Building a Security Operations Center With Incident Response Capabilities

ABSTRACT

Given the prevalence of a wide variety of cyber attacks against businesses of all sizes, it is essential to ensure that adequate security monitoring of organizational assets and infrastructure is in place to ensure the early detection and response to security incidents. By using a security information and event management (SIEM) tool in collaboration with other security tools, such as an extended detection and response (XDR) tool, all housed in an organizational unit, adequate security monitoring and response to detected incidents can be achieved. This research proposes a SOC architecture with various components to ensure complete security visibility across endpoints and digital assets. Then, it proposes low-cost open-source tooling that can be used to implement this architecture. To validate the performance of this architecture, the architecture was implemented using the proposed tools, which included the Wazuh platform as the XDR and SIEM tool, TheHive for case management, and Suricata for network intrusion detection. Subsequently, various cybersecurity scenarios, such as brute force attacks, malware downloads, and DoS attacks, were executed against endpoints monitored by this deployed architecture. The results show that the tools implemented performed the correct exposure assessment and successfully detected and responded to the various scenarios. This paper proposed a security operations center architecture utilizing open-source tools and successfully implemented it to detect common cybersecurity attacks.

Keywords: Security operations center, security information and event management, incident response, extended detection and response, and open-source.

1. INTRODUCTION

In recent years, various cyber-attacks have plagued various businesses and organizations with increased frequency and sophistication. These attacks have ranged from denial of service attacks, SQL injection, and brute force attacks to ransomware attacks. They afflict organizations of various sizes, from small and medium enterprises to big organizations. The cost of cyber-attacks may run into millions of pounds, compromised privacy, and lost man hours. As a result, “businesses and government agencies are implementing security information and event management (SIEM) systems to better secure their employees and the public” [1].

Due to the impact of cyberattacks, every organization with digital assets needs to have a security plan for monitoring their infrastructure to detect intrusions and an incident response plan. According to the National Institute of Standards and Technology (NIST) cybersecurity framework core, “the five concurrent and continuous functions - Identify, Protect, Detect, Respond, Recover - provide a high-level, strategic view of the lifecycle of an organization’s management of cybersecurity risk” [2].

A security operations center (SOC) can help implement and meet the five functions of the NIST CF core. It is a centralized function within an organization that employs people, processes, and technology to continuously monitor and improve its security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents [3]. According to NIST, a cybersecurity incident is “a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices” [4].

It is important to note that the duties of a SOC involve monitoring, detecting, and responding to threats. However, there are scenarios where organizations do not have a SOC, or the SOC may be missing key capabilities such as responding to security incidents. The reasons for this vary from the cost of security solutions to the unavailability of a workable and scalable SOC architecture.

This paper presents a SOC architecture with incident response capabilities that uses open-source, free, or low-cost solutions. The architecture has a low barrier to entry and the ability to scale horizontally in the event of business growth. It is intended for small and medium businesses. The architecture includes automated incident response capabilities and mapping for personnel to man the SOC tools and platforms.

The preceding sections of this paper examined the background of the problem of architecting scalable security operation centers with incident response capabilities. Section 2 presents background information, literature review, and analyses of what a security operations center is. Literature from various authors on SOC design and incident response is reviewed to flesh out frameworks for building the SOC architecture. Section 3 lays out the research methodology and the materials used in this paper. Section 4 analyses the results of the implementation of the proposed architecture, and then conclusions and recommendations for future research on this topic are provided in Section 5.

2. LITERATURE REVIEW

In this section, a SOC's definition, structure, and components are reviewed and laid out. Additionally, what incident response is and the relations between incident response, human capital, and security operations centers are provided. To provide these pieces of information, we leverage existing research from other authors in security operations design, incident

response, and SOC personnel staffing by performing a literature review of articles by authors published in this field.

A security operations center (SOC) is a centralized place for monitoring and frequently managing the safety and security of the company's status. "The primary purpose of SOC is to enable better incident detection, investigation, and response capabilities by using data from endpoint devices, logs, security systems, and network flows" [5]. SOCs exist to improve the security of a business by having a birdseye view of all activities happening in an organization's infrastructure. While SOCs are not compulsory for all organizations, an operational SOC may be required from organizations operating in regulated sectors. The functions of a SOC include but are not limited to:

1. Monitoring of events generated by network and endpoint devices.
2. Detection of security incidents from the monitored events.
3. Investigating and responding to security incidents.
4. Detection of vulnerabilities and configuration weaknesses in organizational assets.
5. Log management of security events for investigations, audit purposes, or compliance requirements.

Vielberth et al. identified the following building blocks of a SOC [6] as people, processes, and technology. People to implement security solutions, monitor security tools, and incident response. Processes and guidelines for operating a SOC and responding to security incidents. Technology for tools employed to execute SOC processes, with various technologies mapping to different process sub-components. These technologies encompass monitored and protected entities, log sources, and SOC tools and solutions. This work does not examine the people component of the SOC as it is out of the scope of this paper.

A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices [4]. As such, incident response refers to the activities encompassing the preparation, identification, and execution of actions in relation to a cybersecurity incident or breach. Incident response is considered a SOC function. However, there is a challenge where responding to cyber attacks requires manual execution and human intervention. Incident response is tightly coupled with a SOC as monitoring analysts first detect the incidents before they are escalated for further investigation. "The computer security incident response team (CSIRT) is a centralized unit tasked with monitoring and identifying security problems in real-time" [1]. Once the security problems have been identified and resolved, the knowledge gained is documented and passed on to the monitoring analysts for future purposes.

Vielbert et al. [6] analyze the structure of a security operations center using the people, processes and technology, governance, and compliance framework. The various architectures of a SOC were outlined in the paper; after that, the constituent teams and personnel were also identified, and then the factors influencing the operation of a SOC were detailed to define what can be called state-of-the-art Security Operations Centres. Based on the research into SOC architectures, processes, and operating factors, the authors of this paper identified challenges affecting the people, processes, and technology in a SOC.

Schinagl, Schoon, and Paans [8] identified generic components for building a SOC and presented a model framework with five functions or building blocks: intelligence, baseline security, monitoring, penetration testing, and forensics.

Saraiva and Mateus-Coelho [1] reviewed various security operation center frameworks to understand the current state of CyberSoc frameworks. The authors analyze the required log sources for security operations and the typical execution flow of security incidents and SOC operations. A search was executed on IExplore to obtain a dataset of papers related to security

operations, CyberSoc, CSIRT, AI, SIEM, and cybersecurity framework for review. The results of the reviewed papers were concise layouts of the Cyber security operations center, interactions with the cyber security incident response team, a CyberSOC architecture, and the architectural components of a SIEM.

Miloslavskaya [9] highlights the roles SOCs play in handling and managing security incidents, particularly given the rise in the use of IoT devices and cloud computing. The paper highlights the duties of a SOC, such as event monitoring, analysis, incident detection, and response. Then, Miloslavskaya covers the requisite skills of SOC personnel and incident responders.

Shatnawi et al. [10] leverage an open-source solution for building a Security Operations Centre in the paper “Adaptable Plug and Play Security Operations Center Leveraging a Novel Programmable Plugin-based Intrusion Detection and Prevention System.” The components of a SOC architecture are outlined. Then, a plug-and-play SOC concept that can be deployed in different environments quickly with modifications only for integrating needed security components is proposed.

In [11], Abd Majid and Zainol Ariffin present factors and measures that can be used to identify a successful security operations center implementation. The identifiers included organizational support, personnel skill ratings, technological advancement and automation level, and continuous monitoring and coverage of organizational assets. Based on these SOC success identifiers, the authors proposed a five-stage model for developing a SOC, which includes the planning and preparation stage, design and infrastructure stage, implementation and integration stage, operation and maintenance stage, and finally, the continuous improvement stage.

3. MATERIALS AND METHODS

In this section, we examine some approaches to designing a low-cost security operations center with incident response capabilities and propose and implement our approach.

3.1 Previous SOC designs

According to the various literature reviewed, the general architecture of a security operations center entails collecting logs from web servers, application servers, mail servers, endpoints, and various user activities to a central source, where they are analyzed, correlated, and compared against rulesets and various metrics to identify and determine if a malicious activity has occurred.

In [1], the authors proposed the architecture in Figure 1 below, which summarizes the proposed components of a SOC and their interactions with each other.

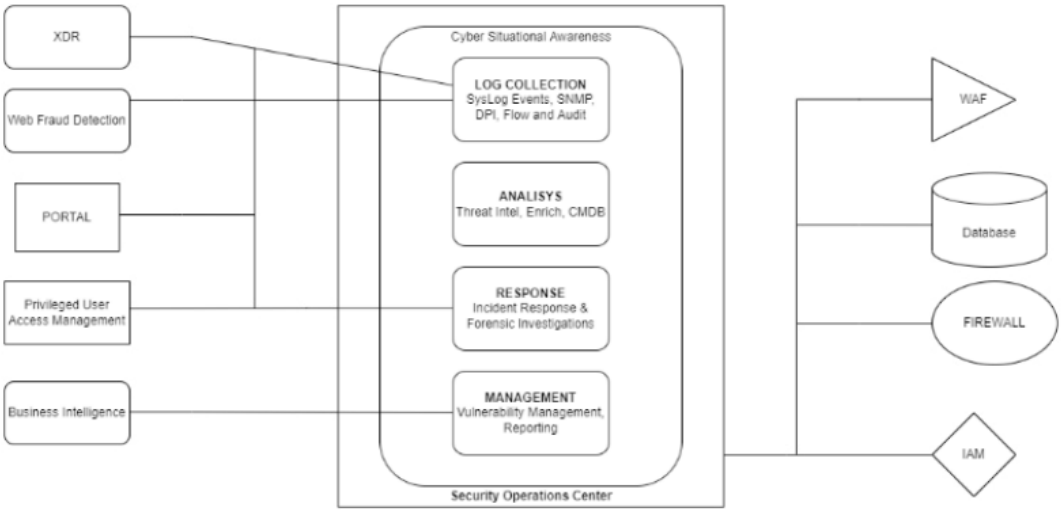

Fig. 1: CyberSOC architecture according to Saraiva and Mateus-Coelho.

The architecture had log collection, analysis, response, forensic investigation, and management components. However, it was missing the configuration assessment, compliance monitoring, automated incident response, and inventory components.

The framework for building a SOC in [8] had intelligence, baseline security, monitoring, penetration testing and forensics as its five functions. It did not provide the interactions for log collection from the different log sources or incident response, compliance, and inventory components. Figure 2 below shows the architecture.

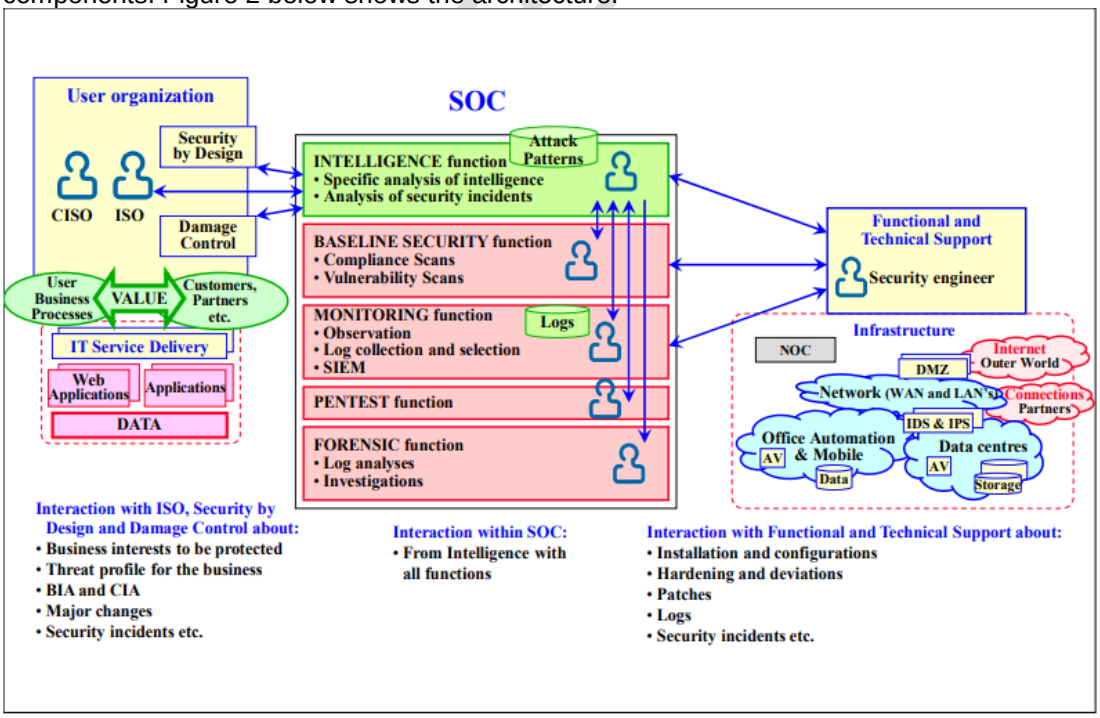

Fig. 2: SOC architecture according to [8].

3.2 Proposed SOC design

A SOC architecture is proposed in various stages based on the previous SOC designs outlined above and the missing components identified. Then, the architecture is subsequently implemented using suitable components.

3.2.1 SOC components and their sub-components

From the literature review, the functions of a SOC can be classified into three components: people, processes, and technology. The following sections look at the processes and technologies in a SOC architecture. The people component of the SOC is not covered in this research paper.

3.2.1.1 Processes

For the processes of a SOC, it is possible to use the Incident Response Lifecycle of the NIST Computer Security Incident Handling Guide to identify the processes of a SOC as preparation, detection and analysis, containment, eradication and recovery, and post-incident activity [4]. Based on these processes, SOC sub-components are assigned.
In the context of SOC operations and design, we determined that the preparation process involves identifying the scope of the organizational infrastructure to protect, then implementing tools processes and drawing up plans to protect it. A SOC operation's detection and analysis process analyzes logs ingested and other artifacts collected from the infrastructure to determine its security state and identify intrusions, misconfigurations, or possible vulnerabilities that may be exploited. The containment, eradication and recovery process in a SOC involves containing and responding to the security incidents identified in the detection and analysis processes run with a view to ensuring full recovery of the infrastructure affected to optimal capacity. In the post-incident activity process, an analysis is carried out on all the prior processes executed for security events and the infrastructure. Reports are drawn up, and cases are opened and closed as necessary; then, further monitoring is done to ensure that the fixes implemented were successful and do not affect the business's confidentiality, integrity, or availability. Based on the information on the SOC processes above, Table 1 below maps the children of the SOC processes component to SOC sub-components. It should be noted that some sub-components span across multiple SOC processes.

Table 1: Proposed SOC subcomponents mapped to the various processes.

SOC sub-component	Description	Processes
Log collection	Collecting and storing logs, events, and security data logs generated by various systems and applications within an organization's infrastructure.	Preparation
Asset inventory	Identifying applications, processes, devices, and assets in an organization.	Preparation
Threat intelligence	Gathering and analyzing information about potential and current cyber threats that could affect an organization's security.	Preparation, detection and analysis, post-incident activity.

Configuration assessment	Validation of system configuration against recommended configuration standards.	Preparation, detection and analysis, containment, eradication and recovery
Log analysis	Analysis of collected logs to identify potential security threats, anomalies, or suspicious activities.	Detection and analysis
Security monitoring	The logs collected and analyzed, configuration changes, and the entire infrastructure are monitored here.	Detection and analysis, post-incident activity.
Incident response	Responsible for responding to security incidents such as cyber-attacks or data breaches.	Containment, eradication, and recovery
Vulnerability management	Identification, prioritization, and remediation of vulnerabilities in an organization's infrastructure.	Detection and analysis, containment, eradication and recovery
Forensics	Investigating, collecting, and preserving any data and information involved in security incidents.	Containment, eradication, and recovery.
Reporting	Reports on an organization's security posture, such as vulnerabilities, incidents, and compliance status.	Post-incident activity.
Compliance monitoring	The responsibility for ensuring that the organization complies with relevant laws, regulations, and standards related to information security lies here.	Post-incident activity.

3.2.1.2 Technology

Here, the technologies used to execute the SOC processes running in the sub-components are identified and mapped to the various sub-components. The technologies identified were:

1. **SIEM tool**: The information provided by the SIEM provides visibility into possible security incidents in an infrastructure. The collection and analysis of the security data is done in near real-time. Security data can be collected through a variety of means. Some devices may send their security data via Syslog, while others may need a log collector agent from the SIEM tool provider to send the logs to the SIEM tool. It is featured in the operations of log collection, log analysis, security monitoring, forensics, and reporting of sub-components of the SOC.
2. **Asset inventory tools**: These tools will be used to determine and keep track of the various applications, processes, and devices running in an organization's infrastructure.

3. **Intrusion detection systems**: Detects malicious or unauthorized activities in network traffic or system activity. It does this detection by analyzing packets, logs, and/or system events and matching them to patterns or signatures of known attacks or abnormal behaviour that may point to malicious activity.
4. **Compliance monitoring tool**: This tool will help monitor devices to determine whether they adhere to regulatory compliance frameworks and standards.
5. **Threat intelligence platform**: This platform will allow analysts to correlate activities in the organizational infrastructure seen in the SIEM with threat activities and other IOCs found in the wild. The platform will factor in the threat intelligence operations, forensics, log analysis, and security monitoring sub-components.
6. **Configuration assessment tool**: To ensure that workstations, servers, and other devices are correctly configured, it is necessary to compare their existing configurations against established secure configuration standards and detect when the configurations change.
7. **Incident response and case management tools**: Used in investigating security incidents, opening cases to track these incidents, and managing the security incident lifecycle.
8. **Vulnerability detection tools**: These tools audit workstations, servers, and other devices to identify vulnerabilities in installed operating systems and packages.

In the subsequent implementation sections, we identify low-cost tools to perform the tasks as mentioned earlier efficiently.

3.2.2 Architecture

To craft an architecture containing all the sub-components, we analyzed the operational flow of the SOC from when an event is received to when it is resolved. The identified architectural interactions are as follows: The components and sub-components of the SOC ingest data from various data sources, devices, workstations, and servers to monitor the infrastructure. The data ingested is collected using the log collector and agents, which generally fall under the log collection module. These logs collected are subsequently analyzed in the log analysis sub-component using technologies like IDS and SIEM, and enriched with information from the threat intelligence platform. The analyzed logs are then monitored using the Security monitoring module for indicators of attack and compromise.

The threat intelligence platform feeds the security monitoring sub-component with information on new and ongoing attacks and trends. While monitoring the logs from the security monitoring component using the SIEM tool, an incident response is executed if any security incidents are detected. In this research, the incident response is automated for common categories of cyber security incidents. The vulnerability management, asset inventory, configuration assessment, and compliance monitoring sub-components check workstations, servers, and other devices to determine their vulnerability status, running processes and services, operating system information, and configuration state and verify if they meet compliance requirements. This is achieved through agents and sensors on the monitored endpoints.

The forensics sub-component utilizes information from all the other components to identify the causes of security incidents and propose mitigations to those issues. The reporting subcomponent generates reports from all the other subcomponents, such as vulnerability management, security monitoring, asset inventory, compliance monitoring, threat intelligence, and configuration assessment subcomponents.

3.3 Implementation

This section of the paper deals with choosing the tools and platforms for implementing the technologies for the various components and sub-components in the proposed architecture.

3.3.1 Implementation phases

The implementation is in two phases as follows:

1. Phase 1 - Tooling, platform selection, and operational architecture design.
2. Phase 2 - Operational architecture infrastructure specification, implementation, configuration, and preliminary testing.

3.3.2 Phase 1 - Tooling, platform selection, and operational architectural design

The different specific tools and platforms to implement the SOC technologies and processes above are identified in this research stage. The license type, usability, versatility, and integration with third-party tooling were factors considered when choosing the tooling for the SOC technologies identified earlier because this architecture is geared towards small and medium-sized businesses with the capacity to scale. Based on this selection criteria, we ended up with the following core technologies to implement:

1. XDR tool.
2. SIEM tool.
3. Case management tool.
4. Intrusion detection system.

All the above tools have been introduced except the XDR tool. An XDR is a security platform that collects security data from various devices and security solutions to automate threat detection, investigation, compliance, configuration assessment, and incident response. It has become an increasingly essential platform due to the “increasing complexity of several products from various manufacturers, together with the number of alerts generated, could easily overload businesses, particularly considering a systemic shortage of cybersecurity skills” [12]. Due to the versatility of the XDR platform, it would cover a wide range of SOC components such as configuration assessment, compliance monitoring, threat intelligence integration, log collection, vulnerability detection, and incident response. Subsequently, this paper illustrates the operational architecture for integrating these tools to create a functional SOC. It is expected that in the operational architecture, the XDR agent on the devices, workstations, and servers will perform log collection, configuration assessment, vulnerability detection, and compliance monitoring while reporting to a centralized XDR server ingesting threat intelligence data with SIEM capabilities for security monitoring. A case is opened in the case management system where security incidents are detected. Subsequently, automated incident responses are sent to the monitored endpoints and executed by the XDR agent residing on them.

3.3.2.1 The specific products

1. SIEM + XDR: Wazuh was chosen as the XDR solution because it was free, open-source, scalable, and had a wide range of operability on many platforms and automated threat response. Wazuh is an open-source security platform that “unifies historically separate functions into a single agent and platform architecture” [13]. It integrates host-based intrusion detection (HID), log analysis, security information and event management (SIEM), file integrity monitoring, and automated threat response capabilities. The Wazuh XDR's platform architecture in Figure 3 below shows that it operates in a client-server architecture with the client having an agent running on it to perform configuration assessment, file integrity

monitoring, log collection, malware detection, system inventory, and active response, among other capabilities.

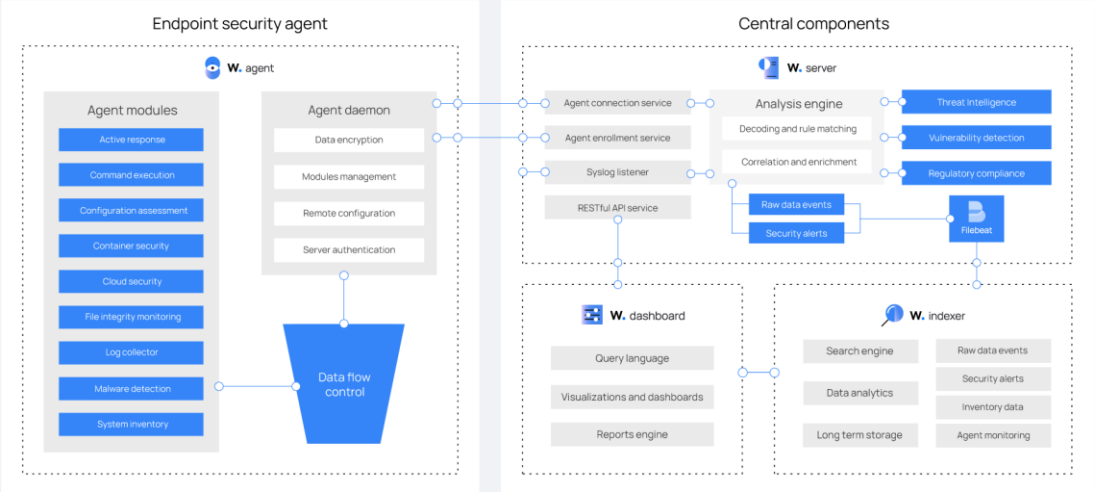

Fig. 3: Wazuh architecture [13].

2. Case management: The chosen case management and incident response platform is TheHive. “TheHive is a scalable Security Incident Response Platform, tightly integrated with MISP (Malware Information Sharing Platform), designed to make life easier for SOCs, CSIRTs, CERTs and any information security practitioner dealing with security incidents that need to be investigated and acted upon swiftly” [14]. It is open-source, free, and integrates with multiple security solutions.

3. Intrusion detection system: To choose an IDS, open-source security intrusion detection solutions - Suricata, Snort and Zeek - were evaluated. Eventually, **Suricata was chosen** for this study because of its broad features, superior performance, and customization capabilities. It can also be integrated with external platforms such as an XDR. Suricata supports network traffic monitoring on hosts. It is fast and multi-threaded, thus making it ideal for real-time network traffic analysis to detect network attacks and other malicious activities.

3.3.3 Phase 2 - Operational architecture infrastructure specification, implementation, configuration, and preliminary testing.

This section covers the requirements for deploying the security platforms identified for the SOC and their subsequent operationalization and integration with each other. The tools were all deployed on individual virtual machines, each running an Ubuntu 22.04 server, a minimum of 2GB of RAM, 70GB of storage, and 2 vCPUs. It should be noted that these specifications should be increased for a production deployment.

The Wazuh XDR/SIEM solution was deployed using its all-in-one installation script, which was run on an Ubuntu 22.04 server. Then, agents were installed on the endpoints to be monitored. To receive advanced intelligence on logs and activities from events occurring in an organizational infrastructure, Virustotal was integrated using the out-of-the-box integration module and a Virustotal API key.

Subsequently, TheHive was deployed to carter for the SOC's case management, incident response, and forensic subcomponents. After the platform's initial set-up, it was integrated with Wazuh using an API key and a custom Python script [15].
Finally, Suricata was installed on the monitored endpoints to collect network flows and send them to Wazuh.

3.5 Testing

To ensure that the SOC architecture with the incident response plan implemented above works, select cybersecurity attacks with a high occurrence rate will be executed against endpoints in our infrastructure, and we will observe the response to those attacks. Brute force login attempts, SQL injection, DoS attack, downloaded malware detection, vulnerability detection, threat intelligence, system misconfigurations, compliance reporting, and system inventory were some tests run against the soc endpoints to validate its performance.

4. RESULTS AND DISCUSSION

In this section, the proposed architecture and the performance of its implementation is evaluated.

4.1 Results of the SOC Architecture Proposed and Implemented

A SOC architecture was proposed from the research and analysis of existing architecture and SOC security detection and scenario needs. The proposed SOC architecture at various stages is presented in the following sections.

4.1.1 Theoretical architecture

The theoretical architecture proposed in this work seeks to satisfy security requirements missing from other SOC designs reviewed in section 3.1. As evidenced in Figure 4, this architecture is well-rounded. It incorporates log monitoring, threat intelligence, asset inventory, configuration assessment, compliance monitoring, and automated incident response to detect and respond to security issues.

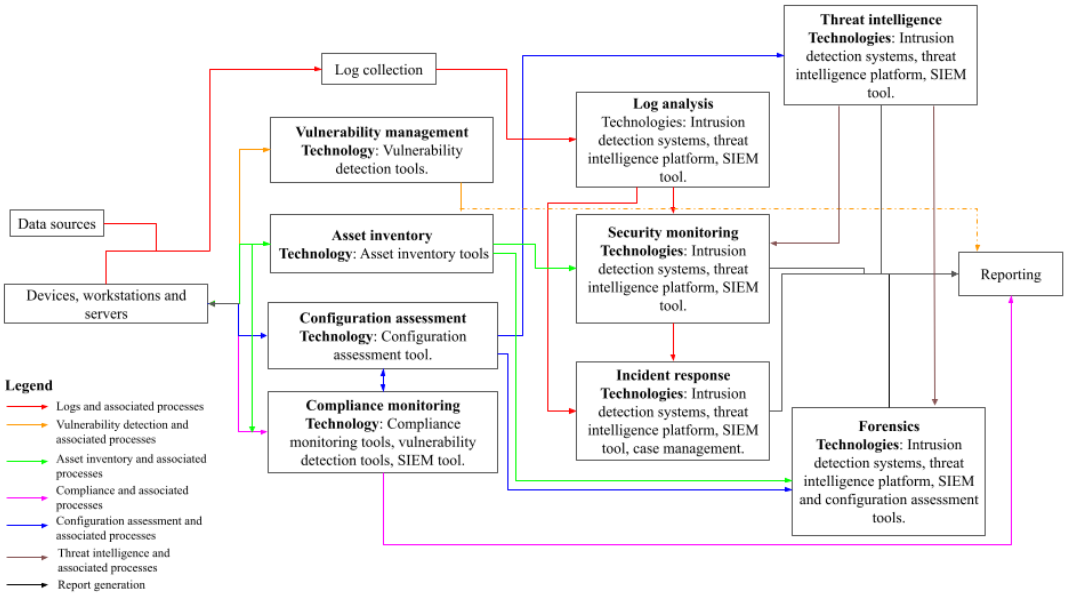

Fig. 4: The theoretical architecture of the SOC

4.1.2 Operational architecture

Based on the theoretical architecture proposed above, to provide a generic operational architecture that would meet the needs of small businesses and avoid the requirements of purchasing multiple tools, the components, and processes of the SOC architecture were mapped to four tools: XDR, SIEM, case management, and intrusion detection system tools. The consolidation of the functional architecture into an operational architecture resulted in Figure 5 below:

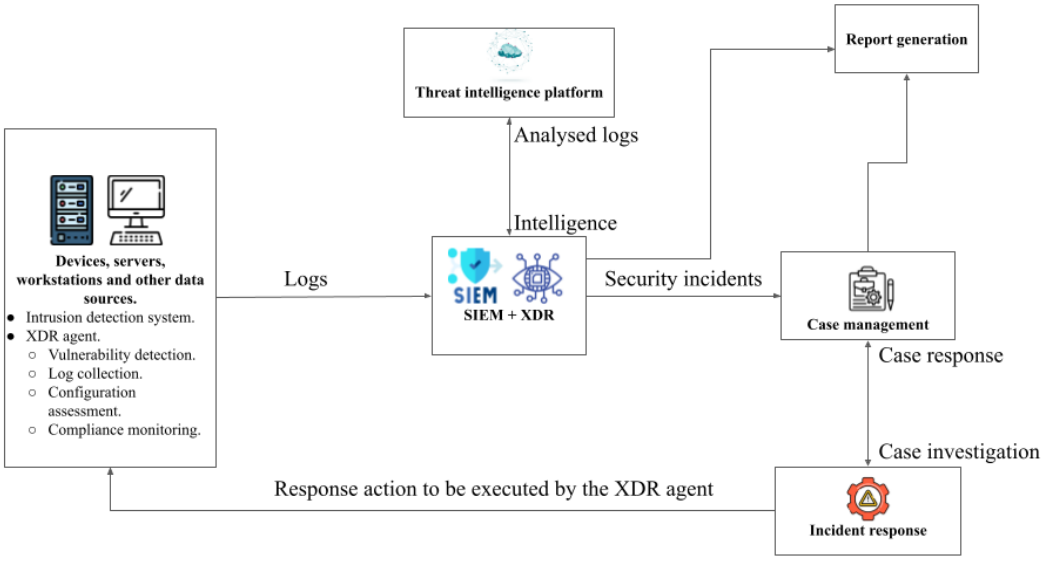

Fig. 5: Result of the consolidated SOC operational architecture.

After mapping the processes and components to various tooling, specific products were identified to be leveraged in executing the roles of those tools. The products identified had to meet the criteria of ease of use, low cost, almost free licensing, and extensibility and integration with other security solutions. The results of the mapping of the tools, the chosen products, and their license costs are defined in Table 2 below:

Table 2: Mapping of the SOC products to SOC components and their licensing costs.

S/N	Tool	SOC components	Product	Cost
1.	Extended detection and response (XDR)	Incident response, threat intelligence, vulnerability management, configuration assessment, compliance monitoring, asset inventory, and forensics.	Wazuh	Open-source and free.
2.	Security information and event management (SIEM)	Security monitoring, forensics, incident response, and compliance monitoring.	Wazuh	Open-source and free.
3.	Case management and incident investigation	Incident response, forensics, compliance monitoring.	TheHive	Open-source and free.
4.	Intrusion detection system	Security monitoring, log collection, log analysis, forensics.	Suricata	Open-source and free.

By inserting the platforms selected into the appropriate positions in the operational architecture, the result is the architectural diagram in Figure 6 below used to implement our low-cost SOC.

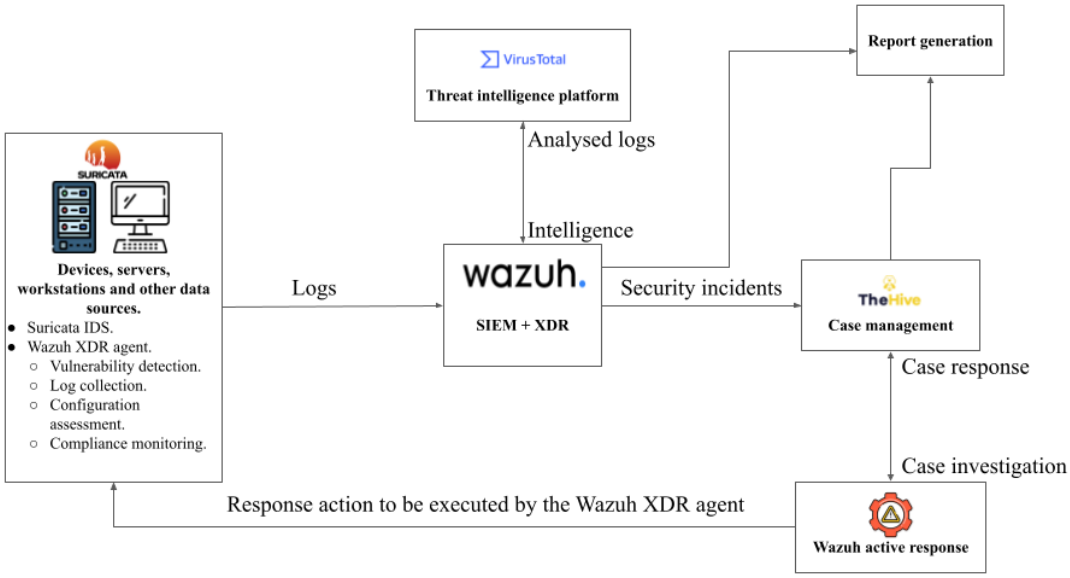

Fig. 6: The implemented consolidated SOC operational architecture.

4.2 Detection and Response Results for The Various Cybersecurity Scenarios

For each cybersecurity scenario, attacks were simulated against an endpoint monitored by the deployed SOC. Then, the SOC dashboards were checked to determine if the scenario was detected, and where necessary, a case was opened and an incident response initiated. Table 3 below shows the detection and response results of the cybersecurity scenarios run.

Table 3: Detection and response results.

Scenario	Detection	Incident Response
Brute force login attempt	Yes	Yes
SQL injection	Yes	Yes
DoS attack	Yes	Yes
Downloaded malware detection	Yes	Yes
Vulnerability detection	Yes	N/A
Threat intelligence	Yes	N/A
System misconfigurations	Yes	N/A
Compliance reporting	Yes	N/A

System inventory	Yes	N/A

Based on the logs collected by the Wazuh log collector and analyzed by the Wazuh log analysis engine, when multiple SSH logins failed in a short time, the events were detected as malicious, and a security alert was triggered; then the Wazuh active response component terminated the connection and blocked the malicious IP address. Cases were also opened in TheHive for this incident. Similarly, when an SQL injection, DoS attack, and malware were executed on a monitored node, the activities were identified and reported, cases opened, and the relevant automated incident response was executed. Utilizing the vulnerability detection module, the applications, packages, and operating systems running on the endpoints were audited for patch status. Additionally, the systems were evaluated for compliance with CIS benchmarks by the Wazuh agent for configuration assessment. The various compliance modules of Wazuh were used to meet the compliance reporting sub-component of the architecture, and network interfaces and open ports on each endpoint were identified using the system inventory module.

4.3 Comparison of Results with Existing Literature

While preparing this research, existing literature exploring security operations center designs was explored. The architecture proposed in this work draws on various existing architectures, such as the frameworks proposed by Saraiva and Mateus-Coelho and Schinagl, Schoon, and Paans, all of which include log collection, analysis, security monitoring, and incident response sub-components. However, this architecture diverges in several vital aspects. Unlike the others, it separates the threat intelligence function from log analysis to provide standalone threat intelligence to SOC analysts while using it for log enrichment and threat hunting. It also includes a configuration assessment module, which is absent in Saraiva and Mateus-Coelho's framework, to ensure devices adhere to security standards. Moreover, this architecture features a compliance monitoring component for regulatory requirements like PCI DSS, HIPAA, NIST, and GDPR, which is missing in the other frameworks. Additionally, it incorporates a case management solution for handling security incidents, a feature not present in the compared frameworks. Furthermore, it details personnel interactions with specific SOC components, offering a depth of specification absent in Schinagl, Schoon, and Paans' work. Finally, it identifies specific free and open-source tools for implementing the architecture. It demonstrates its application through various cybersecurity scenarios, a level of practical guidance not provided in existing literature.

5. CONCLUSION

This work identified the problem of small or medium-sized organizations not having a plan or infrastructure to perform security monitoring on their organisational digital assets and respond to any detected security incidents. A security operations center (SOC) is universally accepted as an organizational, technological unit for monitoring an organization’s security posture. A SOC exists primarily to analyze data from various sources for security incident detection, investigation, and response to detected threats. This paper proposed a theoretical architecture for a security operations center with incident response using free and open-source solutions and subsequently operationalized it. The results of the proposed SOC architecture showed an architecture that improves existing literature by incorporating incident response, case management, compliance monitoring, and configuration assessment sub-components. The operational architecture was tested against various cybersecurity scenarios. The results of the various cybersecurity scenarios show that the proposed architecture, tools used for the implementation, and the implementation itself were sufficient to meet a wide range of cybersecurity scenarios and execute automated incident responses for various detected scenarios. Automated deployment of the SOC technologies, benchmarking the tools used in

the proposed architecture, and integrating the SOC with artificial intelligence are areas for future research.

CONSENT

Not applicable.

ETHICAL APPROVAL

Not applicable

REFERENCES

1. Saraiva, M. and Mateus-Coelho, N. (2022). CyberSoc Framework a Systematic Review of the State-of-Art. Procedia Computer Science, [online] 204, pp.961–972. doi:https://doi.org/10.1016/j.procs.2022.08.117.
2. NIST (2014). Framework for Improving Critical Infrastructure Cybersecurity. Available at: https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf.
3. Habte, F. (2020). What is SOC (Security Operation Center)? [online] Check Point Software. Available at: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-soc/#:~:text=The%20function%20of%20the%20security,cyber%20threats%20around%20the%20clock. [Accessed 6 Mar. 2023].
4. Cichonski, P., Millar, T., Grance, T. and Scarfone, K. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. Computer Security Incident Handling Guide, [online] Rev. 2. doi:https://doi.org/10.6028/nist.sp.800-61r2.
5. Feher David Janos and Dai, P. (2018). Security Concerns Towards Security Operations Centers. IEEE 12th International Symposium on Applied Computational Intelligence and Informatics, May 17-19, pp.273-278.
6. Vielberth, M., Bohm, F., Fichtinger, I. and Pernul, G. (2020). Security Operations Center: A Systematic Study and Open Challenges. IEEE Access, 8, pp.227756–227779. doi:https://doi.org/10.1109/access.2020.3045514.
7. Bourgeois, J., Abdoul, K. G., Kotenko, I. and Ulanov, A. (2007). Software environment for simulation and evaluation of a security operation center in Information Fusion and Geographic Information Systems. Lecture Notes in Geoinformation and Cartography, Springer, pp.111–127.
8. Stef Schinagl, Schoon, K. and Paans, R. (2015). A Framework for Designing a Security Operations Centre (SOC). 2015 48th Hawaii International Conference on System Sciences (HICSS). pp.2253–2262.
9. Miloslavskaya, N.G. (2016). Security Operations Centers for Information Security Incident Management. 4th International Conference «Future Internet of Things and Cloud» (FiCloud 2016), Vienna (Austria). IEEE, pp.131–136.
10. Shatnawi, A., Al-Duwairi, B., Almazari, M., Alshakhatreh, M., Khader, A. and Abdullah, A. (n.d.). Adaptable Plug and Play Security Operations Center Leveraging a Novel Programmable Plugin-based Intrusion Detection and Prevention System. Available at: https://arxiv.org/ftp/arxiv/papers/2204/2204.04576.pdf [Accessed 13 Mar. 2023].

11. Abd Majid, M. and Zainol Ariffin, K.A. (2021). Model for successful development and implementation of Cyber Security Operations Centre (SOC). PLOS ONE, 16(11), p.e0260157. doi:https://doi.org/10.1371/journal.pone.0260157.
12. George, A. S., George, H., Baskar, T., and Pandey, D. (2021). XDR: The Evolution of Endpoint Security Solutions - Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future. International Journal of Advanced Research in Science Communication and Technology (IJARSCT), 8(1), pp.493–501. https://doi.org/10.5281/zenodo.7028219
13. Wazuh (2024). Wazuh - Open Source XDR. Open Source SIEM. [online] Wazuh. Available at: https://wazuh.com/ [Accessed 10 Jun. 2024].
14. Thehive-project.org. (2019). TheHive Project. [online] Available at: https://thehive-project.org/ [Accessed 10 Jun. 2024].
15. Wazuh and Awwal Ishiaku (2022). Wazuh and TheHive: Protection and incident response | Wazuh. [online] Wazuh. Available at: https://wazuh.com/blog/using-wazuh-and-thehive-for-threat-protection-and-incident-response/ [Accessed 9 Jun. 2024].
16. Agyepong, E., Cherdantseva, Y., Reinecke, P. and Burnap, P. (2023). A systematic method for measuring the performance of a cyber security operations centre analyst. Computers & Security, 124, p.102959. doi:https://doi.org/10.1016/j.cose.2022.102959.
17. Anderson, R. J. (2001). "Security Engineering: A Guide to Building Dependable Distributed Systems", Second Edition, Wiley Publishing.
18. Bilal, A. and Kowalski, S. (2016). A Framework and Prototype for A Socio-Technical Security Information and Event Management System (ST-SIEM). 2016 European Intelligence and Security Informatics Conference (EISIC), August 17-19. doi:10.1109/EISIC.2016.049
19. Brown S., Gommers J. and Serrano O. (2015). From cyber security information sharing to threat management. Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security, pp.43-49 https://doi.org/10.1145/2808128.2808133
20. Coppolino, L., Sgaglione, L., D'Antonio, S., et al. (2022). Risk Assessment Driven Use of Advanced SIEM Technology for Cyber Protection of Critical e-Health Processes. SN COMPUT. SCI. 3, 16. https://doi.org/10.1007/s42979-021-00858-4
21. Hassan, R., Maxime Syrame and Bourgeois, J. (2013). Protecting Grids from Cross-Domain Attacks Using Security Alert Sharing Mechanism. [online] ResearchGate. Available at: https://www.researchgate.net/publication/234057531_Protecting_Grids_from_Cross-Domain_Attacks_Using_Security_Alert_Sharing_Mechanism [Accessed 1 Apr. 2023].
22. Jabez, J., and Muthukumar, B. (2015). Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach. Procedia Computer Science, 48, pp.338-346. https://doi.org/10.1016/j.procs.2015.04.191
23. Rosso, M., Campobasso, M., Gankhuyag, G., Allodi, L. (2022). Digital Threats: Research and Practice (DTRAP). (2022). SAIBERSOC: A Methodology and Tool for Experimenting with Security Operation Centers. Digital Threats: Research and Practice, 2(3) pp.1–29. doi:https://doi.org/10.1145/3491266.