SOC STRATEGY

Mini Project 27

Oshe Mazin

Springboard | Cybersecurity Career Track

The number of cyber security threats continues to grow, and organizations must be vigilant in protecting their networks and data. The most effective way to do this is by setting up a Security Operations Center (SOC). A SOC is a team of experts responsible for monitoring and responding to security threats.

SOCs are critical for organizations to detect and respond to cyber threats in real time. In this report, we will compare three different strategies for creating a SOC: using Free and Open-Source Software (FOSS) solutions, using commercial solutions, and outsourcing to a third-party Managed Detection and Response (MDR) or Security Operations as a Service (SOCaaS) provider. We will consider important data points such as additional full-time employees (FTEs), software licenses, cloud instances, and storage requirements. Each approach has its own advantages and disadvantages, and the best solution will depend on the specific needs and resources of the organization.

Creating an in-house Security Operations Center (SOC) using Free and Open Source Software (FOSS) solutions allows organizations to customize their security systems to protect their networks and data. Throughout this paragraph, we will compare the advantages and disadvantages of creating an in-house SOC using FOSS solutions. The main advantage of using FOSS solutions is that they are FREE to use and modify. This means that the organization can save on software licensing costs and customize the solutions to fit their specific needs. Additionally, a large community of users and developers contribute to the development and maintenance of FOSS solutions, making them more stable and secure over time. Examples of FOSS solutions include the ELK Stack, OSSEC, and Kiwi Syslog Server. ELK Stack (Elasticsearch, Logstash, and Kibana) is used primarily for log management and analysis, OSSEC for intrusion detection and response, and Kiwi Syslog Server for log collection and management. The primary disadvantage of creating an in-house SOC using FOSS solutions is the lack of support. Organizations must rely on their own internal resources for support or find support from the community of users. This can be time-consuming and may not be feasible for organizations with limited resources or technical expertise.

Additionally, organizations must ensure that the FOSS solutions meet their security requirements, as there is no guarantee that the solutions are secure or compliant with industry standards. Finally, organizations must ensure the FOSS solutions are kept up-to-date and patched regularly, as there is no vendor to provide updates and patches. Furthermore, creating an in-house SOC using FOSS solutions does not require additional Full Time Employees (FTEs). Organizations can save on FTE costs, which can be significant, as the average salary for a SOC/cybersecurity analyst is about $90,000/yr. Additionally, organizations can save on storage requirements, as the FOSS solutions are hosted on the organization's own server.

In conclusion, creating an in-house SOC using FOSS solutions offers organizations the ability to customize their security systems to protect their networks and data. The primary advantage of using FOSS solutions is cost savings, as no software licenses, cloud instances, or FTEs are required. However, a glaring disadvantage of using FOSS solutions is the lack of support, as organizations must rely on their own resources or the community of users. Organizations must also ensure that the FOSS solutions meet their security requirements and are kept up to date.

Security operations centers (SOCs) are a critical component of any organization's IT security strategy. SOCs provide real-time monitoring and response capabilities to detect and respond to security incidents and threats. Organizations can choose to create an in-house SOC by using commercial solutions, or they can outsource SOC services to a third-party provider. Within this paragraph, we will examine the advantages and disadvantages of creating an in-house SOC using commercial solutions. The main advantage of creating an in-house SOC using commercial solutions is that organizations have full control over the security operations and can customize the solution to their needs. This type of solution provides organizations with flexibility in terms of the technology they use, as well as the ability to scale quickly and easily. Additionally, in-house SOCs can be more cost-effective than outsourcing SOC services as there are no external service fees to pay. Examples of commercial solutions include Splunk for log

management and analysis, Carbon Black for endpoint protection and response, and Firefly for threat detection and response. A critical disadvantage of creating an in-house SOC using commercial solutions is the cost associated with it. Organizations will need to purchase and maintain software licenses, cloud instances, and storage requirements, as well as hire and train additional full-time employees (FTEs) to manage the SOC. For example, a software license for Splunk can cost $150,000/yr, while a software license for Carbon Black can cost $30,000 per year. FTE salaries for SOC/cybersecurity analyst is about $90,000/yr for each employee.

Ultimately, creating an in-house SOC using commercial solutions can be a cost-effective option for organizations looking for full control over their security operations. However, it comes with the associated costs of purchasing and maintaining software licenses, cloud instances, storage requirements, and hiring and training additional FTEs. Organizations should carefully consider the cost and expertise required when deciding whether to create an in-house SOC or outsource SOC services.

The decision to outsource the Security Operations Center (SOC) to a third-party Managed Detection and Response (MDR) or Security-as-a-Service (SOCaaS) provider is a crucial one. Some examples of MDR and SOCaaS providers include CrowdStrike, Alert Logic, and Rapid7. These providers offer a range of services such as threat detection, incident response, and compliance management. Before making a decision, it is important to weigh the potential advantages and disadvantages of this option. Below we will compare the advantages and disadvantages of outsourcing the SOC to a third-party MDR or SOCaaS and will provide data points to further inform the decision. An underlying advantage of outsourcing the SOC to a third-party MDR or SOCaaS provider is the cost savings associated with it. By outsourcing the SOC, organizations can eliminate the need for additional FTEs, software licenses, cloud instances, and storage requirements. The average salary for a SOC/cybersecurity analyst is about $90,000/yr, so outsourcing the SOC to a third-party provider will save money that would have been spent on additional FTEs. Additionally, outsourcing the SOC eliminates the need for additional

software licenses and cloud instances, which can be expensive. Outsourcing the SOC to a third-party provider can also save time and resources. Organizations can avoid the time-consuming process of recruiting and training new FTEs and can instead focus their resources on core activities. Furthermore, third-party providers often have more experience and expertise in SOC operations so they can provide more efficient and effective threat detection and response services. A glaring disadvantage of outsourcing the SOC to a third-party provider is the potential for a lack of control over the security operations. Organizations may not have access to the same level of visibility or control over the security operations as they would if they had an in-house SOC. Additionally, outsourcing the SOC could lead to a lack of alignment between the security operations and the organization's goals and objectives, which could negatively affect the organization's security posture. In conclusion, outsourcing the SOC to a third-party MDR or SOCaaS provider can provide a number of advantages, such as cost savings, time savings, and access to experienced and expert personnel. However, it is important to consider the potential disadvantages, such as a lack of control over the security operations and a lack of alignment between the security operations and the organization's goals and objectives. By weighing the potential advantages and disadvantages of outsourcing the SOC, organizations can make an informed decision that best meets their needs.

Ultimately, each of the three SOC strategies has its own set of specific advantages and disadvantages that must be considered when deciding on a given approach. When deciding which of the three would prove to be the most suitable for our organization it is important to first identify some of the main challenges associated with monitoring multiple operating systems across multiple global locations. Maintaining compliance between various regions, dealing with the overall lack of visibility, and the need for automation are all challenges that will need to be addressed by the chosen method. With that in mind, the approach that would best suit our specific organization would be to outsource the SOC to a third-party MDR or SOCaaS; this will help the company in various ways. First, it will help the company

reduce costs and increase efficiency. An experienced SOC provider will help to quickly identify and respond to security threats, reducing the risk of a data breach or other security incident. Also, an outsource provider will bring specialized skills and resources that the company may not have in-house. Lastly, outsourcing SOC services will help free up internal teams to focus on other important tasks, such as developing new energy products or services. As we continue to grow as an organization through mergers and acquitsations (M&A) this will prove to have been a tremendous move to help manage security operations and boosten the overall morale of the IT department by simply allowing the SOC to handle the OT environment.

Citations

Datashield. (n.d.). *Pros and cons of an Outsourced Security Operations Center (SOC)*. Pros and Cons of an Outsourced Security Operations Center (SOC). Retrieved January 21, 2023, from https://www.datashieldprotect.com/blog/pros-and-cons-of-an-outsourced-soc

Lee Congdon (Enterpriser) February 3, Lee Congdon (Enterpriser), 3, F., |, Register or Login to like I work with IT teams that are so passionate about Red Hat's open source mission that they bring a "default to open, & Lee Congdon is Senior Vice President and Chief Information Officer at Ellucian. (n.d.). *8 advantages of using open source in the Enterprise*. The Enterprisers Project. Retrieved January 21, 2023, from https://enterprisersproject.com/article/2015/1/top-advantages-open-source-offers-over-proprietary-solutions

Pratyush.Raunak. (2022, December 2). *Building SOC from scratch using Open source toolkit part-1*. Payatu. Retrieved January 21, 2023, from https://payatu.com/blog/open-source-soc/

Splunk pricing. Splunk. (n.d.). Retrieved January 21, 2023, from https://www.splunk.com/en_us/products/pricing.html

Sullivan, P. (2020, December 8). *Pros and cons of an outsourced SOC vs. in-house soc: TechTarget*. Security. Retrieved January 21, 2023, from https://www.techtarget.com/searchsecurity/tip/In-house-vs-outsourced-cybersecurity-operations-center-capabilities

VMWare Carbon Black Cloud Enterprise EDR - subscription license (3 years) + - VSEC-EEDR-dir-W-US-3Y-C - Endpoint Security. CDW.com. (n.d.). Retrieved January 21, 2023, from https://www.cdw.com/product/vmware-carbon-black-cloud-enterprise-edr-subscription-license-3-years/6038230