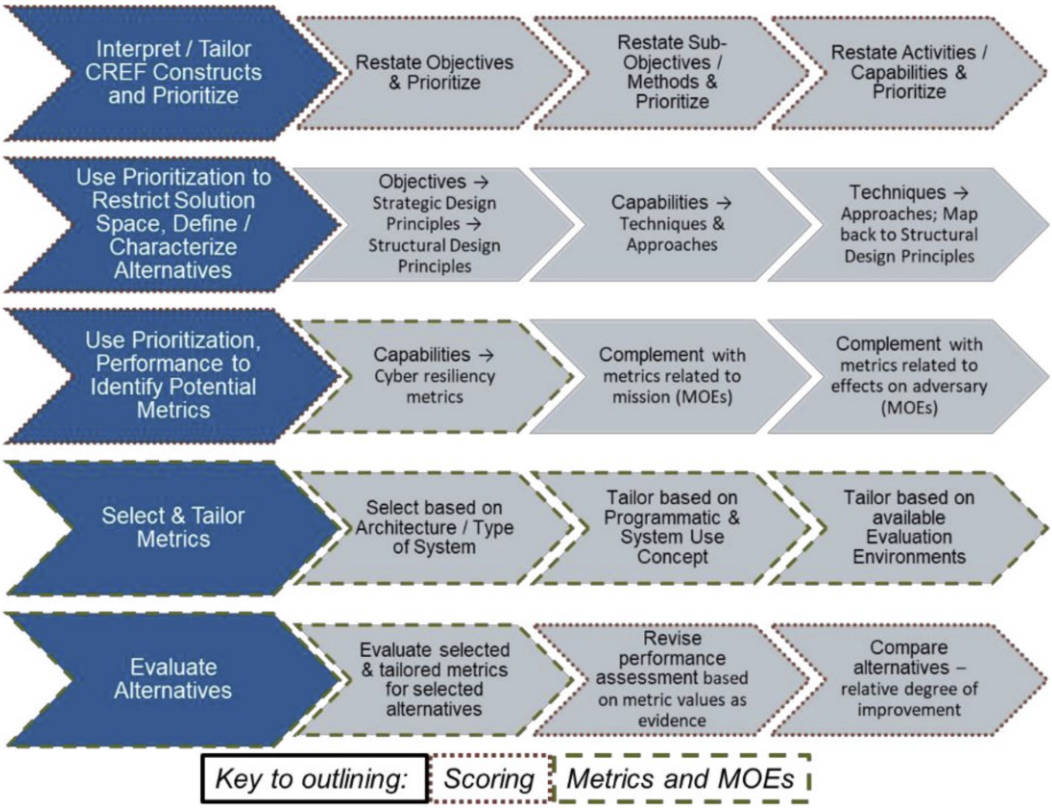
Cyber resiliency scoring methods and metrics are tailorable resources to aid systems engineers, program managers, and others supporting risk management for systems or programs in which cyber resiliency is a concern. A scoring system and a set of metrics

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”



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.

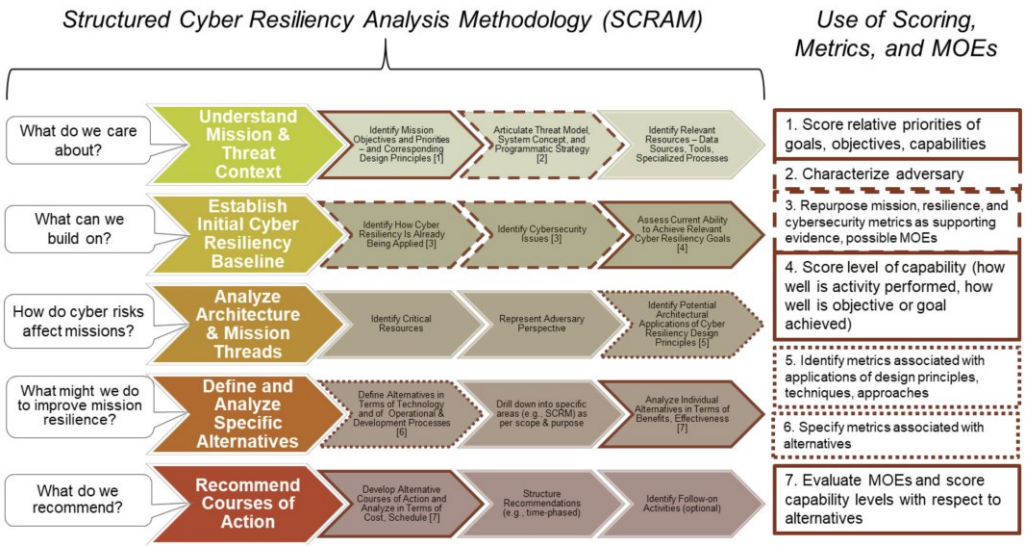
(2) are an outcome of the first step in © 2018 The MITRE Corporation. 2 SCRAM, Understand the mission and threat context. The second step includes identifying how cyber resiliency is already being applied and any cybersecurity issues. Identifying these can indicate existing metrics which could be repurposed 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.

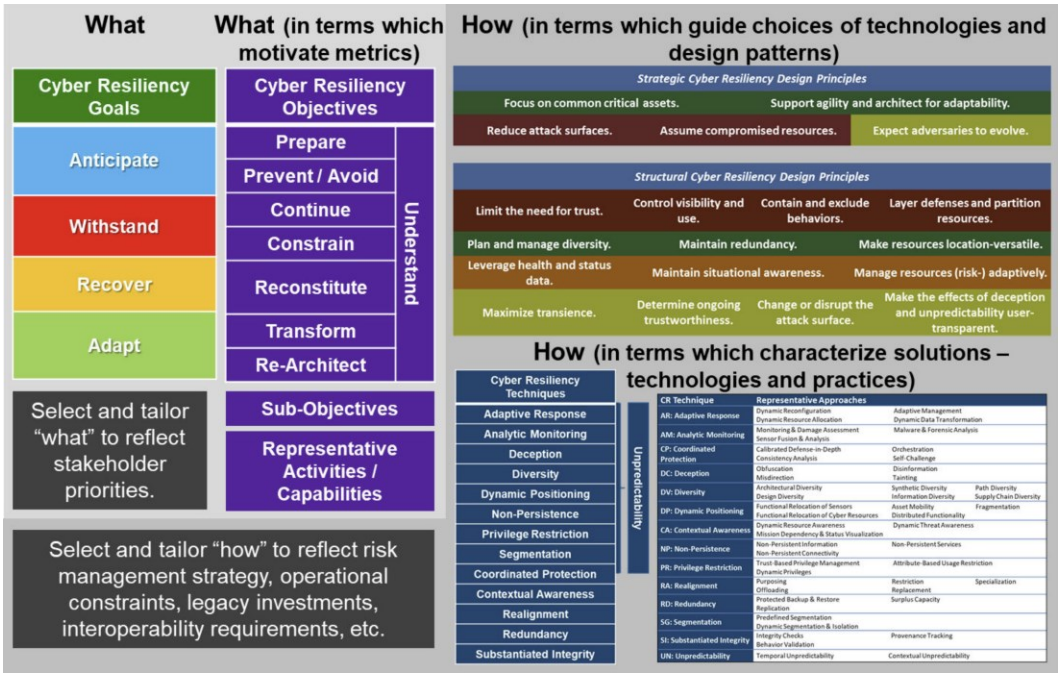
(5) from the metrics catalog. Alternatives are identified in the fourth step, enabling the metrics from the catalog and the metrics identified earlier (3) to be specified in enough detail that they can be evaluated to support comparisons.

(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

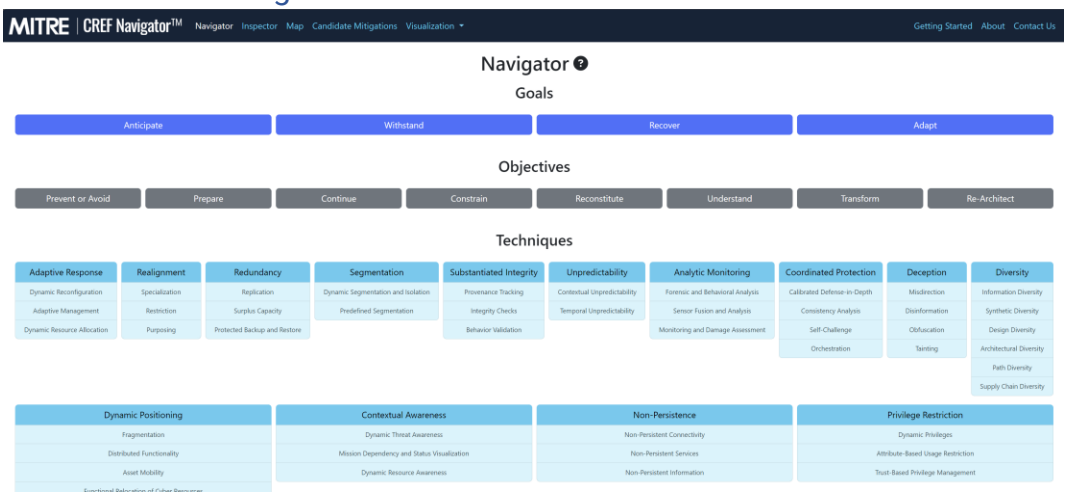


CREF Objectives (The Purple Column)

- **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.)

- **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



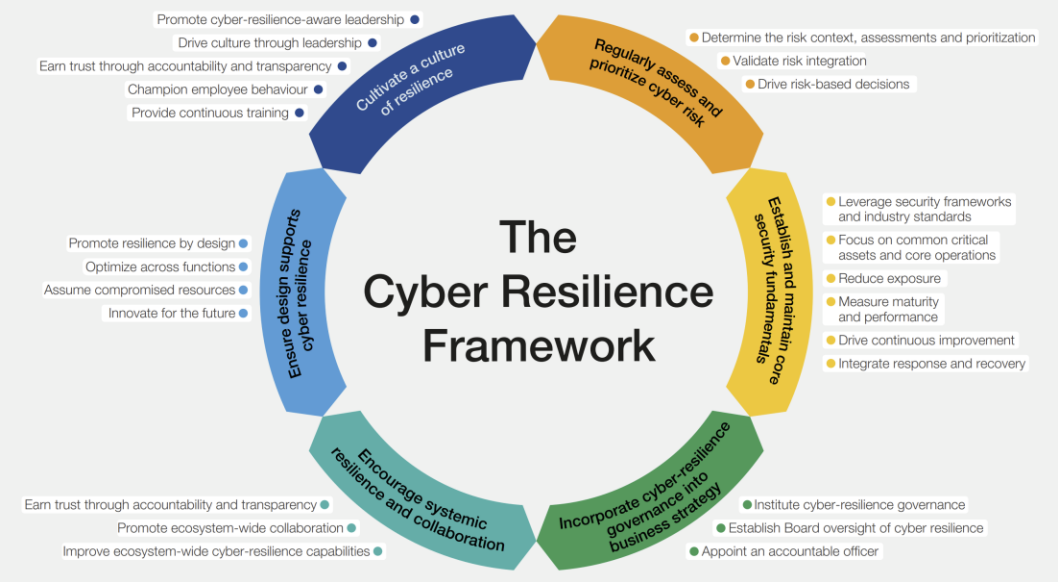
Source: [CREF Navigator (mitre.org)]

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

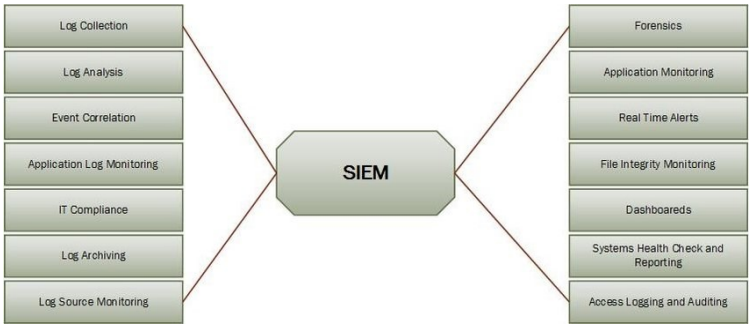
To find new triggers for analysts to review, a content engineer will check the available tools, infrastructure capabilities and current alerts. A content engineer needs to know the visibility required for incident response, but they should not be part of the incident response team to avoid bias in the 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

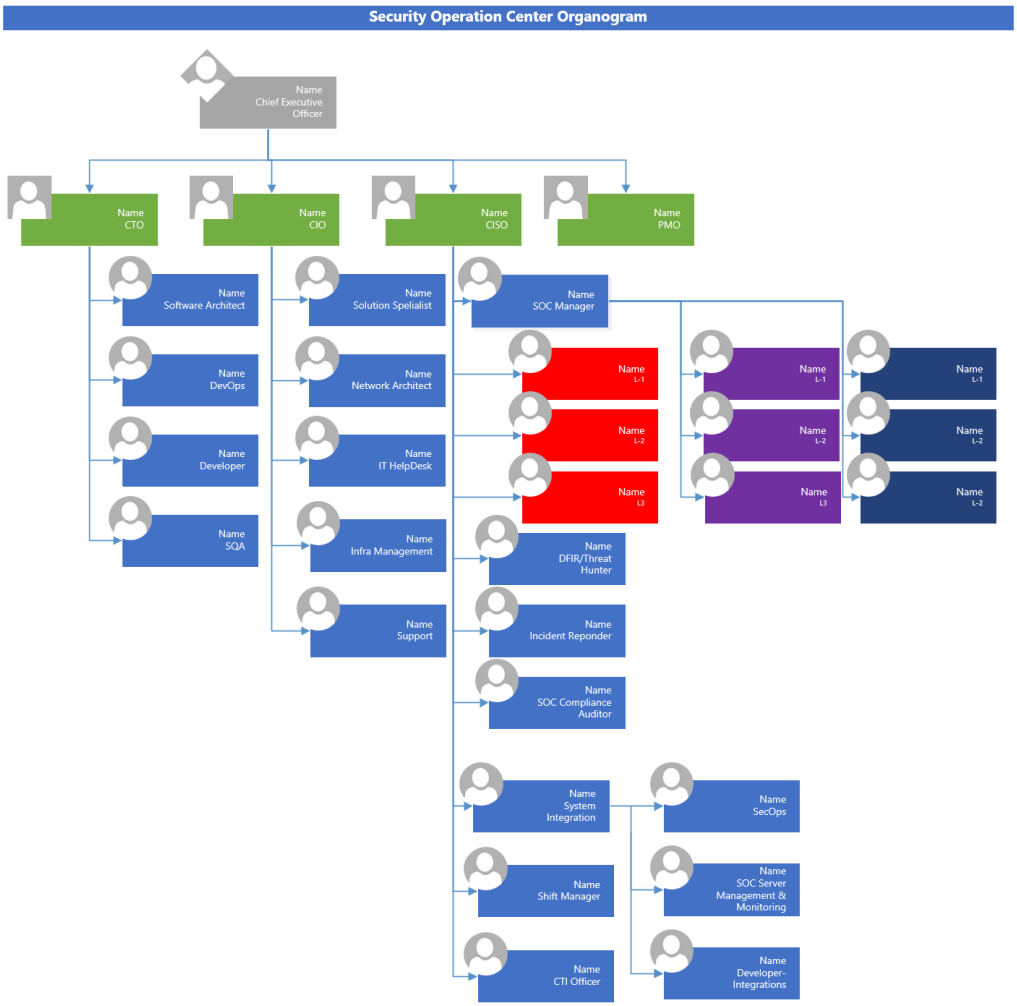
RED MUST KNOW HOW BLUE IS DETECTING RED'S EVASIVE TECHNIQUES, AND BLUE MUST KNOW HOW RED IS USING WHICH TECHNIQUE TO ATTACK! AND BLUE SHOULD HAVE ADEQUATE VISIBILITIES OVER NETWORKED DEVICES. AND THE PURPLE WILL SEE TO IT THAT EACH TEAM IS WELL EQUIPPED AND UNDERSTANDS EACH OTHER'S GOALS TO MINIMIZE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



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

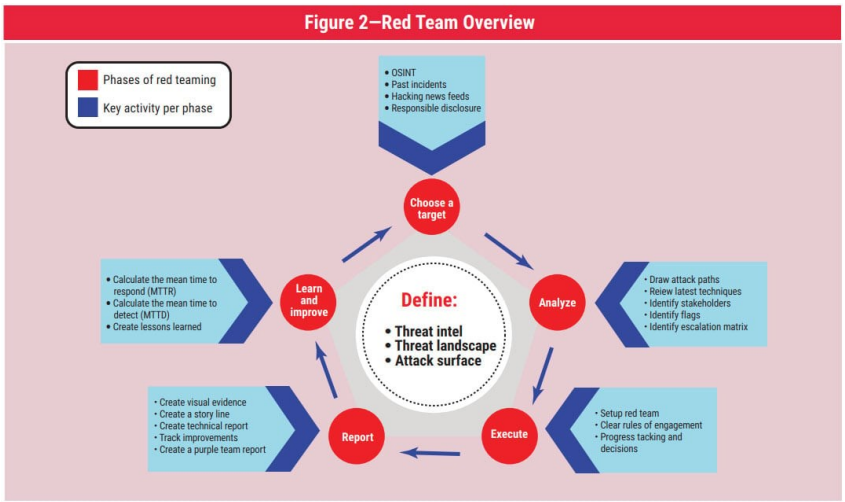
Just like any other cybersecurity framework, red teaming frameworks prescribe a set of tried and tested standard processes and procedures that should be followed by organizations. A red teaming framework has the following components:

- 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

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)

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 receipients 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

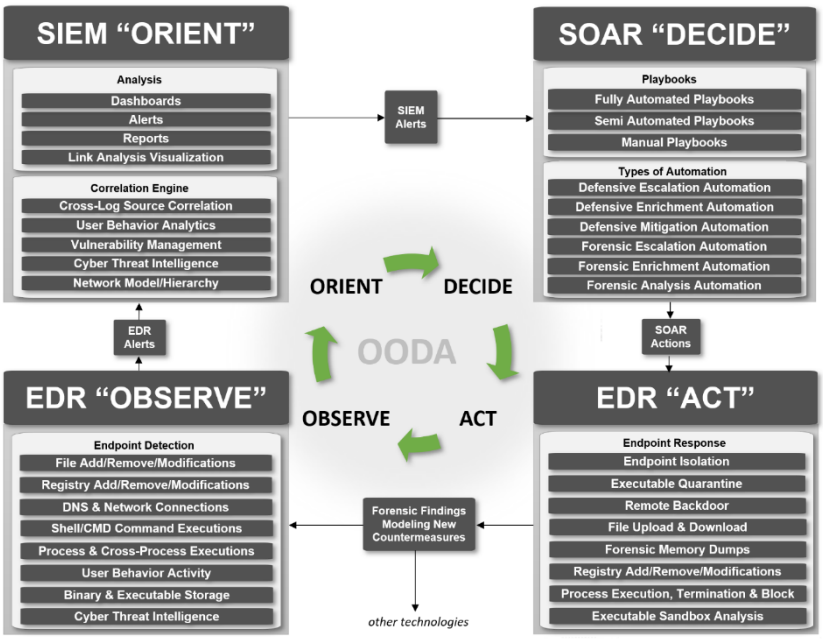
SO HOW DO YOU FIT INTO ANY OF THE SOC ROLES? HOW BEST TO OUTLINE YOUR JD/SKILLS/ACTIVITIES WHICH CAN BE MAPPED TO SOC MATRIX? SOC OPERATION RELIES ON THE EFFECTIVENESS OF YOUR ROLES AND RESPONSIBILITIES. ARCHITECTING, INTEGRATION IS NOT THE WHOLE STORY, OPERATIONALIZE THE SOC WITH YOUR SKILLS, NOT WEAPONIZING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

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.



Source: [An OODA-driven SOC Strategy using: SIEM, SOAR and EDR (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 startegy 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.

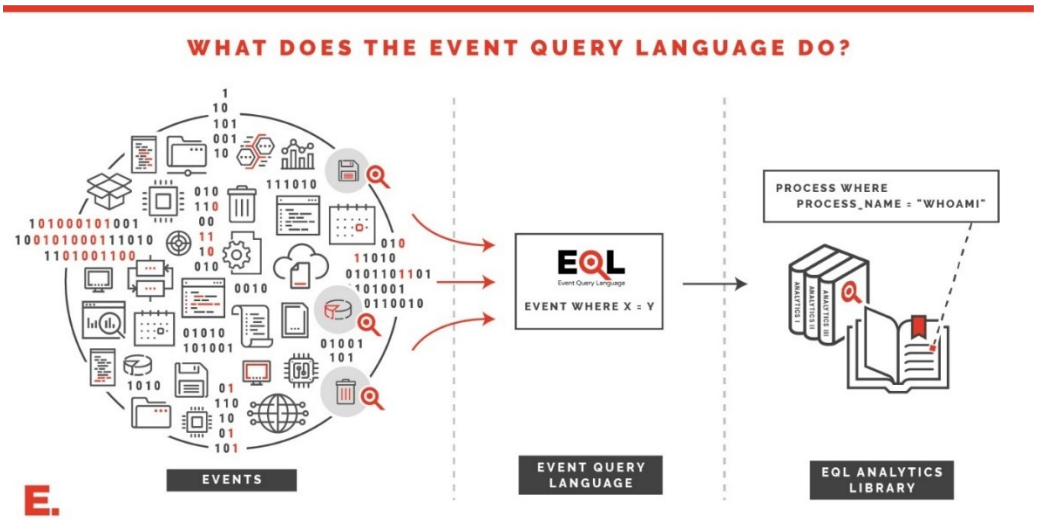
Sigma rules can be converted into a search query specific to your SIEM solution and supports various solutions:

- 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

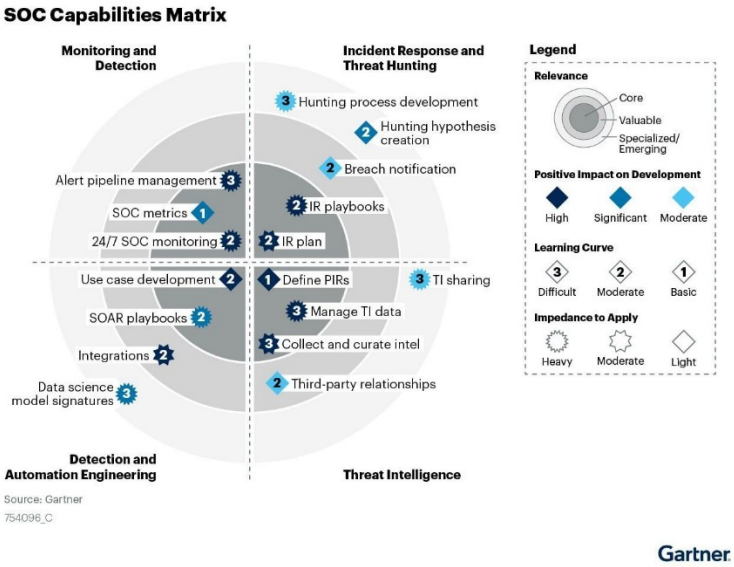
Source: A deep dive into Sigma rules and how to write your own threat detection rules - FourCore

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®.



SOC Capabilities Matrix – Gartner



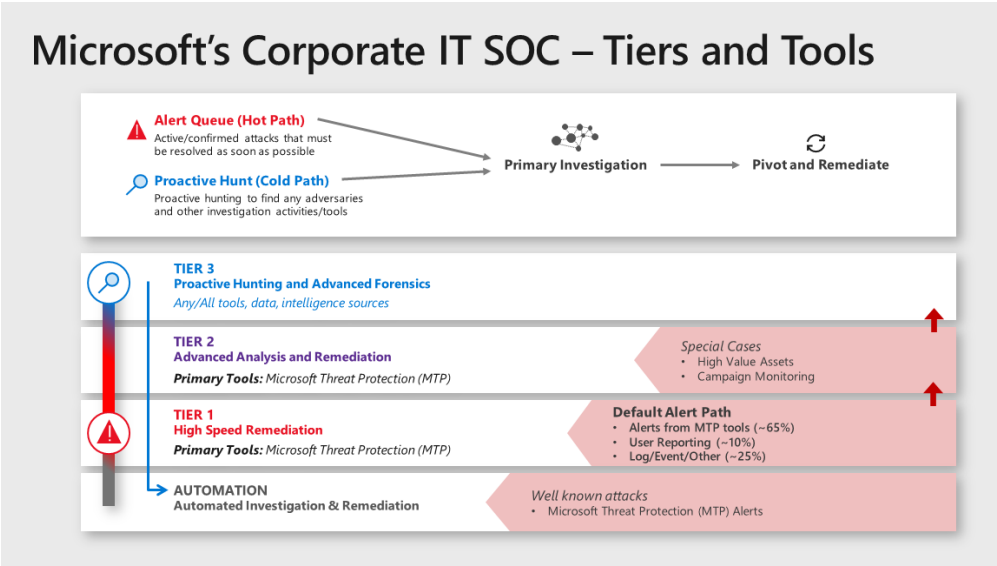
May now you can see that the garner's capability matrix is what we have addressed throughout the book. Interestingly, they have "Data Science Model" included, but not AI.

SOC Roles & Responsibilities

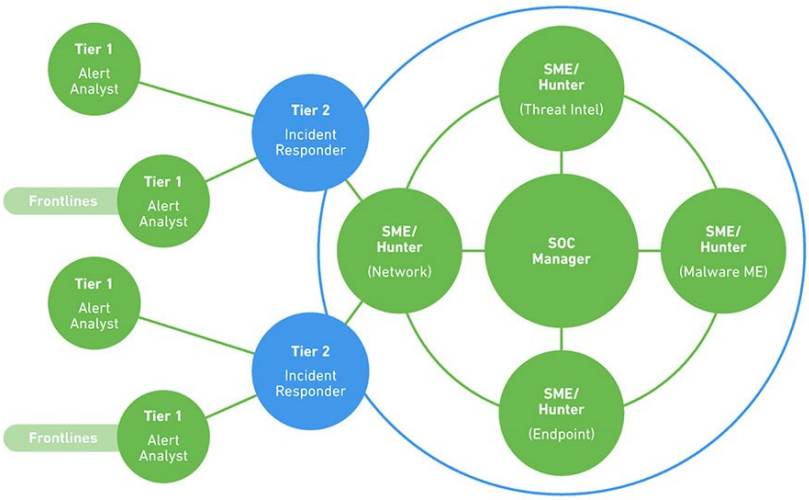
Source: Next-Gen SOC - CyRadar

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.



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



The table below explains each SOC role in more detail.

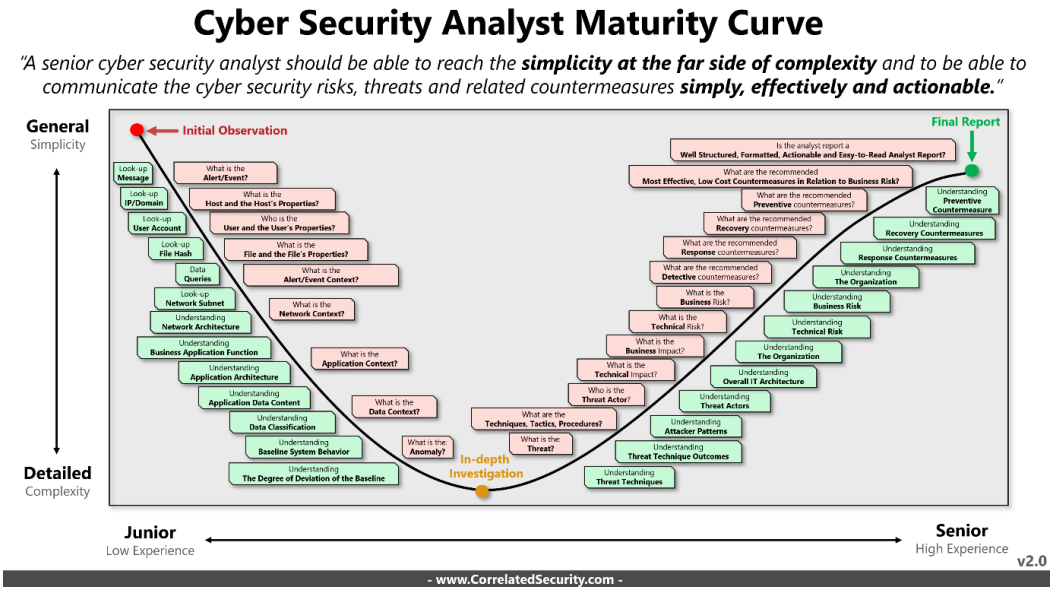
Role	Qualifications	Duties

Tier 1 Analyst **Alert Investigator**	System administration skills; web programming languages, such as Python, Ruby, PHP; scripting languages; security certifications such as CISSP or SANS SEC401	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.
Tier 2 Analyst **Incident Responder**	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.	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.
Tier 3 Analyst **Subject Matter Expert/Threat Hunter**	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.	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.
Tier 4 SOC Manager **Commander**	Similar to Tier 3 analyst, including project management skills, incident response management training, and strong communication skills.	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.
Security Engineer **Support and Infrastructure**	Degree in computer science, computer engineering or information assurance, typically combined with certifications like CISSP.	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

	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

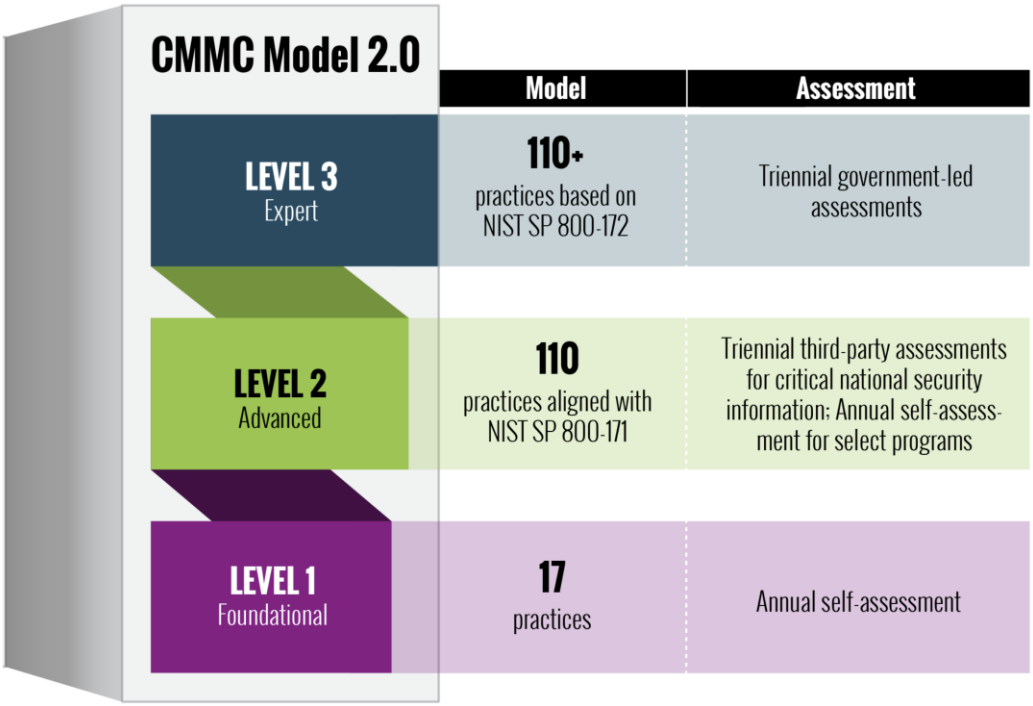
A Cyber Security Analyst Maturity Curve



Source: Cyber Security Analyst Maturity Curve (correlatedsecurity.com)

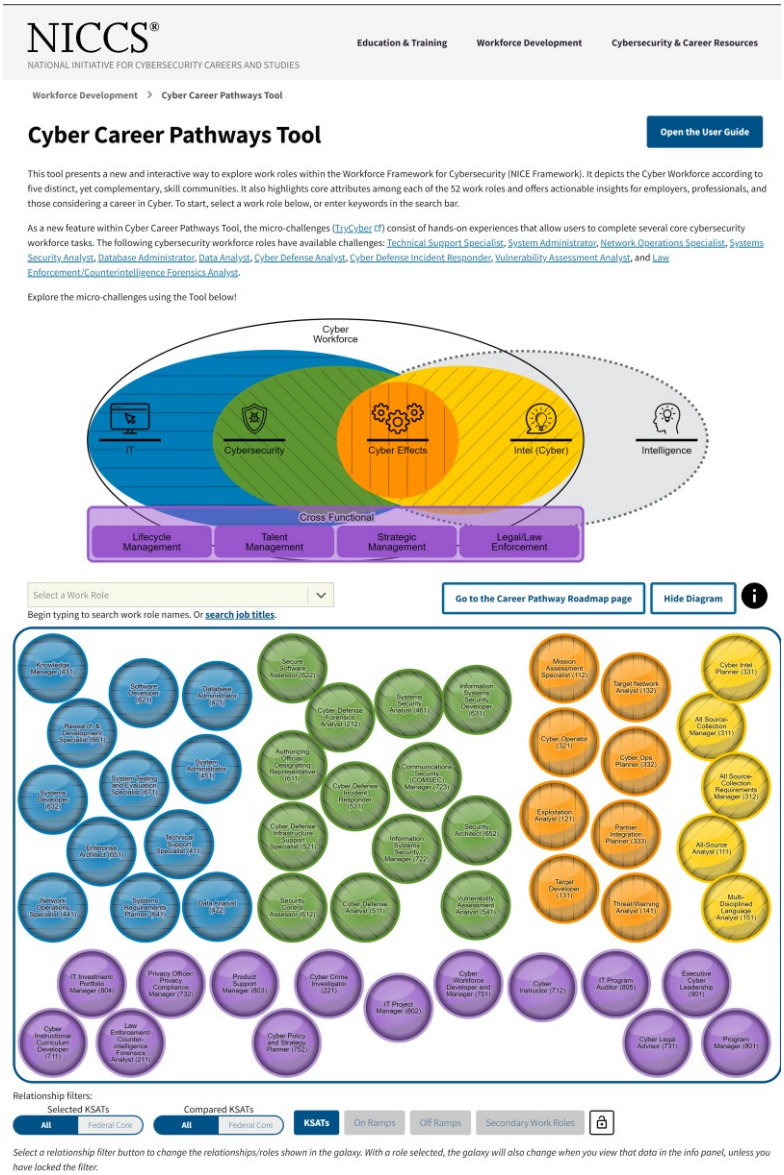
CMMC Maturity Model 2.0

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.

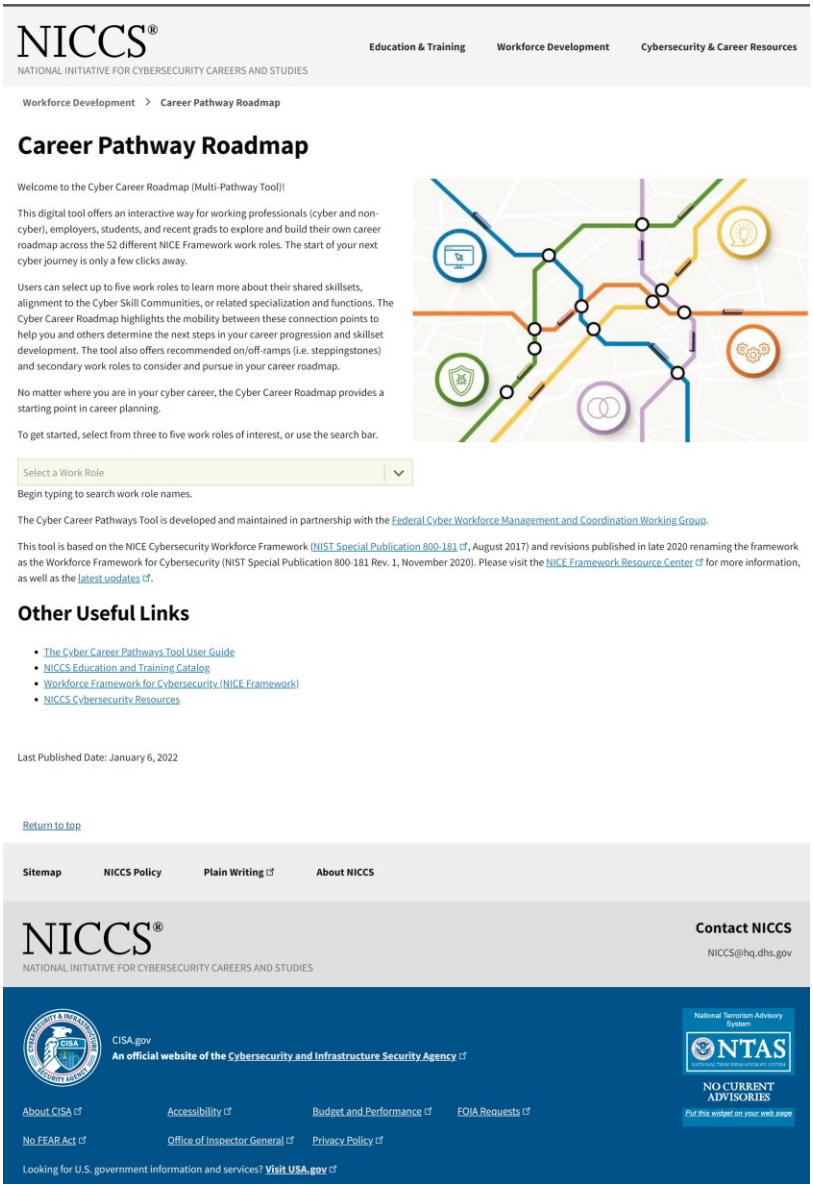


Full documentation can be downloaded from this link: [CMMC Documentation (defense.gov)]

Deriving Your Job Description or Resume



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



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, 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 for more information, as well as the latest updates.

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 | 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

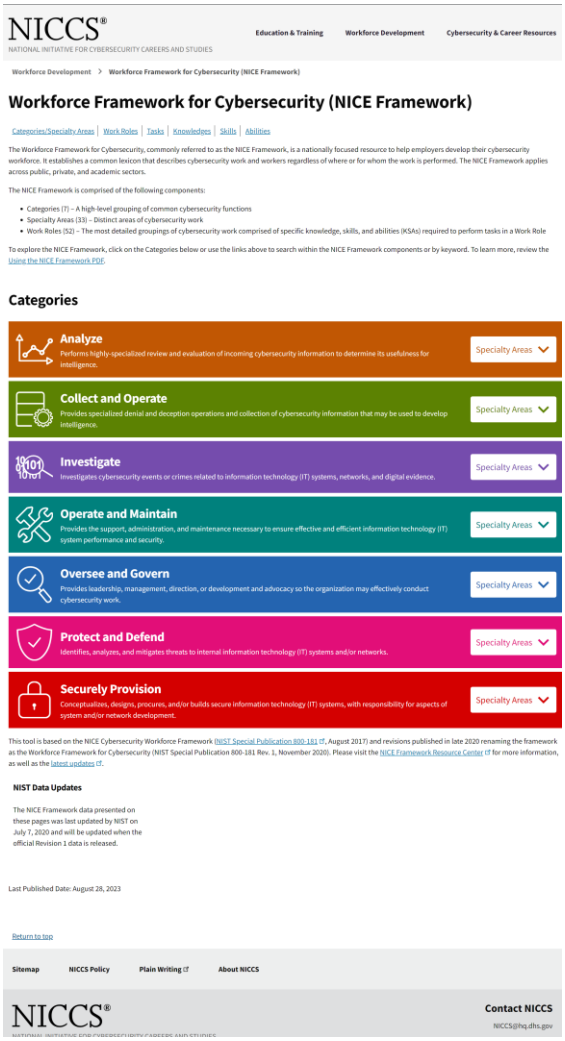
National Terrorism Advisory System
NTAS
NO CURRENT ADVISORIES
Put this widget on your web page

About CISA | Accessibility | Budget and Performance | FOIA Requests | No FEAR Act | Office of Inspector General | Privacy Policy

Looking for U.S. government information and services? Visit USA.gov

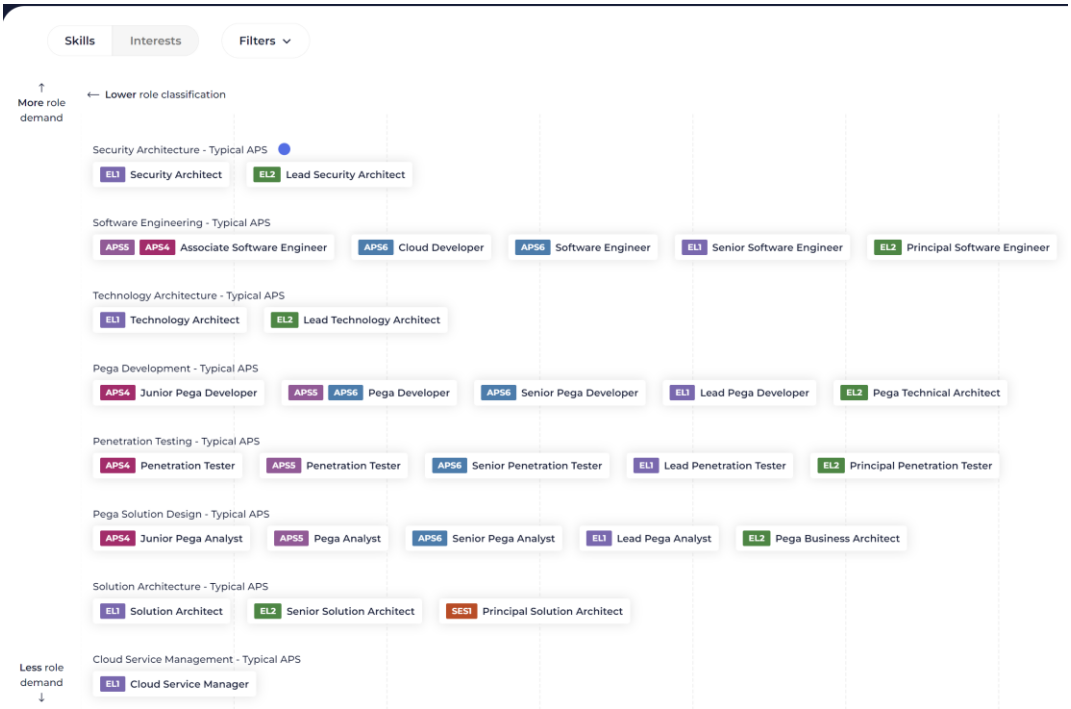
Source: [Career Pathway Roadmap | NICCS (cisa.gov)]

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]



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)]

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 SOCs. 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, obsers 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:

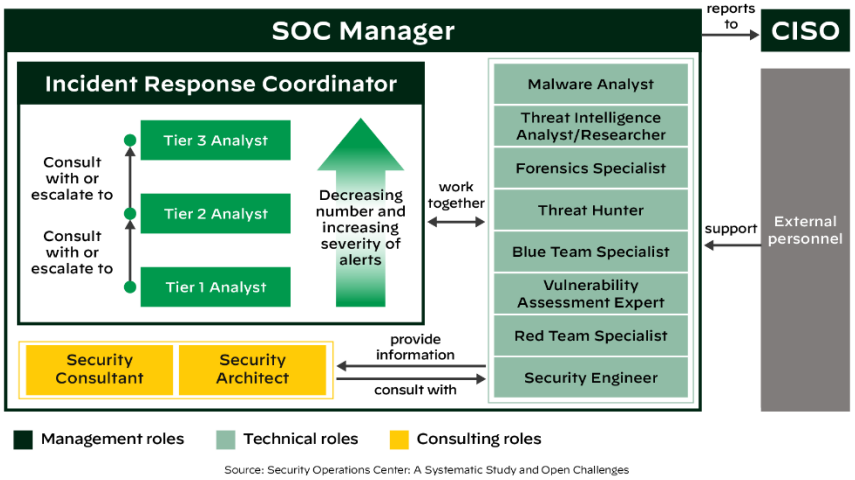
1. **Monitoring and Protecting**: SOC analysts monitor and protect the organization's assets, including personnel data, brand integrity, intellectual property, and operation systems.
2. **Triage Specialist (Tier 1 Analyst)**: Tier 1 analysts collect raw data, review alarms and alerts, confirm or adjust 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.

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.

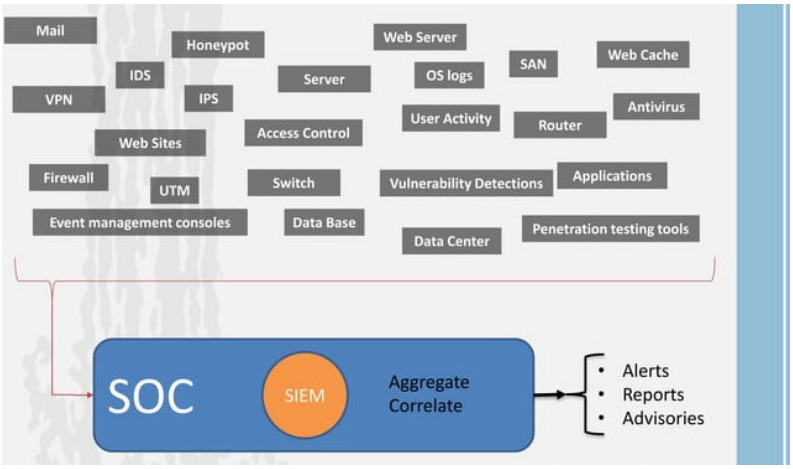
These roles and responsibilities may vary depending on the organization's size, industry, and cybersecurity maturity.



Source: [Security Operations Center (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:



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

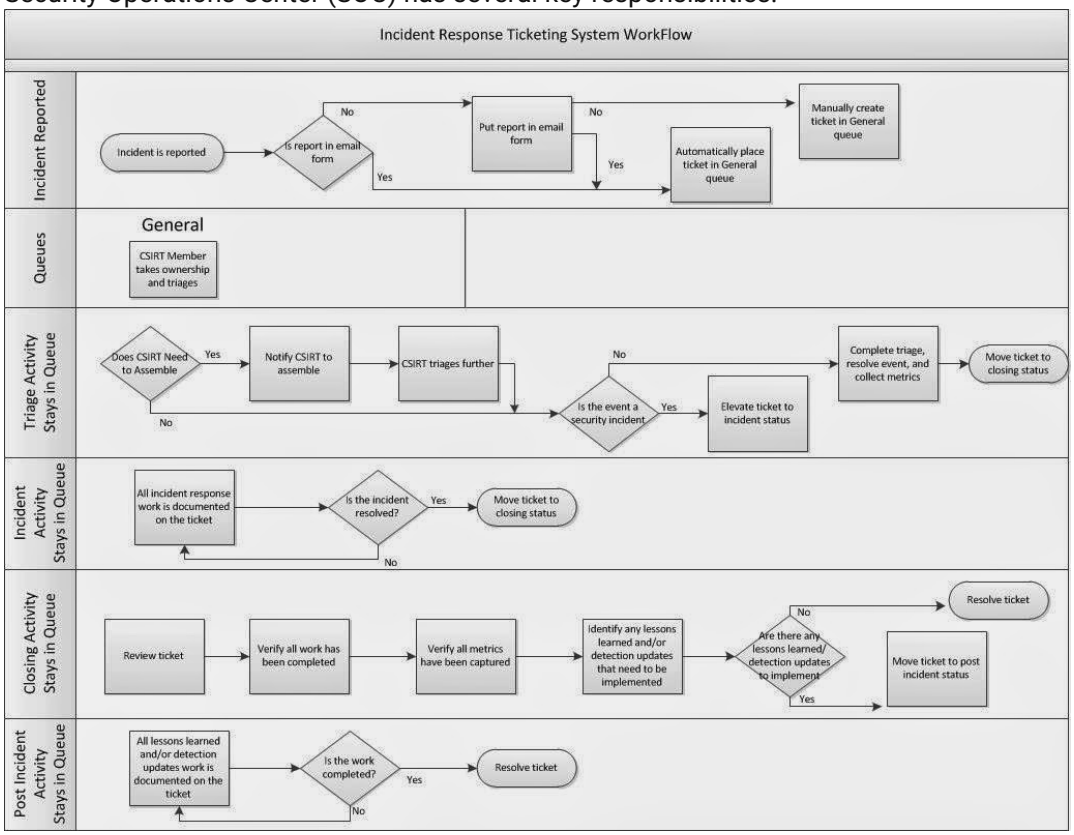
Some of the components that a SOC has visibility and alerts on

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

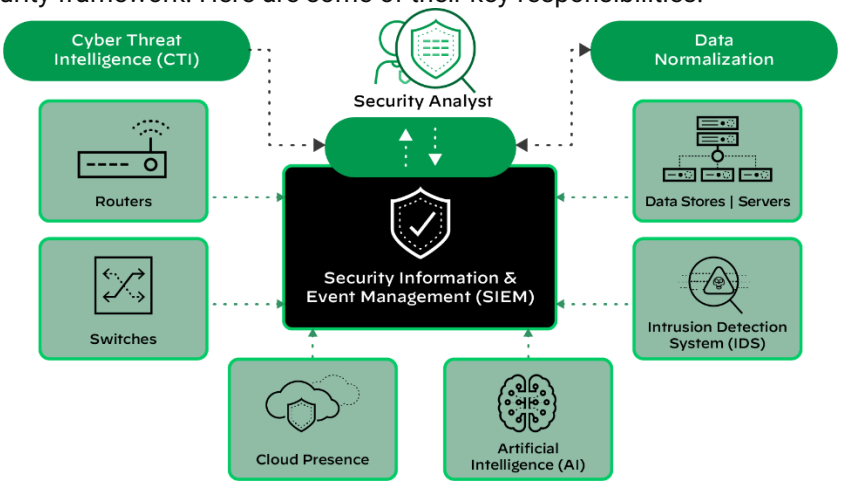
In a Security Operations Center (SOC) has several key responsibilities:

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]

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:

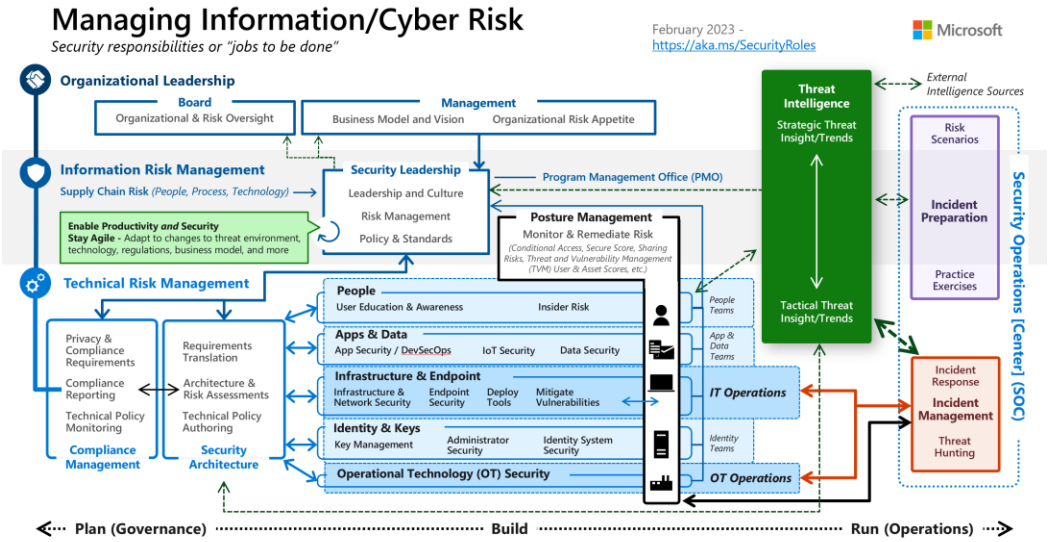
- **Team Management**: They direct SOC operations and are responsible for syncing between analysts and engineers. They oversee the SOC team, ensuring everyone is trained, motivated, and effectively working together.
- **Hiring and Training**: They are responsible for hiring new staff members and providing 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.

- **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.