Infrastructural Challenges and Good Practices in a Security Operation Center

Dimitri Alexandre da Silva
DETI/IEETA, LASI, University of Aveiro, Portugal

José Luís Costa
DETI/IEETA, LASI, University of Aveiro, Portugal

João Rafael Almeida
DETI/IEETA, LASI, University of Aveiro, Portugal

Abstract

Organizations are facing some challenges in cybersecurity, due to the increasing of cyber threats, vulnerabilities, insufficient cybersecurity frameworks, and scarcity of proficient cybersecurity experts. The criticality of mitigating these challenges is underscored by the European Union's Network and Information Systems (NIS) Directive. This directive is instrumental in fostering a uniformly high level of cybersecurity throughout the EU, mandating that Member States implement robust national cybersecurity strategies and collaborate effectively in responding to cyber incidents. A possible solution is the implementation of a Security Operations Center (SOC). However, SOCs are not a one-size-fits-all solution and each organization has specific needs depending on their business domain. This task can be complex, and it can be simplified when organizations can identify in the initial stages the infrastructural challenges that may emerge when implementing a SOC. In this paper, we analyzed the main considerations that should be considered when using current frameworks reviewed in the literature. We identified the core operating models that are currently in use and being deployed, and which are the best practices when designing a SOC's infrastructure.

2012 ACM Subject Classification Security and privacy → Operating systems security; Security and privacy → Intrusion detection systems; Security and privacy → Security requirements; Security and privacy → Formal security models

Keywords and phrases Eduroam, Wi-Fi, Credential stealing, Attack, Network, Security

Digital Object Identifier 10.4230/OASIcs.SLATE.2024.13

Funding This work has received support from the EU/CINEA Innovation and Networks Executive Agency under grant agreement No 29335026.

1 Introduction

According to a recent report on cyber-attack trends, weekly cyber-attacks rose by 42% in the first half of the year, with significant increases in every region [2]. During the still occurring Russia-Ukraine war, there was a 196% increase in cyber-attacks on Ukraine's government-military sector. These attacks were led by Russian APT organizations that are well-known for their highly developed toolkits and have a track record of committing attacks. It is expected that these numbers will increase significantly in the next few years. Financial losses due to cybercrime were $6.1 trillion in 2021 and are projected to increase by 15% annually and reach $10.5 trillion by 2025 [5]. Unfortunately, many attacks go unnoticed for unreasonably extended periods. In the year 2019, the period from compromise to detection took more than 2 days for 42.3% of respondents, while the time from detection to containment took less than 24 hours for 67% and the time from containment to remediation took more than 2 days for 65.2% of responders [8]. These statistics demonstrate how organizations still have a long way to detect, contain and remediate threats in an optimal amount of time.

13th Symposium on Languages, Applications and Technologies (SLATE 2024).
Editors: Mário Rodrigues, José Paulo Leal, and Filipe Portela; Article No. 13; pp. 13:1–13:12
OpenAccess Series in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

A Security Operations Center combines a specialized IT team with the procedures and tools necessary to detect, assess, and respond to threats. SOCs are specialized to continually monitor system and network activity, allowing them to identify and address any threats quickly. All of these capabilities and responsibilities bring a plethora of challenges to guarantee the correct and efficient operation of a SOC. Industry white papers [2, 18] identify many problems that lead to inefficiencies in design and operations, such as a lack of skilled staff, comprehensive processes, and complex technology. Furthermore, when designing and implementing the SOC infrastructure it is extremely relevant to consider a wide range of topics to avoid these inefficiencies in the long run.

The objective of this paper is to provide information and considerations when designing and implementing a SOC's infrastructure. We aim to analyse the current cybersecurity infrastructure, identify emerging challenges and answer the following research question: *"Which infrastructure should a researcher use when building a SOC?"* This includes detailing current SOC frameworks and influential factors in section 2, operational models in section 3, and best practices in section 4. Finally, section 5 summarizes the main points and emphasizes the need for careful design and implementation when it comes to SOC infrastructure.

2 SOC Frameworks and Influential Factors

One of the first attempts at devising a framework for SOC implementation by Schinagl et al. [19] proposed dividing the SOC into five core functions. For each function, the objectives and activities can be outlined and translated into requirements for competencies, experience and number of staff. These core five functions are:

- **Intelligence function:** Analysts exchanging information, analyzing threat patterns, and providing instructions to the rest of the organization.
- **Baseline security function:** Oversees processes for hardening infrastructure, conducts vulnerability and compliance scans, supervises endpoint protection, and ensures operational effectiveness.
- **Monitoring function:** Observes data traffic, identifies anomalies, and filters logging data for relevant alerts.
- **Penetration test function:** Conducts tests for secure development and operational environments. Assesses system reactions to attacks and evaluates defense effectiveness.
- **Forensic function:** Extracts details from data traffic and logging infrastructure data. Assists in forensic investigations, collecting electronic evidence and ensuring the chain of custody.

One of the recent literature reviews on this subject by Vielberth et al. proposed the PPTGC (People, Processes, Technology, Governance and Compliance) framework [24]. When operating under this framework, a SOC employs a holistic approach to enhance organizational security. This framework encompasses dimensions such as governance, and compliance with other functional areas present in the previous frameworks, emphasizing the importance of the entire organizational ecosystem. Although considered a passive and reactive defense mechanism, a well-implemented SOC, guided by the PPTGC framework, can significantly improve a company's security posture by fostering situational awareness, mitigating risks, and ensuring regulatory compliance.

Other relevant frameworks that work at the organization level like the National Institute of Standards and Technology's Cybersecurity Framework 2.0 (NIST CSF 2.0) [16]. These are also very useful when building a SOC as they provide guidelines to measure the maturity of an organization's cybersecurity posture. The European Union Agency for Cybersecurity (ENISA) provides a similar but more limited framework for assessing the maturity level of Cybersecurity Incident Response Teams (CSIRT) in the ENISA CSIRT Maturity Framework [10], based on the SIM3v2 standard [11] by the Open CSIRT Foundation (OCF). These frameworks evaluate the security posture of an organization by measuring several controls according to their current level implementation with the total score being the final measure. These levels are generally related to the state of implementation of that specific control, with the bottom levels used for unimplemented or implicit implementations that are not fully documented and the higher levels for fully implemented mechanisms that have been properly accessed by the management layers of the organization and are reviewed regularly. This approach is very similar to the ITIL [6] and COBIT [9] frameworks that have been a staple in IT Governance for decades.

When designing and implementing a SOC, one of the first steps is to understand the primary factors that may influence the SOC's main requirements. These can vary from organization to organization due to differences in size, industry, and data, among many other factors. The frameworks mentioned allow organizations to devise their target profile, prioritizing whichever functions and controls they determine are more important for their specific scenario. The main aspects in discussion for this article are business requirements, compliance, threat landscape, staffing, and resources. Furthermore, it is important to mention that all of these factors may change over time with the evolution of the organization, cyber threats, and regulations. Thus to guarantee the effectiveness of the SOC, evolution and improvement must be a core part of its design.

2.1 Threat landscape

The threat landscape is comprised of specific types of cyber threats and vulnerabilities that an organization might face when operating, and how they evolve. One of the great references for the current threat landscape is the ENISA Threat Landscape [14]. It consists of a detailed report that provides an overview of the European Union's current cybersecurity threat landscape with data collected from a variety of trust sources, with a dedicated analysis of threat actors' motivations. Furthermore, it includes the impact analysis of the threats across different sectors which helps to specifically identify which threats should be considered for each sector.

During the period of ETL 2022, the most important threats mentioned in this report include ransomware, malware, denial of service, IoT, disinformation, social engineering threats, threats against data, and supply chain attacks. All of these threats will influence the design and implementation of the SOC architecture since they have to be properly addressed, not only when they are occurring, but also in the future. If new threats emerge, SOCs have to incorporate new technology, procedures, and resources which all affect the chosen SOC architecture. This way the SOC architecture must be designed to provide the necessary level of visibility and control over the organization's information systems and data, while also being able to adapt to changing threats over time.

2.2 Business requirements

Business requirements significantly influence how a SOC architecture is designed and implemented. Business requirements provide a framework for the SOC to align its strategies, procedures, and technology in a way that supports these goals by taking into consideration the special requirements and objectives of the organization. The business requirements may differ and the architecture should be custom and tailored. Nonetheless, they should provide the requirements considering compliance, data protection, incident response and alignment with existing infrastructure.

2.2.1 Compliance

Compliance is known as the process of making sure that an organization abides by the laws, rules, standards, and policies that are relevant to its context. The design and implementation of the SOC architecture may be impacted by this business requirement since it affects the security controls and procedures, and the choice of technologies and tools the SOC will employ. SOCs need to be able to show compliance with some regulatory obligations depending on the type of organization. Some of these regulatory requirements include HIPAA [13], PCI-DSS [20], and GDPR [21]. The HIPPA standard affects organizations in the healthcare industry to protect the privacy of protected health information (PHI). The PCI-DSS standard affects organizations in the financial industry to guarantee the protection of credit card data. GDPR compliance affects the European Union and sets standards for protecting the personal data of individuals.

Additionally, at the European Union level, the Network and Information Systems (NIS) 2 Directive [22] contains laws that ensure that any entity operating under their jurisdiction takes appropriate security measures and reports significant incidents to the national authorities. SOCs must be able to show they have implemented efficient security controls and are consistently testing and monitoring them to meet these compliance requirements. To demonstrate compliance, reporting and analytics play a crucial role and, according to the regulations in question, may influence the architecture of the SOC.

2.2.2 Data protection

Data protection is defined as the process of preventing unauthorized access, use, disclosure, modification, or destruction of sensitive data, such as personally identifiable information (PII) and protected health information (PHI). This business requirement is directly tied to the compliance topic where some regulatory requirements depend on the protection of data. Even organizations that are not obligated to comply should enforce this requirement to prevent data breaches that may include financial losses or a decline in the trust and reputation of the organization. For this reason, SOCs must use a variety of security measures, such as encryption, access controls, and data loss prevention (DLP) technologies, to protect data that influence architecture choices. Moreover, this design should also take into account incident response plans and procedures for responding to data breaches or any type of incident involving sensitive data.

2.2.3 Incident Response

Incident response refers to the process of identifying, containing, and mitigating the impact of an incident in an organization. The incident response process includes the implementation and design of incident response procedures and protocols that have to take into account various types of incidents that are likely to occur and the appropriate response. Typically, this takes the form of response playbooks that outline precise instructions for reacting to various types of incidents. Furthermore, the different data from various sources, such as network traffic, log files, and endpoint data, have to be identified to detect and respond to incidents correctly.

2.2.4 Alignment with existing infrastructure

The alignment with existing infrastructure refers to applying the SOC architecture to the existing technology and procedures in the organization. This alignment must be designed and implemented correctly to guarantee the efficiency and effectiveness of a SOC. These include not only network, server, and storage infrastructure, but also existing security solutions such as firewalls, intrusion detection/prevention systems, and endpoint security solutions. Mutemwa et al. outlines some of the challenges of building a SOC around an already existing IT infrastructure [15], one of the main ones being the correct integration of the people, processes and technologies of the SOC to the rest of the organization.

The planning of the necessary security solutions has to be tailored, taking into account multiple factors like the underlying infrastructure, existing tools and processes. For example, if the organization plans to add a specific service that will be hosted in cloud-based infrastructure in the near future, the SOC architecture must be designed and implemented to provide flexibility, allowing agile and efficient addition and integration with this cloud-based infrastructure.

2.3 Staffing and Tools/Equipment

Staffing and tools/equipment are one of the main foundational elements of a SOC along with technology and processes [24]. Adequate staffing and equipment are necessary to ensure that the SOC architecture is designed and implemented with these resources in mind and to effectively operate. In these next subtopics, we performed a deep dive into each topic separately.

2.3.1 Staff

According to the ISC cybersecurity workforce study report [4], “A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution”. This report estimates that there is still a huge worldwide gap of 3.4 million cybersecurity workers missing in the industry. This shortage, intertwined with the lack of experience in the sector creates huge problems for organizations that do not have the capability of hiring professionals, let alone experienced ones. For all of these reasons, staff size and experience play a crucial role in the design and implementation of a SOC.

SOC staff is generally composed of a SOC Manager who manages the SOC and responds to the institution’s Chief Information Security Officer (CISO). To operate the SOC, cybersecurity analysts are required to respond to any incident reported or discovered. These analysts are usually divided into tiers based on skill level and experience to ensure efficient use of human resources, with incidents being escalated from the lower tiers to the higher tiers of analysts if their complexity makes them impossible to handle by the less experienced analysts. Another key role in a SOC is the security engineers, who are tasked with building and maintaining the complex toolset required to run the SOC.

2.3.2 Tools/Equipment

The market for tools/equipment in cybersecurity has grown and is expected to significantly increase in the coming years [3]. A variety of solutions for different use cases exist in the market today, ranging from the detection of network and host-based threats to vulnerability scanners, prevention tools, and incident management solutions. The Gartner market guides for a variety of tools are one of the best references to understand how the status of an emerging market aligns with the organization’s future plans [12]. Commercial tools are not the only viable option, open source tools can offer equivalent features without the licensing costs as demonstrated by Vaarandi et al. in a SOC implementation for a university [23]. One of the main drawbacks of using open-source tools is the extra work required to maintain those tools. This happens in the entire IT field and in the scope of a SOC this work be handled by the security engineers and the staffing costs to operate a tool have to be carefully compared to the licensing costs of equivalent commercial solutions as open source is not always the most cost-effective option.

One of the most significant trends in the market that differentiate vendors is the increasing use of artificial intelligence (AI) and machine learning (ML) technologies to further enhance the tool's performance on detection and response [17]. The selection of tools and equipment influences the architecture of the SOC, as the tools and equipment selected may provide means to the capabilities of the SOC. This ties directly, not only with the cost of purchasing the more adequate solutions but also with the technical know-how of the employees to use these tools effectively. Organizations must carefully assess the current cost of the tools and equipment, as well as the long-term expenses and benefits of each option.

3 SOC Operational Models

A SOC architecture is the overall design and structure of an organization's security operations and incident response capabilities. It includes all of the tools, techniques, and individuals employed in the detection, response, and mitigation of security incidents. There are many ways to operate a SOC and many different classifications for SOCs. Schinagl et al. grouped different SOC operating models based on the SOC's organizational placement and function. According to their classification, SOCs can be integral, technology-driven, partly outsourced or specialized. Radu et al. clustered operational models based on size, scope, and authority with the outcome being the following five classifications: virtual SOC, small SOC, large SOC, tiered SOC, and national SOC [1].

Regarding the technological component of a SOC, one of the first architecture proposals, SOCBox [7] split the core components into categories: event generators, event collectors, message databases, analysis engines and reaction management software which remains relevant to this day except for some shortcomings in forensics and reactive capabilities. Other authors like Radu et al. [1] made a more abstract approach and defined a SOC's architecture by splitting the components into four distinct layers: data generation, data acquisition, data manipulation, and data presentation. At the moment of writing, there is a lack of more in-depth architecture proposals present in the literature that are not tailored for a specific domain.

A SOC architecture often contains components like SIEMs, IDPS, Firewalls, endpoint security tools, and security orchestration and automation solutions. The scope of this work is focused on the decision that must be considered underlining infrastructure, their interconnection with other components and their operational costs. People building a SOC in the current Cloud Computing paradigm can generally select between private clouds, public clouds, and hybrid approaches. A comprehensive detailed explanation for each will be provided in the following sections.

3.1 Private Cloud

A private cloud-based SOC uses a private cloud usually hosted in a physical facility (or multiple facilities) that is located within an organization's premises. This means that all of the technological infrastructure such as servers, storage devices, networking equipment, and other hardware that support the SOC will be hosted in the data centers of the organization. It further implies that all the technological infrastructure is owned, operated, and maintained by the organization itself, and is not dependent on any type of external entities. This provides the highest degree of trust, security and customization. The main disadvantages are higher costs unless done at a very large scale, lower scalability as capacity improvements take more preparation, and lower availability as private clouds generally do not have as many facilities available when compared to their public counterparts.

3.2 Public Cloud

By contrast, cloud-based infrastructure refers to IT systems and components that are owned and controlled by a third-party provider and that may be accessed remotely via the Internet. Public clouds are generally more cost-effective and provide better availability than private clouds. The main drawbacks are lower security due to the involvement of a third party with privileged access to the infrastructure and lower customizability as some of the cloud's service models greatly restrict what its end-users can do with their tools. The service models that exist are infrastructure as a service, platform as a service, and software as a service. The differences between them lie in what types of services are offered, ranging from infrastructure with similar features that a private cloud user would have available to fine-tuned turn-key software services that completely remove most operational concerns from the end users, as shown in Figure 1.

3.2.1 Infrastructure as a Service

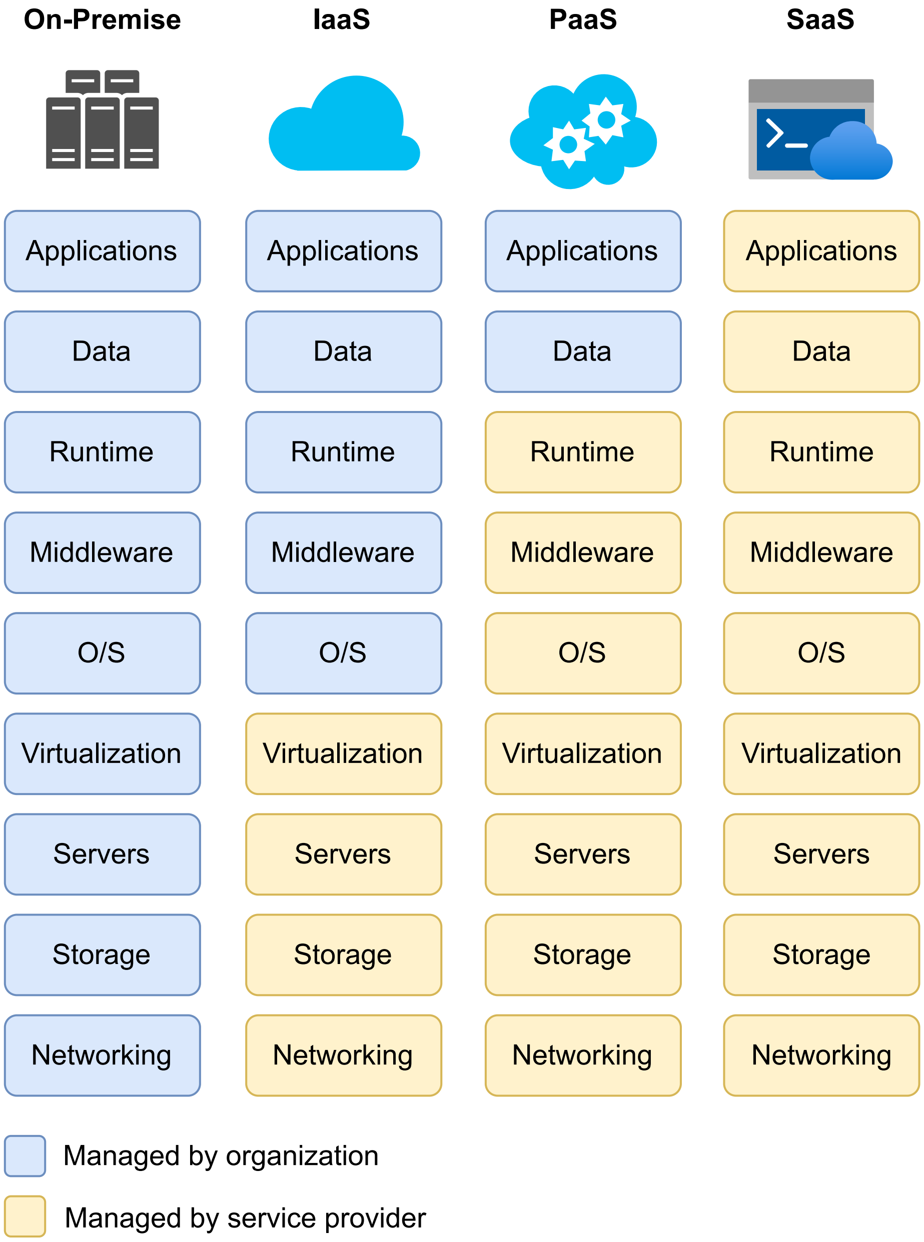
Infrastructure as a Service (IaaS) is a type of cloud computing that provides virtualized computing resources over the Internet. These resources can include servers, storage, and networking and provide a "virtual data center" in the cloud. In the context of a SOC, this solution allows the full/partial hosting of all security tools on the cloud, but the management of aspects such as data, operating systems, and system updates is the responsibility of the SOC team. Furthermore, the configuration and maintenance of all software is also the responsibility of the SOC members.

3.2.2 Platform as a Service

Platform as a Service (PaaS) is a type of cloud computing that provides a platform for developing, running, and managing applications over the Internet. The resources provided by this type of hosting can include servers, storage, and networking as IaaS, but the service provider is responsible not only for operating systems maintenance and updates but also for storage and networking infrastructure. The SOC is only responsible for the data and software solutions used, keeping in mind that these solutions must be compatible with the cloud's platform. Even though the configuration and maintenance of all software is the responsibility of the SOC, most technological services exist in a cloud-hosted form, which will alleviate the workload and maintain these systems, allowing for greater scalability and high availability [25].

3.2.3 Software as a Service

Software as a Service (SaaS) can be used to host and manage software solutions using the internet to deliver applications. In this type of cloud hosting, the service provider is responsible for all aspects of the software and underlying systems including data, thus, differentiating itself from the PaaS solution. These pre-built environments that constitute the technological architecture with the security systems and software are delivered directly to the organization as a ready-to-use solution, generally with vendor support.



On-Premise	IaaS	PaaS	SaaS
🟦 Applications	🟦 Applications	🟦 Applications	🟨 Applications
🟦 Data	🟦 Data	🟦 Data	🟨 Data
🟦 Runtime	🟦 Runtime	🟨 Runtime	🟨 Runtime
🟦 Middleware	🟦 Middleware	🟨 Middleware	🟨 Middleware
🟦 O/S	🟦 O/S	🟨 O/S	🟨 O/S
🟦 Virtualization	🟨 Virtualization	🟨 Virtualization	🟨 Virtualization
🟦 Servers	🟨 Servers	🟨 Servers	🟨 Servers
🟦 Storage	🟨 Storage	🟨 Storage	🟨 Storage
🟦 Networking	🟨 Networking	🟨 Networking	🟨 Networking

🟦 Managed by organization

🟨 Managed by service provider

Figure 1 Differences between cloud-based solutions.

3.3 Hybrid

Hybrid solutions refer to the combination of private and public cloud-based infrastructure. By enabling organizations to benefit from both on-premises and cloud-based technologies, this strategy is practiced in different forms by organizations. The use of SIEMs as SaaS can be adopted in a hybrid architecture with other on-premise security tools such as firewalls, IDPS, and EDR [26]. This can greatly improve the flexibility and scalability of a SOC in dealing with the growing amount of informational systems and logs [26].

Another possible hybrid architecture may include running vulnerability management solutions on a PaaS. This solution provides customization and integration with other security tools. It allows the combination of IaaS and on-premise solutions for different tools when physical resources such as servers and storage are a bottleneck in on-premises solutions. Enabling businesses to benefit from both on-premises and cloud-based technology hybrid solutions in SOC architectures can give businesses a flexible and effective approach to managing their security operations and a reduction in costs and complexity.

4 Best practices when designing a SOC

Designing a SOC can be a complex task, specifically when having to take into account so many factors. Selecting the appropriate solution is of extreme importance for the SOC. Each solution has its own set of advantages and disadvantages, and the choice of a SOC´s architecture deployment can be determined by the factors mentioned in Section 2. In this section, we discuss some best practices for SOC infrastructure design and implementation. The frameworks can provide some guidance to identify which tools are required to build a SOC but they need to be tailored to every specific scenario. Compliance is one of the first primary aspects that should be considered as it goes beyond target profiles and maturity levels due to its mandatory nature, as it places restrictions on what resources can be used and may drastically reduce the options available.

4.1 Scalability, Cost, and Flexibility

The scalability, cost, and flexibility of each solution are impacted by all of the factors mentioned in Section 2. The threat landscape keeps evolving and organizations need to have the ability to adapt and expand to deal with new and emerging threats effectively. Some business requirements, such as data protection, may grow in volume over time and involve more processing power and storage to deal with the organization's expansion.

On-premise SOC solutions may have limitations in terms of scalability and flexibility, as the organization is responsible for maintaining, upgrading, and purchasing the physical infrastructure and the software. These responsibilities lead indirectly to higher costs. Cloud-based SOC solutions, such as SaaS and PaaS, generally offer greater scalability and flexibility at a lower cost since the provider manages the technology and can quickly add resources when needed. Maintenance costs should not be as much issue for cloud-based solutions.

4.2 Security and Compliance

Specific security requirements and compliance exist for certain industries, as mentioned in Section 2.2.1, the SOC implementation must allow conformity in all aspects. This includes the selection of technologies, processes, personnel and infrastructure.

Some cloud-based SOC solutions may provide some compliance with regulations when maintaining and upgrading the infrastructure, however, when it comes to data storage and encryption this may not be the best solution, as it may require additional measures and configuration options not provided by the cloud-based solution. This excludes SaaS solutions as a possibility and includes only some PaaS and IaaS solutions. To be a feasible option, PaaS and IaaS solutions must have a highly configured environment that adheres to the regulations.

On-premise SOC solutions provide more control over security and compliance measures. This solution is not reliant on third-party providers and is free from the disadvantages of a cloud-based solution regarding security and compliance aspects.

4.3 Expertise and Resources

As mentioned in Section 2.3.1, a lack of expertise and resources is a common issue that organizations currently face. For this reason, it's important to consider the availability of in-house engineering expertise and resources when selecting a SOC infrastructure model. For a SOC to be fully deployed on-premise, all resources, including staff, expertise, and tools/equipment, must be readily available and dedicated to the maintenance and operation of the SOC. When this is not possible, cloud-based solutions can alleviate the in-house resources needed for maintenance as some of the infrastructure and engineering-related workloads are shifted to the third-party provider. In both configurations, it is important to select the appropriate technologies with a particular focus on automation tools to reduce staffing requirements.

5 Conclusion

The proper design and implementation of a SOC is essential to an organization's cybersecurity strategy. However, in the initial stages, several challenges may emerge due to several factors. When planning different architectures, it is important to consider these factors, namely the existing infrastructure options, and how they differentiate from each other. Based on this, we identified that to answer the proposed research question, cybersecurity researchers need to include on-premises, cloud-based, or a compilation of the two (a hybrid approach) in their decisions. With the different architectural approaches in mind, the advantages and disadvantages of each solution were analyzed, considering the various influential factors, such as size, industry, and data, among many other factors.

References

1 Comparative analysis of security operations centre architectures; proposals and architectural considerations for frameworks and operating models, author=Radu, Sabina Georgiana. In *Innovative Security Solutions for Information Technology and Communications: 9th International Conference, SECITC 2016, Bucharest, Romania, June 9-10, 2016, Revised Selected Papers 9*, pages 248–260. Springer, 2016.

2 Cyber Attack Trends - Check Point's 2022 Mid-Year Report. Technical report, Check Point, 2022. URL: https://www.checkpoint.com/downloads/resources/cyber-attack-trends-report-mid-year-2022.pdf.

3 Cyber Security Market Overview by Size, Growth & Trends, 2029. Technical report, Fortune Business Insights, 2022. URL: https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165.

4 Cybersecurity Workforce Study. Technical report, (ISC) 2, 2022.

5 State of Cybersecurity. Technical report, CompTIA, 2022. URL: https://www.comptia.org/content/research/cybersecurity-trends-research.

6 Claire Agutter. *ITIL Foundation Essentials ITIL 4 Edition-The Ultimate Revision Guide*. IT Governance Publishing Ltd, 2020.

7 Renaud Bidou, Julien Bourgeois, and Francois Spies. Towards a global security architecture for intrusion detection and reaction management. In *Information Security Applications: 4th International Workshop, WISA 2003 Jeju Island, Korea, August 25-27, 2003 Revised Papers 4*, pages 111–123. Springer, 2004.

8 Matt Bromiley. SANS 2019 Incident Response (IR) Survey: It's Time for a Change A SANS Survey. Technical report, SANS, 2019. URL: https://www.sans.org/white-papers/39070/.

9 Steven De Haes, Wim Van Grembergen, Anant Joshi, and Tim Huygh. *COBIT as a Framework for Enterprise Governance of IT*, pages 125–162. Springer International Publishing, Cham, 2020. doi:10.1007/978-3-030-25918-1_5.

10 European Union Agency for Cybersecurity ENISA. ENISA CSIRT Maturity Framework, 2022. doi:10.2824/35453.

11 Open CSIRT Foundation. SIM3 v2 interim – Security Incident Management Maturity Model, 2023. URL: https://opencsirt.org/wp-content/uploads/2023/11/SIM3_v2_interim_standard.pdf.

12 Gartner. Market Guide Research Methodology, 2023. URL: https://www.gartner.com/en/research/methodologies/market-guide.

13 US HHS. Your Rights Under HIPAA, 2022. URL: https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html.

14 Lella Ifigeneia, Tsekmezoglou Eleni, Malatras Apostolos, and Theocharidou Marianthi. ENISA Threat Landscape 2022. Technical report, ENISA, 2022. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022.

15 Muyowa Mutemwa, Jabu Mtsweni, and Lukhanyo Zimba. Integrating a security operations centre with an organization's existing procedures, policies and information technology systems. *2018 International Conference on Intelligent and Innovative Computing Applications, ICONIC 2018*, 1 2019. doi:10.1109/ICONIC.2018.8601251.

16 National Institute of Standards NIST and Technology. The NIST Cybersecurity Framework (CSF) 2.0, 2024. doi:10.6028/NIST.CSWP.29.

17 Sean Oesch, Robert Bridges, Jared Smith, Justin Beaver, John Goodall, Kelly Huffer, Craig Miles, and Dan Scofield. An Assessment of the Usability of Machine Learning Based Tools for the Security Operations Center. In *2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics)*, pages 634–641, 2020. doi:10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics50389.2020.00111.

18 Cyril Onwubiko and Karim Ouazzane. Challenges towards Building an effective Cyber Security Operations Centre. *International Journal on Cyber Situational Awareness*, 4:11–39, 2 2022. doi:10.22619/IJCSA.2019.100124.

19 Stef Schinagl, Keith Schoon, and Ronald Paans. A Framework for Designing a Security Operations Centre (SOC). In *2015 48th Hawaii International Conference on System Sciences*, pages 2253–2262, 2015. doi:10.1109/HICSS.2015.270.

20 PCI SSC. Official PCI Security Standards Council Site v4.0, 2022. URL: https://www.pcisecuritystandards.org/.

21 European Union. Regulation (EU) 2016/ 679 of the European Parliment and Council, 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

22 European Union. NIS 2 Directive, 2022. URL: http://data.europa.eu/eli/dir/2022/2555/ojf.

23 Risto Vaarandi and Sten Mases. How to Build a SOC on a Budget. *Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience, CSR 2022*, pages 171–177, 2022. doi:10.1109/CSR54599.2022.9850281.

24 Manfred Vielberth, Fabian Bohm, Ines Fichtinger, and Gunther Pernul. Security Operations Center: A Systematic Study and Open Challenges. *IEEE Access*, 2020. doi:10.1109/ACCESS.2020.3045514.

25 Stephen Watts and Muhammad Raza. SaaS vs PaaS vs IaaS: What's The Difference & How To Choose, 2019. URL: https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/.

26 Olga Wenge, Ulrich Lampe, Christoph Rensing, and Ralf Steinmetz. Security Information and Event Monitoring as a Service: a Survey on Current Concerns and Solutions. *PIK - Praxis der Informationsverarbeitung und Kommunikation*, 37:163–170, 6 2014. doi:10.1515/PIK-2014-0009.