DOI: https://doi.org/10.31410/ITEMA.2022.91

Information Security – SOC Potentialities

Pedro Vieira[1]
Leonilde Reis[2]

Received: November 15, 2022
Accepted: January 16, 2023
Published: June 12, 2023

Keywords:
Information;
Information security;
Cybersecurity;
Security Operations Center;
Security information;
Event management

Abstract: *Nowadays, information is an essential resource and a valuable asset. Like any other asset, information is potentially vulnerable and subject to various threats, whether deliberate or accidental. The methodology adopted for the study was exploratory and descriptive, focusing on document analysis of information in the field of the theme. The paper aims to focus on the operationalisation and management of the Security Operations Center (SOC), to foster and optimise the definition of policies and instruments for data loss prevention and recovery, as well as to carry out training actions for employees. The main results emphasise that cybersecurity involves a set of tools, policies, guides, risk management approaches, training actions, good practices and technologies that can be used to protect the assets of organisations and users in cyberspace, to preserve the guarantee the so-called information security triad.*

1. INTRODUCTION

The defence of the security perimeter of organisations is considered and the way they approach cybersecurity internally has gained increasing importance with changes in work regimes caused by the COVID-19 pandemic and the existence and perception of increasing volumes of cyberattacks, some of them triggered against large companies and public entities (Vieira, 2022). In this sense, it is considered urgent to outline strategies for access control and network and infrastructure protection. It is also considered that intrusion tests, as well as vulnerability and threat management, may contribute to optimising the organisation's security levels.

GARTNER report explains that Cyber Risk Management (ISO/IEC 27005, 2018) involves the design and deploy a cyber-risk management program aligned with business needs by using fit-for-purpose methodologies, technology choices and organisational structures (Gartner, 2022). Also to the National Institute of Standards and Technology (NIST), Risk Management is the ongoing process of assessing the risk to IT resources and information, as part of a risk-based approach used to determine adequate security for a system, by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk (NIST, 2022).

2. SECURITY OPERATIONS CENTER

In today's increasingly connected world, where organisations are constantly collecting and storing more data than ever before, having a robust and effective Security Operation Center (SOC) cannot be underestimated. With the right tools and personnel in place, the SOC can help to protect an organisation's most valuable assets and ensure that its data and systems are safe from harm.

[1] Instituto Politécnico de Setúbal, Setúbal - Portugal
[2] Instituto Politécnico de Setúbal, Setúbal - Portugal

It should be noted that the SOC, as a service essentially aimed at risk management, includes the skills underlying the triad people, processes, and technologies responsible for monitoring, analysing and maintaining an organisation's information security, providing the necessary basis for it to protect its most sensitive assets, detecting and responding more quickly to threats.

The SOC is a centralized facility that serves as an intelligence hub for the organisation, gathering data in real-time from across the organisation's networks and other digital assets and using intelligent automation to identify, prioritize and respond to potential cybersecurity threats. When a cyberattack occurs, the SOC acts as the digital front line, responding to the security incident with force while also minimizing the impact on business operations.

It is considered that in an organisational context, SOC's main activities and responsibilities include (Rotich, 2022):

- Asset inventorying to allow better identification of all assets that should be protected (e.g. servers, databases, computing devices, endpoints, etc.) and all tools that are used to protect these assets, such as firewalls or antivirus software;
- Continuous monitoring of the network to detect any nonconformities and to provide a complete overview of the activity. A SOC monitors 24/7/365 the entire IT infrastructure looking for suspicious events;
- Searching proactively for suspicious behaviour and tests and assessing network security to detect advanced threats and identify areas of vulnerability or insufficiently protected assets. The SOC team performs vulnerability assessments and penetration tests that simulate specific attacks. Based on the results of these tests, the team adopts best practices, adjusts software and security policies and draws up better incident response plans;
- Constant monitoring of all used security resources, such as firewalls, IPs, antivirus, anti-DDoS and others to cross data about events, providing a Security Information and Event Management (SIEM) solution that detects almost instantly intrusion attempts;
- Prevention techniques to deter and deflect a range of known and unknown risks;
- Threat intelligence capabilities to assess the source and impact of cybersecurity incidents and identify areas of vulnerability or insufficiently protected assets;
- Development of the organization's incident response plan, establishing roles, tasks, activities and responsibilities in the event of an incident and defining the metrics by which the degree of success of the response will be evaluated. The SOC may also collaborate in designing backup procedures to ensure business continuity if a data breach event occurs;
- Using a combination of automated technologies and human intervention, the SOC provides a decisive response to address a security incident as quickly as possible. These kinds of actions often include an investigation to determine the causes of the vulnerabilities that allowed the hackers to access the systems, the disconnection of the network of compromised terminals, the pause or interruption of compromised processes, the redirection of network traffic, the application of antivirus software, the delete of infected files or the disable of passwords;
- Reporting to ensure all incidents and threats are fed into the data repository, making it more precise and responsive in the future. Reporting also is used, after an incident, the SOC ensures that incident data is kept ensuring evidence and future auditing and that customers, regulators, users, law enforcement, and other related entities are notified as required by applicable regulations;
- Developing compliance mechanisms to ensure reliability and compliance with internal and external rules and regulations. A SOC must ensure that all security systems, tools and

processes are compliant with the General Data Protection Regulation (GDPR) and other data privacy regulations. After an incident occurs, the SOC must be in a position to ensure that law enforcement, regulators, users, clients and other parties will be notified under the law and regulations and that the necessary data from the incident is retained for evidence and future audit processes.

Figure 1 shows a *representation of the main operations developed by a SOC.*

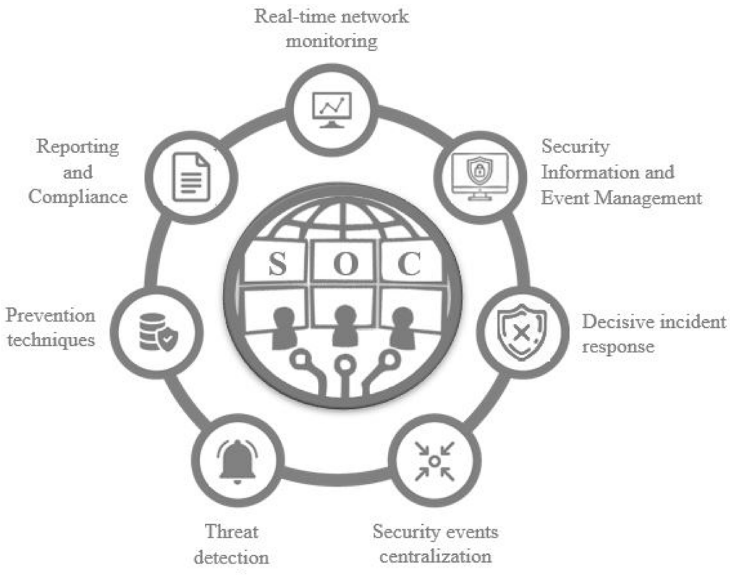

Figure 1. Security Operations Center
Source: Vieira, 2022 adapted from Softwall

As shown in Figure 1, a SOC brings together skilled people, processes, and technologies to continuously carry out different types of activities for the identification, monitoring, prevention, detection, treatment, response, and mitigation of cyber incidents of diverse types and origins.

A SOC team should include employees who have a professional skill set in information security and cybersecurity. The number of team members depends on the type of business, but usually, a SOC team includes security analysts, malware analysts, and cryptography and forensic specialists.

There are several reasons and benefits to the existence of a SOC in an organisation (Rotich, 2022):

1. **Centralized command:** A SOC is a unified command centre that aggregates data across the organisation's IT infrastructure, spanning network devices, computers, and cloud applications. SOCs can help organisations to adopt a comprehensive approach to managing and monitoring cybersecurity risks and to ensure that all major security incidents, such as data breaches, are handled effectively.
2. **Log management and analysis:** The cybersecurity teams must keep networks safe from cyberattacks. Log management and analysis is a fundamental function of the SOC as it helps to identify trends and anomalies that could indicate a security breach, allowing it to take appropriate steps to mitigate them. By focusing the analysis and management of log data across the entire network, the SOC team looks at logs and establishes normal or baseline activity and uncovers anomalies that might provide hints about possible intrusions as well as examining how quickly systems respond when something does go wrong. Many

hackers know that organisations often fail in analysing log data, which can allow viruses and malware to run and be undetected by victims of the attacks for some time.

3. **Compliance requirements:** A SOC helps organisations meet and comply with compliance with industry, national and global privacy regulations by providing an audit trail of all activities related to the security of data and systems. Storage retention policies are also managed by the SOC, ensuring that relevant logs and other data are kept appropriately based on regulatory or business requirements, strengthening the organisation's compliance.
4. **Minimize costs:** While many organisations think that implementing a SOC comes at a very high cost, the costs associated with a data breach - including reputational damages, data theft, corrupted data, or lost customers – is much greater. A SOC also helps mitigate the financial consequences of a cyberattack, as SOCs reduce dwell time, resulting in reduced financial costs when an attack happens. Additionally, partnering with a SOC reduces the significant financial costs of hiring and retaining an in-house team of cybersecurity experts and managing the cybersecurity tools needed to power a SOC.
5. **Threat prevention:** A SOC monitors the organisation's entire environment and configures rules and actions in a preventive way so that threats, virtual attacks and security incidents are dealt with or blocked, preventing them from spreading and protecting critical business data from being compromised or stolen. In addition, a SOC, by providing details of suspicious activity occurring on the network, is also improving network visibility. The SOC also can isolate and contain the threat until it can be fixed or removed. Today's modern SOC can isolate and contain the threat until the remedy is applied.
6. **Communication and collaboration:** The close collaboration between all SOC team members allows organisations to enact their cybersecurity practices much more efficiently. For example, many SOCs are operating 24 hours a day, 7 days a week, allowing for the real-time detection of incidents and continuous monitoring to provide immediate responses.
7. **Faster and effective response:** SOC provides a centralized, complete and real-time view of the performance of the entire infrastructure from a security perspective, detecting and mitigating threats in real time to detect, identify, prevent and resolve problems before they can cause many problems. SOC reduces dwell time, which is the amount of time an attacker is not detected on the network after initial access. Each minute that an attacker remains within the network, the greater the potential for damage. SOCs reduce dwell time from months to minutes, reducing the financial impact when an intrusion occurs.
8. **Continuous protection:** Continuous monitoring is vital to detecting the earliest indications of abnormal behaviour. Adversaries don't work 9-5, nor do they adhere to a traditional Monday-Friday work week. Businesses are under assault 24/7. SOC doesn't stop when all the organisation's employees are asleep, but rather proactively monitors for threat indicators, even throughout holidays and weekends. So, whether in-house, hired, or virtual, SOC team members are on hand to check for potential vulnerabilities and to detect attacks 24 hours a day.
9. **Remote worker protection:** With the increase in employees working remotely from home due to the COVID-19 pandemic, a new set of risks and threats has emerged, leading to the need to put in place robust monitoring controls to counteract these threats. By providing remote cover for these home workers, a SOC helps to reduce eventual cyber risks.
10. **Forensic investigation facilitation:** SOC is responsible for performing forensic investigation during and after an attack to help understand what happened, where it happened, to what systems and machines, and any digital footprint left by intruders, enabling analysts to investigate security incidents more quickly and comprehensively.

These benefits of a SOC are condensed in Figure 2 in five major points.

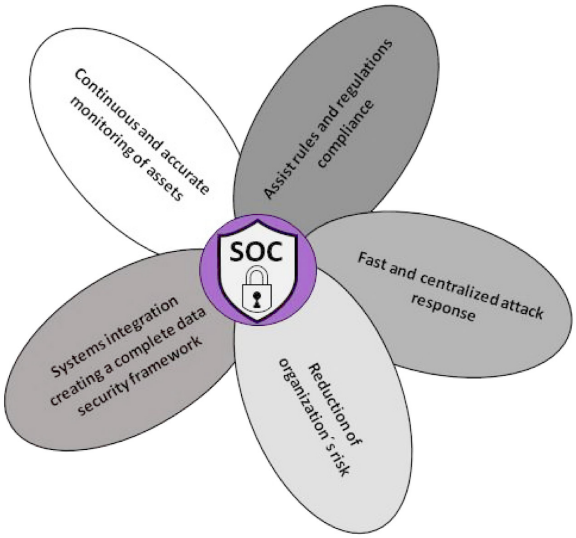

Figure 2. Benefits of a SOC
Source: Vieira, 2022 adapted from Shieldbyte Infosec

As shown in figure 2, a SOC helps to keep sensitive data and systems safe and makes it easier to respond quickly and effectively to any incidents, so by deploying a SOC, organisations can take a proactive approach to cybersecurity instead of waiting for an attack to happen.

3. SECURITY INFORMATION AND EVENT MANAGEMENT

Keeping criminals off networks and protecting data is the essential job of a SOC team. To do so, a SOC team needs a SIEM with the appropriate tools to be able to detect and contain threats, so, SIEM provides organisations with visibility into the activity on their networks so they can detect early and respond quickly to potential cyberattacks and meet compliance requirements.

SIEM is the tool typically used to monitor IT security events, which is a system that aggregates data from various sources, normalizes it, enriches it and sends it to a centralized management console, later used by the SOC team. SIEM is a set of tools and services that combine Security Information Management (SIM), which focuses on collecting and managing logs and other security data, and Security Event Management (SEM), which involves real-time analysis and reporting. SIEM correlates and aggregates event data generated by applications, security devices, data centres, cloud resources and other systems in an organisation's IT ecosystem.

According to Mezmo (2022), "from a user perspective, SIEM is a centralised security information dashboard used to display alerts and suspicious network activity". So, SIEM tools are used within a SOC and use predetermined rules to help security teams analyse network traffic and events, define threats and generate alerts. A SIEM solution helps to demonstrate a pattern of anomalous behaviour by flagging it as a real concern for security analysts to investigate. For example, antivirus software may fail in detecting a recent and as yet unknown type of malware, but a SIEM system, by analysing the bandwidth that machines are using, can generate an event warning if one of them is consuming more resources than it should and alert SOC analysts to look further into the problem.

In the last decade, SIEM technology has evolved to make threat detection and incident response faster and smarter with Artificial Intelligence (AI). Effectively, some SIEM platforms integrate

AI that automates processes and 'learns' from data to improve the detection of suspicious activity. Automatically, these platforms network traffic, prevent access pre-emptively and generate alerts to security analysts to investigate the event even further. In fact, according to Mezmo (2022), "too many false positives from a SIEM create a phenomenon called analyst fatigue or analyst burnout and leaves analysts apathetic to alerts." For this reason, a SIEM solution helps to demonstrate a pattern of anomalous behaviour, flagging it as a real concern for security analysts to investigate and quickly determine the correct steps and procedures that should be followed.

In conclusion, a SIEM's operation allies the log analysis with a comprehensive network security strategy by using a combination of advanced technologies and human resources to detect, contain, respond and remediate a variety of cyber threats. Through mechanisms for monitoring the network and user behaviour, limiting access attempts, monitoring and responding to incidents, SIEM performs log management, automation and correlation of events and uses human experts to respond to potential cyberattacks and mitigate and remediate their consequences.

4. FUTURE RESEARCH DIRECTIONS

Ensuring security levels in an organisational context according to the outlined strategies is an increasing challenge. In this sense, it is considered urgent to explore in detail the circumstances surrounding the definition of alerts through SIEM tools. It is also considered that it will be urgent to establish a set of security metrics to improve the daily operations of the SOC, by strengthening the SIEM system used to monitor and alert security events, improving its alarming capabilities.

5. CONCLUSION

It is advocated that to ensure the security of application systems and infrastructures, the SOC permanently monitors the network and security resources used, detects threats, identifies vulnerabilities and reacts to incidents. Good information security practices should also be a major concern for organisations (ISO/IEC 27002:2022, 2022). On the other hand, once the SOC is certified, it carries out security audits within the scope of ISO 27001:2018 Standard and carries out intrusion exercises for the organisation's network and systems to analyse attack vectors and validate whether there is the monitoring of these vectors, as well as verifying that the SOC's processes are properly implemented to react based on alerts.

It is thus concluded that the SOC is not "just" a blocker but is essentially a service that aims at risk management, demonstrating the existing risk, in the sense of placing the control systems of the most technologically intelligent equipment available in the search for security solutions that can do correlation and alerts in real-time.

Coordinating and unifying an organization's security tools, as well as security incident response and processes, was one of the key benefits of operating or outsourcing a SOC. This centralization usually allows for more timely and rapid detection of threats and a more agile, effective and efficient response. In addition, the existence of a SOC contributes to strengthening the organization's degree of compliance with applicable privacy regulations.

In the current context, teams responsible for ensuring cybersecurity need to monitor many devices, users, applications and, consequently, cybersecurity events related to these elements. The

most used platform to monitor cybersecurity events is the so-called SIEM, which is a system that aggregates all the security information from different sources, standardizing it, enriching it and sending it to a centralized management console. A SIEM, therefore, combines SIM security information management, which focuses on collecting and managing logs and other security data, and SEM which involves real-time analysis and reporting.

References

Gartner. (2022). *Why Cyber Security Starts with ITAM Data - IT Discovery: A Critical First Step in IT Security*. https://content.lansweeper.com/Operational-IT-Security

ISO/IEC 27001:2018. (2018). *Information security management systems - Requirements*, 2018. www.iso.org/isoiec-27001-information-security.html

ISO/IEC 27002:2022. (2022). *Information security, cybersecurity and privacy protection — Information security controls*. https://www.iso.org/standard/75652.html

ISO/IEC 27005:2018. (2018). *Information technology — Security techniques — Information security risk management*. https://www.iso.org/standard/75281.html

Mezmo. (2022). *What is the difference between-SIEM and-SOC*. https://www.mezmo.com/learn-observability/what-is-the-difference-between-siem-and-soc

NIST. (2022). *Information Technology- Cybersecurity*. National Institute of Standards and Technology: https://www.nist.gov/cybersecurity

Rotich, A. (2022). *Security Operation Center (SOC)*. https://medium.com/@thefoursec/security-operation-center-soc-22ac281c6eaa

Shieldbyte Infosec. (2022). *SOC1, SOC2 & SOC3 Compliance*.
https://shieldbyteinfosec.com/SOC1-SOC2-SOC3-compliance.php

Softwall. (2022). *SOC. Security Operations Center.*
https://www.softwall.com.br/solucoes/soc-security-operations-center/

Vieira, P. (2022). *Security & IT Risk*. Bachelor's degree internship report, Instituto Politécnico de Setúbal.