University of Houston – College Of Technology

CIS 6322 – Secure Enterprise Computing

Security Operations Center

Paper Submission

Dhanaraj Chalil
dvchalil@uh.edu

Submitted on: 8th March 2019

TABLE OF CONTENT

SECURITY OPERATIONS CENTER

ABSTRACT

This paper describes on Security Operations Center (SOC), an organizational team responsible for handling security against cyber-attacks and to maintain a good security posture. This paper also describes every aspect related to SOC in detail. This includes a detailed introduction, importance of SOC, and benefits for an organization for hosting it. A projection of the best practices that it follows is also included in this paper. This paper describes how to set up a SOC in an organization. Setting up a SOC involves the importance of three different aspects. They are people, process, and technology. People with professional roles involved in SOC can be classified under different tiers, where they perform some operations. Building a SOC also involves some defined processes, to which this team will be focusing on. The technology involves several categories of toolsets that these team will be handling at different levels. Through this paper, an excellent view of the Security Operations Center can be drafted.

1. INTRODUCTION

In this era of rapidly advancing technology, all types of businesses either big or small must consider effective ways of implementing a strong security posture to protect sensitive information about their clients, employees, partners, internal operations and more. But with the rising sophistication of cybercriminals and hacking practices, this necessity for protection has become an increasingly challenging task. The possibilities of facing a security breach have risen considerably over a decade. A recent study in the United States found that one in four organizations will have their data attacked within a year's time. The cost of facing this attack is high and will have a bad impact on the organization's operations and client's trust. Without the right security measures in place, businesses could start accumulating these costs unawares, as the study further states breaches take an average of 206 days to detect.

Considering these findings and existing facts, businesses need a method to defend themselves reliably against potential cyber-attacks. Some rely on advanced programs to scan their networks, while others outsource their cybersecurity entirely to external service providers. Another effective concept that continues to grow in popularity among strategy-focused organizations is the incorporation of a security operation center.

A security operations center (SOC) is a facility that houses a highly skilled information security team responsible for monitoring and analyzing an organization's security posture on an ongoing basis. The SOC team's goal is to detect, analyze, and respond to cybersecurity incidents using a combination of technology solutions and a strong set of processes. Security operations centers are typically staffed with security analysts and engineers as well as managers who oversee security operations. SOC staff work closes with organizational incident response teams to ensure security issues are addressed quickly upon discovery. Security operations centers monitor and analyze activity on networks, servers, endpoints, databases, applications, websites, and other systems, looking for an anomalous activity that could be indicative of a security incident or compromise. The SOC is responsible for ensuring that potential security incidents are correctly identified, analyzed, defended, investigated, and reported.

A security operations center (SOC) resides as a centralized unit within a building or facility. It acts as a central location from where staff supervises the site, using data processing technology. The technologies SOCs employ include an arsenal of firewalls, probes, security information, and event management systems and solutions that collect and monitor data as it moves across the various platforms and endpoints. The SOC team analyses recent feeds analyze them thoroughly and will establish rules, identify exceptions, enhance responses and keep a close eye on possible vulnerabilities in the defenses they have already set up. Ensuring these programs comply with company, industry and government regulations is also a significant part of a SOC's job.

Different ways to deploy a security operations center are described in the following sections of this paper. On an overview, it can be an in-house SOC, while others opt to outsource it. Irrespective of this deployment pattern, every SOC have the primary goal of preventing breaches and minimizing losses due to cyber-criminal activity. This SOC team need to be included in all organizations regardless of domain, which deals with sensitive data and services. This special team is becoming more prevalent as cybersecurity threats become increasingly catastrophic throughout the public sector, in the military, in health care, among financial institutions, in educational systems and more.

2. IMPORTANCE

One can point out several good reasons for hosting a SOC in their organization. But among these reasons, there are some key points which make it crucial. It's a truth that the organization which embraces more protective measures find themselves ahead of the business world. Within their organizations themselves, SOCs can have a positive impact due to their focus and expertise. Those key benefits of having a security operations center are as follows:

- It centralizes the display of assets – A real-time, holistic view of the software and processes that help run an organization makes it easy to detect problems as they occur or sooner. Even with dispersed materials, the centralized, non-stop visualization SOC monitoring offers is highly advantageous in maintaining smooth operations.

- It helps in building and maintaining solidifying client and employee trust – Consumers and employees alike want to know their information will be safe once they offer it to their company of choice. Taking strict measures to prevent data loss is one of the best ways to improve and maintain brand integrity and trust in the long run.

- Enables collaborating across departments and functions – SOCs are unique, that they are a team of highly trained individuals working for a common goal. As they proceed during cybersecurity incidents, they require other departments to work similarly to operate efficiently. Within these instances, SOCs help with coordinating and communicating the organization as it strives to resolve the problem collectively.

- It maximizes awareness to minimize costs — Overall, the most significant benefit of a SOC is the increasing your ability to control all systems and reduce the potential for losses of data, contributing to higher returns on investment to prevent breaches. SOCs help maintain the integrity of sensitive information, save money in the long run and assist in avoiding the cost of significant recoveries from theft or fraud.

3. ORGANIZATIONAL SOC MODELS

Standard models of SOC model are described below. Organizations will deploy any one of these SOC models depending on various factors and work environment. These models range from internally centralized structures to those that run remotely.

- Internal SOC – These models are made up of IT and security professionals within an organization. These team members are either distributed throughout departments or centrally dedicated to cybersecurity monitoring. Overall, all security-related activities are taken care of within the organization.

- Internal virtual SOC – Without a dedicated facility, these teams are groups of part-time workers who primarily take reactive measures when they receive security alerts. This can be classified as an on-purpose hosted team, which support organization for security virtually as required.

- Co-managed SOC – A team of semi-dedicated individuals within the organization work together with a third-party managed security service provider to maintain security operations. This is an example of an inter-collaborated form of SOC.

- Command SOC – A bit removed from the action, these centers coordinate the efforts of a group of other SOCs, providing additional insights. This is an internal SOC, that provides necessary commands or instructions to the organization on dealing with other external SOCs, where major activities are taken care of. It acts as an interface between the organization and external centers.

- Outsourced virtual SOC – Like the internal virtual SOC mentioned above, these SOCs are remote. However, they are an independent third-party service, rather than coordinating with other in-house employees.

Building a SOC from the ground up, establishing the necessary roles and investing in the proper hardware can be a costly endeavor for businesses that have never intentionally tackled cybersecurity before. Many organizations are turning to service providers for reliable security outcomes, and there are a few different reasons why companies may forego in-house cybersecurity expertise for the outsourced model. Outsourced SOCs operate as a separate team, with less collaboration (w.r.t other models) with internal teams of the organization. Because these SOCs are external vendors who take care of the organization’s security goals and intellectual property. Then security will be featured as a paid service for the organization. There are several reasons for mentioning virtual SOC as the best option for many small to medium businesses. This includes avoiding the costly expenses of hiring skilled security engineers and analysts, funding advanced and adequately powered facilities and keeping up with continuing education costs as new threats and cyber tactics emerge. An external service provider enables you to have the benefits of a SOC without shouldering all the extra expenses. Cybersecurity is still a highly flourishing field in IT with a great need for efficient potential skills and assets.

Apart from these models, another method of implementing SOC in an organization is Virtual Security Operations Centers (V-SOCs). They are a secure, web-based tool that serves as your company’s command and control center for your systems. With a V-SOC, your business can entrust a qualified team of experts to monitor your security around-the-clock and in real-time, alerting the appropriate staff so that they can prioritize and respond to threats. While the design of virtual security operations centers varies by provider, they share an identical goal of monitoring your system and alerting you to vulnerabilities. V-SOCs generate easy-to-read reports as well, which can help your company assess its security stance. If your center detects a breach, you're notified and connected with a security expert.

4. ROLES IN A SOC

From team member responsibilities to SOC location and makeup, the variations in SOCs across business landscapes is substantial. There are many roles to play and business requirements to keep up. Starting from analyst position to SOC manager, these roles have defined rules and procedures to perform. Some elements can affect a SOC's appearance, dynamics, and capabilities, like financial budgets, the number of employees, access to continuing education and the scope of the team's influence across departmental lines. However, a few key member roles stand out as likely to be present within most SOC teams, including:

- Chief Information Security Officer (CISO) – As the title implies, are responsible for the strategy, goals, and objectives of an organization's security operations. They handle risk management and compliance, implementing policies and procedures that meet specific security requirements, and that enhance the organization's security posture. Additionally, they are leaders of the SOC team delegating and prioritizing tasks that meet an organization's objectives set out in their cybersecurity risk management program.

- SOC Manager – The SOC Manager is the person who manages the entire security operations team, reporting directly to the CISO. They are responsible for the successful completion of all tasks in project engagements, which includes technical work, staff supervision, financial activities, and the monitoring and analyzing of resources.

- Security Architect – They design and build a security infrastructure and network security for an organization. They are also responsible for maintaining the security, assessing vulnerabilities, and thinking like a hacker, to prevent a security incident or data breach from occurring. The best security architects are ones that have a greater understanding of how hackers gain unauthorized access into organizations, deploying the latest methods of attacks.

- Security Engineers – Security Engineers help facilitate and drive strategy in an organization's security, performing vulnerability assessments and penetration tests to determine the areas of weakness in security. They are building security systems from the ground up and are focused on potential vulnerabilities and exploits and creating solutions to prevent attacks from occurring.
- SOC Security Analysts – They identify issues and problems with a security system and then repairs and optimizes it for efficient use. Additionally, they are responsible for ensuring security measures are working effectively and that the proper training has been carried out at an organization for the implementation of policies and procedures.

5. BEST PRACTICES

Recent developments in information technologies and much concentration to digital world have led to some of the best SOC cybersecurity practices to consider. They include widening the scope of an organization's security. Not only are cloud-based systems expanding virtual infrastructures, but the growing trend of digitizing nearly every facet of everyday business operation leads to greater exposure. Organizations will need to adequately visualize new processes and communications and monitor them continually, requiring security professionals to be actively engaged in the planning of these procedures, maintaining compliance and detecting potential security incidents across ever-widening horizons.

As these business processes increase the number of events occurring across servers and networks, security teams will also need to collect relevant data. Increase in data intake has become a critical practice to measure whether adequate data is been collected to rank an incident as unusual or hostile and if it needs to be on the priority list. Another best practice identified is enforcing deeper analysis. Retrieving all the data is not enough without advanced capabilities of analyzing it. The right employees need to be readily available to weigh visible criteria with known vulnerabilities to create intelligent plans of action. As with many other areas of business, the introduction of automated processes has infiltrated the realm of cybersecurity. Primarily in tasks related to management or basic assessment, automation is growing in popularity, as it frees up human users to confront unknown threats with plenty of time and energy. This trending method of automating operations of SOC has become one of the best practices to enhance the efficiency of SOC.

6. BUILDING A SOC

Over the world, there are several organizations running their businesses with different operational methods. Every organization is different from one another on different perspectives. As the same way, security implementation in these companies is different. In some companies, the executive team recognizes the importance of cybersecurity to the business bottom line. In these cases, the SOC team is in a great position, with enough budget for good tools, enough staff to manage them, and the human capital of executive visibility and support. Unfortunately, that's not the reality in most cases. Most SOC teams are struggling with never enough staff, never enough time, and never enough visibility or certainty about what's going on. That's why it's essential to focus on technology and staffing while building a SOC in a company. First, we will be describing how to consider technology to frame the SOC. Afterward, we will focus on staffing human resources and detail on their tasks.

There are two important procedures to consider while defining technology for a SOC. The first is setting up your security monitoring tools to receive raw security-relevant data. This includes making sure we have deployed all relevant tools to collect enough data for threat monitoring. This step makes sure that the critical cloud and on-premises infrastructure are all sending their logs to your log management, log analytics, or SIEM tool. The second function is to use these tools to find suspicious or malicious activity by analyzing alerts; investigating indicators of compromise; reviewing and editing event correlation rules; performing triage on these alerts by determining their criticality and scope of impact; evaluating attribution and adversary details; sharing your findings with the threat intelligence community; etc.

Knowing the technology deployed for SOC will help to determine how to staff your team. We have already discussed on various roles security professionals play in a SOC team. For a well-defined SOC team of an organization, we can group up these roles into several tiers. Each tire of staffing consists of a set of roles who work on different technical aspects but focusing on a common goal of providing input to the next tier level. These tiers are

- Triage Specialists (Tier 1) – They review the latest alerts to determine relevancy and urgency, creates new trouble tickets for alerts that signal an incident and require Tier 2 / Incident Response review, runs vulnerability scans and reviews vulnerability assessment reports, and manages and configures security monitoring tools.

- Incident Responders (Tier 2) – Reviews trouble tickets generated by Tier 1, leverages emerging threat intelligence to identify affected systems and the scope of the attack, reviews and collects asset data (configs, running processes, etc.) on these systems for further investigation, and determines and directs remediation and recovery efforts.

- Threat Hunters (Tier 3) - Reviews asset discovery and vulnerability assessment data, explores ways to identify stealthy threats that may have found their way inside your network, without your detection, using the latest threat intelligence, conducts penetration tests on production systems to validate resiliency and identify areas of weakness to fix, and recommends how to optimize security monitoring tools based on threat hunting discoveries.

- Operations & Management (Tier 4) – They are responsible for supervising activities of the SOC team. They recruit, hires, trains, and assesses the staff. They also manage the escalation process and reviews incident reports, develops and executes a crisis communication plan to CISO and other stakeholders. They run compliance reports and supports the audit process, measures SOC performance metrics and communicates the value of security operations to business leaders.

Once the technology and staffing are modeled for a SOC, it is the time to observe and mark the key processes that they need to perform to detect emerging threats; determine their scope and impact and respond effectively and quickly. These are described in detail below.

1. Event Classification and Triage - The true value of collecting, correlating, and analyzing log data is that it gives the ability to find relevant data from a huge stack of log sources. This helps in figuring the key indicators of compromise from data sources including user activity, system events, firewall accept/deny, etc. The key to success in this stage is having a way to classify each event quickly so that you can prioritize and escalate critical events that require additional investigation. Tier 1 analysts are responsible for this activity. Once they've verified that these events require further investigation, they'll escalate the issue to a Tier 2. Another major task of these team members is to document every stage of an investigation, which serves the best reference in the future.

2. Prioritization and Analysis – This set of tasks plays a significant role in the functioning of a SOC team. Prioritization is the key to success in any endeavor. Focus on those events that could be most impactful to business operations, which requires knowing which assets are the most critical. At the end of the day, maintaining business continuity is the most important responsibility entrusted to the SOC team. The SOC team review and respond to any activity that indicates an adversary has infiltrated your environment. Asset discovery and inventory are one of the most important and yet most overlooked cybersecurity capabilities.

3. Remediation and Recovery - The faster you can detect and respond to an incident, the more likely you'll be able to contain the damage and prevent a similar attack from happening in the future. The

SOC team need to work closely with the management team. This collaborative helps to communicate clearly and often and to document everything. Remediation steps for each type of attacks differ from one another, but basically, it will involve steps to re-image systems, patch or update systems, re-configure system access, re-configure network access, review monitoring capabilities on servers and other assets, and to validate patching procedures and other security controls by running vulnerability scans. By the way, some SOC teams hand off remediation and recovery procedures to other groups within IT, by creating tickets or change control request and delegate it to those responsible for desktop and system operations.

4. Assessment and Audit – It is always good to find and fix vulnerabilities before an attacker exploits them to gain access to your environments. The best way to do that is to run periodic vulnerability assessments and review those reports. Running network vulnerability scans and generating compliance reports are some of the most common audit activities for SOC team members. Additionally, SOC team members may also review their SOC processes to determine how to improve performance and efficiency.

7. SOC TOOLS

Security professionals use the term "defense-in-depth" to describe how best to secure critical data and systems against cyber threats. Starting with the data you're protecting at the center, you add layer upon layer of policy enforcement to make it difficult for an attacker to break through each layer to access that data. This stays as an important concept on how cybersecurity industry grew out. The key point to emphasize here is the importance of detection. Organizations need to implement preventative tools along with ensuring that vulnerabilities are patched among other prevention-type activities. Attackers have evolved their capabilities, so organizations need a new approach. It includes combining the essential tools for building a SOC into a workflow, which includes asset discovery, vulnerability assessment, behavioral monitoring, intrusion detection, and SIEM.

- Asset Discovery tools – Knowing what assets are in your environment is the first step in knowing your security posture. It is important to know what all assets and infrastructures are placed in the organization as well as what operations and software are running on those systems. Good and reliable asset inventory tools serve these functions for a SOC team. Highly smart tools should be having the automated ability to discover new assets serves a foundational layer toolset for SOC. Few examples for this category of tools are Spiceworks, OCS Inventory NG, OpenNSM, etc.

- Vulnerability Assessment – Vulnerabilities represent the attack surface that an attacker uses to infiltrate your critical systems. These open when you least expect it and stays unnoticed. That’s why it’s essential to continually assess your entire IT landscape for vulnerabilities. Additionally, you may be subject to a variety of contractual and regulatory mandates that require periodic vulnerability assessments to demonstrate compliance. Some of the vulnerability assessment tools are Metasploit, Nmap, Nessus, Wireshark etc.

- Behavioral Monitoring – At its most basic, effective cybersecurity monitoring comes down to exception management. These toolsets mainly focus on situations when something goes out of normal condition and deals with the handle it. This involves creating a baseline of system and network behavior that provides the essential foundation with which to spot anomalies. This helps in monitoring abnormal behavior when cyber-attack happens. To capture a baseline, it’s critical to combine behavioral monitoring technologies and applying correlation rules against resultant data. This will help you identify and classify the latest risks, as well as support threat and attack investigations.

- Intrusion Detection – Detecting an intruder at the point of entry can have the greatest impact on reducing system compromise and data leakage. With this, intrusion detection systems became important tools that should be deployed in an organization’s network and hosts. On-premises, IDS operate based on correlation rules that detect known patterns of suspicious activity using unique intrusion signatures. If the organization uses cloud infrastructure, then they need access to the management plane for a cloud provider. An essential step is to keep correlation rules up to date with the latest threat intelligence updates, to make IDS able to detect emerging threats. Examples include Snort, Suricata, etc.

- Security Information and Event Management (SIEM) – This toolset handles an important procedure of collecting evidence against cyber-attacks and intrusions from various sources of data logs and anomaly reports. Security Information and Event Management (SIEM) tools were developed on the assumption that by looking for certain patterns of activity and sequences of events, you can detect a cyber-attack as well as validate and demonstrate regulatory compliance. This tool filters whole data collected and prepares an abstract on attack and reports threat details to respective people.

8. CONCLUSION

The Security Operations Center has a significant role in an organization’s security context. We have described the necessity of implementing a SOC to organizations or companies that stay connected to the open network and have huge sets of assets and sensitive information. Facing the cyber attacks and then working to clear its consequences stays a bad idea for these companies as the cost of managing aftereffects will not stay bounded with respect to money to spend, and affects productivity and reputation, view on the organization’s work culture and trust from clients. The SOC is a super flexible team for the organization with respect to deployment, and a smart team to handles all threat activities that will pose a hardship on the organization and provide an extreme layer of protection. As the network grows and become more complex, SOC is becoming a front line of defense. There are challenges in building a good security operations center. Building this risk reducing asset that strengthen the security is not easy as simply hiring new team members. Field of cybersecurity has been facing a significant skill gap. There aren’t enough people skilled with great knowledge and experience on wide variety of security toolsets. This brings a big challenge to the cybersecurity industry. Recent research indicates that many employed professionals are overworked, and they are not able to manage their career proactively. They don’t even receive proper amount of training as the cyber threats are increasing day by day. As availability of professionals matters much on leading a security operations center, it’s a great idea to hire people who are willing to engage in continuous learning. Ongoing certifications and trainings help organizations to keep SOC up-to-speed. Experience shows that a pragmatic approach needs to be taken to implement a professional SOC that can provide reliable results. The theory described above forms the framework for deploying such a SOC.

REFERANCES

1. *Incident Reporting Guidelines – CERT Coordination Center – Carnegie Mellon University*
2. *Security Operation Center Concepts & Implementation – Renaud Biduo*
3. *How to build a Security Operations Center – https://digitalguardian.com/blog/how-build-security-operations-center-soc-peoples-processes-and-technologies - DATAINSIDER Digital Guardian's Blog*
4. *Recent Advances in Intrusion Detection - W. Lee (Editor), L. Me (Editor), A. Wespi (Editor) - ISBN: 3-5404-2702-3*
5. *Security operations center - https://en.wikipedia.org/wiki/Security_operations_center*
6. *Reasons why you need security operations center soc – https://www.lewan.com/blog/5-reasons-you-need-a-security-operations-center-soc - Lewan Technology Blog*
7. *Security Operations Center (SOC) – https://www.rapid7.com/fundamentals/security-operations-center/*
8. *Building a Security Operation Center – https://www.sans.org/cyber-security-summit_/archives_/file/summit-archive-1493840439.pdf*
9. *The SOC Team - https://www.cybrary.it/channelcontent/chapter-1-the-soc-team-roles-and responsibilities/*
10. *Best practices for designing SOC – https://securityintelligence.com/best-practices-for-designing-a-security-operations-center/*
11. *Security Operations Center – https://www.quora.com/topic/Security-Operations-Center*