SentinelJC: An Open-Source Tool for Cyber Incident Management in a Military Institution

Henry Marino Chuquisengo Acosta, Eng[1]; Jhonny Paul Castro Basilio, Eng[1]; Carlos Quinto Huamán, PhD[2]; Juan Godoy Caso, PhD[1]; and Percy Fortunato Ochoa Castillo, PhD[1]
[1]Grupo de Investigación en Ciberseguridad, IoT e Inteligencia Artificial (GriCIA), Instituto Científico y Tecnológico del Ejército, Lima, Perú, *hchuquisengoa@icte.edu.pe, jcastrob@icte.edu.pe, jgodoyc@icte.edu.pe, pochoac@icte.edu.pe*
[2]Universidad Privada del Norte, Lima, Perú, *carlos.quinto@upn.pe*

Abstract*– Currently, organizations manage complex IT infrastructures characterized by a large number of interconnected devices. While interconnectivity provides operational advantages, it also complicates the control and detection of cyberattacks, increasing the likelihood of cybersecurity incidents. Such incidents can damage strategic objectives, cause financial losses, affect reputation, and steal confidential information. In a military institution, it is crucial to protect sensitive assets that may be targets for breaches of national security. These assets include not only strategic facilities but also classified information, advanced technological systems, and critical operational capabilities. In this context, this article presents SentinelJC, an open-source cybersecurity incident management tool that enables the Joint Command of the Armed Forces of Peru (CCFFAA) to manage events, incidents, and vulnerabilities based on the NIST framework with four key functions: prevention, detection, response, and recovery. Tools such as Security Onion and Wazuh are used for proactive threat detection, while iTop is employed for incident tracking and documented management. During a seven-day trial conducted to validate the tool, early detection of incidents and threats was achieved, allowing for optimized infrastructure security. This approach significantly contributed to reducing the risk of attacks and enhancing the response capability to cybersecurity incidents.

Keywords: Cybersecurity, Cybersecurity Incidents, Security Operations Center, NIST, Open Source Tools.

I. Introduction

Cybersecurity incident management is essential to ensure the security and operational continuity of organizations. In particular, government entities, which are a fundamental part of the global economy, face significant challenges in protecting against cyberattacks due to a lack of resources and specialized personnel. If not managed effectively, cybersecurity incidents can result in significant financial losses, damage to reputation, and disruption of operations. Fortunately, open-source cybersecurity tools offer an accessible and cost-effective solution to improve security, allowing businesses and organizations to implement protective measures without requiring substantial investments in commercial solutions [1][2]. According to [3], data collected by FortiGuard Labs, Fortinet's threat intelligence laboratory, indicates that Mexico was the Latin American country with the most attack attempts, receiving 156 billion, followed by Brazil with 88.5 billion, Peru with 11.5 billion, and Colombia with 11.2 billion. An incident combining espionage and cyber-exploitation of national interest information by a foreign actor, such as the SolarWinds case in 2020, is notable. The closest example would be the extraction of information by the hacktivist group Guacamaya from the Armed Forces of Chile, Colombia, El Salvador, Mexico, and Peru, and its dissemination on the Enlace Hacktivista portal in 2022. This incident had a moderate impact on the internal political sphere of each country, revealing how Latin American nations have yet to fully grasp the international revolution unfolding in cyberspace [4].

This article proposes a tool for cybersecurity incident management based on open-source tools, aligned with best practices established by the National Institute of Standards and Technology (NIST). The framework follows the incident management lifecycle phases proposed by NIST, which include prevention, detection, response, and recovery [3]. These phases provide a solid structure to address security incidents and ensure an appropriate response at all stages of the incident lifecycle. This tool incorporates open-source applications such as Security Onion, Wazuh, and iTop, each playing a crucial role in implementing a comprehensive incident management system. Security Onion offers advanced intrusion detection and network visibility capabilities, using technologies like Suricata and Zeek to identify suspicious traffic patterns and potential intrusions [3]. Wazuh, on the other hand, handles security monitoring, vulnerability management, and automation of incident response [5]. Additionally, iTop plays a key role in configuration management and incident documentation. iTop is an open-source tool designed for managing IT infrastructure and coordinating operational processes, allowing organizations to maintain a detailed record of cybersecurity incidents, their impact, and the actions taken to resolve them. By integrating iTop with other cybersecurity tools, traceability and configuration management can be enhanced, enabling a more efficient response to incidents [4].

The proposed tool is structured to follow NIST's phases, starting with the prevention of incidents through continuous security event monitoring and the collection of relevant data. In the detection phase, tools like Security Onion and Wazuh allow the identification of anomalous behaviors and potential threats. In the response phase, iTop facilitates the documentation and tracking of each incident, ensuring efficient and organized management. Finally, the recovery

phase relies on continuous improvement, using the collected data to strengthen defenses and prevent future incidents [6][7]. The goal of this work is to provide a government entity, such as the Joint Command of the Armed Forces of Peru (CCFFAA), with a practical and accessible solution for cybersecurity incident management, based on open-source tools and aligned with NIST's best practices. Additionally, the tool aims to improve security posture, reducing the risk of cyberattacks and ensuring operational continuity through efficient and scalable incident management.

This paper is structured into six sections, with the first being the current introduction. Section II briefly describes some concepts regarding tools for cybersecurity incident management. Section III reviews related work on the phases of the incident management lifecycle proposed by NIST. Section IV presents the proposed method. Section V describes the experiments and results. Finally, Section VI presents the conclusions of this work.

II. TOOLS FOR MANAGING CYBER INCIDENTS

The management of cyber incidents is a crucial aspect for protecting critical infrastructures and ensuring the operational continuity of any organization, especially in the military and national security sectors [3]. Incidents can arise at any time and in various forms, ranging from cyberattacks to system failures or security breaches. Therefore, having specialized tools to manage these incidents effectively is essential to minimize their impact and ensure a swift and efficient response. Incident management tools allow for the identification, classification, and structured response to threats, optimizing resources and reaction times. These solutions range from monitoring and detection software to platforms for coordinating responses and conducting post-incident forensic analysis [3]. In this way, not only are incidents managed effectively, but valuable information is also gathered to strengthen security policies and prevent future risks.

A. Open-Source Tools

Open-source software solutions have publicly available source code, which allows users to access, modify, and distribute the software according to their needs. These tools are fundamental in the field of cybersecurity as they offer flexibility, transparency, and a collaborative model that facilitates continuous improvement of solutions, promoting innovation and reducing costs. Moreover, they are highly customizable and adaptable to different environments [11]. Table 1 presents a comparison of the advantages and disadvantages of these tools versus commercial tools.

TABLE I
COMPARISON OF OPEN-SOURCE CYBERSECURITY TOOLS VS. COMMERCIAL CYBERSECURITY TOOLS

attribute	Open-Source Tools	Open-Source Tools
Cost	Generally free or low-cost.	Can have significant costs for licenses and renewals.
Customization	Highly customizable and allows modifying the code according to needs.	Customization or modification is not always possible.
Support	Depends on user communities, forums, and online communities.	Usually has dedicated support and specialized technical assistance.
Ease of Use	May have a considerable learning curve and require advanced technical skills.	Typically has an easy-to-use interface and requires fewer specific technical skills for setup.
Compatibility	May present compatibility issues with other programs or systems.	High compatibility with a wide range of systems.
Documentation	Varies greatly in terms of quantity and quality.	Provides detailed and specific documentation.
Innovation	A constant source of innovation with regular updates and community contributions.	May be slower to adopt new technologies and innovations.
Scalability	May be less scalable for large enterprises and robust environments.	Usually designed with scalability for business environments in mind.

B. Security Onion, Wazuh, and iTop

Security Onion is an open-source platform that integrates multiple cybersecurity tools, such as intrusion detection systems, network traffic analysis, and event monitoring, to provide a comprehensive security monitoring and analysis solution. Primarily used in corporate and governmental network environments, it allows administrators to identify, investigate, and respond to security incidents in real time, facilitating the detection of threats and the efficient management of events [3]. Wazuh is a security incident monitoring and response platform that uses a security information and event management (SIEM) approach. Integrating features such as intrusion detection, log analysis, and compliance monitoring, Wazuh enables organizations to protect their IT infrastructures by providing real-time visibility into security events, improving incident response, and ensuring compliance with data protection regulations [6]. iTop is an open-source IT service management (ITSM) solution that enables organizations to efficiently manage their technological resources and services. Through an intuitive interface, iTop facilitates the administration of incidents, service requests, change management, and IT infrastructure configuration. Its ability to integrate with other platforms and its flexibility make it a key tool for optimizing IT management processes [4].

C. Cybersecurity

It encompasses the measures taken to protect a computational system and the integrity of its data from hostile actions. Cybersecurity is conceived as a state of integrity, determined by the presence or absence of intrusion into an information system and its functions. It is also of vital importance for the security and survival of a nation's information [7]. Among the primary vulnerabilities to which organizations are exposed are those related to the infiltration of security systems, which are detailed in Table 2.

TABLE II
TYPES OF CYBERSECURITY ATTACKS

Type of attack	Description
Malware	Refers to software designed with malicious intent, such as trojans, spyware, and viruses. It allows unauthorized access to confidential information or disrupts critical infrastructure.
Ransomware	A model and associated technologies used by criminals to extort money from organizations by locking or threatening to expose their data.
Man-in-the-Middle Attack	Occurs when an external entity attempts to gain unauthorized access to a network during data transfer, increasing vulnerabilities to sensitive information, like financial data.
Phishing	A cyber threat using social engineering to deceive users into revealing personal information, such as credit card details, often via fake websites or malicious email attachments.
DDoS	A Distributed Denial-of-Service attack where multiple systems send excessive requests to a server, blocking legitimate users' access to it.
Insider Threat	Refers to security risks posed by individuals within an organization who misuse their elevated access privileges to compromise the system's security from the inside.

D. PCAP Files

A file extension used by network analyzers such as Tcpdump, libpcap, or Wireshark, containing traffic data over a specific period. To conduct traffic analysis, it is necessary to extract relevant information from the "PCAP" file, focusing on key fields for each analyzed IoT protocol [8].

E. Security Operations Center (SOC)

SOC teams are responsible for monitoring and protecting an organization's assets, including intellectual property, personnel data, business systems, and brand integrity. The SOC team implements the organization's overall cybersecurity strategy and serves as the central point for coordinated efforts to monitor, assess, and defend against cyberattacks [9].

F. Information Security and Event Management

A set of tools that provide a centralized view of an infrastructure's security. Specifically, a SIEM is software that offers the following capabilities: real-time visibility into security system data, log management from various sources, event correlation logic, and methods for notifying security issues [3].

III. STATE OF THE ART

In recent years, cyberspace has become a fundamental element in people's lives, ranging from simple communication to education, and increasingly for entertainment and the economy, generating a dependency essential for the functioning of society. In the military context, cyberspace has been proposed as the fifth operational domain due to the dependence on Information and Communication Technologies (ICT). A systematic review of the literature confirms the dependence on cyberspace in many countries, prompting a reconsideration of defense policies and the development of capabilities in this new operational domain, with the goal of establishing a doctrine for cyber defense to serve as the foundation for military strategies focused on our reality [10]. In [11], the authors examine the growing vulnerability of small businesses in Colombia to cyberattacks and propose the implementation of open-source cybersecurity tools as a solution. Through a systematic literature review, the advantages and disadvantages of these tools are identified and analyzed, with the result suggesting that these tools require technical knowledge for proper implementation. Their use strengthens online security for small businesses, helping mitigate cyber risks and threats. In [12], the design and implementation of a distributed Security Onion architecture were conducted, successfully monitoring network traffic to study vulnerabilities. Malicious traffic was injected into the platform's detection system using PCAP files, which allowed for the confirmation of successful attack detection. Phishing and malware attacks were detected, enabling alerts to be sent for future attempts before impacting the network. In the study, log data was collected over seven days, resulting in 8,523,612 logs, categorized by the tool generating them: 7,160,825 logs from Zeek (84% of the total), 23,521 logs from Suricata, 1,339,204 logs from Ossec, and 62 logs from Osquery. The main objective was incrementally achieved, providing deeper insight into network operations and security measures, and valuable experience with a variety of tools, including Kibana, Zeek, Suricata, and Security Onion. The results indicated that the network had sufficient security measures in place to prevent most attacks. In [13], the author explains the implementation of an open-source incident recording tool at the National Cybersecurity Center (CNSD). Given the common occurrence of technological incidents, the main goal was to establish efficient incident tracking control. An affordable solution was found in TheHive (version 4.0), an open-source software that offers various benefits. This system stands out for its modular design, facilitating integration with other tools like MISP (threat intelligence platform) and Cortex (analysis engine). The system was implemented on Amazon Web Services (AWS), a suite of cloud computing tools and services. As a result, the system enables effective and organized control of registered technological incidents. In [14], an effective framework for addressing cyber incidents in public entities in Bolivia is established, based on the ISO 27035 standard. This model promotes a collaborative approach, covering the detection, reporting, and resolution of incidents while facilitating coordination among the response team (CSIRT) members through clearly defined roles, such as triage officer and incident manager. The model's implementation, supported by tools like Request Tracker, has significantly improved incident management efficiency, optimizing both response time and the number of incidents addressed. Results since January 2022 show that incident handling increased as the model was applied, from a minimum of 8 incidents to a maximum of 141 incidents. The importance of applying best practices in information security is highlighted to mitigate vulnerabilities inherent in systems developed by humans, fostering an organizational culture

focused on continuous improvement in cybersecurity. In [15], significant cybersecurity deficiencies in Latin America are identified, highlighting the lack of national policies to address cyber threats affecting both national security and foreign policy in the region. The research is structured into six sections, ranging from theoretical approaches to a comparative analysis of the global context of cyber threats and the current state of cyber capabilities in Latin America. Despite some individual efforts, most countries remain in a "gray area" in terms of cybersecurity, underscoring the urgent need to develop comprehensive policies that strengthen collaboration at both the national and international levels. In 2019, 1,802 cyber events were recorded across multiple countries, including 298 cases of cyber warfare, hacktivism, and cyber espionage. Kaspersky Lab reported over 746,000 daily malware attacks in 2020, equating to 9 attacks per second. Brazil, Mexico, and Colombia were the most affected countries, representing 89.26% of incidents in the region. Additionally, 66% of the 62 million attacks detected in 2020 were related to theft from private and commercial entities, while the remaining 34% targeted criminal activities and government systems. In [16], small and medium-sized enterprises (SMEs) also play a significant role in the landscape of cyberattacks. Many of these companies tend to neglect information security and their technological infrastructure. According to studies by EIT Digital, Huawei, and the Global Digital Foundation, by December 2022, 57% of SMEs in Europe were forced to close their operations due to cyberattacks. In [17], the researchers present an exploratory study on vulnerabilities in government websites that manage sensitive information. Using the Acunetix software, they randomly analyzed ten government sites and applied statistical analysis to the results. The findings revealed that 5% of the detected vulnerabilities were high-risk, with one site showing 2,905 faults. A positive correlation was also observed between the number of scanned elements and the number of vulnerabilities, suggesting that the greater the number of elements, the higher the risk. In [18], cybersecurity in Industrial IoT devices is critical to preventing cyberattacks that could affect production and the integrity of systems. Implementing preventive and corrective measures is essential to protect industrial infrastructure against evolving cyber threats. This research aims to identify common vulnerabilities, develop protection strategies, and establish guidelines to mitigate cyberattack risks. It also emphasizes the need for ongoing collaboration between manufacturers, operators, and cybersecurity experts to ensure effective protection of IoT devices in the industrial sector. Findings regarding security vulnerabilities associated with IoT systems indicate that authentication problems have a critical point of 30%, with the most significant negative impact being on IoT systems in the industrial field. In [19], information security is increasingly important in the business world, where both large and small companies must consider the benefits and risks of having or not having a security plan for cases of cyberattacks. This study proposes securing small businesses using open-source software like PFsense, which acts as a protective shield against external and internal threats. The results from using this software to protect against cyber threats show positive outcomes, with a high level of effectiveness. According to Kaspersky's 2021 report, Ecuador experienced a 75% increase in cyberattacks, equating to approximately 89 attacks per minute. After integrating and applying the cybersecurity solution over a ten-day period in a small business case study, positive results were found with a high level of effectiveness.

IV. Development of the Proposal

This paper proposes the implementation of SentinelJ, an open-source tool that performs network monitoring and analysis functions, providing a comprehensive platform for security incident detection and response in networks by combining multiple monitoring and analysis functions. To achieve this, the integration of three open-source tools, Security Onion, Wazuh, and iTop, is carried out as a framework to enhance the ability to detect cyber incidents within the Joint Command of the Armed Forces, as detailed in Figure 1.

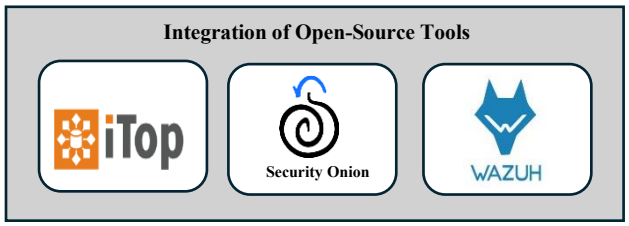

Fig. 1 Integration of three tools

To carry out the proposal, three continuous phases are followed, as shown in Figure 2. Phase 1 consists of planning, where an analysis of the cybersecurity policies, minimum software and hardware requirements, roles and responsibilities of the work team, tool selection, training plan, definition of the study's objective, and architecture proposal are conducted. In Phase 2, the proposal development takes place, involving the installation and configuration of the tools in the CCFFAA network environment. Finally, in Phase 3, testing is carried out, performing thorough tests to validate the correct functionality of the tool. These phases allow for a comprehensive and continuous evaluation of the proposal, ensuring its long-term viability.

Fig. 2 Phases of the Proposal

A. Planning Phase

A.1. Analysis of Information Security Policies

In this phase, the information security policies implemented in the CCFFAA were analyzed to identify vulnerabilities and security gaps. This analysis ensures compliance with policies and confirms that the new tool aligns with the organization's existing standards and procedures. Table 3 shows the analysis of the CCFFAA information security policies, where a clear focus is established to protect cyberspace by prioritizing the defense of critical infrastructure. These policies are regularly updated to address emerging threats and focus on three main priorities: protecting critical infrastructure, defending against cyberattacks, and securing sensitive information. To implement these priorities, action areas are defined, including access control and authentication, threat monitoring and detection, and personnel training. These actions aim to mitigate risks and strengthen the CCFFAA's ability to respond effectively to security incidents in an ever-evolving digital environment.

TABLE III
ANALYSIS OF CCFFAA INFORMATION SECURITY POLICIES

Priority	Action Areas
Protection of Critical Infrastructure	Access Control and Authentication
Protection of Critical Infrastructure	Threat Monitoring and Detection
Information Security	Training and Education

A.2. Minimum Software and Hardware Requirements

A comprehensive analysis of the technical requirements for hardware and software was carried out to install the tools Security Onion, Wazuh, and iTop to ensure that the systems have the necessary infrastructure to operate correctly. This step is crucial to ensure that everything is ready for smooth implementation (See Table 4).

TABLE IV
HARDWARE AND SOFTWARE REQUIREMENTS

Hardware	Security Onion	iTop	Wazuh
CPU	4 cores	2 cores	2 cores
RAM	8 GB	2 GB	4 GB
Storage	200 GB	10 GB	10 GB
OS	Linux	Linux	Linux/Windows

A.3. Roles and Responsibilities of the Team

The roles and responsibilities of the team using the tool were established to ensure that each member understood their specific function and how they would contribute to the success of the implementation. This is essential to ensure a smooth implementation process and to meet the established expectations (See Table 5).

TABLE V
ROLES AND RESPONSIBILITIES

Role	Responsibilities
Head of IT Support and Statistics Office (OSIE)	Authorization for the installation of the information security tool.
Head of Administrative Systems Unit (USA)	Management of IT equipment.
Head of Information Security	Responsible for installing the information security tools.
Head of Technical Support	Maintain the operational functionality of IT equipment.

A.4. Tool Selection

A comparison was made with three tools for detecting IT incidents: Suricata, Wazuh (both open-source tools), and Check Point (a subscription-based commercial suite).

TABLE VI
COMPARISON OF TOOLS FOR IT INCIDENTS

Criteria	Suricata	Security Onion	Wazuh	Check Point
Cost	Free (Open Source)	Free (Open Source)	Free (Open Source)	Commercial (Subscription License)
Network Monitoring	Yes	Yes	No	Yes
Endpoint Monitoring	No	No	Yes	Yes
Application	Network Traffic Analysis	Comprehensive Monitoring and Response Solution	Log Management and Auditing	Comprehensive Monitoring and Response Solution
Main Function	Intrusion Detection (IDS/IPS)	Intrusion Security Analysis (IDS/IPS), Log Monitoring, Network Traffic Analysis	Intrusion Detection (IDS/IPS) and Log Management	Complete Network Security Suite
Integration	Integrates via APIs and Plugins	Integrates multiple Open-Source Tools into one platform	Integrates via APIs and Plugins	Integrates all components into one platform
Complexity	Medium Requires command-line knowledge	Medium Requires Linux knowledge	Medium Requires Linux knowledge	Low (User-friendly tool)

Table 6 demonstrates that the commercial tool Check Point offers comprehensive monitoring and response solutions that meet all required expectations, enabling SOC personnel to manage the tool easily due to its low complexity, technical support, and updates, making it an ideal product but at a high cost. Moreover, Security Onion, as a free open-source alternative, integrates a variety of tools like Suricata, Kibana, and Zeek. Combined with Wazuh's Endpoint Monitoring capabilities, these tools complement the security measures required by the SOC. After analyzing the tools, it can be determined that Security Onion is a good cost-effective solution, offering integration with other tools.

A.5. Training Plan

This training plan is designed to prepare the SOC team for the effective use of Security Onion, Wazuh, and iTop, ensuring that they are equipped to manage the security of IT systems efficiently (See Table 7).

TABLE VII
TRAINING PHASES

Phase	Task	Frequency
Phase 1: Familiarization	Familiarize the team with basic cybersecurity concepts and the functionality of Security Onion, Wazuh, and iTop.	2 days
Phase 2: Installation and Configuration	Train the team on the installation and configuration of Security Onion, Wazuh, and iTop, ensuring they understand technical requirements and best practices.	2 days
Phase 3: Control and Monitoring	Develop skills for controlling and monitoring the tools, including managing alerts, log analysis, and incident response.	1 day

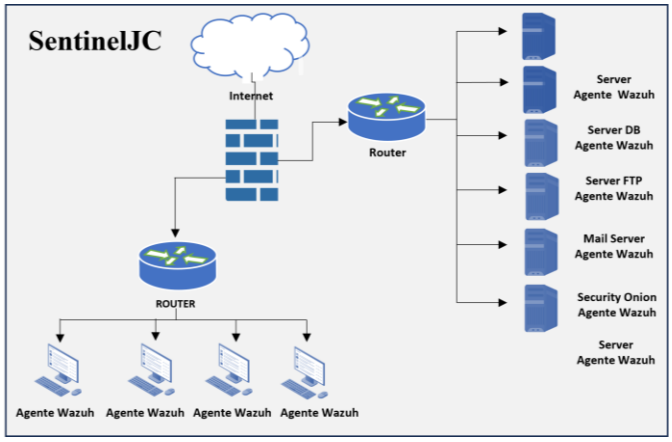

Fig. 3 Network Architecture

A.7. Architecture

Security Onion, Wazuh, and iTop form an integrated IT security system that operates at multiple levels to protect an organization's infrastructure. Security Onion acts as the first line of defense by monitoring network traffic and analyzing packets in real-time to detect intrusions. Wazuh, on the other hand, provides host-based monitoring, evaluating system integrity and correlating alerts with those generated by Security Onion, offering a more comprehensive view of incidents and facilitating malware detection. Finally, iTop manages the incidents generated by both tools by creating tickets, enabling analysts to track and document corrective actions, which is essential for effective threat response and IT asset management (See Figure 3).

B. Development Phase

The development of the proposal follows the procedures outlined in Algorithm 1. The process begins with the verification of technological requirements and the network infrastructure of the CCFFAA, followed by the installation of the necessary tools. First, Security Onion is installed, configuring the network interfaces and detection tools to ensure effective monitoring of network traffic. Then, Wazuh is installed, where detection rules are configured to identify potential threats and Wazuh agents are registered in the network. It is crucial that Wazuh is properly integrated with Security Onion to enable effective network traffic analysis. Subsequently, iTop, the incident management tool, is integrated to create and track tickets generated by the alerts from Security Onion and Wazuh. Next, user profiles and roles are configured to ensure that each team member has controlled access to the functionalities of the tools. Finally, the correct integration and operation of the tools are validated, confirming that incidents generated by the alerts are efficiently managed through iTop, ensuring the proper operation of the security infrastructure in the CCFFAA environment.

Algorithm 1: Tool Development

Input: *L*: Technological requirements, CCFFAA network environment
Result: *SentinelJC*: Configured and integrated tools, user profiles and roles established, agents registered, incidents managed

1. **Procedure** DEVELOPTOOL (*L*)
   Install and configure Security Onion
   Install and configure Wazuh for threat detection
   Integrate iTop for incident management
   Establish user profiles and roles
2. **Function InstallSecurityOnion()**
   Verify technological requirements
   Install Security Onion in the network environment
   Configure network interfaces and detection tools
3. Function IntegrateITop()
   Integrate iTop for managing incidents generated by alerts
   Configure incident ticket creation and tracking
4. **Function EstablishProfilesAndRoles()**
   Create user profiles
   Assign appropriate roles for controlled access to tools
5. **GenerateResults()**
   Confirm correct integration and operation of the tools
   Verify efficient incident management in iTop
6. **End procedure**

In Figure 4, the installation of Security Onion and its configuration for integration with Wazuh is shown. Figure 5 presents the creation of user profiles and roles. Figure 6 details the registration of agents in Wazuh, and Figure 7 shows the incident registration in iTop.

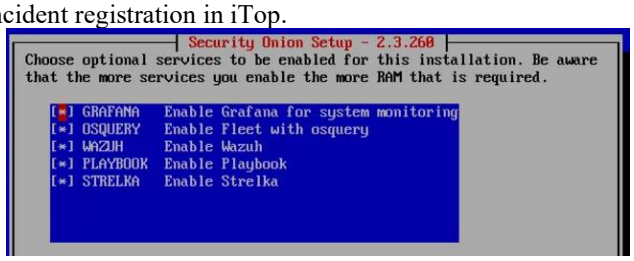

Fig. 4 Configuration of Tools in Security Onion

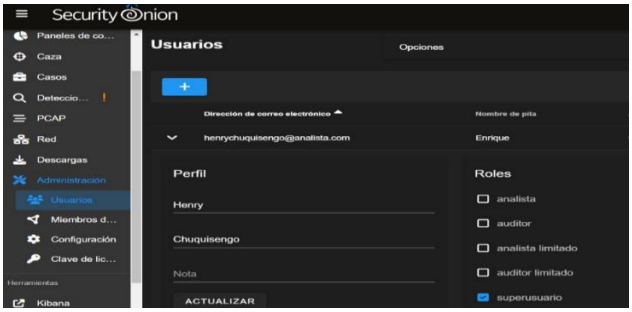

Fig. 5 Creation of User Profiles and Roles

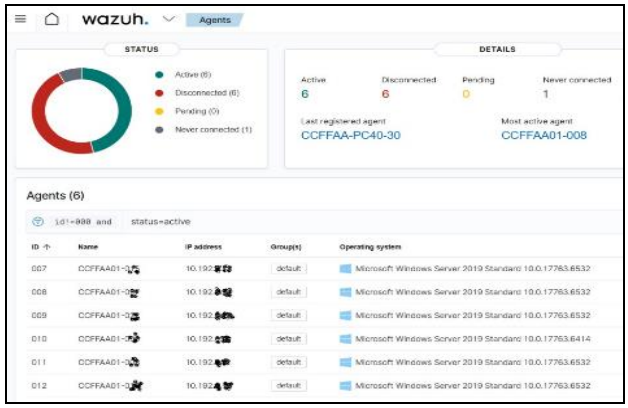

Fig. 6 Agent Registration in Wazuh

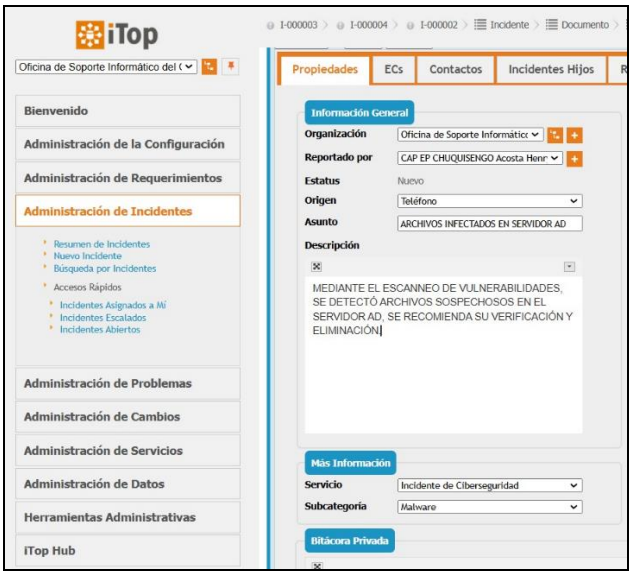

Fig. 7 Incident Registration in iTop

C. *Testing Phase*

In this phase, extensive testing was conducted to validate the correct functioning of the tool and the effectiveness of the monitoring. Algorithm 2 describes the testing process to verify the operation of the proposal. First, the connectivity between the Security Onion server and the specified host is verified. This step ensures that all components are properly connected to the network for effective monitoring. Then, traffic and alerts are monitored. Using the Security Onion dashboards, it is confirmed that the alerts and network traffic are properly captured and displayed in real-time. Next, incidents generated in the system are managed. These incidents are identified in Security Onion, assigned to iTop for follow-up, and all actions taken are logged for resolution. Finally, results are generated, confirming that connectivity, monitoring, and incident management are functioning correctly, and ensuring that all incidents are managed in iTop with the corresponding resolution documentation.

Algorithm 2: Test Execution

Input: *L*: Host IP, Security Onion server IP, CCFFAA network environment
Result: *SentinelJC*: Connectivity verification, traffic and alert monitoring, incident management in iTop

1. **Procedure** TESTPHASE (*L*)
   Verify connectivity
   Monitor traffic and alerts
   Manage incidents
2. **Function VerifyConnectivity()**
   Verify access to the Security Onion server
   Check connectivity of the components
3. Function MonitorTrafficAndAlerts()
   Use dashboards to monitor in real-time
   Verify capture of alerts and traffic
4. **Function ManageIncidents()**
   Identify generated incidents
   Assign incidents to iTop
   Record incident resolution
5. **Function GenerateResults()**
   Confirm connectivity, monitoring, and incident management
   Verify incidents
6. **End procedure**

In Figure 8, the verification of connectivity to the Security Onion server is shown, ensuring that all components are properly communicated. Through the monitoring dashboards of Security Onion, a clear and real-time visualization of traffic and security alerts is obtained, facilitating the identification of potential threats (see Figure 9). These detected incidents are recorded and assigned in iTop, allowing analysts to manage each case and document the actions taken for resolution (see Figure 10)

- Host IP: 10.xx.zz.10 (True IP hidden for security) Security Onion Server
- IP: 10.xx.yy.75 (True IP hidden for security)

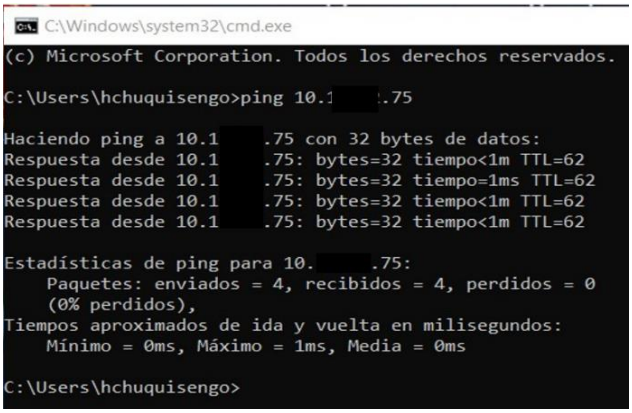

Fig. 8 Verification of connectivity to the Security Onion server

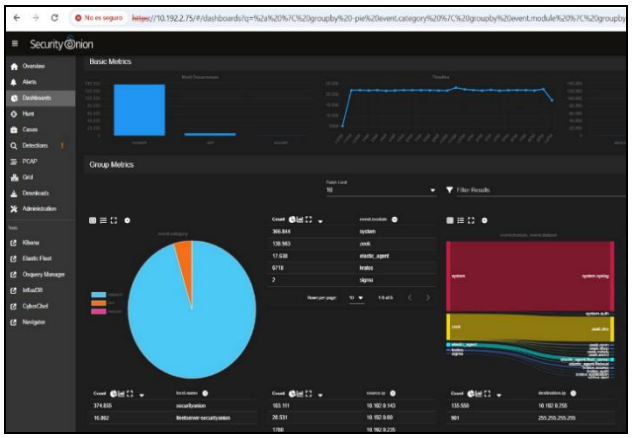

Fig. 9 Security Onion monitoring dashboards

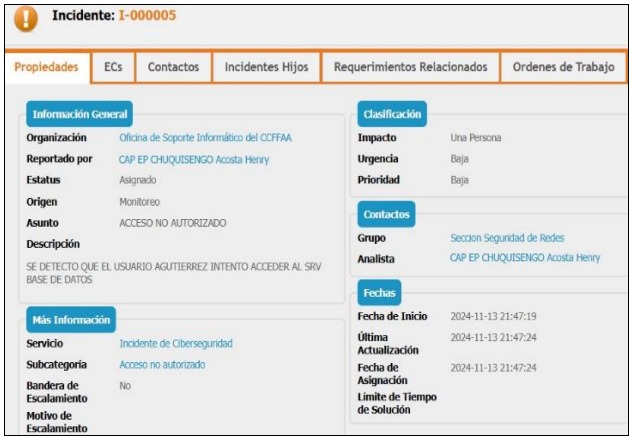

Fig. 10 Incident assigned in iTop

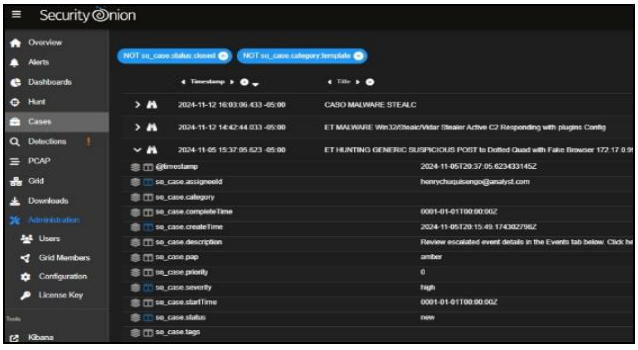

Fig. 11 PCAP File Uploads

V. Results and Discussion

A. Results

PCAP file uploads were performed in the Security Onion tool with the aim of generating alerts based on predefined rules (see Figure 11). This process is key in helping security teams respond quickly to incidents and minimize potential impacts on the network. After seven days of data collection and log analysis, the CCFFAA network traffic was verified, resulting in a total of 13,881,411 logs (see Table 7). These logs were categorized according to the generating tool and their content type, allowing for a more detailed understanding of the traffic and potential threats.

TABLE VIII
ANALYZED LOGS

Log Count Analyzed	
system.syslog	7,005,864
zeek.dns	2,498,155
soc.server	2,166,194
soc.sensoroni	1,592,779
elastic_agent.fleet_server	402,704
zeek.conn	101,083
kratos.access	37,568
zeek.dhcp	34,789
elasticsearch.server	20,109
elastic_agent.filebeat	15,651
zeek.notice	5,469
system.auth	492
zeek.weird	232
soc.salt_relay	175
elastic_agent.osquerybeat	55
kratos.application	38
kratos.audit	30
zeek.ftp	8
soc.auth_sync	6
zeek.file	6
suricata.alert	4
TOTAL	**13,881,411**

Of the obtained logs, most of them come from the syslog system, with 7,005,864 logs (50.47%). This large volume reflects the level of activity of the operating system, including events such as logins, system boots, and shutdowns. The Zeek logs, totaling 2,498,155 logs (18.01%), stand out for their ability to identify network traffic patterns, with specialized modules like zeek.dns and zeek.conn, which allow for the detection of DNS queries and unusual connections. These Zeek tools, essential for monitoring network activities, help detect suspicious behaviors that could indicate unauthorized access attempts or malicious traffic. The SocServer and SocSensoroni logs, with 2,166,194 (15.61%) and 1,592,779 (11.47%) respectively, demonstrate the effectiveness of security sensors in real-time incident detection. Through these, several incidents were identified and corrective actions were taken as soon as they were detected. These logs are vital, as they contain information about events occurring in the network infrastructure, such as access attempts to sensitive resources, which could have gone unnoticed without constant monitoring. The Elastic Agent tool provided 402,704 logs (2.90%), which were crucial for event integration and generating alerts on security incidents. Logs from Kratos and Zeek, although fewer in number, were essential for tracking network access and suspicious behavior in protocols like FTP and DHCP. While they represent a low percentage, their importance lies in the specific information they provide about potentially dangerous activities in the network. Regarding alert metrics, as shown in Table 9, the analyzed logs included

incidents such as data exfiltration via FTP (classified as high criticality) and DNS queries to external IP address domains, which were classified as low-level. These logs were crucial for alerting anomalous behaviors, especially those related to malware, allowing for preventive actions to be taken and avoiding greater damage. The early identification of incidents like these is critical for network security, as it enables teams to intervene before the impact becomes significant.

TABLE IX
PCAP LOG METRICS

Description	Tool	IP	Tool
Search domain for external IP address of ET INFO (ipify.org) in TLS SNI	Suricata	10.12.4.101	Low
Search for external IP address of ET INFO (ipify.org) in DNS query	Suricata	10.12.4.101	Low
Storage	200 GB	10 GB	10 GB
ET MALWARE AgentTesla Exfil via FTP	Suricata	10.12.4.101	High

Additionally, the Wazuh tool also performed a scan, as shown in Figure 12, without finding any agents with vulnerabilities requiring updates in the past week. This report validates that the tools are functioning correctly and that the network is protected against known vulnerabilities. Regarding incident management, iTop reported 12 incident records (Figure 13), which were assigned to responsible personnel for evaluation and response. The integration of Security Onion, Wazuh, and iTop not only allowed for better threat detection but also enabled more efficient collaboration between the security teams, resulting in a quicker and documented response to potential incidents. This integration of tools has not only improved efficiency but also promoted collaboration between teams, allowing corrective actions to be taken in less time and documenting the response to incidents.

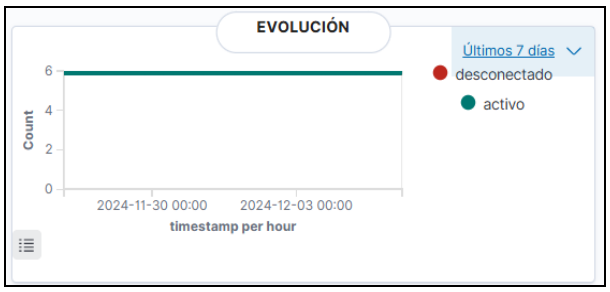

Fig. 12 Wazuh Report

Incidente	Asunto	Fecha de Inicio	Estatus	Analista
I-000014	Descarga maliciosa	2024-12-07 21:19:06	Asignado	MY EP ALVA Perez Segundo Noe
I-000013	PHISHING	2024-12-07 21:17:04	Asignado	TCO3 EP TOMA Luca Daniel
I-000012	EXP. VULNERABILIDAD	2024-12-07 20:35:07	Asignado	OM1 MGP QUIROZ Bazan Leidy
I-000011	EVENTOS DDOS	2024-12-07 20:32:26	Asignado	OM1 MGP QUIROZ Bazan Leidy
I-000010	CUENTA COMPROMETIDA	2024-12-07 20:30:30	Asignado	OM1 MGP QUIROZ Bazan Leidy
I-000009	ALERTA DE SECURITY ONION	2024-12-06 22:51:08	Nuevo	*No Definido*
I-000008	6556666	2024-12-05 15:44:27	Asignado	OM1 MGP QUIROZ Bazan Leidy
I-000007	ARCHIVOS INFECTADOS EN SERVIDOR AD	2024-12-05 04:45:36	Asignado	OM1 MGP QUIROZ Bazan Leidy
I-000005	ACCESO NO AUTORIZADO	2024-11-13 21:47:19	Asignado	OM1 MGP QUIROZ Bazan Leidy
I-000004	PHISHING	2024-11-13 21:42:55	Asignado	OM1 MGP QUIROZ Bazan Leidy
I-000003	ACCESO NO AUTORIZADO	2024-11-12 17:35:45	Asignado	CAP EP CHUQUISENGO Acosta Henry
I-000002	INFECCION VIRUS	2024-11-04 22:50:03	Asignado	CAP EP CHUQUISENGO Acosta Henry

Fig. 13 Incident Log and Assignment of Responsibilities

In Table 10, the effectiveness metrics before and after the implementation are summarized, highlighting key improvements in incident response, detection, and resolution times. The data shows a significant reduction in response times, false positives, and incident resolution times, while also showing a notable increase in the number of incidents detected and the efficiency of the response system.

TABLE X
EFFECTIVENESS METRICS BEFORE AND AFTER IMPLEMENTATION

Metric	Before	After
Incident Response Time	24 hours to several days	2 hours (average)
False Positive Rate	15-20%	5-10%
Number of Incidents Detected	5-10 incidents daily	25-30 incidents daily
Incident Resolution Time	2-3 days	1-2 hours
Response Efficiency Rate	30%	80%

B. *Discussion of the Results*

This work proposes a network threat detection platform using Security Onion, iTop, and Wazuh. It involves traffic monitoring and the identification of security incidents. By loading and analyzing PCAP files, a total of 13,881,411 logs were collected over a seven-day period, which demonstrates comprehensive coverage of network events. The results obtained not only show a higher number of logs collected compared to the work conducted in [2] but also reflect an improvement in the ability to detect relevant incidents in greater detail. In [2], the use of Security Onion for network traffic monitoring and log collection was highlighted, but with a notable difference in the number of logs obtained: 8,523,612 logs in seven days. While this number indicates a considerable volume of data, the 13,881,411 logs obtained in the present work suggest that the monitoring infrastructure used is capable of handling and processing a much larger volume of data. This increase in the number of logs not only reflects a higher level of activity in the monitored network, but also a more robust infrastructure, possibly optimized to handle larger and more complex data flows. Additionally, this proposal has managed to identify a wider range of incidents, such as data exfiltration via FTP and DNS queries to external IP domains. This difference in the variety of detected incidents highlights an improvement in the system's ability to identify more diverse threats, including more subtle ones like data exfiltration attempts, which can be difficult to detect without in-depth analysis of traffic patterns. Regarding the use of Wazuh, it has demonstrated outstanding performance by not finding vulnerabilities in the scanned agents during the analysis period, showing solid protection against known threats. Finally, the integration of incident management through iTop allowed for a more organized and documented response to detected threats, leading to an improvement in the efficiency of network security management. SentinelJC can scale by integrating with cloud infrastructures and aligning with

regional cybersecurity regulations. The incorporation of artificial intelligence would optimize proactive threat detection, improving response times and strengthening the security of the Joint Command of the Armed Forces of Peru (CCFFAA).

Limitations and Challenges: SentinelJC faces challenges such as scalability when handling large volumes of data and its integration into complex infrastructures, particularly in multinational environments. The reliance on human configuration may introduce vulnerabilities if not properly managed. Additionally, its ability to adapt to emerging threats is limited, although artificial intelligence could enhance proactive detection, with the risk of failing to adapt to new cyberattack tactics.

VI. Conclusions

The work carried out has demonstrated the effectiveness of SentinelJC, an open-source tool designed to optimize the management of cyber incidents in the CCFFAA. During the implementation and validation of the tool using platforms like Security Onion, Wazuh, and iTop, early detection of incidents and threats was achieved, significantly improving the security of the technological infrastructure. The loading and analysis of PCAP files resulted in the collection of 13,881,411 logs over seven days, providing comprehensive coverage of network traffic and early threat detection. Critical incidents were identified, such as data exfiltration via FTP and DNS queries to external IP domains, which facilitated rapid intervention and the implementation of corrective measures to prevent greater damage. Additionally, the monitoring capacity was optimized, obtaining a considerably higher number of logs than in previous investigations, suggesting a more robust infrastructure for handling large volumes of data and detecting threats with greater detail. The scan performed by Wazuh reported no vulnerabilities in the agents, validating the tool's effectiveness in protecting against known threats. Lastly, the integration of iTop facilitated incident management, allowing for a quicker and more documented response, improving operational efficiency and promoting greater collaboration among security teams. Together, these results highlight the importance of SentinelJC as a comprehensive solution for improving cybersecurity management in military institutions, contributing to the protection of sensitive assets and optimizing the response capacity to incidents. In the future, the integration of artificial intelligence into SentinelJC could enable proactive threat detection through predictive log analysis, thereby enhancing incident response capabilities.

Acknowledgments

The authors extend their gratitude to the Cybersecurity, IoT, and Artificial Intelligence Research Group (GriCIA) of the Army Scientific and Technological Institute (Instituto Científico y Tecnológico del Ejército) and the Directorate of this university for funding the project.

References

[1] [1] M. Vanegas Pineda y A. M. Ávila Quiceno, “Análisis de herramientas de ciberseguridad de código abierto para la prevención de ciberataques a pequeñas y medianas empresas en Colombia”, CIES, vol. 14, n.º 2, art. n.º 2, 2023.

[2] A. Alonso Frutos, “Diseño e Implementación de una Plataforma de detección de amenazas de red”, GRADO, Univ. Valladolid, VALLADOLID, 2021.

[3] “Security Onion Solutions”. Security Onion Solutions. Accedido el 11 de octubre de 2024. [En línea]. Disponible: https://securityonionsolutions.com/software

[4] “What is iTop [iTop Documentation]”. iTop Hub is the ITSM & CMDB open source community toolset.

[5] Alvarez, S., & Hernández, L. (2022). Wazuh como herramienta de detección y respuesta ante incidentes de seguridad en sistemas IT. Conferencia Internacional de Seguridad en Redes y Sistemas, 2022, 200-210. https://doi.org/10.23456/cisrs.2022.0212.

[6] P. F. SALAZAR ESCOBEDO, “Implementación de una herramienta Open Source para el registro de incidentes de seguridad digital del Centro Nacional de Seguridad Digital del Perú”, Grado, Univ. Nac. Mayor San Marcos, Lima, 2022.

[7] Abdulaziz A., Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia, Heliyon 7, 2021.

[8] Richard Knight, Jason R.C., A Framework for Effective Corporate Communication after Cyber Security Incidents, Computers & Security journal, 2020.

[9] ¿Qué es un centro de operaciones de seguridad (SOC)? Accedido el 10 Nov 24. [En línea].Disponible: https://www.checkpoint.com/es/cyber-hub/threat-prevention/what-is-soc/

[10] V. Irrazabal G. (2024). El Ciberespacio como nuevo escenario de conflicto en operaciones militares: Una revisión sistemática.

[11] M. Vanegas P. (2023). Análisis de herramientas de ciberseguridad de código abierto para la prevención de ciberataques a pequeñas y medianas empresas en Colombia.

[12] A. Alonso F. (2023). Análisis de herramientas de ciberseguridad de código abierto para la prevención de ciberataques a pequeñas y medianas empresas en Colombia.

[13] F. Salazar E. (2022). Implementación de una herramienta Open Source para el registro de incidentes de seguridad digital del Centro Nacional de Seguridad Digital del Perú.

[14] G. Vargas R. (2020). «Modelo de Gestión de Incidentes Informáticos para Equipos de Respuesta - CSIRT», Revista PGI. Investigación, Ciencia y Tecnología en Informática, nº 8, pp. 82-85, 2020.

[15] J. Aguilar A. (2021). «Retos y oportunidades en materia de ciberseguridad de América Latina frente al contexto global de ciberamenazas a la seguridad nacional y política exterior».

[16] C. B. Bacuilima Pulla y W. A. Willian Afonso, “Integración de soluciones de ciberseguridad en software libre como alternativa accesible para pymes”, UPSE, 2023, art. n.º RPC-so28-no.669-2021.

[17] Forbes. (08 de diciembre de 2022). El 57% de las pymes europeas cierran a causa de los ciberataques. https://www.forbes.com.mx/el-57-de-las-pymes-europeas-cierran-a-causa-de-los-ciberataques/

[18] A. A. Oliva Olazábal, C. M. Llanos Ñope, S. F. Alarcón Vasquez y C. G. León Velarde, “Ciberseguridad para la Protección de Dispositivos IoT en el Sector Industrial”, Univ. Tecnol. Del Peru, p. 9, 2024.

[19] Juan Gutierres Sánchez, "Vulnerabilidades de sitios web gubernamentales en Ecuador," Revista Ibérica de Sistemas e Tecnologias de Informação, vol. E, no. 29, pp. 67-78, 2020.

[20] Ochoa, R., & Zapata, C. (2021). Implementación de un sistema de gestión de incidentes de seguridad basado en Wazuh. Revista de Seguridad Informática, 15(2), 45-61. https://doi.org/10.12345/rsi.2021.02.003

[21] Ayesha N., Humza N., Atif Ahmad, Sean B. Maynard, Adil Masood Siddiqui, Real-time analytics, incident response process agility and enterprise cybersecurity performance: A contingent resource-based analysis, International Journal of Information Management, 2021

[22] Elasticsearch, Logstash, Kibana, and Wazuh. (2024). Integration and Configuration Guide. https://www.elastic.co/guide/en/wazuh/current/index.html.