INTECHBIZ2025
International Conference on Industrial Technology and Business

Implementation of Wazuh as a SIEM System for Network Attack Detection

Nurmi Hidayasari[1], Kasmawi[2], Mansu[3], Zuliar Efendi[4]
[1,2,3,4]*Department of Informatics Engineering, Politeknik Negeri Bengkalis, Indonesia*)
nurmihidayasari@polbeng.ac.id[1], kasmawi@polbeng.ac.id[2], mansur@polbeng.ac.id[3],
zuliarefendi@polbeng.ac.id[4]

Abstract

This study presents the deployment of Wazuh as a Security Information and Event Management (SIEM) system for detecting attacks on a network. Wazuh is configured as an open-source solution capable of collecting, monitoring, and analyzing security logs in a centralized manner. In this implementation, the Wazuh Manager is deployed on a Virtual Private Server (VPS) as the central log processing component, while the Wazuh Agent is installed on a web server to monitor system activities, collect web server logs, and detect file modifications through the File Integrity Monitoring (FIM) feature. Testing was conducted by simulating attacks such asSQL Injection and file modifications within the web directory. The results demonstrate that Wazuh successfully detected these suspicious activities and displayed real-time alerts through its dashboard. These findings indicate that Wazuh is effective as a SIEM system for attack detection, enhancing security visibility and strengthening early threat detection within network environments. Furthermore, this implementation provides a foundation for future development, including the integration of automated incident response and AI-based threat analysis.

Keywords : Wazuh, SIEM, Attack Detection, Security Log, Network Monitoring

1. INTRODUCTION

The evolution of computer network infrastructures has introduced new challenges to safeguarding information systems. Threats such as malware, data exfiltration, and unauthorized activities are increasing in both volume and sophistication, requiring organizations continuous monitoring to detect anomalies, and respond to suspicious behavior in real time. In practice, many small-to-medium organizations and academic environments still lack early-detection capabilities and centralized security monitoring, leading to delayed discovery and suboptimal mitigation of incidents.

Security Information and Event Management (SIEM) aggregates, analyzes, and visualizes security logs from diverse sources to enhance visibility and support incident response. Recent surveys describe SIEM core functions (collection, correlation, prioritization) and emerging needs such as visual analytics and automation (González-Granadillo et al., 2021). However, commercial SIEMs (e.g., Splunk, IBM QRadar, ArcSight) often entail high licensing costs and deployment complexity, which can be misaligned with constrained budgets and teams. In this context, open-source platforms—particularly Wazuh—offer a viable alternative by delivering core SIEM functions with lower cost and flexible integration with the Elastic Stack. Comparative evaluations find open-source SIEMs appropriate for SMEs and educational labs, with attention to performance metrics such as events per second (EPS) and security feature coverage (Manzoor et al., 2024). Head-to-head studies between IBM QRadar and Wazuh further illuminate cost–capability trade-offs relevant to adopters (Šuškalo et al., 2023).

Beyond baseline correlation and alerting, applied works show Wazuh's extensibility—e.g., enriching detection with machine learning to improve alert quality (Chamkar et al., 2025), integrating Wazuh with TheHive to streamline case management and incident response (Jumiaty & Soewito, 2024), and leveraging File Integrity Monitoring (FIM) to flag near-real-time web content tampering/defacement (Kurniawan & Triayudi, 2024). Despite these advances, there remains a shortage of compact, well-documented, end-to-end prototypes that smaller organizations can deploy readily—from guided setup and common attack simulations (e.g., repeated failed logins, website file changes) to on-dashboard alert verification.

Despite these findings, most studies still have certain limitations, such as focusing only on specific attack types, lacking detailed configuration documentation, or conducting experiments on small-scale environments. Few studies have examined practical implementation and real attack simulation (e.g., SQL Injection, file modification) that can be easily replicated by small organizations or academic environments.

Therefore, this research focuses on the implementation of Wazuh as a SIEM system for detecting attacks in a controlled network environment. The study includes architecture preparation, installation, configuration and attack simulations to assess system responsiveness. The outcomes is a practical overview of how Wazuh can be applied in real-world monitoring environments.

2. REVIEW OF LITERATURE

2.1 SIEM (Security Information and Event Management)

SIEM is a system used to monitor and detect attacks and to coordinate security responses by analyzing logs from diverse events collected in real time. The technology has broad data-collection coverage and can correlate and analyze events from multiple sources to determine whether an incident constitutes an attack. SIEM analytics span all enterprise applications, network devices, security appliances, and servers. In practice, a SIEM aggregates and analyzes data from across an organization's IT infrastructure—such as logs from network devices, operating systems, applications, and security tools—to detect suspicious activity or security threats (Shafiyyah, 2024).

Research by Garcia et al. emphasizes that SIEM plays a pivotal role in early detection of security incidents and serves as a foundational component within cyber threat intelligence architectures (Garcia et al., 2018).

2.2 Wazuh as an Open Source SIEM Platform

Wazuh is an open-source SIEM platform that provides threat detection, file integrity monitoring, log analysis, and automated response capabilities. Wazuh integrates with the ELK Stack (Elasticsearch, Logstash, and Kibana) for log data storage and visualization. According to its official documentation (Wazuh, 2023), Wazuh is capable of detecting abnoarmal behavior , such as brute force attacks, SQL injection attacks, XSS attacks, privilege escalation attacks, and many more using a signature-based detection rule system.

3. METHOD

This research model is built on an input–process–output approach to illustrate the research flow related to the implementation of a Wazuh-based SIEM. This can be seen in the figure below.

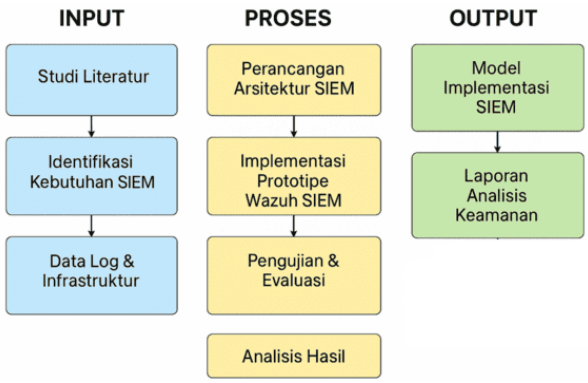


Fig. 1. Research Model

Input (Preparation and System Design Phase)

The research began by identifying the core issue of information security, particularly the need for a centralized system capable of monitoring and detecting security incidents in

real time. A comprehensive literature review was conducted covering the concepts of SIEM, supporting technologies such as Wazuh, Elastic Stack, and IDS/IPS mechanisms, as well as previous studies relevant to open-source SIEM implementations. Based on the review, system requirements were defined, including the necessary hardware and software specifications to support the development of the prototype.

Process (Implementation and Testing)

The core research process consisted of three main stages:

System Design:

The design stage focused on developing the SIEM architecture tailored to the research objectives, covering data flow for log collection, analysis mechanisms, and visualization processes. The architecture ensures centralized management of security events across monitored hosts. The designed architecture can be seen in Figure 2.

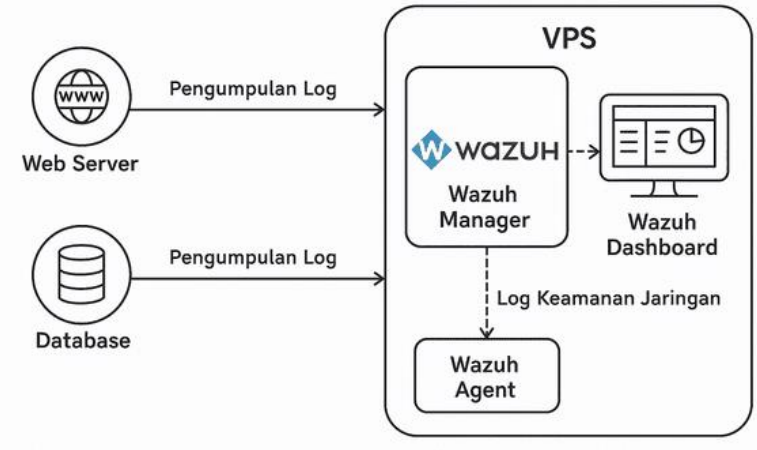


Fig. 2. Wazuh-Based SIEM Architecture

Prototype Implementation:

The prototype implementation involved installing and configuring Wazuh components — including the *Wazuh Manager*, *Wazuh Agent*, and the visualization dashboard. Detection rules were also customized to identify specific security incidents such as unauthorized login attempts and file modifications.

Testing and Evaluation:

In this stage, several simulated attacks were conducted to assess the detection capability of the system. The simulated scenarios included vulnerability scanning, port scanning, and SQL injection attacks. The generated alerts and detection accuracy were then evaluated to measure the system's effectiveness in identifying real-time threats.

Output (Results and Discussion)

The output of this research is a functional prototype of a Wazuh-based SIEM system capable of collecting, analyzing, and visualizing security data through alerts and dashboard representations. Additionally, the study produced an analysis of SIEM effectiveness in detecting various attack scenarios and provided recommendations for practical implementation and future system enhancement in real organizational environments.

4. RESULT & DISCUSSION

System Implementation Overview

The prototype of the Wazuh-based SIEM system was successfully deployed according to the planned architecture. The *Wazuh Manager* was hosted on a Virtual Private Server (VPS) to serve as the central log analysis and management node, while *Wazuh Agents* were installed on monitored hosts, including a web server running Apache. The integration with the Wazuh dashboard provided a real-time monitoring interface for visualizing security alerts and system health status.

- Install Wazuh using the following commands:
- curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add -
- echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee /etc/apt/sources.list.d/wazuh.list
- sudo apt update
- sudo apt install wazuh-manager -y

The basic configuration of the Wazuh Manager was carried out by accessing its main configuration file located at `/var/ossec/etc/ossec.conf`. The contents of this file can be modified according to the system requirements. After completing the configuration, the Wazuh Manager service was activated using the following commands:

- `sudo systemctl enable wazuh-manager`
- `sudo systemctl start wazuh-manager`
- `sudo systemctl status wazuh-manager`

To enable log monitoring through the graphical user interface (GUI), the Wazuh dashboard was installed by executing the following commands:

- `curl -s0 https://packages.wazuh.com/4.9/wazuh-install.sh`
- `sudo bash wazuh-install.sh -I`

Once the installation was completed, the Wazuh Manager dashboard could be accessed via a web browser using the following URL: *https://103.210.221.65*. The initial display image of Wazuh Manager or Wazuh Monitor can be seen in Figure 3.

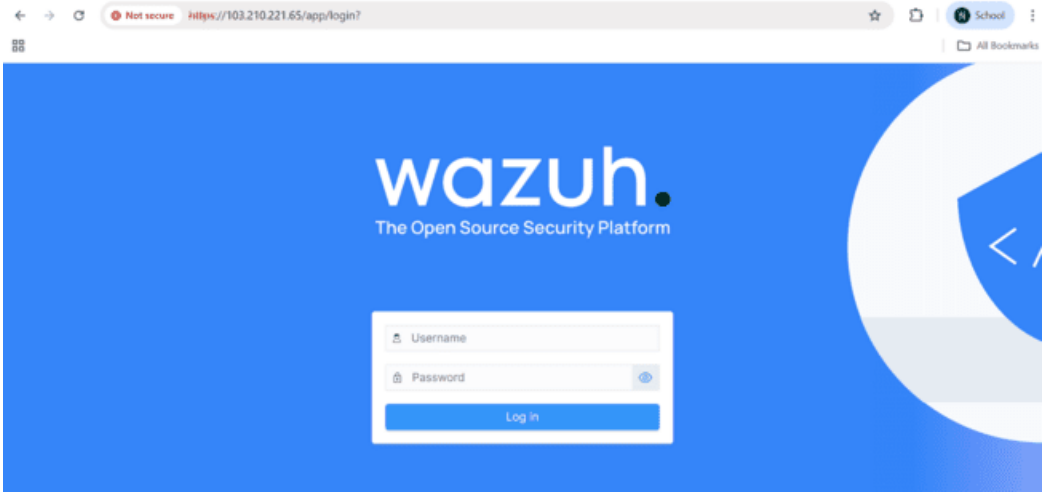


Fig. 3. Wazuh Manager Initial View

The next step was the configuration process of the Wazuh Agent, which is the component of Wazuh installed on the endpoint. In this study, the Wazuh Agent was deployed on a cloned version of the website application belonging to the Department of Informatics Engineering (TI), which was hosted on a separate Virtual Private Server (VPS). This setup allowed the system to simulate real network activity and security events for monitoring and detection.

The installation of the Wazuh Agent was performed using the following commands:

```
sudo apt update
sudo apt install wazuh-agent -y
```

After installation, the main configuration file located at `/var/ossec/etc/ossec.conf` was modified to define the connection between the agent and the Wazuh Manager. The manager's IP address (`<address>103.210.221.65</address>`) was specified in the `<server>` section to ensure that all logs collected by the agent would be transmitted to the centralized management server.

Once the configuration was completed, the agent service was activated and registered with the Wazuh Manager using the following commands:

```
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
sudo systemctl status wazuh-agent
```

The registration process was verified through the Wazuh dashboard, where the newly added agent appeared in the *Agents* section with an "Active" status. This confirmed that communication between the agent and the manager had been successfully established, enabling real-time monitoring of security events generated by the web server.

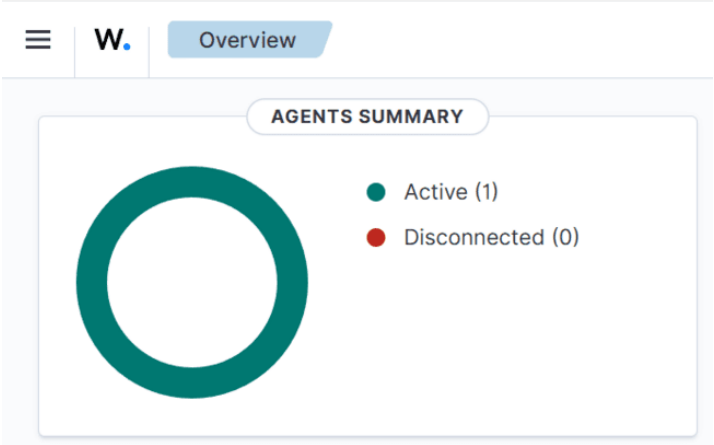


Fig. 4. Agent Successfully Activated

Attack Simulation and Detection Results

To evaluate the performance of the prototype, several attack scenarios were simulated in a controlled environment:

Vulnerability Scanning:

Active scanning was performed using the OWASP ZAP tools to examine the system's detection capability by generating automated vulnerability-scanning attacks and monitoring the system's corresponding responses.

Port Scanning Activity:

Network scanning was conducted using *Nmap* to map open ports on the target host. The Wazuh agent detected the unusual connection pattern through the *ossec.conf* active response module, classifying the behavior as reconnaissance activity. The system logged detailed information, including the scanned ports and source host, allowing the administrator to identify potential intrusion attempts.

SQL Injection Attempt:

In this evaluation, SQL Injection attacks were simulated on two common web input points: the URL parameter and the search form. The URL-based test was performed by manipulating query parameters using simple payload. For the search form, SQL Injection attempts were executed by inserting logical expressions to determine whether the application processed user input without sanitization. These simulations were conducted to assess the system's ability to detect and handle SQL Injection attempts on areas other than the login form.

File Modification Detection:

The *File Integrity Monitoring (FIM)* module detected unauthorized changes in critical web directories. When a modified file was uploaded or altered, Wazuh automatically recorded the event and generated a high-priority alert, displaying the modified path, file hash changes, and the responsible process.

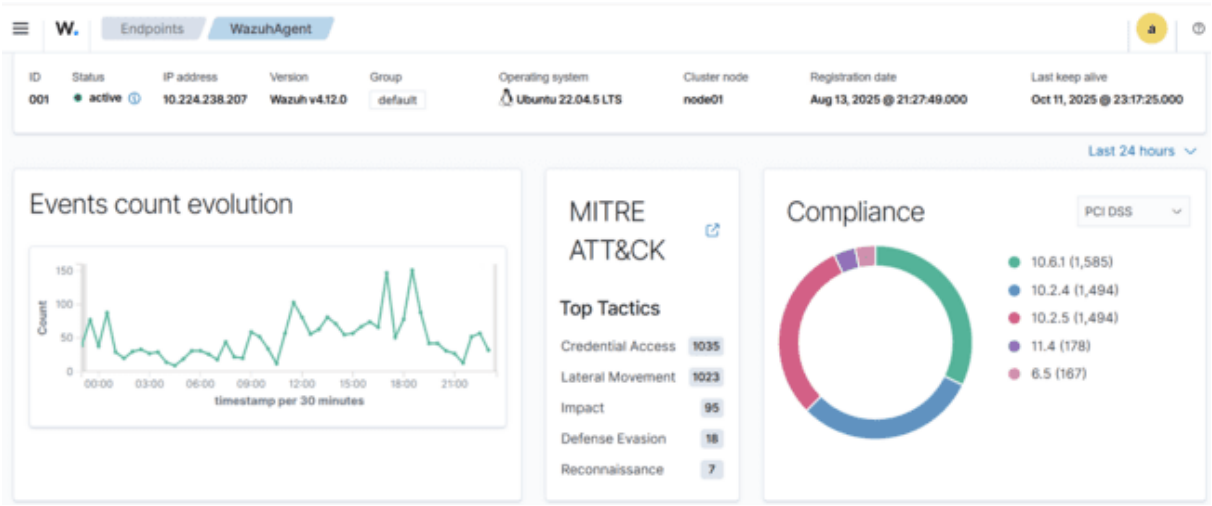


Fig. 5. Wazuh Dashboard showing real-time alerts and agent status.

Figure 5 illustrates the Wazuh Dashboard interface that provides a comprehensive view of real-time security monitoring. The "Events Count Evolution" graph shows fluctuations in detected events within a 24-hour window, indicating system activity intensity. The MITRE ATT&CK panel categorizes detected behaviors into tactical groups such as Credential Access, Lateral Movement, and Impact. Meanwhile, the Compliance section displays adherence to PCI DSS standards. This visualization enables administrators to quickly interpret system health, identify abnormal patterns, and take proactive measures in maintaining network security.

Discussion

The test results indicate that Wazuh can effectively function as a lightweight SIEM platform capable of detecting and alerting on multiple types of attacks in real time. Its modular design allows integration of additional open-source tools such as Suricata or Zeek for advanced intrusion detection.

The Wazuh dashboard provided detailed and interactive visualization of all alerts in real time. Each alert displayed contextual information, including timestamp, source IP, severity level, and event description, allowing analysts to quickly identify and respond to potential threats. The dashboard also categorized alerts by severity (low, medium, high, critical), helping prioritize incident handling efficiently.

Overall, the testing demonstrated that Wazuh's open-source SIEM framework can perform comprehensive log collection, real-time event correlation, and alert visualization effectively. Despite being a lightweight and cost-efficient system, the prototype showed performance comparable to commercial SIEM platforms in small-to-medium network environments.

5. CONCLUSION

This study successfully implemented Wazuh as an open-source Security Information and Event Management (SIEM) system for real-time detection of network attacks. The developed prototype effectively collected, analyzed, and visualized security logs from multiple sources, providing actionable insights for incident detection and monitoring.

Experimental results demonstrated that Wazuh was capable of identifying several types of network attacks such as vulnerability scanning, port scanning, SQL injection, and file modification. The alert dashboard provided interactive visualization and facilitated fast threat assessment, allowing administrators to identify attack sources and affected endpoints efficiently.

The implementation also showed that open-source SIEM solutions like Wazuh can serve as viable alternatives to commercial systems, particularly for academic institutions or small organizations with limited resources. However, the current prototype still faces several limitations, including scalability challenges and dependency on regularly updated rule sets for accurate detection.

For future work, the system can be enhanced by:

- Integrating Wazuh with other security monitoring tools such as Suricata or Zeek to expand network visibility.
- Applying machine learning–based anomaly detection to improve threat prediction and reduce false positives.
- Developing automated incident response mechanisms to accelerate mitigation and containment actions.

In summary, this research demonstrates that Wazuh can serve as a strong foundation for building a comprehensive and intelligent SIEM framework that enhances network visibility, improves threat detection capabilities, and supports proactive cybersecurity management.

.

6. ACKNOWLEDGEMENTS (optional)

The authors would like to acknowledge the financial and technical support provided by Politeknik Negeri Bengkalis (Polbeng) under the institutional research grant scheme. This support has been instrumental in enabling the successful execution of this research project.

7. REFERENCES

Chamkar, S. A., Zaydi, M., Maleh, Y., & Gherabi, N. (2025). Improving threat detection in Wazuh using machine learning techniques. *Journal of Cybersecurity and Privacy, 5*(2), 34. https://doi.org/10.3390/jcp5020034.

Garcia, S. (2018). A Framework for Evaluating SIEMs in Real Environments. *Journal of Information Security and Applications*.

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors, 21*(14), 4759. https://doi.org/10.3390/s21144759.

Jumiaty, & Soewito, B. (2024). SIEM and threat intelligence: Protecting applications with Wazuh and TheHive. *International Journal of Advanced Computer Science and Applications, 15*(9), 239–251. https://doi.org/10.14569/IJACSA.2024.0150923.

Kurniawan, C., & Triayudi, A. (2024). File integrity monitoring as a method for detecting and preventing web defacement attacks. *JOIN: Jurnal Online Informatika, 9*(2), 276–285. https://doi.org/10.15575/join.v9i2.1326.

Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *PLOS ONE, 19*(3), e0301183. https://doi.org/10.1371/journal.pone.0301183

Shafiyyah, A. (2024). *Implementasi Sistem Keamanan Jaringan Di Psdku Universitas Lampung Waykanan Menggunakan Server Wazuh Untuk Deteksi Dan Respon Serangan Siber*.

Šuškalo, D., Morić, Z., Redžepagić, J., & Regvart, D. (2023). Comparative analysis of IBM QRadar and Wazuh for security information and event management. In B. Katalinic (Ed.), *Proceedings of the 34th DAAAM International Symposium* (pp. 96–102). DAAAM International. https://doi.org/10.2507/34th.daaam.proceedings.014