DetectEP: A Vulnerability Monitoring and Detection Tool Using Wazuh in a Military Institution

Antony Uribe Arroyo, Eng[1]; Javier Altamirano Irigoin, Eng[1]; Carlos Quinto Huamán, PhD[2]; Sonia Lidia Romero Vela, 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, *auribearroyo@icte.edu.pe, jaltamiranoi@icte.edu.pe, sromerov@icte.edu.pe, pochoac@icte.edu.pe*
[2]Universidad Privada del Norte, Lima, Perú, *carlos.quinto@upn.pe*

Abstract*– Currently, information security is essential for organizations across all sectors, particularly for military institutions, which handle sensitive data and operate in high-security environments. Cyberattacks, such as unauthorized access and data manipulation, are rapidly evolving in complexity, significantly increasing the risks faced, both personally and organizationally. Vulnerabilities in technological infrastructures, caused by software failures, misconfigurations, or weaknesses in security protocols, create openings for attackers, jeopardizing the integrity of systems. This article proposes a security monitoring tool designed to detect and manage vulnerabilities in real-time, using the Wazuh tool. A methodology was implemented, including the installation and configuration of Wazuh in the institution's technological infrastructure, followed by continuous monitoring. The results showed that, through monitoring, 115,311 events were detected in total, of which 37 were identified as authentication failures. Additionally, 135 vulnerabilities were detected, ranging from critical to medium levels. Wazuh demonstrated accuracy in monitoring and vulnerability detection, allowing for the timely implementation of corrective measures and strengthening system security.

Keywords: Wazuh, vulnerabilities, security monitoring, threat detection, Open Source

I. Introduction

In an era of rapidly evolving technology, institutions face growing challenges in information security, demanding a proactive approach to protect their infrastructures. This challenge is intensified in military institutions, where the sensitive nature of the data requires even stricter and more comprehensive security measures. In the Army of Peru, the General Library and Virtual Classroom (BGyAVE) is an essential unit for knowledge management and academic development, playing a key role in the training and dissemination of information within the institution. However, this unit is also exposed to various cyber threats that could jeopardize its operations. Therefore, ensuring the protection of these infrastructures is crucial to safeguard their integrity, availability, and confidentiality, thus ensuring the protection of critical information, which is vital for the Army's operations and mission.

According to a report by ESET [1], one of the leading cybersecurity companies, Peru is among the five countries most affected by cyber threats, alongside Mexico, Ecuador, Brazil, and Argentina. In the first half of 2024, more than 909,000 threats were detected in the country, ranking it first in terms of the incidence of cyberattacks. This data highlights the urgent need to strengthen cybersecurity policies and strategies in both the public and private sectors to mitigate the risks posed by digital threats. Figure 1 presents the magnitude of the problem, highlighting the urgent need to mitigate risks and protect institutions from cybercriminals. Furthermore, another clear indicator of the growing cyber threat is the significant increase in reports of cyber fraud in the country. According to the High-Tech Crime Investigation Division (DIVINDAT) of the National Police of Peru (PNP), cyber fraud has become the most investigated cybercrime, with a 58% increase in cases in 2023 [2]. This phenomenon shows that cybercriminals are no longer an abstract or distant threat, but a tangible reality affecting thousands of people and businesses on a daily basis. Additionally, between July 2023 and July 2024, Peru experienced an alarming increase in malware detection, with a total of 64,752,156 incidents reported, representing a 2.9% increase compared to the same period the previous year. This scenario reflects the growing cyber threat that has significantly impacted the country, with the government sector being the most vulnerable. In fact, 41.74% of the attacks were directed at public institutions, revealing the magnitude of the challenge faced by state entities to protect their systems and data against the increasing sophistication of cybercriminals [3].

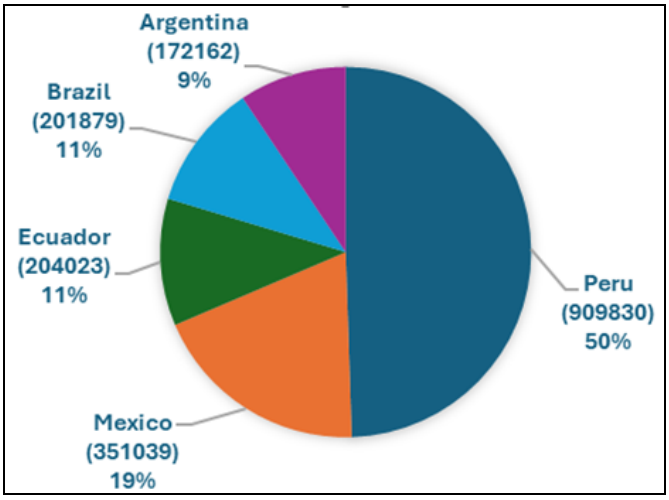

Fig. 1 Latin American countries with the highest number of threats - 2024

In this context, this article proposes the implementation of DetectEP, a real-time monitoring and vulnerability detection tool based on Wazuh. The tool was integrated with Slack to send immediate notifications, enabling a quick and efficient response to security events. The primary goal of this implementation was to evaluate its potential as a proactive monitoring tool in the technological environments of military institutions, analyzing its effectiveness in identifying, managing, and responding to security incidents.

This work is structured into six sections, with the first being the current introduction. Section II briefly describes some concepts related to monitoring and vulnerability detection. Section III reviews related works on monitoring and vulnerability detection. Section IV presents the development of the proposal, which involves performing four phases sequentially. Section V describes the results and discussion obtained. Finally, Section VI presents the conclusions of this research.

II. Vulnerability Monitoring and Detection

Vulnerability monitoring and detection are essential in cybersecurity to protect organizations' digital infrastructures from threats and cyberattacks [4]. The following section conceptualizes the associated terms:

A. Cybersecurity

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks [5]. It is also known as information technology security or electronic information security. The term is applied in different contexts, from business to mobile computing, and can be divided into several common categories. Cybersecurity aims to protect computer systems, applications, devices, data, financial assets, and individuals from ransomware and other malware, phishing scams, data theft, and other cyber threats [6].

B. Security Information and Event Management

Security Information and Event Management (SIEM) is a platform that provides a real-time view of an organization's IT environment, collecting, analyzing, and presenting security-related information [7]. Its main objective is to detect, prevent, and respond to security threats, all in a single integrated and centralized solution. The process of a SIEM solution consists of several key stages: first, security data is collected from across the organizational network. Then, this data is aggregated and normalized to ensure consistency and facilitate analysis. Next, security policies are applied, and data is analyzed to identify potential threats, both through predefined patterns and new indications of attacks. Finally, if a threat is detected, an alert is generated to notify the security team, enabling an immediate and effective response [8]. In [9], several high-quality SIEM solutions are presented, each designed to adapt to different organizational needs, budgets, and integration capabilities. Some of the most notable include Splunk Enterprise Security, SolarWinds Security Event Manager, Microsoft Sentinel, IBM QRadar, Elastic, and Wazuh.

C. Wazuh Intrusion Detection System

Wazuh is a SIEM platform designed to collect, analyze, and correlate security events in real-time. Its flexible and extensible architecture makes it a highly effective tool for both small businesses and large organizations [10]. In [11], Wazuh is described as a comprehensive security platform that offers advanced capabilities such as log analysis for threat detection, real-time file integrity monitoring, and vulnerability detection in systems. Additionally, it evaluates security configurations, facilitates automated incident response, and ensures regulatory compliance with international standards. Its monitoring extends to cloud environments and containers such as Docker and Kubernetes, and it integrates with external security management tools to enhance overall infrastructure protection. Furthermore, Wazuh is used globally by organizations such as the European Organization for Nuclear Research (CERN), the Ministry of Defense of Spain, and Alfamart in Indonesia for security monitoring, log management, and regulatory compliance. Its open-source flexibility and real-time threat detection capabilities make it popular among educational institutions, government agencies, and telecommunications companies such as Wind Telecom in the Dominican Republic.

D. Vulnerabilities and Computer Security Monitoring

A security vulnerability is any flaw or weakness in the structure, functionality, or implementation of a network or networked asset that hackers can exploit to launch cyberattacks, gain unauthorized access to systems or data, or harm an organization. Common examples of vulnerabilities include misconfigurations in firewalls that could allow certain types of malwares to enter the network, or unpatched errors in the remote desktop protocol of an operating system that could enable hackers to take control of a device [12]. Computer security monitoring is an ongoing process that involves the active supervision of an organization’s systems, networks, and data to detect and respond to potential threats or anomalies. It includes the collection, analysis, and correlation of security data to identify suspicious or malicious activities that could compromise the company's technological infrastructure [13]. This monitoring is crucial to prevent cyberattacks and minimize risks, ensuring the integrity and continuity of operations. With the use of automated tools, incident response can be faster and more effective.

F. Open-Source Software

Open-Source Software is a tool developed and maintained through open collaboration [14]. It is available for anyone to use, examine, modify, and redistribute as they wish, usually at no cost. According to [15], the characteristics of open-source software are: i) Open and unrestricted license, allowing distribution, modification, and use without commercial limitations or discrimination; ii) Accessible source code,

allowing its distribution and the creation of derivative works; iii) Open design, ensuring a transparent and participatory process where the community influences the software's planning and direction; iv) Open development, with inclusive and transparent processes, setting clear rules for contributions from all participants, regardless of their experience level; and v) Open community, providing an inclusive environment where anyone can contribute and rise to leadership positions within the project.

G. Slack

Slack is a real-time communication and collaboration platform designed for work teams [16]. It allows organizing conversations through thematic channels, direct messages, and groups, facilitating efficient collaboration among team members. Additionally, Slack supports integrations with various productivity tools and applications, including monitoring and security systems, enabling real-time notifications and improving response to critical incidents. It is commonly used in business and technological environments due to its ability to organize communication and facilitate fast decision-making. In [17], the most important features of Slack are described as: i) Team-oriented communication, which allows the creation of dedicated channels for specific projects or topics, accessible from mobile and desktop devices; ii) Video conferencing, enabling audio and video meetings without leaving the platform; iii) File and document sharing, allowing users to easily upload and share content within workspaces; iv) Automated reminders, which help keep teams organized by setting up reminders for important tasks or events; v) Third-party integrations, allowing connections with apps like Google Drive or Dropbox to facilitate project management; vi) Scalability, as Slack adapts to teams of any size, allowing the creation of multiple workspaces and customized channels; and vii) Security and privacy, with strong policies to protect data and control access to messages and private channels.

III. State of the Art

In recent years, due to the growing number of cyberattacks globally, constant and determined efforts have been made to counter this threat. Both public and private organizations are implementing increasingly sophisticated measures to protect their systems and data, aware that cybersecurity has become a priority in an ever-more interconnected world. Simultaneously, new technologies, security protocols, and regulatory frameworks have been developed to address emerging threats.

In this context, the literature offers various studies on the use of Wazuh as a cybersecurity solution. In [18], a free software-based SIEM (Wazuh and ELK) was implemented to detect vulnerabilities, monitor critical devices and files, and track detailed system modifications. In [19], a combination of tools such as Wazuh, TheHive, Telegram, and CVSS is used to identify vulnerabilities and improve risk detection in organizational applications. In [20], the forensic analysis of web servers was optimized through the use of these same tools, allowing the identification of attacker tactics on websites. In [21], the use of Wazuh is proposed to detect SQL injection attacks in academic information systems. These approaches highlight the effectiveness of tools like Wazuh and TheHive to enhance security, monitoring, and response to threats in various technological environments. However, various solutions have proven effective in identifying and mitigating vulnerabilities and cyber threats in different settings. According to [22], an economic and flexible prototype for small and medium-sized enterprises is proposed, using Raspberry Pi and open-source software, which helps improve threat detection and strengthen security. In [23], the researchers propose implementing network monitoring as an open-source tool to prevent attacks and vulnerabilities in computer systems, particularly in the transportation sector. Using the Greenbone tool, real-time scanning of common threats such as SSH issues, repeated logins, Windows SMB updates, and SSL/TLS services can be conducted. The results show that this approach is effective for quickly identifying and addressing vulnerabilities, which helps strengthen the security of networks in this sector. Thus, continuous monitoring not only prevents risks but also optimizes the response to potential threats. In [24], the researchers propose an exploratory study on vulnerabilities in government websites, focusing on those that handle sensitive information. Using the Acunetix software, they analyzed ten randomly selected 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 flaws. Additionally, a positive correlation was observed between the number of scanned elements and the number of vulnerabilities, indicating that the more elements scanned, the higher the risk. In [25], the researchers propose using centralized systems in cybersecurity, highlighting the effectiveness of AlienVault OSSIM in evaluating vulnerabilities and detecting intruders. Through its implementation as a SIEM solution, threat management and incident response are enhanced. The results indicate that AlienVault OSSIM protects data accessible on the network, preventing its modification, theft, or misuse. This centralized approach strengthens defense against cyberattacks and proves to be an effective tool in system protection. In [26], the researchers propose using the SIEM tool Splunk to detect anomalies in the system of the Islamic University of Indonesia (UII) and anticipate cyber threats. By processing the firewall logs of PaloAlto, Splunk analyzes the data and presents the results on a dashboard, making it easier to identify potential threats early and prevent possible attacks. In [27], the project improved the cybersecurity of a government entity by implementing OSSIM AlienVault, optimizing technological performance and enhancing the ability to detect and mitigate IT risks and threats. Finally, in [28], it is concluded that the Peruvian Army must strengthen its cybersecurity through early threat detection, automated responses, and other measures to improve the resilience of its systems.

IV. Development of the Proposal

To develop the proposal, an experimental flow was followed, structured in four successive phases. The first phase, planning, corresponds to the initial stage in which the project objectives are defined, necessary resources are organized, and the appropriate tool is selected to achieve those objectives. The second phase, implementation, involves the preparation, installation, and configuration of the components that will interact within the system, ensuring their correct integration. In the third phase, testing, the connectivity of each component, as well as the tool intended for notifications, is verified in order to evaluate its operability and performance. Finally, the fourth phase, observation and maintenance, focuses on the continuous monitoring of the system, carrying out detailed observations and periodic analyses to ensure its proper functioning. In this phase, a maintenance plan was also developed, which includes specific procedures for system review and optimization. This cycle of phases allows for a comprehensive and progressive evaluation of the project, ensuring its sustainability and long-term viability (See Figure 2).

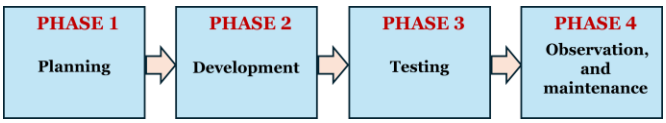

Fig. 2 Flow of the proposal development

A. Planning Phase

A.1. First, a detailed analysis of the hardware and software technical requirements was conducted to ensure that the systems had the appropriate infrastructure for their operation. This step was crucial to guarantee that everything was prepared for a smooth implementation, aligned with the project's objectives (See Tables 1 and 2).

TABLE I
Hardware Requirements for Wazuh Implementation

No	Component	Quantity	RAM (GB)	CPU (Cores)	Hard Drive
1	Server	1	8	8	1 TB
2	Desktop Computer	17	8	8	500 GB

TABLE II
Software Requirements for Wazuh Implementation

No	Component	Name and Version	Notes
1	Server Hosting Wazuh	Ubuntu Server 24.04.1	Open Source
2	Virtualization System	VirtualBox 7.1.4	Open Source
3	Messaging System	Slack 4.41.98	Free Plan
4	SIEM	Wazuh 4.9.2	Open Source

Additionally, the roles and responsibilities of the team responsible for using the tool were clearly defined, ensuring that each person knew exactly what they needed to do and how to collaborate for the success of the implementation (See Table 3).

TABLE III
Roles and Responsibilities of the Personnel for Wazuh Implementation

No	Role	Responsibilities
1	Head of the Telecommunication Department	• Configure the tool (servers, integrations, customization). • Assign roles and permissions to users.
2	Head of the Virtual Classroom Section	• Perform system updates and backups. • Execute assigned tasks.
3	Head of the Technical Support Section	• Provide support, resolve technical issues.

As part of the selection process, three open-source SIEM tools were evaluated: Wazuh, AlienVault OSSIM, and OSSEC, considering key aspects such as ease of implementation, real-time monitoring, scalability, integration with other tools, and community support (ee Table 4). Wazuh demonstrated significant technical advantages. Its modular architecture facilitates deployment in hybrid environments, offering advanced monitoring capabilities through integration with the ELK stack. In contrast to OSSIM, which requires more complex configuration and resource allocation, and OSSEC, whose flexibility and analysis capabilities are limited, Wazuh enables event correlation, automated alerts, and efficient visualization of threats in real time. Moreover, it stands out for its high scalability, allowing it to handle large volumes of distributed data, and its ability to integrate with multiple tools such as Snort, VirusTotal, and Slack. This versatility, combined with an active and well-supported community, makes it highly suitable for demanding operational environments. These combined characteristics support the selection of Wazuh as the most appropriate solution to meet the project's objectives.

TABLE IV
Comparison of Open Source SIEM Tools

Feature	Wazuh	AlienVault OSSI	OSSEC
License Type	Open Source (GPLv2)	Open Source (GPLv2)	Open Source (GPLv2)
Ease of Implementation	High: Easy to implement, supports hybrid environments, and scalability.	Medium: Requires complex configuration and more resources.	High: Relatively easy, but less flexible.
Real-Time Monitoring	High: Advanced monitoring, detailed analysis, automated alerts.	Medium: Good monitoring, but with more complex configuration and less detail.	Low: Basic monitoring, limited interface.
Scalability	High: Ideal for large and distributed environments.	Medium: Moderate scalability, ideal for medium environments.	Low: Limited scalability, not ideal for large environments.
Integration with Other Tools	High: Extensive integration with ELK Stack, Syslog, Snort, Slack, and other tools.	Medium: Integrates some security tools like Snort, OpenVAS, but less flexible.	Low: Limited integration, less flexible.
Support and Community	High: Large community and active support.	Medium: Active community, but less extensive.	Low: Smaller community, limited support.

A.2. Secondly, a training plan was designed to ensure that the BGyAVE staff can use Wazuh effectively, managing system security efficiently and sustainably (See Table 5). The goal is not only to teach them how to use the tool but also to empower them to adapt it to daily needs and manage it independently. This ensures that the technological infrastructure is always protected, even when new challenges or threats arise.

TABLE V
TRAINING PLAN FOR WAZUH IMPLEMENTATION

Phase	Objective	Duration
1. Introduction	Familiarization with basic security concepts and Wazuh.	4 hours
2.Installation and Configuration	Installation and basic configuration of Wazuh and Slack.	6 hours
3. Administration and Monitoring	Training on real-time event monitoring and vulnerability detection.	6 hours
4. Advanced Management	Advanced management and preventive maintenance of Wazuh.	4 hours

A.3. Thirdly, the objectives of the work were defined, focusing on ensuring the proper functioning and security of the systems. The first of these objectives is to conduct real-time monitoring of the configured devices to detect any incidents in a timely manner. The second objective is to identify the vulnerabilities present in the technological infrastructure to anticipate potential risks. Finally, the need to define appropriate technical solutions to address these vulnerabilities was established, which involves applying corrective measures such as software updates and security configuration adjustments. This comprehensive approach aims to ensure not only the stability of the system but also continuous improvement in its performance and protection.

A.4. Fourthly, the deployment of Wazuh components and the configuration of the devices were designed to ensure their proper functioning. This process includes the proper distribution of the system's different elements, such as the Wazuh servers, the agents installed on the hosts (or devices), and the communication between these components. It is ensured that each element is correctly configured and optimized to guarantee that the system can efficiently collect, process, and analyze data. This phase is crucial for integrating all monitored devices into the system, enabling their management and real-time monitoring (See Figure 3).

B. *Development Phase*

In this phase, the entire process of preparation, installation, and configuration of the system components was carried out to ensure their proper integration and functionality.

The first step involved preparation, which ensured that the 17 available computers (See Table 1) were fully operational. The operating system of each machine was also verified to ensure compatibility with the tools selected for this project (See Table 2). This process was crucial as it allowed for the evaluation of both the capabilities and limitations of the BGyAVE infrastructure, facilitating an efficient implementation adapted to its specific needs. Additionally, particular attention was given to safeguarding the privacy of the information, considering the sensitivity of the data to be handled throughout the process.

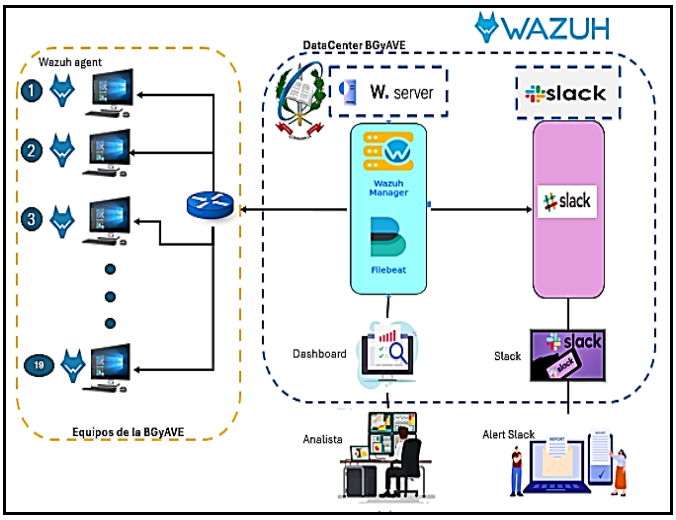

Fig. 3 Wazuh Architecture Diagram

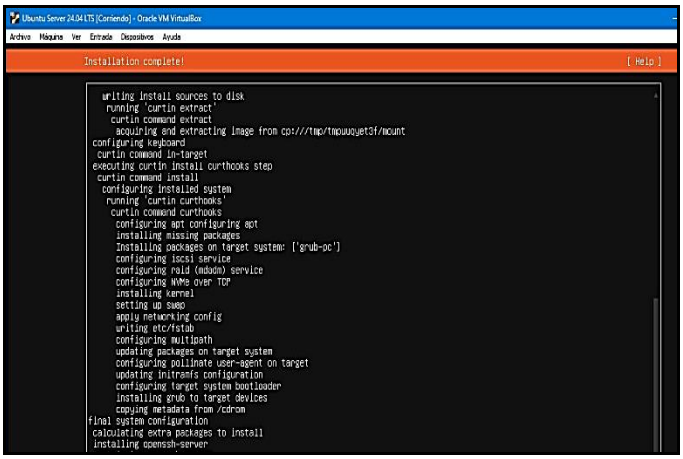

Fig. 4 Installation of Ubuntu Server 20.04.1

The second step of the process was the installation of the key components necessary for the system to function properly. We began with VirtualBox 7.1.4, which allowed for the creation of virtual machines to test and configure the environment without affecting the physical system. This tool was essential for simulating various conditions and performing tests in isolation. Once virtualization was set up, we proceeded to install Ubuntu Server 24.04.1, selected for its stability, security, and compatibility with the required tools (See Figure 4). After configuring the operating system, the next step was the installation of Wazuh 4.9.2, our monitoring and intrusion detection platform (See Figure 5). Finally, we configured Wazuh agents on the respective nodes to ensure continuous and real-time data collection (See Figures 6, 7, and 8).

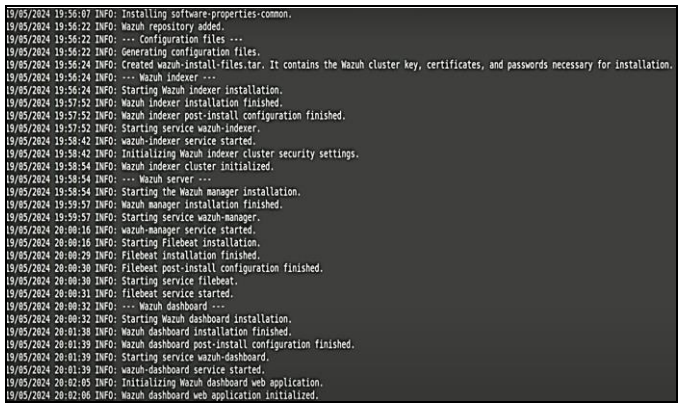

Fig. 5 Installation of Wazuh Server on Ubuntu

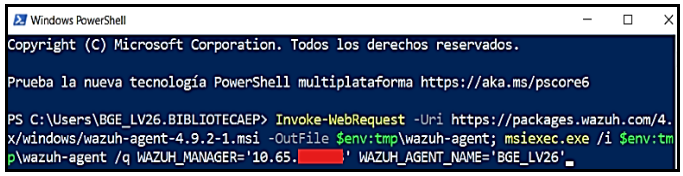

Fig. 6 Installation of Agents on Windows (PowerShell)

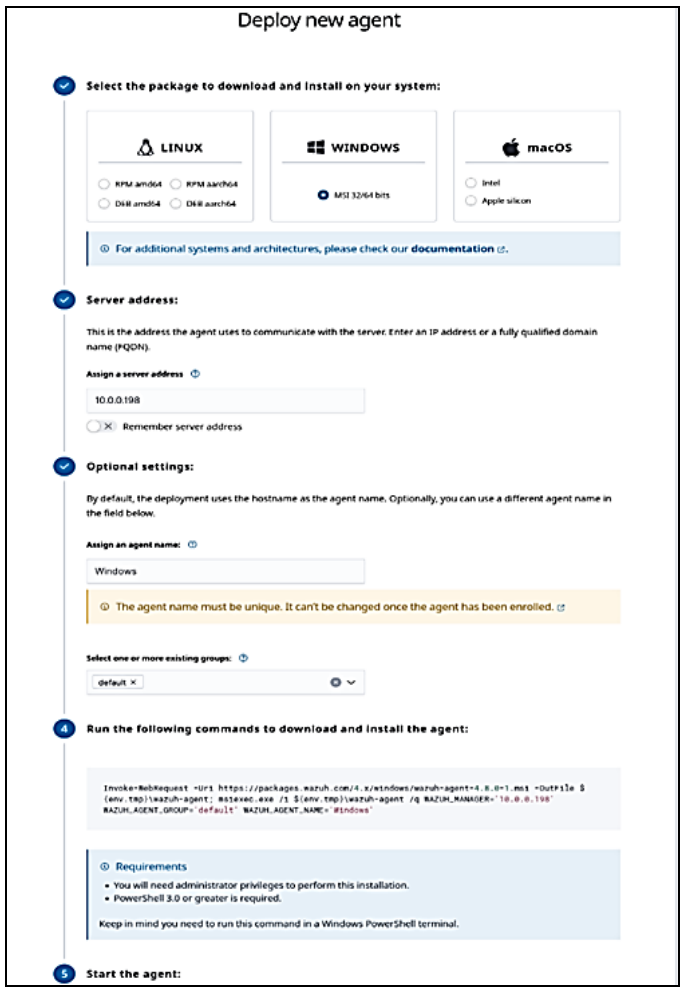

Fig. 7 Installation of Wazuh Agents on Windows

The third step involved configuring the Wazuh server to enable integration with Slack (See Figure 9), with the objective of efficiently managing event notifications. This process ensures that the security alerts generated by Wazuh are communicated in real-time to the responsible team, thereby facilitating a timely response to any threats or incidents. To achieve this, the Wazuh configuration file was modified, specifically the /var/ossec/etc/ossec.conf file, where the necessary parameters for the Slack integration were enabled and adjusted. A specific Slack channel was configured where notifications would be sent automatically each time Wazuh detected a relevant security event. Additionally, the Slack authentication details, such as the access token and webhook, were configured to ensure that the alerts reached the designated channel securely and directly.

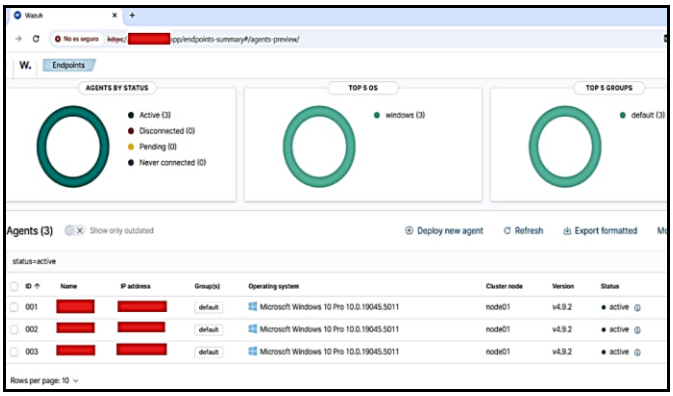

Fig. 8 List of Agents Registered in Wazuh

Fig. 9 Configuration for Wazuh Integration with Slack

Furthermore, the necessary configuration was implemented to conduct vulnerability analysis on the agents connected to the Wazuh server. This configuration allowed for continuous evaluation of the security of the systems involved, identifying potential security flaws and misconfigurations that could compromise the integrity of the infrastructure (See Figure 10).

```
admon@ubuntus: ~
 GNU nano 7.2
 <sca>
   <enabled>yes</enabled>
   <scan_on_start>yes</scan_on_start>
   <interval>12h</interval>
   <skip_nfs>yes</skip_nfs>
 </sca>

 <vulnerability-detection>
   <enabled>yes</enabled>
   <index-status>yes</index-status>
   <feed-update-interval>60m</feed-update-interval>
 </vulnerability-detection>

 <indexer>
   <enabled>yes</enabled>
   <hosts>
     <host>https://127.0.0.1:9200</host>
   </hosts>
   <ssl>
     <certificate_authorities>
       <ca>/etc/filebeat/certs/root-ca.pem</ca>
     </certificate_authorities>
     <certificate>/etc/filebeat/certs/wazuh-server.pem</certificate>
     <key>/etc/filebeat/certs/wazuh-server-key.pem</key>
   </ssl>
 </indexer>
```

Fig. 10 Wazuh Configuration for Vulnerability Scanning

C. *Testing Phase*

In this phase, the verification process is carried out to ensure the proper functioning of the system. This includes checking the connectivity between each of the involved components (See Figure 3), such as servers, agents, and monitored devices, with the goal of ensuring that all elements of the system communicate effectively and without interruptions. Additionally, a detailed evaluation of the notification tool is performed, verifying its ability to generate alerts (See Figure 11). In this context, the agents connected to the Wazuh server were also verified (See Figure 12). This testing process is crucial to identify potential failures, optimize the configuration, and ensure that the system operates smoothly and effectively in real-world situations.

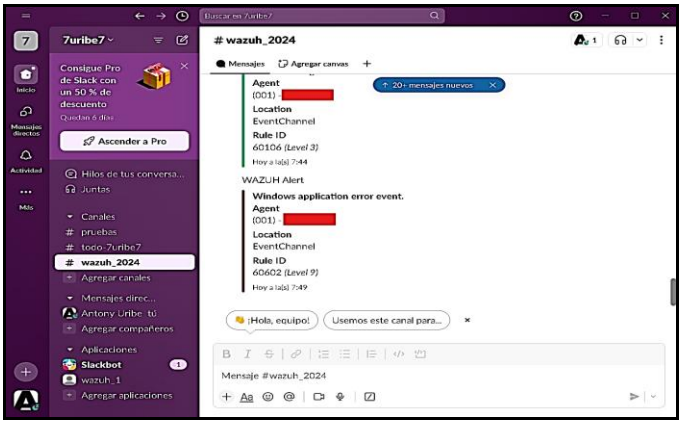

Fig. 11 Connectivity Testing of Components

D. *Observation and Maintenance Phase*

Finally, the fourth phase focuses on the continuous monitoring of the system to ensure its proper functioning in the long term. This phase includes detailed observations and periodic performance analyses of the components, with the goal of detecting possible anomalies or areas for improvement. To ensure an efficient response, a maintenance plan (See Table 6) has been developed, which includes ongoing improvements and adjustments based on the results of these analyses. These adjustments may include software updates, modifications to detection rules, or changes to the configuration of the agents and notification tools. This process ensures that the system maintains its efficiency, reliability, and security, adapting to any changes in the environment or new threats.

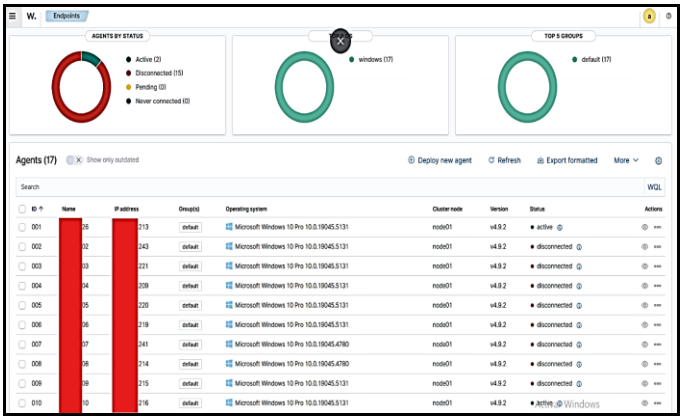

Fig. 12 List of Connected Agents

TABLE VI
MAINTENANCE PLAN

Phase	Task	Frequency
Monthly Maintenance	Review of alerts, configuration adjustments, and continuous improvements	Monthly
Updates	Installation of Wazuh and Slack updates	Quarterly
Constant Technical Support	Ongoing support for problem resolution and system adjustments.	Daily / Ad-hoc
Integration with Other Applications	Evaluation and integration of new applications with Wazuh and Slack.	Annual
Continuous Adjustments and Improvements	Implementation of adjustments based on feedback and performance analysis.	Monthly / Ad-hoc

V. RESULTS AND DISCUSSION

To evaluate the proposed method, which involves implementing Wazuh for monitoring and vulnerability detection, the results obtained were analyzed in terms of effectiveness and responsiveness. In this chapter, we present the most relevant findings, highlighting how the system has met expectations and comparing it with other similar solutions available in the market.

A. *Results*

A.1. Event Monitoring: Wazuh enabled effective monitoring of security events, providing a clear overview of activities within the BGyAVE infrastructure. During November 2024, a total of 115,311 events were recorded, including 44,584 successful authentication events and 37 authentication failure events (see

Figure 13). The latter represent failed login attempts, which may indicate possible intrusion attempts or errors in the login process. Although the number of failures is low compared to successful logins, the early identification of these events is crucial for strengthening security and preventing unauthorized access. Continuous monitoring of these events, provided by Wazuh, allows for the detection of unusual patterns and a swift response to any potential threat.

A.2. Vulnerability Detection: The deployment of Wazuh on the 17 computers of the BGyAVE during November 2024 allowed for the identification of a total of 135 vulnerabilities, which were classified according to their severity into four levels: Critical Severity, High Severity, Medium Severity, and Low Severity (see Table 7). These vulnerabilities were detected throughout the evaluation period, ranging from critical risks that could have severely compromised system security to lower-impact vulnerabilities that, while not urgent, required monitoring and correction to maintain a secure environment. The distribution of vulnerabilities by severity level is presented in Table 8, which details the number of vulnerabilities identified on each computer (agent) of the BGyAVE. Additionally, the statistics are graphically presented in Figure 14, providing a clearer and more understandable visualization of the data.

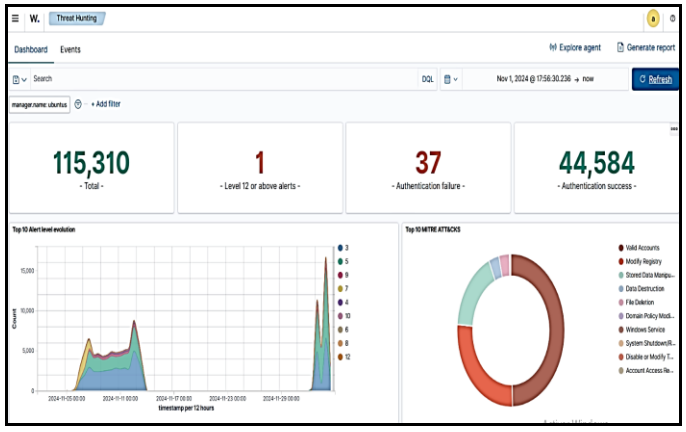

Fig. 13 Total events monitored by Wazuh - November 2024

TABLE VII
SEVERITY LEVEL OF IDENTIFIED VULNERABILITIES

No	Severity Level	Description (related to vulnerabilities)
1	Critical Severity	Critical vulnerabilities that can be exploited immediately, severely compromising system security. Urgent resolution required.
2	High Severity	Serious vulnerabilities that pose a significant risk, but not imminent. Should be addressed promptly to prevent exploitation.
3	Medium Severity	Moderate vulnerabilities that present a risk, but not immediate. Requires monitoring and correction to prevent escalation.
4	Low Severity	Minor vulnerabilities with low impact on security but should be monitored and corrected to maintain adequate protection.

TABLE VIII
NUMBER OF IDENTIFIED VULNERABILITIES

Agent	Critical Severity	High Severity	Medium Severity	Low Severity
001	1	2	5	0
002	1	2	5	0
003	1	2	5	0
004	1	2	5	0
005	1	2	5	0
006	1	2	5	0
007	1	2	5	0
008	1	2	5	0
009	1	2	5	0
010	1	2	5	0
011	1	2	5	0
012	0	22	9	0
013	1	2	5	0
014	1	2	5	0
015	0	0	0	0
016	0	0	0	0
017	0	0	0	0
Total	**13**	**48**	**74**	**0**

Fig. 14 Total Identified Vulnerabilities by Severity Level

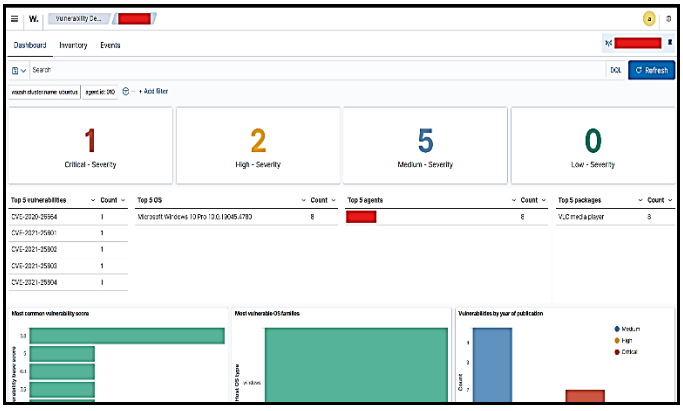

Fig. 15 Individual Vulnerability Report of a Device (Host)

Wazuh enabled precise and detailed identification of vulnerabilities across each of the 17 computers (agents) of the BGyAVE, revealing that the detected vulnerabilities primarily affected operating systems such as Microsoft Windows 10 Pro, as well as specific applications like VLC Media Player (see Figure 15). A key aspect of these reports is the use of Common Vulnerabilities and Exposures (CVE), a standardized database that assigns a unique identifier to each known vulnerability. The reports highlighted critical and high-severity vulnerabilities that could have compromised system security, underscoring the importance of constant monitoring and the implementation of corrective measures.

A.3. Notifications: The integration of Wazuh with Slack has generated 115,310 automatic notifications in November 2024, marking a significant shift from the previous system, where alerts were not managed automatically and the entire process was manual. This advancement has enabled the BGyAVE Telematics Section team to receive real-time alerts, transforming the way they monitor security events. The visibility of incidents has improved significantly, and the response to threats has become faster and more efficient. Figure 16 shows how these notifications arrive in Slack, providing detailed information on events, such as those related to "unknown user" or "incorrect password," which are classified as level 5 alerts.

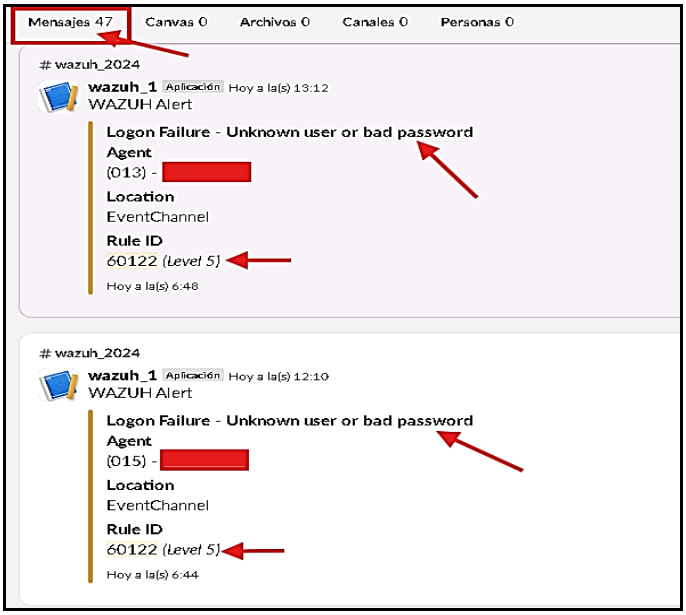

Fig. 16 Event Notifications in Slack

B. Discussion

The implementation of Wazuh in BGyAVE has transformed cybersecurity management, providing a comprehensive approach to detecting, monitoring, and responding to vulnerabilities and security events. Thanks to its ability to automatically identify vulnerabilities from the moment the agent is installed and configured, the team has been able to address security issues more quickly and efficiently. During the evaluation period, Wazuh recorded a total of 115,311 events, including 44,584 successful authentications and 37 authentication failures, enabling the detection of unusual patterns and rapid response to unauthorized access attempts. Additionally, real-time monitoring has facilitated the identification of more complex events, such as unauthorized access, modifications to sensitive files, and privilege escalations, enhancing infrastructure visibility and enabling more agile and coordinated responses. In terms of vulnerability detection, Wazuh identified 135 vulnerabilities across 17 computers in BGyAVE, categorizing them by severity levels for efficient prioritization. Its ability to use CVE identifiers has allowed for structured corrective measures, significantly reducing exposure time to security risks. One of the most significant aspects of the implementation has been the transformation of alert management. With 115,310 automatic notifications generated in November 2024, the team has shifted from reactive monitoring to a proactive approach, ensuring a faster response to potential incidents. This improvement has optimized operational security and reduced reaction times to critical threats. Unlike tools such as Greenbone Security Assistant [29], which primarily focus on identifying vulnerabilities and assessing their severity, Wazuh offers a more comprehensive approach. It not only detects threats but also generates real-time notifications, allowing for immediate and coordinated responses. While Greenbone is limited to a static vulnerability analysis without active monitoring, Wazuh has proven to be a more effective solution for BGyAVE's operational security, ensuring that every incident is managed with greater efficiency. However, when considering Wazuh for larger-scale deployments, certain challenges must be addressed. As the number of monitored endpoints increases, the system may require additional resources in terms of hardware and network capabilities to maintain its performance. Managing a higher volume of data can lead to increased demands on storage and processing power, requiring careful scaling and configuration to ensure optimal functionality. Additionally, coordination among multiple teams might be needed to maintain the system's responsiveness in large, complex environments. Despite these challenges, Wazuh's architecture allows for flexibility and scalability, meaning that with proper planning and investment, it can effectively support large-scale deployments without compromising performance.

VI. Conclusions

The implementation of Wazuh in BGyAVE represents a significant advancement in cybersecurity management, optimizing the processes of threat detection, monitoring, and response. Throughout its deployment, 115,311 security events were recorded, providing the Telematics Section team with a comprehensive view of network activity and enhancing its ability to respond to critical incidents efficiently. One of the most notable achievements was the identification of 135

vulnerabilities across the 17 computers where the agent was installed, demonstrating Wazuh's effectiveness in early risk detection. Unlike other solutions, such as Greenbone Security Assistant, Wazuh not only identifies vulnerabilities but also offers continuous monitoring and a real-time alert system, significantly reducing response times to potential threats. The ability of Wazuh to generate automated notifications has been a crucial factor in improving security monitoring. These real-time alerts have facilitated the prompt detection and mitigation of critical events, including unauthorized access attempts, modifications to sensitive configurations, and privilege escalations. This functionality has enabled the team to optimize response times and achieve more efficient coordination in incident management. Finally, Wazuh has proven to be a powerful tool in security event monitoring, optimizing both vulnerability detection and incident management through its integration with Slack for automatic notifications. This solution has substantially improved the response capability to attacks, becoming a key element in protecting the institution's technological infrastructure. Looking ahead, future improvements could involve integrating machine learning-based threat detection systems. This innovation would further enhance the ability to identify complex attack patterns, offering a more dynamic and proactive approach to cybersecurity management.

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] D. G. Cuautle, "ESET," 18 09 2024. [En línea]. Disponible en: https://www.welivesecurity.com/es/malware/amenazas-mas-detectadas-latam-primer-semestre-2024/. [Accedido: 20 11 2024].

[2] M. M. Riofrío, "Ebiz," 06 09 2024. [En línea]. Disponible en: https://ebiz.pe/noticias/el-alto-costo-de-la-cibercriminalidad-jorge-zeballos/.

[3] P. Valdivia, "El Comercio," 22 08 2024. [En línea]. Disponible en: https://elcomercio.pe/tecnologia/ciberseguridad/peru-se-alza-como-un-foco-de-ataques-ciberneticos-en-latinoamerica-malwere-phishing-ransomware-noticia/.

[4] "Digital.ai," [En línea]. Disponible en: https://digital.ai/es/glossary/what-is-threat-monitoring/. [Accedido: 2 12 2024].

[5] "Kaspersky," [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security. [Accedido: 2 12 2024].

[6] M. K. Gregg Lindemulder, "IBM - cybersecurity," 12 agosto 2024. [En línea]. Disponible en: https://www.ibm.com/es-es/topics/cybersecurity.

[7] A. de L. Dueñas, "Minery Report," abril 2024. [En línea]. Disponible en: https://mineryreport.com/blog/siem-ciberseguridad-unificacion-seguridad-inteligencia/. [Accedido: 2 12 2024].

[8] "CHECK POINT," [En línea]. Disponible en: https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-siem-security-information-and-event-management/. [Accedido: 2 12 2024].

[9] "CyberSeg," 8 junio 2023. [En línea]. Disponible en: https://www.cyberseg.solutions/los-mejores-siem-security-information-and-event-management/. [Accedido: 2 12 2024].

[10] M. F. Delgado, "linkedin.com," 13 agosto 2023. [En línea]. Disponible en: https://es.linkedin.com/pulse/wazuh-como-herramienta-siem-esencial-para-la-de-tu-maurice.

[11] 4Geeks, "4Geeks," [En línea]. Disponible en: https://4geeks.com/es/lesson/wazuh-siem-y-edr-para-ciberseguridad#wazuh-es-utilizado-por-una-amplia-gama-de-organiza. [Accedido: 2 12 2024].

[12] IBM, "vulnerability-management," [En línea]. Disponible en: https://www.ibm.com/mx-es/topics/vulnerability-management.

[13] C. S. Global, "cyber security global," 5 abril 2024. [En línea]. Disponible en: https://cyber-security.global/monitoreo-seguridad-informatica/.

[14] IBM, "open-source," [En línea]. Disponible en: https://www.ibm.com/mx-es/topics/open-source.

[15] Amazon Web Services, "Amazon Web Services," [En línea]. Disponible en: https://aws.amazon.com/es/what-is/open-source/. [Accedido: 02 diciembre 2024].

[16] "Slack," [En línea]. Disponible en: https://slack.com/.

[17] Y. Hernandez, "DONGEE," 15 diciembre 2022. [En línea]. Disponible en: https://www.dongee.com/tutoriales/que-es-slack-y-como-funciona/. [Accedido: 02 diciembre 2024].

[18] J. P. Cózar, Implementación de Wazuh en una Organización Pública, Cataluña: Universidad Oberta de Cataluña, 2020, p. 137.

[19] B. S. Jumiaty, SIEM e Inteligencia de amenazas: Protección de aplicaciones con Wazuh y Thehive, Indonesia: Proquest, 2024.

[20] R. E. Sousa y S. Vale, "Un enfoque para la identificación y el análisis forense de ataques DNS," *Rev. Cient. Multidisciplinar Núcleo do Conhecimento*, vol. 8, no. 7, pp. 24-44, jul. 2023. [En línea]. Disponible en: https://www.nucleodoconhecimento.com.br/ciencias-de-la-computacion/analisis-forense. [Accedido: 29 ene. 2025].

[21] C. A. Clavijo Salazar, C. A. Solórzano Ramón, J. E. Sanmartín Pangay, y R. A. Castro Arreaga, *Detección de ataques informáticos mediante un SIEM Open Source Wazuh para los servicios digitales de la banca web*, Maestría en Ciberseguridad, UIDE, Quito, 2024, 70 p.

[22] E. Alanis, "Ciberseguridad: Impacto y detección de eventos de seguridad mediante prototipo de monitoreo," *Ciencia Latina Internacional*, vol. 8, no. 3, p. 16, 2024.

[23] L. E. Luis Chiluiza, "Detección y solución de vulnerabilidades con," *Revista Ibérica de Sistemas e Tecnologías de Información*, vol. E, no. 57, pp. 560-570, 2023.

[24] J. G. Sánchez, M. N. Mendoza, and G. M. Garzón, "Vulnerabilidades de sitios web gubernamentales en Ecuador: Un estudio exploratorio pre-muestral," *Rev. Ibérica de Sistemas e Tecnologias de Informação*, vol. E, no. 29, pp. 67–78, 2020.

[25] E. C. F. Gómez, O. X. B. Almeida, and L. M. A. Gamboa, "Análisis de los sistemas centralizados de seguridad informática a través de la herramienta Alienvault Ossim," *Ecuadorian Science Journal*, 2022.

[26] M. R. Kamal, "Detection of anomalies with security information and event management (SIEM) using Splunk on the network of Islamic University of Indonesia," *AUTOMATA*, vol. 2, no. 2, 2021.

[27] J. X. Játiva Alvarez and L. A. Muñoz Alvarez, "Implementación de un gestor de información y eventos de seguridad (SIEM) para la prevención y detección de ciber amenazas en una entidad gubernamental," *Universidad Internacional Sek*, Oct. 2022.

[28] Quinto Huamán, C., & Picón Huacarpuma, R. M. (2023). Uso de la Inteligencia Artificial en el Ejército del Perú: Desafíos y Oportunidades. *Revista CITEK*, *6*(06). Recuperado a partir de https://revistas.icte.edu.pe/citek/article/view/34

[29] L. Chiluiza and L. Enciso, *Detección y solución de vulnerabilidades con Greenbone Security Assistant*, Loja - Ecuador: Proquest, 2023