Implementation of a Security Operation Center - An Essential Cybersecurity Solution for Organizations

2023 27th International Conference on System Theory, Control and Computing (ICSTCC) | 979-8-3503-3798-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICSTCC59206.2023.10308432

Florin Mocanu[1], Luminița Scripcariu[1]
[1] "Gheorghe Asachi" Technical University of Iași, Romania
fmocanu@etti.tuiasi.ro

Abstract - **Cybersecurity is vital in our world that uses the public Internet to communicate in every field of activity. In this paper, we present a concise overview of a Security Operation Center (SOC) implementation that combines open source components and operates as a service (SOCaaS). The focus is on the case study of Security Onion, an open source security-monitoring platform, to highlight the effectiveness of this approach. The paper highlights the architecture, key features, and benefits of the SOCaaS model with open source components, emphasizing the integration of Security Onion's intrusion detection, network security monitoring, and log management capabilities. The case study demonstrates the practicality and scalability of Security Onion within the SOCaaS framework. It also addresses challenges and considerations, such as resource requirements, skill gaps, and data privacy. The paper offers insights into how organizations can leverage open source tools like Security Onion to enhance security operations while maintaining control and optimizing costs.**

I. Introduction

In a world where cyber threats are rapidly evolving, organizations face significant challenges in protecting their critical data and resources [1].

A Security Operation Center (SOC) is a critical component within any organization, providing an active line of defense against cyberattacks and ensuring business continuity [2].

A SOC is a center dedicated to monitoring, analyzing and managing security incidents to protect an organization against cyber threats [3]. By combining advanced technology, well-defined processes, and a team of cybersecurity experts, a SOC can quickly identify and respond to incidents to minimize the impact on the organization.

The advantages of implementing a SOC include:

a) Early detection of threats: A SOC can identify and assess threats in real time, thus enabling rapid intervention to prevent or limit the impact on the organization.

b) Reducing the risk of data breaches - through constant monitoring and analysis of activity, a SOC helps identify and remediate vulnerabilities, thereby protecting the organization's sensitive data.

c) Compliance and reporting - a SOC ensures that the organization complies with cybersecurity regulations and requirements, while facilitating effective reporting and auditing.

d) Improved response time - by having a cyber-specialist, a cybersecurity team and advanced technology, a SOC can respond quickly to the incident, reduce downtime and impact on the organization's operations.

e) Increasing security awareness among employees - implementing a SOC and integrating it into the culture of the organization helping to educate employees and increase awareness of the importance of cyber security.

After a brief introduction in SOC, Section II describes some open-source tools for SOC that can be all included in one single platform, *Security Onion*. Section III presents SOC implementation based on a distributed architecture. Section IV aims SOC as a service provided as a cybersecurity solution for organizations. Finally, conclusions and references end the paper.

II. Tools for SOC

Implementing a Security Operation Center is an important step in protecting organizations against ever-evolving cyber threats. By combining advanced technology, well-defined processes, and a team of cybersecurity specialists, a SOC can provide a high level of security and resilience for any organization. Ensuring that a SOC is integrated into the organization's culture and promoting security awareness among employees can significantly contribute to the long-term success and protection of an organization. However, the costs associated with implementing a traditional SOC can be prohibitive for many organizations. One solution to this problem can be the use of high-quality open-source tools that allow organizations to build their own SOC at a fraction of the cost of a commercial solution.

We can build an efficient and affordable SOC by combining the following but not limited to open-source tools [4]:

a) Suricata - a high-performance, open-source network intrusion detection and prevention system (NIDS/NIPS), capable of analyzing real-time traffic and generating alerts for suspicious activity.

b) Zeek - an open-source tool for network metadata analysis that provides a detailed view of network traffic, facilitating the detection and investigation of security incidents.

c) Stenographer - an open-source full packet capture solution that allows the recording (storage) and subsequent access of network traffic in order to identify, analyze and respond to cyber security incidents.

d) As Zeek and Suricata monitor network traffic, it is possible to extract files that are transferred over the network. These files can be further analyzed with the Strelka tool that scans and extracts information about suspicious files, providing additional metadata and facilitating threat identification and management.

e) Elastic Agent - an open-source endpoint monitoring and response solution that provides visibility into system activities and enables remediation and/or isolation (quarantine) actions.

f) Elastic Fleet - an open-source agent management system that allows centralized management of Elastic agents and security policies.

g) Elastic Stack: an open-source suite of solutions for data analysis and visualization, which includes the tools Elasticsearch (engine with advanced data indexing, search and analysis functions), Logstash (data processing tool that collects, transforms and sends data to Elasticsearch) and Kibana (web interface for viewing and exploring data stored in Elasticsearch).

Integrating these open-source solutions into a cybersecurity platform to implement a SOC can be a difficult task for certain organizations due to the complexity of the implementation, therefore it is preferable to identify a technical solution that integrates all the necessary tools in a single platform like *Security Onion*.

Security Onion is an open-source Linux distribution specifically designed for network security and traffic monitoring. By integrating the previously listed tools, the Security Onion platform offers a number of advantages including:

a) Cost savings - being an open-source solution, it reduces costs associated with licenses and support for commercial products.

b) Flexibility and customization - allows organizations to configure and customize their own SOC according to their needs and resources, without being limited by the restrictions imposed by commercial solutions.

c) Community and support - users benefit from an active community and online resources that provide support, documentation and instructions to help implement and use the solution effectively

d) Simplified integration - unified platform that integrates all the open-source tools listed above, facilitating the implementation and centralized management of a SOC.

e) Improved security - the platform allows organizations to benefit from a wide range of security tools and techniques, providing a high level of protection against cyber threats.

f) scalability - due to the open-source and modular nature of the platform, organizations can add and integrate new tools and technologies as they become available, ensuring their SOC stays abreast of cybersecurity developments.

Security Onion's distributed architecture enables scalability and flexibility in deploying the solution in different environments and scenarios.

III. Implementing a SOC

SOC implementation can use various architecture principles [5].

In a standard distributed deployment, Security Onion components are installed on multiple nodes (a Manager Node, one or more Forward Nodes, and one or more Search Nodes respectively), each with specific roles.

A. Manager Node

This node is responsible for coordinating all other nodes in the infrastructure. It hosts core services such as Elasticsearch, Logstash, Kibana, and Redis and manages system-wide security policy and configuration.

Currently, the minimum recommended hardware configuration for this type of node is: 4-8 processor cores, 16 GB of memory and 200 GB to 1 TB of disk space and can be virtualized.

The processor will be used mainly to take incoming events and place them in Redis, run all front-end web components and aggregate search results from the Search Node.

RAM will be used for Logstash and Redis, the amount of available RAM directly influences the Redis queue size and overall system performance.

Disk space is used for long-term data storage, including for general operating system purposes and for storing Kibana dashboards.

B. Search Nodes

These nodes are dedicated to process Elasticsearch queries and searches. They enable horizontal scaling of search and storage capacity, improving performance and reducing the time it takes to get results. The Search Node(s) consumes data from Redis, powered by the Manager Node.

The minimum hardware configuration recommended for this type of node is: 4-8 processor cores, 16-64 GB of memory and 200 GB or more disk space, depending on the desired retention period.

The processor analyzes and indexes the received events.

The RAM will be used by the Logstash, Elasticsearch, and disk cache components for Apache Lucence that is an open-source software library written in Java that provides advanced text search and indexing functionality. The required amount of RAM may vary depending on the volume of data and the complexity of queries and will have a direct impact on search speed and reliability.

Disk space is used to store indexed metadata, a larger amount of storage space allows for a longer retention period. It is not recommended to keep more than 30 days of Elasticsearch indexes that contain recent data and are heavily used for queries and writes (hot indexes).

C. Forward Node (Sensor)

The forward nodes also called *sensors* are responsible for capturing network traffic and generating logs from this traffic. Sensors may include components such as Meerkat, Zeek, and Stenographer.

These nodes send the captured metadata and generated logs to the Manager Node for processing and storage. The PCAP (Packet Capture) files containing the network traffic capture are stored on this node and are accessed through an agent.

The processor analyzes and stores network traffic. Suricata and Zeek are CPU intensive and as the bandwidth being monitored increases, more processing power is required. A rough estimate would be about 200 Mbps of network traffic per Suricata or Zeek thread or process. For example, if we want to use Suricata for NIDS (Network Intrusion Detection System) alerts and Zeek for metadata, in the case of a saturated data link of 1 Gbps, we will need at least ten processor cores for Suricata and Zeek and additionally other processor cores available for Stenographer and the other services. If the available resources are limited or a very large amount of traffic is monitored, for a more efficient use of resources, it is recommended to use Suricata for both alerts and metadata.

RAM will be used for packet processing and write cache (temporary data storage area in fast memory, used to optimize the speed of writing data to a storage device). The amount of RAM required depends on several variables such as active services, the type and amount of monitored traffic, and the percentage of packet loss accepted in the organization. If we deploy in production, in a large network (1 Gbps -10 Gbps), a sensor with all services - with Suricata for NIDS alerts, Zeek for metadata and Stenographer for FPC (Full Packet Capture), an estimated 128 GB up to 256 GB of memory is required. For higher performance, we recommend an additional amount of memory and disabling swap.

Disk space is used to store PCAP files. FPC-enabled sensor nodes require a lot of storage space. A larger storage size will allow for a longer retention period and the ability to have data available for investigations for a longer period of time. For example, if a data connection with an average transfer rate of 100 Mbps (12.5 MB/s) is monitored, it means that in one minute 750 MB are stored on the disk, then 45 GB in one hour, respectively approximately 1 TB of data in 24 hours.

D. Additional Nodes

Other nodes with specific use can be implemented, such as:

- *Elastic Fleet Standalone Node* - hosts the Elastic Fleet service that manages the Elastic Agent agents on the various terminals and devices in the network and allows the centralization of agent management and the application of security policies. It is necessary that all agents connect to this node, in order not to expose the other nodes to analysis, and, therefore, in complex infrastructures, installing it in the DMZ is recommendable.

  Intrusion Detection Honeypot Node - hosts honeypot Services or tokens designed to attract and detect attackers; the data captured by the honeypots is sent to the Manager Node to be analyzed and generate alerts

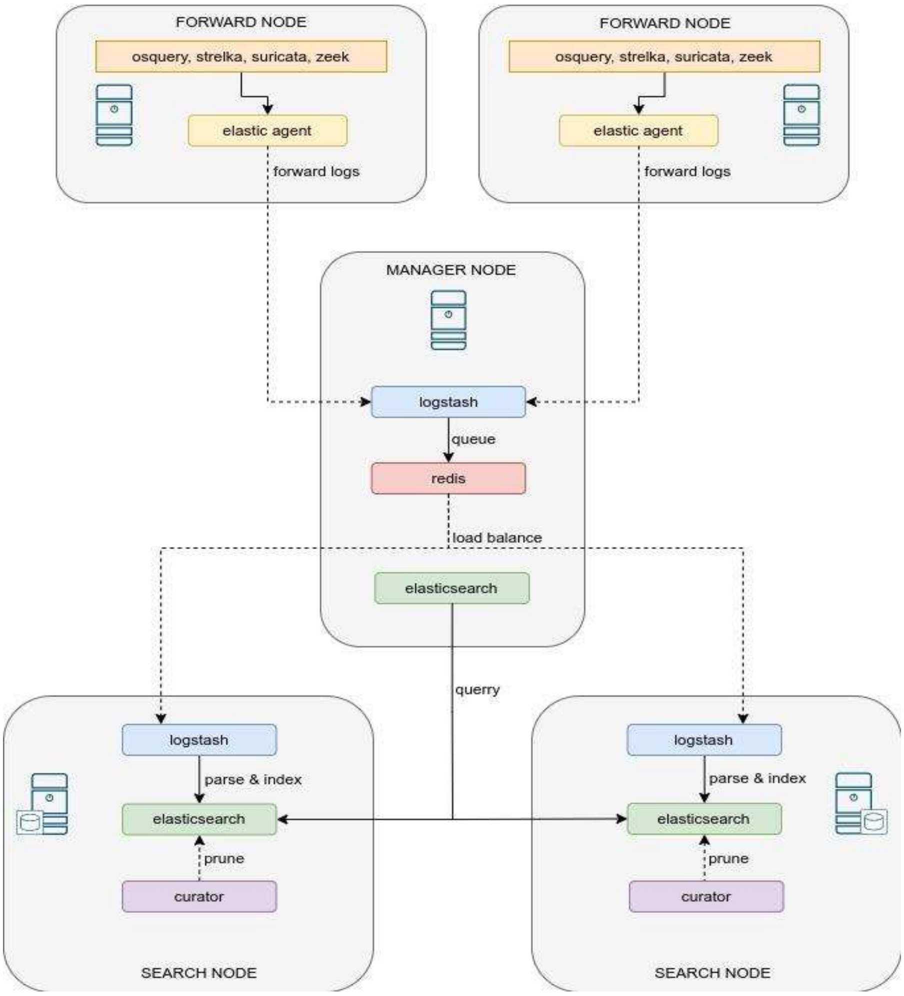

Figure 1. Example of a SOC distributed architecture.

based on suspicious activities. An "Intrusion Detection Honeypot" (IDH) is essentially a combination of two concepts (Intrusion Detection System and Honeypot) where the honeypot system is a part of an intrusion detection strategy. However, with the use of honeypots within the network, any interaction is likely to be illegitimate, as these assets are not meant to be used for authentic purposes. Thus, any activity is deemed suspicious, reducing the chance of false positives. This makes IDH a highly effective form of intrusion detection that necessitates minimal adjustments. This method can be adapted and scaled according to the needs of any organization, regardless of its size. For this type of node, the system requirements are minimal: 1 GB RAM, 2 CPU cores, 100 GB and 1 NIC.

An example of the standard distributed architecture, presented in Fig. 1, contains the manager node, two search nodes and two forward nodes.

Security Onion's distributed architecture allows organizations to adapt to various environments and requirements, providing a scalable and powerful solution for monitoring, analyzing and managing network and host security [6]. In the Security Onion platform, the data flow refers to the process of importing, transferring or collecting data from various sources and entering it into a system or database to be processed, analyzed and stored. The data flow may include importing raw data, transforming and processing it to match the structure of the target system, and ensuring data quality before storage. In the Security Onion platform, the data flow is a process that takes place in several stages:

a) Data collection

b) Data processing and storage

c) Data analysis and visualization.

To work effectively, the Security Onion platform must collect data from various sources.

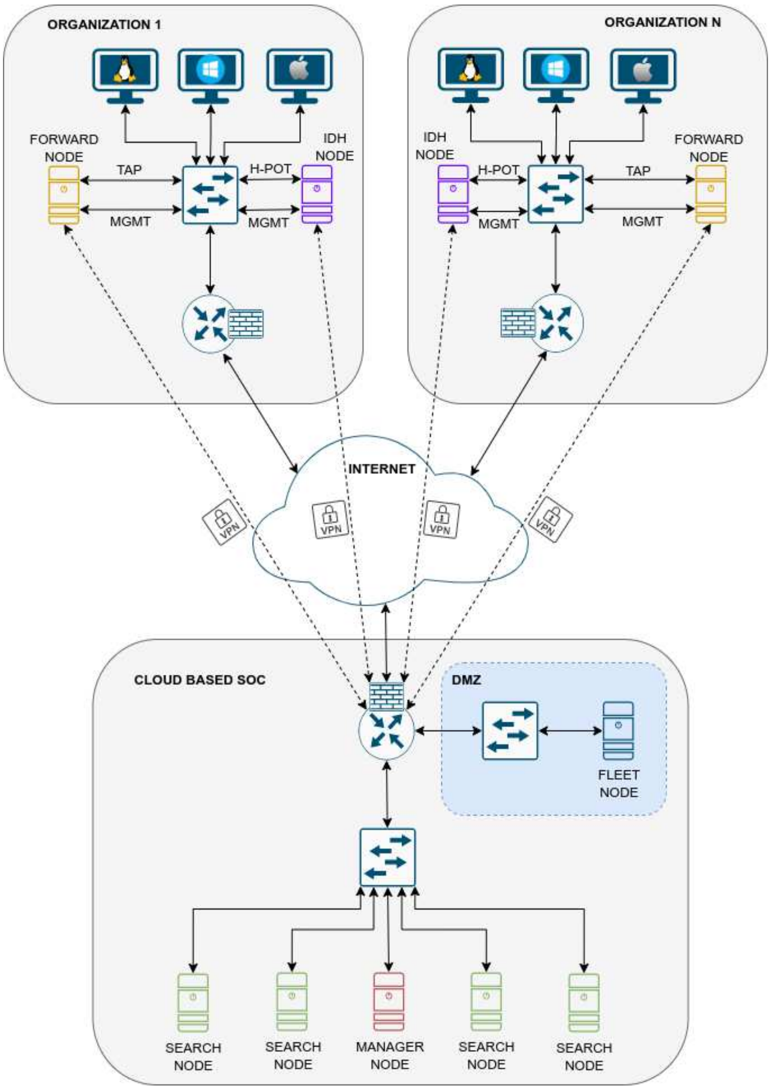

Figure 2. Example of a SOCaaS

These sources can be network equipment such as firewalls, routers and switches, or applications and operating systems such as web servers, databases and file systems. In addition, the Security Onion platform can collect and analyze logs from various applications and systems to detect suspicious behavior and unauthorized activity.

IV. Security Operation Center as a Service

There are many organizations that do not have the necessary resources to implement their own SOC, but they can adopt an outsourced solution for monitoring and managing IT infrastructure security, in the form of a service: SOCaaS (Security Operation Center as a Service) (Fig. 2).

SOCaaS allows organizations to benefit from the expertise and technologies needed to protect themselves against cyber threats, without having to invest their own resources in the analysis infrastructure - Manager, Search and Elastic Fleet Standalone Node(s), but possibly only in the infrastructure of acquisition of Sensor and Intrusion Detection Honeypot Node(s) [7].

Security Service Providers can set up IDH nodes as virtual machines. By using the VXLAN tunneling protocol, they have the capability to extend an organizational Layer 2 network over the Internet and integrate the virtual IDH nodes in it. To ensure data in transit is encrypted and authenticated, we encapsulate it in a Wireguard VPN tunnel, resulting a cost effective platform that detects and analyzes cybersecurity threats [8].

We use GNS3 Network Emulator to simulate and test this type of platform and validate our approach (Fig. 3). In our implementation, we use MikroTik routers that have a version intended to be used as a virtual machine instance.

In order to keep the compatibility with older networks, in the SSP network we create VLANs (one for each connected organization) and place a virtual machine acting as IDH in each VLAN.

Port e0 in SSP-SW switch configured as trunk transports VLANs to the SSP-RTR router.

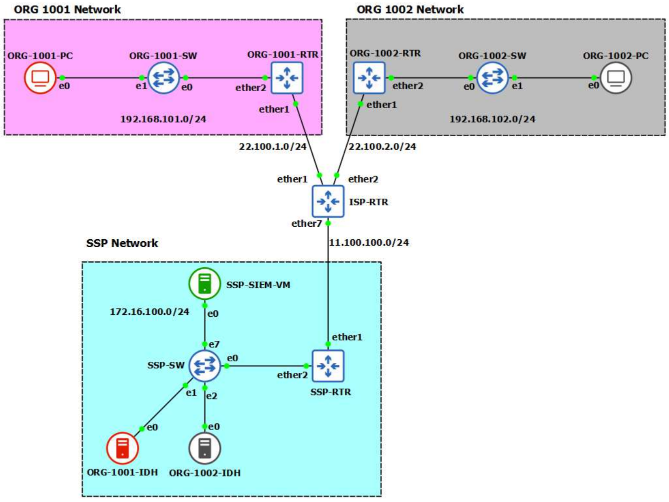

Figure 3. The network simulated in GNS3.

On the SSP router, we configure one bridge interface for each organization, and add the corresponding VXLAN and VLAN interfaces as bridge ports.

After configuring all devices, we test successfully the connectivity between IDHs and the organizations' networks.

The simulation shows that this security approach is a valid solution that can be provided to various organizations by the SSP. This solution integrates Security Onion as an open platform into SOCaaS to provide a complete suite of tools for monitoring, analyzing and managing network and host security:

- Security Onion Console (Alerts, Dashboards, Hunt, Cases, PCAP, Grid, Downloads, Admin)
- Kibana
- Elastic Fleet
- Osquery Manager
- InfluxDB
- Playbook
- ATT&CK Navigator.

The Security Onion solution integrates these tools into a unified and flexible platform, offering significant advantages in terms of cost, customization, community support and scalability.

V. Conclusions

This paper provides a brief overview of the benefits and considerations of implementing a Security Operation Center with open source components as a provided service (SOCaaS).

Implementing a Security Operation Center using open-source tools can provide organizations with a high level of cyber security at a significantly reduced cost compared to traditional commercial solutions. By adopting an approach based on open-source tools, organizations can build an efficient and affordable SOC capable of meeting the ever-evolving cybersecurity challenges but they also can use SOCaaS from specialized providers. The Security Onion case study highlights the effectiveness of this approach, providing valuable insights for organizations seeking to leverage open source tools for their security operations. We can use this approach to provide securely other domain services to an organization over the public network.

References

[1] C. J. Brooks, C. Grow, P. A. Craig, Jr., D. Short, Cybersecurity Essentials, John Wiley & Sons, 2018.

[2] M. Vielberth, F. Böhm, I. Fichtinger and G. Pernul, Security Operations Center: A Systematic Study and Open Challenges, in *IEEE Access*, vol. 8, pp. 227756-227779, 2020.

[3] M. Majid and K. Ariffi, Success factors for cyber security operation center (SOC) establishment, in Proc. 1st Int. Conf. Informat., Eng., Sci. Technol., Bandung, IN, USA, May 2019, pp. 1–11.

[4] SOCRadar, Top Open Source Solutions for Building Security Operations Center II, published online August 31, 2022, Available: https://socradar.io/top-open-source-solutions-for-building-security-operations-center-2/.

[5] S. Radu, ‘‘Comparative analysis of security operations centre architectures; Proposals and architectural considerations for frameworks and operating models,’’ in Innovative Security Solutions for Information Technology and Communications (Lecture Notes in Computer Science), vol. 10006. Cham, Switzerland: Springer, 2016, pp. 248–260.

[6] Security Onion Solutions, LLC, About Security Onion, 2023, Available: https://docs.securityonion.net/en/2.4/about.html#security-onion-solutions-llc.

[7] C. Sanders, Intrusion Detection Honeypots: Detection through Deception, Applied Network Defense, GA, USA, 2020.

[8] F. Mocanu, L. Scripcariu, “Intrusion Detection Platform with Virtual Honeypots,” International Symposium on Signals, Circuits and Systems, ISSCS 2023, Iasi, Romania, July 2023, pp. 1-4.