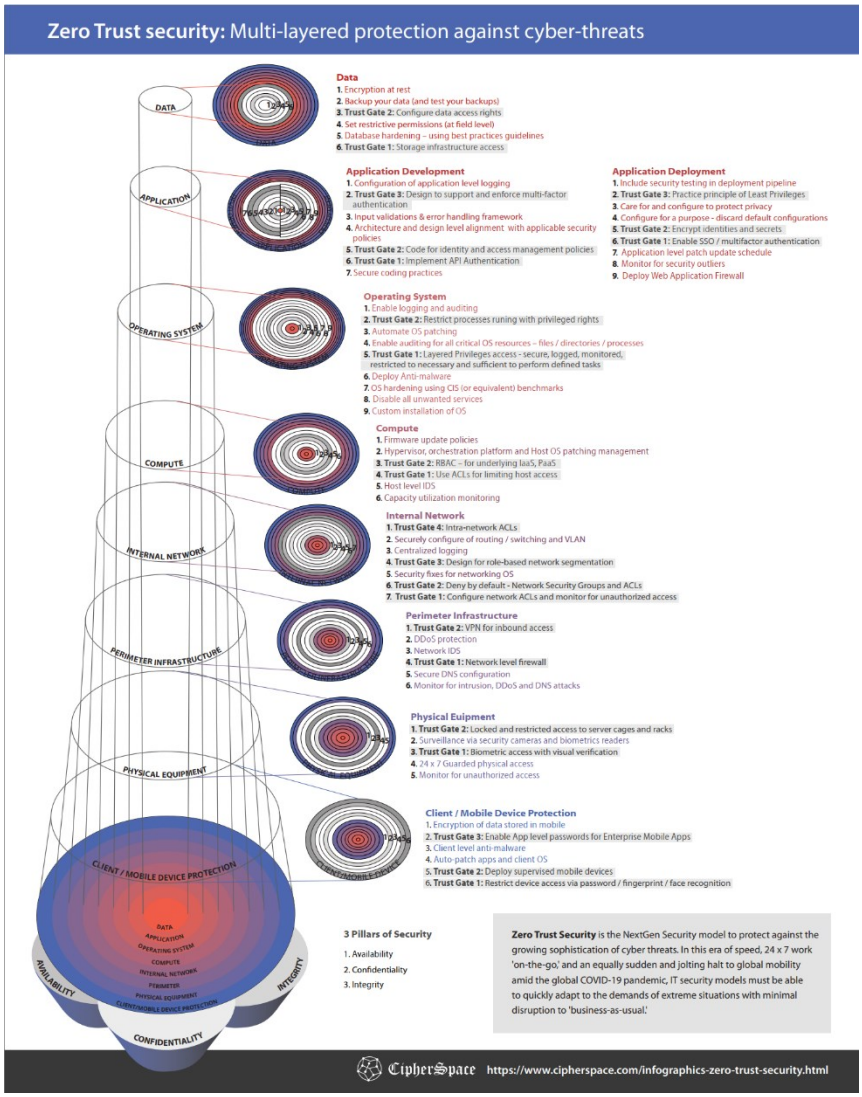
- **Meeting regulatory guidelines.** If you operate in a regulated industry, you may be subject to certain regulatory guidelines for cybersecurity. Implementing a principle of least privilege policy can support the audit process related to regulatory compliance, as it can provide audit trails of activity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



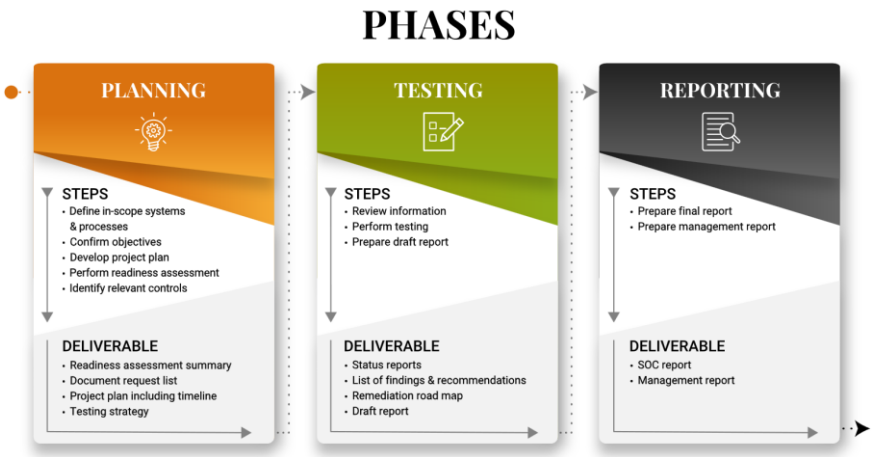
example, if your organization must comply with General Data Protection Regulation (GDPR), you may be audited to ensure compliance. With the right

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

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

Functions of a SOC Compliance Auditor in a SOC

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



Source: SOC Audit & SOC Compliance | Armanino

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

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

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

Knowledge Area (not an exhaustive list)

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

Pro-Tip

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

Your 1-Stop Point for all Benchmark Checklists from CISECURITY

Cloud Providers

- Alibaba Cloud
- Amazon Web Services
- Google Cloud Computing Platform
- Google Workspace
- IBM Cloud Foundations
- Microsoft 365
- Microsoft Azure
- Microsoft Dynamics 365 Power Platform
- Oracle Cloud Infrastructure

Desktop Software

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

- Safari Browser

DevSecOps Tools

- Software Supply Chain Security

Mobile Devices

- Apple iOS
- Google Android

Multi Function Print Devices

- Print Devices

Network Devices

- Check Point Firewall
- Cisco
- F5
- Fortinet
- Juniper
- Palo Alto Networks
- pfSense Firewall
- Sophos

Operating Systems

- IBM i
- IBM Z System
- Aliyun Linux
- AlmaLinux OS
- Amazon Linux
- Bottlerocket
- CentOS Linux
- Debian Family Linux
- Debian Linux
- Distribution Independent Linux
- Fedora Family Linux
- LXD
- Oracle Linux
- Red Hat Enterprise Linux
- Robot Operating System (ROS)
- Rocky Linux
- SUSE Linux Enterprise Server
- Ubuntu Linux
- Microsoft Intune for Windows
- Microsoft Windows Desktop
- Microsoft Windows Server
- Apple macOS
- IBM AIX
- Oracle Solaris

Server Software

- MIT Kerberos
- Microsoft SharePoint
- Apache Cassandra
- IBM Db2
- MariaDB
- Microsoft SQL Server
- MongoDB
- Oracle Database
- Oracle MySQL
- PostgreSQL
- BIND
- Docker
- Kubernetes
- VMware
- Apache HTTP Server
- Apache Tomcat
- IBM WebSphere
- Microsoft IIS
- NGINX

Source: [CIS Benchmarks (cisecurity.org)]

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

Pro-Tip

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

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

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

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

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

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

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

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

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

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

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

Malware Sandbox Tools for Analysis

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

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

Attack Flow v2.1.0 — Attack Flow v2.1.0 documentation (center-for-threat-informed-defense.github.io)

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

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

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

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

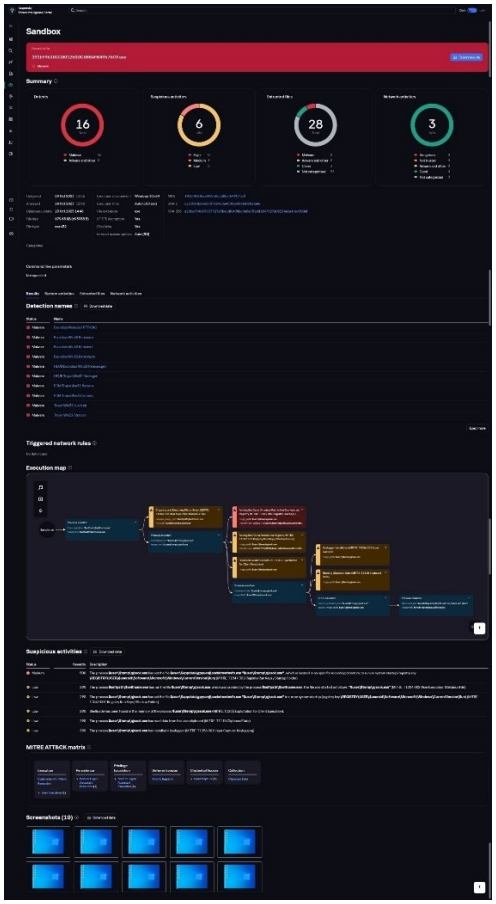
Source: Kaspersky Research Sandbox Datasheet (screenshot provided below): Advanced Automated Malware Analysis – Kaspersky Research Sandbox | Kaspersky

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

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

Pro-Tip

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



Indicators of Compromise (IoC)

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

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

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

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

Some common Indicators of Compromise (IoCs) are:

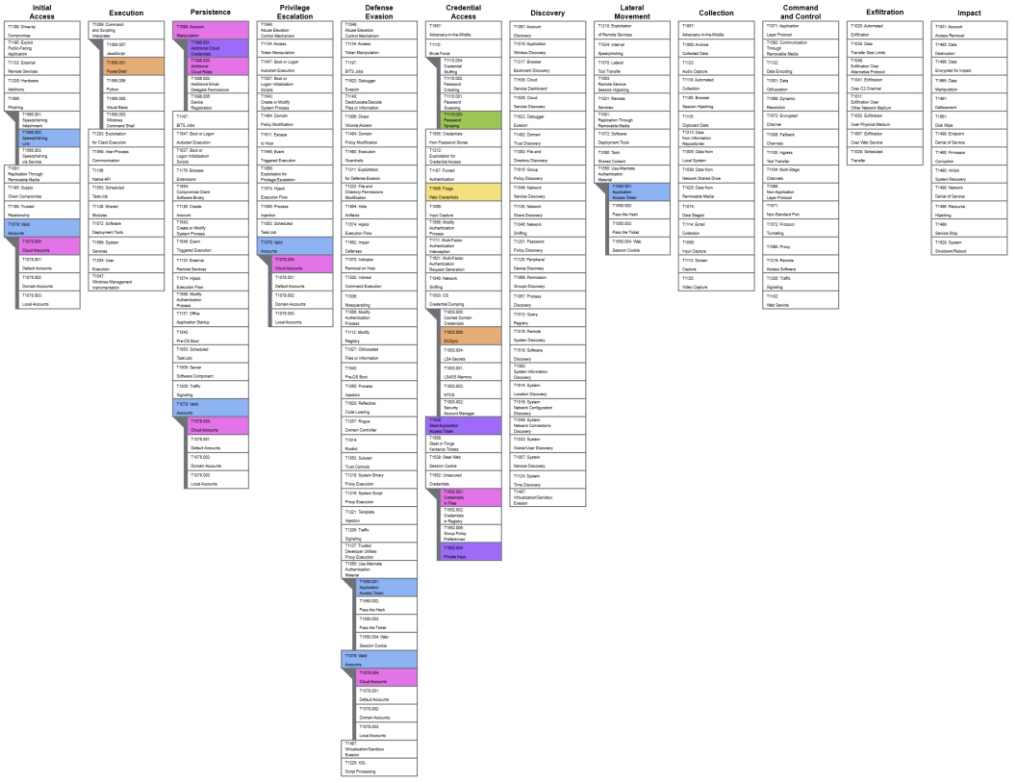
1. Unusual traffic patterns between internal systems
2. Unusual usage patterns for privileged accounts
3. Administrative access to your network from unsuspected geographical locations
4. A spike in database read volume
5. A high rate of authentication attempts and failures
6. Unusual configuration changes

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

TTP (Tactics, Techniques, Procedures)

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

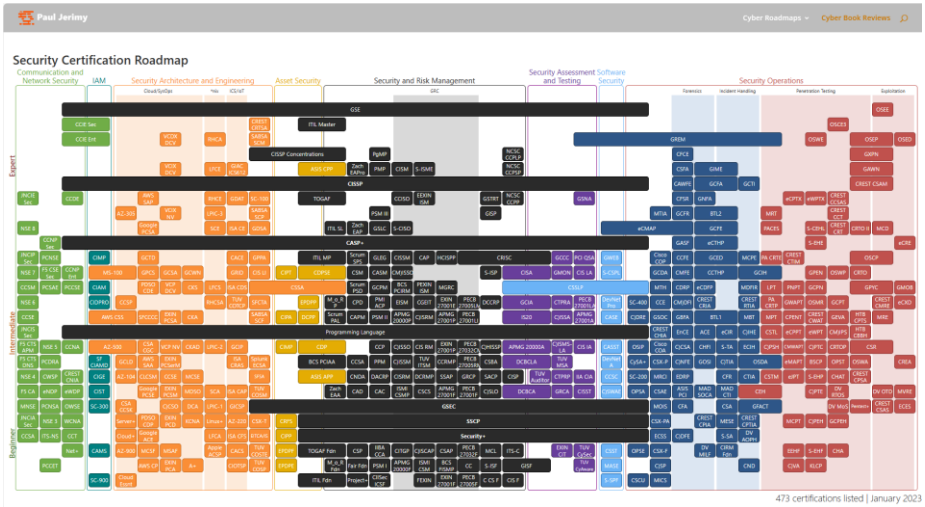
Map of Attack Scenarios to TTP (Sample)



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

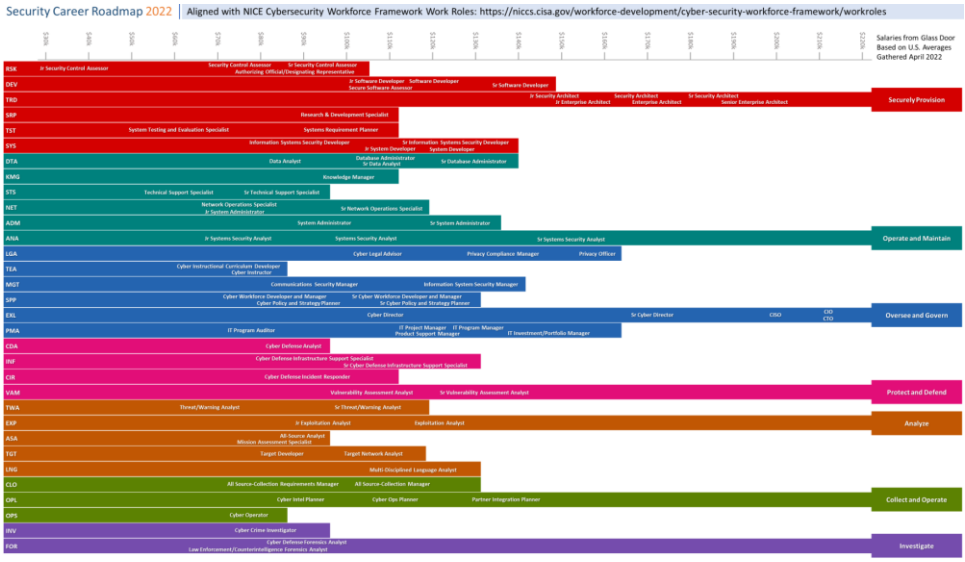
Source: [GitHub - Cloud-Architekt/AzureAD-Attack-Defense: This publication is a collection of various common attack scenarios on Azure Active Directory and how they can be mitigated or detected.]

Certification & Knowledge Mapping

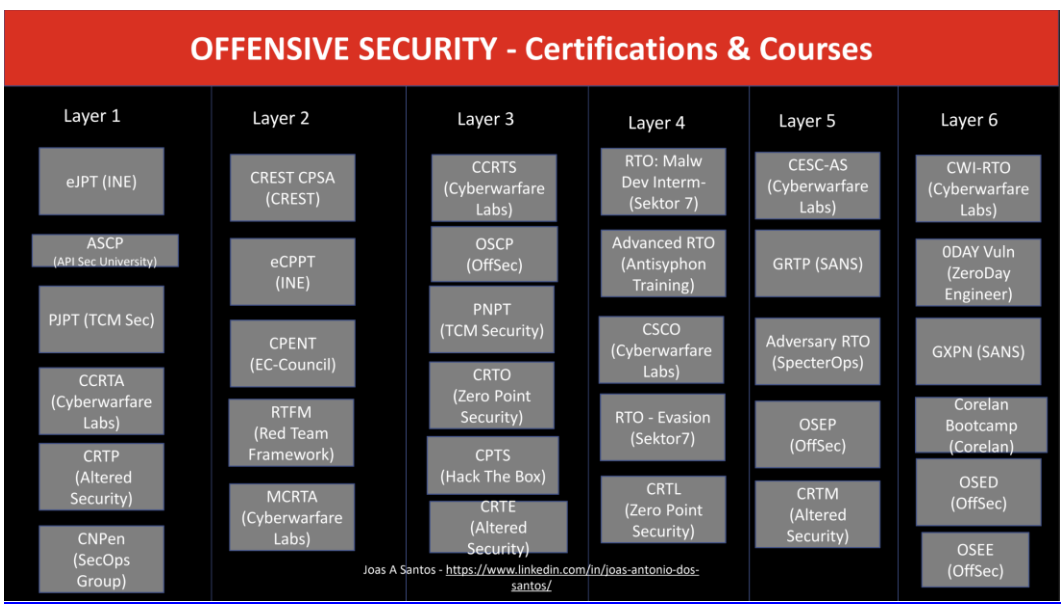


Source: [Security Certification Roadmap - Paul Jerimy Media]

Security Career Roadmap



Source: [IT Career Roadmap - Paul Jerimy Media]



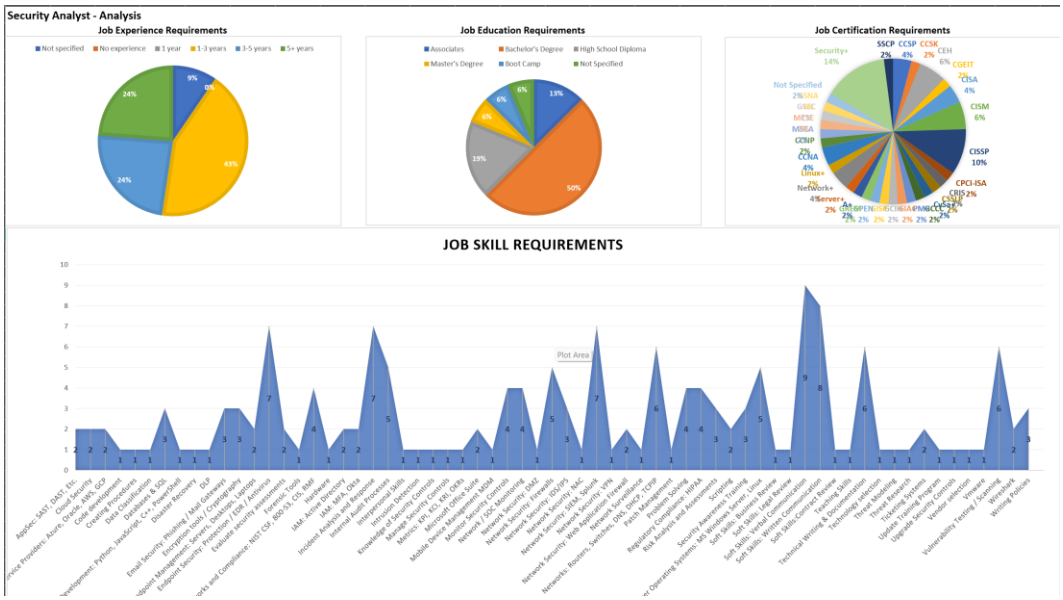
Source: [Joas A Santos - https://www.linkedin.com/in/joas-antonio-dos-santos/](https://www.linkedin.com/in/joas-antonio-dos-santos/)

A wonderful outline presented by Joas, and you can follow the provided outline to mature your skills. It's still not understood that the blue team and the red team functions as they share the same skill sets, which is always welcome in an operational perspective, and can be very useful to properly formulate and place them into your SOC hierarchy, as you see fit. But the functional achievement needs to be adhered to, and proper functional levels needs to be understood for proper delivery with actionable outcomes.

Here is another outline created by BRAD VORIS, a very professional acquaintance and a friend of professional capacity, and an identical mindset who has been working his way up towards the cause, and he has observed the skills gaps and requirements of a properly developed SOC and its importance.

He has been instrumental in what he does on a daily basis, mentoring a group of talents to reach their potential and shares his thoughts and they are made available, and lends a hand to the cause as well.

He was also a contributor to the Peerlyst forum, where some of his articles and chapters were published. Unfortunately, the site was deprecated, but their developed content is still out there serving technology folks till today.



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

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

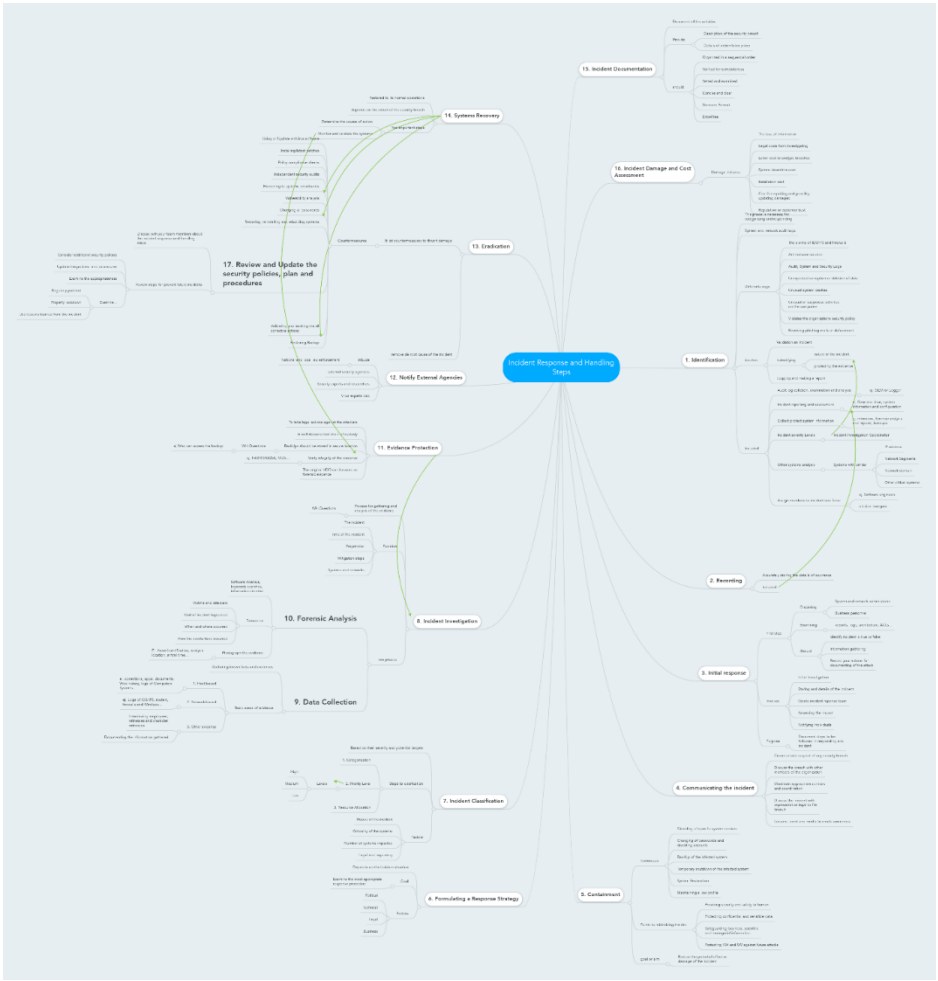
CHAPTER 10

Incident Response

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

There are different frameworks and methodologies available in the web for incident response, but they generally share some common steps:

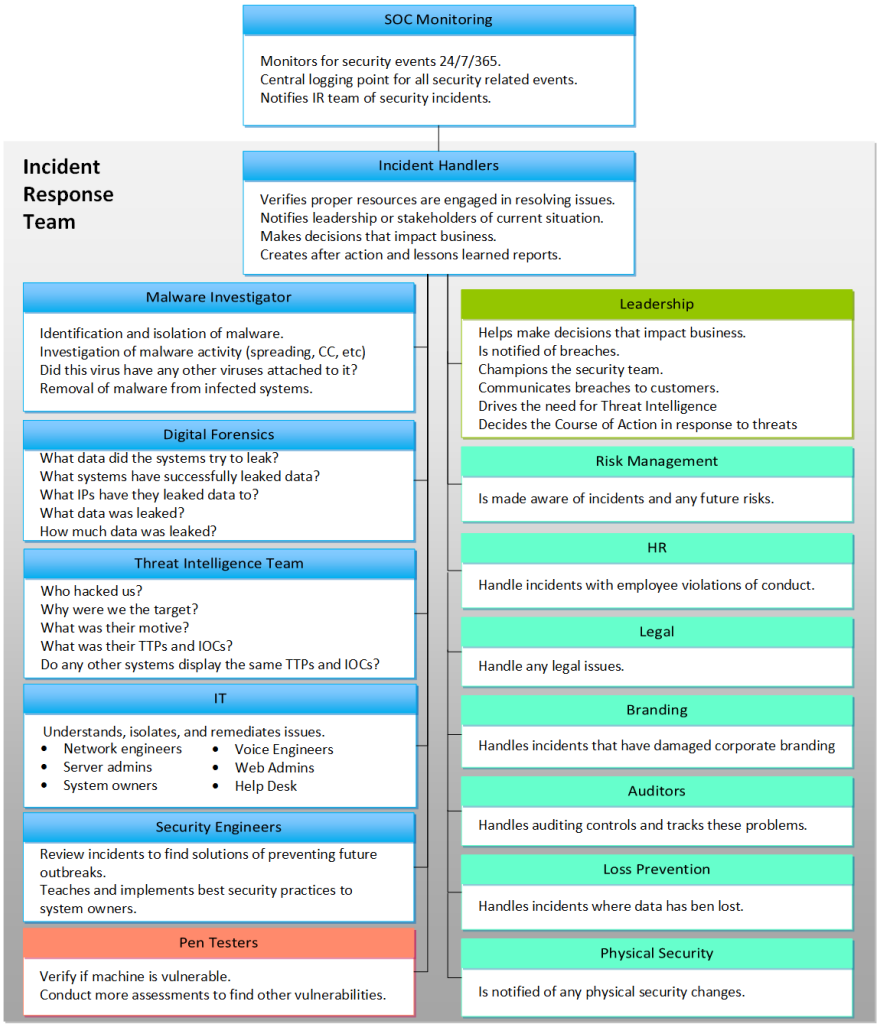
- **Preparation**: This step involves preparing the resources, tools, policies, and personnel needed to handle incidents effectively. It also includes training, awareness, and prevention measures to reduce the likelihood and impact of incidents.
- **Detection and Analysis**: This step involves identifying and verifying the occurrence, scope, and severity of an incident, as well as collecting and analyzing relevant data and evidence. It also includes reporting and escalating the incident to the appropriate stakeholders and authorities.
- **Containment, Eradication, and Recovery**: This step involves isolating and removing the threat from the affected systems and networks, as well as restoring normal operations and functionality. It also includes verifying the effectiveness of the containment and eradication measures and applying patches and updates to prevent recurrence.



Source: [Incident Response and Handling Steps - MindMeister Mind Map]

- **Post-Incident Activity**: This step involves reviewing and evaluating the incident response process and outcomes, as well as identifying and implementing lessons learned and best practices. It also includes documenting and reporting the incident details, findings, and recommendations, as well as conducting audits and follow-ups to ensure compliance and improvement.

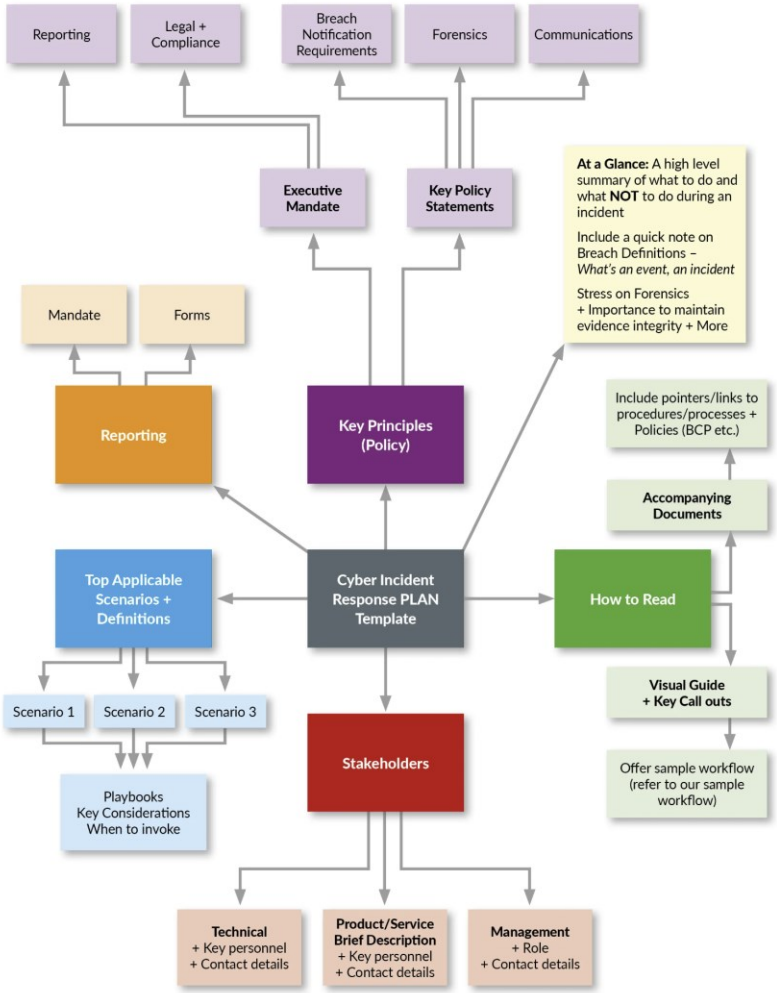
Incident Response Roles



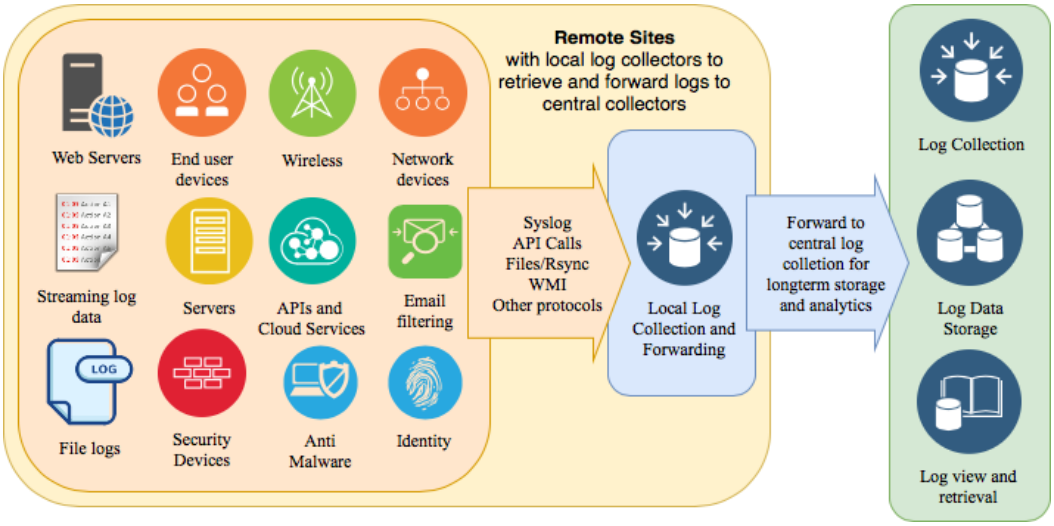
Source: [Computer incident response team roles and responsibilities (rolesresponsibility.netlify.app)]

Generic Incident Response Playbook

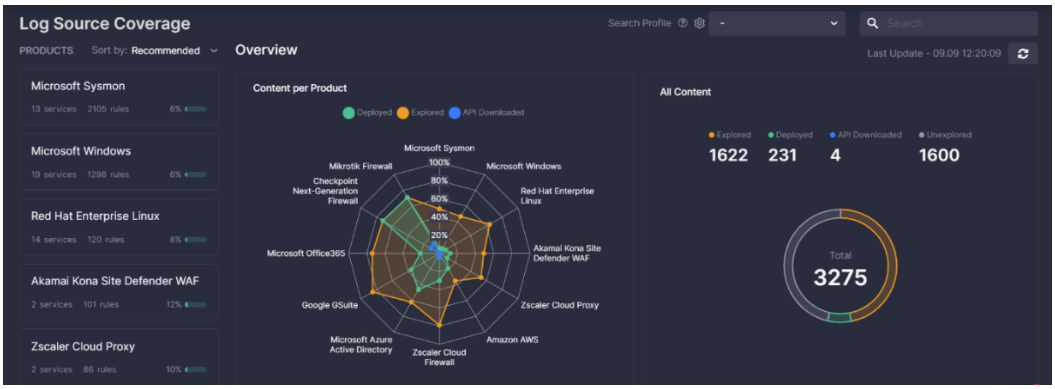
Download the freely provided and a useful template from CM-Alliance: [Cybersecurity Incident Response Plan Template and Example UK - Cyber Management Alliance (cm-alliance.com)]



Prioritizing Log Sources



Source: [Security Operations Center (SOC): Prioritizing Log Sources Rafeeq Rehman | Cyber | Automation | Digital]



Source: [SOC Prime's Innovation for Collaborative Cyber Defense - SOC Prime]

There are several factors to consider when it comes to prioritizing log sources for a Security Information and Event Management (SIEM) system. One approach is to focus on logs coming from security devices such as firewalls, IDS, content filtering and proxy servers, identity management systems, proxies, VPN concentrators, end-point detection and response systems, etc. Another approach is to evaluate the relevance of each log source to your organization's security goals. Focus on log sources that provide

information about potential threats or vulnerabilities that align with your security goals. Consider legal and compliance requirements specific to your industry. For organizations with compliance requirements, compliance frameworks offer a good starting point. It is also important to consider the potential impact and severity of each log source. By prioritizing log sources based on their relevance and potential impact, organizations can allocate resources effectively and focus on the most important security risks.

Windows Event Logs Artifact

The artifact contains Event Logs in Windows operating systems. The details you can view include:

1. **Level** - Event log level/type. This can be information, warning, error, success/failure audit.
2. **Channel** - Event log channel or category. Security, Application, System etc.
3. **Computer** - Local system name.
4. **Event ID** - Event identification number. By filtering according to ID we can get the important events.
5. **Keywords** - They are used to group the event with other similar events based on the usage of the events.
6. **Opcode** - The activity or a point within an activity that the application was performing when it raised the event.
7. **Provider GUID** - The unique GUID for the provider. It is useful when performing research or operations on a specific provider.
8. **Provider Name** - Name of event provider.
9. **Security User ID** - It is used to uniquely identify a security principal or security group.
10. **Task** - Identifies the type of recorded event log. Application developers can define custom task categories for providing additional details.
11. **Event Record Order** - Order of the event in the main event category.
12. **Located At** - File offset location of the specific event.
13. **Event Record ID** - Event record identification number in the main category.
14. **XML** - XML view of the event,
15. **Record Length** - Length of the event.

Windows Reports – What to look for?

As a security-conscious administrator, you want to keep an eye on a number of events such as:

1. Successful or failed login attempts to the Windows network, domain controller or member servers.
2. Successful or failed attempts of remote desktop sessions.
3. Password lockouts after repeated login attempts.
4. Successful or failed login attempts outside business hours.
5. Adding, deleting, or modifying local or domain user accounts or groups.
6. Adding users to privileged local or active directory groups.
7. Clearing event logs in domain controllers or member servers.
8. Changing local audit policies and group policies.
9. Changing or disabling Windows firewall or firewall rules.
10. Adding new services, stopping or deleting existing services.
11. Changing registry settings.
12. Changing critical files or directories.

Common Windows Log Events Used in Security Investigations

Here are a few common event codes on Windows 7/Vista/8/10 and Windows Server 2008/2012R2/2016/2019 (previous versions of Windows have different codes), commonly used in security investigations:

Event ID	What it means
4624	Successful log on
4625	Failed log on
4634	Account log off
4648	Log on attempt with explicit credentials
4719	System audit policy change
4964	Special group assigned to new log on attempt
1102	Audit log cleared
4720	New user account created
4722	User account enabled
4723	Attempt to change password
4725	User account disabled
4728	User added to privileged global group
4732	User added to privileged local group
4756	User was added to privileged universal group
4738	Change to user account
4740	User locked out of an account
4767	User account unlocked
4735	Change to privileged local group
4737	Change to privileged global group
4755	Change to universal group

4772	Failed request for Kerberos ticket
4777	Domain controller failed to validate credentials
4782	Account password hash accessed
4616	System time changed
4657	Change to registry value
4697	Service install attempt
4946	Rule added to Windows Firewall exception
4947	Rule modified in Windows Firewall exception
4950	Windows Firewall settings change
4954	Change to Windows Firewall Group Policy
5025	Windows Firewall service stopped
5031	Application blocked by Windows Firewall from accepting traffic
5155	Windows Filtering Platform blocked a service from listening on a port

Source: Event Log: Leveraging Events and Endpoint Logs for Security (exabeam.com)

Furthermore, the following table contents also will be helpful for SOC feed for Network Traffic Analysis:

Log Item - What it is - Why it's Important		
Source IP Address	Where the traffic originates.	Tracking the source of attacks or suspicious activities.
Destination IP Address	Target of the traffic.	Determining potential internal targets and external threat sources.

Source Port	Port on the source IP initiating the connection.	Identifying specific applications or services being used.
Destination Port	Port being accessed on the destination IP.	Detecting unusual access patterns or services being targeted.
Timestamps	Exact time of events.	Correlating events across different systems for incident response.
Protocol (TCP/UDP/ICMP, etc.)	Communication protocol used.	Understanding the nature and purpose of the traffic.
Packet Size	Size of packets.	Indicating malicious activities through large or unusually sized packets.
TCP Flags (SYN, ACK, FIN, etc.)	State of TCP connections.	Identifying different stages of network communication and potential scanning activities.
DNS Queries and Responses	Domain name resolutions.	Detecting malicious domain communications.
HTTP Methods (GET, POST, etc.)	Types of HTTP requests.	Monitoring web applications and identifying potential web-based attacks.
URLs Accessed	The URLs requested.	Identifying access to malicious or

		inappropriate websites.
HTTP Status Codes (200, 404, 503, etc.)	Response status.	Spotting errors, server issues, or high rates of specific responses.
SSL/TLS Handshakes	Encrypted communication initiation.	Ensuring secure communications and detecting anomalies.
VPN Logins and Logouts	VPN access monitoring.	Ensuring only authorized remote access.
Email Logs (Sender, Receiver, Subject)	Email traffic monitoring.	Detecting phishing attempts and email based threats.
File Transfers (FTP/SFTP)	Tracking file uploads and downloads.	Preventing data loss and spotting unauthorized transfers.
Authentication Logs (Success/Failure)	Records login attempts.	Detecting brute-force attacks and unauthorized access.
IDS/IPS Alerts	Intrusion detection/prevention alerts.	Early detection of potential threats and intrusions.
Bandwidth Usage	Amount of data transferred.	Signaling data exfiltration or denial-of service attacks.
NetFlow Data	Information about network traffic flow.	Network behavior analysis and anomaly detection.

Firewall Allow/Deny Logs	Allowed and blocked traffic records.	Security policy enforcement and detecting breaches.
DHCP Leases	IP address assignments.	Tracking devices and identifying rogue devices.
ARP Traffic	Address Resolution Protocol traffic.	Detecting ARP poisoning and MitM attacks.
Geolocation of IP Addresses	Geographical location of IP addresses.	Identifying traffic from unusual or high-risk locations.
Wi-Fi Connection Logs	Wireless network	Securing wireless networks and detecting
	connections tracking.	unauthorized access.
ARP Requests and Responses	Monitors ARP protocol traffic.	Mapping network addresses and detecting spoofing.
SNMP Traps	Alerts from network devices.	Identifying events or issues on network devices.
SMTP Traffic	Monitors Simple Mail Transfer Protocol activities.	Tracking email delivery and detecting spam or malicious emails.
ICMP Traffic	Monitors Internet Control Message Protocol.	Error message analysis and operational network information.
SIP Traffic	Monitors Session Initiation Protocol in VoIP.	Managing VoIP communications and identifying potential abuses.
NTP Traffic	Monitors Network Time Protocol.	Ensuring time synchronization and detecting man-in-the-middle attacks.

DHCP Discover/Offer/Request/Acknowledge	Monitors the DHCP process.	Tracking IP address allocation and identifying rogue DHCP servers.
LDAP Queries	Monitors Lightweight Directory Access Protocol.	Accessing directory services and detecting unauthorized queries.
SQL Queries	Monitors Structured Query Language traffic.	Database interaction monitoring and detecting SQL injection attacks.
RADIUS Authentication Logs	Monitors RADIUS protocol.	Authentication and authorization process tracking.
Kerberos Authentication Attempts	Monitors Kerberos protocol.	Network authentication security analysis.
Syslog Messages	Collects and analyzes system logs.	Gathering crucial information from various network devices.
SSL Certificate Information	Monitors SSL certificates in communications.	Ensuring secure communications and detecting certificate issues.
IPv6 Traffic	Monitors IPv6 protocol traffic.	Future-proofing network monitoring as IPv6 adoption increases.
Traceroute Information	Monitors packet paths through a network.	Network path analysis and troubleshooting.
Wireshark Captures	Analyzes detailed packet captures.	In-depth network analysis and issue identification.
DDoS Attack Indicators	Monitors for signs of DDoS attacks.	Early detection and mitigation of DDoS attacks.

Tor Traffic	Monitors Tor network usage.	Detecting anonymous communication potentially used for malicious activities.
Malware Callbacks	Monitors for compromised system communications.	Identifying systems communicating with command and control servers.
Zero-Day Attack Indicators	Monitors for unknown attack patterns.	Detecting new, potentially unpatched vulnerabilities.
Mobile Device Management (MDM) Logs	Monitors mobile device activities.	Managing and securing mobile device usage within the network.
Cloud Service Access Logs	Monitors access to cloud based services.	Securing cloud services and detecting unauthorized access.
VPN Tunnel Status	Monitors the status of VPN tunnels.	Ensuring the health and security of VPN connections.
VoIP Call Logs	Monitors Voice over IP call details.	Tracking VoIP communications for abuse or data leakage.
Data Leakage Indicators	Monitors for unauthorized data transmission.	Preventing sensitive data from leaving the network.

Source: LinkedIn Shares – Credit- Writer's name was not found

Windows Events: Valuable, but Expensive

These are Windows event codes that can be prohibitively expensive to log, as they can generate hundreds of events in a short period of time. However they provide a great level of insight into an environment, so if disk space – or log ingestion into a SIEM – allows for these to be collected, I encourage them to be logged.

Event Code	Description	Why?
4657	A registry value was changed	A loud event code, this is still very valuable to detect suspicious registry value changes, as another common foothold for persistence is for attackers to alter or add a registry key. There

		are some key areas in the Windows registry that these footholds would be placed to be most effective – startup registry keys "run" and "run once" – so you can narrow your scope to just these registry paths if needed. See section below, "4657 Registry Keys to Monitor"
4688	New process was created	This will allow you to see any and all new processes that are run in the environment. If that sounds incredibly noisy, it is – however it provides an amazing insight into an endpoint. Additionally you can enable it to include process command line arguments, which allows for endpoint visibility not usually seen without a paid-for tool. If your disk space – or license if ingesting into a SIEM platform – allows for this event code with command line to be ingested, I do suggest it, however it is extremely loud.
4697	An attempt was made to install a service	This event code would be very loud to monitor across all areas, so we want to ensure it's monitored on critical or otherwise sensitive systems. Service installations should be planned and there are services that attackers would want to install on a high value system. The service type field should be monitored to determine the access level of this new service, while the service start type field should be monitored for how the service is set to run.

Registry Keys to Monitor

Below are some very solid registry keys to monitor, all of which cover the persistence methods discussed above. Rather than log all registry changes, instead focus on these locations to best detect suspicious registry behavior. Credit goes to MITRE ATT&CK for these paths below – https://attack.mitre.org/techniques/T1547/001/

Run at startup keys:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

Startup folder items:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders

Automatic service startups:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices

Policy-driven startup programs:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

User Logon Program Launch – within “load” value:

- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows

Autocheck launch – within BootExecute value

- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager
    - This last one is interesting as it’s the path of the automatic disk checking service Microsoft employs upon abnormal shutdowns. Since it’s an automatic function, attackers realized they can adjust this value to also add that same automatic run functionality to their program/process for persistence. It’s pretty cool!

Source: Windows Security Event Logs – What to Monitor? - Critical Start

Which Are The Most Critical Linux Logs to Monitor?

- /var/log/syslog or /var/log/messages — stores all activity data across the Linux system.
- /var/log/auth.log or /var/log/secure — stores authentication logs
- /var/log/boot.log — messages logged during startup
- /var/log/maillog or var/log/mail.log — events related to email servers
- /var/log/kern — Kernel logs
- /var/log/dmesg — device driver logs
- /var/log/faillog — failed login attempts
- /var/log/cron — events related to cron jobs or the cron daemon
- /var/log/yum.log — events related to installation of yum packages
- /var/log/httpd/ — HTTP errors and access logs containing all HTTP requests
- /var/log/mysqld.log or /var/log/mysql.log — MySQL log files

Using Linux Event Logs for Security

The Linux operating system stores a timeline of events related to the server, kernel, and running applications. The main log categories are:

- Application logs
- Event logs
- Service logs
- System logs

There are several ways to view logs in Linux:

- Access the directory `cd/var/log`. Specific log types are stored in subfolders under the log folder, for example, `var/log/syslog`.
- Use the `dmseg` command to browse through all system logs
- Use the `tail` command, which displays the last lines written to a certain log file, where problems are usually found. For example `tail -f /var/log/syslog` prints the next line written to the file, letting you follow changes to the syslog file as they happen.

Following are commonly used Linux log files:

- **/var/log/syslog or /var/log/messages** – general system activity logs. Used to detect problems that may occur during startup or to isolate application service errors. RedHat-based systems store information in the messages folder while Debian-based systems store them in the syslog folder.
- **/var/log/auth.log or /var/log/secure** – all authentication and authorization logs. Used to investigate failed login attempts. RedHat-based systems store these in the auth.log folder while Debian-based systems store them in the secure folder.
- **/var/log/kern.log** – kernel activity logs, including custom kernels.
- **/var/log/faillog** – failed login attempts.
- **/var/log/maillog or var/log/mail.log** – logs related to mail servers. Used to track issues like emails tagged as spam, and suspicious use of postfix or smtpd.

Common Log Sources for Cloud Services

Cloud Threat Hunting

Elli Shlomo

Scenario	M365	Azure	AWS	GCP	GWS
Cloud ENUM	UAL	Activity Logs	CloudTrail	System Event Logs	Service Logs
Password Spray	UAL	Sign-in Logs	CloudTrail	Login Audit Logs	User Log Events
Storage Canaries	UAL	Storage Logs	CloudTrail	Storage Logs	Drive Log Events
Lateral Movement	UAL	Activity Logs	CloudTrail	System Event Logs	User Log Events
Exposed Keys	UAL	Activity Logs	CloudTrail	System Event Logs	OAuth Log Events

Determine the Best Log Data Sources

Below picture lists some common data sources in a suggested order of priority, starting with identity and access management (IAM) logs and primary security controls, and then the other categories as your program matures:

Order	Data Source	Logs to Collect/Monitor
Tackle first	IAM	• Single sign-on (SSO) • Multifactor authentication (MFA) • Host-based collection (e.g., Windows servers)
	Security controls	• IDS • Endpoint security (anti-virus, anti-malware, etc.) • Data loss prevention (DLP) • Virtual private network (VPN) concentrators • Web filters • Honeypots • Firewalls
Tackle second	Network infrastructure	• Routers • Switches • Domain controllers • Wireless access points • Application servers • Databases • Intranet applications
Tackle third	Non-log infrastructure information	• Configuration • Locations • Owners • Network maps • Vulnerability reports • Software inventory
	Non-log business information	• Business process mappings • Points of contact • Partner information

Logs to Avoid

There are also categories of data you should not consider logging, such as:

- Data from test environments that are not an essential part of your software delivery pipeline (CI/CD). These data would confuse your SIEM, and will produce undesired results, culminating a huge number of incident record to pop-up, cleaning it up would increase the man-hour and Analyst burn-outs.
- Data that could adversely impact compliance. For example, data associated with users who enable do-not-track settings should not be logged. Similarly, try to avoid logging highly sensitive data, such as credit card numbers, unless you are certain your logging and storage processes meet the security requirements for that data (PCI-DSS).

Best Practices for MacOS Logging & Monitoring

Source: [SOC Logging and Monitoring Best Practices | IANS Research]

Organizations can pull the right logs to manage MacOS platforms in a variety of ways, including using endpoint detection and response (EDR) tools, integrating within Active Directory (AD) or leveraging a Mac management platform like Jamf. From there, it's a matter of specifying the logs you want and sending them to your SIEM. This piece details

the options and shows you how to build an optimal MacOS logging and monitoring capability.

Challenges of MacOS Logging

Local system logging in the MacOS world is a challenging endeavor due to a variety of reasons.

First, Microsoft is still the center of the enterprise computing landscape, and most organizations either don't allow Macs or turn a blind eye to their use.

Second, Apple has typically been consumer-focused, so in cases like this, its solutions don't quite fit the needs of the enterprise. That said, MacOS is an excellent operating system, and getting what you need is usually possible.

Choosing a MacOS Logging Method

A few years back, Apple rewrote the entire logging engine on its MacOS platform and retitled it unified logging. Unified logging normalizes the log engines across Apple's iOS and MacOS platforms. This caused changes to every aspect of logging, including creating logs, storing logs and using logs.

One key change is that Mac converted all its log storage to a format called .tracev3, which is a compressed binary format. This means you must use native tools to get the logs back out. Also, you can't write simple scripts to just copy certain log files off the underlying Unix file system.

There are a few different approaches to consider when trying to figure out how to get the appropriate logs to monitor:

EDR: The first, and perhaps easiest approach is to look at the capabilities of your EDR tools. Tools such as CylanceOPTICS and CrowdStrike have extensive cross-platform telemetry monitoring and logging capabilities that may be able to get most of this data quite easily. Those systems will often already be integrated with your SIEM solutions, easing the implementation burden.

AD: Another option is to explore integrating your Mac population into AD, so you can log any network logon events by default through the standard AD integration.

Mac management platforms: These provide another option for gathering and shipping log data from your fleet of systems. Jamf (aka Casper) is the de facto standard here, and it includes features similar to Microsoft System Center Configuration Manager (SCCM).

Jamf offers an enterprise log management framework for shipping logs to your SIEM. You must define specific predicates (i.e., queries) to filter down the stream of events to ship. (Beware shipping all events, because there is an extraordinary amount of logs with no apparent value.)

Choose What to Monitor in MacOS

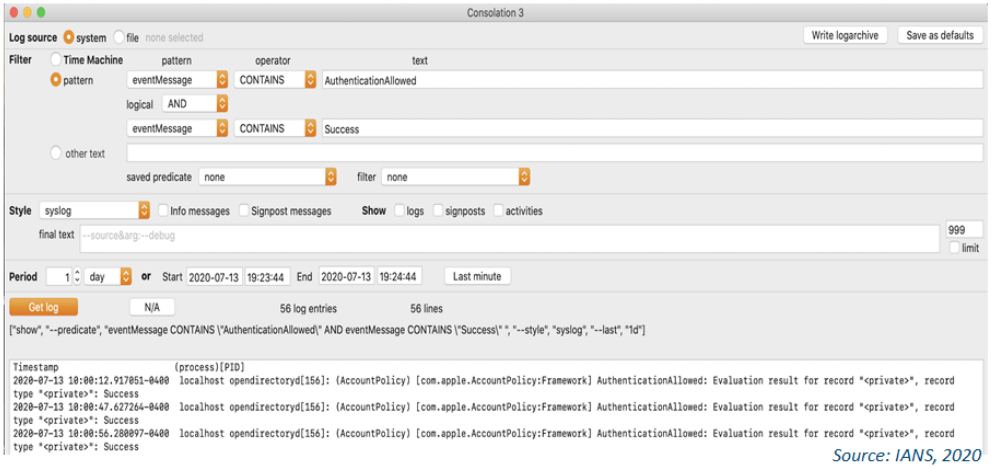
Once you've got a solution to actually get the logs out, try to identify the specific logs you care about seeing. Consider a dedicated work effort with your Mac management team to pinpoint exactly the logs to search for.

Specific logs can be loosely attributed to a few different key items (see Table 1).

Table 1: Specifying What to Monitor on MacOS

Logging Topic	Mac Considerations
System integrity	Monitor for local user account creations through native logging, Filevault 2 failures.
Security state change	This depends on what is meant by state change, but it would ideally be monitored by EDR (ensuring no uninstalls of security tools, for example).
Logon	Do a native logs search for "AuthenticationAllowed" and "Success," or rely on an AD domain join (see Figure 1). As you can see, Mac now does not even record usernames to show who logged in. Instead it's redacted with <private>, unless you create a special profile to retrieve it.
Logoff	Do a native logs search for "point of no return" or rely on an AD domain join.
Registry	Mac doesn't use registry in the same way, but it has a distributed file format tied to each application called a .plist file. These are not centrally managed like the Windows registry. To monitor for change, you'll need to identify critical applications to monitor first.
Sensitive privilege use	Search for process=sudo to get user permission escalation events. You can also use "AuthenticationAllowed completed"
User account management	Look for password changes "PasswordChangeAllowed" and user account creations.

Figure 1: Native Log Search Results for "AuthenticationAllowed"



Source: IANS, 2020

Identifying the logs you want to track can be done with a log viewer like Consolation 3 (shown in Figure 1). Use its user interface (UI) to define search criteria and review and tune the results. Then, take the “predicate” generated at the bottom and use that in your log shipping solution to pluck those logs from the log stream and send them to your logging solution.

Logging Solution for MacOS

There is no dedicated, one-size-fits-all logging solution for MacOS that directly correlates to traditional Windows logging. To get a workable solution in place:

Be systematic: Apple has highly verbose logs, but they can be culled down through a dedicated process.

Realize you can’t set it and forget it: Apple’s logging standards should be considered subject to change as they don't typically have the longevity of Windows logs. Expect logging standard to change and also anticipate maintenance with each OS upgrade.

Common Ports Monitored by The SOC Analysts

Port Number	Use	Cyber Risk
20, 21	FTP (File Transfer Protocol)	Unencrypted, susceptible to sniffing, spoofing, and brute force attacks.
22	SSH (Secure Shell)	Target for brute force attacks; vulnerable if weak credentials are used.
23	Telnet	Unencrypted, prone to eavesdropping, hijacking, and credential theft.
25	SMTP (Simple Mail Transfer Protocol)	Can be exploited for spamming and relay attacks.
53	DNS (Domain Name System)	Vulnerable to DNS spoofing and DDoS attacks.
80	HTTP (Hypertext Transfer Protocol)	Unencrypted, susceptible to interception and manipulation.
110	POP3 (Post Office Protocol version 3)	Unencrypted, vulnerable to eavesdropping if not secured.
119	NNTP (Network News Transfer Protocol)	Can be exploited in distributing malicious content.

123	NTP (Network Time Protocol)	Can be misused for DDoS attacks.
137-139	NetBIOS	Vulnerable to unauthorized access and spreading malware.
143	IMAP (Internet Message Access Protocol)	Unencrypted, potential for credential theft.
161, 162	SNMP (Simple Network Management Protocol)	Vulnerable to unauthorized access and information disclosure.
443	HTTPS (HTTP Secure)	Can be targeted by SSL stripping or MiTM attacks, though less risky than HTTP.
445	SMB (Server Message Block)	Known for vulnerabilities like EternalBlue, used in ransomware attacks like WannaCry.
993	IMAPS (Internet Message Access Protocol over SSL)	While encrypted, it can be a vector for targeted attacks if credentials are compromised.
135	Microsoft RPC	Can be exploited for unauthorized remote procedure calls.
139	NetBIOS Session Service	Vulnerable to unauthorized access and attacks on Windows networks.
143	IMAP (Internet Message Access Protocol)	Susceptible to interception, especially if unencrypted.
389	LDAP (Lightweight Directory Access Protocol)	Can be exploited in injection attacks and unauthorized access.
443	HTTPS (Hypertext Transfer Protocol Secure)	Potential for SSL/TLS vulnerabilities, MiTM attacks.
445	Microsoft-DS (Active Directory, Windows shares)	Known for SMB vulnerabilities, like EternalBlue.
465	SMTPS (Secure SMTP)	Can be targeted for spam and phishing attacks, even though encrypted.
587	SMTP with TLS/SSL	Secure, but can be targeted in mail-based attacks.
636	LDAPS (LDAP over SSL)	Encrypted, but vulnerable to specific SSL/TLS attacks.

993	IMAPS (IMAP over SSL)	Encrypted, but susceptible to targeted email attacks.
995	POP3S (POP3 over SSL)	Encrypted, but vulnerable to targeted email attacks.
1723	PPTP (Point-to-Point Tunneling Protocol)	Known vulnerabilities in VPN connections.
3306	MySQL Database Service	Vulnerable to SQL injection and unauthorized access.
3389	RDP (Remote Desktop Protocol)	Target for brute force and credential stuffing attacks.
5900	VNC (Virtual Network Computing)	Vulnerable to eavesdropping and remote control if unsecured.
69	TFTP (Trivial File Transfer Protocol)	Unsecured, vulnerable to interception and unauthorized access.
88	Kerberos	Can be targeted for authentication attacks.
109	POP2 (Post Office Protocol version 2)	Unencrypted, susceptible to eavesdropping.
156	SQL Service	Vulnerable to SQL injection and unauthorized access.
194	IRC (Internet Relay Chat)	Can be used for communication in botnets, susceptible to eavesdropping.
220	IMAP3 (Internet Message Access Protocol version 3)	Prone to the same risks as IMAP.
389	LDAP (Lightweight Directory Access Protocol)	Susceptible to directory traversal and unauthorized access.
427	SLP (Service Location Protocol)	Vulnerable to spoofing and DoS attacks.
546, 547	DHCPv6 (Dynamic Host Configuration Protocol for IPv6)	Vulnerable to unauthorized DHCP servers and MITM attacks.
554	RTSP (Real Time Streaming Protocol)	Can be exploited in streaming and DoS attacks.
631	IPP (Internet Printing Protocol)	Vulnerable to interception and unauthorized printing/access.

989, 990	FTPS (FTP over SSL)	More secure than FTP, but still can be targeted for data interception.
1194	OpenVPN	Can be targeted in VPN bypass and DoS attacks.
1433, 1434	Microsoft SQL Server	Vulnerable to SQL injection and unauthorized access.
1701	L2TP (Layer 2 Tunneling Protocol)	Vulnerable in unencrypted implementations.
1812, 1813	RADIUS (Remote Authentication Dial-In User Service)	Vulnerable to credential theft and replay attacks.
2049	NFS (Network File System)	Vulnerable to unauthorized file access and interception.
2082, 2083	cPanel	Can be targeted for web hosting control panel attacks.
2483, 2484	Oracle Database	Vulnerable to SQL injection and unauthorized access.
5060, 5061	SIP (Session Initiation Protocol)	Vulnerable to VoIP spam, eavesdropping, and hijacking.

Common Tools Used by SOC

Security Operations Centers (SOCs) use a variety of tools to monitor, detect, and respond to security incidents. Here are some of the common tools used by SOCs:

Most used tools:

- 100 Best Free Red Team Tools in 2023 - Cyber Security News
- A-poc/RedTeam-Tools: Tools and Techniques for Red Team / Penetration Testing (github.com)
- A-poc/BlueTeam-Tools: Tools and Techniques for Blue Team / Incident Response (github.com)
- bigb0sss/RedTeam-OffensiveSecurity: Tools & Interesting Things for RedTeam Ops (github.com)

Best Linux Distros for Cybersecurity

1. **Kodachi**: Kodachi uses a customized Xfce desktop and aims to give users access to a wide variety of security and privacy tools.

2. **Qubes OS**: Qubes has established itself as arguably the most popular security-centric distro. It works on the principle of compartmentalization, isolating different tasks into separate virtual machines for enhanced security.
3. **ParrotOS**: Based on Debian, ParrotOS provides a cloud-friendly environment with online anonymity and an encrypted system. It's suitable for penetration testers and security enthusiasts.
4. **BlackArch**: Built on Arch Linux, BlackArch offers a repository containing thousands of security tools organized into various groups. It's specialized for penetration testing.
5. **Tails (The Amnesic Incognito Live System)**: Tails is designed for privacy-conscious users. It routes internet traffic through the Tor network and leaves no trace on the host system.
6. **Kali Linux:** Kali Linux, formerly known as BackTrack, distribution of the Linux operating system was developed by Offensive Security and is derived from the Debian distribution of Linux.
7. **Node Zero:** NodeZero was built around the Ubuntu distribution of the original Linux software as a complete system designed with penetration testing in mind.
8. **CAINE Linux:** An Ubuntu-based variation of the Linux software, the Computer-Aided Investigative Environment (CAINE). CAINE was created as part of a project for digital forensics software, organizing cyber forensic tools with a user-friendly graphical interface
9. **BackBox:** BackBox is an Ubuntu based open-source Operating System that offers a penetration test and security assessment facility. This system also provides a network analysis toolkit for security in the IT environment.
10. **Fedora Security Lab:** Fedora Security environment enables you to work on security auditing, forensics, and hacking. It comes with a clean and fast desktop environment.
11. **Dracos Linux:** Dracos Linux is an open-source OS that is packed with a wide range of tools, like forensics, information gathering, malware analysis, and more.
12. **Samurai Web Testing Framework:** Samurai Web Testing Framework is a virtual machine that is supported on VMWare (cloud computing software) VirtualBox (virtualization product). This live Linux environment is configured to perform web pen-testing. It contains various tools for attacking websites.
13. **Network Security Toolkit (NST):** Network Security Toolkit (NST) is a Linux-based Live USB/DVD flash drive. It offers free and open-source network and computer security tools that can be used for hacking. This distribution is used by hackers to perform routine security and network traffic monitoring task.
14. **ArchStrike:** ArchStrike is an OS that can be used for security professionals and researchers. It follows Arch Linux OS standards to maintain packages properly. This environment can be used for pen testing and security layer.

Each distribution of the Linux operating software was developed by individuals or by a community who want to custom tailor it to what they feel is the best version for cybersecurity purposes. Each one will have different advantages and shortcomings. If you are unsure about which Linux distribution will best suit you, the best detail is that you can try them all out without a penalty since they are all open-source and will not cost you a dime. However, if reviews are any indication, Kali Linux appears to be the top contender. Choose the one that aligns best with your needs and expertise!

CHAPTER 11

SOC Reference Archiecture

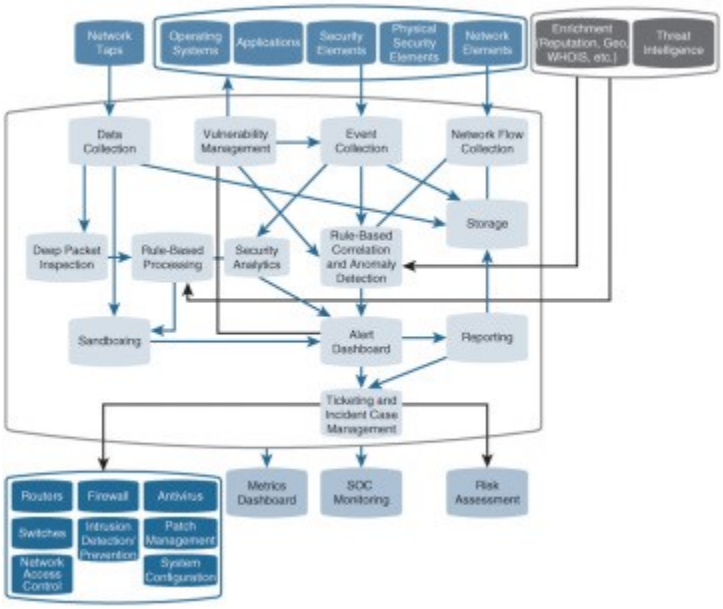
TRY TO GRAB THE KNOWLEDGE OF FINDING AND STUDYING REFERENCE ARCHITECTURES AS MUCH AS POSSIBLE, THE PROVIDED RA LINKS ARE GOOD FOR A FRESH START, BUT THAT'S NOT THE END, AS YOU WILL SEE DIFFERENT PERSPECTIVES ARE ADDED TO DIFFERENT ARCHITECTURE THAT CAN BE STANDALONE, CLUSTERED (OS OR SERVICES), WITH OR WITHOUT HA.

A well-structured SOC is crucial for effective cybersecurity management. Here are some insights:

1. **SOC Conceptual Architecture**:
    - To optimize your investment, it's essential to operate various SOC technologies within a cohesive architecture.
    - The proposed reference conceptual architecture formalizes several key aspects:

- **Input Sources**: These are categorized data sources that feed information into the SOC.
- **Output**: The SOC generates alerts and takes necessary actions based on the analyzed data.
- **Technologies**: The suite of tools and technologies employed within the SOC.
- **Relationships**: How these technologies interact and collaborate.
- **Measurement Points**: Areas where data can be collected (e.g., type, value, frequency).

- Refer to below picture for an illustration of this conceptual architecture.



Source: [SOC Conceptual Architecture > Overview of Security Operations Center Technologies | Cisco Press]

2. **Managed Threat Defense Services**:

   - Additionally, consider an alternative architecture where SOC responsibilities are outsourced to a managed service provider.

   - Cisco's architecture for managed threat defense services caters to customers seeking to outsource some or all of their SOC functions. See the below picture:

Source: [SOC Conceptual Architecture > Overview of Security Operations Center Technologies | Cisco Press]

Microsoft Reference Architecture for Security Operations

Modern Security Operations (SecOps) reduces organizational risk from active attacks by rapidly detecting and remediating them

While a highly technical discipline, SecOps is first a human-centric function that empowers people with technology (rather than trying to replace people). Modern security operations technology helps extend **human** skills & expertise across today's 'hybrid of everything' technical environments to meet the threats posed by adaptable **human** attackers (who often use automated tools).

Because serious cyberattacks are often driven in near-real time by human attack operators, success metrics for security operations (SecOps / SOCs) should focus heavily on the ***time*** attackers have in the environment and helping defenders reduce attacker dwell time (measured in **Mean Time to Remediate or MTTR).** This reduces attacker ability to inflict damage on the organization.

Raw Data and Classic SecOps

Historically, security operations focused on collecting as much activity/event data from the environment as they could in a Security Incident & Event Management (SIEM). While collection is an important foundational step, this often led to a '*collection is not detection*' problem where very few actionable insights were actually gleaned from the data collected.

Queries authored by human analysts sometimes help detect anomalies that were malicious attacks, but these static queries often generated many false positive detections because of the continuously changing attacks, organizational assets, user behavior patterns, and data source scenarios. These false positives (false alarms) waste precious human analyst time and attention, taking them away from managing real attacks and increasing analyst fatigue/burnout.

Automation (SOAR) and Integration

Another key element for empowering security operations comes from the adoption of Security Orchestration, Automation, and Remediation **(SOAR)** technologies and **integration** of toolsets together (natively or by providing APIs).

SOAR/Automation and Integration:

- **Reduce manual work** for analysts and other roles with seamless experiences. Manual steps take time away from meaningful work and erode analyst morale, they would rather be fighting the bad guys than copy/pasting between tools and switching consoles
- **Speed Up** response time because the automation happens at machine speed rather than human speed.
- **Increase Scale** of security operations to meet the growing volume of attacks and increased scope/complexity of modern multi-cloud hybrid enterprises.

Microsoft focuses on automation and integration by

- **Embedding SOAR** technologies throughout our tools (AutoIR in Defender XDR, Azure Logic Apps in Microsoft Sentinel)
- **Single Microsoft 365 Defender console** to integrate experience for endpoint, email, SaaS
- **Natively integrating** Microsoft tools together (SIEM and XDR) to simplify SecOps workflows
- **Creating APIs** to connect with existing 3rd party tools

Microsoft Sentinel and SIEM Modernization

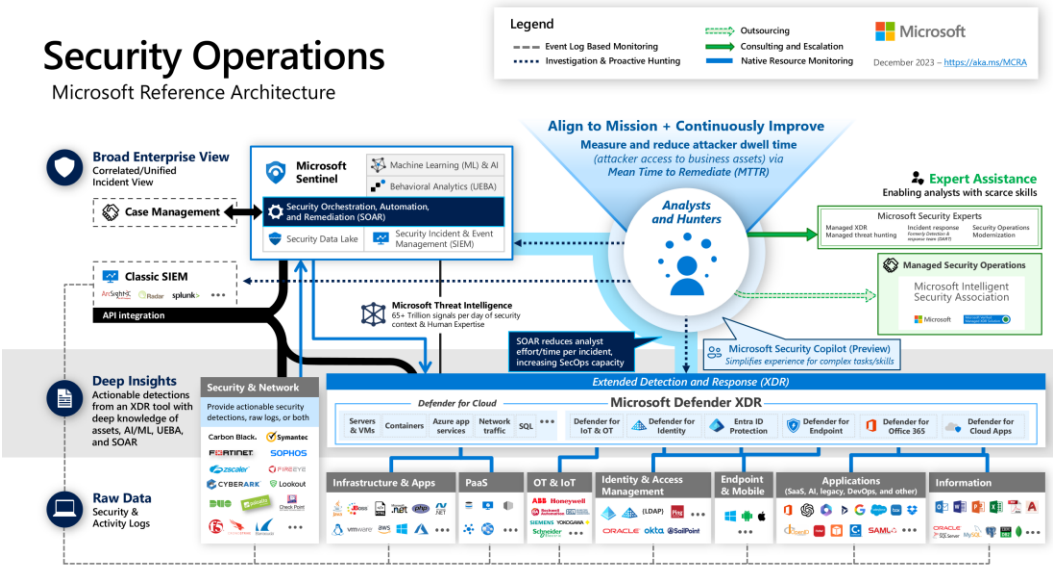
The need for SIEM technology has not gone away with the advent of XDR, but has shifted to the cases where it's needed most - creating custom detections (not duplicating XDR common detections) and analyzing multiple different data sources (including existing 3rd party security tools).

Microsoft Sentinel is a cloud-native SIEM that complements XDR tooling by providing analytics to create custom detections and hunt for threats across arbitrary log/data sources from any platform, cloud, application, or device.

Microsoft Sentinel alerts and workflows are integrated into Microsoft Defender XDR to streamline the analyst experience and minimize the need to change console/interfaces during time-sensitive incidents.

Notes:

- In addition to traditional SIEM functionality of static analysis of event logs, Microsoft Sentinel incorporates SOAR, ML, UEBA, Jupyter Notebooks, Threat Intelligence, and Security Data Lake approaches to refine threat detection, investigation, and threat hunting processes. Microsoft Sentinel also supports lower cost archival storage for large volumes of data.
- Microsoft Sentinel also offers many playbooks and other features to streamline investigation & remediation of critically important assets like SAP® applications and Operational Technology (OT) and Industrial internet of things (IIoT) [lso known as Industrial Control Systems (ICS) / Supervisory Control and Data Acquisition (SCADA)].



Source: [Microsoft MCRA (December 2023 Edition)]

1. **Security Information and Event Management (SIEM)**: SIEM tools aggregate log data from various sources, examine it for possible attack patterns, and raise an alert if a threat is found.
2. **Log Collection and Management Tool**: These tools automate the process of log collection, parsing, and analysis.
3. **Vulnerability Management Tools**: These tools scan and monitor the organization's network periodically for any vulnerabilities.
4. **Endpoint Detection and Response (EDR)**: EDR tools continuously monitor various endpoints, collect data from them, and analyze the information for any suspicious activities and attack patterns.
5. **Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)**: These systems monitor network traffic for suspicious activity and issue alerts when such activity is discovered.
6. **Firewalls and Next-Generation Firewalls (NGFW)**: These tools monitor and control incoming and outgoing network traffic based on predetermined security rules.
7. **Governance, Risk, and Compliance (GRC) Systems**: These tools help organizations to strategically align IT with business objectives, while effectively managing risk and meeting compliance requirements.
8. **Investigation Tools**: These tools are used to investigate security incidents.

9. **Vulnerabilities Feeds and Databases**: These tools provide information about the latest vulnerabilities.

These tools help SOCs to protect the organization's information assets by providing real-time analysis of security alerts generated by applications and network hardware.

Demonstrating Privacy Accountability (NYMITY)

Source: PMAF Poster - January 2017 (vvena.nl)

Providing complete overview of the framework, delving deeper into the 13 core Privacy Management Activities (PMAs) may be helpful to you:

1. Governance:

- Establish a privacy steering committee.
- Appoint a data protection officer (DPO).
- Develop and implement a privacy policy.
- Conduct regular privacy risk assessments.
- Train employees on privacy policies and procedures.

2. Risk Management:

- Identify and assess privacy risks for all data processing activities.
- Implement appropriate controls to mitigate identified risks.
- Conduct regular reviews of data security measures.
- Respond to and report data breaches promptly.

3. Data Mapping:

- Create a complete inventory of all personal data collected, stored, and processed.
- Map data flows to understand how personal data moves throughout the organization.
- Implement data classification procedures to identify sensitive information.

4. Data Subject Rights:

- Establish clear processes for individuals to exercise their data subject rights, such as access, rectification, and erasure.
- Provide easily accessible information on how individuals can contact the organization regarding their data rights.
- Train employees on handling data subject rights requests.

5. Third-Party Risk Management:

- Conduct due diligence on third-party vendors that handle personal data.
- Implement contractual clauses to ensure third-party compliance with data privacy regulations.
- Monitor third-party data security practices and conduct audits as needed.

6. Data Security:

- Implement appropriate technical and organizational security measures to protect personal data.
- Conduct regular penetration testing and vulnerability assessments.
- Encrypt sensitive data at rest and in transit.

7. Incident Response:

- Develop and document an incident response plan for data breaches and other privacy incidents.
- Train employees on identifying and reporting privacy incidents.
- Conduct regular incident response drills and exercises.

8. Privacy Impact Assessments:

- Conduct PIAs for any new projects or technologies that involve personal data.
- Identify and mitigate potential privacy risks associated with the project or technology.
- Document the PIA findings and incorporate them into the project design.

9. Training and Awareness:

- Provide regular training for all employees on data privacy policies, procedures, and regulations.
- Conduct targeted training for employees with access to sensitive data.

- Raise awareness of data privacy throughout the organization.

10. Transparency and Reporting:

- Publish a clear and accessible privacy policy on the organization's website.
- Disclose personal data breaches and other privacy incidents promptly.
- Prepare and submit data protection reports as required by applicable regulations.

11. Cross-Border Data Flows:

- Implement appropriate safeguards for transferring personal data outside the organization's jurisdiction.
- Conduct risk assessments and comply with relevant data transfer mechanisms.
- Train employees on cross-border data transfer procedures.

12. Privacy by Design:

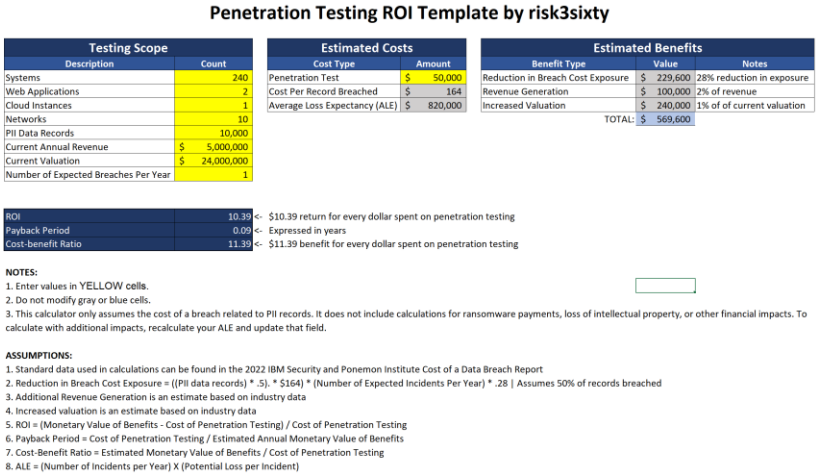
- Integrate privacy considerations into the design of new products, services, and processes.
- Minimize data collection and retention.
- Implement data-minimization principles throughout the data lifecycle.

13. Data Retention and Disposal:

- Define and document data retention periods for different types of personal data.
- Implement secure disposal procedures for data that is no longer needed.
- Train employees on proper data retention and disposal practices.

Please note that this is a high-level overview of the 13 core PMAs within the Nymity PAMF. Each PMA can be further broken down into even more specific tasks and actions, providing organizations with a detailed roadmap for implementing a comprehensive data privacy program.

Penetration Testing ROI Template by risk3sixty



Penetration Testing ROI Template by risk3sixty

Testing Scope	
Description	Count
Systems	240
Web Applications	2
Cloud Instances	1
Networks	10
PII Data Records	10,000
Current Annual Revenue	$ 5,000,000
Current Valuation	$ 24,000,000
Number of Expected Breaches Per Year	1

Estimated Costs	
Cost Type	Amount
Penetration Test	$ 50,000
Cost Per Record Breached	$ 164
Average Loss Expectancy (ALE)	$ 820,000

Estimated Benefits		
Benefit Type	Value	Notes
Reduction in Breach Cost Exposure	$ 229,600	28% reduction in exposure
Revenue Generation	$ 100,000	2% of revenue
Increased Valuation	$ 240,000	1% of of current valuation
TOTAL:	$ 569,600	

ROI	10.39	<- $10.39 return for every dollar spent on penetration testing
Payback Period	0.09	<- Expressed in years
Cost-benefit Ratio	11.39	<- $11.39 benefit for every dollar spent on penetration testing

NOTES:
1. Enter values in YELLOW cells.
2. Do not modify gray or blue cells.
3. This calculator only assumes the cost of a breach related to PII records. It does not include calculations for ransomware payments, loss of intellectual property, or other financial impacts. To calculate with additional impacts, recalculate your ALE and update that field.

ASSUMPTIONS:
1. Standard data used in calculations can be found in the 2022 IBM Security and Ponemon Institute Cost of a Data Breach Report
2. Reduction in Breach Cost Exposure = ((PII data records) * .5). * $164) * (Number of Expected Incidents Per Year) * .28 | Assumes 50% of records breached
3. Additional Revenue Generation is an estimate based on industry data
4. Increased valuation is an estimate based on industry data
5. ROI = (Monetary Value of Benefits - Cost of Penetration Testing) / Cost of Penetration Testing
6. Payback Period = Cost of Penetration Testing / Estimated Annual Monetary Value of Benefits
7. Cost-Benefit Ratio = Estimated Monetary Value of Benefits / Cost of Penetration Testing
8. ALE = (Number of Incidents per Year) X (Potential Loss per Incident)

Source: [Penetration Testing ROI Calculator - risk3sixty]

Automated Penetration Testing

There are number of platforms that has their own developed platforms which has automated testing services both for your on-premise and cloud platforms. It's important to note that while automated tools can speed up the testing process and provide valuable insights, they should be complemented with manual testing and a comprehensive security program to ensure a thorough evaluation of the overall security posture.

Automated penetration testing can help organizations identify and address security weaknesses before malicious actors can exploit them. Here are some key aspects of automated penetration testing:

1. **Tools and Frameworks:**
    - **Open Source Tools:** Tools like Metasploit, OWASP ZAP, Nikto, and Nmap are commonly used in automated penetration testing. These tools provide a wide range of functionalities for vulnerability scanning, exploitation, and post-exploitation activities.
    - **Commercial Solutions:** There are also commercial penetration testing tools and platforms available, such as Rapid7's Nexpose, Qualys, and Burp Suite, Evolve:PT Professional. These tools often provide additional features and support, which can be proven very useful.

2. **Vulnerability Scanning:**
    - Automated penetration testing tools typically start with vulnerability scanning to identify potential weaknesses in a system. This involves scanning the target for known vulnerabilities in software, configurations, or network infrastructure.
3. **Exploitation:**
    - Once vulnerabilities are identified, automated tools may attempt to exploit them to gain unauthorized access or escalate privileges. This step helps assess the severity and impact of the vulnerabilities.
4. **Post-Exploitation:**
    - Some automated penetration testing tools include post-exploitation modules to simulate what an attacker could do after gaining access. This may involve extracting sensitive information, lateral movement within the network, or establishing persistence.
5. **Reporting:**
    - After the automated penetration testing is complete, a detailed report is generated. This report includes information about the vulnerabilities discovered, their severity, and recommendations for remediation. The report is crucial for organizations to understand their security posture and prioritize remediation efforts.

Pro-Tip

- These reports can be compared with other known frameworks (NIST, CIS, 27001 etc.) and how it affects the organizational structure as well.

6. **Continuous Testing:**
    - Automated penetration testing can be integrated into a continuous testing and deployment pipeline. This allows organizations to identify and address security issues early in the development process, reducing the overall risk.

Pro-Tip

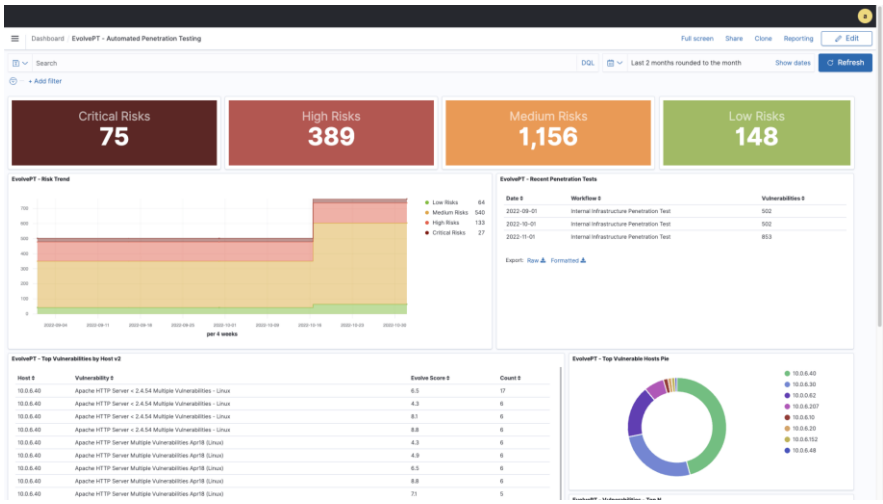
- As the devices firmware's, application patches take place, which also calls for VA/PT over and over again.

7. **Challenges:**
    - While automated penetration testing is a valuable tool, it has limitations. It may not identify certain complex vulnerabilities that require manual testing or advanced understanding of the application's logic. False positives and negatives are also potential challenges that need to be considered.
8. **Compliance:**
    - Automated penetration testing is often used to meet compliance requirements in various industries. Organizations may be required to conduct regular penetration tests to demonstrate the security of their existing systems.

Pro-Tip

- Personally, I would go for engaging a human being in manual testing for specific testing on a specific target and would try to receive valuable insights, that didn't get identified in the automated scenario.

Though at times it could be costly, but on a holistic view and with a shorter amount of time, this option could really come in handy. One of the Automated-PT service providers I have seen is from EVOLVE-PT with insights (in your case things may not be the same as it depends on the complexity of your network infrastructure, integrations of various components and their provided visibility will affect the outcome of the below picture):



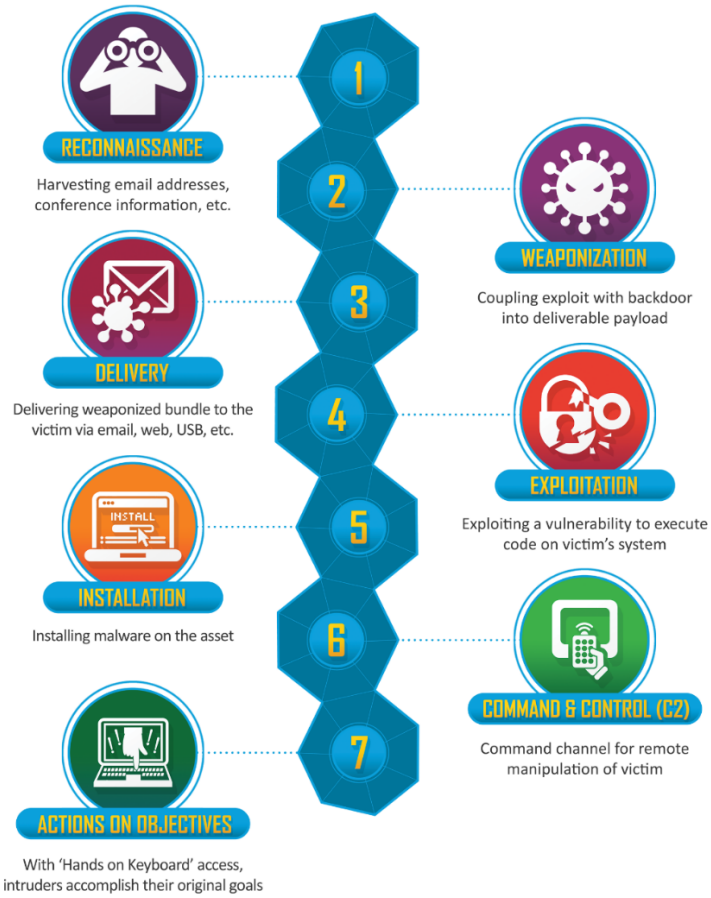
Source: [EvolvePT - The Most Comprehensive Penetration Testing Tool (threatintelligence.com)]

CHAPTER 12

Frameworks Used by SOC

DIFFERENT FRAMEWORKS ARE APPLIED TO THE SOC INFRASTRUCTURE, REASON WHY ITS IMPERATIVE THAT YOU SHOULD HAVE GOOD KNOWLEDGE ON THE REFERENCE ARCHITECTURES, SERVICES INTEGRATED, MAPPED TO DIFFERENT VISIBILITY REQUIREMENTS, PLAYBOOKS AND DIFFERENT TYPES OF OPERATIONAL ACTIVITIES.

Security Operations Centers (SOCs) use various frameworks to standardize their defense strategies, manage cybersecurity risks, and improve operations. Here are some of the common frameworks used by SOCs (Major & high level shown only):



Source: [Cyber Kill Chain® | Lockheed Martin]

The Cyber Kill Chain is a concept developed by Lockheed Martin to describe the various stages of a cyber-attack, from initial reconnaissance to achieving the attacker's objectives. Understanding and utilizing the Cyber Kill Chain is crucial in the field of cybersecurity for several reasons:

Early Detection and Prevention: The Cyber Kill Chain allows organizations to detect and prevent cyber-attacks at an early stage. By breaking down the attack lifecycle into stages, security teams can identify indicators of compromise, recognize patterns, and intervene before an attack progresses.

Attack Visualization and Understanding: It provides a visual representation of the different stages an attacker goes through, helping security professionals understand the attack process. This visualization aids in creating effective defense strategies and responses tailored to each stage.

Risk Mitigation: Understanding the Cyber Kill Chain enables organizations to implement targeted security measures at each stage, mitigating risks effectively. By focusing on vulnerable points in the chain, security controls can be optimized to disrupt the attack before it reaches its final objective.

Incident Response Planning: The Cyber Kill Chain is a valuable tool in incident response planning. It allows organizations to create and refine incident response plans based on a clear understanding of the stages an attacker must go through. This proactive approach improves the organization's resilience against potential threats.

Threat Intelligence Integration: The Kill Chain framework integrates well with threat intelligence. Security teams can map threat intelligence data to specific stages of the Kill Chain, providing context and relevance to potential threats. This integration enhances the organization's ability to respond to real-world, targeted attacks.

Continuous Improvement: By analyzing successful and attempted attacks through the lens of the Kill Chain, organizations can continuously improve their cybersecurity strategies. Lessons learned from previous incidents can be used to enhance security controls, update policies, and adapt defenses to evolving threats.

Efficient Resource Allocation: The Kill Chain helps organizations allocate resources more efficiently by identifying critical stages in the attack lifecycle. This strategic allocation ensures that security measures are concentrated where they are most needed, optimizing the use of resources.

Communication and Collaboration: The Cyber Kill Chain provides a common language for cybersecurity professionals. It facilitates better communication and collaboration within security teams and between different organizations. This shared understanding is essential in addressing and mitigating threats collectively.

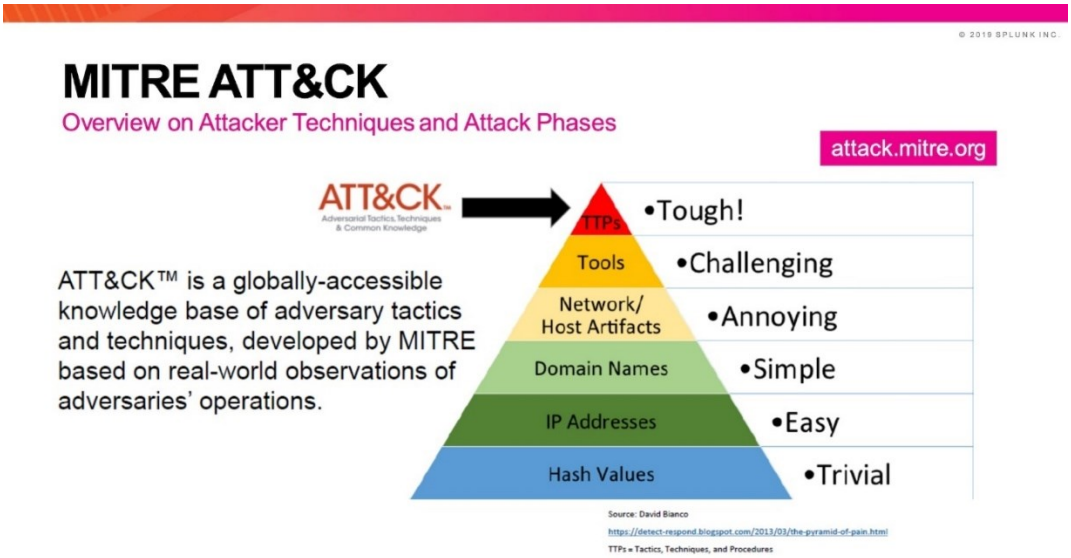
Advanced Threat Detection: The Kill Chain enables the development and deployment of advanced threat detection mechanisms. By understanding the tactics, techniques, and procedures (TTPs) employed by attackers at each stage, organizations can design and implement more sophisticated detection and monitoring systems.

Adapting to Evolving Threats: The Kill Chain framework is dynamic and adaptable. As cyber threats evolve, security professionals can update and refine their defense

strategies based on the changing tactics of attackers. This adaptability ensures that cybersecurity measures remain effective over time.

The Famous Non-Controlling Body - NIST

1. **NIST Cybersecurity Framework (CSF)**: The NIST CSF includes threat lifecycle management standards, best practices, and guidelines. It helps organizations protect critical infrastructure by increasing security in various ways. The five core functions of the NIST CSF are (in short IPDRR, now "G" is added for Governance):
    - Identify: Learn how to better manage cybersecurity risks to various components like assets, systems, and data.
    - Protect: Implement safeguards to protect critical infrastructure services.
    - Detect: Define what constitutes a cybersecurity event.
    - Respond: Specify actions performed in response to a detected cybersecurity event.
    - Recover: Identify services to focus on for resilience, and outline the required restore capabilities of impaired services.
2. **MITRE ATT&CK Framework**: The MITRE ATT&CK framework provides observable adversarial behaviors to help intelligently identify tactics occurring after an attack has started. It helps inform threat intelligence, threat detection, and analysis, red teaming and adversary emulation, as well as engineering and assessment. (Matrix - Enterprise | MITRE ATT&CK®)



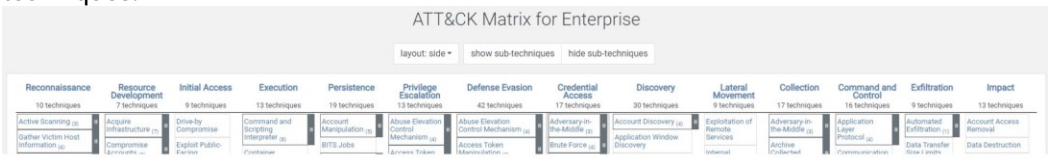
Source: [Q&A Follow-Up: So nutzt Datev MITRE ATT&CK & Splunk im SOC | Splunk]

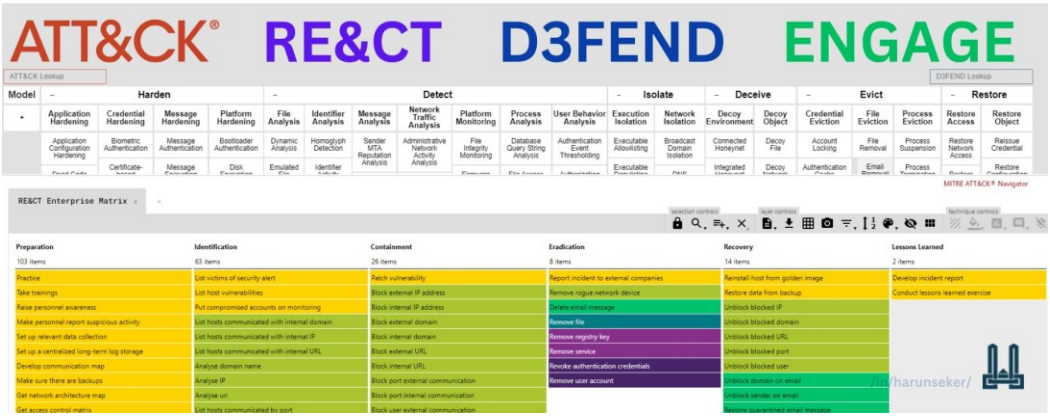
3. **Cyber Kill Chain Framework**: This framework is used to understand and prevent intrusions into the network.
4. **Unified Kill Chain Framework**: This framework is an extension of the Cyber Kill Chain and is used to analyze threats from all vectors.
5. **ISO 27XXX series:** these series are prepared for certification and covers some areas of working domains. The problem with these series are, they overlap, and require multiple certifications to achieve domain coverage on information security, cybersecurity and for privacy protection.

MITRE has developed several frameworks to help organizations defend against cyber attacks:

MITRE ATT&CK framework is to help organizations and security professionals improve their cyber defense by identifying and understanding the methods and techniques used by attackers. It is used to identify and categorize tactics, techniques, and procedures (TTPs) used by cyber attackers to compromise systems.

MITRE D3FEND framework is a knowledge base, but more specifically a knowledge graph, of cybersecurity countermeasure techniques. In the simplest sense, it is a catalog of defensive cybersecurity techniques and their relationships to offensive/adversary techniques.





MITRE RE&CT Framework is designed for accumulating, describing and categorizing actionable Incident Response techniques. RE&CT's philosophy is based on the MITRE's ATT&CK framework, which comes with a navigator too.

MITRE Engage combines several active defense types, including basic cyber defensive actions alongside adversary engagement and cyber deception operations. Together, these defenses enable organizations to counter attacks while also obtaining additional information about the adversary.

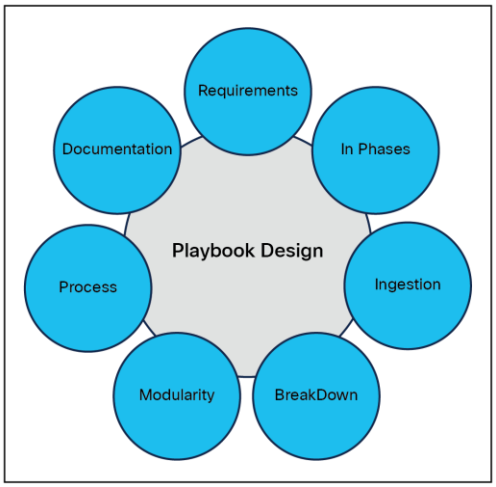
ATT&CK Framework and Navigator :	http://attack.mitre.org/
D3FEND Framework and Navigator :	https://d3fend.mitre.org/
RE&CT Framework :	https://lnkd.in/edCj2qh7
RE&CT Navigator:	https://lnkd.in/ekYsfV-c
ENGAGE Navigator:	https://lnkd.in/ev4S3vdb

A plethora of certifications on information security, cybersecurity and for privacy protection @iso.org: ISO/IEC JTC 1/SC 27 - Information security, cybersecurity and privacy protection

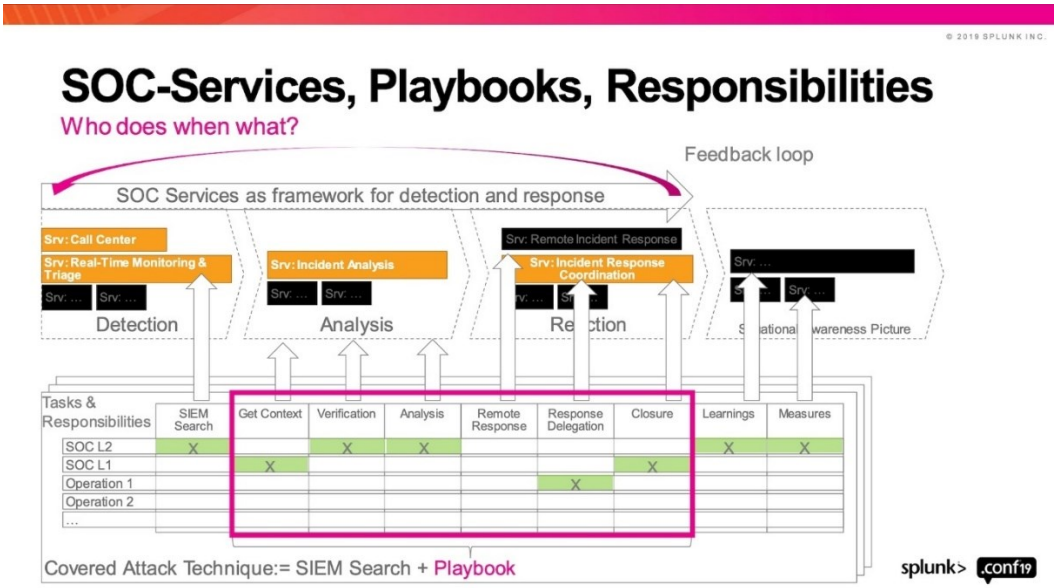
These frameworks help SOCs to protect the organization’s information assets by providing real-time analysis of security alerts generated by applications and network hardware.

Building an Effective Security Operations Center (SOC) Playbook

Developing a playbook involves several steps:



1. **Understand your Environment**: Get a clear picture of your IT infrastructure, including the IP addresses, endpoints, firewalls, and other elements.
2. **Identify Threat Vectors**: Understand the common cyber threats that your organization is likely to face. This could include phishing emails, ransomware attacks, and more.
3. **Define Roles and Responsibilities**: Clearly outline who is responsible for what during an incident response process. This includes the security team, response teams, stakeholders, and others involved.
4. **Outline the Procedures**: Provide step-by-step procedures for different incidents. This should include everything from identification, triage, escalation, remediation, and follow-up steps.
5. **Integrate Tools**: Mention the tools that will be used during the incident response process such as SIEM, EDR, sandbox, etc.
6. **Test the Playbook**: Once the playbook is created, it needs to be tested and refined based on the results. Some good playbook links are shared in the reference section.



Source: [soc services playbooks & responsibilities in splunk - Search Images (bing.com)]

SOC Services, Playbooks and Responsibilities

The SOC provides various services, utilizes playbooks, and assigns specific responsibilities to ensure effective cybersecurity operations. Here's an overview of SOC services, playbooks, and responsibilities:

Services:

- Continuous Monitoring:
  - Service Description: The SOC continuously monitors the organization's networks, systems, applications, and data for any signs of security incidents or anomalies.
  - Objective: Early detection of potential threats and vulnerabilities to minimize the impact of Security incidents.
- Incident Detection and Analysis:
  - Service Description: Rapid detection and analysis of security incidents, including suspicious activities, anomalies, and potential breaches.
  - Objective: Identify and understand the nature and scope of security incidents.
- Incident Response:

    - Service Description: Immediate response to confirmed security incidents, including containment, eradication, and recovery efforts.
    - Objective: Minimize the impact of security incidents and restore normal operations swiftly.
- Threat Intelligence Integration:
    - Service Description: Integration of threat intelligence feeds to enhance the SOC's understanding of current and emerging threats.
    - Objective: Stay informed about the threat landscape to proactively defend against potential attacks.
- Vulnerability Management:
    - Service Description: Identification, assessment, and management of vulnerabilities in the organization's infrastructure.
    - Objective: Mitigate vulnerabilities before they can be exploited by attackers.
- Log Management and Analysis:
    - Service Description: Collection, storage, and analysis of logs and events from various sources to identify security incidents.
    - Objective: Detect anomalous activities and track potential indicators of compromise.
- Security Awareness and Training:
    - Service Description: Providing security awareness training for employees to recognize and report potential security threats.
    - Objective: Create a security-aware culture within the organization to reduce the likelihood of human error leading to security incidents.

Playbooks:

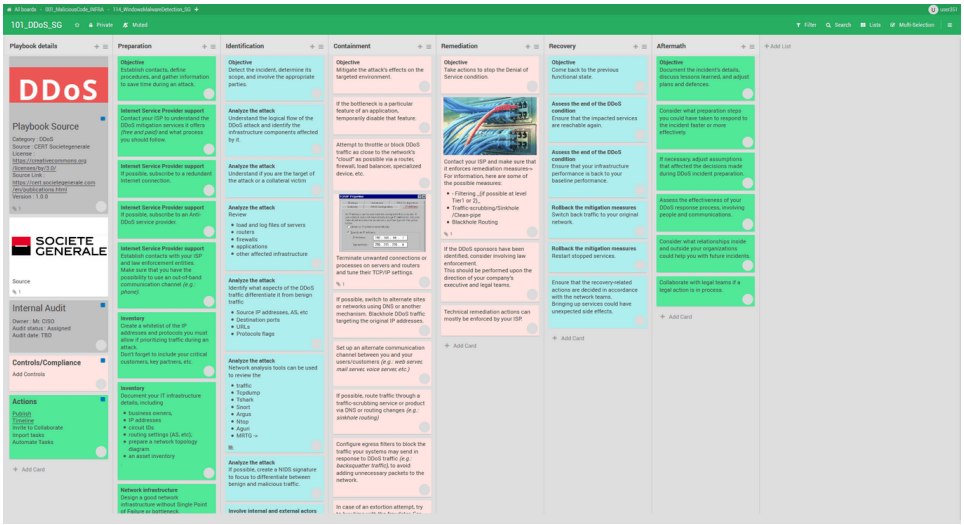
- Incident Detection and Response Playbook:
    - Description: Step-by-step procedures for detecting, analyzing, and responding to security incidents.
    - Use Case: Provides a structured approach for SOC analysts to follow when responding to alerts or incidents.
- Phishing Response Playbook:
    - Description: Guidelines for identifying, analyzing, and responding to phishing attacks.
    - Use Case: Helps SOC analysts and incident responders effectively handle phishing incidents, protecting against social engineering threats.
- Malware Analysis Playbook:

    - Description: Procedures for analyzing and responding to malware incidents.
    - Use Case: Enables the SOC team to identify the type and impact of malware and initiate appropriate response measures.
- Data Breach Response Playbook:
    - Description: Outlines steps to follow when responding to a data breach, including legal, communication, and technical aspects.
    - Use Case: Ensures a coordinated and effective response to data breaches, minimizing reputational damage.
- Patch Management Playbook:
    - Description: Procedures for managing and applying patches to address vulnerabilities.
    - Use Case: Ensures a systematic approach to patching to mitigate potential security risks.

Responsibilities:

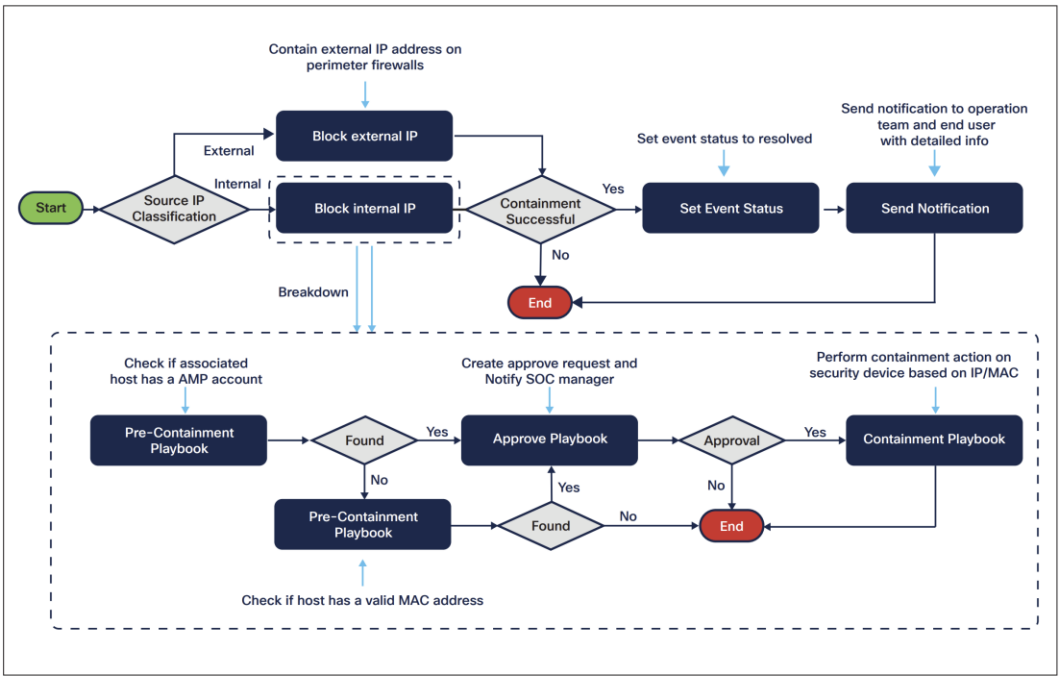
- SOC Analysts:
    - Responsibilities: Monitor alerts, investigate incidents, and execute response procedures based on playbooks.
- Incident Responders:
    - Responsibilities: Lead the response to confirmed security incidents, coordinate containment and recovery efforts, and collaborate with relevant stakeholders.
- Threat Intelligence Analysts:
    - Responsibilities: Analyze threat intelligence, identify potential threats, and provide actionable insights to enhance security measures.
- Security Engineers:
    - Responsibilities: Implement and maintain security technologies, conduct vulnerability assessments, and contribute to the development of playbooks.
- Security Awareness Trainers:
    - Responsibilities: Develop and deliver security awareness training programs to educate employees on security best practices.
- SOC Manager:
    - Responsibilities: Oversee SOC operations, set strategic goals, collaborate with leadership, and ensure the SOC's effectiveness in addressing security threats.
- Security Operations Director:

- Responsibilities: Provide leadership and strategic direction for the overall security operations, aligning with organizational goals and objectives.



Source: [Cyber Security Incident management system using Flexible Evolving Playbooks (flexibleir.com)]

Below is part of the containment playbook workflow for showing the high-level and breakdown process for the internal IP/MAC address block:



Source: [Designing Security Automation Playbooks - Sharing Lessons Learned with Practitioners White Paper (cisco.com)]

Playbook Battle Cards: [gsvsoc_cirt-playbook-battle-cards/GSPBC-1000 - Impact - Data Encrypted For Impact - Ransomware.pdf at master · guardsight/gsvsoc_cirt-playbook-battle-cards (github.com)]

Remember, creating an event specific SOC playbook is an ever-ending process. It needs to be updated regularly as new threats emerge and changes occur in the IT environment. Incorporating tools like Tufin can greatly enhance the effectiveness of your SOC playbook.

Designing Security Automation Playbooks

Designing security automation playbooks is a crucial aspect of a well-structured Security Operations Center (SOC). Playbooks are step-by-step guides that define the processes and actions to be taken in response to specific security incidents or events. Here's a comprehensive guide on designing security automation playbooks:

1. Identify Common Security Incidents:

- **Objective:** Understand the types of security incidents your organization is likely to encounter.
- **Action:**
  - Conduct a thorough risk assessment.
  - Analyze historical incident data.
  - Collaborate with threat intelligence sources.

2. Define Playbook Objectives:

- **Objective:** Clearly outline the goals and objectives of each playbook.
- **Action:**
  - Identify the specific security incidents or scenarios the playbook will address.
  - Define the desired outcomes and response objectives.

3. Document Playbook Steps:

- **Objective:** Clearly document the sequence of steps to be followed during an incident.
- **Action:**
  - Break down the incident response process into actionable steps.
  - Provide detailed instructions for each step.

4. Automate Repetitive Tasks:

- **Objective:** Automate routine and repetitive tasks to increase efficiency.
- **Action:**
  - Identify tasks that can be automated, such as log analysis or threat intelligence correlation.
  - Integrate automation scripts or tools into the playbook.

5. Integrate with Security Tools:

- **Objective:** Ensure seamless integration with existing security tools.
- **Action:**
  - Identify the security tools used in your environment.
  - Develop integrations or connectors to facilitate automated actions.

6. Include Decision Points:

- **Objective:** Build flexibility into playbooks by incorporating decision points.
- **Action:**
  - Identify decision criteria based on incident characteristics.
  - Provide guidance for analysts to make informed decisions.

7. Consider Playbook Dependencies:

- **Objective:** Ensure that playbooks are designed to account for dependencies on other processes or teams.
- **Action:**
  - Clearly outline any dependencies, such as involving legal or communication teams.
  - Provide escalation paths when needed.

8. Define Trigger Conditions:

- **Objective:** Clearly define the conditions that trigger the execution of a playbook.
- **Action:**
  - Identify specific indicators or events that initiate the playbook.
  - Set threshold conditions for triggering the playbook.

9. Incorporate Threat Intelligence:

- **Objective:** Enhance playbooks with real-time threat intelligence.
- **Action:**
  - Integrate threat intelligence feeds to enrich incident context.
  - Define actions based on threat intelligence indicators.

10. Continuous Improvement:

- **Objective:** Facilitate ongoing refinement and improvement of playbooks.

- **Action:** - Establish a feedback loop for analysts to provide input. - Regularly review and update playbooks based on lessons learned and changes in the threat landscape.

11. Training and Documentation:

- **Objective:** Ensure that analysts are well-trained on playbook usage.

- **Action:** - Develop comprehensive documentation for each playbook. - Conduct regular training sessions for SOC analysts.

12. Test Playbooks Regularly:

- **Objective:** Validate the effectiveness of playbooks through regular testing.

- **Action:** - Conduct tabletop exercises to simulate real-world scenarios. - Evaluate the efficiency of playbooks and identify areas for improvement.

13. Compliance and Reporting:

- **Objective:** Incorporate compliance requirements into playbooks.

- **Action:** - Ensure that playbooks adhere to regulatory and compliance standards. - Implement reporting mechanisms for audit trails.

14. Cross-Functional Collaboration:

- **Objective:** Encourage collaboration between different teams within the organization.

- **Action:** - Include communication and collaboration steps within playbooks. - Foster a culture of information sharing and teamwork.

15. Regular Review and Update:

- **Objective:** Keep playbooks up-to-date with evolving threats and technologies.

- **Action:** - Establish a periodic review process for playbooks. - Update playbooks based on changes in the threat landscape or organizational structure.

By following these steps, with the SOC manager's help, team players can develop playbooks that enhance the efficiency of their incident response processes and contribute to a more resilient cybersecurity posture.

Security Automation

To improve the incident response process, the security automation team implements automation opportunities using automation tools that they own and maintain. The security automation function needs to know the incident response process well and figure out where automation can make the response more accurate and faster overall.

Before investing in automation, the return on investment (ROI) is always important. The ongoing cost of maintenance and support should be carefully considered when doing a ROI analysis. Use cases that can be automated more often should be given priority during automation development. This improvement will pay up for a long time, and in 3 to 5 years' time, the SOC maturity will be higher and from detection to incident response time will be much decreased, and over a year these savings will be very significant. In most cases, the DevSecOps team will be doing the automations.

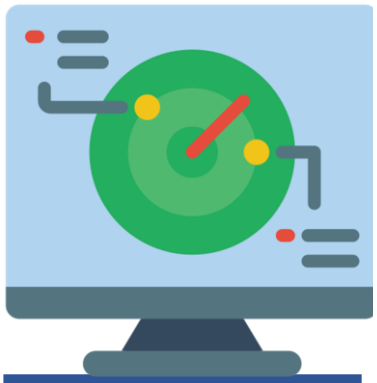
How SOC Handles an Ongoing Attack

A Security Operations Center (SOC) follows a structured process to handle an ongoing attack. Here are the typical steps involved:

1. **Incident Identification**: The SOC identifies the incident by monitoring systems and analyzing alerts.

2. **Incident Triage**: SOC analysts determine the severity of the incident and prioritize it accordingly.
3. **Incident Investigation**: The SOC team investigates the incident to understand its nature and scope. This could involve analyzing logs, network traffic, and other relevant data.
4. **Containment**: The SOC team works to contain the incident to prevent further damage. This could involve isolating affected systems or blocking malicious IP addresses.
5. **Eradication and Recovery**: The SOC team eradicates the threat from the system and recovers the affected systems. This could involve removing malware, patching vulnerabilities, and restoring systems from backups. But if your backups contain malware inside of them, then a sad scenario emerges.
6. **Post-Incident Analysis**: After the incident has been resolved, the SOC team conducts a post-incident analysis to understand what happened, why it happened, and how similar incidents can be prevented in the future.
7. **Communication**: Throughout the incident response process, the SOC team communicates with relevant stakeholders, including management, employees, and possibly customers.

These steps help ensure that incidents are handled effectively and efficiently, minimizing the impact on the organization.

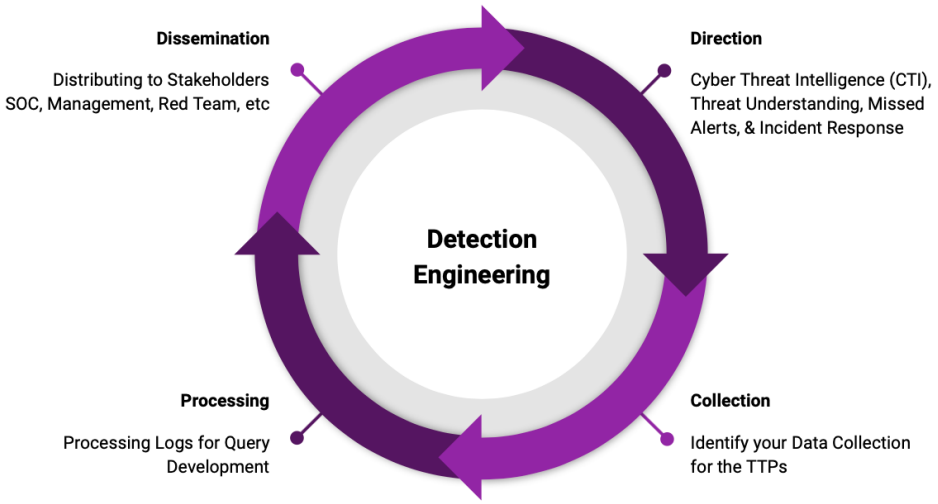


CHAPTER 13

Process of Detection Engineering

AGAIN, COMES THE REFERENCE ARCHITECTURE THAT'S PRE-FABRICATED TO ESTABLISH SUPPORTABILITY, INDEXING, PARSING, SEARCH CONCURRENCY ETC.

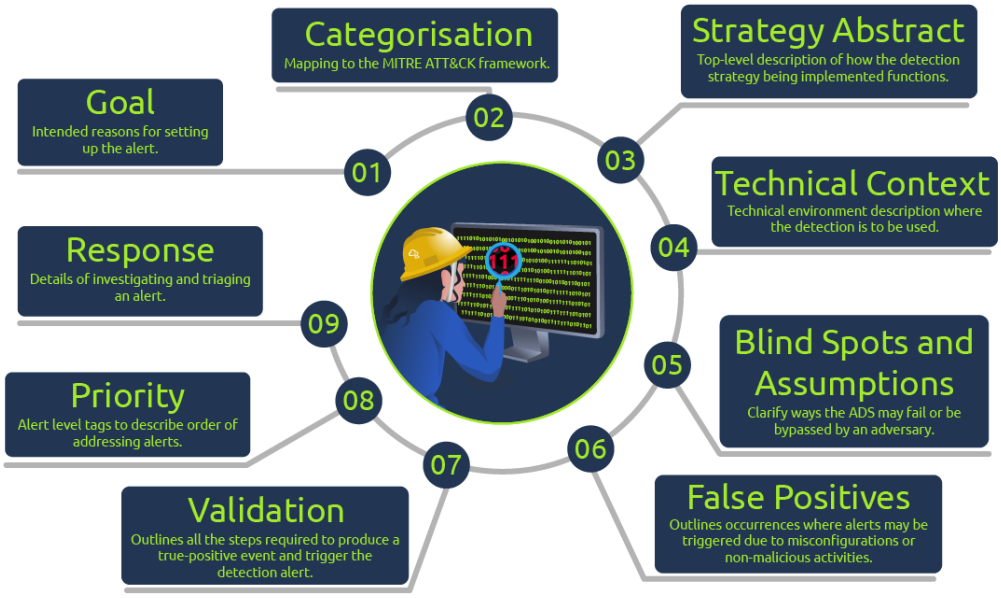
Detection Engineering (DE) is a crucial aspect of a Security Operations Center (SOC). It involves designing, developing, testing, and maintaining threat detection logic. This threat detection logic can be a rule, a pattern, or even a textual description. The scope of DE is wide and works in multiple dimensions, from risk management to threat intelligence.



Source: [Purple Teaming and Threat-Informed Detection Engineering | SANS Blog]

At first the data is collected and correlated by types by SIEM, and SIEM provides the case data to the event management services. All TTPs and IoC data collected and provided within the case. Red team then looks out for actual telemetry data, maps the hash to relevant data sources and confirms the event which can then move to the blue team or to the IR team. In most cases, the internal system flaw that detected the vulnerability, sent out to the server or the application management admin team for resolving the detected issue.

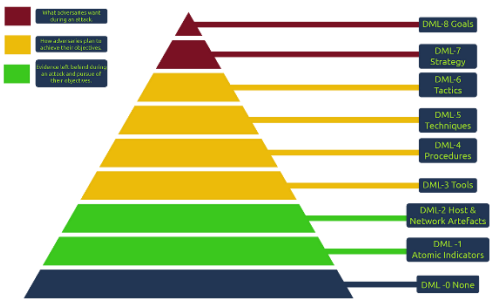
In most cases false positives are minimized by fine tuning the playbooks or the runbooks as they are well known by the team. By letting SIEM know that these data should not be generated in the future. But the catch is, 2/3 out of a 100 events, these may be the RCA for a cause that they are continuously been flagged, and if they come across continuously, these events then be looked into seriously.



Source: [TryHackMe — Intro to Detection Engineering — Walkthrough | by Hamza Anjum | Medium]

Detection Maturity Level Model

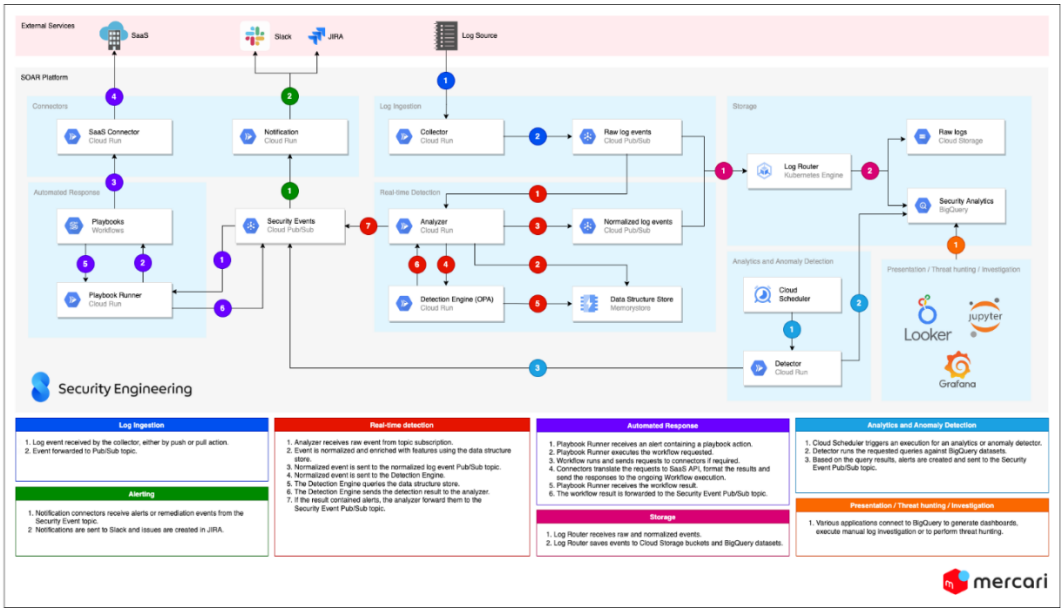
The DML model comprises nine dedicated maturity levels, numbered from 0 to 8, with the lowest value representing technical aspects of an attack and the highest level representing abstract and intelligence-based aspects of an attack. The image from the THM platform describes at which level we achieve what kind of detection.



Source: [TryHackMe — Intro to Detection Engineering — Walkthrough | by Hamza Anjum | Medium]

The goal of detection engineering is to create an automated system of threat detection which is customizable, flexible, repeatable, and produces high-quality alerts for security teams to act upon. It's about developing an environment inside an organization where several teams collaborate to address risks and target potential threats better.

One of the important concepts of detection engineering is Detection-as-Code (DaC). Essentially, DaC means that detection will involve the best implementation practices of software engineering by using the modern agile CI/CD (continuous integration and continuous delivery) pipeline.



Source: [Detection Engineering and SOAR at Mercari | Mercari Engineering]

Benefits of Detection Engineering

- **Dynamic threat identification**: Advanced techniques and tactics help detection engineers to identify risks at an early stage of the attack lifecycle. It discovers dynamic and sophisticated threats in real time.
- **Improved incident response**: Activities related to incident response are made easier by automation and adaptability employed in detection engineering.

Quicker response times are made possible by automated systems that can quickly analyze and prioritize security events.

In a SOC, the first tier is SOC-I Engineers. They are responsible for detecting, identifying, and troubleshooting security events that come in. Their main functions are detection, classification, and escalation of attacks. Thus, detection engineering plays a vital role in the functioning of a SOC. It helps in the early detection of threats, thereby enabling the SOC to respond effectively and efficiently to security incidents.

Detection Engineering vs Threat Hunting

Detection engineering is not a new concept, as it has been used for a long time with systems like Intrusion Detection Systems (IDS). To create detection signatures, analysts, engineers, and researchers would spend a lot of resources on analyzing logs and network traffic. However, Detection engineering has evolved over time. In addition to automated detections for atomic indicators, such as IP addresses and domains, modern detection engineering also uses indicators based on the tools and behaviors of threat actors (TTPs).

Detections go through several stages before they result in signals of malicious activity, also known as rules or alerts. These efforts focus on known indicators or behavior and aim to generate signals that will capture malicious activity. The detection engineering process is different from threat hunting. Let's look at some of the aspects of this process. One of the most crucial and time-consuming tasks in detection engineering is handling false positives. False positives can be overwhelming, so some compromises must be made. Another important task is evaluating the current state of detections and adjusting existing rules based on their performance. This could mean lowering the priority of a rule if needed. In this way, Detection engineering has a more structured process. Similar to the development process, rules go through a testing and development phase before they are deployed.

Key Differences:

1. **Threat Awareness:** Detection Engineering focuses on known threats, while Threat Hunting targets unknown threats.
2. **Use of Infrastructure:** Both use existing security tools, but Detection Engineering enhances detection mechanisms, while Threat Hunting leverages the tools to seek hidden threats.
3. **Focus:** Detection Engineering centers on detecting specific artifacts or meta-characteristics, whereas Threat Hunting focuses on suspicious behaviors.

4. **Process:** Detection Engineers work on balancing detection with minimizing false positives. Threat Hunting content, however, is written to accommodate non-malicious results that may show suspicious behaviors.
5. **Automation:** Detection content is designed for automation, while Threat Hunting content requires careful interpretation by skilled threat hunters.

Source (Differences): [Detection Engineering vs Threat Hunting: What Are They, Really? (cyborgsecurity.com)]

Pro-Tip

- Bad Queue & Timing problem of the SIEM from detection to generating an alert is an ongoing problem, simply put, the timestamps logs and a timestamp of the local time zones will have a bliss all together, have the detection engine configured in either with UTC or GMT, this will affect your detection rules, if a new one is added. Time stamp on events must be placed automatically.

Evasive Techniques

Attackers use evasive techniques to bypass intrusion detection systems (IDSs). These techniques include (not an exhaustive list):

- Flooding.
- Fragmentation.
- Encryption.
- Obfuscation.
- Packet fragmentation.
- Source routing.
- Source port manipulation.

CHAPTER 14

OSINT Tools and Their Usage

THIS IS WHERE YOUR FOCUS NEEDS MORE ATTENTION AS DATA IS COLLECTED FROM VARIOUS WEB SOURCES WHO PROVIDES THESE DATA, SOMETIMES UNVERIFIED. EVERYONE NEEDS HELP, ASK FOR ONE!

OSINT tools are designed to collect and aggregate important information about a target from various online platforms. These tools are openly accessible and can be used by anyone, but they are primarily used by hackers and security professionals who rely heavily on this information. OSINT, short for Open-Source Intelligence, is the practice of gathering intelligence from publicly available sources and data. Unlike classified information that requires specific access, OSINT relies on accessible data that can be legally obtained without constraints. This includes data from the internet, public records, and news sources.

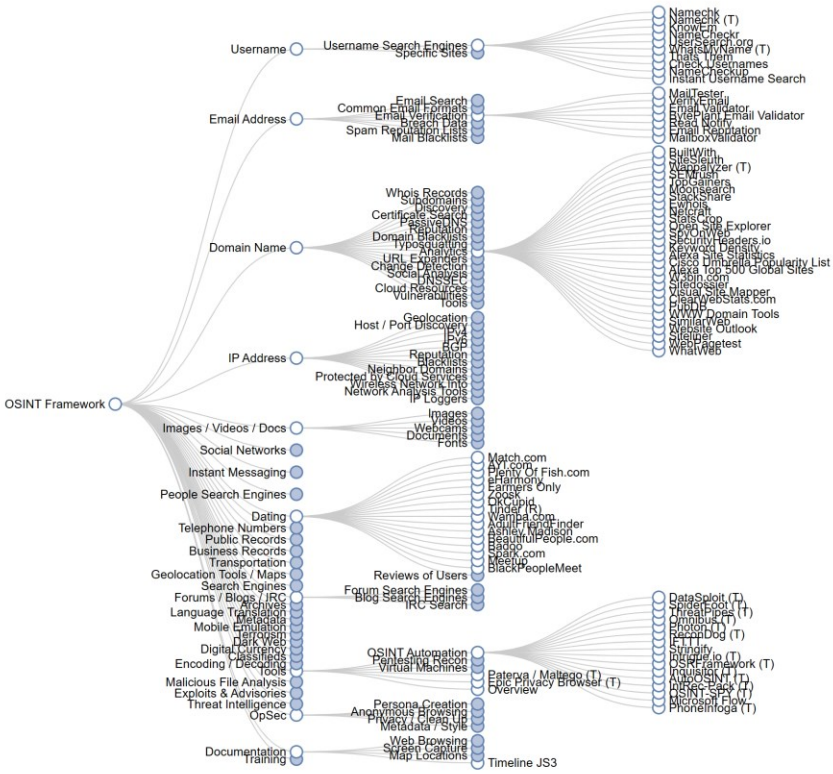
While our focus has been on OSINT tools within the context of our security operations center (SOC), these techniques and tools have diverse applications across various

functions. Penetration testers and bug bounty hunters use them to gather public intelligence on organizations, aiding in prioritizing testing based on exposed technologies and vulnerabilities.

OSINT tools are adaptable for both offensive and defensive purposes, contingent on the user's objectives. Security professionals find great value in OSINT tools for simplifying otherwise laborious tasks. Within SOCs, OSINT tools and methodologies are leveraged to fortify security stance. Common applications of OSINT in cybersecurity encompass external threat analysis, mapping the attack surface, surveying infrastructure, identifying network vulnerabilities, and more.

OSINT Framework

i.e. this mindmap is not fully expanded: click on the link to see the expanded view



Source: OSINT Framework

OSINT is Primary Used for Different Visibilities

1. **Threat Intelligence** — OSINT empowers us to explore the latest hacking methodologies, emerging threats, real-world vulnerabilities, and exploits. This external threat intelligence assists us in enhancing infrastructure security against contemporary attack vectors.
2. **Incident Response** — OSINT aids in swiftly gathering context during security incidents surrounding suspicious indicators such as IP addresses, domains, and file hashes potentially involved in an attack. This expedites incident investigation and response efforts.
3. **Attack Surface Mapping** — Through OSINT utilization, we unveil exposed systems, open ports, utilized technologies, subdomains, and other outward-facing assets. This process enables us to map potential attack surfaces and mitigate associated risks.
4. **Infrastructure Mapping** — OSINT tools provide comprehensive visualization of our entire online infrastructure footprint encompassing cloud providers, domains, networks, and services. Such holistic visibility of assets significantly bolsters security measures.
5. **Breach Assessment** — In scenarios of suspected compromise, OSINT techniques assist in assessing the impact by scouring for organizational data on sale within dark web markets and other public sources.

Most Commonly Used OSINT's

1. Recon-NG
2. Maltego
3. URL Scan
4. SpiderFoot
5. FOCA
6. theHarvester
7. Google Dorks
8. Creepy
9. TweetDeck
10. Mitaka
11. Spyse
12. BuiltWith
13. Intelligence X
14. DarkSearch.io
15. Grep.app
16. Shodan
17. Metagoofil
18. Searchcode
19. Babel X

Differences between open-source intelligence (OSINT) and classified intelligence:

1. **Nature and Accessibility**:
    - **Open-Source Intelligence (OSINT)**:

        - **Nature**: OSINT refers to information collected from publicly available sources. These sources include news articles, social media, websites, academic papers, and other openly accessible data.
        - **Accessibility**: OSINT is openly available to anyone without the need for special clearances or permissions.
    - **Classified Intelligence**:
        - **Nature**: Classified intelligence involves sensitive information that is not publicly accessible. It includes data related to national security, military operations, and other confidential matters.
        - **Accessibility**: Classified intelligence is restricted and accessible only to authorized personnel with appropriate security clearances.
2. **Collection Methods**:
    - **OSINT**:
        - Collected from open sources such as websites, social media platforms, and public records.
        - Techniques include web scraping, data mining, and analysis of publicly available information.
    - **Classified Intelligence**:
        - Gathered through specialized channels, covert operations, and classified sources.
        - Requires specialized training and access to secure databases.
3. **Purpose and Use**:
    - **OSINT**:
        - Used for situational awareness, threat assessment, and understanding public sentiment.
        - Supports decision-making in various domains, including business, law enforcement, and cybersecurity.
    - **Classified Intelligence**:
        - Supports national security, military operations, and strategic planning.
        - Provides insights into adversary capabilities, intentions, and vulnerabilities.
4. **Handling and Security**:
    - **OSINT**:
        - Generally unclassified and does not require strict handling procedures.
        - However, ethical considerations are essential to avoid privacy violations.
    - **Classified Intelligence**:
        - Requires rigorous security protocols.

        - Classified information is compartmentalized, encrypted, and protected to prevent unauthorized access.

5. **Examples**:
    - **OSINT**:
        - Monitoring social media trends during a crisis.
        - Analyzing news articles to track geopolitical developments.
    - **Classified Intelligence**:
        - Intercepted communications between foreign entities.
        - Satellite imagery revealing military installations.

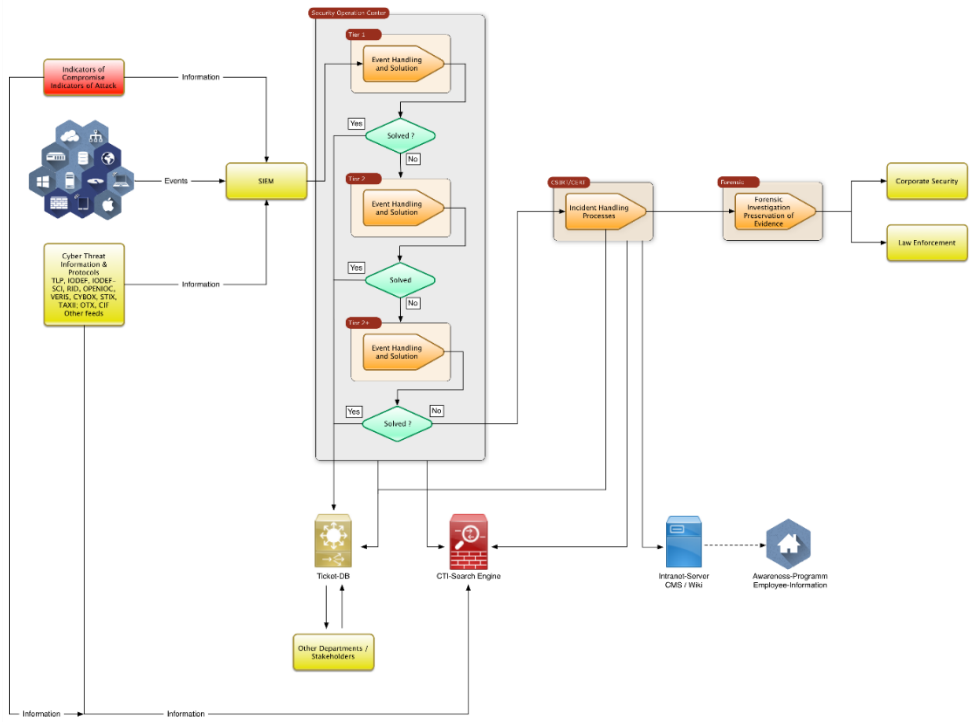
CHAPTER 15

SOC and CSIRT, Better Together

A SIEM IS BETTER COUPLED TOGETHER WITH SOAR, THAT WE HAVE COVERED FOR BETTER DATA COMPOSITION & CASE MANAGEMENT, AND CSIRT FULFILLS INCIDENT RESPONSE MANAGEMENT TO THE RESPONDER, WITH INTEGRATED OSINT.

A Security Operations Center (SOC) and a Computer Security Incident Response Team (CSIRT) are two key components of an organization's cybersecurity infrastructure. They work together to ensure the security of the organization's information systems.

The SOC is responsible for the detection and prevention of cyberattacks on an organization. It is a centralized function that actively monitors the organization's networks, servers, and other IT structures for potential threats. When a security incident is detected, the SOC performs initial analysis and passes the incident to the CSIRT.



Source: SOC-CSIRT Workflow - SecureGlobal

The CSIRT, on the other hand, is a multi-functional team that responds to security incidents. It can be an ad hoc group that comes together when a security incident occurs, or it can be a more established group with a recognized membership that immediately knows its responsibilities when an incident occurs. The CSIRT is activated if the SOC requires help with additional analysis.

There are also documents available on how to develop and integrate CSIRT in your SOC by ENISA @ How to set up CSIRT and SOC — ENISA (europa.eu) and their assessment maturity level for CSIRT is located @ SIM3v2i self-assessment tool — ENISA (europa.eu). other sites for CSIRT:

- insights.sei.cmu.edu

FIRST Services Framework – Typical CSIRT Services

Source: How to set up CSIRT and SOC — ENISA (europa.eu)
Another good resource center for CSIRT: Resources for Creating a CSIRT (cmu.edu)

Current Maturity Level

Info-table view: This table is updated in real-time. You can click on any ID to navigate to it in the web version, link provided above (SIM3v2i self-assessment tool — ENISA (europa.eu)).

ID	Title	Maturity	Relative to Basic	Basic	Intermediate	Advanced
O-1	Mandate	0	Improvement needed	3	4	4
O-2	Constituency	0	Improvement needed	3	4	4
O-3	Authority	0	Improvement needed	3	4	4
O-4	Responsibility	0	Improvement needed	3	4	4
O-5	Service Description	0	Improvement needed	3	4	4

O-6	Public Media Policy	0	Improvement needed	2	3	4
O-7	Service Level Description	0	Improvement needed	3	4	4
O-8	Incident Classification	0	Improvement needed	2	3	3
O-9	Participation in CSIRT Systems	0	Improvement needed	3	4	4
O-10	Organisational Framework	0	Improvement needed	3	3	3
O-11	Security Policy	0	Improvement needed	2	3	4
H-1	Code of Conduct/Practice/Ethics	0	Improvement needed	2	3	3
H-2	Staff Resilience	0	Improvement needed	2	3	4
H-3	Skillset Description	0	Improvement needed	2	2	3
H-4	Staff Development	0	Improvement needed	2	3	4
H-5	Technical Training	0	Improvement needed	1	2	3
H-6	Soft Skills Training	0	Improvement needed	1	2	3
H-7	External Networking	0	Improvement needed	2	3	3
T-1	IT Assets & Configuration	0	Improvement needed	1	2	3
T-2	Information Sources List	0	Improvement needed	2	3	4
T-3	Consolidated Messaging System(s)	0	Improvement needed	2	3	3
T-4	Incident Tracking System	0	Improvement needed	2	3	3
T-5	Resilient Voice Calls	0	Improvement needed	2	3	3

T-6	Resilient Messaging	0	Improvement needed	2	3	3
T-7	Resilient Internet Access	0	Improvement needed	2	3	3
T-8	Incident Prevention Toolset	0	Improvement needed	2	2	3
T-9	Incident Detection Toolset	0	Improvement needed	2	3	3
T-10	Incident Resolution Toolset	0	Improvement needed	2	3	3
P-1	Escalation to Governance Level	0	Improvement needed	3	4	4
P-2	Escalation to Press Function	0	Improvement needed	2	3	3
P-3	Escalation to Legal Function	0	Improvement needed	2	3	3
P-4	Incident Prevention Process	0	Improvement needed	2	3	4
P-5	Incident Detection Process	0	Improvement needed	2	3	4
P-6	Incident Resolution Process	0	Improvement needed	2	3	4
P-7	Specific Incident Processes	0	Improvement needed	2	3	4
P-8	Audit & Feedback Process	0	Improvement needed	3	4	4
P-9	Emergency Reachability Process	0	Improvement needed	2	3	3
P-10	Best Practice Internet Presence	0	Improvement needed	2	3	3
P-11	Secure Information Handling Process	0	Improvement needed	2	3	3
P-12	Information Sources Process	0	Improvement needed	2	3	4
P-13	Outreach Process	0	Improvement needed	2	3	4

P-14	Governance Reporting Process	0	Improvement needed	3	4	4
P-15	Constituency Reporting Process	0	Improvement needed	2	3	3
P-16	Meeting Process	0	Improvement needed	2	2	3
P-17	Peers Collaboration Process	0	Improvement needed	2	3	4

The CSIRT performs three main tasks:

1. Receives information on a security breach.
2. Analyzes it.
3. Responds to the sender.

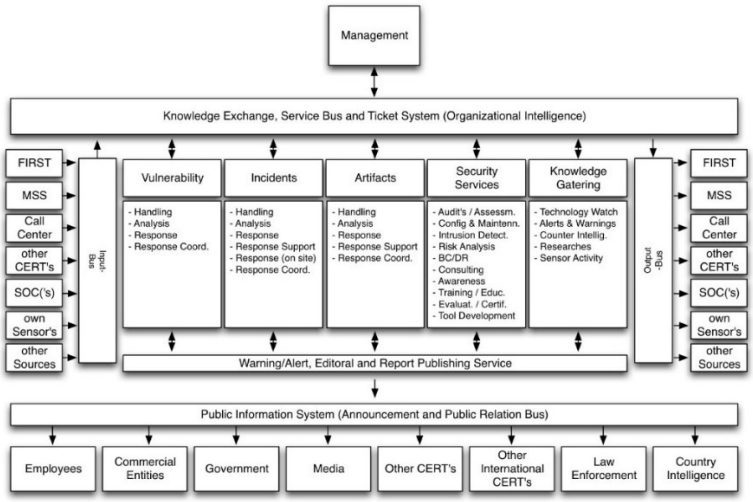
In addition to these tasks, CSIRTs may also support SOCs by:

- Reviewing standard security arrangements.
- Managing audits and training for new threats.
- Investigating new vulnerabilities and sharing the latest industry-level responses.
- Liaising with different internal and external stakeholders when an incident occurs.
- Managing remotely-stored critical information (passwords, network configs, etc.) in an emergency.

- A CSIRT consists of 5 pillars, which represent the basic activities.

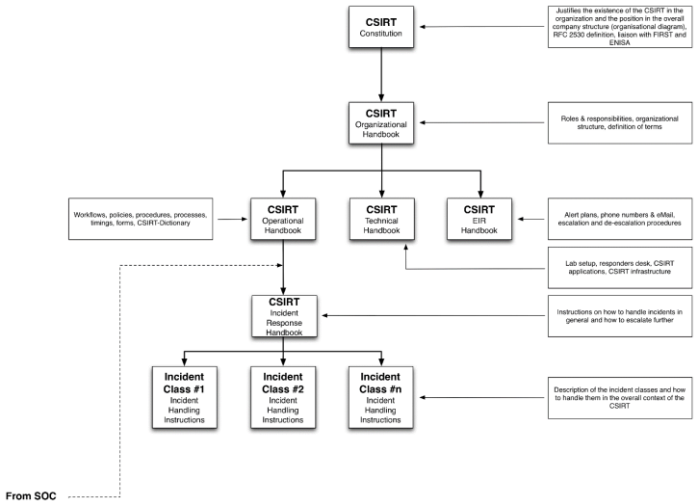
Basisaktivität (Säule)	Services
Vulnerability	- Handling - Analysis - Response - Response Coordination
Incident	- Handling - Analysis - Response Support - Response (On-Site) - Response Coordination
Artifact	- Handling - Analysis - Response - Response Support - Response Coordination
Security Services	- Audits and Assessments - Configuration & Management - Intrusion Detection - Risk Analysis - Business Continuity, Disaster Recovery - Consulting - Awareness - Training / Education - Evaluation / Certification - Tool Development
Knowledge Gathering	- Technology Watch - Alerts & Warnings - Counter Intelligence - Researches - Sensor Activity

5 CSIRT Pillars



Source: [The CSIRT methodology - SecureGlobal]

CSIRT Documentation Framework



Source: The CSIRT methodology - SecureGlobal

In essence, while the SOC is focused on proactive monitoring and detection, the CSIRT is reactive, responding to incidents as they occur. Both teams work closely together, with the SOC acting as a front end for the CSIRT. This collaboration ensures a comprehensive approach to cybersecurity, enhancing the organization's ability to prevent, detect, and respond to cyber threats.

CHAPTER 16

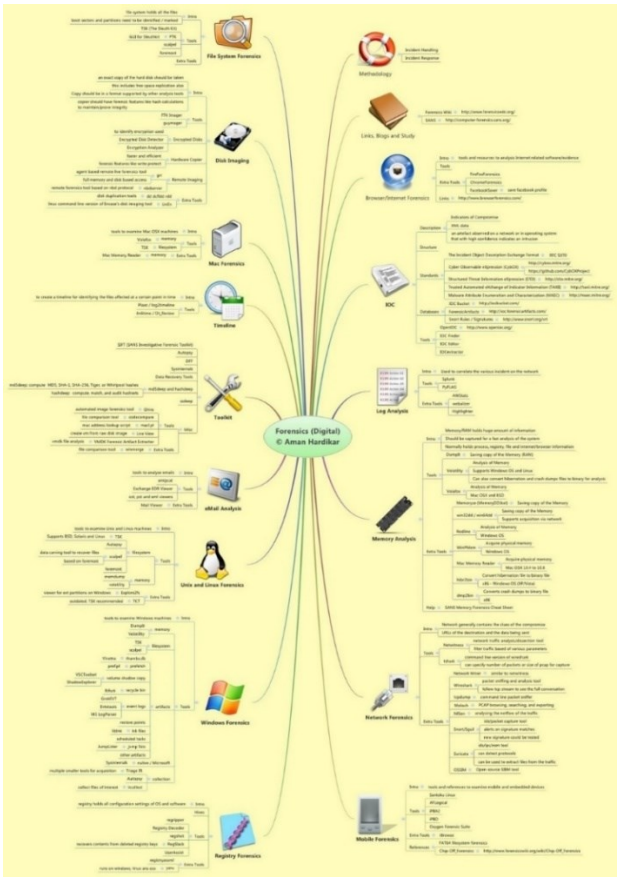
Digital Forensics and Incident Response (DFIR)

TRACING BACK WHAT HAPPENED DURING A BREACH, OR AN EARLY DETECTION OF BREACH IS WHAT YOU ARE GETTING TRAINED FOR IN YOUR DOMAIN AND IN YOUR SPACE. YOUR FINDINGS WILL BE ULTIMATUM TO THE ABUSER AS ELECTRONIC EVIDENCE ARE PRODUCED.

DFIR stands for Digital Forensics and Incident Response. It is a field within cybersecurity that focuses on the identification, investigation, and remediation of cyberattacks. DFIR has two main components: Digital Forensics and Incident Response. Digital Forensics is a subset of forensic science that examines system data, user activity, and other pieces of digital evidence to determine if an attack is in progress and who may be behind the

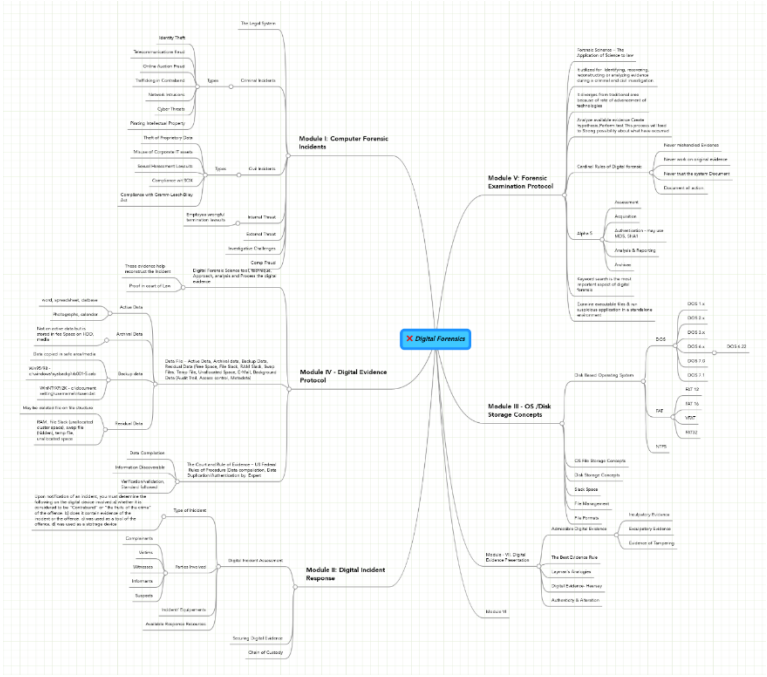
activity. Incident Response is the overarching process that an organization will follow in order to prepare for, detect, contain, and recover from a data breach. DFIR has become a central capability within the organization's security strategy and threat hunting capabilities due to the proliferation of endpoints and an escalation of cybersecurity attacks in general. The shift to the cloud, as well as the acceleration of remote-based work, has further heightened the need for organizations to ensure protection from a wide variety of threats across all devices that are connected to the network. Though DFIR is traditionally a reactive security function, sophisticated tooling and advanced technology, such as artificial intelligence (AI) and machine learning (ML), have enabled some organizations to leverage DFIR activity to influence and inform preventative measures. In such cases, DFIR can also be considered a component within the proactive security strategy.

Digital Forensic Mindmap



Source: [(scoop.it)]

Another Mindmap of DFIR



Source: [Digital Forensics - MindMeister Mind Map]

How is Digital Forensics Used in the Incident Response Plan

Digital forensics provides the necessary information and evidence that the computer emergency response team (CERT) or computer security incident response team (CSIRT) needs to respond to a security incident.

Digital forensics may include:

- **File System Forensics:** Analyzing file systems within the endpoint for signs of compromise.
- **Memory Forensics:** Analyzing memory for attack indicators that may not appear within the file system.
- **Network Forensics:** Reviewing network activity, including emailing, messaging and web browsing, to identify an attack, understand the cybercriminal's attack techniques and gauge the scope of the incident.

- **Log Analysis:** Reviewing and interpreting activity records or logs to identify suspicious activity or anomalous events.

The Value of Integrated Digital Forensics and Incident Response (DFIR)

While digital forensics and incident response are two distinct functions, they are closely related and, in some ways, interdependent. Taking an integrated approach to DFIR provides organizations with several important advantages, including the ability to:

- **Respond** to incidents with speed and precision
- **Follow** a consistent process when investigating and evaluating incidents
- **Minimize** data loss or theft, as well as reputational harm, as a result of a cybersecurity attack
- **Strengthen** existing security protocols and procedures through a more complete understanding of the threat landscape and existing risks
- **Recover** from security events more quickly and with limited disruption to business operations
- **Assist** in the prosecution of the threat actor through evidence and documentation

Source: [Digital Forensics and Incident Response (DFIR) - CrowdStrike]

Types of Forensics

- **File system forensics:** File system forensics is a subset of digital forensics. The process allows us to analyze machines on the data storage level, which usually includes remote devices.
- **Memory forensics:** Memory forensics helps analyze volatile forms of evidence like system memory and detect signs of malware, even when traditional protection mechanisms like an antivirus don't find anything.
- **Network forensics:** Network forensics is the process of investigating what happens in a digital network. Did an infection originate from an email or link? Understanding this process can be helpful, as it's one that digital forensics experts encounter regularly.
- **Malware triage:** The malware triage service is designed to help DFIR teams identify particular malware strains and better address the damage it causes.
- **Log analysis:** Log analysis is a valuable skill for identifying abnormal activity happening on a system. Automating this task saves time, but you'll want to ensure that your log analysis software is reliable and accurate.

- **Software development:** Software development and technology change rapidly, so staying up to date with trends is essential for DFIR teams. Being able to code and script can be a huge asset.
- **Communication:** How you communicate with team members, other organizations, and management can often determine how successful an incident response is.
- **Analytical thinking:** Analytical thinking is a challenging but essential skill for DFIRs. It takes focus to gather relevant information and challenge your assumptions before testing them out. Even if you're three steps ahead, it's worth slowing down to reflect on analytical thinking.
- **Teamwork:** It's important to remember that incident response is a high-stakes experience, and team members must know how to work together as a cohesive unit. It takes commitment, communication, and responsibility to succeed.

DFIR Timeline Generator

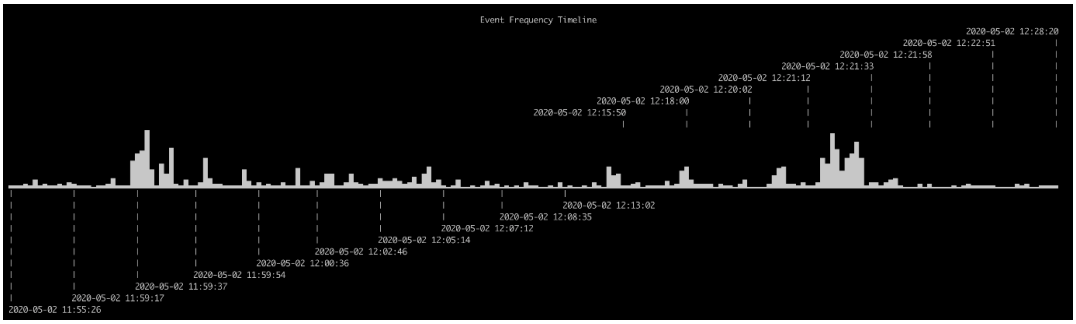
A Free Threat Hunting Tool and Fast Forensics Timeline Generator.

Timeline analysis involves reviewing events over some time to construct the story of events to look for potential attacks and uncover hidden threats.

It allows us to differentiate routine events from suspicious ones by considering the context and timing of each action.

Hayabusa is a sigma-based threat hunting and fast forensics timeline generator for Windows event logs, developed by Yamato Security group:

- Cross-platform: Works on Windows, Linux, macOS.
- Simplified forensic timelines.
- Converts Sigma rules to Hayabusa rules.
- MITRE ATT&CK tactics mapping.
- Evtx record carving from slack space.
- Parses and extracts from PowerShell classic logs.
- Multi-threaded for up to 5x speed boost.



Source: [GitHub - Yamato-Security/hayabusa: Hayabusa (隼) is a sigma-based threat hunting and fast forensics timeline generator for Windows event logs.]

CVE, CVSS, NVD, KEV

CVE (Common Vulnerabilities and Exposure) is the largest repository which enlists product-wise vulnerabilities which are publicly disclosed, and each vulnerability is allotted a unique alphanumeric number that corresponds to the product's identified vulnerability. Later on, these CVE numbers are cataloged per product.

You should also know that CVE is sponsored by the U.S. Department of Homeland Security (DHS) and Cybersecurity and Infrastructure Security Agency (CISA)

Historically MITRE hosted the CVE site https://cve.mitre.org/ and the registered owner of the CVE list and the CVE logo, which were the originally popular amongst security analysts, and now the new site (https://www.cve.org/) has been launched, where you still can search of CVE's for products.

Operating under the authority of the CVE Program, "CNAs" (CVE Numbering Authorities) are organizations that are authorized to assign CVE IDs to vulnerabilities affecting products within their distinct, agreed upon scope, for inclusion in first-time public announcements of new vulnerabilities. These CVE IDs are provided to researchers, vulnerability discoverers or reporters, and information technology vendors.

The CVSS specifications are owned and managed by FIRST.Org, Inc. (FIRST), a US-based non-profit organization, whose mission is to help computer security incident response teams across the world. The official CVSS documentation can be found at https://www.first.org/cvss/

NVD (National Vulnerability Database): The NVD (NVD - Home (nist.gov)) is the U.S. government repository of standards-based vulnerability management data represented

using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, product names, and impact metrics. You should know that this is not updated to the same frequency as CVSS or CVE.

CVEShield provides additional insights, such as:

- **V-Score**: Estimates the likelihood of a vulnerability being exploited by threat actors. By incorporating a range of open-source data sources including NVD, MITRE, CISA KEV (Known Exploited Vulnerability), and social media.
- **E-Score**: Evaluates the probability of a software vulnerability being exploited in the wild.
- **CVSS Score**: A standardized vulnerability severity rating
- **Description**: A brief summary of each vulnerability for quick insight.

You can check it out from the link: CVEShield

CHAPTER 17

Continuous Threat Exposure Management - CTEM

SCENARIO DEMANDS FOR EARLY NOTIFICATIONS FROM SOC, AS VULNERABILITIES CHANGES STATES TO DIFFERENT DEVICE CONFIGURATIONS. SOC ALSO MONITORS COMPROMISED TYPES AND LOCATES SOURCES, MERGES DATA FROM OSINT, DETECTION ENGINEERING DATA, ALONG WITH YOUR DFIR DATA INTO A ONE GIANT CASE FILE FOR 1 SINGLE EVENT.

Continuous Threat Exposure Management (CTEM) is a cybersecurity process that leverages attack simulations to identify and mitigate threats to an organization's

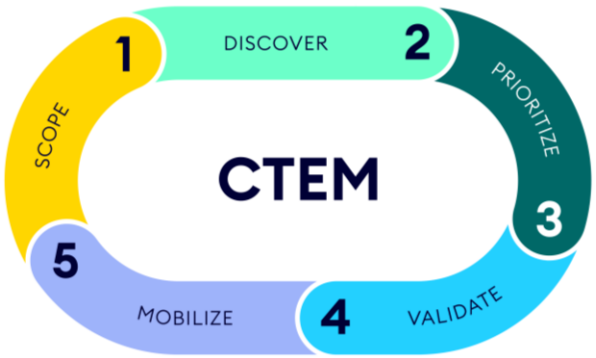
networks and systems. This allows organizations to test their security posture and identify vulnerabilities before they are exploited by real attackers.

CTEM consists of five stages: scoping, discovery, prioritization, validation, and remediation. The goal of CTEM is to establish well-defined security and risk management strategies that align with business objectives and reduce the attack surface of the enterprise.

CTEM is a forward-thinking framework that goes beyond traditional vulnerability management methods by actively and regularly identifying, assessing, monitoring, and reducing security weaknesses in an organization's infrastructure. CTEM also promotes collaboration among all stakeholders, including IT operations, governance, risk, compliance, and asset owners.

In another perspective from XM Cyber (very detailed explanation from them – click on the picture source link to see details), their perspective is as follows, only change observed for the number 5 and that's to "Mobilize" in reference to Gartner:

Source: CTEM | XM Cyber



How is CTEM Different from Cloud Security Posture Management (CSPM)?

CTEM and CSPM are both cloud security technologies that help organizations identify and mitigate risks in their cloud environments. However, they focus on different aspects of cloud security:

- CTEM is mainly concerned with **attack simulations** that test the security posture and resilience of the cloud infrastructure against various threat scenarios. CTEM helps organizations find and fix vulnerabilities before they are exploited by real attackers.
- CSPM is mainly concerned with **configuration management** that monitors and assesses the compliance and risk of various cloud services and settings. CSPM

helps organizations detect and remediate misconfigurations that expose cloud resources to potential breaches.

Both CTEM and CSPM complement each other by addressing different attack surfaces and providing different insights into the cloud security posture. Some of the key benefits of using both CTEM and CSPM are:

- Improved visibility and control over cloud assets and services
- Enhanced detection and prevention of cloud-based attacks
- Reduced attack surface and exposure to threats
- Increased compliance with security standards and regulations
- Optimized cloud security performance and efficiency

Security and risk management leaders should aim for visibility into exposures and attract the interest of other senior leaders byctem highlighting the issues with the most potential impact on an organization's critical operations. They should define a narrower scope for CTEM, aligned with business objectives, using familiar language, and explaining the impact on the business, not technology.

As part of a CTEM plan, security leaders should expand communication with other department heads, asset owners and third parties to have clear paths to mobilize responses and remediations. They should also get traction with business departments and asset owners by clearly articulating and discussing the residual risk associated with the postponement of remediation efforts, offering short-term and long-term options to reduce or eliminate exposure.

If you want to learn more about CTEM and CSPM, you can check out these articles:

- CSPM Vs. CIEM: Demystifying Two Popular Cloud Security Acronyms
- CIEM vs CSPM: Which is Better for Reducing Public Cloud Risk?
- CIEM vs CSPM
- Real Life Use Cases CIEM vs CWPP vs CSPM
- CIEM vs CSPM: Which Is the Right Solution for Your Cloud?

Readiness Requirements to Implement CTEM and CSPM

Implementing CTEM and CSPM in your organization requires a strategic and collaborative approach that involves various stakeholders, tools, and processes. Here are some general steps that you can follow to get started:

- Define your scope and objectives: Identify your business-critical assets, services, and settings that need to be protected and monitored in the cloud. Align your security goals with your business priorities and compliance requirements.
- Choose your tools and platforms: Select the appropriate CTEM and CSPM solutions that suit your cloud environment and security needs. You can use a combination of tools that provide different functionalities, such as attack simulation, configuration monitoring, vulnerability scanning, risk assessment, and remediation automation.
- Establish your workflows and policies: Define your roles and responsibilities, communication channels, reporting mechanisms, and escalation procedures for managing and responding to cloud security issues. Establish clear and consistent policies and standards for configuring and securing your cloud resources and services.
- Execute and monitor your CTEM and CSPM programs: Run regular and continuous tests and scans to identify and prioritize your cloud security exposures. Validate and verify the effectiveness and accuracy of your findings and recommendations. Remediate and resolve the identified issues as soon as possible, following the best practices and guidelines.
- Review and improve your CTEM and CSPM programs: Analyze and measure your cloud security performance and progress over time. Identify and address any gaps, challenges, or opportunities for improvement. Update and refine your scope, objectives, tools, workflows, and policies as needed.

Threat Intelligence Platform for SOC Security

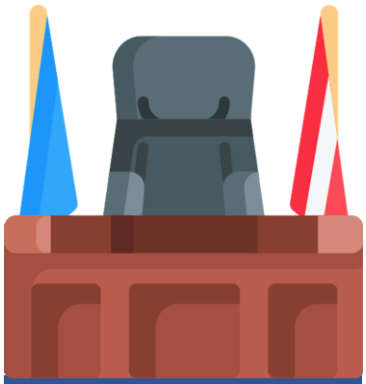
A Threat Intelligence Platform (TIP) is a crucial tool for Security Operations Centers (SOCs). It allows SOC teams to collect, collate, and parse threat data in real-time, enabling security teams to identify and prevent attacks even before they occur. TIPs help security teams better understand the threat landscape as they accumulate and analyze information from various sources.

Here are a few examples of Threat Intelligence Platforms for SOCs:

1. ThreatConnect
2. **SOCRadar® Digital Risk Protection Platform**: This product combines External Attack Surface Management, Digital Risk Protection, and Cyber Threat Intelligence modules to improve your security posture. It provides visibility and context regarding the severity of unknown external-facing digital assets with automated continuous monitoring. It also offers actionable intelligence alerts with instant phishing domain identification, compromised credential and credit card detection.
3. **Recorded Future Intelligence Cloud**: This tool provides real-time intelligence on a wide range of topics, including cybersecurity, geopolitical events, and financial

markets. The platform is user-friendly and easy to navigate with intuitive visualizations that allow users to quickly identify trends and patterns.

4. **ThreatQuotient™ ThreatQ v5**: This platform supports the SOC of the future, where data is the foundation. ThreatQ's newest features include a unique DataLinq Engine for connecting disparate systems and sources to enable extended detection and response (XDR), Smart Collections for driving automation, and an enhanced ThreatQ Data Exchange for bi-directional sharing of data, context, and threat intelligence.



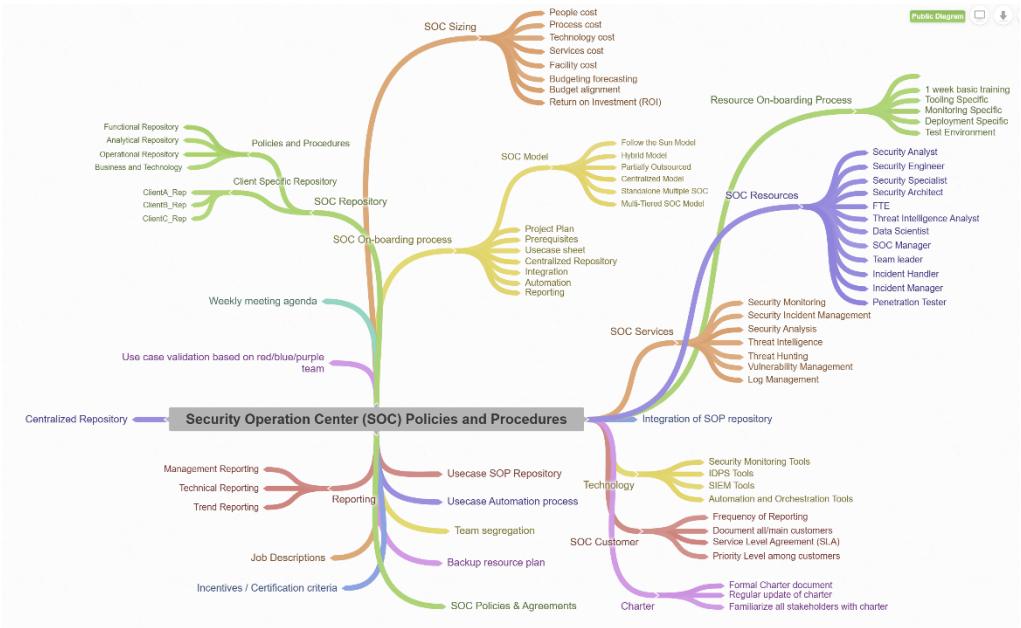
CHAPTER 18

SOC Policies & Processes

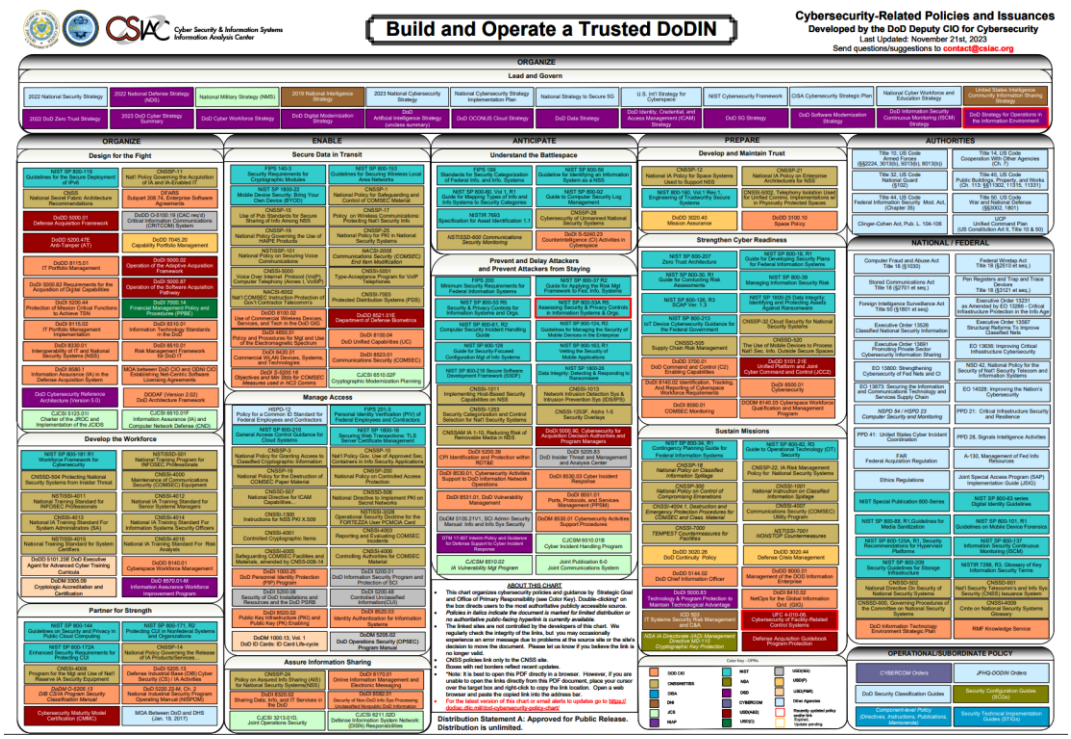
SOME GUIDANCE DOCUMENTATION IS REQUIRED AND MADE A DE-FACTO TO OPERATE THE SOC IN A DESIRED LEVEL OF FUNCTIONALITY. AS HEAVILY INVESTED INTO A SOC, IT IS EXPECTED THAT THE OUTCOME MUST BE PRODUCED IN AN ORDERLY FASHION WITH A RISK MANAGEMENT SCENARIO TO PROTECT AGAINST ANY TYPE OF THREATS.

These are some of the policies, processes and procedures to follow. At some times, security analysts can be seen reacting to these policies as they are already overburdened with too many things to follow these outlines, but it can be slowly injected into the SOC processes, you would want to be creative in applying these controls into the SOC formation, the art of it is that your analysts will become more effective and professional, the downside of this, they will move out even faster. But it's a job nonetheless that you will need to carry out.

The below CSIAC document also outlines some of the best designed governance matrices for a countries cybersecurity governance framework. Each of the boxes are clickable and will land you on a linked page to that respective framework and which has links to relevant resources. This can be too much as well since too many frameworks, processes, policies are interrelated, and tracing those to a map is nearly impossible. But the knowledgebase is worth browsing it, when you require it, for a specific tasks, events, activities or guidelines are needed.

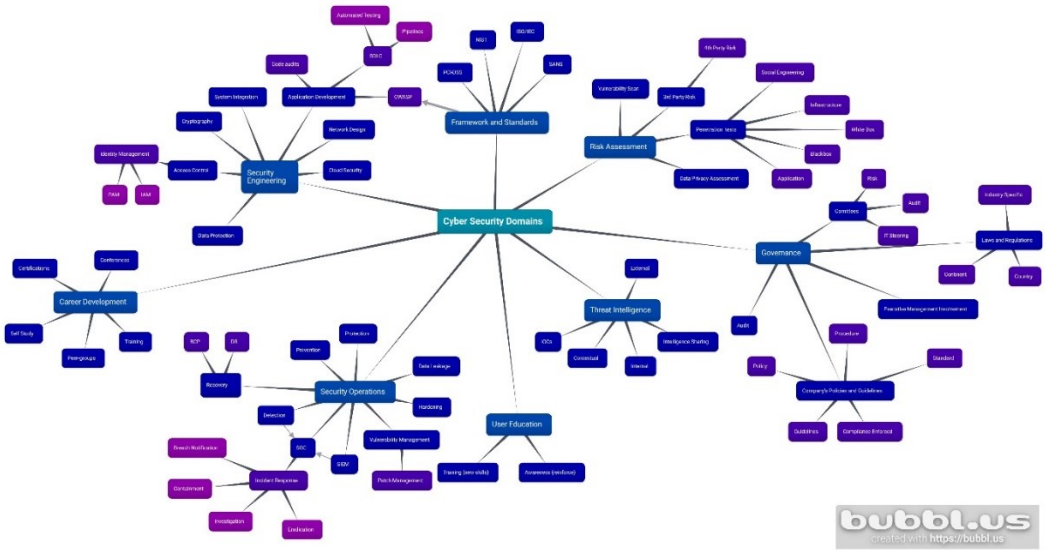


Source: [Security Operation Center (SOC) Policies and Procedures (coggle.it)]



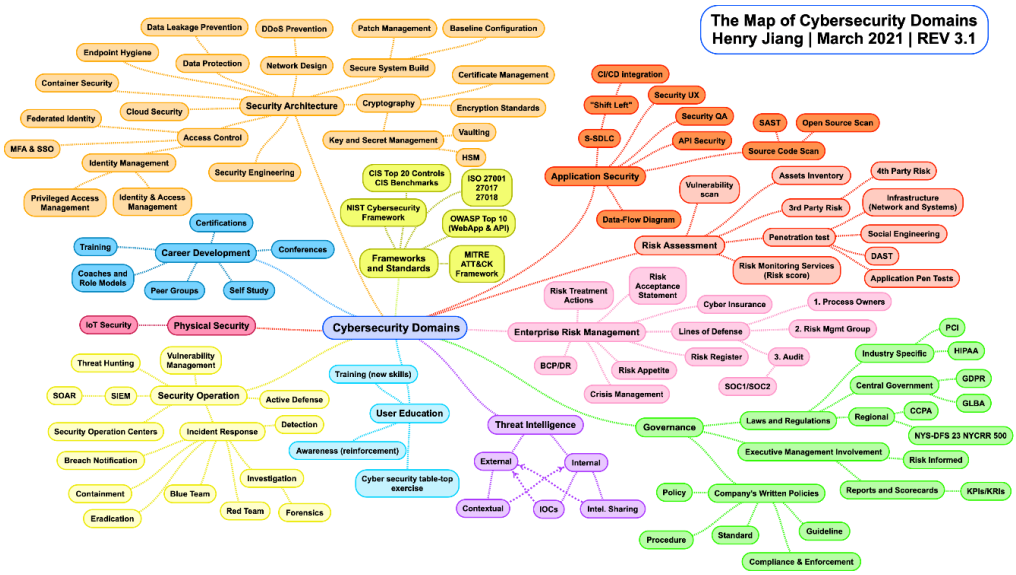
Source: [The DoD Cybersecurity Policy Chart – CSIAC]

Cyber Security Domains



Source: [Bubbl.us - Cyber Security Domains]

Another good mind map here from Henry Jiang:



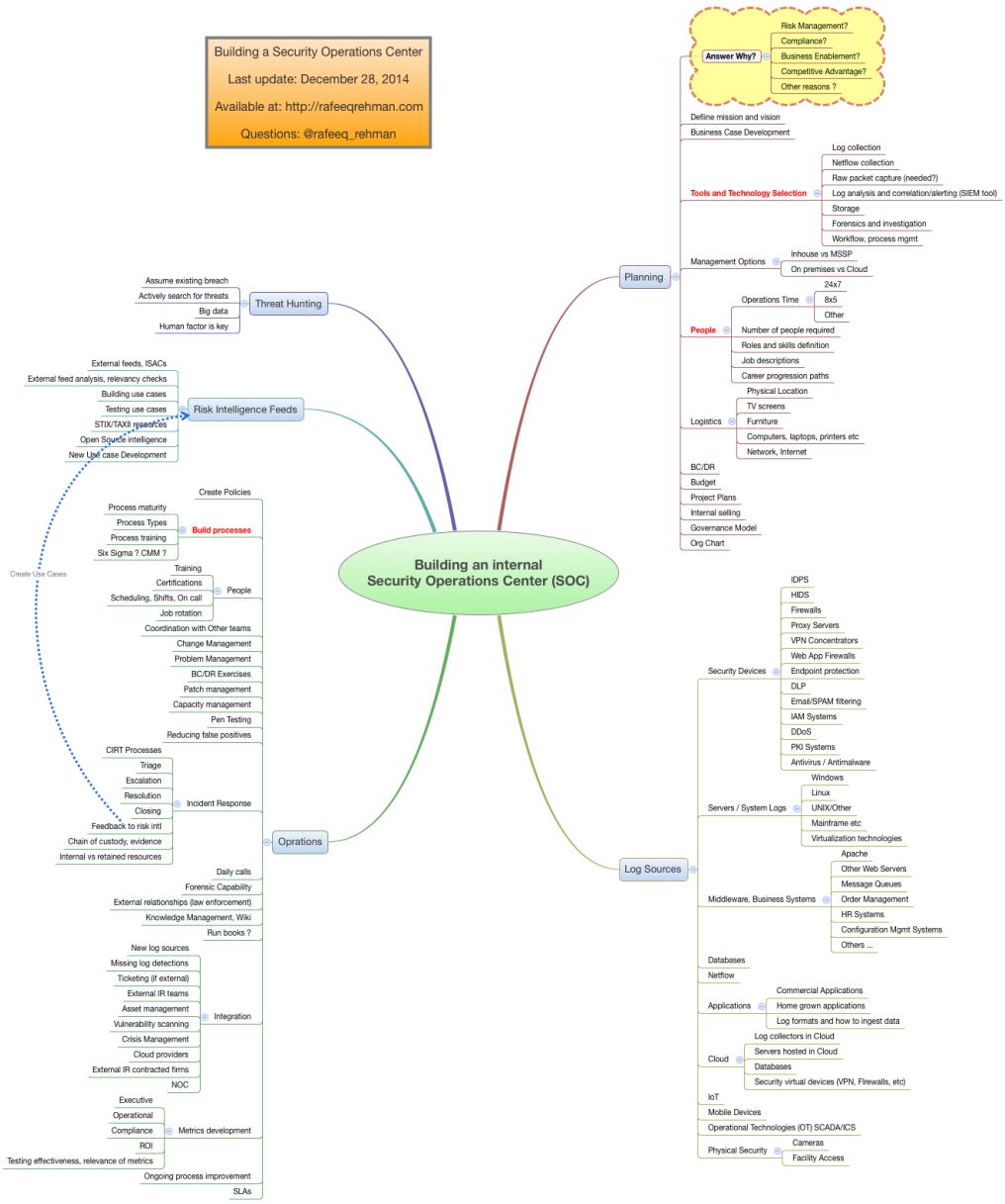
Source: [LinkedIn Share | Powered by Box]

But these are not nearly complete, as you may feel that there are lot of domain missing from the above two pictures. There is also another mindmap you can explore and here is the link: [Cyber Security | MindMeister Mind Map]

Cybersecurity & Data Privacy by Design Principles

As you can see there is no shortage of available frameworks, and it is very easy to get lost around all of them frameworks. But you should know what your infrastructure security level is, what's required, and what are the things to fix. The SCF also aligned some of the critical design principles as well (33 line items, breakdowns you can download from their site, its freely available with an excel worksheet). These are the things for you to know and to figure out how best to fit it in your infrastructure management and therefore, choose a method on how to fix it, by following a framework.

Building a SOC by Rafeeq Rehman



Source: [Building_SOC.png (1366×1602) (rafeeqrehman.com)]

The above picture has the most mentioned domains in one picture, other pictures may be out there, but I haven't come across those yet, but tried to add most mindmaps and shared in the job aids folder as images or mindmeister files.

Rafeeq Rehman also has a CISO mindmap which could be very useful if you are willing to step up your career and want to understand these domains and enrich your understanding, you can download it from here: Rafeeq Rehman | Cyber | Automation | Digital - Rafeeq Rehman - Personal

CHAPTER 19

Generating and Consuming SOC Reports

THIS IS WHERE THE CLARITY OF THE CASE FILES MEETS THE CLOSURE, IF IT'S A FALSE ALARM, IF NOT, THEN THE RCA GETS INTO ACCOUNT, LATER ON REMEDIATED AND THE CASE GETS CLOSED WITH A WEALTH OF INCORPORATED DATA.

Security Operation Center (SOC) reports are documents that provide information and insights on the activities and performance of a SOC, such as the number, type, and severity of security incidents, the time and resources spent on detection and response, and the effectiveness and efficiency of the SOC's tools and processes. SOC reports can help SOC managers and stakeholders to evaluate and improve the SOC's capabilities and maturity, as well as to communicate and demonstrate the value and impact of the SOC to the organization.

Some of the best practices in generating and consuming SOC reports are:

- For SOC managers:
  - Define the purpose, scope, and audience of the SOC report. What are the main objectives and questions that the SOC report aims to address? What are the key metrics and indicators that the SOC report will use to measure and demonstrate the SOC's performance and value? Who are the intended recipients and users of the SOC report, and what are their expectations and needs?
  - Collect and analyze the relevant data and information from the SOC's tools and processes. Use various sources and methods, such as logs, alerts, incidents, tickets, surveys, feedback, and audits, to gather and validate the data and information that will support the SOC report's findings and conclusions. Use appropriate tools and techniques, such as dashboards, charts, graphs, and tables, to visualize and summarize the data and information in a clear and concise manner.
  - Write and format the SOC report in a professional and consistent way. Use a standard template and structure, such as executive summary, introduction, methodology, results, discussion, recommendations, and appendix, to organize and present the SOC report's content and layout. Use clear and concise language, avoid jargon and acronyms, and proofread and edit the SOC report for accuracy, completeness, and readability.
  - Distribute and share the SOC report with the relevant stakeholders and users. Use secure and appropriate channels and formats, such as email, web, or print, to deliver and disseminate the SOC report to the intended recipients and users. Obtain feedback and comments from the stakeholders and users, and address any questions, concerns, or issues that may arise from the SOC report.
- For SOC stakeholders and users:
  - Review and understand the SOC report's purpose, scope, and audience. What are the main objectives and questions that the SOC report aims to address? What are the key metrics and indicators that the SOC report uses to measure and demonstrate the SOC's performance and value? Who are the intended recipients and users of the SOC report, and what are their expectations and needs?
  - Evaluate and verify the SOC report's data and information. How reliable and valid are the data and information that support the SOC report's findings and conclusions? How well do the data and information reflect the actual activities and performance of the SOC? How relevant and

useful are the data and information for the SOC report's purpose and scope?
- Interpret and apply the SOC report's findings and conclusions. What are the main strengths and weaknesses of the SOC's capabilities and maturity? What are the main opportunities and challenges for the SOC's improvement and development? What are the main recommendations and actions that the SOC report suggests for the SOC and the organization?
- Communicate and collaborate with the SOC manager and other stakeholders and users. Provide feedback and comments on the SOC report, and ask questions, raise concerns, or suggest issues that may need further clarification or investigation. Share and discuss the SOC report's findings and conclusions with other stakeholders and users, and align and coordinate the implementation and follow-up of the SOC report's recommendations and actions.

Case Documentation

Case documentation is a complete record of incident response actions, which helps SOC teams use previous experiences and lessons learned to handle incidents better in the future. It also helps team members and stakeholders work together, communicate clearly, and improve continuously by finding areas for process improvement and boosting security operations. By keeping precise and thorough case documentation, SOC teams can improve their incident response skills and defend organizations better from changing cyberthreats by tuning the visibility requirements. Some of the process relations and group activity follows:

Pro-Tip

- when a breach is detected and showing up in the SIEM, DO NOT panic (also shows your fear, and it will spread across your peers), this is what you have been trained for, help out to facilitate, do not engage every available personnel for the incident response

1. Breach detection & alert notification.
2. Red & purple teams' engagement is mostly required in this case.
3. Blue teams' engagement on fine tuning the notification time, visibility increment requirement outline generated, further protection requirements generated and share with the SOC manager.
4. Associated TTP's & IoC's are generated and integrated.

5. Investigation results accumulation.
6. Investigation research accumulation.
7. Pre-approved mitigation criteria.
8. Threat intelligence accumulation & data validation.
9. Severity triage, affected systems, parties, people, data analytics.
10. Review quality of the case documentation.
11. SOC manager – breach response & reporting to the stakeholders.
12. Preventative measures, lessons learned, store KB for future use, possibility of automation for such investigation and remediation process.
13. Document everything, sign-off for closure.

Difference Between TTP and IoC

Though mentioned earlier, TTP stands for **Tactics, Techniques, and Procedures**, which are the strategies and methods used by threat actors to conduct cyberattacks. TTPs focus on the overall behavior and patterns of the attackers, rather than specific artifacts or evidence.

IoC stands for **Indicators of Compromise**, which are observable and verifiable signs that a security incident has occurred or is occurring. IoCs are often derived from specific events or data points observed during an attack or intrusion, such as file hashes, IP addresses, domain names, or network traffic.

The main difference between TTP and IoC is that TTP is a **proactive** approach that tries to understand and anticipate the attacker's intentions and capabilities, while IoC is a **reactive** approach that tries to identify and analyze the current or previous threats based on specific evidence. TTPs can help organizations develop more effective and comprehensive defense strategies, while IoCs can help organizations detect and respond to threats faster and more accurately, as time passes, these KBs can be used for future and for faster and easier understanding of a threat, if that threat is previously observed and the mitigation playbook can be associated and updated, and the immediate resolution can be drawn, and the case will be closed if no remediation needs to be taken or any process is in place for automatic remediation or cleanup.

KPI's for a Security Operation Center

Key Performance Indicators (KPIs) are a way of measuring the success or failure of a business goal, function, or objective, and they provide actionable information on which decisions can be based. Here are some commonly used KPIs for a Security Operations Center (SOC):

1. **Ingress:** Risk assessment for systems conveyed to SOC, and number of devices log shipped to SOC.
2. **Occurrence:** Incident occurrence due to known vs. unknown vulnerability.
3. **Threat Level:** Threat actor attribution (using threat intelligence). Thoroughness and accuracy of enterprise sweeping (check all information systems for indicators of compromise)
4. **Incident Response Time**: These measures how quickly the SOC responds to a security incident.
5. **Threat Detection Rate**: These measures how effectively the SOC is identifying threats. Time from detection to containment to eradication.
6. **False Positive Rates**: This measures the accuracy of threat detection.
7. **Mean Time to Resolve (MTTR)**: These measures show how fast the organization can identify a security incident and provide a complete resolution. Number of incidents closed in one shift. Thoroughness of eradication (no recurrence of original or similar compromise).
8. **Mean Time to Detect (MTTD)**: This measures the time it takes for the organization to detect a security incident.
9. **Impact**: Time to discover all impacted assets and users. Downtime for workers or duration of business outage per incident.
10. **Number of Incidents Handled or Resolved**: This measures the effectiveness of the SOC's incident response and remediation efforts.
11. **Avoidability** of incident (could the incident have been avoided with common security practices in place?). Monetary cost per incident. Losses accrued vs. losses prevented.

These are for your standard KPI's in a SOC, but you are not limited to anything, add as many KPI's as per your requirement, and as per your team constructions. Overdoing it will also have a negative impact, as your analysts will have faster burnouts.

Remember, the most effective way to develop meaningful KPIs is to start by identifying which security operations goals or functions are the most critical to the security operations program, and who is assigned for particular jobs. Suppose a number of analysts are assigned for inside threat events, and another team is for outside. Inside team can be divided into running 2 major tasks or activities for Windows systems and one for Linux based systems, but it also depends on your requirements, and availability of analysts. Also, these KPIs should be regularly reviewed and updated to ensure they continue to align with the organization's goals and the evolving threat landscape.

Benefits of SOC KPI's

While security operations may have similar goals, most security operations goals are less finite. Most security operations goals are more focused on positive or negative trends

over time than achieving a specific target. Let's discuss why KPIs are important, how to choose the best KPIs for a given organization, and how many KPIs are appropriate. Quality KPI's serve as a security program enabler and driver for continuous improvement. The threat landscape is a dynamic and ever-changing environment, and effective security operations programs require actionable information on which decisive action can be based. KPIs help ensure that a security operations program continues to remain effective and that any process or technology gaps are addressed appropriately. Most common KPI's are based on the following criteria:

- Analysts Skills.
- Process Success.
- Detection Success.
- Key Risk Findings.
- Workloads & its Distributions to L1, L2, L3.
- Mitigation Success.

The following list is intended to be used as a primer to inspire ideas to identify the most important KPIs for an organization:

PI	Why Do We Care?	Possible Measurements	Assessment of:
Number of devices being monitored	How many devices are being monitored? Is the number increasing or decreasing? Why?	Number of devices Number of devices / analyst	Workload
Total number of events	How many events are being handling? Is the number increasing or decreasing? Why? Are the current staffing levels adequate?	Number of events / hour (/ analyst) Number of events / day (/ analyst) Number of events / month (/ analyst) Number of events / year (/ analyst) Number of events / event type	Cost to value Key risks Workload
Number of events per device or host	How many events are received for each device or host?	Number of events per device or host / day	Detection success Key risks

	Are there certain devices or hosts which are more prone to security issues, causing increased risk? Why? Are there certain devices or hosts which are more prone to false positive events? Why?	Number of events per device or host / month Number of events per device or host / year Number of events / device or host type Number of events / operating system type	
Number of events per service or application	How many events are received for each service or application? Are there certain services or applications which are more prone to security issues, causing increased risk? Why? Are there certain services or applications which are more prone to false positive events? Why?	Number of events / service Number of events / application	Detection success Key risks
Number of events per account	How many events are received for account? Are there certain accounts (users) which are more likely to perform risky behavior, leading to security events and increased risk? Why?	Number of events / account Number of events / user	Detection success Key risks
Number of events per location	How many events are received per geographic location, office, etc.? Are certain locations more prone to security events? Why?	Number of events / department Number of events / office Number of events / region	Key risks

Number of false positive alerts	How many false positive events are received? Is this acceptable? Can the number of false positive events be reduced? How?	Number of false positives / hour Number of false positives / day Number of false positives / month Number of false positives / year Percentage of events that are false positives	Detection success
Time to detection	How long is it taking your organization to detect a security event? Is this acceptable? Are there ways this time to detection can be reduced? How?	Measured in minutes, hours or days… Average time to detection Average time to detection / technology Average time to detection / event type Outliers	Detection success Process success
Time to resolution	How long is it taking your organization to resolve an actual security event? Is this acceptable? Are there process or technology improvements that can be made to reduce this time? What are they? Are additional staff or training required? How many staff or what additional training is required?	Measured in minutes, hours or days… Average time to resolution Average time to resolution / event type	Mitigation success Process success

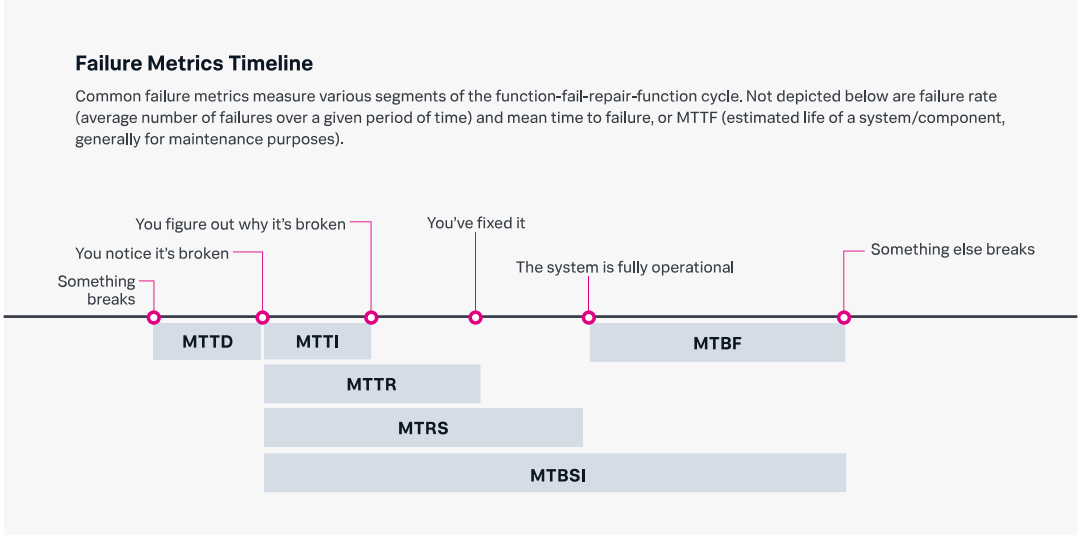
		Average time to resolution / resolution strategy Outliers	
Time to identify event as false positive	How long is it taking your organization to determine that an event is a false positive? Is this acceptable? Are analysts spending too much time investigating false positives? Why? Is additional training required? What kind?	Measured in minutes, hours or days… Average time to identify Average time to identify / technology Average time to identify / event type Outliers	Analyst skills Process success
Number of analysts assigned	How many analysts are being assigned to each event? Is it the proper number? Are too many analysts being assigned to one event meaning that they are not available to response to other events? Why? Are too few analysts being assigned to an event due to staff shortages?	Average number of analysts / event Average number of analysts / event type Average number of analysts (per level) / event Average number of analysts (per level) / event type	Analyst skills Cost to value Workload
Escalation level	How many events are being escalated and to what level? Are events being escalated too quickly or not soon enough? Why?	Average number of events / level Average number of events / level / (time period)	Analyst skills Cost to value

	Are there improvements to the escalation process that can make event handling more efficient? What are they?	Escalation level / event type	Process success
	Is the training for each level sufficient to produce the desired skill level? If not, what additional training is required?	Escalation level / technology	
		Average time (min or hours) to escalate	
Event source	Are certain detection technologies more or less effective at detecting security events? Why?	Total number of events / technology	Detection success Key risks
	Are certain detection technologies more prone to false positives? Why?	Total number of events / technology /	
	How often are users or analysts manually detecting an event before it is detected by a detection technology? Why?	(time period)	
		Total number of false positives / technology	

Source: SOAR-KPIs.pdf (acadiatech.com)

You will be doomed if your SIEM dashboard is not grouped based on locations, devices, infrastructures etc.

Failure Metrics Timeline



Source: [SOC Metrics: Security Metrics & KPIs for Measuring SOC Success | Splunk]

- MTTI: Mean time to identify or investigate.
- MTRS: Mean time to restore service.
- MTBSI: Mean time to between system incidents.
- MTBF: Mean time before failure.
- MTTF: Mean time to failure.

Defining Success for Your Ideal Reporting Model

Source, a great article from Cyril Simonnet: [The Optimal Reporting Structure for Your SOC: Enabling Effective Security Operations | LinkedIn]

The "right" reporting structure for your SOC depends on your unique risk profile, corporate politics, leadership, and culture. But across any model, the hallmarks of success remain the same:

- The SOC has adequate resources and budget to meet operational demands. No skimping on what they need to get the job done!
- Security operations and detection content remain properly focused based on likely threats. Stay on target and ignore distractions!
- Visibility exists in the SOC's capabilities and gaps.

- The SOC retains autonomy over core technical functions while adhering to corporate standards.
- Collaboration between the SOC and CISO is fostered to create security alignment.
- Executive management has trust and confidence in the SOC's competence.

Rather than get distracted by abstract debates over organizational boxes and lines, focus on these tangible outcomes that demonstrate SOC effectiveness.

CHAPTER 20

Cybersecurity Tabletop Exercises

CONTINUOUS EXERCISING YOUR ACTIVITY WITHIN THE SOC HIERARCHY ENABLES DEPENDENCIES ON YOUR PEERS DATA COLLECTION REQUIREMENTS, MATERIALS PREPAREDNESS, COORDINATED EFFORT FOR CASE MANAGEMENT ETC. YOU ARE NOT MEANT TO DO EVERYTHING, TRUST YOUR PEERS, AND THEY WILL TRUST YOU AS WELL, WELL, DEFINITELY, IN TIME.

Conducting cybersecurity tabletop exercises is a valuable practice for organizations to test their incident response plans, enhance team collaboration, and improve overall cybersecurity preparedness. Here's a comprehensive guide on how to prepare for and conduct tabletop exercises, along with the desired results and awareness you want to achieve:

How to Prepare for Cybersecurity Tabletop Exercises

1. Define Objectives:

- Clearly outline the objectives of the tabletop exercise. Common objectives include testing incident response procedures, evaluating communication channels, and assessing team coordination.

2. Identify Scenarios:

- Select realistic and relevant scenarios based on potential cybersecurity threats and risks to your organization. Consider incidents such as ransomware attacks, data breaches, or phishing campaigns.

3. Build a Scenario Script:

- Develop a detailed scenario script that outlines the progression of the incident. Include information on how the incident is discovered, who is involved, and the potential impacts on the organization.

4. Engage Stakeholders:

- Identify key stakeholders who should participate in the exercise, including representatives from IT, security, legal, communications, and executive leadership.

5. Establish Ground Rules:

- Define the rules and parameters of the tabletop exercise, including whether it will be a full simulation or a discussion-based exercise. Clarify the roles and responsibilities of participants.

6. Prepare Materials:

- Gather all necessary materials, including the scenario script, communication templates, incident response plans, and any relevant documentation. Distribute these materials to participants in advance.

7. Schedule and Coordinate:

- Set a date and time for the tabletop exercise, ensuring that key participants can attend. Coordinate with facilitators and participants to ensure everyone is aware of their roles.

8. Facilitator Training:

- Train facilitators who will guide the exercise. Facilitators should understand the scenario, objectives, and expected outcomes, as well as how to manage the flow of the discussion or simulation.

How to Conduct Cybersecurity Tabletop Exercises

1. Introduction:

- Begin the exercise with an introduction, outlining the objectives, ground rules, and the scenario participants will be addressing.

2. Scenario Presentation:

- Present the scenario to participants, detailing the incident's unfolding events. Encourage participants to react as they would in a real-world situation.

3. Discussion and Decision-Making:

- Facilitate a discussion among participants as they make decisions and respond to the evolving scenario. Encourage open communication and collaboration.

4. Injects and Surprises:

- Introduce injects or surprises into the scenario to simulate unexpected developments or new information. This challenges participants to adapt their response strategies.

5. Documentation:

- Require participants to document their decisions, actions taken, and any lessons learned during the exercise. This documentation is valuable for post-exercise analysis.

6. Debrief Session:

- Conclude the exercise with a debrief session. Discuss what went well, areas for improvement, and lessons learned. Encourage participants to share insights and feedback.

7. Post-Exercise Analysis:

- Conduct a thorough analysis of the exercise outcomes. Evaluate the effectiveness of communication, decision-making, and coordination. Identify areas for improvement in processes, documentation, or team dynamics.

8. Actionable Recommendations:

- Generate actionable recommendations based on the lessons learned from the exercise. These recommendations should drive improvements in incident response plans, communication protocols, and overall cybersecurity posture.

Desired Results and Awareness

1. Improved Incident Response Planning:

- Identify gaps or weaknesses in the incident response plan and make necessary improvements.

2. Enhanced Communication and Coordination:

- Strengthen communication channels and coordination among different teams involved in incident response.

3. Increased Situational Awareness:

- Improve participants' ability to assess and respond to evolving situations by enhancing their situational awareness.

4. Team Building and Collaboration:

- Foster a collaborative and cohesive incident response team by providing opportunities for team members to work together effectively.

5. Adaptability and Flexibility:

- Test the team's ability to adapt to unexpected developments and demonstrate flexibility in response strategies.

6. Identifying Improvement Areas:

- Identify specific areas for improvement in processes, procedures, and technical capabilities.

7. Crisis Communication Skills:

- Enhance the organization's crisis communication skills by practicing communication during a simulated incident.

8. Executive Leadership Awareness:

- Increase awareness among executive leadership about the organization's cybersecurity preparedness and potential challenges.

9. Compliance Testing:

- Evaluate the organization's ability to comply with regulatory requirements and industry standards during a cybersecurity incident.

10. Continuous Improvement Culture:

- Instill a culture of continuous improvement by regularly conducting tabletop exercises and incorporating lessons learned into cybersecurity practices.

These exercises contribute to a more resilient cybersecurity posture and help teams refine their incident response capabilities.

Outcome of the Cybersecurity Tabletop Exercise

The outcome of a cybersecurity tabletop exercise is multi-faceted and serves several critical purposes in enhancing an organization's cybersecurity resilience. Here are key outcomes that organizations can expect from conducting cybersecurity tabletop exercises:

1. **Identification of Weaknesses and Gaps:**
    - One of the primary outcomes is the identification of weaknesses and gaps in the organization's cybersecurity posture. This includes weaknesses in incident response plans, communication protocols, technical controls, and overall preparedness.
2. **Improved Incident Response Planning:**
    - The exercise highlights areas for improvement in the incident response plan. Organizations can refine and update their plans based on the insights gained during the exercise, ensuring that they are better equipped to handle real-world incidents.
3. **Enhanced Communication and Collaboration:**

- Tabletop exercises facilitate improved communication and collaboration among different teams involved in incident response. Participants learn to share information effectively, coordinate actions, and work together cohesively during a simulated incident.

4. **Increased Situational Awareness:**
    - Participants develop a heightened sense of situational awareness, learning to assess and respond to evolving scenarios. This outcome is crucial for effective decision-making and response in the face of a real cybersecurity incident.
5. **Team Building and Collaboration Skills:**
    - The exercise serves as a team-building opportunity, allowing participants to work together, understand each other's roles, and build trust. This collaborative experience contributes to a more effective and resilient incident response team.
6. **Adaptability and Flexibility Testing:**
    - Tabletop exercises test the team's ability to adapt to unexpected developments and demonstrate flexibility in response strategies. This outcome ensures that the organization's incident response capabilities can handle dynamic and evolving cyber threats.
7. **Identification of Improvement Areas:**
    - The exercise identifies specific areas for improvement, not only in processes and procedures but also in technical capabilities. This outcome helps organizations prioritize and address weaknesses in their cybersecurity infrastructure.
8. **Crisis Communication Skills Enhancement:**
    - Organizations enhance their crisis communication skills by practicing communication during a simulated incident. This includes communicating internally within the organization and externally with stakeholders, regulatory bodies, and the public.
9. **Executive Leadership Awareness:**

- Tabletop exercises increase awareness among executive leadership about the organization's cybersecurity preparedness and potential challenges. This heightened awareness can lead to better-informed decision-making and resource allocation.

10. **Compliance Testing and Validation:**
    - The exercise serves as a test of the organization's ability to comply with regulatory requirements and industry standards during a cybersecurity incident. This outcome is crucial for maintaining compliance and avoiding potential legal and regulatory consequences.
11. **Continuous Improvement Culture:**
    - Through regular tabletop exercises, organizations foster a culture of continuous improvement. Lessons learned from each exercise are used to refine and enhance cybersecurity practices, ensuring that the organization stays resilient in the face of evolving cyber threats.
12. **Actionable Recommendations:**
    - Following the exercise, organizations generate actionable recommendations based on the lessons learned. These recommendations drive improvements in incident response plans, communication protocols, and overall cybersecurity posture.

In summary, it empowers SOC members to identify and address weaknesses, enhance collaboration, and continuously improve their cybersecurity defenses to effectively mitigate and respond to cyber threats.

If you look at the big picture, the collaboration I am talking about is to have triangular synergy with the CIO, CTO & the CISO. If the ego comes in the play and professionalism is absent in either of the three, the SOC goes nowhere, even if powerful team members are present.

There are some exercises available for you to checkout, the most prominent ones are:

1. CTEP Package Documents | CISA
2. Cybersecurity Tabletop Exercise Examples, Best Practices, and Considerations | RSI Security
3. Tabletop Exercises (TTX) (cisecurity.org)
4. Implementing Your First Cybersecurity Tabletop Exercise - JumpCloud

CHAPTER 21

Artificial Intelligence in Cybersecurity Operation Center

AN AI BASED SYSTEM CAN DO BOTH, INFILTRATE BY SCANNING AND IDENTIFYING BREAKS IN YOUR NETWORK, AND AS WELL THE OTHER SIDE, CAN LAY OUT HONEYPOTS TO TRAP AND TRACE THE SAME FUNCTIONS, AND REPORT TO SOC PROCESSES FOR INTERVENTION.

AI is a powerful tool that can enhance the capabilities and efficiency of security teams, but it also poses new challenges and risks. Therefore, it is important to design, deploy, and use AI securely, and to be aware of the potential threats that AI can enable or amplify, such as adversarial attacks, deepfakes, or automated exploits.

Increase in AI adoption and expansion, many organizations are evaluating whether artificial intelligence can help improve business operations that normally require human intelligence, such as analyzing vast amounts of data, managing the increasing complexity of environments, and as a powerful tool for implementing cybersecurity strategies to protect business-critical elements like customer data and other sensitive information and in future analytics for threat hunting, threat engineering, detection engineering etc.

While the full extent and implications of AI capabilities within the cybersecurity industry are not yet understood, here is a simplified overview of common problem areas in which AI-powered systems could show promising results:

1. Increase efficiency.
2. Improve accuracy.
3. Improve threat detection.
4. Improve scalability.
5. Improve integration capabilities which produces actionable results.
6. Effective location identification of threats bounced or generated from.
7. OTC cost of the AI reduces overall costs for data mapping.
8. Automated responses to security threats.
9. Accelerate incident investigation.
10. Provide predictive threat prevention.
11. Determine root cause.
12. Data & input validation of the data from different sources.
13. Combining OSINT data into one glass view of the treat vectors.

Security Teams Need AI to Help Them Find Threats

AI can help security teams detect threats by using sophisticated algorithms and predictive intelligence to analyze data, identify patterns and anomalies, and find and stop attacks before they cause damage. AI can also help security teams manage their workload, reduce false positives, and learn from past incidents. Some examples of how AI can help security teams detect threats are:

- AI can hunt down malware by comparing files and traffic against known malicious signatures or behaviors, or by using machine learning to classify new or unknown malware based on its features.
- AI can run pattern recognition to detect phishing schemes, ransomware, credential stuffing, and domain hijacking by looking for indicators of compromise, such as suspicious URLs, attachments, or login attempts.

- AI can find and thwart attacks by using anomaly detection to spot deviations from normal network or user activity, such as unusual data transfers, connections, or commands.
- AI can prevent future threats by learning from past incidents and identifying patterns in data that may indicate a potential attack before it happens, such as correlations, trends, or outliers.

Limitations of AI in SOC

Some of the limitations of AI in SOC that need to be addressed by SOC managers, analysts, and developers, as well as other stakeholders such as governments, businesses, researchers, and civil society. AI is a powerful and evolving technology that can offer many benefits and challenges for SOC, and it requires constant monitoring, evaluation, and improvement.

AI in SOC (Security Operations Center) is a valuable tool for detecting and responding to cyber threats, but it also has some limitations that need to be addressed. Some of the limitations of AI in SOC are:

- **Data quality and availability**: AI relies on large and diverse data sets to learn and improve its performance, but data quality and availability may vary depending on the source, format, and context of the data. Poor or insufficient data can lead to inaccurate or biased results or reduce the effectiveness of AI models.
- **Human factors**: AI cannot replace human judgment, expertise, and intervention in SOC, but rather complement and augment them. However, human factors such as trust, communication, collaboration, and ethics may affect how AI is perceived, used, and supervised by SOC analysts and managers. For example, human operators may over-trust or under-trust AI, fail to understand or explain AI outputs, or misuse or abuse AI for malicious purposes.
- **Adversarial attacks**: AI may be targeted by malicious actors who seek to compromise, manipulate, or deceive AI systems or their users. For example, attackers may use adversarial examples, deepfakes, or poisoning attacks to fool or corrupt AI models, or exploit their vulnerabilities or weaknesses.
- **Regulatory and ethical challenges**: AI may pose regulatory and ethical challenges for SOC, such as privacy, security, accountability, fairness, and transparency. For example, AI may collect, process, or share sensitive or personal data without proper consent, security, or governance, or produce outcomes that are unfair or discriminatory to certain groups or individuals.

Ensure the Transparency and Explainability of AI Outputs in SOC

AI outputs in CSOC (cybersecurity operations center) are the results or decisions produced by AI systems that are used to detect and respond to cyber threats. Transparency and explainability of AI outputs in SOC are important for building trust, accountability, and compliance among various stakeholders, such as SOC analysts, managers, customers, regulators, and auditors. Some of the ways to ensure the transparency and explainability of AI outputs in SOC are:

- **Data governance**: This involves establishing clear policies and procedures for data collection, processing, storage, and sharing, and ensuring compliance with relevant laws and regulations. Data governance can help ensure that the data used by AI systems is accurate, fair, and representative, and that the data sources, quality, and limitations are disclosed and documented.
- **Algorithmic transparency**: This involves making the AI systems and their outcomes understandable and explainable to users, regulators, and developers, and allowing for scrutiny and challenge. Algorithmic transparency can help ensure that the AI systems are designed and developed with ethical and social considerations, and that the functioning mechanisms, assumptions, and limitations are disclosed and documented.
- **User control**: This involves giving users the ability to access, correct, delete, or withdraw their data, and obtaining their informed consent for data use. User control can help ensure that the users have the right to know, understand, and influence how their data is used by AI systems, and that the users can opt out or appeal the AI outputs if they disagree or are dissatisfied.
- **Human oversight**: This involves ensuring that human judgment, expertise, and intervention are involved in the development, deployment, and use of AI systems. Human oversight can help ensure that the AI systems are aligned with human values and goals, and that the human operators can monitor, evaluate, and correct the AI outputs if needed.
- **Plain language explanations**: This involves providing clear and concise explanations of how the AI systems work, why they produce certain outputs, and what the implications and consequences are. Plain language explanations can help ensure that the AI outputs are understandable and interpretable by users, regardless of their technical expertise, and that the users can make informed and rational decisions based on the AI outputs.

Possibilities of Implementing AI in SOC

Implementing AI for your organization's security can be a complex and challenging task, but also a rewarding one. AI can help you enhance your security posture, detect and prevent threats, and automate tedious tasks. Here are some steps you can take to implement AI for your organization's security:

- Align AI strategy with business and security objectives. Before embarking on AI implementation, you should define your goals, scope, and expected outcomes. You should also identify the key use cases and scenarios where AI can add value to your security operations.
- Invest in skilled AI talent. AI requires specialized skills and expertise, such as data science, machine learning, and security engineering. You should either hire or train your staff to acquire these skills, or partner with external vendors or consultants who can provide them.
- Thoroughly evaluate AI solutions. There are many AI solutions available in the market, but not all of them are suitable for your needs. You should conduct a thorough assessment of the features, capabilities, performance, and reliability of the AI solutions you are considering. You should also test them in your environment and compare them with your existing tools and processes.
- Establish a robust data governance framework. Data is the fuel for AI, and you need to ensure that you have enough, high-quality, and relevant data to feed your AI systems. You should also ensure that your data is secure, compliant, and ethical. You should establish clear policies and procedures for data collection, storage, access, sharing, and deletion.
- Implement strong security measures for AI infrastructure. AI systems are not immune to cyberattacks, and you need to protect them from malicious actors. You should implement strong security measures for your AI infrastructure, such as encryption, authentication, authorization, monitoring, and auditing. You should also update your AI systems regularly and patch any vulnerabilities.

Challenges of Using AI in SOC

AI in cybersecurity can offer many benefits, such as automating threat detection and response, improving risk assessment and compliance, and enhancing cost management. However, AI also poses some challenges and risks, such as:

- **Lack of transparency and explainability**: AI systems often operate as black boxes, making it difficult to understand how they reach their decisions or outcomes. This can lead to trust issues, ethical dilemmas, and legal liabilities.
- **Overreliance on AI**: AI systems are not infallible, and they may make mistakes or fail to account for all possible scenarios. Relying too much on AI can reduce human vigilance, expertise, and intervention, and create a false sense of security.
- **Bias and discrimination**: AI systems may reflect or amplify the biases and prejudices of their data, developers, or users. This can result in unfair or inaccurate outcomes, such as misidentifying or discriminating against certain groups or individuals.
- **Vulnerability to attacks**: AI systems may be targeted by malicious actors who seek to compromise, manipulate, or deceive them. For example, attackers may use adversarial examples, deepfakes, or poisoning attacks to fool or corrupt AI systems.
- **Lack of human oversight**: AI systems may act autonomously or unpredictably, without sufficient human supervision or control. This can raise ethical, legal, and social issues, such as accountability, responsibility, and consent.
- **High cost**: AI systems may require significant resources, such as data, computing power, and talent, to develop, deploy, and maintain. This can create barriers to entry, widen the digital divide, and increase the risk of cyberattacks.
- **Privacy concerns**: AI systems may collect, process, and share large amounts of personal or sensitive data, without proper consent, security, or governance. This can expose individuals or organizations to data breaches, identity theft, or surveillance.

Common Pitfalls of AI Performance Optimization

AI performance optimization is the process of improving the efficiency, accuracy, and reliability of AI systems. However, it can also involve some challenges and pitfalls that can hinder the desired outcomes. Some of the common pitfalls of AI performance optimization are:

- **Poor architecture choices**: Choosing the wrong architecture for your AI system can lead to poor performance, scalability, and manageability. You should consider the complexity, accuracy, interpretability, scalability, and robustness of

the available architectures, and select the one that matches your problem characteristics and performance criteria.

- **Inaccurate or insufficient training data**: The quality and quantity of your training data will determine the quality and accuracy of your AI system. You should ensure that your data is clean, relevant, and representative of your problem domain. You should also perform data cleaning, preprocessing, and augmentation to remove noise, outliers, missing values, and biases from your data.
- **Lack of AI explainability**: AI systems can be difficult to understand and interpret, especially when they use complex or black-box models. This can lead to a lack of trust, accountability, and transparency in your AI system. You should use methods and tools that can provide explanations for your AI system's decisions, such as feature importance, saliency maps, or counterfactual examples.
- **Difficulty in reproducing results**: AI systems can be sensitive to changes in data, parameters, or environments, which can cause inconsistencies or discrepancies in the results. This can make it hard to validate, verify, or compare your AI system's performance. You should use rigorous methods and standards to document, share, and reproduce your AI system's results, such as code versioning, data provenance, or reproducibility frameworks.
- **Ethical and social challenges**: AI systems can have ethical and social implications, such as privacy, fairness, bias, or human dignity. These can affect the acceptance, adoption, and impact of your AI system. You should consider the ethical and social aspects of your AI system and follow the principles and guidelines that can ensure the responsible and beneficial use of AI, such as human values, human agency, or human oversight.

Ensure the Fairness of the AI System

Ensuring the fairness of your AI system is a complex and important task that requires careful consideration of the data, models, algorithms, and outcomes of your AI system. Fairness is not only a legal and ethical obligation, but also a business and social benefit, as it can enhance the trust, acceptance, and impact of your AI system. Here are some general steps that you can take to ensure the fairness of your AI system:

- Define what fairness means for your AI system and its stakeholders. Fairness is a context-dependent and multi-dimensional concept that can have different interpretations and implications depending on the problem domain, the data

sources, the target groups, and the intended outcomes of your AI system. You should consult with your stakeholders, including your customers, employees, regulators, and the public, to understand their expectations, needs, and values, and to define the fairness criteria and metrics that are relevant and appropriate for your AI system.

- Assess the potential sources and impacts of bias and discrimination in your AI system. Bias and discrimination can arise at any stage of the AI lifecycle, from data collection and processing to model development and deployment, to outcome evaluation and feedback. You should identify and analyze the potential sources and impacts of bias and discrimination in your AI system, such as data quality, representativeness, and diversity, model complexity, accuracy, and explainability, algorithmic assumptions, parameters, and objectives, and outcome fairness, accountability, and transparency. You should also consider the potential direct and indirect harm that your AI system could cause to individuals or groups, such as privacy violations, dignity infringements, or opportunity losses.
- Implement appropriate measures and techniques to mitigate bias and discrimination in your AI system. There are various measures and techniques that you can use to mitigate bias and discrimination in your AI system, depending on the type, level, and severity of the bias and discrimination, and the trade-offs and constraints that you face. Some of the common measures and techniques are:
    - Data preprocessing: This involves applying methods and tools to clean, augment, balance, or anonymize your data before feeding it to your AI system, to reduce noise, outliers, missing values, or biases in your data.
    - Model regularization: This involves applying methods and tools to constrain, simplify, or regularize your model during the training process, to reduce overfitting, underfitting, or complexity in your model.
    - Algorithmic debiasing: This involves applying methods and tools to modify, adjust, or optimize your algorithm during or after the training process, to reduce unfairness, discrimination, or bias in your algorithm.
    - Outcome postprocessing: This involves applying methods and tools to evaluate, correct, or explain your outcomes after the inference process, to reduce unfairness, discrimination, or bias in your outcomes.

- Monitor and evaluate the fairness of your AI system regularly and continuously. Fairness is not a static or one-time property, but a dynamic and ongoing process that requires constant monitoring and evaluation. You should collect and analyze feedback and data from your AI system deployment and use them to measure and evaluate the fairness of your AI system, using the criteria and metrics that you defined. You should also identify and address any issues, errors, or changes that may affect the fairness of your AI system, such as data drift, concept drift, or model degradation. You should update your AI system with new data, features, or algorithms to keep it fair and accurate.

Examples of AI Bias and Discrimination in SOC

SOC stands for Cybersecurity Operations Center, which is a centralized unit that monitors, detects, and responds to cyber threats and incidents. AI systems can be used to enhance the capabilities and efficiency of SOC, such as by automating tasks, analyzing data, or providing insights. However, AI systems can also introduce bias and discrimination in SOC, which can affect the security and privacy of users, as well as the trust and accountability of SOC. Here are some examples of AI bias and discrimination in SOC from different domains and applications:

- **Incident response**: AI systems can be used to assist SOC analysts in responding to cyber incidents, such as by providing recommendations, actions, or solutions. However, if the data or algorithms are biased, they can lead to inaccurate or inappropriate incident response that affects the recovery and resilience of users. For example, a study found that an AI system used to prioritize cyber incidents was biased against certain types of incidents, such as phishing or ransomware, as it used features that were more common in other types of incidents, such as denial-of-service or malware.
- **Threat intelligence**: AI systems can be used to collect, analyze, and share information about cyber threats, such as their sources, methods, or targets. However, if the data or algorithms are biased, they can lead to incomplete or misleading threat intelligence that affects the awareness and preparedness of users. For example, a report found that an AI system used to generate threat reports was biased against certain regions, such as Africa or Asia, as it used sources that were more focused on other regions, such as Europe or North America.
- **User behavior analytics**: AI systems can be used to monitor and analyze the behavior of users on networks, devices, or applications, and detect anomalies, risks, or violations. However, if the data or algorithms are biased, they can lead to

unfair or intrusive user behavior analytics that affect the access and usability of users. For example, a study found that an AI system used to identify insider threats was biased against certain user groups, such as contractors or remote workers, as it used features that were more common in regular employees, such as working hours or location.

To prevent or mitigate AI bias and discrimination in SOC, it is important to ensure that the data, algorithms, and objectives of AI systems are fair, transparent, and accountable, and that the stakeholders, including the developers, analysts, and users, are involved and informed in the AI development and deployment process.

Algorithmic Debiasing

Algorithmic debiasing is the process of reducing or eliminating unfairness, discrimination, or bias in AI algorithms, models, or outcomes. There are many tools available for algorithmic debiasing, but one of the most comprehensive and extensible ones is the AI Fairness 360 (AIF360) toolkit by IBM. AIF360 is an open-source library that contains techniques developed by the research community to help detect and mitigate bias in machine learning models throughout the AI application lifecycle. AIF360 is available in both Python and R, and supports various types of bias mitigation methods, such as data preprocessing, model regularization, algorithmic debiasing, and outcome postprocessing. AIF360 also provides interactive web demos, tutorials, notebooks, and videos to help users learn and apply the toolkit. You can find more information and resources about AIF360 on its website or GitHub repository. AI Fairness 360 (ibm.com)

Mitigate the Risks of AI in SOC

There are several strategies and measures that we can take to mitigate the risks of AI in cybersecurity, such as:

- **Data governance**: We can use effective data governance to help ensure that data is properly classified, protected, and managed throughout its life cycle. This can help prevent model poisoning attacks, protect data security, maintain data hygiene, and ensure accurate outputs.
- **Threat-modelling**: We can use threat-modelling techniques to identify and prioritize the potential threats and vulnerabilities of AI systems, and design appropriate countermeasures and controls.
- **Access controls**: We can use access controls to limit who can access, modify or influence the AI systems, data and outputs, and monitor and audit the activities of authorized users.

- **Encryption and steganography**: We can use encryption and steganography to protect the confidentiality and integrity of data and models and prevent unauthorized access or tampering.
- **End-point security, or user and entity behavior analytics**: We can use end-point security or user and entity behavior analytics to detect and respond to anomalous or malicious behaviors of users or devices that interact with AI systems.
- **Vulnerability management**: We can use vulnerability management tools to scan, test and patch the AI systems and components, and reduce the exposure to known or unknown exploits.
- **Security awareness**: We can use security awareness programs to educate and train the users and developers of AI systems on the best practices and ethical principles of AI security and foster a culture of responsibility and accountability.

Emerging Trends in AI Security

Some emerging trends in AI security are:

- **AI-based threat detection**: This involves using machine learning algorithms to analyze large amounts of data and identify patterns that may indicate a potential threat. For example, AI can hunt down malware, detect phishing schemes, and find and thwart attacks by using anomaly detection.
- **Behavioral analytics**: This involves using AI to monitor and understand the behavior of users, devices, and networks, and detect any deviations or anomalies that may signal a compromise or an attack. For example, AI can run pattern recognition to spot credential stuffing, domain hijacking, or insider threats.
- **Cybersecurity automation**: This involves using AI to automate and streamline various cybersecurity tasks, such as threat hunting, incident response, vulnerability management, and risk assessment. For example, AI can provide autonomous remediation, behavioral analysis, real-time forensics, and predictive intelligence.
- **AI-powered authentication**: This involves using AI to enhance the security and convenience of authentication methods, such as biometrics, multi-factor authentication, and behavioral authentication. For example, AI can use facial recognition, voice recognition, or keystroke dynamics to verify the identity of users.

- **Adversarial machine learning**: This involves using AI to attack or defend against other AI systems, by exploiting their weaknesses or enhancing their strengths. For example, attackers may use adversarial examples, deepfakes, or poisoning attacks to fool or corrupt AI systems, while defenders may use robustness testing, encryption, or steganography to protect or hide AI systems.
- **AI in IoT security**: This involves using AI to secure the growing number of connected devices, such as smart home gadgets, industrial sensors, and wearable devices, that form the Internet of Things (IoT). For example, AI can provide network monitoring, device management, data protection, and threat prevention for IoT devices.
- **Cyber threat intelligence**: This involves using AI to collect, analyze, and share information about current or emerging cyber threats, such as threat actors, attack vectors, indicators of compromise, and mitigation strategies. For example, AI can provide contextualized and actionable intelligence, such as threat profiles, attack trends, or risk scores.

Examples of AI solutions for the SOC

AI solutions for the SOC are applications or systems that use artificial intelligence to enhance the capabilities and efficiency of the cybersecurity operations center. Some examples of AI solutions for the SOC are:

- **AI-powered threat detection and response**: These solutions use AI techniques, such as machine learning, natural language processing, or computer vision, to monitor, analyze, and respond to cyberthreats and incidents in real time. They can help SOC analysts to identify and prioritize the most critical alerts, automate tasks, and provide recommendations or solutions. For example, IBM QRadar Advisor with Watson is an AI solution that uses cognitive reasoning to investigate security incidents and provide actionable insights.
- **AI-powered threat intelligence and analytics**: These solutions use AI techniques, such as data mining, statistical analysis, or deep learning, to collect, process, and share information about cyberthreats, such as their sources, methods, or targets. They can help SOC analysts to gain situational awareness, understand the threat landscape, and anticipate future attacks. For example, Recorded Future is an AI solution that uses natural language processing and machine learning to provide threat intelligence from various sources, such as the web, social media, or dark web.

- **AI-powered user behavior analytics and insider threat detection**: These solutions use AI techniques, such as anomaly detection, behavioral modeling, or biometrics, to monitor and analyze the behavior of users on networks, devices, or applications, and detect anomalies, risks, or violations. They can help SOC analysts to prevent or mitigate insider threats, such as data leakage, sabotage, or fraud. For example, Securonix is an AI solution that uses machine learning and big data analytics to provide user behavior analytics and insider threat detection.

There are many AI-based security products that can help organizations protect their data and systems from cyber threats. Some of them are:

- **Darktrace**: A versatile platform that uses self-learning AI to neutralize novel threats, such as ransomware, insider attacks, and IoT breaches.
- **CrowdStrike**: A cloud-native platform that uses AI to monitor user endpoint behavior and prevent sophisticated attacks, such as nation-state intrusions, supply chain compromises, and zero-day exploits.
- **SentinelOne**: A platform that uses AI to provide advanced threat-hunting and incident response capabilities, such as autonomous remediation, behavioral analysis, and real-time forensics.
- **Check Point Software**: A platform that uses AI to provide network monitoring and security, such as firewall, VPN, threat prevention, and cloud security.
- **Fortinet**: A platform that uses AI to prevent zero-day threats, such as malware, botnets, and phishing, by using deep learning and sandboxing technologies.
- **Zscaler**: A platform that uses AI to provide data loss prevention, such as encryption, policy enforcement, and anomaly detection, for cloud-based applications and services.
- **Trellix**: A platform that uses AI to provide continuous monitoring and security for complex IT environments, such as data centers, edge computing, and IoT devices.
- **Vectra AI**: A platform that uses AI to provide hybrid attack detection, investigation, and response, such as network traffic analysis, threat intelligence, and automated response.

- **Cybereason**: A platform that uses AI to defend against MalOps, which are coordinated and malicious operations that target multiple endpoints, users, and networks.
- **Tessian**: A platform that uses AI to protect against email-based threats, such as phishing, spear phishing, and business email compromise, by analyzing human behavior and communication patterns.

Ethical Use of AI in SOC

The ethical use of AI in SOC is the use of AI systems that respect the values, rights, and interests of the stakeholders involved in or affected by the cybersecurity operations center, such as the developers, analysts, users, and the public. To ensure the ethical use of AI in SOC, we can follow some general steps, such as:

- Establish clear and transparent policies and guidelines for the development, deployment, and evaluation of AI systems in SOC, based on the principles and standards of ethical AI, such as fairness, accountability, transparency, and human dignity.
- Involve and consult with the stakeholders in the design, implementation, and oversight of AI systems in SOC, and ensure that they are informed and empowered to participate in the decision-making and feedback processes.
- Monitor and audit the performance and impact of AI systems in SOC, and identify and address any issues, errors, or risks that may arise, such as bias, discrimination, privacy, security, or reliability.
- Review and update the AI systems in SOC regularly and continuously, and incorporate new data, features, or algorithms to improve their accuracy, efficiency, and fairness.

Offensive AI Tools

Artificial intelligence driven offensive tools are used to automate or enhance cyberattacks, such as generating phishing emails, exploiting vulnerabilities, or even creating deepfakes.

SOC can benefit from AI-driven offensive tools in several ways, such as:

- **Simulating attacks**: SOC can use AI-driven offensive tools to test the security posture of their own network and systems and identify potential weaknesses or

gaps. This can help them improve their own defenses and resilience against real attacks and gain real visibility.

- **Gaining intelligence**: SOC can use AI-driven offensive tools to gather information about their adversaries as well, such as their capabilities, intentions, strategies, and targets. This can help SOC anticipate and counter adversary movement, and gain advantage in the cyber domain.
- **Conducting operations**: SOC can use AI-driven offensive tools to launch or support cyber operations against their adversaries, such as disrupting, degrading, or destroying their assets, networks, or data. This can help them achieve their objectives and deter future attacks if so wanted intentionally, although this type mentality is dangerous for the team, and should be avoided. If you are in a position where you are a part of state sponsored activities, and offensive tools are developed or used, then you should rethink your future.

SOC need to ensure the ethical use of AI-driven offensive tools by following best practices, such as:

- **Establishing clear guidelines and policies**: SOC should define the scope, purpose, and principles of using AI-driven offensive tools, and communicate them to all relevant stakeholders. They should also monitor and audit the compliance and effectiveness of these guidelines and policies and update them as needed. One misunderstood steps or exposed identities, or origination country exposure could ruin very cautiously built relationship with countries.
- **Ensuring accountability and transparency**: SOC should be able to explain the rationale, methods, and outcomes of using AI-driven offensive tools, and provide evidence of their validity and reliability. They should also be able to identify and report any errors, risks, or harm that may arise from their use, and take corrective actions accordingly.
- **Respecting human rights and values**: SOC should respect the dignity, privacy, and autonomy of the individuals and groups that may be affected by their use of AI-driven offensive tools, and avoid any discrimination, exploitation, or harm. They should also consider the social and ethical implications of their use, and balance them with the security and strategic objectives.
- **Seeking external input and feedback**: SOC should consult with experts, peers, and stakeholders from different disciplines, sectors, and backgrounds, to gain diverse perspectives and insights on the ethical use of AI-driven offensive tools. They should also solicit feedback from the users and beneficiaries of their use and incorporate their views and preferences.

Privacy and Confidentiality of Data Used by AI Systems

Privacy and confidentiality of data used by AI systems are important issues that require careful attention and solutions. Some of the possible ways to ensure them are:

- **Data governance**: This involves establishing clear policies and procedures for data collection, processing, storage, and sharing, and ensuring compliance with relevant laws and regulations.
- **Data hygiene**: This involves collecting only the data types necessary to create the AI, keeping the data secure, and maintaining the data only for as long as needed.
- **Data sets**: This involves building AI using accurate, fair, and representative data sets, and avoiding or correcting any biases or errors in the data. Do validate inputs before using it.
- **User control**: This involves giving users the ability to access, correct, delete, or withdraw their data, and obtaining their informed consent for data use.
- **Algorithmic transparency**: This involves making the AI systems and their outcomes understandable and explainable to users, regulators, and developers, and allowing for scrutiny and challenge.
- **Encryption and steganography**: This involves protecting the confidentiality and integrity of data and models, and preventing unauthorized access or tampering.
- **Access controls**: This involves limiting who can access, modify, or influence the AI systems, data, and outputs, and monitoring and auditing the activities of authorized users.
- **Vulnerability management**: This involves scanning, testing, and patching the AI systems and components, and reducing the exposure to known or unknown exploits.
- **Security awareness**: This involves educating and training the users and developers of AI systems on the best practices and ethical principles of AI security and fostering a culture of responsibility and accountability.

Legal and Regulatory Frameworks for AI Security

AI security is a complex and evolving field that requires coordination and cooperation among various stakeholders, such as governments, businesses, researchers, and civil society. There are different legal and regulatory frameworks for AI security in different

regions and countries, each reflecting their own values, priorities, and challenges. Some of the examples are:

- **The EU Artificial Intelligence Act**: This is a comprehensive and risk-based regulation that aims to ensure that AI systems are trustworthy, safe, and respect fundamental rights and values. The act proposes to ban or limit certain high-risk applications of AI, such as mass surveillance, social scoring, or biometric identification, and to impose obligations on providers and users of AI systems, such as transparency, human oversight, and quality assurance.
- **The US AI Bill of Rights**: This is a set of principles and guidelines that seeks to promote the ethical and responsible development and use of AI in the US. The bill of rights covers topics such as privacy, security, accountability, fairness, and human dignity, and calls for the establishment of a national AI commission to oversee and regulate AI activities.
- **The UK AI Strategy**: This is a framework that aims to establish the UK as an "AI superpower" by fostering innovation, growth, and public trust in AI. The strategy focuses on four pillars: research and development, skills and talent, adoption and transformation, and governance and ethics. The strategy also proposes to create a new AI regulatory body to ensure compliance with existing and future laws.
- **The Singapore Model AI Governance Framework**: This is a voluntary and non-binding framework that provides practical guidance and best practices for organizations to implement AI governance and ethics. The framework covers aspects such as human involvement, explainability, data quality, security, and accountability, and encourages organizations to conduct self-assessments and disclose their AI policies to stakeholders.
- **The China Administrative Measures for Generative Artificial Intelligence Services**: This is a draft regulation that aims to ensure that content created by generative AI is consistent with social order and morals, avoids discrimination, is accurate, and respects intellectual property. The regulation requires providers and users of generative AI services to obtain licenses, conduct audits, and label the content as AI-generated.

These are some of the legal and regulatory frameworks for AI security that are currently in place or under development in different regions and countries. However, there are many more initiatives and proposals that address different aspects of AI security, such as data protection, consumer protection, cybersecurity, human rights, and international

cooperation. AI security is a dynamic and evolving field, and it requires constant monitoring, evaluation, and improvement.

Measure ROI of AI in SOC

Measuring the ROI of AI in security can be a challenging task, as it involves quantifying the benefits and costs of AI solutions in a complex and dynamic environment. However, it is also an important task, as it can help you justify your AI investments, optimize your AI performance, and align your AI strategy with your business and security objectives.

There are different methods and metrics that you can use to measure the ROI of AI in security, depending on your specific use cases and goals. Some of the common methods and metrics are:

- **Hard ROI**: This is the traditional financial ratio of the net gain or loss from AI investments relative to their total cost. It can be calculated by subtracting the total cost of AI (including development, deployment, maintenance, and operational costs) from the total value of AI (including revenue increase, cost savings, productivity gains, and risk reduction) and dividing the result by the total cost of AI. Hard ROI can help you evaluate the profitability and efficiency of your AI solutions, but it may not capture the full range of benefits and costs that AI can bring to your security operations.
- **Soft ROI**: This is a broader measure of the qualitative and intangible benefits and costs of AI, such as customer satisfaction, employee engagement, brand reputation, innovation, and ethics. Soft ROI can be assessed by using surveys, feedback, ratings, reviews, or other indicators of stakeholder perception and satisfaction. Soft ROI can help you understand the impact of AI on your security culture, values, and relationships, but it may not be easily quantified or compared across different AI solutions.
- **Balanced scorecard**: This is a strategic management tool that combines both hard and soft ROI metrics into a comprehensive and balanced framework. It can help you align your AI objectives with your security vision, mission, and strategy, and track your AI performance across four key dimensions: financial, customer, internal, and learning and growth. Balanced scorecard can help you measure and communicate the value of AI in security from multiple perspectives, but it may require a lot of data collection and analysis, as well as stakeholder involvement and alignment.

To measure the ROI of AI in security effectively, you should follow some best practices, such as:

- Define your AI goals and expectations clearly and realistically, align them with your security and business objectives.
- Choose the most appropriate method and metrics for your AI use cases and goals and use a combination of hard and soft ROI metrics to capture the full value of AI.
- Collect and analyze relevant and reliable data to measure your AI outcomes and impacts and use benchmarks and baselines to compare your AI performance with your current state or industry standards.
- Monitor and evaluate your AI results and progress regularly and use feedback and insights to improve your AI solutions and strategy.
- Communicate and report your AI ROI clearly and transparently to your stakeholders and use stories and examples to illustrate the value of AI in security.

Optimize AI Performance for Better ROI

Optimizing your AI performance for better ROI is a key goal for any AI project. There are many factors that can affect your AI performance, such as data quality, model selection, parameter tuning, deployment strategy, and monitoring and feedback. Here are some general tips and techniques that can help you optimize your AI performance for better ROI:

- Ensure that your data is clean, relevant, and representative of your problem domain. Data is the foundation of AI, and the quality of your data will determine the quality of your AI solutions. You should perform data cleaning, preprocessing, and augmentation to remove noise, outliers, missing values, and biases from your data. You should also use appropriate data sources, formats, and splits to ensure that your data covers the range and diversity of your use cases and scenarios.
- Choose the right model and algorithm for your problem and objective. There are many AI models and algorithms available, but not all of them are suitable for your needs. You should consider the complexity, accuracy, interpretability, scalability, and robustness of the models and algorithms, and select the ones that match your problem characteristics and performance criteria. You should also compare

and evaluate different models and algorithms using appropriate metrics and validation methods.

- Fine-tune your model parameters and hyperparameters to optimize your model performance. Model parameters and hyperparameters are the settings that control the behavior and learning of your model. You should adjust and optimize these settings to improve your model performance and avoid overfitting or underfitting. You can use various methods, such as grid search, random search, or Bayesian optimization, to find the optimal values for your parameters and hyperparameters.
- Deploy your model in a suitable environment and platform that can support your AI requirements and goals. You should consider the availability, reliability, security, and scalability of your deployment environment and platform, and ensure that they can handle your AI workload and demand. You should also choose the right deployment mode, such as batch, online, or hybrid, depending on your use case and latency requirements.
- Monitor and update your model regularly to maintain and improve your model performance and ROI. You should collect and analyze feedback and data from your model deployment and use them to measure and evaluate your model performance and ROI. You should also identify and address any issues, errors, or changes that may affect your model performance and ROI, such as data drift, concept drift, or model degradation. You should update your model with new data, features, or algorithms to keep it relevant and accurate.

Can AI Replace Human Analysts in SOC?

AI can replace some of the tasks that human analysts perform in SOC, such as data collection, processing, analysis, and visualization, but it cannot replace the human judgment, creativity, and intuition that are essential for effective cybersecurity operations.

AI can augment and assist human analysts in SOC, by providing them with faster, smarter, and more accurate tools and insights, but it cannot replace the human skills and values, such as critical thinking, problem-solving, communication, collaboration, and ethics, that are required for cybersecurity decision-making and response. Therefore, AI can be seen as a partner, not a competitor, for human analysts in SOC, and the future of SOC will depend on the synergy and collaboration between AI and human analysts.

CHAPTER 22

Open-Source SOC

Developing an **open-source-based Security Operations Center (SOC)** involves several key steps. Let's break it down:

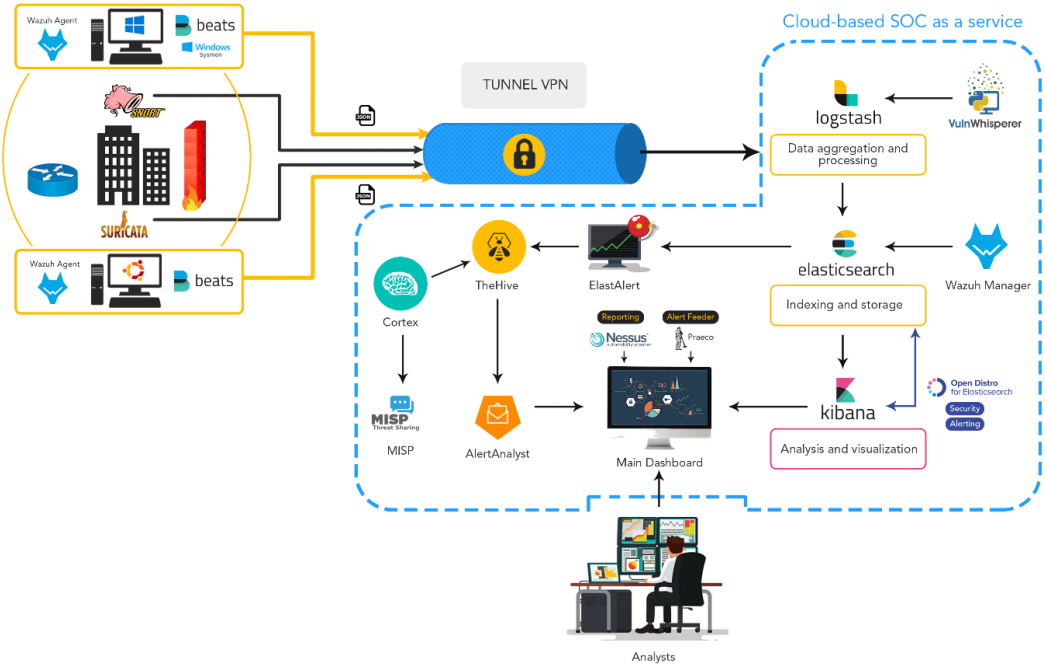
1. **Human Resources**:
    - Start by training your existing staff or hiring individuals with skills and experience in monitoring, incident management, threat hunting, intrusion detection, reverse engineering, and malware analysis.
    - Consider combining internal and external resources to build a strong SOC team.
2. **Processes**:
    - Establish clear workflows for incident management. Define roles, responsibilities, and documented processes.
    - Ensure that each team member understands their position and tasks within the SOC.
3. **Technology Stack**:

- Assemble a comprehensive set of open-source tools to support your SOC's visibility and response capabilities:
  - **SIEM (Security Information and Event Management)**: Combines security information management (SIM) and security event management (SEM) functions into a single framework.
  - **Incident Tracking and Management System**: Helps organize and track incidents.
  - **Intrusion Detection and Prevention Systems (IDS/IPS/IDPS)**: Monitor network traffic for signs of malicious activity.
  - **Threat Intelligence (CTI) Platform**: Enriches data with indicators of compromise (IOCs).
  - **Packet Capture and Analysis Tools**: Investigate network traffic.
  - **Automation Tools**: Automate routine tasks to free up analysts' time.
  - **Malware analysis tools:** investigate any malware's workflows within a sandboxed environment like ANY.RUN which lets your DFIR teams to analyze sophisticated ransomware or malware in a Linux environment.

4. **Network Monitoring**:
   - Use tools to monitor network traffic and detect anomalies.
   - Implement behavioral monitoring and data loss prevention mechanisms.
5. **Endpoint Management**:
   - Securely manage endpoints (devices) within your network.
6. **Asset Discovery**:
   - Identify and track assets (servers, workstations, devices) on your network.
7. **Incident Response**:
   - Develop incident response playbooks and procedures.
   - Implement ticketing systems for efficient case management.

Remember that open-source solutions offer flexibility, adaptability, and mostly cost-effectiveness that cannot be beaten. But do leverage the community support and customize your SOC to fit your organization's needs!

Designing the Open-source SOC



- Source: [archanchoudhury/SOC-OpenSource: This is a Project Designed for Security Analysts and all SOC audiences who wants to play with implementation and explore the Modern SOC architecture. (github.com)]
- [Deploying of infrastructure and technologies for a SOC as a Service (SOCasS) | by Ibrahim Ayadhi | Medium]

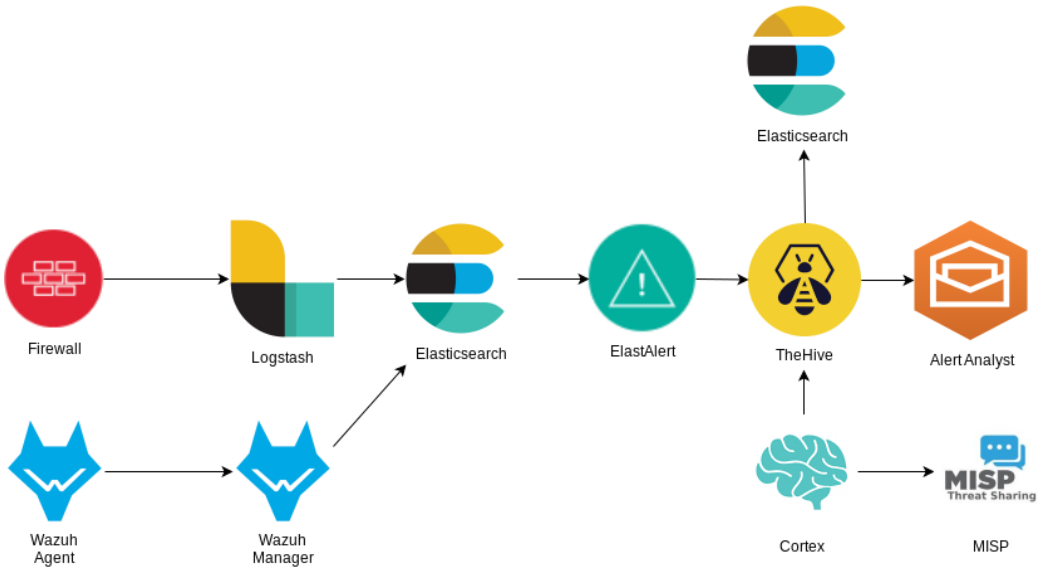
Designing an Open-Source Cybersecurity Operations Center (CSOC) using Wazuh, an impressive open-source security platform. Wazuh provides a comprehensive toolkit for threat detection, investigation, and response. Here's how you can architect your CSOC with Wazuh:

1. **Understanding Wazuh**:
    - **Wazuh** is more than just a **SIEM (Security Information and Event Management)** solution. It goes beyond simple log aggregation and analysis.
    - Key capabilities include:

- **Endpoint Detection and Response (EDR)**: Monitors endpoints for suspicious activity, detects malware, and enables incident response actions.
- **File Integrity Monitoring (FIM)**: Watches critical files and systems for unauthorized changes.
- **Vulnerability Assessment and Scoring (VAS)**: Proactively identifies vulnerabilities and prioritizes them.
- **Threat Hunting and Investigation**: Empowers SOC analysts to uncover hidden threats and investigate incidents.
- **Cloud Security Monitoring**: Seamlessly integrates with AWS, Azure, or GCP for cloud deployments.

2. **Open-Source Advantage**:
   - **Cost-Effectiveness**: Wazuh is budget-friendly, making it ideal for organizations conscious of costs.
   - **Customization**: The open-source code allows tailoring Wazuh to specific needs and seamless integration with existing security tools.
   - **Transparency and Security**: Community-driven development ensures continuous improvement and reliability.
3. **Wazuh Architecture**:
   - The architecture consists of:
     - **Wazuh Server**: Central component for managing agents, rules, and alerts.
     - **Elastic Stack**: Used for log storage, analysis, and visualization.
     - **Wazuh Agents**: Deployed on endpoints for data collection.
   - Clustering options provide **load balancing** and **high availability**.
4. **Deployment Steps**:
   - **Install Wazuh**: Set up the Wazuh server and deploy agents on endpoints.
   - **Configure Rules**: Customize rules to match your organization's security policies.
   - **Integrate with Elastic Stack**: Use Elasticsearch, Logstash, and Kibana for log analysis and visualization.
   - **Threat Hunting**: Empower analysts to proactively hunt for threats.
   - **Incident Response**: Define actions for detected incidents.
   - **Cloud Integration**: Extend monitoring to cloud environments.
5. **Why Choose Wazuh?**
   - **Versatility**: Whether you're a seasoned SOC warrior or just starting, Wazuh fits all sizes.
   - **Affordability**: No vendor lock-in, no license costs.
   - **Community Support**: Trusted by thousands of enterprise users.

Wazuh's open-source nature, powerful features, and cost-effectiveness make it an excellent choice for designing your CSOC. Arm your digital kingdom with vigilant guards and invisible shields!



Source: [Using Elasticsearch and TheHive to Build an Open-Source Security Emergency Response Platform_thehive csdn-CSDN Blog] (Translate to English)

I am going to provide you with the total solution design picture gradually, including the specifications, the sizing guides, the network BoQ, the firewall BoQ for better understanding the open-source based SOC design. Also, the following 2 network designs have a 1500 user base and another has a 350,000user base, which can adequately provide the insights desired by the SOC.

Products used in conjunction for developing the open source-based SOC:

1. Wazuh: Wazuh - Open Source XDR. Open Source SIEM.
2. Suricata: Home - Suricata
3. Snort: Snort - Network Intrusion Detection & Prevention System
4. Windows Sysmon: Sysmon - Sysinternals | Microsoft Learn
5. ELK Stack: Elasticsearch Platform — Find real-time answers at scale | Elastic
6. Cortex: TheHive-Project/Cortex: Cortex: a Powerful Observable Analysis and Active Response Engine (github.com)

7. TheHive: TheHive Project (thehive-project.org)
8. Filebeat: Filebeat: Lightweight Log Analysis & Elasticsearch | Elastic | elastic/beats: :tropical_fish: Beats - Lightweight shippers for Elasticsearch & Logstash (github.com)
9. Praeco: johnsusek/praeco: Elasticsearch alerting made simple. (github.com)
10. Vulnwhisperer: HASecuritySolutions/VulnWhisperer: Create actionable data from your Vulnerability Scans (github.com)
11. MISP: MISP/MISP: MISP (core software) - Open Source Threat Intelligence and Sharing Platform (github.com)
12. checkMK
13. Open UBA
14. Open-XDR

Wazuh and Associated Components Integrations

The integration links are provided below that can be used to integrate each services mentioned above.

- Deploying Wazuh agents using Windows Group Policy Objects (GPO) | Wazuh

At some point, it may seem that the above integrations could be an easy way to develop your open source-based SOC. but my team still has challenges because in most cases, these are community supported, and lots of other things can happen using free software's, they are not actually free. Also, I have the understanding that nothing is for free, and those software's can come with its internal challenges of data infiltration as well. Some cons:

1. Not fully interactable.
2. Services stopped running without any cause.
3. Data transfers can generate errors.
4. Individual model breaks.
5. Reinstallation takes place.
6. DB cannot be retrieved.
7. OS patches destroyed some applications.

Here are some insights for your SOC's hardware specification for an enterprise network, not to be taken seriously, but for discussion purpose and configuration management purpose, these designs are here to help you to specify the BoQ in total.

Pro-Tip

- Nothing is actually free, you need to look out for the trasmissions of your software services thats getting out of your network, block them! imagine a printer is sending out gigabytes of data to the outside of your network, it shouldn't have right? you are right.

Create a New Detection Rule in CSOC

Creating a new detection rule in a Cybersecurity Operations Center (CSOC) involves defining patterns, behaviors, or indicators of compromise (IoCs) that are associated with known threats. These rules are designed to trigger alerts when the logic returns True during log monitoring. Here's a general process to create a new detection rule:

1. **Identify the Threat**: Understand the threat you want to detect. This could be a specific type of malware, an attack pattern, or any suspicious behavior.
2. **Define the Rule**: Based on the threat, define a rule that can detect it. This usually involves specifying patterns or behaviors that are indicative of the threat.
3. **Implement the Rule in the SIEM System**: The Security Information and Event Management (SIEM) system is where these rules live. It's a tool used to aggregate and analyze log data from various sources. Implement your rules in this system.
4. **Test the Rule**: Once the rule is implemented, it's important to test it to ensure it's working as expected and not generating false positives.

For example, if you're a Security Engineer tasked with writing a Detection Rule to trigger whenever a log comes through alerting that a user authenticated successfully to AWS without using MFA, you would follow these steps.

The exact process can vary depending on the specific CSOC and the tools they use. It's always best to refer to your organization's specific guidelines or procedures for creating detection rules. If you're using a specific tool or platform and need more detailed instructions, please let me know!

An Example of a Detection Rule

Here are a couple of examples of detection rules:

1. **Monitoring Email Logs for Specific Domains**: This rule monitors email logs of user-sent emails and includes a filter criteria that checks for external recipient email address domain. It excludes a list of users (like the marketing team) who are known to send emails to external addresses.
2. **Brute-force Attack Detection**: This rule detects instances of brute-force attacks by looking for a large number of failed login attempts from the same IP address within a short period of time. The rule is defined as follows in Sigma format:

```
title: Brute-force attack detected
description: This rule detects instances of brute-force attacks
by looking for a large number of failed login attempts from the
same IP address within a short period of time.

author: John Doe
tags: brute-force, password guessing, security
index: audit
detection:
  selection:
    event_id: 4625
    log_name: security
  condition: selection: failed_login_count > 10 duration < 30m
ip_address = *
```

3. **Snort Rule for Win.Trojan.Doublepulsar Variant**: Network Intrusion Prevention Systems (NIPS) like Snort can block threats by leveraging rule-based detection. For example, the Snort rule Sid 1-42329 is able to detect the Win.Trojan.Doublepulsar variant.

The exact syntax and parameters can vary depending on the specific detection system or tool you are using.

Custom rule creation in Snort

Creating a custom rule in Snort involves defining the protocol, direction, source and destination IP addresses and ports, and rule options. Here's a step-by-step guide:

1. **Define the Protocol**: Specify the protocol you want to match. This can be ICMP, TCP, UDP, or other protocols.
2. **Determine the Direction**: Determine the direction of the traffic you want to match.

3. **Determine the Source and Destination IP Addresses and Ports**: Specify the source and destination IP addresses and ports.
4. **Define the Rule Options**: Specify the rule options.

For example, if you had a `malware.rules` file in the same directory as your Lua configuration file, you could include that rules file like so:

Lua
```
ips = { include =  'malware.rules'  }
```

If you want to include multiple .rules files, then you can do so like:

Lua
```
ips = { rules =  [[ include /path/to/rulesfile1.rules include
/path/to/rulesfile2.rules ]]  }
```

Alternatively, a single rules file or a path to a rules directory can be passed directly to Snort on the command line. This is done either with the `-R` option for a single rules file or the `--rule-path` option to pass in a whole directory of rules files.

For example, the below command will run all the rules present in `malware.rules` against the traffic in `bad.pcap`:

```
$ snort -c $my_path/lua/snort.lua -R malware.rules -r bad.pcap
```

It's always best to refer to your organization's specific guidelines or procedures for creating detection rules, they may already be laid out or standardized for your specific platform.

Testing Your Custom Rules to Ensure They Work as Expected

Here's a general process you can follow:

1. **Load the Rules**: First, make sure that your rules are loaded correctly. You can do this by running Snort with the `-T` option, which validates the configuration.

```
$ snort -c /path/to/snort.conf -T
```

2. **Run Snort with a PCAP File**: You can test your rules against a pcap file using the `-r` option. This allows you to see if your rules trigger any alerts with the given network traffic.

```
$ snort -c /path/to/snort.conf -R /path/to/rulesfile.rules -r
/path/to/test.pcap
```

3. Check the Alerts: Snort provides several “alert mode” options that can be set on the command line to tweak the way alerts are displayed. These modes include `cmg` which displays alerts alongside a hexdump of the alerting packet(s), as well as a few different `alert_*` modes.

```
$ snort -c /path/to/snort.conf -q -r /path/to/test.pcap -R
/path/to/rulesfile.rules -A cmg
```

Generate a Detection Rule for APT-41

APT41 is a prolific Chinese cyber threat group that carries out state-sponsored espionage activity in parallel with financially motivated operations. They are known to adapt quickly to changes and detections within victim environments, often recompiling malware within hours of incident responder activity.

Here’s an example of a Snort rule that could be used to detect APT41 activity based on the information available:

```
alert tcp any any -> $HOME_NET any (msg:"APT41 activity
detected"; flow:established,to_server; content:"|00 01 00 00 00
01 00 00 00 00 00 00|"; depth:12;
reference:url,mandiant.com/resources/blog/game-over-detecting-
and-stopping-an-apt41-operation; classtype:trojan-activity;
sid:1000001; rev:1;)
```

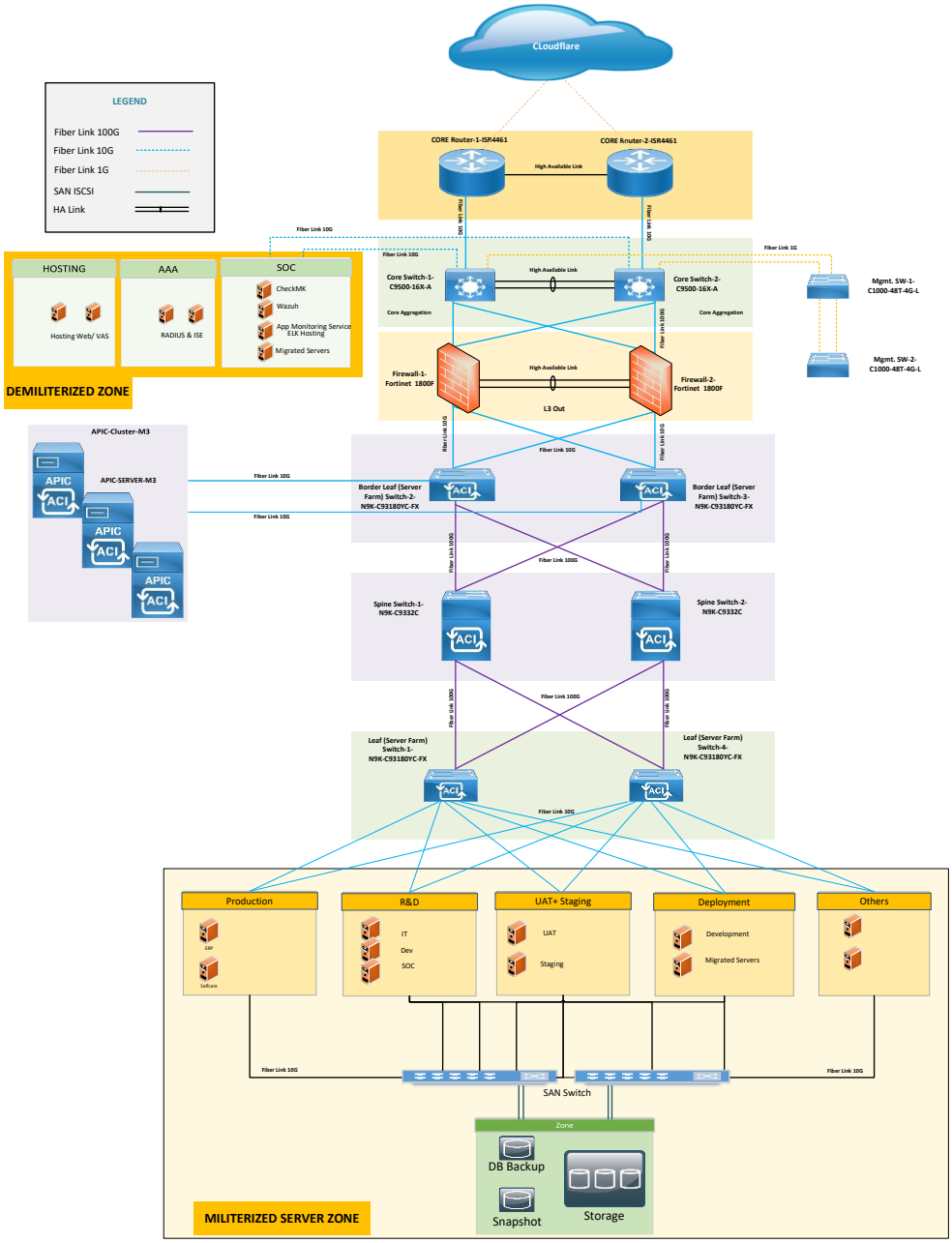
This rule will trigger an alert whenever it detects a TCP packet from any IP address and port to your home network (replace `$HOME_NET` with your network range) that contains the specific content pattern associated with APT41.

Please note that this is a simplified example and real-world detection rules might need to be more complex to accurately detect APT41 activity and reduce false positives. The exact content pattern, source, and destination you should use depend on the specific characteristics of APT41 that you want to detect.

Also, keep in mind that APT41 is known for its ability to adapt quickly to changes and detections within victim environments. Therefore, it's important to continuously update your detection rules to keep up with any new tactics, techniques, and procedures (TTPs) used by APT41.

The Network Design

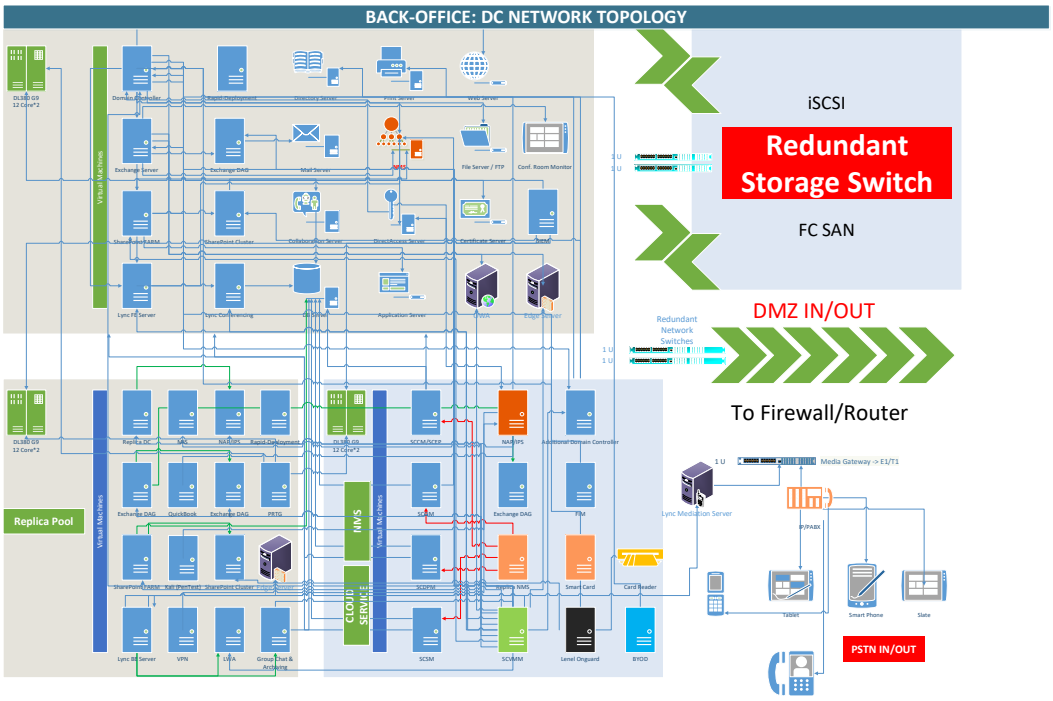
Please be mindful that all the SOC traffic should not be fed into the Firewall, but the SOC should be placed outside of the firewall, just like the design, but you are free to put it into the zones and collect all the data from within. In the below design, I will share the BoQ of each device, that might help you understand how to generate device specifications for your SOC. Though the BoQ's are shared in this study, the SOC is above the firewall, residing in the DMZ. You can separate them through a firewall as well, not shown in the design.


CLoudflare
LEGEND
Fiber Link 100G
Fiber Link 10G
Fiber Link 1G
SAN ISCSI
HA Link
CORE Router-1-ISR4461
CORE Router-2-ISR4461
High Available Link
HOSTING
AAA
SOC
Hosting Web/ VAS
RADIUS & ISE
CheckMK
Wazuh
App Monitoring Service ELK Hosting
Migrated Servers
DEMILITERIZED ZONE
Core Switch-1-C9500-16X-A
Core Switch-2-C9500-16X-A
Core Aggregation
Mgmt. SW-1-C1000-48T-4G-L
Mgmt. SW-2-C1000-48T-4G-L
Firewall-1-Fortinet 1800F
Firewall-2-Fortinet 1800F
L3 Out
APIC-Cluster-M3
APIC-SERVER-M3
Border Leaf (Server Farm) Switch-2-N9K-C93180YC-FX
Border Leaf (Server Farm) Switch-3-N9K-C93180YC-FX
Spine Switch-1-N9K-C9332C
Spine Switch-2-N9K-C9332C
Leaf (Server Farm) Switch-1-N9K-C93180YC-FX
Leaf (Server Farm) Switch-4-N9K-C93180YC-FX
Production
R&D
UAT+ Staging
Deployment
Others
IT
Dev
SOC
UAT
Staging
Development
Migrated Servers
SAN Switch
Zone
DB Backup
Snapshot
Storage
MILITERIZED SERVER ZONE

Back-office Network Design (1500 Users)

In summary, you should have the following items in your back-office (on-prem (3* HP DL380 G9 in total physical servers) and without HA for DR) (the Visio file is also provided in the job aids for your future use):

1. Active Directory or any LDAP or any RADIUS or any type of ID provider.
2. Email server: Exchange, SendMail, Postfix, cPanel based Squirrel Mail etc.
3. SharePoint or Private Cloud Services like OwnCloud or something similar.
4. Communication Stack: IM, CHAT, Conferencing like Lync/Teams.
5. System Center: SCCM, SCSM, SCDPM, SCOM, SCO, SCVMM etc.
6. Laptop Image Storage for image backup for rapid deployment.
7. IP Telephony, PSTN gateway.
8. File integrity monitoring (FIM).
9. Office door control and access control management.
10. Paessler PRTG or MRTG monitoring for data graph.
11. Storage backup for replication, snapshots etc.

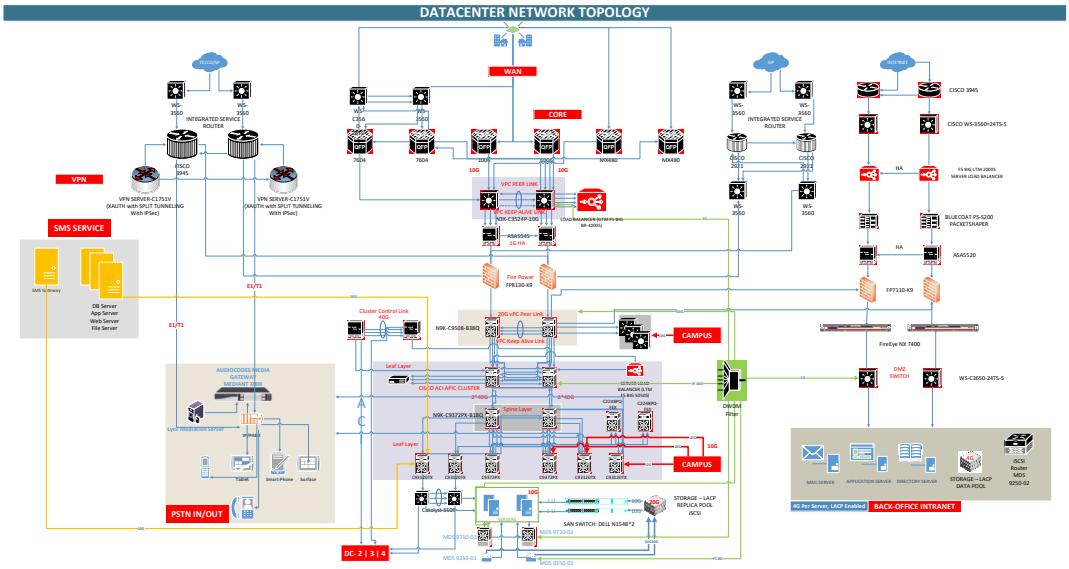


DETAILED PHYSICAL NETWORK DIAGRAM (Enterprise Architecture)

These designs, connectivity and integration ensure optimal network transmission for a small business with up-to 1500++ personnel. Make no mistake, the better the architecture, the better results, and integrations service it would provide for SOC data collection, monitoring and remediations.

Back-office Network Design (350K Users)

You should have your own design devised either by your team of architects or from a hired gun! But in any situation, you will need to specify what are the workflows, business requirements, and then map it out to the service requirements. Here campus means that there is a distribution network and connectivity requirements as well accommodating more than 350,000 user bases. Network capacity building is also an art, you can build whatever you want, but there is an “if”, whether you want to learn the transmission requirements as well, then you dive into these designs as time passes, and you are growing to become a race-horse, never stop, and don’t give up.



The above network is designed for providing the following services in addition to the back-office network, all in-house applications, monitoring, and management and then some more (the Visio file is also provided in the job aids for your future use):

1. Mass mailer service
2. Mass SMS service
3. ERP level developments

4. Integrated payment gateways etc.

VM List for Open-Source SOC Deployment

SL	Category	VM Name	Name	Purpose	IP Address
1	Syslog Server	FHSYSLOG (Syslog Server)	Syslog Server	Collect All Syslog from All devices	
2	Wazuh Cluster	FHWAINDEXER02{Wazuh Indexer (Elasticsearch)}	Wazuh Indexer01	Wazuh Master Node	
3		FHWAINDEXER01{Wazuh Indexer (Elasticsearch)}	Wazuh Indexer02	Wazuh Worker Node	
4		FHWASERVER (Wazuh Manager Server Master node)	Wazuh Server	Wazuh Server	
5		FHWALB01(Wazuh Load Balancer)	Loadbalancer01	Wazuh server LB	
6		FHWALB02(Wazuh Load Balancer)	Loadbalancer02	Wazuh server LB	
7		FHWADASHBOARD(Wazuh dashboard)	Wazuh Dashboard	Wazuh Dashboard	
8	ELK	FHELKAPM(APM)	Elastic Search	ELK with APM	
9		FHKIBANA(ELK Dashboard, Logstash)	APM with Kibana	ELK with APM	
10	IDS	FHSURICATA(IPS IDS)	Suricata	IDS & IPS	
11	IR	FHSOCTHEHIVE(MISP to TheHive)	Thehive	Case Management & Incident Responder	
12	Threat Intel	FHCORTEX (Threat Intel-Cortex)	Cortex		
13	Misp	FHSOCMISP(Malware Information Sharing Platform)	MISP		

14	OpnCTI Stack	FHTIOPENCTI01(Threat Intel(OpenCTI) for docker Swarm)	Stack Master	Docker swarm master	
15		FHTIOPENCTI02(Threat Intel(OpenCTI) for docker Swarm)	Stack worker	Docker swarm worker	

Physical Server BoQ (DELL): 2 Servers Required

Option	Selection	SKU / Product Code	Quantity
Base	PowerEdge R550 Server	[210-AZEG] / G8S6JX7	1
Motherboard	PowerEdge R550 Motherboard with Broadcom 5720 Dual Port 1Gb On-Board LOM	[329-BGIB] / GQLSN36	1
Trusted Platform Module	No Trusted Platform Module	[461-AADZ] / GMHJL5Y	1
Chassis	2.5" Chassis with up to 16 Hard Drives (SAS/SATA), 2 CPU	[321-BGSK] / G1PZLO9	1
Fans	Standard Fan Cold Swap 2U,V2 x5	[750-ADIN] / G2ZA0YM	1
Shipping	PowerEdge R550 Shipping	[340-CVKM] / GDE6JS2	1
Shipping Material	PowerEdge R550 Shipping Material	[343-BBRT] / GEUHQ4M	1
Regulatory	PowerEdge 2U CCC Marking, No BIS or CE Marking	[389-DYHB][389-DYMO] / GWVOG2D	1
OEM Regulatory	None		
Processor	Intel® Xeon® Silver 4316 2.3G, 20C/40T, 10.4GT/s, 30M Cache, Turbo, HT (150W) DDR4-2666	[338-CBWL] / GF0RKH9	1
Additional Processor	Intel® Xeon® Silver 4316 2.3G, 20C/40T, 10.4GT/s, 30M Cache,	[338-CBWL][379-BDCO] / G6AS94T	1

	Turbo, HT (150W) DDR4-2666		
Processor Thermal Configuration	Standard Heatsink for 2 CPU configuration	[412-AAVU][412-AAVU] / GF2HDPU	1
Memory DIMM Type and Speed	3200MT/s RDIMMs	[370-AEVR] / GR3CFNV	1
Memory Configuration Type	Performance Optimized	[370-AAIP] / GH9QBEI	1
Memory	64GB RDIMM, 3200MT/s, Dual Rank, 16Gb	[370-AEVP] / GQC5KJW	8
RAID	C1, No RAID for HDDs/SSDs (Mixed Drive Types Allowed)	[780-BCDI] / G8510ID	1
RAID/Internal Storage Controllers	Front HBA355i Rear Load	[405-AAXY][750-ACFQ] / GXRV4JM	1
Internal Optical Drive	No Internal Optical Drive	[429-AAIQ] / GZP2ROB	1
Storage	960GB SSD SATA Read Intensive 6Gbps 512 2.5in Hot-plug AG Drive, 1 DWPD	[400-AXSW] / GA16FX3	8
Boot Optimized Storage Cards	No BOSS Card	[403-BCID] / GIEP1Z6	1
Operating System	No Operating System	[611-BBBF] / G78MU35	1
OS Media Kits	No Media Required	[605-BBFN] / GKH7AZI	1
Embedded Systems Management	iDRAC9 Datacenter 15G	[528-CRVW] / G6CD9OH	1
Group Manager	iDRAC Group Manager, Enabled	[379-BCQV] / GTC0D81	1
Password	iDRAC, Factory Generated Password	[379-BCSF] / G2T768J	1
IDRAC Service Module	None		
OCP 3.0 Network Adapters	Broadcom 57412 Dual Port 10GbE SFP+, OCP NIC 3.0	[540-BCNT] / G81KH5Z	1
IDSDM Card Reader	None		
Internal SD Module	None		

Power Supply	Dual, Hot-Plug, Power Supply Fault Tolerant Redundant (1+1), 1100W MM (100-240Vac) Titanium, NAF	[450-AKLF] / GWT5F27	1
Power Cords	C13 to C14, PDU Style, 12 AMP, 6.5 Feet (2m) Power Cord, North America	[492-BBDI] / GC1DFVJ	4
Bezel	PowerEdge 2U LCD Bezel	[325-BEBV][350-BCFM] / G98L4KP	1
Quick Sync	No Quick Sync	[350-BCER] / GLUIZE1	1
BIOS and Advanced System Configuration Settings	Performance BIOS Setting	[384-BBBL] / GJO594B	1
Advanced System Configurations	UEFI BIOS Boot Mode with GPT Partition	[800-BBDM] / GSFTG4Y	1
Rack Rails	ReadyRails Static Rails for 2/4-post Racks	[770-BDZN] / GW0EL38	1
System Documentation	OpenManage DVD Kit, PowerEdge R550	[631-ADDZ] / GPO85GA	1
Secondary OS	None		
Enabled Virtualization	None		
Microsoft SQL Server	None		
Web Tracking	None		
OCONUS	None		
GSA Purchase Order	None		
SERVICES & SUPPORT			
Option	**Selection**	**SKU / Product Code**	**Quantity**
Protect your purchase - View Support offers below	Basic Next Business Day 36 Months, 36 Month(s)	[709-BBFL] / G32DMTS	1
Extended Services	NO WARRANTY UPGRADE SELECTED, 36 Month(s)	[883-BBBD] / GKQE3CR	1
Keep Your Hard Drive for Enterprise Services	None		
Keep Your Component for Enterprise Services	None		

Partner Operations Support	None		
Services: On-site Diagnosis Service	None		
Configuration Services Asset Report	None		
Enterprise Deployment Services	No Installation	[900-9997] / NOINSTL	1

Networking Device BoQ

Line Number	Part Number	Description	Service Duration (Months)	Estimated Lead Time (Days)	Qty
1.0	**ISR4461/K9 (CORE Router)**	Cisco ISR 4461 Router (2x10GE+4x1GE,3NIM,3SM,8G FLASH,4G DRAM)	---	70	2
1.0.1	CON-SNT-ISR44619	SNTC-8X5XNBD Cisco ISR 4461 (4GE,3NIM,3SM,8G FLASH,4G	60	N/A	2
1.1	SL-44-IPB-K9	IP Base License for Cisco ISR 4400 Series	---	28	2
1.2	PWR-4460-650-AC	650W AC Power Supply for Cisco ISR 4461	---	28	2
1.3	PWR-4460-650-AC2	Redundant 650W AC Power Supply for Cisco ISR 4461	---	28	2
1.4	CAB-C13-C14-2M	Power Cord Jumper, C13-C14 Connectors, 2 Meter Length	---	35	4
1.5	ACS-4460-FANASSY	Cisco ISR 4460 Fan Assembly	---	28	2
1.6	SM-F-BLANK	Fixed faceplate for SM slot on Cisco 4461 ISR	---	28	2
1.7	MEM-4460-DP-4G	4G DRAM for Cisco ISR 4460 Data Plane	---	28	2
1.8	POE-COVER-4450	Cover for empty POE slot on Cisco ISR 4450	---	28	4

1.9	NIM-BLANK	Blank faceplate for NIM slot on Cisco ISR 4400	---	28	2
1.10	SM-S-BLANK	Removable faceplate for SM slot on Cisco 2900,3900,4400 ISR	---	28	6
1.11	CAB-CONSOLE-RJ45	Console Cable 6ft with RJ45 and DB9F	---	14	2
1.12	CAB-CONSOLE-USB	Console Cable 6ft with USB Type A and mini-B	---	14	2
1.13	SISR44V2UK9173	Cisco ISR 4400 Series IOS XE Universal	---	28	2
1.14	SL-44-SEC-K9	Security License for Cisco ISR 4400 Series	---	28	2
1.15	SL-44-APP-K9	AppX License for Cisco ISR 4400 Series	---	28	2
1.16	FL-44-HSEC-K9	U.S. Export Restriction Compliance license for 4400 series	---	28	2
1.17	FL-4460-PERF-K9	Performance on Demand License for 4460 Series	---	28	2
1.18	MEM-4460-32G	32G DRAM (1 DIMM) for Cisco ISR 4460	---	28	2
1.19	MEM-FLSH-8GU32G	8G to 32G Flash Memory Upgrade for Cisco ISR 4460	---	28	2
1.20	NIM-ES2-8	8-port Layer 2 GE Switch Network Interface Module	---	70	2
1.21	NIM-SSD	NIM Carrier Card for SSD Drives	---	28	2
1.22	SSD-SATA-400G	400 GB, SATA Solid State Disk	---	28	2
		Server Farm Switch			
2.0	**N9K-C93180YC-FX (Core Switch)**	Nexus 9300 with 48p 1/10/25G, 6p 40/100G, MACsec	---	70	4
2.0.1	CON-SNT-N93YCFX	SNTC-8X5XNBD Nexus 9300 with 48p	60	N/A	4
2.1	NXK-AF-PI	Dummy PID for Airflow Selection Port-side Intake	---	14	4
2.2	NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	---	14	4

2.3	CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	---	70	8
2.4	NXA-PAC-500W-PI	Nexus NEBs AC 500W PSU - Port Side Intake	---	14	8
2.5	NXA-FAN-30CFM-B	Nexus Fan, 30CFM, port side intake airflow	---	7	16
2.6	C1E1TN9300 XF-5Y	Data Center Networking Essentials Term N9300 XF, 5Y	---	3	4
2.7	SVS-B-N9K-ESS-XF	EMBEDDED SOLN SUPPORT SWSS FOR ACI NEXUS 9K	---	3	4
2.8	MODE-ACI-LEAF	Dummy PID for mode selection	---	14	4
2.9	ACI-N9KDK9-16.0	Nexus 9500 or 9300 ACI Base Software NX-OS Rel 16.0	---	14	4
Management Switch					
3.0	**C1000-48T-4G-L**	Catalyst 1000 48port GE, 4x1G SFP	---	126	2
3.0.1	CON-SNT-C10T48GL	SNTC-8X5XNBD Catalyst 1000 48port GE, 4x1G SFP, LANBa	60	N/A	2
3.1	CAB-C15-CBN	Cabinet Jumper Power Cord, 250 VAC 13A, C14-C15 Connectors	---	14	2
3.2	PWR-CLP	Power Retainer Clip For 3560-C, 2960-L & C1000 Switches	---	14	2
CORE Aggregator Switch					
4.0	**C9500-16X-A**	Catalyst 9500 16-port 10Gig switch, Advantage	---	70	2
4.0.1	CON-SNT-C95K16XA	SNTC-8X5XNBD Catalyst 9500 16-por	60	N/A	2
4.1	CAB-C15-CBN	Cabinet Jumper Power Cord, 250 VAC 13A, C14-C15 Connectors	---	14	4
4.2	PWR-C4-950WAC-R	950W AC Config 4 Power Supply front to back cooling	---	14	2
4.3	PWR-C4-950WAC-R/2	950W AC Config 4 Power Supply front to back cooling	---	14	2
4.4	C9500-NW-A	C9500 Network Stack, Advantage	---	14	2

4.5	S9500UK9-179	Cisco Catalyst 9500 XE 17.9 UNIVERSAL	---	14	2
4.6	C9500-NM-8X	Cisco Catalyst 9500 8 x 10GE Network Module	---	14	2
4.7	C9500-DNA-16X-A	C9500 DNA Advantage, Term licenses	---	14	2
4.7.0.1	C9500-DNA-L-A-5Y	DNA Advantage 5 Year License	60	N/A	2
4.8	PI-LFAS-T	Prime Infrastructure Lifecycle & Assurance Term - Smart Lic	---	14	6
4.8.0.1	PI-LFAS-AP-T-5Y	PI Dev Lic for Lifecycle & Assurance Term 5Y	60	N/A	6
4.9	NETWORK-PNP-LIC	Network Plug-n-Play Connect for zero-touch device deployment	---	3	2
	Cisco 10G Fiber Module				
5.0	**SFP-10G-SR=**	10GBASE-SR SFP Module	---	14	70
6.0					
		Spine Switch - N9K-C9332C			
6.0.1	CON-SNT-N9KC9332	SNTC-8X5XNBD Nexus 9K ACI NX-OS Spine, 32p 40/100G	60	N/A	2
6.1	MODE-ACI-SPINE	Dummy PID for mode selection	---	14	2
6.2	NXK-AF-PI	Dummy PID for Airflow Selection Port-side Intake	---	14	2
6.3	ACI-N9KDK9-16.0	Nexus 9500 or 9300 ACI Base Software NX-OS Rel 16.0	---	14	2
6.4	NXK-ACC-KIT-1RU	Nexus 3K/9K Fixed Accessory Kit, 1RU front and rear removal	---	14	2
6.5	NXA-PAC-750W-PI	Nexus AC 750W PSU - Port Side Intake	---	14	4
6.6	NXA-FAN-35CFM-PI	Nexus Fan, 35CFM, port side intake airflow	---	70	10
6.7	CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	---	70	4
7.0	**APIC-CLUSTER-M3**	APIC Cluster - Medium Configurations (Up to 1200 Edge Ports)	---	14	1
7.0.1	CON-L1NBD-APICCLM3	CX LEVEL 1 8X5XNBD APIC Cluster Medium	60	N/A	1

7.1	APIC-SERVER-M3	APIC Appliance - Medium Configuration (up to 1200 Edge Ports)	---	14	1
7.2	APIC-DK9-5.2	APIC Base Software Release 5.2	---	14	1
7.3	APIC-PCIE-C25Q-04	Cisco APIC VIC 1455 Quad Port 10/25G SFP28 CNA PCIE	---	14	1
7.4	APIC-PSU1-770W	770W power supply for USC C-Series	---	14	2
7.5	APIC-TPM2-002	Trusted Platform Module 2.0 for UCS servers	---	14	1
7.6	APIC-RAID-M5	Cisco 12G Modular RAID controller with 2GB cache	---	14	1
7.7	APIC-HD1T7K12N	1 TB 12G SAS 7.2K RPM SFF HDD	---	14	2
7.8	APIC-CPU-3106	1.7 GHz 3106/85W 8C/11MB Cache/DDR4 2133MHz	---	14	2
7.9	APIC-SD800GK3X-EP	800GB 2.5in Enterprise Performance 12G SAS SSD (3X endurance)	---	14	1
7.10	APIC-MSTOR-SD	Mini Storage Carrier for SD (holds up to 2)	---	14	1
7.11	APIC-SD-32G-S	32GB SD Card for UCS servers	---	14	1
7.12	APIC-MR-X16G1RW	16GB RDIMM SRx4 3200 (8Gb)	---	14	6
7.13	APIC-SERVER-M3	APIC Appliance - Medium Configuration (up to 1200 Edge Ports)	---	14	1
7.14	APIC-DK9-5.2	APIC Base Software Release 5.2	---	14	1
7.15	APIC-PCIE-C25Q-04	Cisco APIC VIC 1455 Quad Port 10/25G SFP28 CNA PCIE	---	14	1
7.16	APIC-PSU1-770W	770W power supply for USC C-Series	---	14	2
7.17	APIC-TPM2-002	Trusted Platform Module 2.0 for UCS servers	---	14	1
7.18	APIC-RAID-M5	Cisco 12G Modular RAID controller with 2GB cache	---	14	1
7.19	APIC-HD1T7K12N	1 TB 12G SAS 7.2K RPM SFF HDD	---	14	2
7.20	APIC-CPU-3106	1.7 GHz 3106/85W 8C/11MB Cache/DDR4 2133MHz	---	14	2

7.21	APIC-SD800GK3X-EP	800GB 2.5in Enterprise Performance 12G SAS SSD (3X endurance)	---	14	1
7.22	APIC-MSTOR-SD	Mini Storage Carrier for SD (holds up to 2)	---	14	1
7.23	APIC-SD-32G-S	32GB SD Card for UCS servers	---	14	1
7.24	APIC-MR-X16G1RW	16GB RDIMM SRx4 3200 (8Gb)	---	14	6
7.25	APIC-SERVER-M3	APIC Appliance - Medium Configuration (Up to 1200 Edge Ports)	---	14	1
7.26	APIC-DK9-5.2	APIC Base Software Release 5.2	---	14	1
7.27	APIC-PCIE-C25Q-04	Cisco APIC VIC 1455 Quad Port 10/25G SFP28 CNA PCIE	---	14	1
7.28	APIC-PSU1-770W	770W power supply for USC C-Series	---	14	2
7.29	APIC-TPM2-002	Trusted Platform Module 2.0 for UCS servers	---	14	1
7.30	APIC-RAID-M5	Cisco 12G Modular RAID controller with 2GB cache	---	14	1
7.31	APIC-HD1T7K12N	1 TB 12G SAS 7.2K RPM SFF HDD	---	14	2
7.32	APIC-CPU-3106	1.7 GHz 3106/85W 8C/11MB Cache/DDR4 2133MHz	---	14	2
7.33	APIC-SD800GK3X-EP	800GB 2.5in Enterprise Performance 12G SAS SSD (3X endurance)	---	14	1
7.34	APIC-MSTOR-SD	Mini Storage Carrier for SD (holds up to 2)	---	14	1
7.35	APIC-SD-32G-S	32GB SD Card for UCS servers	---	14	1
7.36	APIC-MR-X16G1RW	16GB RDIMM SRx4 3200 (8Gb)	---	14	6
7.37	CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	---	70	2
7.38	CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	---	70	2
7.39	CAB-C13-CBN	Cabinet Jumper Power Cord, 250 VAC 10A, C14-C13 Connectors	---	70	2

8.0	**SFP-10G-SR=**	10GBASE-SR SFP Module	---	14	12
9.0	**QSFP-100G-SR4-S=**	100GBASE SR4 QSFP Transceiver, MPO, 100m over OM4 MMF	---	14	16
10.0	**GLC-TE=**	1000BASE-T SFP transceiver module for Category 5 copper wire	---	14	4
11.0	**GLC-SX-MMD=**	1000BASE-SX SFP transceiver module, MMF, 850nm, DOM	---	14	8

Fortinet Firewall BoQ

Item	SKU	Description	Qty
FortiGate-1800F	FG-1800F	4 x 40GE QSFP+ slots, 12 x 25GE SFP28 /10GE SFP+ slots, 2x10GE SFP+ HA slots, 8 x GE SFP slots, 18 x GE RJ45 ports. SPU NP7 and CP9 accelerated, dual AC power supplies	2
	FC-10-F18HF-928-02-60	FortiGate-1800F 5 Year Advanced Threat Protection (IPS, Advanced Malware Protection Service, Application Control, and FortiCare Premium)	2
	FC-10-F18HF-204-02-60	Upgrade FortiCare Premium to Elite (Require FortiCare Premium)-Five years	2
	FN-TRAN-SFP+SR	10GE SFP+ transceiver module, short range for systems with SFP+ and SFP/SFP+ slots	8
			14

There is a lot more to it than meets the eye for developing a functional SOC. It is not like any off-the-shelf software deployment that will end up working and providing services that's it supposed to. A SOC can be very tiresome to develop with in-house resources or buying a complete solution; though there is no complete solution yet, not even close. SOC frameworks and compliance requirements are aligning to its core requirements, but above functions under PPTD (people, process, technology, data) are still scarce, even though SIEM, CTI, IoC's OSINT, Cyber Counterintelligence (CCI) are playing their part, and yet Artificial Intelligence is now used to develop malicious codes.

But open-source solutions have ways to integrate to a much efficient SOC, but you will end up managing a large number of integrations and a blunder likely to occur when

upgrades or patches comes in. Moreover, you will need an army of team members to manage all the software components, tuning it precisely what you want out of it, producing actionable results.

This document is a broad example for developing your own SOC, at times, information overflow can be a daunting task to shape the documentation correctly, and the specific workings can vary based on the organization's size, needs and resources requirements.

BONUS CHAPTER 1

Project Management

THE SOC CANNOT BE DERIVED FROM A SINGULAR PERSON'S VIEW, IT REQUIRES BUSINESS (BPM) TO TECHNOLOGY MAPPING WHICH MUST HAVE INTEGRATION CAPABILITIES THROUGHOUT THE INFRASTRUCTURE, THAT'S WHERE ITS BEST TO LEAVE THE PROJECT MANAGEMENT TO THE RIGHT PERSONNEL. EVENTUALLY, YOU WILL END UP DERIVING BITS AND PIECES OF INFORMATION AND PUT TOGETHER, YOU WILL BECOME A PROJECT MANAGER AS WELL.

The below process groups reflect on how a project should be managed according to the PMI, assuming that you have a PMO in place to track project performance and relevant activities. Though this is a PMI standard, you are to initiate what works, doesn't have to be by the book, making it overly simplified, or overly complex, either of them is going to

land you with undesired results, and you have to be creative about how to place to your PMO and achieve your goal.

Project Management by PMI Terms

Knowledge Areas	Project Management Process Groups				
	Initiating Process Group	Planning Process Group	Executing Process Group	Monitoring and Controlling Process Group	Closing Process Group
4. Project Integration Management	4.1 Develop Project Charter	4.2 Develop Project Management Plan	4.3 Direct and Manage Project Work 4.4 Manage Project Knowledge	4.5 Monitor and Control Project Work 4.6 Perform Integrated Change Control	4.7 Close Project or Phase
5. Project Scope Management		5.1 Plan Scope Management 5.2 Collect Requirements 5.3 Define Scope 5.4 Create WBS		5.5 Validate Scope 5.6 Control Scope	
6. Project Schedule Management		6.1 Plan Schedule Management 6.2 Define Activities 6.3 Sequence Activities 6.4 Estimate Activity Durations 6.5 Develop Schedule		6.6 Control Schedule	
7. Project Cost Management		7.1 Plan Cost Management 7.2 Estimate Costs 7.3 Determine Budget		7.4 Control Costs	
8. Project Quality Management		8.1 Plan Quality Management	8.2 Manage Quality	8.3 Control Quality	
9. Project Resource Management		9.1 Plan Resource Management 9.2 Estimate Activity Resources	9.3 Acquire Resources 9.4 Develop Team 9.5 Manage Team	9.6 Control Resources	
10. Project Communications Management		10.1 Plan Communications Management	10.2 Manage Communications	10.3 Monitor Communications	
11. Project Risk Management		11.1 Plan Risk Management 11.2 Identify Risks 11.3 Perform Qualitative Risk Analysis 11.4 Perform Quantitative Risk Analysis 11.5 Plan Risk Responses	11.6 Implement Risk Responses	11.7 Monitor Risks	
12. Project Procurement Management		12.1 Plan Procurement Management	12.2 Conduct Procurements	12.3 Control Procurements	
13. Project Stakeholder Management	13.1 Identify Stakeholders	13.2 Plan Stakeholder Engagement	13.3 Manage Stakeholder Engagement	13.4 Monitor Stakeholder Engagement	

Table 1-4 (Guide). Project Management Process Group and Knowledge Area Mapping

The following project charter directly corresponds to the above BoQ, and the network design provided. You can take advantage of the format for your primary requirements. But do make changes as you see fit.

A very good starter kit can be found from the below link (combine and tailor to your need) for your all types of PM requirements, but make sure you use what's required, overly complicating things will not be understood by business personnel, which in turn, will complicate achieving your target, eyes on the ball!

Download the PM files from here: [850+ FREE Project Management Templates in Excel and Word (engineeringmanagement.info)]

Project Charter

Project Charter: Back-office Infrastructure Modernization		
General Project Information		
Project Name	Back-office Infrastructure Modernization	Extra Notes:
Project Sponsor	CEO	Most Importantly, this is initiated by the board member as the value presentation is provided multiple times. Securing and segmenting the core ERP system needs to be segmented as the network broadcast hits the ERP system infrastructure, and from security perspective, this infrastructure will be placed in a safe zone. Reason why the separation is required to secure the ERP and its associated services. This initiative is undertaken as the previous MIS went through a surgery and it's
Project Manager	xxxxxxxxxxxxxxxxx	
Email Address		
Phone Number	xxxxxxxxxxxxxx	
Organizational Unit	Information Security, I&I	
Process Impacted	M365, MIS, Server Re-allocations, VM's, according to the design etc.	
Expected Start Date	1st August 2023 (Assumed all HW Received)	
Expected Completion Date	27 Working Days	
Expected Savings (if any)	**N/A**	
Estimated Costs (BDT)	**N/A**	
Green Belts Assigned	N/A	

Black Belts Assigned	N/A	architecture were out of time and the old design flaws were making the application ineffective, thus the initiation of the TechStack needs to be in place to take the old MIS to a new ERP based architectural design. In order to do that, the platform needed to be upgraded to the latest build for speed, HA and monitoring purposes, microservices and latest technological advancement were introduced.

Describe the Problem or Issue, Goals, Objectives, and Deliverables of this Project	
Problem or Issue	Performance information related to the current MIS is not there and is not reliable and accurate as reported in the discussion groups. Processes are poorly defined, inconsistent, and prone to high error rates each month. Incidents were recorded of high severity, which led us to develop components, integrate new movements, and a complete makeover was required in order for the MIS to be functional. As the MIS is the heart of company's daily networked operations, its is of utmost interest that the back-office network is separated for the following primary reasons: 1. Separate office-network and its resources from the distribution network & retail network 2. Provide NGFW type firewall to provide secure access to the militarized zone 3. Block DDoS attacks on the ERP, M365 4. Block distribution network's unusual broadcasts, stop hits to the back-office network devices 5. Block unusual IP hits on the back-office networked, application, servers etc. 6. Enablement of application performance delivery and monitoring etc.

Purpose of Project	This project identifies root causes behind distortions with actual problems of the AD, ADC, AD-Azure Sync Servers, Synology backup servers and implement solutions to in capturing and reporting business losses accordingly, while finalizing a new ERP and redevelop the complete platform
Business Case	Critical business decisions regarding IT investments depend upon reliable and accurate cost information. The current process needs upgradation and there are development distortions in the reporting of actual costs for IT projects within the Project Management System. This project will attempt to fix this broken process and give management the correct information needed for properly managing multi-million-dollar investments in information technology for future readiness in an automated scalable and robust system. The main benefit of this project has to do with improving the integrity of the critical business application, data and the corresponding decision-making processes surrounding this data, security, access control, server-side monitoring, application monitoring such as the Monthly Performance Reports.
Goals / Metrics	Design and develop a complete set of solutions to address root causes behind the impairment of actual cost data in the Project Management System for the uncontrolled downtime of the platform, placed in the current datacenter. At the highest level, this involves two data streams, determine the full extent of the problem through data analysis, micromodule development, and other tests regarding the current platform establishment. Develop solutions for improving all the application and network processes and monitor the results of the implemented solutions with the CISO staff. Server VM migration study is not included here, this will be announced as per movement of server migration plan.
Expected Deliverables	Project Charter, newly developed network design, implementation plan, control Plans, and Project Summary Close Out
Define the Project Scope and Schedule	

Within Scope	This project is limited to only the project that are considered "developmental" since these project components must report development phases on the Azure DevOps. IS team will devise the transformation & movement checklist to transfer OLD-DC devices to the new DC Servers, which is mentioned in the plan & WBS document.
Outside of Scope	Projects not using the Project Management System will not be reviewed. Additionally, this project will not develop detailed system requirements for the Project Management System. The focus will be on the process itself and how the process relates to source systems for data, and other than the new network design, device installation, everything else is out of scope

Tentative Schedule (27 working days)

Key Milestone	Start		Complete
Form Project Team / Preliminary Review / Scope	TBA		TBA
Finalize Project Plan / Charter / Kick Off	TBA		TBA
Define Phase	TBA		TBA
Deploy IaaS and provision all physical servers	TBA		TBA
Measurement Phase	TBA		TBA
Analysis Phase	TBA		TBA
Improvement Phase	TBA		TBA
Control Phase	TBA		TBA
Project Summary Report and Close Out	TBA		TBA

Define the Project Resources and Costs

Project Team	Shahab Al Yamin Chawdhury. In addition to the ten (10) core team members, System Administrative support & deliverables is understood for the life cycle of the project.

Support Resources	Project Management Office staff will provide some administrative help. Projects that are reviewed may get tasked to help with data gathering and collection, HW movement etc.
Special Needs	At least two of the core team members will need network access to the Project Management System (Imran & Uzzal). The project will also need programming support to extract data from two other systems: All NMS and AppPlat NMS for IS Configuration & Verification.

Cost Type	Vendor / Labor Names	Rate-BDT	Qty	Amount-BDT
Labor	In House Developer Team	0	0	0
Colocation Addition (Monthly recurring chargeable items)	Rack (2) Power (2) Internet (40mbps)	0	0	0
3rd Party Channel Movement	3rd Party channel availability without having more than 3 HOP (source><DC><destination)	0	0	0
HW & SW Configuration	Cisco, Fortinet, DELL Storage, DELL Server, EMS & DC Accessories (Please see individual BoQ on different sheets)	0	0	0
Logistics	In House - Admin Team	0	0	0
VA/PT	In House - CSOC Team	0	0	0
Partner Support	Relevant partners for HW	0	0	0
Sanitization	In House - IS Team	0	0	0
Food & Hotel Cost	Support for In-house team members (Strategy Session)	0	0	0
		Total Cost		**0**

Define the Project Benefits and Customers

Process Owner	CISO owns the overall process over this movement reporting for the new application development (ERP), IT Hardware installation to the DC. Each Project Manager must make sure they follow a set of procedures for capturing and reporting actual costs correctly. The Project Management Office provides oversight and support for the processes and completion reporting of activities.
Key Stakeholders	All personnel assigned to IT Developmental Projects, including Project Managers, Project Analyst, Project Planners, Project Schedulers, and Budget Managers. All personnel who provide leadership support above the project level, including the Chief Information Security Officer, the CISO Staff, Directors and Senior Managers within the IT Department.
Final Customer	Chief Information Security Officer and Chief Technology Officer
Expected Benefits	Sustainable AppPlat, which now supports the ground for improvement, in terms of architectural superiority

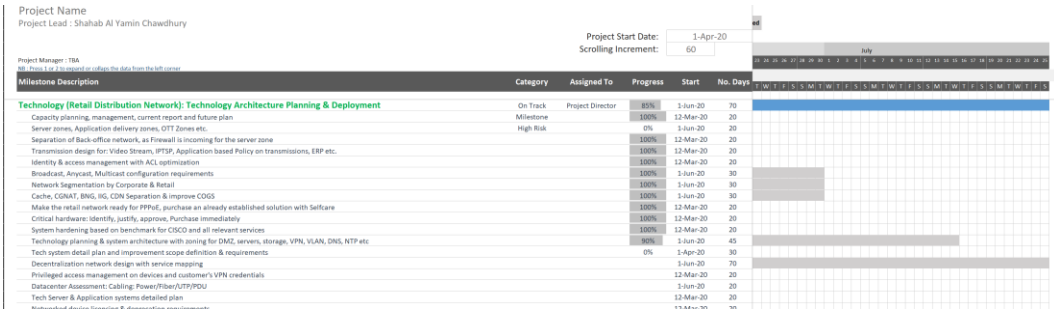
Tasks	Descriptions	Percentile
Power	Consistency of sustainable power and precision air conditioners in DC	99
Internet	Network & internet availability	99.99
Channel	3rd Party channel availability without having more than 3 HOP (source><DC><destination)	97
MNO	All MNO Connectivity with Fiber Backbone	97
3 Datacenter Links	Lambda ring network connectivity for DC, NDC, DR	98
Lambda speed	PDC to NDC or FDC is 2ms< | PDC & NDC to FDR 3ms<	98
Maintenance on DC	Manned maintenance	99
Monitoring	Network monitoring services (TBA)	98
Goal	DC Service Uptime Assurance to 98.00%	98
Application Platform Development	Clusters will be Installed into multiple physical servers	98

Describe Project Risks, Constraints, and Assumptions	
Risks	1. Changes to Project Scope - Project needs to stay focused on root causes behind the source data and not expand the project into developing system requirements for problems with various applications. 2. Bad Data - The availability of cost data within the Project Management System may be so poor that even a basic level of performance cannot be established. 3. Implementation of Solutions - This project will most likely require changes in how Project Managers currently capture and process DB data. In some cases, Project Managers may resist and refuse to adopt these new procedures and recommendations. Thus, the problem with bad data will continue. 4. The understanding of the stakeholder on ERP is somewhat limited, where reluctance to in-house delivery is not understood and intention to purchase 3rd party software & integrations can be continuous, even though the value of the MIS 2.0 may not be understood properly, as the stakeholders limited understanding on adding ad-hoc based solution could lead to an uncontrollable situation on cost, CR, access issues, access rights etc.
Constraints	1. Resources will be constrained to four full-time personnel + 1 System Administrator. IS team does not have adequate manpower to allocate any additional resources for this project. 2. The project team will have direct access to PMP or Six Sigma Black Belts, but the project will be constrained by the fact that a Certified Black Belt is not assigned full time to this project. 3. Programming support will be limited for the project and pulling extracts of data from source systems could be slow since a System Request must be submitted if canned extracts or queries are not adequately available.

Assumptions	1. The project is following a Six Sigma DMAIC approach. The organization has limited personnel who are experienced in doing projects according to this methodology. This project assumes that all stakeholders will understand and accept the six sigma related work products and deliverables. 2. This project has support from the CEO & MD and the PMO. This project assumes that this sponsorship and support is sufficient to push successful implementation of solutions that result from this project.
Prepared by:	Shahab Al Yamin Chawdhury Date: May 1, 2023

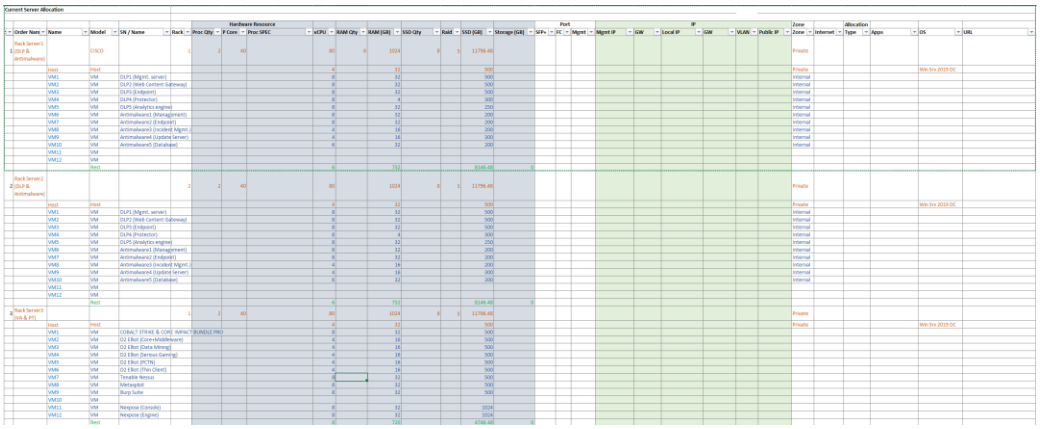
Project WBS

A sample project WBS could look like the following picture (the Gantt chart is provided in the job aids):



Virtual Machine Allocation Plan

The excel worksheet below is for your design and tracking purposes of how the VM's were deployed, and what resources are taken up from the physical server, due to the size of the worksheet, only a screenshot is provided, which I trust you can easily recreate. (also provided in the job aids)



BONUS CHAPTER 2

VA/PT Plan

A PLAN FOR THE VULNERABILITY ASSESSMENT AND PENETRATION TESTING NEEDS TO BE DERIVED IF YOU ARE UPGRADING CERTAIN INFRASTRUCTURE DEVICES OR ADDING A NEW SOC. THE FOLLOWING PLAN WAS DERIVED LONG BACK AND COULD HELP YOU GET STARTED.

Plan Document

Purpose

Complexity of systems is increasing day by day. This leads to more and more vulnerabilities in Systems. Attackers use these vulnerabilities to exploit the victim's system. It is better to find out these vulnerabilities in advance before the attacker do. The

power of Vulnerability assessment is usually underestimated. While Vulnerability Assessment and Penetration Testing can be used as a cyber-defense technology to provide proactive cyber defense with an enclosed proposal where we are fundamentally approving Vulnerability Assessment and Penetration Testing (VAPT) as a Cyber defense technology on our most critical systems. We will describe the complete life cycle of Vulnerability Assessment and Penetration Testing on systems or networks and afterwards proactive action will be taken to resolve that vulnerability and stop possible attacks in our systems.

We will describe complete process flow on how to use Vulnerability Assessment and Penetration Testing as a powerful Cyber Defense Technology and will authorize a PenTester (internal or hired) for conducting such testing on our critical systems. Primary focus areas for deploying an effective cyber security measure are:

a. Detection of network and all systems vulnerabilities
b. Initiate a Perimeter for Securing Internal Application Services
c. Limit and Monitor Access to Internal Network
d. Secure Application & Data Access within the network
e. Intrusion Detection & Prevention
f. Minimize Network Crawlers, Ransomwares, Zero Day Exploits
g. Layer-7 Intelligence and Granular Visibility
h. Prevention against Unknown Attacks
i. Threat Intelligence, Context, Granular Visibility on Modern Attacks

Scope of the Project

- **Hardware**. In particular, the servers that are used for hosting multiple critical services like applications, databases housed within virtual machines to be secured should be considered. Virtual Machines and their IP Addresses (155 VM's in total):

SL	Device Type	Quantity	DC/DR
1	Network Switch	11	DC and DR
2	Router	5	DC and DR
3	Firewall	3	DC and DR
4	Load Balancer/WAF	3	DC and DR
5	Blade Server	14	DC and DR
6	Rack Server	7	DC and DR
7	SAN Switch	4	DC and DR
8	Fabric Switch	4	DC and DR

	Total	51	

This is not limited to the following (not an exhaustive list):

SL	Task Description	Modality
1	Information gathering	
2	Requirement analysis	
3	Network diagram review	
4	Vulnerability scan from external	
5	Vulnerability scan from internal	
6	Vulnerability assessment for external	
7	Vulnerability assessment for internal	
8	Attack simulate	
9	Bruit force for SSH	
10	SQL injection	
11	execute exploit based on vulnerability	
12	DoS attack for web application	
13	Segmentation Test	
14	Configuration review	
15	Physical Site visit	
16	Follow up with team to resolve issues	
17	Generate Remediation Report Per Device	

Description of VAPT Services

A vulnerability is a weakness in the application which can be an implementation bug or a design flaw that allows an attacker to cause harm to the user of the application and get extra privilege. Vulnerability is the potential risk for the system. Attacker uses these vulnerabilities to exploit the system and get unauthorized and elevated access and information.

Vulnerabilities are a big flaw in system security and Information assurance. A vulnerability free system can provide more Information Assurance and system security. Though it is almost impossible to have a 100% vulnerability free system, but by removing as many vulnerabilities as possible, we can increase system security. The need of

Vulnerability Assessment and Penetration Testing is usually underestimated till now. It is just considered as a formal activity and use by very less people. By using regular and efficient Vulnerability Assessment, we can reduce the substantial amount of risk to be attacked and have more secured systems.

In this plan, we will describe Vulnerability Assessment and Penetration Testing as an important Cyber Defense Technology. By using VAPT as a Cyber Defense Technology, we can gradually remove vulnerabilities from our system and reduce the possibility of cyber-attack and harden each system. We will describe the complete life cycle of a VAPT for proactive defense. This will also provide a complete process on how to use VAPT as a cyber-defense strategy.

Vulnerability Assessment and Penetration Testing

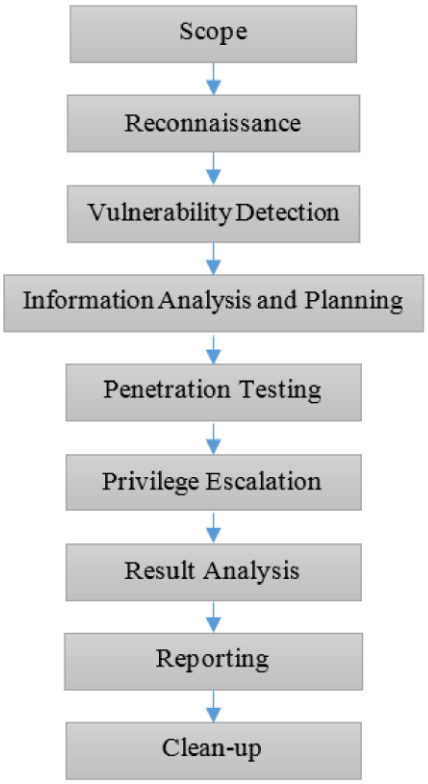
Vulnerability assessment is the process of scanning the system or software or a network to find out the weakness and loophole in that. These loopholes can provide backdoor to attacker to attack the victimized device or an application platform. A system may have access control vulnerability, Boundary condition vulnerability, Input validation vulnerability, Authentication Vulnerabilities, Configuration Weakness Vulnerabilities, and Exception Handling Vulnerabilities etc.

Penetration testing is the next step after vulnerability assessment. Penetration testing is to try to exploit the system in authorized manner to find out the possible exploits in the system. In penetration testing, the tester will have authority to do penetration testing and he intently exploits the system and find out possible exploits. We will provide replica VM's for testing, no live system will be tested, or no configuration will be changed to perform the VA & the PT.

Lifecycle of VAPT

Vulnerability Assessment and Penetration Testing is a total 9 step process. These steps are shown in the below figure. First, the tester has to decide the scope of the assignment (Black/grey/white box). After deciding the scope, the tester gets information about the operating system, network, and IP address in reconnaissance step. After this tester will use various vulnerability assessment technique (explained further) on the testing object to find out vulnerabilities. Then the tester analyses the found vulnerability and make plan for penetration testing. The tester uses this plan to penetrate the victim's system. After penetrating the system, the tester increases the privilege in the system. In result analysis

step, tester analyses all the results and devise recommendation to resolve the vulnerability from the system. All these activities are documented and sent to management to take suitable action. It is crucial to understand that IT Admins will be present during the penetration testing, and no systems will be internally touched / take control of the system / exploit its vulnerabilities and such activities will not take place, even no system or OS level components will not be altered at any point of time.



Vulnerability Assessment & penetration testing techniques

In this section, we will describe some popular VAPT techniques which will be used to conduct in our previously mentioned proposed systems.

Vulnerability Assessment technique

Static analysis

In this technique we do not execute any test case or exploit. We analyze the code structure and contents of the system. With this technique we can find out about all types of vulnerabilities. In this technique we do not exploit the system, so there would be no bad effect of this testing on the system. One of the big disadvantages of this technique is that it is quite slow and require many man-hours to perform.

Manual Testing

In this technique, we do not require any tool or any software to find out vulnerabilities. In this test the pentester uses his own knowledge and experience to find out the vulnerabilities in the system. This testing can be performed with prepared test plan (Systematic manual testing) or without any test plan (Exploratory manual testing). This technique costs higher compared to other techniques, because we do not need to buy any vulnerability assessment tool for this technique, but experience of the pentester is also very costly.

Automated Testing

In automated testing technique the pentester will use automated vulnerability testing tools to find out vulnerabilities in the system. These tools execute all the test cases to find out vulnerabilities. This reduces the man-hours and time required to perform testing. Because of tool repeated testing can also be performed very easily.

Automated testing provides better accuracy than what other techniques provide. It takes very less time and same test cases can be used for future operations over again. But tools increase cost of testing. A single tool is not capable to find out all type of vulnerabilities. So, this increases the total cost to perform vulnerability assessment.

Fuzz Testing

In this test the pentester will try to get response from the system. To check if the system returns or responds or the system crashes or completely gets unresponsive. This is like robustness testing. This technique can be applied with very less human interaction. This technique also can be used to find out zero-day vulnerability.

Penetration Testing Techniques

Black Box Testing

In this technique, the tester does not have any prior knowledge of the network architecture or systems of the testing network. Usually, black box testing is performed from external

network to internal network. A tester have to use his expertise and skills to perform this testing.

Grey Box Testing

In this technique, the tester has some partial knowledge of the testing network. Tester do not have knowledge of complete network architecture, but he will know some basic information of testing network and system configuration. In actuality, Grey box testing is the combination of both the other techniques. This can be performed from internal or external network.

White Box Testing

Testers have complete knowledge of the network configuration of the testing network and the system configuration of the testing network/system. Usually, this testing is performed from the internal network. White box testing requires deep understanding of the testing network or system and provides better results.

Vulnerability Assessment and Penetration Testing Tools

There are many open sources or premium VAPT tools available in the market. Every tool has its expertise and limitations. In Table 1 we have listed Top 15 VAPT tools, their usage and the operating systems on which they are compatible. These make VAPT process fast and more accurate to assess and detect vulnerability in a given system.

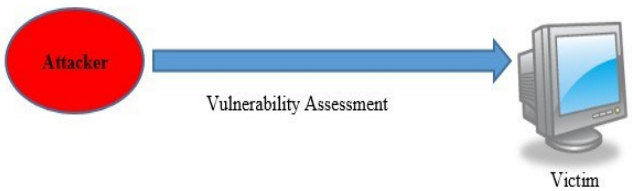
Table: Top 15 VAPT tools.

NO.	Name	License	Type	Operating System
1	Metasploit	Proprietary	Vulnerability scanner and exploit	Cross-platform
2	Nessus	Proprietary	Vulnerability scanner	Cross-platform
3	Kali Linux	GPL	Collection of various tools	Linux
4	Burp Suite	Proprietary	web vulnerability scanner	Cross-platform
5	w3af	GPL	web vulnerability scanner	Cross-platform
6	OpenVAS	GPL	Vulnerability scanner	Cross-platform
7	Paros proxy	GPL	web vulnerability scanner	Cross-platform
8	Core Impact	Proprietary	Vulnerability scanner and exploit	Windows
9	Nexpose	Proprietary	Entire vulnerability management lifecycle	Linux, Windows
10	GFI LanGuard	Proprietary	Vulnerability scanner	Windows

11	Acunetix WVS	Proprietary	web vulnerability scanner	Windows
12	QualysGuard	Proprietary	Vulnerability scanner	Cross-platform
13	MBSA	Freeware	Vulnerability scanner	Windows
14	AppScan	Proprietary	web vulnerability scanner	Windows
15	Canvas	Proprietary	Vulnerability scanner and exploit	Cross-platform

VA/PT As A Cyber Defense Technology

In this section we will show how we can consider vulnerability analysis as a cyber-defense technology. What usually attacker do is he reconnaissance the victim's network and get information about victim's network. After receiving system information, attacker performs vulnerability assessment on the victim's network/system and generate a vulnerability list. This is shown in the below picture.



After getting the vulnerability list of the victim, the attacker plans for the possible attack layer by layer. With that list enriches gradually, the attacker exploits the victim's network or system and compromises his system security and information. This is shown in the below picture. But if Victim removes majority of the vulnerabilities from his system, the attacker would not be able to exploit the victim's network/system. By applying VAPT technique user can find out the vulnerabilities those can result in various severe attacks like – Zero-day exploits, DDoS attack, RA flooding, ARP poisoning etc. After finding out the vulnerabilities, a user can apply countermeasures against them. To fix the system from known vulnerabilities, Administrator should find out vulnerabilities in his own system/network. The administrator should apply complete vulnerability and penetration testing cycle on the system/network. When the administrator gets the list of available vulnerability in his system, he should remove those vulnerabilities. To remove the vulnerabilities, the administrator should apply the necessary patches, updates, install

necessary software's and other requisites. In this way an administrator should remove all vulnerabilities from his system/network.

Figure 1 Attacker exploiting victim's system

Now, if the attacker would run a vulnerability assessment of the victim's system/network, he would not find any known open vulnerability in the victim's system/network. In the absence of open vulnerabilities in the system, the attacker would not be able to exploit victim's system/network. Therefore, by using Vulnerability Assessment and Penetration Testing as a cyber- defense, technology administrators can be able to save his resources and critical information and can achieve proactive cyber defense.

Conclusion and Future Work

In this plan, we have explained how Vulnerability Assessment and Penetration Testing can be used as an effective cyber defense technology. We have also described why VAPT should be made a compulsory activity for cyber defense in a periodic manner. This document clearly explains the necessity to increase use of VAPT for complete system security and would be able to withstand open and known system vulnerabilities, and can stop major cyber-attacks and would be able to provide hardened system security.

Point of Contact

Communicating points of contact for all phases of a project is vital in order to ensure stakeholders understand who can address questions or concerns related to various aspects of the project. This is especially true for implementation and migration of applications as this may be an extremely fluid part of the project, and the responsibility may be shifting from one IT Group to another.

The VAPT Testing Project spans several different levels of operations of the company is an extremely fluid in technical projects. As such, it is important to understand the points of contact for the various aspects of this project. The chart below provides all stakeholders with points of contact should any urgent questions or concerns arise. All stakeholders should ensure their communications are compliant with the VAPT Testing Plan.

Name	Role	Contact Information
TBA	Project Sponsor	
TBA	Independent Director	
Shahab Al Yamin Chawdhury	CISO	
	IT Admin	
	IT Admin	
TBA	Project Manager	

Project Manager Nomination

I/We hereby undersigned nominate the following person to be the **"Project Director"** for the deployment of **"VA/PT Testing"**:

Name	Title	Date
Nomination Accepted by SHAHAB AL YAMIN CHAWDHURY	 CISO	

Computer Forensic & Cyber Security Tools, Open-Source)

Disk Tools & Data Capture

Name	From	Description
Arsenal Image Mounter	Arsenal Recon	Mounts disk images as complete disks in Windows, giving access to Volume Shadow Copies, etc.
DumpIt	MoonSols	Generates physical memory dump of Windows machines, 32 bits 64 bit. Can run from a USB flash drive.
EnCase Forensic Imager	Guidance Software	Create EnCase evidence files and EnCase logical evidence files [direct download link]
Encrypted Disk Detector	Magnet Forensics	Checks local physical drives on a system for TrueCrypt, PGP, or Bitlocker encrypted volumes.
FAT32 Format	Ridgecrop	Enables large capacity disks to be formatted as FAT32.
Forensics Acquisition of Websites	Web Content Protection Association	Browser designed to forensically capture web pages.
FTK Imager	AccessData	Imaging tool, disk viewer and image mounter.
Guymager	vogu00	Multi-threaded GUI imager under running under Linux.
Live RAM Capturer	Belkasoft	Extracts RAM dump including that protected by an anti-debugging or anti-dumping system. 32 and 64 bit builds
NetworkMiner	Hjelmvik	Network analysis tool. Detects OS, hostname and open ports of network hosts through packet sniffing/PCAP parsing.
Nmap	Nmap	Utility for network discovery and security auditing.
Magnet RAM Capture	Magnet Forensics	Captures physical memory of a suspect's computer. Windows XP to Windows 10, and 2003, 2008, 2012. 32 & 64 bit.

OSFClone	Passmark Software	Boot utility for CD/DVD or USB flash drives to create dd or AFF images/clones.
OSFMount	Passmark Software	Mounts a wide range of disk images. Also allows creation of RAM disks.

Email Analysis

Name	From	Description
EDB Viewer	Lepide Software	Open and view (not export) Outlook EDB files without an Exchange server.
Mail Viewer	MiTeC	Viewer for Outlook Express, Windows Mail/Windows Live Mail, Mozilla Thunderbird message databases and single EML files.
MBOX Viewer	SysTools	View MBOX emails and attachments.
OST Viewer	Lepide Software	Open and view (not export) Outlook OST files without connecting to an Exchange server.
PST Viewer	Lepide Software	Open and view (not export) Outlook PST files without needing Outlook.

General Tools

Name	From	Description
Agent Ransack	Mythicsoft	Search multiple files using Boolean operators and Perl Regex.
Computer Forensic Reference Data Sets	NIST	Collated forensic images for training, practice and validation.
EvidenceMover	Nuix	Copies data between locations, with file comparison, verification, logging.
FastCopy	Shirouzu Hiroaki	Self labelled ‘fastest’ copy/delete Windows software. Can verify with SHA-1, etc.
File Signatures	Gary Kessler	Table of file signatures.
HexBrowser	Peter Fiskerstrand	Identifies over 1000 file types by examining their signatures.

HashMyFiles	Nirsoft	Calculate MD5 and SHA1 hashes.
MobaLiveCD	Mobatek	Run Linux live CDs from their ISO image without having to boot to them.
Mouse Jiggler	Arkane Systems	Automatically moves mouse pointer stopping screen saver, hibernation etc..
Notepad ++	Notepad ++	Advanced Notepad replacement.
NSRL	NIST	Hash sets of 'known' (ignorable) files.
Quick Hash	Ted Technology	A Linux & Windows GUI for individual and recursive SHA1 hashing of files.
USB Write Blocker	DSi	Enables software write-blocking of USB ports.
Volix	FH Aachen	Application that simplifies the use of the Volatility Framework.
Windows Forensic Environment	Troy Larson	Guide by Brett Shavers to creating and working with a Windows boot CD.

File and Data Analysis

Name	From	Description
Advanced Prefetch Analyser	Allan Hay	Reads Windows XP,Vista and Windows 7 prefetch files.
analyzeMFT	David Kovar	Parses the MFT from an NTFS file system allowing results to be analysed with other tools.
bstrings	Eric Zimmerman	Find strings in binary data, including regular expression searching.
CapAnalysis	Evolka	PCAP viewer.
Crowd Response	CrowdStike	Windows console application to aid gathering of system information for incident response and security engagements.
Crowd Inspect	CrowdStrike	Details network processes, listing binaries associated with each process. Queries VirusTotal, other malware repositories & reputation services to produce "at-a-glance" state of the system.

DCode	Digital Detective	Converts various data types to date/time values.
Defraser	Various	Detects full and partial multimedia files in unallocated space.
eCryptfs Parser	Ted Technology	Recursively parses headers of every eCryptfs file in selected directory. Outputs encryption algorithm used, original file size, signature used, etc.
Encryption Analyzer	Passware	Scans a computer for password-protected & encrypted files, reports encryption complexity and decryption options for each file.
ExifTool	Phil Harvey	Read, write and edit Exif data in a large number of file types.
File Identifier	Toolsley.com	Drag and drop web-browser JavaScript tool for identification of over 2000 file types.
Forensic Image Viewer	Sanderson Forensics	View various picture formats, image enhancer, extraction of embedded Exif, GPS data.
Ghiro	Alessandro Tanasi	In-depth analysis of image (picture) files.
Highlighter	Mandiant	Examine log files using text, graphic or histogram views.
Link Parser	4Discovery	Recursively parses folders extracting 30+ attributes from Windows .lnk (shortcut) files.
LiveContactsView	Nirsoft	View and export Windows Live Messenger contact details.
PECmd	Eric Zimmerman	Prefetch Explorer.
RSA Netwitness Investigator	EMC	Network packet capture and analysis.

Mac OS Tools

Name	From	Description
Audit	Twocanoes Software	Audit Preference Pane and Log Reader for OS X.

Disk Arbitrator	Aaron Burghardt	Blocks the mounting of file systems, complimenting a write blocker in disabling disk arbitration.
Epoch Converter	Blackbag Technologies	Converts epoch times to local time and UTC.
FTK Imager CLI for Mac OS	AccessData	Command line Mac OS version of AccessData's FTK Imager.
IORegInfo	Blackbag Technologies	Lists items connected to the computer (e.g., SATA, USB and FireWire Drives, software RAID sets). Can locate partition information, including sizes, types, and the bus to which the device is connected.
mac_apt	Yogesh Khatri, Champlain College	Mac OS triage tool, works usable against E01, DD, DMG and mounted images
Volafox	Kyeongsik Lee	Memory forensic toolkit for Mac OS X

Mobile Devices

Name	From	Description
iPBA2	Mario Piccinelli	Explore iOS backups.
iPhone Analyzer	Leo Crawford, Mat Proud	Explore the internal file structure of Pad, iPod and iPhones.
ivMeta	CSI Tech	Extracts phone model and software version and created date and GPS data from iPhone videos.
SAFT	SignalSEC Corp	Obtain SMS Messages, call logs and contacts from Android devices.

Data Analysis Suites

Name	From	Description
Autopsy	Brian Carrier	Graphical interface to the command line digital investigation analysis tools in The Sleuth Kit (see below).

Backtrack	Backtrack	Penetration testing and security audit with forensic boot capability.
Caine	Nanni Bassetti	Linux based live CD, featuring a number of analysis tools.
Digital Forensics Framework	ArxSys	Analyses volumes, file systems, user and applications data, extracting metadata, deleted and hidden items.
Forensic Scanner	Harlan Carvey	Automates 'repetitive tasks of data collection'. Fuller description here.
Kali Linux	Offensive Security	Comprehensive penetration testing platform
Paladin	Sumuri	Ubuntu based live boot CD for imaging and analysis.
SIFT	SANS	VMware Appliance pre-configured with multiple tools allowing digital forensic examinations.
The Sleuth Kit	Brian Carrier	Collection of UNIX-based command line file and volume system forensic analysis tools.
Volatility Framework	Volatile Systems	Collection of tools for the extraction of artefacts from RAM.

File Viewers

Name	From	Description
BKF Viewer	SysTools	https://www.systoolsgroup.com/lotus-dxl-viewer.html
DXL Viewer	SysTools	View (not save or export) Loutus Notes DXL file emails and attachments.
E01 Viewer	SysTools	View (not save or export from) E01 files & view messages within EDB, PST & OST files.
MDF Viewer	SysTools	View (not save or export) MS SQL MDF files.
MSG Viewer	SysTools	View (not save or export) MSG file emails and attachments.
OLM Viewer	SysTools	View (not save or export) OLM file emails and attachments.

Internet Analysis

Name	From	Description
Browser History Capturer	Foxton Software	Captures history from Firefox, Chrome, Internet Explorer and Edge web browsers running on Windows computers.
Browser History Viewer	Foxton Software	Extract, view and analyse internet history from Firefox, Chrome, Internet Explorer and Edge web browsers.
Chrome Session Parser	CCL Forensics	Python module for performing off-line parsing of Chrome session files (“Current Session”, “Last Session”, “Current Tabs”, “Last Tabs”).
ChromeCacheView	Nirsoft	Reads the cache folder of Google Chrome Web browser, and displays the list of all files currently stored in the cache.
Cookie Cutter	Mike’s Forensic Tools	Extracts embedded data held within Google Analytics cookies. Shows search terms used as well as dates of and the number of visits.
Dumpzilla	Busindre	Runs in Python 3.x, extracting forensic information from Firefox, Iceweasel and Seamonkey browsers. See manual for more information.
Facebook Profile Saver	Belkasoft	Captures information publicly available in Facebook profiles.
IECookiesView	Nirsoft	Extracts various details of Internet Explorer cookies.
IEPassView	Nirsoft	Extract stored passwords from Internet Explorer versions 4 to 8.
MozillaCacheView	Nirsoft	Reads the cache folder of Firefox/Mozilla/Netscape Web browsers.
MozillaCookieView	Nirsoft	Parses the cookie folder of Firefox/Mozilla/Netscape Web browsers.
MozillaHistoryView	Nirsoft	Reads the history.dat of Firefox/Mozilla/Netscape Web browsers, and displays the list of all visited Web page.

MyLastSearch	Nirsoft	Extracts search queries made with popular search engines (Google, Yahoo and MSN) and social networking sites (Twitter, Facebook, MySpace).
PasswordFox	Nirsoft	Extracts the user names and passwords stored by Mozilla Firefox Web browser.
OperaCacheView	Nirsoft	Reads the cache folder of Opera Web browser, and displays the list of all files currently stored in the cache.
OperaPassView	Nirsoft	Decrypts the content of the Opera Web browser password file, wand.dat
Web Historian	Mandiant	Reviews list of URLs stored in the history files of the most commonly used browsers.
Web Page Saver	Magnet Forensics	Captures how web pages look at a specific point in time

Registry Analysis

Name	From	Description
AppCompatCache Parser	Eric Zimmerman	Dumps list of shimcache entries showing which executables were run and their modification dates. Further details.
ForensicUserInfo	Woanware	Extracts user information from the SAM, SOFTWARE and SYSTEM hives files and decrypts the LM/NT hashes from the SAM file.
Process Monitor	Microsoft	Examine Windows processes and registry threads in real time.
RECmd	Eric Zimmerman	Command line access to offline Registry hives. Supports simple & regular expression searches as well as searching by last write timestamp. Further details.
Registry Decoder	US National Institute of Justice, Digital Forensics Solutions	For the acquisition, analysis, and reporting of registry contents.

Registry Explorer	Eric Zimmerman	Offline Registry viewer. Provides deleted artefact recovery, value slack support, and robust searching. Further details.
RegRipper	Harlan Carvey	Registry data extraction and correlation tool.
Regshot	Regshot	Takes snapshots of the registry allowing comparisons e.g., show registry changes after installing software.
ShellBags Explorer	Eric Zimmerman	Presents visual representation of what a user's directory structure looked like. Additionally exposes various timestamps (e.g., first explored, last explored for a given folder. Further details.
USB Device Forensics	Woanware	Details previously attached USB devices on exported registry hives.
USB Historian	4Discovery	Displays 20+ attributes relating to USB device use on Windows systems.
USBDeview	Nirsoft	Details previously attached USB devices.
PasswordFox	Nirsoft	Extracts the user names and passwords stored by Mozilla Firefox Web browser.
UserAssist	Didier Stevens	Displays list of programs run, with run count and last run date and time.
Windows Registry Recovery	MiTec	Extracts configuration settings and other information from the Registry.

Application Analysis

Name	From	Description
DFIR	Magnet Forensics	Various Tools
Google Maps Tile Investigator	Magnet Forensics	Takes x,y,z coordinates found in a tile filename and downloads surrounding tiles providing more context.
KaZAlyser	Sanderson Forensics	Extracts various data from the KaZaA application.
LiveContactsView	Nirsoft	View and export Windows Live Messenger contact details.
SkypeLogView	Nirsoft	View Skype calls and chats.

For Reference

Name	From	Description
HotSwap	Kazuyuki Nakayama	Safely remove SATA disks similar to the “Safely Remove Hardware” icon in the notification area.
IEHistoryView	Nirsoft	Extracts recently visited Internet Explorer URLs.
LiveView	CERT	Allows examiner to boot dd images in VMware.
Ubuntu guide	How-To Geek	Guide to using an Unbuntu live disk to recover partitions, carve files, etc.
WhatsApp Forensics	Zena Forensics	Extract WhatApp messages from iOS and Android backups.
iPhone Backup Browser	Rene Devichi	View unencrypted backups of iPad, iPod and iPhones.

Password Protection

Name	From	Description
Password Strength Test	How Secure Is My Password	Enter your password and see how long it will take for a computer to crack it
Secure Password Check	Kaspersky	Check how secure a password is
Password Manager	LastPass	Password storer with AES-256 bit encryption with PBKDF2 SHA-256 and salted hashes.
Password Manager	StickyPassword	Password Manager using AES-256 encryption

Password Hacking Protection

Name	From	Description

HaveIBeenPwnd	haveibeenpwned	Check if you have an account that has been compromised in a data breach

Browsing Security

Name	From	Description
No Script	NoScript	NoScript Firefox extension provides extra protection for Firefox, Seamonkey and other mozilla-based browsers
Comodo Dragon	Comodo Cybersecurity	A Chromium technology-based Web Browser that offers you all of Chrome's features PLUS the unparalleled level of security and privacy
TOR	TOR Project	Experience real private browsing without tracking, surveillance, or censorship.
Disconnect	Disconnect	Get greater transparency and control over the personal information you share online

Redirect Checkers

Name	From	Description
Where Goes	Where Goes	takes a URL and shows you the entire path of redirects and meta-refreshes that leads to the final destination.
Redirect Detective	Redirect Detective	Redirect Detective is a free URL redirection checker that allows you to see the complete path a redirected URL goes through.
Redirect Check	Redirect Check	This site is used to chase the redirection of URLs.

Website URL Checkers

Name	From	Description

VirusTotal	Virus Total	Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community
ScanURL	Scan URL	See if a website has been reported for phishing, hosting malware/viruses, or poor reputation. We check with reputable 3rd-party services, such as Google Safe Browsing Diagnostic, PhishTank, and Web of Trust (WOT).
Site Safety Center	TrendMicro	can check the safety of a particular URL that might seem suspicious
Zulu	Zscaler	Zulu is a dynamic risk scoring engine for web based content

Data Removal

Name	From	Description
Eraser	Heidi	Completely remove sensitive data from your hard drive

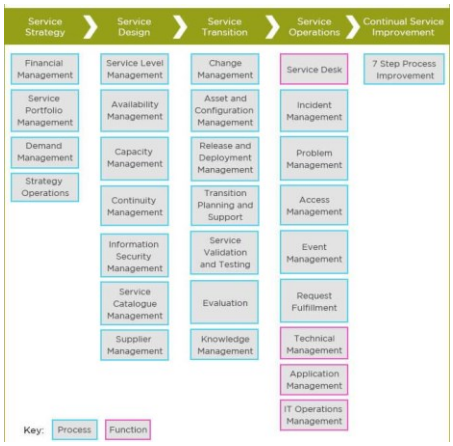
BONUS CHAPTER 3

IT Service Strategy Planning

SINCE YOUR HELPDESK WILL BE THE EPICENTER OF ALERTS OF SERVICE CALLS AND GENERATION OF TICKET, ITS ALWAYS BENEFICIAL TO INTEGRATE THE SERVICE OR SUPPORT OR YOUR CALL CENTER TO THE SAME CAUSE. YOU ARE ALSO FREE TO HAVE A SEPARATE SOC CALL CENTER AS WELL IF YOU HAVE THE EXTRA BUDGET.

Service Strategy deals with the strategic analysis, planning, positioning, and implementation relating to IT service models, strategies, and objectives. It provides guidance on leveraging service management capabilities to effectively deliver value to customers and illustrates value for service providers. In short:

Process & Functions



The following people, process and products combine to make this a functional operating unit with IT:

- People
    - Service Definition Manager

    - Service Research Manager
    - Financial Analysis Manager
    - Service Marketing Manager
    - Service Forecast Manager
- Process
    - Portfolio Management
    - Financial Management
    - Demand Management
- Products
    - Service Request & Planning Tools
    - Service Knowledge & Configuration Management Tools

IT Service Design –Modeling the IT Services

Service Design translates strategic plans and objectives and creates the designs and specifications for execution through service transition and operations.

- People
    - Enterprise Architect: Network, NOC, SOC
    - Application Architect
    - Security Engineering Manager
    - Desktop Engineering Manager
    - Network Engineering Manager
    - Systems, Servers & Storage Engineering Manager
    - Applications Engineering Manager
- Process
    - Service Catalogue Management
    - Service Level Management
    - Capacity Management
    - Availability Management
    - Continuity Management
    - Information Security Management
    - Supplier Management
- Products
    - Service Catalogue Tools
    - Service Level Management Tools
    - Capacity Planning Tools
    - Service Modeling Tools
    - Service Knowledge & Configuration Management Tools

IT Service Transition - Implementing the IT Services

Service Transition provides guidance on the service design and implementation, ensuring that the service delivers the intended strategy and can be operated and maintained effectively.

People

- Security Asset Manager
- Desktop Asset Manager
- Network Asset Manager
- Systems, Servers & Storage Asset Manager
- Applications Asset Manager

Process

- Support & Transition Management
- Change Management
- Asset & Configuration Management
- Release & Deploy Management
- Validation Management
- Evaluation Management
- Knowledge Management

Products

- Asset Management Tool
- Service provision Tool
- Run Book Task Automation Tools
- Service Knowledge & Configuration Management Tools

IT Service Operation – Managing the IT Services

Service Operation provides guidance on managing a service through its day-to-day production life. It also provides guidance on supporting operations by means of new models and architectures such as shared services, utility computing, web services, and mobile commerce.

People

- Security Operation Manager
- Desktop Operations Manager
- Network Operations Manager
- Systems, Server & Storage Operations Manager
- Applications Operations Manager

Process

- Event Management
- Incident Management
- Problem Management
- Fulfillment Management
- Access Management
- Service Desk Function Management
- Service Operations Function Management
- Technical Operations Function Management
- Application Operations Function Management

Products

- Service Desk with Incident Management Tool
- Problem Management Tool
- Event Management Tool
- Run Book Technology Troubleshooting Tool
- Run Book Application Troubleshooting Tool
- Service Knowledge & Configuration Management Tools

IT Continual Service Improvement – Measuring the IT Services

Continual Service Improvement provides guidance on measuring service performance through the service life cycle, suggesting improvements in service quality, operational efficiency and business continuity.

People

- Service Measurement Manager
- Quality Measurement Manager

- Compliance Measurement Manager
- Security Measurement Manager
- Resource Measurement Manager

Process

- IT Governance Management (using COBIT best practices)
- IT Resource Management (using PMI methods)
- IT Quality Management (using Six Sigma methods)
- IT Security Management (using ISO standards)

Products

- Compliance Management & Measurement Tools
- Service Knowledge & Configuration Management Tools

Standardize the IT Service Desk

Standardizing the IT Service Desk or HelpDesk to improve the quality and consistency of IT support services. It involves defining and implementing best practices, policies, and procedures for handling IT incidents and requests. By standardizing the IT Service Desk or HelpDesk, you can achieve the following benefits:

- Increase customer satisfaction and loyalty by providing timely and reliable IT support.
- Reduce costs and risks by minimizing errors, rework, and escalations.
- Improve efficiency and productivity by streamlining workflows and automating tasks.
- Enhance collaboration and communication by aligning IT teams and stakeholders.
- Foster continuous improvement and innovation by measuring and reporting on performance and outcomes.

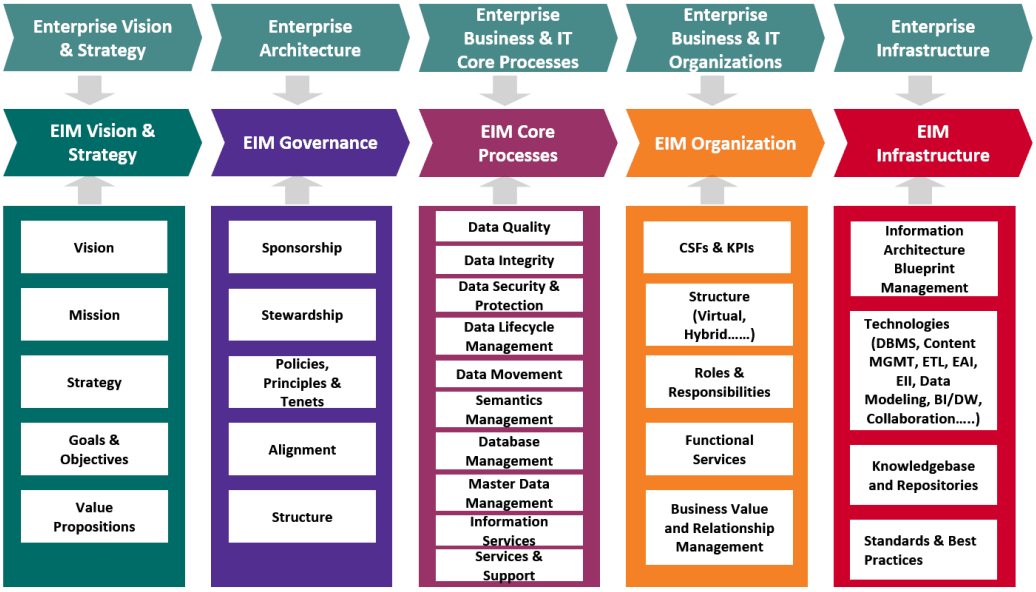
IT Governance & Management Principles

Source: Enterprise Information Management Framework - Xtensible Solutions

Like many data-driven organizations, utilities often become involved with maintaining numerous data silos underlying the systems used to manage their business. Often the focus becomes managing the data silos rather than leveraging the systems to the benefit of the enterprise.

To correct or avoid this situation, enterprises must establish a strategy that includes best practices around people, processes, and technologies to facilitate agile and adaptable information management solutions.

This strategy, called Enterprise Information Management (EIM), encompasses five key components: Vision and Strategy, Governance, Core Processes, Organization, and Infrastructure.



EIM Vision and Strategy

EIM vision and strategy focuses on developing a comprehensive framework and effective road map for iterative and incremental implementation of an enterprise approach to information management. This approach will lead to accurate, consistent, secure, and transparent access to data that flows seamlessly and continuously throughout the enterprise. EIM vision and strategy promotes consensus among business and IT on the meaning of EIM, what problems EIM will address and the value it will bring to the enterprise.

EIM Governance

EIM governance is required to achieve alignment between business and IT as well as to establish respective roles and responsibilities for data and information management

across the enterprise. The governance structure addresses the development, maintenance, communication and enforcement of data management policies and procedures, in addition to the data quality, services, tools and technologies needed to move to an enterprise-wide data management and services culture. EIM governance is critical to ensuring that stakeholders feel confident in leading the charge toward realizing EIM vision and strategy.

EIM Core Processes

EIM includes the definition of core information management processes that support EIM governance and services as well as integration of the processes at user, business and data levels. These core processes target increased accountability and transparency of information across the enterprise and define metadata and master data strategies. Semantic formalization of information is added to the EIM through the development, management and use of an Enterprise Semantic Model (ESM). An ESM provides consistent design and implementation of data and information services across transactional and analytical systems.

EIM Organization

A complete EIM strategy addresses the organization required to ensure a successful EIM initiative. It provides a formal mechanism for developing required EIM core competencies and enables the realization of EIM's value by both IT and business. EIM organization considers key performance indicators and critical success factors as well as roles and responsibilities, structure, and deployment using a logical, incremental approach for resourcing.

EIM Infrastructure

EIM infrastructure provides the definition of a standards-based open platform that consists of data, metadata management, semantic reconciliation and closed-loop information flows for master data and converged content. Decisions to make when establishing the EIM infrastructure include:

- Selecting standards and best practices using existing or new tools and technologies to implement information services.
- Procuring tools that allow data assets to be more widely available.
- Acquiring resources that enable business intelligence and near real time dashboards for more effective and intelligent business operations.

Most Used Frameworks

COBIT: Published by ISACA, COBIT is a comprehensive framework of "globally accepted practices, analytical tools and models" (PDF) designed for governance and management of enterprise IT. With its roots in IT auditing, ISACA expanded COBIT's scope over the years to fully support IT governance. The latest version is COBIT 5, which is widely used by organizations focused on risk management and mitigation.

ITIL: Formerly an acronym for Information Technology Infrastructure Library, ITIL focuses on IT service management. It aims to ensure that IT services support core processes of the business. ITIL comprises five sets of management best practices for service strategy, design, transition (such as change management), operation and continual service improvement.

COSO: This model for evaluating internal controls is from the Committee of Sponsoring Organizations of the Treadway Commission (COSO). COSO's focus is less IT-specific than the other frameworks, concentrating more on business aspects like enterprise risk management (ERM) and fraud deterrence.

CMMI: The Capability Maturity Model Integration method, developed by the Software Engineering Institute, is an approach to performance improvement. CMMI uses a scale of 1 to 5 to gauge an organization's performance, quality and profitability maturity level. According to Calatayud, "allowing for mixed mode and objective measurements to be inserted is critical in measuring risks that are qualitative in nature."

FAIR: Factor Analysis of Information Risk (FAIR) is a relatively new model that helps organizations quantify risk. The focus is on cyber security and operational risk, with the goal of making more well-informed decisions. Although it's newer than other frameworks mentioned here, Calatayud points out that it's already gained a lot of traction with Fortune 500 companies.

COBIT Framework v5

Control Objectives for Information and Related Technology (COBIT) is a framework created by ISACA for information technology (IT) management and smart IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues, and business risks.

COBIT 5 Process Reference Model

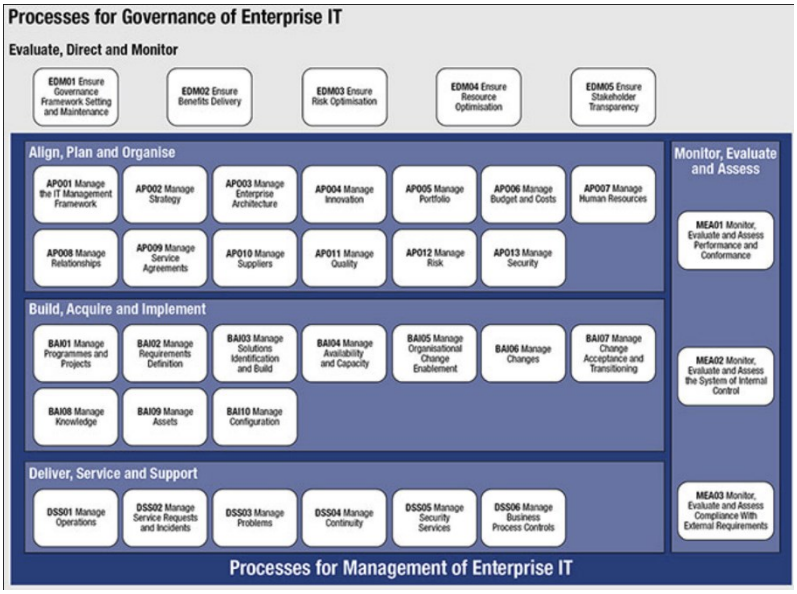
COBIT 5 contains a process reference model which consists of 37 generic processes required for the governance and management of enterprise IT. These processes are organized in 5 groups:

- Evaluate Direct and Monitor (EDM)
- Align, Plan and Organize (APO)
- Build, Acquire and Implement (BAI)
- Deliver, Service and Support (DSS)
- Monitor, Evaluate and Assess (MEA)

These processes are described in detail in *COBIT 5: Enabling Processes*. The COBIT 5 process reference model subdivides the IT-related practices and activities of the enterprise into 2 main areas—governance and management—with management further divided into domains of processes:

The governance domain contains 5 governance processes. Within each process, Evaluate, Direct and Monitor (EDM) practices are defined.

The management domains are in line with the responsibility areas of Plan, Build, Run and Monitor (PBRM).



Source: [Portfolio, Program and Project Management Using COBIT 5 (isaca.org)]

Common Service Desk Challenges

- Low business satisfaction

    - Disconnected to SOC services where a critical vulnerability is reported yet it's not conveyed to the SOC team. The tool is not provide by SOC and not monitored, independently operating.
    - Users are unable to get assistance with IT services quickly.
    - Users go to their favorite technician instead of using the service desk.
    - Service desk managers struggle to set and meet service-level expectations, which further compromises end-user satisfaction.
- High cost to resolve
    - Connected SOC tools are inadequate and the helpdesk manager got multiple portals to support.
    - Tier 2 and tier 3 resolve issues that should be resolved at tier 1.
    - Tier 2 and tier 3 often interrupt projects to focus on service support.
    - Specialists would rather work on projects than provide service support.
- Unresolved issues
    - Tickets are not created for all incidents.
    - Tickets are lost or escalated to the wrong technicians.
    - Poor data (input validation is not maintained) impedes root-cause analysis of incidents.
- Poor planning
    - Lack of data for effective trend analysis leads to poor demand planning.
    - Lack of data leads to lost opportunities for templating and automation.
    - The Service Desk lacks processes and workflows to provide consistent service.
- Lost resources or accountability
    - Lack of cross-training and knowledge sharing.
    - Lack of skills coverage for critical applications and services.
    - Time wasted troubleshooting recurring issues. o Reports unavailable due to lack of data and ineffective categorization.

Ways That the Service Desk Handles Cybersecurity

- The service desk follows the best practices and guidelines for IT service management, such as the ITIL framework, which covers various aspects of IT security, such as security incident management, security policy, and security awareness.
- The service desk uses the right software and tools to monitor, manage, and secure the IT environment, such as antivirus software, firewalls, backups, automation, and encryption. The service desk also keeps the devices and applications updated and patched to prevent vulnerabilities and exploits.

- The service desk trains its staff and end users on how to identify and prevent cybersecurity risks, such as phishing, malware, ransomware, and social engineering and report to SOC with collected or recorded data. The service desk also educates them on how to follow the security policies and procedures, such as using strong passwords, avoiding public Wi-Fi, and reporting suspicious activities.
- The service desk collaborates and communicates with other IT teams and stakeholders, such as the InfoSec team, the IT governance team, and the business units, to ensure a coordinated and consistent approach to cybersecurity. The service desk also reports and analyzes security incidents and requests and provides feedback and recommendations for improvement.

If your service desk is not up to the mark, try starting from the start, again. By checking on the following:

12. Assess current state. Time, resource and quality of manpower. Input validation by the T1, T2, T3 and train properly for problem inputs.
13. Communication & implementation roadmap, documented processes and process performance.
14. Assurance: Service desk SoP. Integrated remote support options.
15. Maturity assessment & current model analysis, if the SOC requirements are addressed in the model or not.
16. Incident and ticket generation workflows with integrated data collection and video recording methods.
17. Review ticket handling procedures (chat, walk-ins, web portal, phone, email etc.) (this portal should have ID provider integration for better visibility and lesser typing) (application-based notifications or SMS based or web based apps were used).
18. Identify metrics and reports, mapped to RACI.
19. Import incident escalation management workflows from SOC. Service level response and resolution (SLOR&R) time.
20. Revisit ticket category-wise service list, and update as required with integrated KB generations.

Pro-Tip

- IT & SOC must not use different ticketing system, otherwise there will be a workflow conflict. most of the ITSM softwares are now equipped with AI as well, take advantage of that feature.

BONUS CHAPTER 4

Jurisdiction Assignment Matrix

THIS IS THE BUSINESS AND OPERATIONAL REQUIREMENTS WHERE IT'S OUTLINED ON WHO WILL DO WHAT BY MARKING THEIR LIMIT TO AUTHORITATIVE TASKS AND ACTIVITIES. THIS PERSPECTIVE ALSO DEFINES WORK ROLES PERFORMED BY CERTAIN INDIVIDUALS, AND THEIR ROLES ARE AUTHORIZED AND UNDERSTOOD BY THE STAKEHOLDERS AND APPROVED. DO CHANGE AS REQUIRED.

The file is provided in the Job-aid folder named "Technology Responsibility and Jurisdiction Assignment Matrix_V3.1.xlsx"

Technology Responsibility & Jurisdiction Assignment Matrix

Operational & Organizational Risk Management

Partial Fulfillment for ISO/IEC 27001, ER(Risk & Resource)M, BCP, DRP

Document Number: XX/ISMS/TRJAM/01 | **Version:** 3.1 | **Submitted Date:** 6th July 2022 | **Last Review Date:** 25th January 2024

R-Responsible
A-Accountable
C-Consulted
I-Informed

SL	Task Head	Task Sub-head	Current Status	Progress	RACI	Owner	Submit to	Audit	Description
	Board Reporting	Policy Development	N/A		RA	IS	Board	I	Board will periodically review process and security measure requirement analysis and take necessary improvement requirements
		Direct Board Reporting	N/A		RA	IS, Audit, PMO	Board	I	Security team, Audit, PMO
		Organizational Risk Management	N/A		RA	IS	Board	I	Board will periodically review process and security measure requirement analysis directly related to business, and take necessary improvement requirements
	IT, IS Governance Program	Identity & Access Management	N/A		RA	I (IS)	IC (IS)	I	All networked devices access management including VPN access will be managed and maintained by IS team
		Enterprise Risk Management (ERM)	N/A		RA	I (IS)	Board	I	Whole networked device assessment according to the NIST / CISECURITY standard and provide actionable guidance to the stakeholders and to the Board
		Policy & process development	N/A		RA	I (IS)	Board	I	Will be vetted by IS team

You can also add different roles and their profiles into this worksheet as well for the SOC manager, L1/L2/L3 analysts tasks and roles explicitly carried out on a daily basis, and the accompanied RACI will enable them jurisdictions to perform certain tasks, so that no one questions their authority over certain aspects of their job functions, roles and responsibilities, tasks, and activities.

References

1. What is a security operations center (SOC)? | Microsoft Security
2. The Importance of the Security Operations Center (SOC) - Check Point Software
3. What is Security Operations Center (SOC)? Working Structure and Benefits | by Ismail Tasdelen | DataBulls | Medium
4. What is a Security Operations Center (SOC)? | Stackscale
5. What Is a Security Operations Center | Cybersecurity | CompTIA
6. What is Security Operations Center (SOC)? | IBM
7. Security Operations Center (SOC) Best Practices - Check Point Software
8. What Is a Security Operations Center? Complete Guide (exabeam.com)
9. A Small Business Guide to the Security Operations Center (fool.com)
10. 7 Steps to Building A Security Operations Center (SOC) | LogRhythm
11. How to Build a Security Operations Center (SOC): Peoples, Processes, and Technologies (digitalguardian.com)
12. Cybersecurity Career Master Plan (packt-cdn.com) | by Dr. Gerald Auger
13. Sigma rules explained: When and how to use them to log events | CSO Online
14. The Ultimate Guide to Sigma Rules (graylog.org)
15. Career Scope as a SOC Professional - InfosecTrain
16. Security Operations Center (SOC) Roles and Responsibilities - Palo Alto Networks
17. What Is an SOC Analyst? (Background, Skills, & Requirements) (springboard.com)
18. What is Tier 1, 2, 3 Incident Response? A Cybersecurity Expert Explains - Cyber Insight
19. SOC Analyst Types Explained: Tier 1, 2 & 3 | Legends of Tech Blog
20. What Is a Security Operations Center (SOC)? - Palo Alto Networks
21. Tier 3 Advanced Security Analyst or Threat Hunter - Trilight Security
22. What is a SOC-as-a-Service (SOCaaS)? - CrowdStrike
23. Kickstart Your Cybersecurity Career as a SOC Analyst | Infosec (infosecinstitute.com)
24. What is Cyberthreat Intelligence (CTI)? - Palo Alto Networks
25. Cyber Threat Intelligence (CTI): A Beginner's Guide | Splunk
26. A day in the life of a SOC architect - Hurricane Labs
27. Security Operations Center (SOC) Roles and Responsibilities - Check Point Software
28. How to Coordinate CTI and Vulnerability Management | IANS Research
29. Security Operations Center (SOC) tools and technologies | ManageEngine Log360
30. SOC Tools | AT&T Cybersecurity (att.com)
31. CISO_mindmap_2020_recommendations.pdf (rafeeqrehman.com)

32. SOC vs. SIEM: Understanding The Role of SIEM Solutions in the SOC (exabeam.com)
33. 4 Security Operations Center Frameworks You Should Know (bluevoyant.com)
34. What is SOC (checkpoint.com)
35. What Is a Security Operations Center (SOC)? (bluevoyant.com)
36. Supercharge Your SOC With an Automated Approach to Incident Response - SentinelOne
37. 8 Steps to Improving Your SOC's Incident Detection & Response (cyberproof.com)
38. What Is a SOC? 10 Core Functions and 6 Key Challenges (cynet.com)
39. SecurityOperationsCenter_eBook.pdf (bluesec.pl)
40. Best Practices for Setting Up a Cybersecurity Operations Center (isaca.org)
41. OWASP SOC Project
42. 7 Steps to Build a SOC with Limited Resources | PPT (slideshare.net)
43. CrowdStrike-Services-SOC-Assessment-Data-Sheet.pdf
44. SOAR-KPIs.pdf (acadiatech.com)
45. Top SOC Metrics and KPI 2023: Mastering Security Operations (blueteamresources.in)
46. SOC Metrics: Security Metrics & KPIs for Measuring SOC Success | Splunk
47. The SOC methodology - SecureGlobal
48. What is a secure enterprise architecture roadmap? | PPT (slideshare.net)
49. Microsoft Word - Threat-Driven Approach whitepaper v3.03a.docx (lockheedmartin.com)
50. Cyber Kill Chain® | Lockheed Martin
51. The Cyber Kill Chain: The Seven Steps of a Cyberattack (eccouncil.org)
52. Gaining_the_Advantage_Cyber_Kill_Chain.pdf (lockheedmartin.com)
53. Building an Effective SOC Playbook | Tufin
54. Incident response playbooks | Microsoft Learn
55. Incident response planning | Microsoft Learn
56. LDR551: Building, Leading, & Managing (SOC) Security Operations Center | SANS Institute
57. The Fundamental Guide to Building a Better Security Operations Center (SOC) (splunk.com)
58. DetailedPhishingV01 - (flexibleir.com)
59. Cyber Security Incident management system using Flexible Evolving Playbooks (flexibleir.com)
60. SOC Operations: 6 Vital Lessons & Pitfalls (darkreading.com)
61. Toreon | News | 4 pitfalls to avoid when building a CSOC

62. SOC Processes, Operations, Challenges, and Best Practices - Sapphire.net
63. OODA loop - Wikipedia
64. SOC Processes | AT&T Cybersecurity (att.com)
65. CSIRT vs SOC: What Are the Differences? (ryadel.com)
66. What Is a Security Operations Center? Complete Guide (exabeam.com)
67. What is Security Operations Center - SOC: Roles & Responsibilities - Exabeam
68. Top 36 Threat Intelligence Providers for SOC Teams - Maltego
69. Purple Teaming and Threat-Informed Detection Engineering | SANS Blog
70. What Is Detection Engineering? | Detection Engineering Explained (uptycs.com)
71. Detection Engineering is Painful — and It Shouldn't Be (Part 1) | by Anton Chuvakin | Anton on Security | Medium
72. How to Build a Security Operations Center (SOC Guide) - 2023 (gbhackers.com)
73. What Is A Security Operations Center (SOC)? (A Complete Guide For 2023) - Cybersecurity For Me
74. Chief Information Security Officer (CISO) Workshop - Security documentation | Microsoft Learn
75. Download Security Compliance Toolkit and Baselines from Official Microsoft Download Center
76. https://www.microsoft.com/en-us/security/blog/2019/02/21/lessons-learned-from-the-microsoft-soc-part-1-organization/
77. Microsoft Cybersecurity Reference Architectures (MCRA) - Security documentation | Microsoft Learn
78. Top Open Source Solutions for Building Security Operations Center II (socradar.io)
79. SOC Open Source, ELK- TheHive- Cortex- MISP Complete Setup Guide, Part 1 - YouTube
80. SOC Open Source, Build own SOAR with Shuffle, ELK-TheHive-Cortex-Teams Full Automation, Part 2 - YouTube
81. archanchoudhury/SOC-OpenSource: This is a Project Designed for Security Analysts and all SOC audiences who wants to play with implementation and explore the Modern SOC architecture. (github.com)
82. andreafortuna/autotimeliner: Automagically extract forensic timeline from volatile memory dump (github.com)
83. Eric Zimmerman's tools
84. Welcome to the Plaso documentation — Plaso (log2timeline) 20230717 documentation
85. SANS Digital Forensics and Incident Response Blog | Digital Forensic SIFTing: Colorized Super Timeline Template for Log2timeline Output Files | SANS Institute

86. Helping CTI Analysts Approach and Report on Emerging Technology Threats and Trends | SANS
87. Linux Incident Response - Introduction to Rootkits | SANS
88. Linux Incident Response - Using ss for Network Analysis | SANS
89. Linux Incident Response - A Guide to syslog-ng | SANS
90. Timeline Analysis in DFIR, Full Process Explained - YouTube
91. SOC-Community/Awesome-SOC: A collection of sources of documentation and best practices to build and run a SOC (github.com)
92. How To Build A SIEM with Suricata and Elastic Stack on Rocky Linux 8 | DigitalOcean
93. SoC Mind Map (cm-alliance.com)
94. DoD CIO Library (defense.gov)
95. Playbook for DDOS Security Response - All Articles - CISO Platform
96. gsvsoc_cirt-playbook-battle-cards/GSPBC-1000 - Impact - Data Encrypted For Impact - Ransomware.pdf at master · guardsight/gsvsoc_cirt-playbook-battle-cards (github.com)
97. How to Build a Great SOC (isaca.org)
98. Event Log: Leveraging Events and Endpoint Logs for Security (exabeam.com)
99. SIEM Tools: Top 6 SIEM Platforms, Features, Use Cases and TCO (exabeam.com)
100. DDoS Quick Guide (cisa.gov)
101. Protect Your Business Assets With a Roadmap for a Maturing Cybersecurity Program (gartner.com)
102. GitHub - cisagov/ScubaGear: Automation to assess the state of your M365 tenant against CISA's baselines
103. Cyber Security Toolkit for Boards - NCSC.GOV.UK
104. Cyber risk modelling and quantification (kpmg.com)
105. CMMC Documentation (defense.gov)
106. What are Indicators of Compromise (IoCs)? (packetlabs.net)
107. Indicators of Compromise (IOCs) | Fortinet
108. What are Indicators of Compromise? IOC Explained - CrowdStrike
109. CRMP | Cyber Risk Management | Interactive Framework
110. Getting Started with the NICE Framework | NIST
111. Publications | CSRC (nist.gov)
112. Cyber Security Posters | SANS Institute
113. 7 Key Enterprise Architecture Metrics - Simplicable
114. Enterprise Architecture Guide - Simplicable
115. Three Diagrams Architects Can't Live Without | by Susannah Plaisted | Salesforce Architects | Medium

116. Yara Toolkit (securitybreak.io)
117. Digital Forensics and Incident Response (DFIR) - CrowdStrike
118. What is Digital Forensics and Incident Response (DFIR)? (bluevoyant.com)
119. Cyber Security Tools | SANS Institute
120. Digital Forensics & Incident Response Framework for Embedded Systems (mandiant.com)
121. macOS and iOS Forensic Analysis | SANS Institute
122. Digital Forensics and Incident Response (DFIR) Framework for Operational Technology (OT) | NIST
123. DFIR Cheatsheet Booklet | SANS
124. Common Secure Security Operations Centre - UNICC
125. Security Operation Center - Design & Build | PPT (slideshare.net)
126. DTS Solution - Building a SOC (Security Operations Center) | PPT (slideshare.net)
127. Full Library | RSA Conference
128. Cyber Security Posters | SANS Institute
129. Russell Reynolds - Cyber Security: The CISO Assessment Level Model CALM | AESC
130. ciso-radar-2023-wavestone-uai-2880x1908.png (2880×1908)
131. Demos, Templates, Charts and Maps on Dragon1
132. About the Authors | Red Team Development and Operations
133. Cybersecurity Red Team Guide. My first blog was on the Blue Team side… | by Joshua Speshock | Medium
134. Cybersecurity Red Team Guide. My first blog was on the Blue Team side… | by Joshua Speshock | Medium
135. Red Team | The GitLab Handbook
136. Handbooks, Guides and Articles | US Army Combined Arms Center
137. Red Teaming Handbook - GOV.UK (www.gov.uk)
138. What Is Red Teaming and How Does It Work? | Synopsys
139. Top 3 Red Teaming Frameworks (TIBER,AASE,CBEST) - BreachLock
140. Red Teaming as a Service | BreachLock
141. Red Teaming for Cybersecurity (isaca.org)
142. RT_Handbook_v6.pdf (army.mil)
143. Comparing open source attack simulation platforms for red teams (redcanary.com)
144. GitHub - praetorian-inc/purple-team-attack-automation: Praetorian's public release of our Metasploit automation of MITRE ATT&CK™ TTPs

145. TIBER-EU FRAMEWORK – How to implement the European framework for Threat Intelligence-based Ethical Red Teaming (europa.eu)
146. Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions (bis.org)
147. What is Red Teaming? Methodology & Tools (varonis.com)
148. What is a Security Operations Center (SOC)? (varonis.com)
149. Red Team Framework | PPT (slideshare.net)
150. Building an InfoSec RedTeam | PPT (slideshare.net)
151. Red Team vs. Blue Team | PPT (slideshare.net)
152. Red team and blue team in ethical hacking | PPT (slideshare.net)
153. GitHub - infosecn1nja/Red-Teaming-Toolkit: This repository contains cutting-edge open-source security tools (OST) for a red teamer and threat hunter.
154. 5 Best C2 Framework for Red Teaming - The Sec Master
155. What is Red Team? How Red Teaming is Different Than Penetration Testing? - The Sec Master
156. The roles of red, blue and purple teams - Content+Cloud (contentandcloud.com)
157. Red, Blue, and Purple Teams in Cybersecurity: Understanding the Roles and Tools (todyl.com)
158. How do Red Team Exercises help CISO to Validate the Security Controls Effectively? - Security Boulevard
159. What Should Influence Your SOC Strategy in 2023? (sightgain.com)
160. SOC Metrics: PowerPoint Presentation (first.org)
161. Incident Response Plan: Frameworks and Steps - CrowdStrike
162. Computer Security Incident Handling Guide - NIST
163. 6 Incident Response Steps to Take After a Security Event - Exabeam
164. Step-By-Step Guide To An Effective Incident Response Plan
165. The complete 6-step incident response lifecycle | incident.io
166. OWASP Security Operations Centre Framework Project OWASP
167. How to: Setup Powershell Logging for SIEM | by Secprentice | Medium
168. Windows+Sysmon+Logging+Cheat+Sheet_Aug_2019.pdf (squarespace.com)
169. Module 11 Logs and Event Analysis.pdf (cemca.org)
170. Windows_Event_Log_Analysis_IR_Guide.pdf (0ut3r.space)
171. PROTECT - Windows Event Logging and Forwarding (October 2021).pdf (cyber.gov.au)
172. How to: Setup Powershell Logging for SIEM | by Secprentice | Medium
173. Security Operation Center - Design & Build | PPT (slideshare.net)
174. SEC's new cyber disclosure rule: PwC

175. Enterprise Cybersecurity Architecture (jamesjfisher.org)
176. Cybersecurity roadmap : Global healthcare security architecture | PPT (slideshare.net)
177. Building a Next-Generation Security Operation Center Based on IBM QRadar and Security Intelligence Concepts | PPT (slideshare.net)
178. From SIEM to SOC: Crossing the Cybersecurity Chasm | PPT (slideshare.net)
179. Security operations center-SOC Presentation-مرکز عملیات امنیت | PPT (slideshare.net)
180. Building Security Operation Center | PPT (slideshare.net)
181. redteam-plan/README.md at master · magoo/redteam-plan · GitHub
182. Red Team Guides | Red Team Development and Operations
183. GitHub - J0hnbX/RedTeam-Resources
184. Microsoft Word - Threat-Driven Approach whitepaper v3.03a.docx (lockheedmartin.com)
185. Cyber Resiliency Level: CRL_v3.01_Whitepaper_29Aug23_FINAL.pdf (lockheedmartin.com)
186. Threats - Microsoft Threat Modeling Tool - Azure | Microsoft Learn
187. Microsoft Threat Modeling Tool overview - Azure | Microsoft Learn
188. Threat Modeling Process | OWASP Foundation
189. What is STRIDE Threat Model? (practical-devsecops.com)
190. STRIDE-LM Threat Model - CSF Tools
191. Using the STRIDE-LM Threat Model to Drive Security Control Selection - CSF Tools
192. Microsoft Word - Threat-Driven Approach whitepaper v3.03a.docx (lockheedmartin.com)
193. Security Quality Requirements Engineering (SQUARE) Methodology (cmu.edu)
194. Security Modeling and Threat Modeling Resources - Cybersecurity Memo (51sec.org)
195. Security Modeling and Threat Modeling Resources - Cybersecurity Memo (51sec.org)
196. A Threat Modeling Process to Improve Resiliency of Cybersecurity ProgramRafeeq Rehman | Cyber | Automation | Digital
197. Research Publications | CSA (cloudsecurityalliance.org)
198. ITIL 4 Introduction- ITIL 4 Certification Scheme & ITIL 4 Framework (knowledgehut.com)
199. What is ITIL®? | YaSM Service Management Wiki

200. EQL search in Elastic SIEM Detection rules | LinkedIn
201. Analytics — EQL Analytics Library documentation (eqllib.readthedocs.io)
202. A deep dive into Sigma rules and how to write your own threat detection rules - FourCore
203. GitHub - SigmaHQ/sigma: Main Sigma Rule Repository
204. Uncoder AI: Active Threat-Informed Defense | Sigma Rules & ATT&CK
205. Analytics — EQL Analytics Library documentation (eqllib.readthedocs.io)
206. The No Hassle Guide to Event Query Language (EQL) for Threat Hunting (varonis.com)
207. EQL syntax reference | Elasticsearch Guide [8.12] | Elastic
208. A_Mind_Map_on_the_Use_of_Information_and_Communication_Technology_ICT_in_Educational_Assessment.jpg (2048×1463)
209. CSIRT Framework Development SIG (first.org)
210. How Purple Team Can Use Continuous Adversary Simulation | SANS Institute
211. Adversary Emulation Library - MITRE Engenuity (mitre-engenuity.org)
212. The Center for Threat-Informed Defense · GitHub
213. The First 100 Days Of An Enterprise Architect (gartner.com)
214. OVAL - Documents (mitre.org)
215. HIDS A Guide To Host Based Intrusion Detection Systems (bulletproof.co.uk)
216. A Guide to Network Intrusion Detection Systems (bulletproof.co.uk)
217. CWE - Common Weakness Enumeration (mitre.org)
218. Policy Mapping Poster with US Cyber Centers Map | Behance :: Behance
219. OMG Standards Introduction | Object Management Group
220. It governance and management framework (management-club.com)
221. IT Management Framework - Information Professionals (informpros.com.au)
222. ISO/IEC 38500:2015 - Information technology — Governance of IT for the organization
223. SOC Operations: 6 Vital Lessons & Pitfalls (darkreading.com)
224. Building a Modern CSOC - A Complete Guide for SOC Analysts (cybersecuritynews.com)
225. The VERIS Framework
226. Publications | Offensive AI Lab (offensive-ai-lab.github.io)
227. Counter-AI Offensive Tools and Techniques – CSIAC
228. Preparing for AI-enabled cyberattacks | MIT Technology Review

229. Full article: The Emerging Threat of Ai-driven Cyber Attacks: A Review (tandfonline.com)
230. Risk Modeling: Quantify Cyber Insights for Effective Risk Management – Series (brighttalk.com)
231. What is Attack Tree Model: A Comprehensive Cyber Security Tool? - Cyber Insight
232. NIST CSF & FAIR - Part 1 (fairinstitute.org)
233. Selecting the Right Cyber Risk Quantification Model (cybersaint.io)
234. Cybersecurity Tabletop Exercise Examples, Best Practices, and Considerations | RSI Security
235. Cyber Attack Incident Response Tabletop Exercise | Scenarios & Process (zcybersecurity.com)
236. How to Build an Effective Cyber Tabletop Exercise (freecodecamp.org)
237. The Complete Guide to Running a Cybersecurity Tabletop Exercise - Red Goat (red-goat.com)
238. Tabletop Exercises: Real Life Scenarios and Best Practices (threatintelligence.com)
239. Top 5 ICS Incident Response Tabletops and How to Run Them | SANS Institute
240. Tabletop exercises explained: Definition, examples, and objectives | CSO Online
241. Cybersecurity Incident Response Exercise Guidance (isaca.org)
242. Tabletop Simulations for Security Programs | Red Canary
243. Implementing Your First Cybersecurity Tabletop Exercise - JumpCloud
244. Everything You Need to Know about Cyber Crisis Tabletop Exercises | Tripwire
245. Tabletop Exercise: Pretty Much Everything You Need to Know | RedLegg
246. Cyber Resiliency Engineering Framework | MITRE
247. How to Write an Actionable Alert - Catscrdl
248. Writing Practical Splunk Detection Rules — Part 1 | by Vit Bukac | Medium

Body of Knowledge & Control Frameworks

BoK for the Cybersecurity and essentially the enterprise risk management

1. **Zachman**: About the Zachman Framework - Zachman International - FEAC Institute (zachman-feac.com)
2. **Dragon1**: Dragon1 Software for Managing Risk, Projects, Strategy, Data
3. **TOGAF & IT4IT**- The Open Group Architecture Framework
4. **Q4IT**: DCMM, IT Quality Index (q4it.eu)
5. **OSA**: Open Security Architecture
6. **DoD Reference Architecture:** DoD Cybersecurity Reference Architecture (defense.gov)
7. **DoD Architecture Framework 2.02**: DODAF - DOD Architecture Framework Version 2.02 - DOD Deputy Chief Information Officer (defense.gov)
8. **DoD Library:** DoD CIO Library (defense.gov)
9. **FedRAMP:** Search For Any FedRAMP Policy or Guidance Resource | FedRAMP.gov
10. **CMMC:** CMMC Documentation (defense.gov)
11. **DAMA:** DMBoK - Data Management Body of Knowledge (dama.org)
12. **FAIR:** The Importance and Effectiveness of Cyber Risk Quantification (fairinstitute.org)
13. **SCF – Secure Controls Framework:** Secure Controls Framework (SCF) Download
14. **ENISA**: Publications — ENISA (europa.eu)
15. **APQC's Process Classification Framework (PCF):** Process Frameworks | APQC
16. The DoD Cybersecurity Policy Chart: The DoD Cybersecurity Policy Chart – CSIAC
17. The IIA: Internal Audit Competency Framework (theiia.org)
18. The Chartered Institute of IT: Security / data / privacy | BCS
19. **BCI** - Business Continuity Institute: Introduction to Business Continuity | The Business Continuity Institute (BCI) | BCI (thebci.org)
20. **IAPP**: International Association of Privacy Professionals (iapp.org)
21. **IEEE** - IEEE Cybersecurity – Home of the IEEE Cybersecurity Initiative
22. **SANS** - Cyber Security
23. **IRM** - Institute of Risk Management: Special Interest Groups (SIGs) (theirm.org)
24. **IASA** - An Association for All IT Architects Btabok - BTABoK (iasaglobal.org)
25. **CIISEC** - Chartered Institute of Information Security Resource Centre - CIISec
26. **SABSA** – Enterprise Security Architecture SABSA Executive Summary - The SABSA Institute
27. **ICTTF** - International Cyber Security Task Force
28. **CyBOK** - Cyber Security Body of Knowledge

29. **BABOK**: Business Analysis | The Global Standard | IIBA®
30. **SWEBOK**: Software Engineering Body of Knowledge SWEBOK- Version 3 (computer.org)
31. **SIA** - Center of Excellence - Security Industry Association
32. **SFIA** - Skills Framework for the Information Age: SFIAv9 Levels of responsibility and generic attributes — English (sfia-online.org)
33. **IVI Institute** - IT Capability Maturity Framework: IT-CMF - Innovation Value Institute (ivi.ie)
34. **ADCG** - Association for Data & Cyber Governance: Benefits — ADCG
35. **SCF** - Secure Controls Framework: Secure Controls Framework
36. **CGI** - Corporate Governance Institute: Corporate Governance Courses for Directors and Non-Executive Directors (thecorporategovernanceinstitute.com)
37. **COSO** - Enterprise Risk Management: COSO ERM Framework | COSO
38. **DORA** – Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554 (digital-operational-resilience-act.com)
39. **NIST CSF:** Cybersecurity Framework | NIST
40. **NIS-2:** The NIS2 Directive: A high common level of cybersecurity in the EU | Think Tank | European Parliament (europa.eu)
41. PMI BoK - PMBOK Guide | Project Management Institute (pmi.org)
42. Global Cyber Alliance: Actionable Cybersecurity Tools (globalcyberalliance.org)
43. NCSC UK: 10 Steps to Cyber Security - NCSC.GOV.UK
44. OSA: Pattern Landscape (opensecurityarchitecture.org)
45. ISA: International Society of Automation (ISA)
46. DRJ: Disaster Recovery Journal (drj.com)
47. NYMITY: Charts_Cover_Final.ai (oasis-open.org)
48. NYMITY: Privacy Management Accountability Framework - Hong Kong.ai (pcpd.org.hk)
49. NYMITY: PMAF Poster - January 2017 (vvena.nl)
50. The Ultimate Guide to Privacy Management | Blog | OneTrust
51. Information and Privacy Commission New South Wales (nsw.gov.au)
52. SME Guides | SBS SME (sbs-sme.eu)
53. About Cyber Essentials - NCSC.GOV.UK
54. Cyber Essentials Toolkits | CISA
55. CISA Cyber Essentials Starter Kit | CISA
56. Home Page - CREST (crest-approved.org)
57. CERT Resilience Management Model (CERT-RMM) Collection: CERT Resilience Management Model (CERT-RMM) Collection (cmu.edu)

58. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2): cybersecurity-capability-maturity-model-february-2014 (energy.gov)
59. NICE Framework Resource Center | NIST
60. CSA Cloud Control Matrix: CSA (cloudsecurityalliance.org)
61. White Papers (insaonline.org)

Acronyms

Access Control List (ACL), 66
Advanced Persistent Threat (APT), 108, 187
Advanced Threat Protection (ATP), 197
Alert Detection Strategy (ADS), 160
Align, Plan and Organize (APO), 447
Application Centric Infrastructure (ACI), 66, 110, 228, 231
Application Performance Monitoring (APM), 231
Architecture Development Method (ADM), 50
Artificial Intelligence (AI), 86
Automatic Call Distribution (ACD), 66

Bring Your Own Device (BYOD), 72, 154, 155
Build, Acquire and Implement (BAI), 447
Business Continuity Plan (BCP), 26, 46, 65, 83, 156, 157
Business Continuity Planning (BCP), 26
Business Process Management (BPM), 55, 56, 63, 231, 405, 474
Business Support System (BSS), 50

Capability Maturity Model (CMM), 104, 105
Center for Internet Security (CIS), 225
Cloud Access Security Broker (CASB), 63, 64, 107, 109, 112, 232
Cloud Identity Governance (CIG), 232
Cloud Infrastructure Entitlement Management (CIEM), 232
Cloud Security Posture Management (CSPM), 232
Cloud Workload Protection Platforms (CWPP), 232
Command & Control (C2), 68
Computer Security Incident Response Team (CSIRT), 309, 310, 311, 312, 314, 316, 317, 321, 454, 459
Continuous Threat Exposure Management (CTEM), 63, 232, 326, 327, 328, 329
Control Objectives for Information and Related Technologies (COBIT), 68, 106, 229, 443, 446, 447
Could Access Security Broker (CASB), 232
Courses of Action (CoA), 126
Cyber Intelligence Operation Center (CIOC), 70
Cyber Open-Source Intelligence (COSI), 70
Cyber Resiliency Engineering Framework

Author Brief

Thank you for downloading this book, I hope it helped you gain some insights on how to break into cybersecurity and its domain knowledge requirements and essentially help build your SOC.

This book is my 10th book, the other nine were not this extensive in their nature but had different views and insights in it. I wanted to see if I could be up for it and I was collecting information's that's reflected throughout the book, which are quite old, like 10yrs old and from more than 600+ documents combined. My family supported my time away from them, and because of their sacrifices, this book came to completion.

While I was in junior high, I used to make guitar amplifier and sell it to the store back in the young days for the guitar players, local players bought those amps and it was a good hit for me as the money started to pour in, and I've used those earnings to train myself in different things, like bikes and car engine reconstructions 😊. I borrowed some money from my dad for a side business and started a CD duplication station with 12 Sony SCSI drives, had 4 towers producing 48 CDs approximately in 6 minutes at 12x write speed with Padus DiskJuggler software equipped with Adaptec UW-39320 Dual Channel SCSI controllers, one channel holding 6 SCSI drives. Fish breeding was also one of my hobbies, having trillions of babies! from Angel, Black Moors, and for huge number of aquariums I've made a custom water heater as those available in the market were too expensive.

At the the beginning of my career I have enrolled myself into learning dBase and Lotus123 in the year 1993, and later moved gradually to software development in the year 2005 with FoxPro 2.6 with SQL Personal Edition, later closely worked with Visual Studio and TFS. Side by side, I started using the Linux Slackware and SCO Unix for banking app installations throughout 2005 (on an individual contributor capacity). I have been observing that Banking and local enterprises do not want to use Linux as its too complex to manage and dependency lies with the administrators and those folks are in limited supply, and Windows Administrators are flooding the country with their deployment expertise, and I started losing the battles but not the war. Therefore, organizations started to move to Microsoft Windows systems, and then I started using IBM PC-DOS v2.1, and the last usage of MS-DOS was v6.22. Meanwhile, I started to work on NT v3.51(PDC & BDC deployments) in the year 1998 approximately, and gradually went up to

it till date with all of Microsoft Services (AD, Exchange, SharePoint, Lync & Communication Server, ISA Server, System Center Components like SCCM, SCOM, SCDPM, SCVMM, SCO, SCSM etc.), and occasionally Linux for SOC purposes.

I also have tried different things in the past and failed miserably and wasted a lifetime of money in learning things my way, as when it comes to knowledge, I've found out that everything people shared with me confidently, are 20%-30% correct and the rest is just plain made-up lies. But still at that time, I came in late for frameworks, certifications, and achieved the MCP since 2002, and never looked back of what I didn't achieve, but competing against my peers and myself for enriching my knowledge day after day, planned of the things that I wanted to go for, and astonishingly, at that time, Bangladesh were not in the internet era. I had some friends who were rich enough to buy USRobotics Modem (Sportster 14.4K) and I've bunked at their office at night and used their lines all day long (weekends) creating an email address, subscribing to news of gadgets and technology roadmaps, market share of the top players and things of that sort. Side by side I've spent handsomely for my training like repairing TV & Radio's, started a small HAM-Radio project, amplifier builds using STK IC with cassette player, guitar amplifier, hobby electronics, NLE video editing, started to learn 3D Studio Max v4, guitar lessons! Web site development training, power generator calibration, Datacenter development, TV Broadcasting with MCR design, Audio Booth design, etc.

Side by side, my enormous hunger for knowledge and to know the "why" and the "how" lead me to different paths all together. While I was deploying country's largest network that resides in the Government of Bangladesh, the Ministry of Finance to be exact, led me explore and learn at a fast pace, as devices were coming in like a waterfall, and I felt like "I am doomed", as I didn't have the knowledge to configure a Cisco Router, a Cisco Switch, Cisco ASA, but I have acquired those skills in a matter of a month, and configured them properly, and later on got CCNA certified in 2008. That's not the end, "properly" has a different meaning all together back in the days in 2005. At that time, someone from my team changed something into the router, and then I learned to harden these systems, activating log, and harder passwords employed. But my mentality changed, as the network went down, and I got the blame onto me, though I have found out who changed the configurations. Since then, every networked device got deployed, developed the first checklist of configurations to set forth.

Side by side, I have been supporting offices, individuals to integrate their PC's, build their PC's, connecting multiple PC's into a network, provide a shared printer etc. that were done using Microsoft Windows for Workgroups 3.11 in the year 1998-2000. Amazingly, I received a task offer from my connections, to establish a 20-computer network within the National Parliament Library, and did it within a month with Compaq Servers (AD

developed with PDC only), which were equipped with Pentium-pro processors, that was the first time I got to see the Pentium-pro processors. And some laptop purchased from a US manufacturer, I forgot the name, but the processors were made by Transmeta Effcion! Weird, but true, never heard their names but worked well alongside of Cyrix. Later, I got to work with Cyrix Processors from IBM as well. In those times, I bought myself a bike, small but fearsome, a Honda MBX-125F. Once it's time to change the piston, bored a bigger housing and replaced the piston with a Yamaha DT-200 piston 😊 it was a radiator cooled 6-gear engine, imagine the thrust, but broke the engine in 6 months' time. And since I got a ride for myself, my engagement with customers exploded, I've received orders to set networks, sell PC's like 40 PC's a month, and with that money I've got myself into electronic courses, camera operation courses, soundproofing for recording room courses, BetaCAM-SP operation and export courses etc.

Afterwards, I really got tired of having to support 64 districts network operations, though there were nine personnel in my team to support the vast network from 64 regional government offices. Applied for a SysAdmin job in BBC, and finally landed the job after six interviews, the last one was terrifying for me, I am one small me, having a meeting with the BBC-UK's technology team lead with a bunch of other folks, and I was just like the picture on the left side 😊. But acquired my strength, and on my last interview meeting, the country manager finalized me on the spot after one and a half hours of rigorous technical discussion. Landed on another candy land, with so many broadcasts equipment to get my hands on, my dream started again, heart pumped like a race-horse and acquired so many hands on knowledge, and lastly got trained in the BBC-UK's Wood Norton for the broadcast system deployments, BBC Bush House @ Strand for datacenter storage management services, connecting satellites & broadcast live streams, soundproofing a room, deployed gallery and recording systems with Final-cut Pro with Mac systems etc.

From BBC, I have received a lead to join Microsoft, since I was working on with AD, Exchange 2003, MS-SQL Server 2000, SMS Server and with lot other components from Microsoft (I have made great use of these documents from MoF, IPD etc.) it was an easy win for me to land the job. But a surprise was waiting for me again. Whatever I did, was not enough! And I was totally stoked to get my hands into those literatures on the Microsoft's central encyclopedia. And as a country's technical lead for Bangladesh & Nepal I've got so many companies to look out for their enterprise grade deployments, and I got engaged with so many different types of network deployments, opened so many doors….and that was the fastest learning time of my life…what a rush! My head literally

got bombarded with frameworks like MoF (Microsoft's Operational Framework), technical guides, deployment guides, system tuning guides, architecture design and things of these sort from the TechNet and from TechNet-Gallery as well, what a candy land for me 😊 and during my stay at Microsoft, I've had the life changing experience to discipline myself and to embrace larger perspectives and to roll with the trends, never thought of my limitations, and thanks to all my friends who never helped me and just because of those guys, I have learned to do things myself, hands-on, head on.

As my forum grew, I took on mentees and always gave them everything they ever could have asked for, and they grew to be such fierce competitors, and those friends warned that never to create any competitor so I would lose the competitive edge, but turned out, it was totally opposite, we as a team, an IT governance team, a SOC team, a Developer team, a DevOps team, we could go to war!

In those times, I was able to mature and capture and opportunity to develop an MFS (mobile financial service) organization. A battle took place for the MFS application, whether to develop with in-house resources or buy one? in-house won the debate as a monumental cost saving took place and granted to develop and deploy the service. Business requirements (BPM) mapped to SRS, IT requirements mapped and purchase of the equipment started momentarily. Completely new MFS platform developed with an eighty three FTE's (IT, & Dev, SOC) worked day and night with Kubernetes and Blockchain services, which is the 1st ever MFS application built in the country, and it's a massive application architected with microservices, mobile app UX developed and released publicly both for Android & Apple, two collocated datacenter deployed as DC & DR, and we did it within 9 months since its inception to production for the whole MFS deployment services.

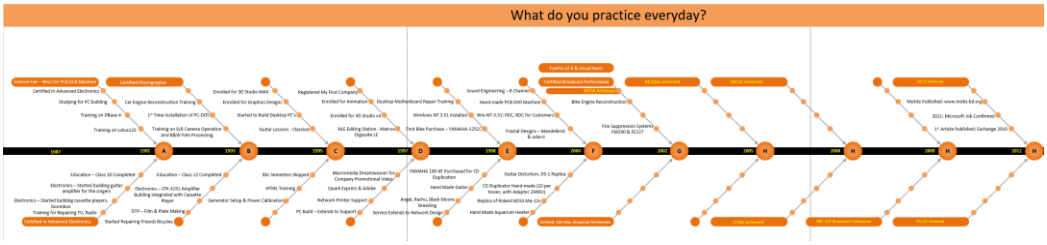
I have always tried to engage myself to create new doors of new opportunities from my connections, as wanted to explore for gaining different knowledge. Joined the largest nationwide ISP in Bangladesh, and enriched myself with their networking topology, scanned thousands of devices for vulnerabilities, how to detect configurations mishaps, how to detect network anomalies, benchmarking everything, documenting everything, breach & incident response, re-architected a gigantic ERP with 50+ core functional modules that controls different Router hardware for activating and deactivating clients automatically, various external & internal portals, revenue generating services, ERP portals, BI dashboards, payment gateway integrations, DDoS threat remediation techniques etc. and we did it with a fifty three personnel team (IT, Dev, SOC, & IPT).

I consider myself lucky, though I am not from a wealthy family, as I had many opportunities to choose from as they presented to me, and I eagerly explored different

paths, and managed to build SOC four times in Bangladesh in the last six years, in a 3rd world country with open-source tools, and still there are too many things I couldn't figure out yet. The first thing I did is to connect and collaborate whoever I meet and I have always placed myself as a credible source of technology integrations and knowledge provider, and as a technical advisor, whether it's a friend, an organization, a peer, where I never looked into the monetary part, and decreased it wherever I could, but never compromised with quality of service and friendship, and never shown ego, arrogance whatsoever.

I am thankful to the one who leads me and the people who influenced me (my team from my tech-forum), and I value their presence in my life, and it's an honor that I could make a difference in their lives and improved them a little.

A small effort came up in a very big way and many paths opened for me to run like there is no tomorrow (not suggesting you become a workaholic like me):



Areas of Expertise

- 360 Cyber Security Program
- Risk assessment & Testing
- Threat management
- IT governance
- Cybersecurity strategy
- Architecture roadmaps
- Enterprise cybersecurity architecture
- Portfolio management
- Program management
- Project management
- Very large-scale network deployment
- Network security monitoring
- Data & privacy protection
- Incident response
- Cloud service implementation
- Program charters
- Vulnerability management
- Secure development lifecycle
- Information security program
- System audit
- Business continuity
- Disaster recovery
- Cross-functional leadership
- Stakeholder communication
- Team building & Development

- ERP - planning & software development
- Policy, standards, processes & procedure development
- Architecting integration solutions & middleware
- ERM risk reporting
- Risk management strategy
- Risk analysis
- Control framework deployment
- Vulnerability assessment & penetration testing
- Database security architecture
- System security architecture
- Cloud security architecture
- Awareness training
- Business process development
- Database security architecture
- Operations Management
- Team Management
- Coaching/Mentoring
- Application security architecture
- SoP development
- Information protection, processes & procedures
- Plans (IR, BC, DR)
- Major frameworks: NIST, CISECURITY, ITIL, ISMS, TOGAF, SFIA, CMMC, SCF

I know this is too much to claim for, but in Bangladesh, the JD comes through in the Job Boards, they are horrible, and they wanted everything in a single person, I mean who writes these JD's? but somehow tried to do whatever I can that enriched my understanding a hundred fold, and evidential documentations, project documentations are the things that made what I came to be.

Industry: ISP, Bank & NBFI, MFS (Mobile Financial Service), System Integrator (SI), Broadcast & Terrestrial etc.

Certifications: Microsoft Cybersecurity Architect Expert, CISM, CISA, CDPSE, CRISC, CGEIT, PCCS-CCIP (Datacenter), PMP, CCNA, MCT*10, MCSE*4, Prince2, MCSA, MCITP, ITILv3, MCTS, MSBS.

You can reach out to me in different ways:

- My blog site: MOBS Bangladesh (mobs-bd.org)
- Download this FREE eBook (pdf) from the "Article" Section: Articles | MOBS Bangladesh (mobs-bd.org)
- Join Discord: Please message me on LinkedIn
- Connect with me in LinkedIn: Shahab Al Yamin Chawdhury | LinkedIn
- Job aids – download documentation: Book-SOC Job Aids

I am aware that, I have been able to successfully confused you throughout the book, but as you grow, you will see that it was not intentional, it's just what things are right now, maybe in 20 years' time, everything will be automated and integrated to a platform sized solution, management plane, data plane and control or console plane will have synergies all together and in a better way to sharing things to the monitoring services, devices firmware's will have better API's prepared to share data instantly, management and AI based detection and protection techniques will reach an astounding level, and attackers will be highly sophisticated as well adopting to AI services to do human-less works for them.

Lastly, if you want to connect, please drop me a line on LinkedIn, and for the eBook, if you want the DOCX version, I will send out the link to download the editable version of the book. If you need consultation or strategy development, or seeking any type of help, you can always contact me on LinkedIn as well.

Please be mindful that I get a lot of messages from my peers, don't get offended if I cannot reply to you all for attending your queries.

Good luck on your journey, I hope that you succeed on every step you take in your lifetime, and your path will shine brighter every day in the coming years.

Let's grow together and share knowledge, as they are meant to be free.

Regards | Shahab