20th August 2023

SECURITY OPERATIONS CENTER

A proposal and guide to an effective SOC design and implementation which maps well with the evolving adversarial threat landscape. Prevent, Detect, Respond and Recover from security incidents like never before. A holistic approach towards protecting your enterprise assets and business operations.

PREPARED BY ADEEL JAVAID
adeel.javaid@owasp.org

Table of Contents

Executive Summary

In terms of internet activity and the clicks made online, the distance between an individual and the threat actor is mere 2-3 clicks away, or often in many cases, the victim doesn't need to make clicks even consider weaponized 0-click RCEs, exploiting insecure networks, vulnerable applications, and hosts.

Imagine a user receives a malicious password reset email in their mailbox, they open that email (**1st click**), either click the URL embedded in the email body or download the file attachment (**2nd click**), and then they either enter their credentials on the redirected web page or open the downloaded document (**3rd click**). That's all it takes to gain a firm foothold inside a network.

We don't have to get into the intricate details of every threat here, that's the part to be done in Threat Modelling exercises. Phishing campaigns are getting more sophisticated, and so are ransomware groups. I will brief on the aftermath because the ransomware ecosystem is complex and warrants a separate discussion.

Evolved Threats

Ransomware groups have evolved and there's a recent trend of Double and Triple extortion, here's how -

Keeping victims' networks and systems hostage, locking down business operations, all data is encrypted and backup servers are rendered useless, and destroyed. This is classic ransomware.

Double Extorsion: Threatening to release data and demand heavy amounts of cryptocurrency in a short time. The amount increases with any/every mistake/delay.

Triple Extorsion: Threatening to inform the victim's clients/customers about the data breach, via personalized communication channels and/or publicly leaking/selling the stolen data. Loss of reputation, monetary loss via Governance, Compliance, and regulations, and loss of clientele.

REvil is a prominent ransomware group and I will highly recommend reading their chats (which is publicly released) here.

It's a real conversation between REVil and one of its victims, among several other conversations of various ransomware groups, you can observe how they negotiate and impose pressure on the victim, initially treating them as a client.

Insights into the Threat Landscape

According to **Qualys TruRisk Research report 2023,** if we take into account the vulnerabilities alone, In 2022, there were a total of 25,228 known vulnerabilities, out of which 7786 (30%) were vulnerabilities with exploits available, 159 (0.6%) were the vulnerabilities with weaponized exploit code available. Interestingly only 93 (0.36%) of the vulnerabilities were exploited by malware, 23 (0.09%) were exploited by threat actors -APT groups and alike, and 18 (0.07%) were exploited by ransomware groups.

Executive Summary

Another useful insight we can derive based on the Industry segmentation is, Retail (3.4%) and Finance Industries (3.5%) were victims of destructive ransomware outbreaks. This data is enriched from **"Five lessons from 1000 destructive ransomware events" by Riskrecon, January 2023 report**.

Almost every threat classification will have reports and statistics associated with it. Major and emerging threats out there are -Ransomware groups and affiliates, Intrusion Access Brokers, Business Email Compromise, Phishing, Automated botnets, Insider threats, and so on...

Security Operations Center - SOC

This document will serve as a foundation to give you insights into a modern enterprise-grade SOC which is scalable. I have laid down the proposal of SOC design, build, and deployment into the timeline of **1 month, 2 months, 3 months, 6 months** down the road, and **1 year and beyond.**

As a security operations engineer, what exactly does my role encompass? especially starting from scratch. It has been highlighted by the end of 1 year and beyond module with a nice representation of SOC Personnel and their Hierarchy. Following it up, there's the Risk Matrix for SOC deployment, potential cost projection - investment into personnel training and purchase of security solutions, and finally ending with giving insights into the operational working of SOC - dealing with alerts i.e., Alert Triaging.

1 Month

In the initial phases, i.e The 1st month, I will focus on an in-depth enumeration of people, processes, and the technology in place. That would enable me to lay the foundation for executive functions of the SOC operations.

# PEOPLE

1. Who do I need to contact for presenting investment proposals? Demonstrating the progress, debriefing on security incidents (if any) etc... Involvement of management in decision-making - at this level - need not be done in isolation.

2. C-suite and stakeholders involved - technical, non-technical, legal etc. Should have interacted at least once.

3. Understand the lay of the land of various divisions and departments, which will help me segment them later, based on security needs. Zero-Trust architecture and the Principle of Least privilege.

4. Point-of-contact: Contacting relevant individuals/parties involved in the event of any security incident(s).

5. Helpful in asset inventory management (disabling accounts of former employees etc...)

# How will I do that?

1. Circulating Google forms internally to collect the relevant information, or working closely with HR / Management (staff) to map the organizational structure and people involved. The questionnaire would incorporate questions like - Individual’s name, position, contact details, brief bullet points on their roles and responsibilities, whom they report to, who reports to them, what access they have in terms of assets like network & host resources, and especially if they are the ones working with PII data.

If any one of these is not fulfilled, then there will be an ineffective design and implementation of the SOC - because I am responsible for the operations and engineering altogether, it’s not just a matter of assumed responsibility anymore, it is a necessity.

Worst case - weak SOC infrastructure because investment in security tools wasn't deemed worthy, lack of point-of-contacts when security incidents happen: that accounts for delays, lack of visibility, resistance in collaborative efforts and giving threat actors more time in the networks to continue invoking damages. If HR accesses a production environment and the Network Monitoring Solutions show packets leaving our network - that's a problem.

That's why - the visibility into the people involved in the organization, also helps in baselining the operations. Baselining what's normal, so that we can identify what isn't normal i.e., abnormal activity, such as logging from different hosts or networks altogether when they shouldn't have. Humans are the weakest link in the security posture of any organization. This will help mitigate insider threats as well, which I will brief on later.

PROCESS

People interact with people, and technology, under a certain process, which should be well-defined. Lack of visibility in processes happening in the organization would mean - a lack of visibility and lack of execution rights.

Business Logic flaws - not just in applications, but business operations too, breach of trust via phishing emails/SMS/calls which impose urgency by a superior entity in the organization - which was impersonated by a threat actor, advanced social engineering tactics to hand over confidential data, etc all these threat vectors amount to lack of rigorous process in place which should be ideally security oriented. Since we are into data analytics, I would examine how the client hands over data to DitchData.ai, how we process it, how we store it - using secure encryption methods or not, data at rest and in transit's safety, etc… securing that workflow would require an in-depth understanding of the intricate details of the processes involved. Apart from that, the essence of DevSecOps will be incorporated later on.

It's just one of the workflows, there are many in the organization, think about its security. I will give a few more scenarios: Imagine 3 years ago Vishal mega mart handed their customer's data to some data analytics company - Company X, now this company X suffered a data breach last month, but at the time DitchData.ai is handling the data analytics of Vishal mega mart, so Vishal mega mart suspects the security of DitchData.ai (internally).

The Ideal case should be - DitchData.ai approaches Vishal mega mart confidently and hands over the network packet logs and host-based logs which depict how we handled their data, and DitchData.ai confirms that it hadn't faced any security incident. Based on those logs Vishal mega mart's security team can collaborate closely with us to confirm that we are not the source of the data leak, but some 3rd party compromise that happened due to inefficient ways of handling PII data by company X. This will save our reputation, will enhance the bond with our customer(s), and gain their trust in the way we are handling their data.

This is just one specific example of - processes in place. Another could be - no file exchanges happening over other mediums/networks (other than the corporate network) - Like the developer went on vacation and connected to a rogue WiFi Access Point and some guy on Linkedin approached him pretending to seek an Internship in the devs dept. And he handed him a malicious resume (pdf/ word file), or the Dev clicked on the URL sent by the threat actor impersonating someone (HR), via email spoofing etc... especially when WiFi is already compromised, everything on the network can be intercepted and modified on the fly, a bank account transfer even. So it's deadly.

A mature security posture would incorporate a well-documented security policy and guidelines in place, which requires extensive enhancements over time.

HOW WILL I DO THAT?

Making rigorous security policies and guidelines and imposing them across the organization. This document will evolve over time, it'll define technical details - like password policy, MFA implementation etc, non-technical - whom to contact and whom to not contact immediately, the process of escalating matters etc, legal - if things went south (especially in case of Insider threats, the role of the company, legal implications etc). And industry best practices and security guidelines to be followed by the employees respectively.

Knowing people	=	Knowing the tools
Knowing the process	=	How to use the tools
Knowing technology	=	When and where to use the tools

TECHNOLOGY

Asset Inventory Management (AIM) - employees, their user accounts, the access to data, what they're allowed to do with that data - in major cases - exfiltrating the data (PII) is not allowed, or tampering with it / poisoning it with external sources. Employee's access to networks, HRs can't access the production environment, and vice versa. Need to work closely with Network administrators and System admins to implement it.

Host/endpoint names, their static IP address, their utility where they belong to rightfully. Installed software on the host, allowed tools to execute in-memory code/scripts, Interpreters, Code Libraries used for the project, etc. So whenever a library/dependency being used in the codebase observes any 0-day or software vulnerability, we will keep a tab of it and hence resolve it as a priority, so threat actors can't exploit it. Servers - DNS server, Name server, Mail server, File and Network Share server, web server, Backup server etc. What technology stacks are we using ? Dockers? Kubernetes? Do we have wireless network integration? APIs? Active Directory? Cloud infrastructure etc...

Privilege escalation of users on the endpoint is valid or not, users moving laterally in the network/hosts is valid or not, data exfiltration/transfer is valid or not, the disabled user account has been activated again - valid or not, and vice versa, etc, all these concerns will be mitigated by rigorous AIM. Maintaining AIM is an ongoing process, in case we are scaling rapidly, and newer assets are integrated into our networks and hosts, all of it'll be documented so we retain our visibility into the infrastructure.

Patch Management - It gets easier once AIM is in place. I can then maintain and document the patches in a centralized changelog, and even automate the patch management. Some patches introduce instability and dependency issues with the existing code base, so we can design and test those patches in a controlled environment before pushing them to production. Availability is an important pillar of the CIA triad. Overall, every asset should be patched, and up to date with security and bug fixes. Patch management would differ based on host-host, network-network, and security appliances / sensors (if in place), to ensure that the patches are applied correctly.

Assets segmentation - To design an infrastructure that scales securely, we need to segregate the company's assets from the individual's assets. It gets exponentially difficult to manage and monitor the devices an individual owns, it's easier once devices fall under the corporate network. Examples - Work email vs personal email, hosts/endpoints where data processing happening should definitely not be someone's personal computer, it'll lack visibility and network telemetry data will be inconsistent over time, even if we designed a monitoring solution for it. These acts unnecessarily increase the attack surface. A sufficiently advanced threat actor can compromise that personal computer and exfiltrate the data, which would otherwise be not possible via the corporate network.

Under any circumstances, SOC should remain unaffected by any incident - security incident or else. The SOC should be fully working, operational, up 24/7, 365 days a year, continuously ingesting the logs, aggregating them, and displaying them in SIEM solutions. This workflow should not be affected at any cost, and SOC's deployment resides in the most secure networks. The worst thing that could happen after all these security architecture deployments is - your SOC getting compromised/affected in its workflow because of some security incident, rendering it absolutely useless/helpless. This is why, although the SOC has access to harvest the data from the endpoints, ideally it should be separated from the network in a secure way. Suppose in cloud infrastructure we are using Azure, then the SOC should be deployed up in either AWS or GCP or any other cloud with the highest uptime. Again, if it's on-premise, then SOC would ideally be in a proper network-segmented area, or even air-gapped in some cases.

NOTE: If there are more than hundreds of assets and several networks, then we will need some external tool to accompany the entire patch management and AIM process. And that solution will be scalable too.

2 Months

By the 2nd month - I will focus heavily on system hardening, each and every documented host and network will be hardened according to -

- CIS Benchmarks - https://learn.cisecurity.org/benchmarks
- Exploitation vectors unveiled by security tools for host and network enumeration, like LinPEAS, WinPEAS, GTFO Bins, the utility of Living-off-the Land binaries, etc
- Configuring Host-based firewalls on each endpoint, stopping unnecessary services, processes and ports, baselining them etc…

This is where my Red Teaming experience and expertise come into play. CIS Benchmarks are a mere Blue teaming component, to aid it with more enhanced security, we need system hardening which mitigates most of the exploitation vectors which are uncovered by the offensive tools.

- AppArmor and SELinux for Linux-based servers - web, mail, DNS, Lynis, OpenSCAP
- Bitlocker for Windows, Microsoft Baseline Security Analyzer (MBSA), Microsoft Security Compliance Toolkit, PowerShell Script Blocking etc...
- Subjecting the endpoint to widely accepted system hardening checklists available online, based on the Industry grade security practices.

I will harden different technology stacks, one at a time, Applications - web apps, desktop apps, android apps, servers, clients, APIs, Docker, cloud infrastructure via Identity Access Management solutions (IAM),

Depending upon the scale of operations, the security architecture engineering might have to purchase enterprise-grade solutions to address system hardening in a scalable and effective way, AWS IAM, Office 365 E5 licensing from Microsoft, or other IAM services like integrated with Active Directory and cloud (Azure AD) etc…

The 1st month is an ongoing process, like creation, it’s ever going and it’s not a finished state of process. Hence, it’ll add up to what I am going to do in the 2nd month, and so on, these processes will get easier once they attain a certain level of maturity.

3 Months

By the 3rd month I will - focus on security solutions deployment - which goes hand in hand with - security architecture deployment and/or engineering,

Security solutions such as - Enterprise grade VPNs, VNC softwares, Password policies, password rotation policy, passphrase adoption, MFAs implementation, Next-Generation Firewalls (Juniper Networks SRX Series) etc, Host-based Intrusion Detection Systems (HIDS) -OSSEC and Host-based Intrusion Prevention systems (HIPS) like Snort IDS/IPS, Bro - Zeek, Network-based Intrusion Detection System and Prevention System (NIDS/NIPS). EDR -Endpoint Detection and Response system - CrowdStrike Falcon, SentinelOne, CarbonBlack etc then XDRs - eXtended Detection and Response Systems - Microsoft 365 Defender, CrowdStrike Falcon, Cortex XDR, Cisco SecureX, etc… Email security solutions - to prevent phishing. Web application firewalls - CloudFlare, Akamai etc, I've already stated the host and network-based firewalls.

Of course, I will implement one - one each from EDR and XDR, meanwhile a combination of HIDS/HIPS and/or NIDS/NIPS are required subsequently. Purchasing EDR and XDR are necessary investments. Meanwhile we can adopt a mix / hybrid model of incorporating NIDS/NIPS/HIPS/HIDS in our networks and hosts, open-sourced + paid subscription to their rules, configurations, and threat intel even.

The Main goal of this month and onwards would be to implement these security solutions and test them subsequently if they are working fine as expected/configured. Notice that this is happening on top of our hardened systems, and servers. Moto is - "**EXPLICIT DENY**" . This phase will also incorporate automated vulnerability scans - using tools like Burp Suite Pro and Nessus.

There's a concept of blacklisting and whitelisting, and it will fairly apply here, both of them have their own pros and cons, but ideally a secure environment would incorporate explicit denial until given access to the operation / resource. This is especially helpful to align well with our zero trust architecture and the Principle of Least privileges, which would be fruitful to prevent damages from Insider Threats and other adversaries alike.

Wireshark will be monitoring the network traffic sitting on the switch in promiscuous mode on the mirrored port, generating network logs, and forwarding it to the centralized log aggregation server, this is one of the network-based artifacts collection, then snort will be deployed in IPS mode - Intrusion Prevention System - directly sitting in-line between the internal hosts and the firewall / DMZ network, this will ensure that even if the next-gen firewall fails/bypassed/breached due to some 0day vulnerability, this alignment would not let that packet pass through the snort IPS, and even if the exploitation happens, the reverse shell will be thwarted, allowing the remote attacker only a limited remote code injection/execution over the app/service. It's good for packet harvesting in the network, but in-depth insights into the analysis of packets could be rendered via zeek, which will remain at our disposal in the workstation, ingesting its logs and visualizing them.

Similarly, on the endpoints - hosts, we configure osquery for endpoint monitoring and analysis, it can run in File Integrity monitoring mode and as well as monitoring the entirety of the endpoint -using PowerShell remoting, and WMI scripts, we can configure it to execute commands on n number of hosts and fetch the results quickly, which isn't possible via traditional SIEM / SOAR solutions, that's the power of scaled security solutions and executing commands immediately across the endpoints.

Sources of logs are plenty, and we will focus on the most essential ones - Windows EventIDs, windows sysmon operational - configured and customized, Windows antivirus and firewall logs, windows defender 365 logs, and any logs generated in the clouds assets will be collected and forwarded to the centralized server too, network-based logs (perimeter based) - HIDS/HIPS, next-gen firewall logs, mail server logs, email security solution logs (.eml), web server logs, web application logs, DNS server logs, Proxy server logs, VPN logs, Authentication logs - host and Active Directory-based, Docker logs etc. You get an idea, we should not miss any of it. The goal here is to collect all these logs and forward them to the centralized SIEM server. There these logs will be ingested into the SIEM/SOAR solutions accordingly.

Two more important things to notice, which are happening at this point -

- **Security logs generation**
- **Security workflow - Including backup servers & Centralized log collection server**. At this point, I have devised, engineered, implemented and configured security solutions, and automation, in a certain way that it protects our assets - networks, hosts etc, and generates logs of it, and those logs are forwarded to a centralized SIEM server, there it's stored for a longer period of time, because often we might have to present valuable logs in our own favor, remember the Vishal Mega Mart case, or consider this - an organization can't confirm if they were victims of solarwinds attack, but their security team has centralized logs, now they can confirm quickly if they have been compromised, via investigating those older logs based on the Indicator of Compromise (IOCs) shared in the Threat Intelligence community.

Log harvesting is done in a secure manner, protecting the integrity of our logs, because often attackers try to manipulate, delete or alter the logs to their advantage. A secured security workflow for SOC will be designed accordingly.

Apart from the security of log files generated, right here at this stage of security, backup servers will be implemented, and battle-tested to be secure against even in the ransomware outbreak. Assume the worst and start preparing for it accordingly. Backups of data of DitchData.ai clients, of DitchData.ai infrastructure etc... Again, it'll follow the secured workflow of data at rest and in transit.

Addressing Future Threats

With the advent of **Quantum Computing**, many threat actors are performing **HNDL (Harvest Now, Decrypt Later)** attacks - in the hope that in the next 5-15 years when quantum computers will be effective and operational, then they could render the encrypted data useless, cracking all algorithms. So ensuring that just-in-case if threat actors are performing data exfiltration, there are several ways to render that data useless - because here the encryption will be broken later on, and sometimes, data is better kept secret. Bit-flipping might help in this case, rendering it useless - gibberish, junk, there are several other methods of data overwriting and corruption too. Even using forensics methods data can't be acquired back, hence useless.

6 Months

At this stage, DitchData's security posture will begin to mature. There are already 3 phases and iterations of defensive security happening. In case you haven't realized, the above phase is also about zero trust architecture + principle of least privileges + Defense In-Depth / Layered defenses.

Recall that the 2nd month was heavy on the host/system/server hardening, from here onwards I will focus solely on Network hardening to continue with. That includes securing the network protocols and services enterprise-wide, as well as collecting logs necessary for conducting Threat Hunting on the network level - including **DEEP PACKET INSPECTION**. Phase 3 has already enabled me to execute commands on any endpoint and gain visibility into it. This phase requires extensive focus to address the issues of advanced adversarial tactics like - Low and slow data exfiltration, data exfiltration over legitimate cloud data storage services, covert channels, encrypted channels, tunneling attacks like DNS/ICMP/SSH tunneling, etc, and configure our network to prevent, detect and respond to the data exfiltration attacks, network pivoting, advanced firewall bypasses, credential harvesting over the network, etc... all of this requires **advanced adversarial emulation - Red Teaming**, to test the deployed security measures. Many organizations don't have this in-house capability and it's also not a comprehensive way to address this challenge. Any outsourced red-teaming consultancy firm will perform the offensive assessment - via exploiting one, two or maybe three distinct exploitation vectors to gain access to your networks and systems, then they'll debrief upon it and move on via giving some generic recommendations. Understand that each network is distinct from the other, each organization's requirements are different, operational needs, etc. So an in-house red-teamer / a person who is knowledgeable in the offensive security operations is needed to better defend the infrastructure.

Adversary Emulation

Many of the **Breach and Attack Simulation (BAS)** softwares are available in the market, but they are as effective as their creators intend them to be, they don't know your networks, be smart and emulate threats accordingly.

Recall that as previously discussed, EDR and XDR solutions are running already, they're configured. Now SIEM and SOAR solutions will be fully configured to ingest the data stored in the centralized servers and run their agents which collect the logs generated in real time. Then I will create a custom dashboard that reflects what kind of attacks I am focused on, classify them under categories, then create rules and their alerts - which will be triaged accordingly based on priority, severity, and impact. Here - SOC & Incident Response playbooks will be made, and everything will be well documented as usual. As I am working on fine-tuning the alerts (because the volume of logs will be tremendous), I will work on reducing the false positives and false negatives.

This is the exact moment where the Threat Intelligence feeds will be ingested into our **Threat Hunting suite** - which can conduct (automate it to some extent) threat hunting exercises based on Indicators of Compromise like hashes of malware - MD5/SHA256 etc, their names, file size, I will use sigma for detection engineering, YaRa for detecting the threats, Mandiant RedLine to quickly analyze the host, etc … there will be an entire workstation dedicated to the threat hunting and Incident Response capabilities.

Coming back to the XDRs and EDRs, realize that no traditional tools can stop/prevent sophisticated adversaries which use in-memory methods to evade detection, and for the most part, this is exactly what's happening out there in the wild and emulated red-team assessments. A process can initiate a network connection, exfiltrate the data / receive C2 commands and execute it on the host and then terminate. AMSI bypass, UAC Bypass, credential guard and application guard bypass etc are all common for a competent threat. Their payloads and malware won't touch the disk, consequently, there are very less or NO logs which can be generated out of kernel- level operations - imagine detecting advanced rootkits. So to at least prevent this from happening in real-time, to whatever extent, we need XDR and EDR solutions. They get regularly updated and are effective in mitigating most of the non-sophisticated threats.

Detecting network / disk-based threats, Windows host-based and Active Directory attacks - Kerberoasting, ASReproasting, GPO abuse, Golden and Silver Tickets, Pass the Hash, AD Certificate-based attacks, PKI - ESC8, Object ACLs, DCSync, LLMNR NBT-NS Poisoning, NTLM / SMB Relay attack, Delegation Attacks etc … Registry key modification, WMI / Service based persistence, disk-based malware specimen can still be detected and prevented easily, but I want to emphasize on prevention first, imagine in-memory threat Injection attacks, there's a lot of variety in process injection attacks, process hollowing, ghosting, DLL sideloading, DLL Proxying, DLL Hijacking, etc, Customized Command and Control (C2). Nobody can monitor them manually 24/7 by examining memory artifacts every now and then.

Enterprise Grade Memory Forensics Workstation

This brings me to the need of implementing enterprise-wide **Memory forensics and Threat-Hunting** workstation, to quickly acquire forensics data and analyze it before it's too late. Which I will design using volatility, automating it with several other integrations, it's a lengthy and hectic configuration. The workflow will be routined, scheduled and automated.

One can only imagine what amount of effort and resources go into implementing such a security architecture.

In the middle of, or by the end of this phase - I will conduct **end-user training** against the most common threats out there. They will already have exposure to security policies and guidelines in place, but the training is different because at the end I will assess the employees via an **Emulated Phishing campaign**, some social engineering tactics - smishing, vishing, physical security aspects (if in person), etc. As I had said already, humans are the weakest link in cybersecurity, but we need to transform that into our strength. That will limit us to the technological realm and focus on more sophisticated threats as a priority.

It shines out!

This is the exact phase where significant differences will shine, between a blue teamer who knows only blue teaming vs a blue teamer who knows both Red and Blue teaming. Approach to securing a system will be different, Ideologies will differ, their stance on any security incident will be different too, and need not say, the way they handle it will also differ. **Thinking like an attacker is a real thing, and that comes from knowledge and experience. Think Red, Act Blue.**

If you've read till this point, you would have realized my layered and structured approach toward addressing the issue of building SOC from scratch in hand. I bring a lot of valuable experience and expertise from my Red Teaming background, especially while testing the security solutions deployment - where I emulate the threat to trip on the alerts to test it. **Sustaining all of this operation under the evolving threat landscape is a very challenging task**, and I have demonstrated my vision towards addressing this challenge too. I embrace it wholeheartedly.

These 6 months will be reserved for this phase.

1 Year & beyond

Above all, discussed strategy and methodology could be aided with more than what most of the organizations can imagine. This is so close and special to me, it's called "Cyber Deception" and it's exactly what it sounds like.

By definition - **Cyber Deception** is a proactive security measure that involves the use of deceptive tactics to mislead threat actors, manipulating them or forcing them to reveal themselves. The objective is to detect, divert, and neutralize attacks in real-time while collecting data to better understand the attacker and their tactics, techniques, and procedures (TTPs).

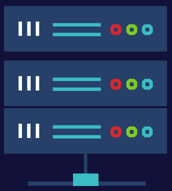
What are the technologies utilized you may ask ?

I use **MITRE's ENGAGE** framework for cyber deception - https://engage.mitre.org/matrix/ it's a brand new and awesome resource for reference,

Some technologies at disposal are - canary tokens, honeypots, honeynets - decoy networks, False data and traps - baits, for instance false credentials that the adversary gains access to in honeynet and tried to password spray across the AD domain, got caught and kicked out of the network immediately. It's a cat-mouse game of using psychological tactics and cyberwarfare in a real-live environment. Once they know that their identity has been potentially compromised, the chances of them coming back are drastically low. Threat's OPSEC is up for the grab once they trip into the cyber deception, here defenders have some upper hand over them.

As I said, it's a game of psychological tactics too, so thinking like an adversary is a must, moving beyond the 6 months phase.

Moving ahead with the deployment of the cyber deception tech stack, I will ensure we have a killswitch mechanism across the endpoints, some SIEM solutions like ELK stack already have that, one which I have used already - to lockdown the host immediately.



At this point in our organization's security posture, I can spend time emulating advanced threats which operate at their **peak Red-Teaming performance**, and identify if there are certain loopholes to be addressed. Full-fledged Red-Blue teaming exercises, the essence of purple teaming. I will also explore the possibility of "**Adversarial Threat Landscape for Artificial Intelligence System**" ATLAS by MITRE (https://atlas.mitre.org/), that would be beyond my scope of work, but certainly, I can reach out to the AI folks at our organization - DitchData.ai and then discuss the scope of threats and incorporate defenses accordingly.

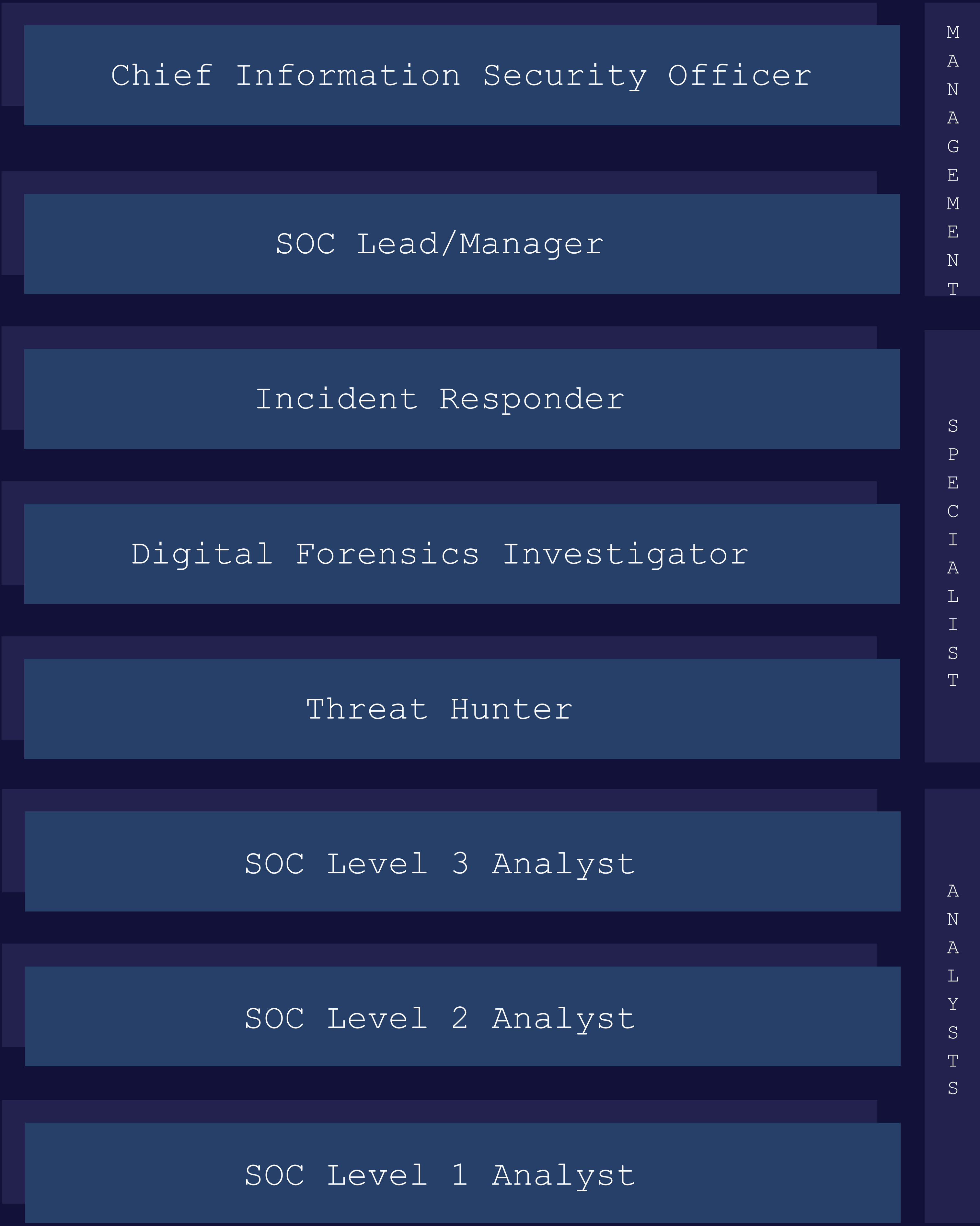
Delegation of work will begin from this phase, I can single-handedly do everything, but I have just 24 hours in my hand every single day. Work-Life balance, mental health, and personnel training would constitute significant portions of it too. SOC team building, Tiering it up, scaling it across the global offices as pleased, Conducting **Dark web Intelligence** - proactively looking out for any Intrusion Access Brokers eyes on our organization, Ransomware affiliates, Hacktivism etc, monitoring dark web forums, marketplace, if employees data is being leaked in data breached etc … could be rendered via outsourced Dark Web Intelligence, or devising an in-house mechanism as necessary.

Compliance-based vulnerability assessments and penetration testing could be done further at this point, complying with GDPR, HIPPA, PCI-DSS and whichever applicable.

I will present a breakdown of SOC personnel and their hierarchy, that will help derive an insight into the essence of designing, building, deploying, and sustaining a SOC from scratch.

It's a definite composition of both technical and non-technical aspects of a full-fledged operational SOC. It aligns well with the strategic, operational, and tactical goals of having a SOC in place. Organizations have different names and job roles for various positions, as such cybersecurity analyst, security engineer, etc. But the division of labor is very well defined in each plane. The managerial plane comprises a CISO (Chief Information Security Officer) and SOC Lead/Manager, then a group of specialists or at least one of them - Incident Responder, Digital Forensics Expert, and Threat Hunter. Then there are three tiers of analysts, divided by the increasing workload and responsibilities -SOC Level 1, 2, and 3 respectively.

SOC/Security Personnel Hierarchy



Chief Information Security Officer

SOC Lead/Manager

Incident Responder

Digital Forensics Investigator

Threat Hunter

SOC Level 3 Analyst

SOC Level 2 Analyst

SOC Level 1 Analyst

Risk Matrix

For effective risk management associated with the SOC engineering and deployment project, I will brief upon the risk acceptance, transfer, avoidance and mitigation. They allow the SOC to effectively manage cybersecurity risks by understanding and choosing which risks to accept, avoid, transfer, or mitigate. These strategies help prioritize resources, align security efforts with business objectives, ensure regulatory compliance, and ultimately safeguard the organization's assets and reputation. They are the cornerstone of a proactive, adaptive, and resilient cybersecurity posture.

RISK ACCEPTANCE

- Tolerance of informational/Low impact alerts
- Limited resources allocation
- Residual risk acceptance
- Monitoring over Mitigation(s)

RISK TRANSFER

- Outsourcing SOC operations
- Cyber Insurance coverage
- Shared responsibility models - Cloud Service Providers
- 3rd Part engagement(s) - secure email gateways, Bug Bounty programs,etc.

RISK AVOIDANCE

- Avoidance of unsafe practices
- Secure configurations, system hardening
- Network segmentation, Zero Trust architecture, Principle of Least privileges, Defense in-depth, Threat Informed Defense, etc.
- Identity and Access Management, strict access control policy, etc.

RISK MITIGATION

- Incident Response planning
- Regular automated Patch management
- Security awareness training, end-user phishing assessment
- Continuous logging and monitoring

Cost Projection

For Personnel Training and upskilling & Security Solutions

Offensive - Training

- **HTB - Business**: https://www.hackthebox.com/business-cyber-security-training
- **HTB- BlackSky:** https://www.hackthebox.com/business/professional-labs/cloud-labs-blacksky

Offensive - Certs

- **Azure Application Security:** https://www.alteredsecurity.com/azureappsec
- **Attacking & Defending Azure AD:** https://www.alteredsecurity.com/azureadlab

Defensive - Training

- Blue Team Labs Online
- LetsDefend.io
- CyberDefenders
- RangeForce.com
- Pluralsight.com

Defensive - Certs

- **Cisco Certified CyberOps Associate certification**
- **CompTIA CySA+**
- **EC Council Certified incident Handler**
- **eLearnSecurity Certified Digital Forensics Professional**
- **INE Enterprise Defense Administrator**

These are some specific training platforms and certifications to begin with, with time it'll expand respectively.

Security Solutions

Security solutions as discussed in the SOC engineering modules are enterprise-grade, which implies that often their pricing and quotation vary from one company to another, depending upon the volume of assets. We might need to contact their sales to get the pricing details.

Pricing might be based on annual purchases or subscription-based. For open source tools with paid versions enrich additional features we need for scaling into the enterprise, this hybrid model is cost-effective and efficient too.

Alert Triaging

Alert triaging, is the process of evaluating and prioritizing security alerts generated by various monitoring and detection systems to determine their level of threat and potential impact on an organization's systems and data. It involves systematically reviewing and categorizing alerts to effectively allocate resources and respond to security incidents.

Too many alerts can lead to alert fatigue, where critical alerts may be overlooked due to the high volume of alerts. On the other hand, too few alerts could suggest inadequate coverage of the organization's threat landscape. An ideal scenario has the right balance of alert volume -quality wise and the actionable alerts - meaning they provide meaningful information that can directly facilitate an effective response.

6 Months phase and onward constitute the Integration of all security solutions under one centralized SIEM server in the cloud, also fine-tuning the alerts, reducing false positives, testing those alerts based on the rules configured and increasing the visibility into the endpoints and networks. Below is the example of what alerts would look like -classified under critical, high, medium and low severity.

Alerts

#	SIEM/SOAR/EDR/XDR/Firewalls, AV Engines	Priority
1	Ongoing data breach alert: Large volume of data transfer is happening from a secured PII database to an unknown IP address.	● CRITICAL
2	Multiple failed login attempts detected within Internal network - to a server hosting sensitive data, within a short span of time.	● HIGH
3	Unusual spikes in the CPU Usage from a user account on Administrator's machine, accompanied by spikes in DNS requests and a large volume of ICMP packets.	● MEDIUM
4	A network perimeter scan [TCP Connect] has been detected from a group of external IP addresses targeting hosts in the DMZ network.	● LOW

Contact Me

adeel.javaid@owasp.org

LinkedIn