6th International Scientific Conference ITEMA 2022 – Proceedings
DOI: https://doi.org/10.31410/ITEMA.2022.99

Cybersecurity – Security Operations Center

Pedro Falé[1]
Leonilde Reis[2]
Rui Almeida[3]

Received: November 6, 2022
Accepted: January 12, 2023
Published: June 12, 2023

Keywords:
Cybersecurity;
SOC;
Cybersecurity threats;
Incident response;
Incident control

Abstract: *Currently, most organizations are dependent on Information and Communication Technologies, in the sense of accomplishing their underlying business activities. In this scope, cybersecurity is considered the domain that has the strength to protect sensitive information, be it at the individual level or in an organizational context. The objective of this paper is to introduce the concept, relevance, and functions of a Security Operations Centre. The methodology underlying the study was based on the use of the MITRE Adversarial Tactics, Techniques and Common Knowledge framework as a matrix of tactics and techniques based on real scenario observations. The main results emphasize the importance of incorporating the Security Operations Center as a barrier against cybersecurity threats. Security Operations Center brings additional value to the organizational context, through people, processes and technologies while also using several frameworks to improve work management, incident response and incident control.*

1. INTRODUCTION

Information security is the process that protects information and assets (Falé, 2022). It is considered that (Russo & Reis, 2020) the analysis of risks and vulnerabilities are fundamental in an organizational context as well as the procedures underlying business continuity.

In this regard, the three pillars of cybersecurity with a first known reference dates back to 1977, to a paper entitled Audit and evaluation of computer security by the U.S. Department of Commerce. This model has no author, but even now it focuses (Microsoft, 2022) on Confidentiality - Keeping data secret and ensuring that only authorized people can access your files and accounts; Integrity - Ensuring that information remains intact without data being inserted, modified, or deleted without proper permission; Access/Availability - Ensuring access to information and systems when it is needed.

However, the three pillars previously mentioned characterize only the minimum, the elementary ones; The pillar of Authenticity, linked to basic access mechanisms such as logins, passwords, and tokens, and the pillar of Irretrievability, linked to the authorship of the information provided using digital certificates and digital signatures, should also be included.

SOC potentiates the cybersecurity posture of an organization. It serves as a barrier against cyberattacks and therefore ensures the proper functioning of an organization. SOC must be aligned with the use of ISO/IEC27002:2013, which incorporates a set of good practices and controls that help in information security management (ISO/IEC 27002:2013, 2013). It uses the MITRE ATT&CK framework as a matrix of tactics and techniques based on real scenario observations and NIST as an incident response framework.

[1] Instituto Politécnico de Setúbal, Setúbal - Portugal
[2] Instituto Politécnico de Setúbal, Setúbal - Portugal
[3] Cybersafe Lda, Alfragide-Portugal

In this sequence of concerns regarding the current good practices emanating from international standards, it is considered that the analysis of the threats and vulnerabilities underlying each organization is of particular interest. Thus, identity theft, extortion, and data loss, among others, should be covered. In this sense, outlining a cybersecurity strategy should be a justified concern by organizations to define the layers of defense corresponding to the various levels necessary for the functioning of the organization. The use of the National Institute of Standards and Technology (NIST) reference framework for the different phases associated with a Cybersecurity Incident Response Cycle can be added value given the specificity of the issue.

According to the report prepared by the National Center for Cybersecurity (CNCS, 2022), which describes that "The dominant cyber threats in Portugal during 2021 were phishing/smishing/vishing, ransomware, online fraud/burglary and account compromise". Phishing/smishing (40% of incidents), social engineering (14%) and malware distribution (13%) were the types of incidents most recorded by CERT.PT in 2021. Thus, analysis, monitoring, and control are considered urgent because of the possible implications in the event of an incident.

2. SECURITY OPERATION CENTER

The Security Operation Center (SOC) is an organizational unit. According to Splunk (2022), the SOC promotes the existence of a centralized function within an organization, involving people, processes, and technology to perform continuous monitoring and improve the organizational posture of security. It aims to predict, detect, analyze, and respond to cybersecurity incidents. That is, the SOC not only identifies threats, but it must also analyze, investigate, respond, report vulnerabilities and plan how to prevent such occurrences from happening again in the future.

The SOC responds to cybersecurity incidents in real-time and in duality seeks to improve the cybersecurity posture of the organization. As a function that focuses on preventing and mitigating cybersecurity risks, the sectors in which it operates are homogeneous. It can play a role in financial markets, industry, government, energy, etc. Most SOCs, adopt a hierarchical approach to incident management, where analysts and engineers are categorized based on experience and skills.

In general, the SOC response to an incident is divided into lines. It has a SOC Manager (L4), Engineers, and incident responders such as level one, level two, and level three SOC analysts (L1, L2, L3). The SOC reports to the CISO, and the CISO to the CIO or CEO. Figure 1 presents the general flow of an incident response, delimited by each analyst level.

So, figure 1 shows a general workflow for responding to a cybersecurity incident, a function performed by the SOC. As the figure indicates, the tasks of the SOC are subdivided by lines, its purpose being to escalate incidents according to the specificity and skills required for its resolution. This workflow is intended to be general and can be adapted to the reality of each organization.

The L1 analyst starts in the triage phase, identifying the incident. If the incident has the profile of an existing playbook, the L1 analyst will proceed to resolve it. If the existence of the playbook is not confirmed, the L1 should escalate the incident to the L2. L2 core functions revolve around investigation, more robust threat and vulnerability knowledge, incident mitigation/containment, and finally documentation, creating playbooks and runbooks. L2 should escalate to L3 when deep, complex analysis is required, determining the origin of threats, whether they pose a threat to the organization and how to stop them. This activity is called Threat Hunting.

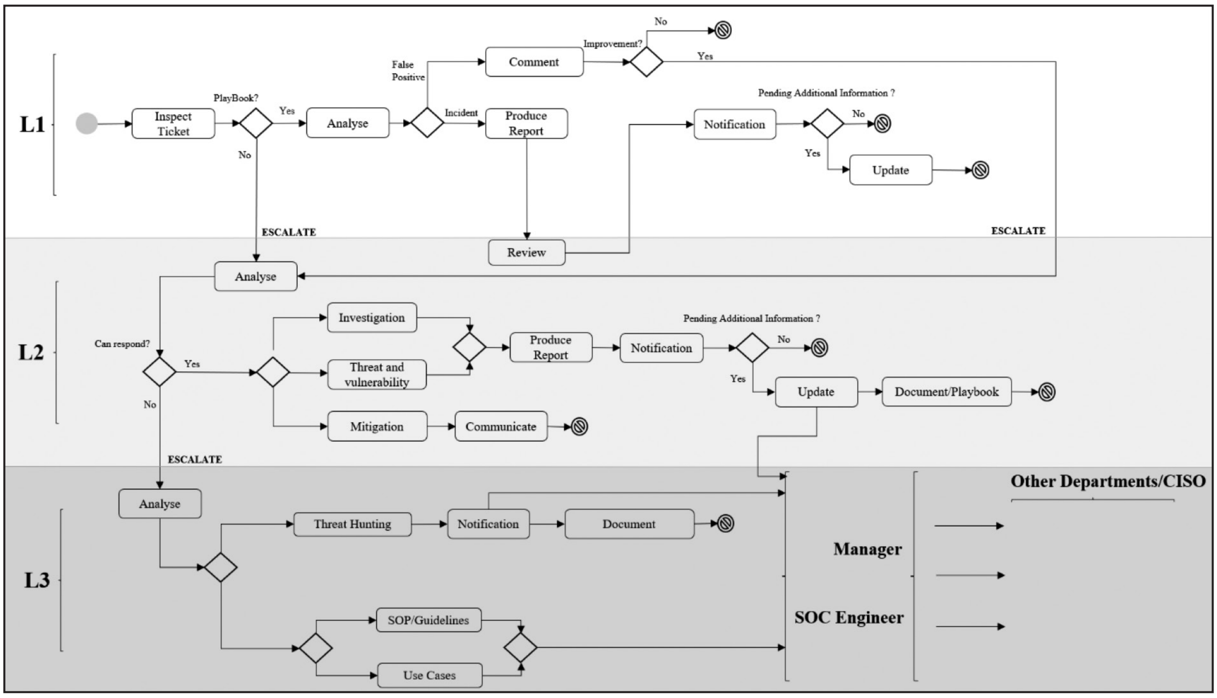

Figure 1. SOC incident response workflow

Source: Falé, 2022.

The SOC engineer has the responsibility of designing managing and maintaining the SOC infrastructure and network. They must work closely with the SOC manager whose function is to manage the day-to-day operations of the SOC team, and the SOC analyst to ensure everything works as intended.

The resolution of the various incidents is embodied in tickets. Tickets contain fields that can be adjusted to classify and categorize them, before their final resolved status. This flexibility allows tickets to be searched and filtered by each specific field. The status of the ticket varies depending on its resolution phase. Figure 2 is designed to show the different states of a ticket.

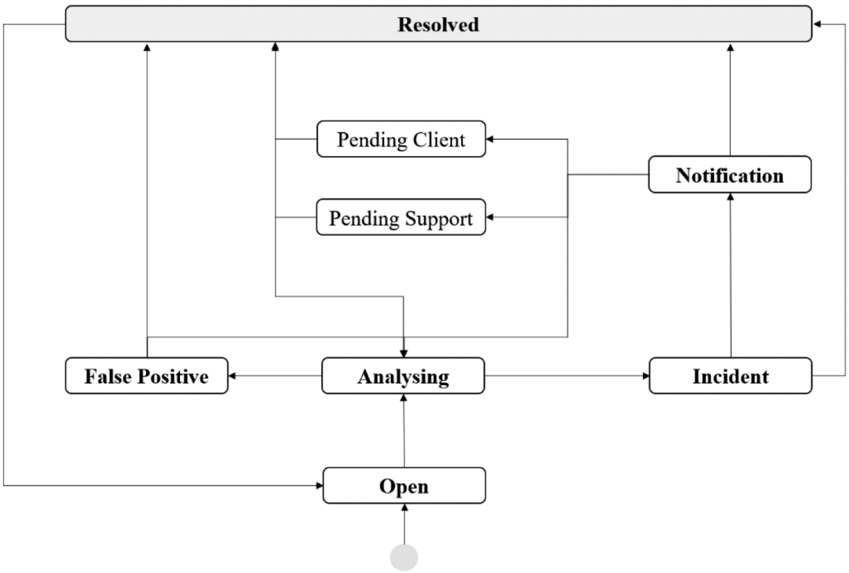

Figure 2. SOC ticket status workflow

Source: Falé, 2022.

We highlight the importance of the ticket management presented in Figure 2 given the criticality of the information handled, and given the specificity of each resolution phase. Figure 2 intends to establish a general workflow of a ticket state. The different ticket core phases derive from two main states: false positive or incident. These two states originate after the ticket starts in the analysis state. The end point of the ticket goes through the internal or external notification state and the resolved state. The workflow also has great flexibility that allows the reiteration of previous phases.

It is considered that a cybersecurity strategy must have layers of defense corresponding to the various levels required for the operation and specificity of the organization. As such, the SOC provides added value to an organization by acting as an external and internal barrier, an extra all-around layer of protection, following the zero-trust policy. Continuous monitoring ensures that threats are detected and resolved in real-time, more efficiently protecting the business, and minimizing the costs and losses of a data breach. Any large enterprise subject to compliance with privacy regulations should consider having a SOC.

From the customer's point of view, the SOC can be not only a protection tool but also an analysis and support tool to define strategies. The SOC through its research and documentation provides visibility to the trends of cyber-attacks and vulnerabilities in systems. Therefore, it contributes to the overall observability of the organization, allowing leadership to make informed decisions, considering cybersecurity. Currently more than ever in organizations, cybersecurity has a guaranteed place in the strategic decision-making of companies/organizations. The cybersecurity strategy must always be aligned with the business strategy and consequently the SOC also.

3. FUTURE RESEARCH DIRECTIONS

It is considered that in the current context, the SOC analyst must keep up to date with the latest trends, news and adversaries' tactics, techniques and procedures. One of the critical success factors of providing a good SOC service is emphasizing the added value in your team, the ability to adapt, and respond with regards to trend analysis, the latest developments and cybersecurity threats to the specificity of the business.

The SOC can add value in terms of monitoring and responding to a diverse set of cybersecurity incidents. We emphasize the importance of the existence of a continuous improvement perspective, to optimize the SOC, either by updating detection and prevention rules, establishing procedures and protocols, or adjusting measures and expectations with customers.

4. CONCLUSION

The area of cybersecurity is in an emerging position, with exponential growth (Cisco, 2022). This is not surprising, considering that the transition to digital, requires this information to be kept secure. Increasingly, organizations are taking the cost related to cybersecurity as essential. According to Morgan (2021) the "U.S. Bureau of Labor Statistics projects" identifies that the information security analyst position will be the 10th fastest growing occupation in employment growth, with a growth percentage of 31%, with the average growth rate of all occupations being 4%. In the cybersecurity field, over the past 8 years, the number of unfilled job openings has grown by 350%.

According to (IBM, 2022), and in summary form, the countermeasures must ensure the following topics: Critical infrastructure security - Protection of systems, networks and other assets;

Network security - Cable and Wi-Fi; application security - Use of data, authentication, permissions and other; Cloud security - confidential computing, encryption of data stored, in transfer and during processing; Information security - Data protection measures and compliance with standards and regulations such as RGPD; User education - Awareness and training of the organization's employees in order to strengthen end-point security; Continuity planning and disaster recovery - Tools and procedures for response and unplanned events; Storage security - Encryption, isolated data copies; Mobile security - Security of apps, mail, etc.

In Portugal, it is possible to identify that partnerships and cooperation between entities on the subject of cybersecurity have recently corroborated and strengthened the national space. However, with the ending of the National Strategic Plan for Cyberspace Security (ENSC) in 2023 and given the recent developments such as the pandemic, telework and division between East and West, the ENSC should be strengthened in its greater esteem post-2023.

Another relevant problem in this context is to link this set of concerns to the domains of sustainability given the context of innovation often underlying the issue under study (Reis, et al., 2021).

SOC is a centralized function inside of an organization, involving people, processes, and technology to continuously and better monitor the organizational security posture. It aims to prevent, detect, analyze, and respond to cybersecurity incidents. We also highlight the importance of all cybersecurity solutions. These solutions are necessary for the protection of information, which in turn protects the organization altogether, meaning its people, clients, processes, products and services.

References

Cisco (2022). *What Is Cybersecurity?* https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

CNCS (2022). *CERT.PT: Centro Nacional de Cibersegurança Portugal.* CERT.PT: https://www.cncs.gov.pt/pt/certpt/

Falé, P. (2022). *Cybersecurity - Security Operations Center.* Relatório de estágio de licenciatura, Instituto Politécnico de Setúbal.

IBM (2022). *What is cybersecurity?* https://www.ibm.com/topics/cybersecurity

ISO/IEC 27002:2013 (2013). *Information Technology – Security techniques – Code of practice for information security controls.*

Microsoft. (2022). *O que é a cibersegurança?* https://support.microsoft.com/pt-pt/topic/o-que-%C3%A9-a-ciberseguran%C3%A7a-8b6e-fd59-41ff-4743-87c8-0850a352a390

Morgan, S. (2021). *Cybersecurity Jobs Report: 3.5 Million Openings In 2025* https://cybersecurityventures.com/jobs/

Reis, L., Cagica Carvalho, L., Silveira, C., Marques, A., & Russo, N. (2021). *Inovação e Sustentabilidade em TIC.* Silabo.

Russo, N., & Reis, L. (2020). *Certificação de Programas de Faturação - Guia para a Continuidade de Negócio.* FCA.

Splunk. (2022). *What Is a Security Operations Center (SOC)?* https://www.splunk.com/en_us/data-insider/what-is-a-security-operations-center.html