DOI: https://doi.org/10.30837/csitic52021231860

Enterprise Security Operations Center

Oleksandr Sievierinov[1]

[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave,
Kharkiv UA-61166, Ukraine,
e-mail: oleksandr.sievierinov@nure.ua

Marharyta Ovcharenko[2]

[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave,
Kharkiv UA-61166, Ukraine,
e-mail: marharyta.ovcharenko@nure.ua

Andrii Vlasov [3]

[3]Kharkiv National University of Radio Electronics, 14 Nauky Ave,
Kharkiv UA-61166, Ukraine, e-mail: andrii.vlasov@nure.ua

Abstract*. This article examines the main components of enterprise security operations centers. The main particular models of enterprise security operations centers are considered - classic, MDR and mixed. Also considered and characterized the main levels of SOC implementation in the enterprise.*

Keywords: *information security, enterprise security operations center, incident, event, classic model, MDR model, mixed model, technology, process, staff, SOC, maturity level, security operations model.*

I. Introduction

Today enterprises have begun to pay much more attention to the problems of protecting commercial information, as well as their information systems and their components. To solve these problems, an enterprise can resort to the use of several units and sometimes dozens of various and disparate hardware and software information protection tools, which can process information security events and incidents in the information system in different ways and can also be incompatible [1]. Thus, any enterprise in the modern world needs a unified service and solution that would carry out the tasks of monitoring, auditing, responding to events and incidents in the system, investigating incidents, as well as developing and implementing a set of internal rules of the enterprise that would be used to prevent an incident or to minimize its consequences and when responding to information security events and incidents. Given the constant emergence of new and modification of old methods of carrying out attacks and means of their implementation, the only solution that can cope with all of the above tasks is the creation and implementation of an enterprise security operations management center (SOC) into the information system.

Today SOC is one of the most common means of monitoring the state of information security of an enterprise, managing information security incidents and monitoring compliance with regulatory legal acts, internal rules of the enterprise and requirements, therefore it is necessary at the design stage to determine the type and structure of the SOC. In this article we will discuss and analyze the main types of SOC implementations and identify information security incident management systems that can be used in the SOC.

II. Problem Solution and Results

A SOC acts like the hub or central command post, taking in telemetry from across an organization's IT infrastructure, including its networks, devices, appliances, and information stores, wherever those assets reside. The proliferation of advanced threats places a premium on collecting context from diverse sources. Essentially, the SOC is the correlation point for every event logged within the organization that is being monitored. For each of these events, the SOC must decide how they will be managed and acted upon.

In practice the enterprise security operations center basically contains 3 components:

1. Technologies - operational identification and response to events and incidents in the system;
2. Processes - structured, debugged and tested schemes, methods and procedures for monitoring, auditing and responding to events and incidents in the system;
3. People - qualified, trained and competent staff, a 24x7 emergency response team.

In addition to the emergency response team in the SOC, security analysts are required to investigate high-priority incidents or those that have caused significant damage, analytics and reporting, as well as certified engineers who know down to the smallest detail the technologies and processes used in the SOC, and are competent to conduct effective administration and support of the center.

Before designing a SOC, it is necessary to assess the current state of the information system and its main assets (determine all assets, determine the current degree of security, analyze the architecture of the network and its components, and also evaluate using qualitative or quantitative methods the damage that will be caused to the information system and the reputation of the enterprise when implementation of each specific threat or groups of threats), determine the structural content of the SOC, gather a team of experts, keep abreast of new threats, provide infrastructure to support the SOC, determine the methodology for the functioning of the SOC, the volume of staff labor costs for processing information security events and incidents, as well as determine the target indicators for which the analysis will be carried out for the compliance of the enterprise security operations center with the stated requirements and its further modernization if necessary [2, 3].

Problematic moments in the design and implementation of a SOC in an enterprise can be the lack of a process owners or an exact goal, the SOC as the only end goal, lack of qualified staff to implement and launch processes, concentration on the "best" technologies that, when combined into a single whole system, may not provide the desired best properties that have been desired, the inability of software and hardware to solve all the tasks that were assigned to it, as well as the lack of a clear formalization of processes [3].

SOC's areas of activity are [4]:

1. Technologies, which include monitoring technology (correlation, collection, provision of data), as well as support technology (center communications, knowledge base, data

storage and archiving, analyst workstations, operating systems and databases);

2. Organizational relationships with management, staff, system owners, data owners, partners, contractors, customers, as well as security and audit;

3. Extraction of intelligence by obtaining information from internal sources (analysis of information security events and incidents, as well as processing reports), as well as from external sources (commercial subscriptions, open sources of information);

4. Resource management implies the developed and implemented ventilation, cooling systems, power supply network, as well as the placement of the SOC in the Data Processing Center;

5. Personnel management;

6. Processes and procedures;

7. Compliance, policy and risk management, which involves collecting configuration files and rules from active network equipment, detecting errors in the configuration of firewalls, helping to remove ineffective rules, visualizing existing and alternative information flows in an organization, automating analysis and modeling of a potential development process of threats, analysis of the compliance of the network topology and data flows according to laws, regulations and information security policy in the organization;

8. Monitoring of systems and networks, which includes monitoring network performance, managing device configurations, creating a network topology, analyzing the load of communication channels, identifying bottlenecks in the network, monitoring servers and applications, managing the data storage system;

9. Protection against attacks such as denial of service (DoS), which includes protection against attacks that are aimed at exploiting application vulnerabilities, overload and unavailability of servers, protection against flooding and overload of network channels, as well as the correct identification and neutralization of attacks without blocking legal user traffic;

10. Vulnerability management system, which includes assistance in detecting and preventing destructive attacks, assistance in prioritizing recovery actions and reducing organizational losses, online scanning of the network both after a predetermined period of time and as a response to suspicious network activity, and also detection of vulnerabilities in the organization's information protection system by searching for vulnerabilities, dangerous default settings, incorrect device configurations and vendor flaws;

11. Security information and event management system (SIEM system), which allows you to implement the management of organization assets, security, reporting documentation, information security events and incidents, collection and correlation of data about information security events and incidents in the organization, reconstruction of all sessions and artifacts, visual display of connections in the process of implementing an attack, recreating all actions that took place in the organization's information system during the implementation of the attack in chronological order with indicating the sources.

The processes and procedures in the SOC are divided into business, technological, operational, and analytical processes. Business processes include market continuity, internal and external compliance requirements, process improvement. Technological processes in a SOC are SOC design, change and configuration management, and system administration. The operational processes in the SOC include the management of information security events and incidents, operations that are performed on a daily basis, as well as trainings and processes of training the organization's staff on the rules for working with the resources and assets of the organization, as well as the rules of conduct and actions in critical situations for the organization., namely, when events or incidents of information security occur. In turn, analytical processes combine the management of information security incidents, the formation and analysis of reporting documentation, the analysis of intrusions into the organization's information system, as well as the detection of hidden information security events.

SOC human resources management consists of two subsets, such as organizational structure and organizational measures. The organizational structure of human resources management in the SOC includes staff whose functional responsibilities are directly related to ensuring the correct functioning of the SOC, and, therefore, ensuring information security in the organization. Such staff includes SOC managers, analysts, operators, system administrators, security administrators, Information Security Service and information security and Security Agence, if any, in the organization, as well as any support staff whose functional responsibilities include maintaining proper operating conditions for tangible assets of the organizations that are part of the SOC, as well as ensuring a comfortable working environment for staff which is working directly with these assets. In turn, organizational measures mean the principles and rules of staff selection, work plans, education, training, the formation of a staff reserve, the formation of a career plan for each employee, as well as the formation of a system of incentives and motivation to stimulate staff to pay increased attention to the slightest changes in the functional state or configuration of the system.

The goals and objectives of the SOC are [4]:

1. Aggregation of information security events and information flows;

2. Monitoring and analysis of information security events and incidents;

3. Analysis of threats and vulnerabilities of the organization's information system;

4. Responding to 0-day cyber threats;

5. Identification of vectors of cyberattacks;

6. Proactive monitoring of the state of information security in the organization;

7. Detection and response to information security events and incidents;

8. Formation and analysis of reporting documentation.

There are 3 main SOC models [2]:

1. Classic model;

2. MDR model;

3. Mixed model.

The classic SOC is engaged in monitoring the operation of information security systems and failures in their work, as well as illegal actions of users of the information system, that is, it manages events and incidents, but is not able to trace the entire life path of an attack through the infrastructure of the enterprise. The processes of this center are the management of security events and incidents, the coordination of response to them. At its core, the classic SOC uses a SIEM system that processes statements from information security tools using correlation rules and notifies the security administrator about previously unknown events or attacks, and a mandatory element is ServiceDesk, in which the response to previously unknown security events and incidents is coordinated [5]. Basically, the staff of such a center are people with minimal competencies. The 9x5 model involves 2 operators, 2 analysts, an architect and a manager, while the 24x7 model involves 10 operators, an analyst and an architect who is also a manager. One of the essential advantages of building a classical SOC is maximum visibility and responsiveness across the network. A dedicated internal team will have the capability to monitor the environment and its applications, providing a complete picture from a threat landscape perspective. The disadvantage of the classic SOC model is the large number of false alerts due to the low degree of processing of information about security events and incidents. Building a dedicated in-house Security Operations Center is recommended for mature cybersecurity enterprises.

In the MDR model, the vector of monitoring priorities is shifted towards the creation and implementation of scenarios for monitoring external attacks and events and incidents resulting from errors of security administrators and system administrators. The MDR model is based on the analysis of vulnerabilities, monitoring external threats, searching for previously unknown threats, analyzing already collected information about threats, managing the development of scenarios for monitoring and rules for detecting attacks. The core of this model contains of a platform for monitoring external threats (Threat Intelligence Platform), a database for managing settings, an element for analyzing samples of malicious code, as well as additional elements in the form of network asset scanners. Events about new assets, processes, logins to workstations and servers are collected not only from active network elements, but also from network IDS. The staff must have at least 3 years of experience in monitoring scenarios, knowledge of the distinctive features of different operating systems, knowledge of scripting languages, knowledge of non-standard methods and means of conducting threats. In this model, it makes no sense to work according to the 24x7 model, since anomalies are detected within the framework of low-intensity attacks, which are characterized by attempts by an attacker to disguise himself as a legitimate user and act slowly. In turn MDR's activities to detect and eliminate errors in network configuration and threat detection rules can further slowdown the course of an attack, since an attacker will have to conduct passive attacks on network monitoring at regular intervals in order to determine ways to implement unauthorized access to network assets and invisible carrying out an attack. Selecting a MDR model of the SOC is recommended for organizations that seek assistance from an outside firm to perform highly skilled monitoring and detection tasks. The advantages of this model include: quickest, simplest, most scalable, and cost-effective to implement. Since there are a wide variety of clients and industries that MSSPs (Managed Security Services Providers) typically support, the expertise and wealth of additional intelligence can be invaluable. The biggest difference between a classical SOC and one including MDR services is that these providers will not only detect and analyze threats but also respond to them. When a threat is detected, they will verify the criticality while responding and informing you about the incident.

The mixed SOC-MDR model allows monitoring and auditing of both pressing information security issues and complex anomalies. However, the main disadvantages are the complexity and high cost of implementation in practice. The SOC-MDR is based on the management of performance, security of data sources, competencies and verification of staff for immediate response to incidents when necessary. The main technologies of SOC-MDR are the incident management platform and knowledge base, which allow processing significant amounts of data per unit of time. The staff of such models consists of 10 or more employees. Significant disadvantages include the fact that some data will be handled through a third party and that this model can be costly to sustain long-term.

According to [3], there are 6 levels that describe the degree of maturity of the security operations model, which correspond to the respective levels of implementation of the enterprise security operations center. Table 1 lists these levels and provides a brief description of them.

Table 1 – Maturity levels of the security operations model

Security Operations Maturity Level	SOC level	Description
Level 0	Absent	Fundamental SOC elements are absent
Level 1	Initial	Monitoring is present, but process documentation is absent
Level 2	Basic	Monitoring is present, most of the processes are documented
Level 3	Appropriate	Processes are fully documented, constantly updated
Level 4	Meaningful	Regular assessment of SOC performance, restructuring processes to maximize efficiency
Level 5	Maximum	Maximum specification of processes, a plan for further modernization and restructuring of the SOC has been developed

III. Conclusion

Thus, as a result of all of the above, the implementation of an enterprise security operations center allows monitoring and auditing in 24x7 mode, blocking attacks in real time, quickly adapting to new attacks, investigating incidents and carrying out system modifications in accordance with its results, managing vulnerabilities, preserve investments in business, ensure the continuity of business processes, more accurately determine the cost of risks, security events and incidents [2].

REFERENCES

[1] Ушатов В. Проблеми оперативного виявлення і реагування на інциденти інформаційної безпеки / В. Ушатов, О. Сєвєрінов // GLOBAL CYBER SECURITY FORUM. Матеріали першого міжнародного науково-практичного форуму – Х.: ХНУРЕ, 2019. – С. 104-105.

[2] Демидов В. Организация оперативного управления киберезопасностью на производстве / В. Демидов, В Караваев // GLOBAL CYBER SECURITY FORUM. Матеріали першого міжнародного науково-практичного форуму – Х.: ХНУРЕ, 2019. – С. 45.

[3] Security Operation Center: роскошь или необходимость [Электронный ресурс] // IT.Integrator – 2018 – Режим доступа: https://it-integrator.ua/sites/default/files/imce/SecurityCisco/soc.pdf.

[4] Центр оперативного управления информацией: от идеи к реализации [Электронный ресурс] /// БМС консалтинг – 2013 – Режим доступа: https://pt.slideshare.net/sapran/ss-22866687?ref=&smtNoRedir=1

[5] Овчаренко М. Аналіз сучасних систем управління інформаційною безпекою та інцидентами безпеки / М. Овчаренко, О. Сєвєрінов // Проблеми інформатизації: Тези доповідей сьомої мужнародної науково-технічної конференції – Х.: НТУ «ХПІ», 2019 – С.102.