Engineering and Technology Journal e-ISSN: 2456-3358

Volume 11 Issue 05 May-2026, Page No.-10138-10143

DOI: 10.47191/etj/v11i05.50, I.F. – 8.595

Wazuh SIEM Implementation with Agent and pfSense Integration

Ashvini Bais[1], Asakti Rautkar[2], Ketan Bodhe[3], Kamlesh Kalbande[4], Pooja Kalbande[5]

[1,2,3,4,] Faculty, G H Raisoni College of Engineering, Nagpur, Maharashtra, India.

[5]Faculty, G H Raisoni College of Engineering and Managment, Nagpur, Maharashtra, India.

ABSTRACT: In the current digital era, organizations are constantly facing an array of security threats that can compromise sensitive information and interfere with their operations. For them to properly safeguard their assets, companies need to implement powerful security monitoring systems. One example is Wazuh, an open-source security information and event management (SIEM) system that provides end-to-end visibility into an organization's security posture. The focus of this project is to install and set up Wazuh, including the installation of agents on different endpoints, such as Windows and Linux. Through log gathering and forwarding to the Wazuh server, we can guarantee that important security incidents are recorded and analyzed. The integration of log sources, such as pfSense firewalls, is an essential part of this process and helps us to better identify possible security threats. Also, the project will entail the establishment and personalization of rules and decoders in Wazuh to adapt its detection to the particular requirements of our company. This will allow us to better detect and react to security incidents by correlating events and triggering timely alerts. In addition to incident detection and response, Wazuh will also be used for monitoring compliance, ensuring our organization complies with applicable security standards and regulations. With the ability to produce compliance reports and observe system configurations, we are able to stay in a robust security stance and avoid risks. The significance of this project is underscored by the burgeoning number of cybersecurity incidents. As per CERT-In (Indian Computer Emergency Response Team), more than 1.2 million cybersecurity incidents occurred in India during 2023 alone, such as targeted attacks on government, healthcare, and financial institutions. The scenario turned worse in 2024 with cybercrime complaints crossing 25 lakh and estimated losses crossing Rs 20,000 crore. Through this project, we hope to create an overarching security monitoring system that not only increases our ability to respond to incidents, but also assists with compliance. In the end, we hope to help create a safer organizational environment in the wake of these increasing threats.

KEYWORDS: Cyber security, Wazuh, Threat Detection, Compliance Monitoring, pfSense firewall.

I. INTRODUCTION

Organizations in today's cybersecurity scenario are confronted with some major challenges, such as an ineffectual security stance resulting from the limitation of implementing Wazuh and pfSense separately, resulting in gaps in the detection and response to threats. Moreover, the lack of automated response usually leads to delayed incident response times, resulting in higher possibilities of the impact of security vulnerabilities. Inaccurate threat detection is also a problem, as decoupling log analysis and network traffic monitoring can cause security events to be missed or misread. In addition, regulatory compliance for security monitoring and reporting becomes tedious without an integrated unification of security tools. Security operations teams will also experience usability problems with multiple separate solutions to deal with, having trouble effectively handling incidents when they have multiple standalone solutions to work with. Finally, organizations would have to bear greater expense and less ROI when using conventional security measures rather than taking advantage of the combined functionality of Wazuh and pfSense.

The integration of Wazuh and pfSense was selected for its power to integrate real-time log examination with effective network security, offering a complete security solution. This approach is simpler than others since the two tools are open-source, highly supported, and have automated many security operations, thus minimizing the effort required and accelerating incident response. This integration provides centralized visibility and simplified management and hence is a cost-effective and cost-effective for organizations.

The growing complexity of cyber threats, IT environment complexity, regulatory compliance requirements, and the demand for real-time monitoring and response have made it an urgent requirement for the availability of efficient security solutions. Wazuh and pfSense fill this gap through effective monitoring, threat detection, and network protection features that allow organizations to strengthen their security posture amidst the ever-changing cyber environment.

The coupling of Wazuh with pfSense strengthens security monitoring by allowing thorough analysis of firewall logs and security incidents, providing in-depth insights into network security. This coupling also allows for the triggering of automated actions in response to identified threats, including blocking the malicious IP addresses and notifying administrators, thus reducing incident response times. Additionally, it provides an end-to-end security strategy that integrates network perimeter defenses (pfSense) and internal monitoring and analysis (Wazuh), providing a layered security plan. Wazuh identifies security concerns by monitoring and analyzing log data in real-time, allowing for rapid detection and mitigation of events. This is supplemented by pfSense, which tracks network activity and produces alerts for unusual behavior, allowing automated remediation for threats and reducing overall incident response time. The combination of Wazuh and pfSense plays a vital role in the detection and resolution of security incidents in a timely manner, which is essential for security maintenance.

Wazuh constantly monitors log data to detect anomalies, while pfSense sends alerts for suspected breaches. The automated response of the system towards the detected threat, for instance, blocking the malicious IP address, minimizes the time taken to resolve incidents, thus enhancing the security posture. Early detection and response are critical to reducing potential harm and data loss, enabling organizations to have an active security posture. This combination of Wazuh and pfSense improves the ability to quickly detect and respond to security incidents, protecting organizational assets efficiently.

II. BACKGROUND

A. Overview of SIEM Solutions

Security Information and Event Management (SIEM) solutions are a vital piece of contemporary cybersecurity measures. They offer organizations the capability to gather, analyze, and act on security information from disparate sources in real-time. SIEM systems collect log information from servers, network devices, applications, and other endpoints, allowing security teams to identify anomalies, investigate events, and verify compliance with regulatory requirements. The active monitoring and threat detection features of SIEM tools are necessary for the prevention of risk and guarding sensitive data.

B. Wazuh Overview

Wazuh is an open-source SIEM tool that has emerged as popular due to its extensive security monitoring features. Initially a fork of the OSSEC project, Wazuh has grown to encompass features like log data analysis, intrusion detection, vulnerability detection, and compliance reporting. It offers a single pane of glass for the monitoring of security events across multiple environments so that organizations can have insights into their security stance. Wazuh's scalability and flexibility make it an ideal solution for small, medium, and large organizations.

C. Overview of pfSense

pfSense is open-source firewall and router software that provides advanced network security features. It is heavily used due to its capacity for traffic filtering, virtual private networks (VPNs) support, and granular logging and monitoring. pfSense enables organizations to build secure network designs and manage traffic efficiently. It has an easy-to-use interface and has well-documented features, which make it easily available for use by both beginner and advanced network administrators. Using pfSense, organizations can boost the security of their networks as well as their understanding of the network traffic.

D. Significance of Integration

Integrating pfSense with Wazuh is important as it offers numerous benefits to organizations looking to strengthen their security monitoring function. By correlating network traffic information from pfSense with security events from Wazuh, the detection of threats and response to incidents are enhanced. By synergizing the capabilities of the two platforms, organizations are able to attain a better understanding of their security environment, helping them detect and respond to threats better. Furthermore, this integration aids in compliance initiatives with detailed logs and reports that show compliance with security norms.

E. Current Cybersecurity Landscape

The current cybersecurity environment is defined by a rising frequency and intensity of cyber threats. Organizations are confronted with a multitude of threats, such as ransomware, data breaches, and APTs. With increasingly sophisticated measures from cybercriminals, organizations have to implement preemptive security practices in order to safeguard their assets. Complexity in IT environments, with the growth of cloud services, remote work, and IoT devices, makes security even more challenging. Here, strong security monitoring tools such as Wazuh and pfSense are necessary for detecting vulnerabilities and reducing risks.

F. Scope of the Study

The study will cover the installation of Wazuh agents on multiple endpoints such as servers, workstations, and network devices to gather and analyze security information. It will cover the pfSense configuration to ensure easy integration with Wazuh, such as setting up firewall rules and logging configurations. The study will also discuss data collection, analysis, and visualization methods from both pfSense and Wazuh, as well as incident response strategies to effectively act on security incidents identified through the integrated system. The study will also discuss potential limitations and challenges in the deployment and integration process. Notably, the study will focus solely on the Wazuh and pfSense integration, and not on other SIEM products or firewall technologies, in order to give a clear understanding of their combined functionality in developing security monitoring.

III. LITERATURE REVIEW

Recent studies increasingly highlight the significance of open-source SIEM solutions such as Wazuh, owing to the cost-friendly nature of cybersecurity tools. Few studies, however, investigate the technical amalgamation of Wazuh with firewall technologies such as pfSense, which is tantamount to its adequate network security. This review discusses the existing research to situate the current study in this novel domain.

Several research studies attest to the use of Wazuh as an efficient open-source SIEM tool, especially in budget-limited environments. González-Granadillo et al. (2021) [4] tested the strengths and weaknesses of several SIEM tools in critical infrastructure and concluded that light, open-source solutions such as Wazuh are necessary in low-budget environments. Their findings warrant your choice of Wazuh for university or SME-scale deployments.

Hidayat et al. (2023) [5] investigated extending Wazuh by integrating with Cyber Threat Intelligence platforms like MISP and DFIR-IRIS. It demonstrated that Wazuh can be extended to support advanced threat detection, though it dealt mostly with malware and not firewall logs. This supports your objective of integrating pfSense logs by highlighting Wazuh's flexibility.

A more general comparative evaluation by Bezas & Filippidou (2023) [6] tested open-source SIEM platforms such as Wazuh. They tested performance, usability, and threat response functionality and concluded Wazuh to be a well-balanced and proficient choice. While devoid of any precise information on integrating log sources, the research confirms Wazuh's overall appropriateness for SIEM installations. Farrel et al. (2024) [1] showed live intrusion detection with Wazuh's active response module coupled with Telegram notifications. Although their article was centered on brute

force attacks, it shows the responsiveness of Wazuh and presents a model that can be used for pfSense log alerts.
In an industry-case example, Islam & Rafique (2024) [7] used Wazuh in the apparel industry for centralized log management and threat prevention. This illustrated Wazuh's capability of dealing with custom log sources and enterprise deployment, further establishing its applicability for pfSense integration within diverse environments. The most immediately applicable research is by Bhavana et al. (2025) [8], who implemented pfSense on Wazuh and utilized automation via SOAR tools. Their study was conclusive in proving that pfSense logs can be efficiently parsed and leveraged within Wazuh, enabling rich alerting and response.

Table 1. Comparative analysis of previous methods

Reference No.	Gaps in Literature
[4]	Limited focus on open-source SIEM tools like Wazuh.
[5]	Focused primarily on malware detection; limited discussion on firewall log integration.
[6]	General comparison without in-depth analysis of specific integrations like pfSense.
[1]	Specific to brute force attacks; does not cover firewall log integration.
[7]	Industry-specific study; lacks focus on firewall integration.
[8]	High-level overview; limited technical details on integration processes.

Throughout all of the publications, Wazuh always presents itself as a scalable, effective, and versatile open-source SIEM solution. The literature clearly provides sound theoretical and practical rationale for its implementation across numerous industries, ranging from critical infrastructure to niche environments such as apparel production. The gap found across most of these studies is that few delve very deeply technically into pfSense firewall log integration—barring the 2025 study by Bhavana et al., which offers a scarce, applicable illustration. Not only does this project fill that gap but also has the potential to contribute usefully by offering an in-depth, real-world example of Wazuh with pfSense integration, rule configuration, and threat identification, upon which further studies may build.

IV. METHODOLOGY

This paper describes the research methodology used in this thesis to serve an assessment of cybersecurity practices in an on-premises lab environment. Using various tools such as Wazuh, Ubuntu, Kali Linux and pfSense the study bridges the gap between theoretical cyber security concepts and practical implementations.
This study employs a descriptive research design to evaluate the effectiveness of Wazuh SIEM in conjunction with pfSense for security monitoring. The research aims to systematically assess how the integration of Wazuh SIEM agents with pfSense enhances the detection and response capabilities to security incidents within an organizational network.

By collecting and analyzing data from both Wazuh and pfSense, the study will provide insights into the improvements in threat detection rates, incident response times, and overall security posture before and after the integration. This design allows for a comprehensive understanding of the operational benefits and challenges associated with deploying Wazuh SIEM alongside pfSense in a real-world environment.

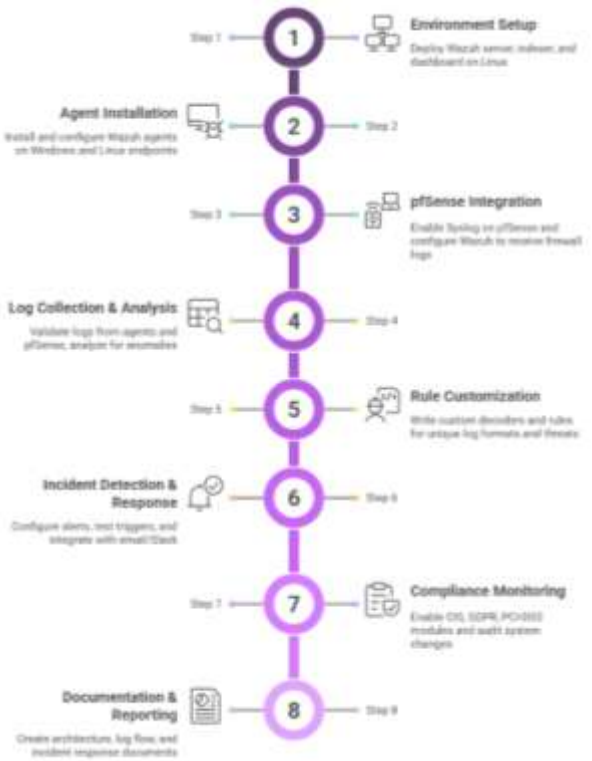

Figure 1. Workflow of model

The research will be conducted in a virtual machines specifically designed for cybersecurity testing. This environment will be equipped with the following necessary hardware and software:

A. Deployment and Configuration of Wazuh SIEM
Objective: Set up a fully functional Wazuh SIEM environment, including the server, indexer, and dashboard.
Process:

- Environment Setup: Installed the Wazuh server on a Linux-based system (Ubuntu) and configured the necessary dependencies.
- Indexer Installation: Deployed the Wazuh indexer to store and manage log data efficiently.
- Dashboard Configuration: Set up the Wazuh dashboard (Linux-based) for visualizing and analyzing security events.
- Integration: Ensured seamless communication between the Wazuh server, indexer, and dashboard.

Tools Used: Wazuh documentation, Linux terminal, and Wazuh installation scripts.
Outcome: Successfully deployed a centralized Wazuh SIEM platform for log management and analysis.
Outcome: Successfully deployed a centralized Wazuh SIEM platform for log management and analysis.

Figure 2. Architecture of wazuh

B. Agent Installation and Management

Objective: Install and configure Wazuh agents on multiple endpoints to collect and forward logs to the Wazuh server.

Process:

- Agent Installation: Installed Wazuh agents on Windows and Linux systems using the provided installation packages.
- Agent Registration: Registered agents with the Wazuh server to establish a secure connection.
- Configuration: Configured agents to monitor system logs, file integrity, and network activity.
- Testing: Verified that logs from agents were successfully forwarded to the Wazuh server.

Tools Used: Wazuh agent installation packages, Wazuh manager, and endpoint systems (Windows/Linux).

Outcome: Enabled real-time log collection from multiple endpoints for centralized monitoring.

C. Log Collection and Analysis

Objective: To integrate pfSense with Wazuh to forward firewall logs for centralized monitoring and analysis.

- Configure pfSense for Remote Logging: Open the pfSense web interface and navigate to Status > System Logs > Settings.
- Configure Wazuh to Receive Logs**:** Ensure that the Wazuh manager is set up to receive syslog messages
- Verify Log Reception: Open the Wazuh dashboard and go to Security Events or Logs and Confirm that pfSense logs are successfully being received and parsed.

D. Log Analysis and Rule Creation and Customization:

Objective**:** To analyze logs and create custom detection rules in Wazuh for identifying specific security threats.

- Analyze Logs in Wazuh: Review incoming logs from all integrated sources including pfSense, Linux, and Windows endpoints.
- Identify patterns, IPs, or events that may indicate suspicious behavior or threats.
- Create and Apply Custom Rules: Add a custom rule to detect a suspicious IP accessing the network and save the file and restart the Wazuh manager to activate the new rule.
- Test and Confirm Rule Functionality: Simulate traffic or generate logs matching the rule
- Check the Wazuh dashboard to verify that the alert appears with the correct rule ID and description.

E. Incident Detection and Response:

Objective: To simulate security incidents and verify Wazuh's ability to detect and respond to threats effectively.

- Simulate Security Incidents: On the Linux or Windows endpoint, simulate a brute-force attack by attempting multiple failed SSH login attempts. Try to access protected or sensitive files without the necessary permissions. Use security tools like hydra, nmap, or create custom scripts for simulation.
- Monitor Alert Generation: Observe if the simulated activities trigger alerts with appropriate severity and timestamps in Alerts or Security Events of Wazuh dashboard.
- Confirm the alerts contain relevant metadata like source IP, action taken, and rule matched.
- Create an Automated Response (Optional**):** Write a shell script that blocks IPs involved in certain alerts. Integrate the script with Wazuh using log triggers or API calls for automated incident response.
- Network connectivity was established using host-only adapters. All VMs communicated via a local private subnet.

F. Compliance Monitoring:

Objective: To enable Wazuh's compliance modules for evaluating system configurations against standards like CIS, GDPR, and PCI-DSS.

- Enable Compliance Modules.
- Run Compliance Scans and View Results.

V. SYSTEM REQUIREMENT

Hardware:

- A dedicated server running Wazuh SIEM to manage and analyze security events.
- A virtual or physical machine configured with pfSense as the firewall and network security solution.
- Multiple endpoints (both Windows and Linux systems) to deploy Wazuh agents for comprehensive monitoring

Table 2. Hardware components

Component	Specification
Host Laptop	Personal laptop used for setting up VirtualBox environment.
Processor	Intel Core i5-1135G7 (11th Gen)
RAM	16 GB (to support multiple virtual machines simultaneously)
Storage	Minimum 100 GB available (SSD recommended for performance)
Network Adapter	VirtualBox Host-only Adapter used to simulate internal VM communication

Software:

- Wazuh SIEM (latest version) installed on the server for centralized log management and threat detection.
- pfSense (latest version) configured to manage network traffic and enforce security policies.
- Data analysis tools (e.g., statistical software) for evaluating the effectiveness of the integration.

Table 3. Software Components

Software	Version/Details
VirtualBox	Latest stable version (7.x recommended)
Wazuh	Version 4.x (latest stable at time of project)
pfSense	Community Edition (2.7.x or higher)
Ubuntu Linux	22.04 LTS (for Wazuh manager and Linux agent)
Windows 10	Pro or Enterprise edition (for agent installation)
Elasticsearch	Bundled with Wazuh (7.10 or compatible)
Kibana	Bundled with Wazuh

This controlled setting will facilitate the systematic deployment of Wazuh agents and the integration with pfSense, allowing for accurate data collection and analysis of security monitoring capabilities in a simulated organizational network environment.

VI. RESULT AND DISCUSSION

Implementation led to successful identification of simulated threats via custom rules, with all endpoint logs and pfSense firewall logs properly correlated for in-depth analysis. Compliance scans revealed system misconfiguration and provided actionable remediation guidance, while the Wazuh dashboard provided concise and centralized visibility into the security posture. Wazuh was effective in serving as a comprehensive security monitoring solution. Its compatibility across different platforms (Linux, Windows, pfSense) and customization features allow it to be applicable to different organizational requirements. Drawbacks noted are moderate learning complexity and performance limits on underpowered hardware. Potential areas of improvement for the future are integration with threat intelligence feeds and automated response capabilities.

VII. CONCLUSIONS

1. The ability to successfully carry out this project shows a good grasp and real-world implementation of installing and managing a SIEM solution with Wazuh.
2. We were able to successfully install and configure the Wazuh server and agents on various operating systems (Windows and Linux) and achieved centralized log gathering and monitoring.
3. By correlating pfSense firewall logs, we provided real-time insight into network activity and possible threats.
4. Custom decoders and rules were created to identify known anomalies specific to the simulated organizational context, and threat detection capabilities were augmented. Additionally, incident response capabilities were built-in by correlating events and triggering alerts to proactively reduce risks.
5. Compliance monitoring was also covered in the project by using Wazuh's native capabilities to evaluate system settings and output compliance reports based on security best practices and standards.
6. The paper proves the pragmatic feasibility of Wazuh as an affordable SIEM for real-time threat detection and compliance.
7. The study features Wazuh's capabilities in log collection, correlation, incident response, and regulatory monitoring.
8. It acted as a guide for organizations looking for open-source alternatives to commercially available SIEM solutions. As a whole, this hands-on deployment reinforced our grasp of SIEM architecture and its pivotal position in contemporary cybersecurity operations.

ACKNOWLEDGMENT

The heading of the Acknowledgment section and the References section must not be numbered.

REFERENCES

1. Farrel, S., et al. (2024). "Real-Time SIEM Response Using Telegram Alerts." IEEE Conference on Cybersecurity and Threat Intelligence
2. IEEE Conference Proceedings. (2025). "Open Source SIEMs for National Cyber Defense." IEEE Symposium on Open Source Security Tools.
3. S. Moiz, A. Majid, A. Basit, M. Ebrahim, A. A. Abro and M. Naeem, "Security and Threat Detection through Cloud-Based Wazuh Deployment," 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), Tandojam, Pakistan, 2024, pp. 1-5, doi: 10.1109/KHI-HTC60760.2024.10482206.
4. González-Granadillo, G., et al. (2021). "SIEMs in Critical Infrastructures: A Comparative Study." Journal of Information Security and Applications, Elsevier.
5. Hidayat, A., et al. (2023). "CTI-based Malware Detection using Wazuh and MISP." International Journal of Cyber-Security and Digital Forensics.
6. Bezas, K., & Filippidou, F. (2023). "Evaluation of Open-Source SIEM Tools for SMEs." Proceedings of the 17th International Conference on Cyber Warfare and Security (ICCWS).
7. Islam, M. R., and Raisa Rafique. "Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries." International Journal of Engineering Materials and Manufacture, vol. 9, no. 4, Oct. 2024, pp. 136–44, doi:10.26776/ijemm.09.04.2024.02.
8. Bhavana, V., et al. (2025). "SIEM and SOAR Integration for Automated Security Monitoring." Proceedings of the ACM Symposium on Security Automation.
9. M. R. Islam, M. Akhtaruzzaman, M. M. Rahman, M. T. Rahman, and M. R. Mehedi, "Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries," ResearchGate, 2024.
10. D. Pawar and A. Choubey, "WAZUH – New Age Security Monitoring SIEM Tool," International Research Journal of Modernization in Engineering Technology and Science, vol. 6, no. 5, 2024.
11. The Science and Information Organization, "SIEM and Threat Intelligence: Protecting Applications with Wazuh, TheHive, and Telegram," International Journal of Advanced Computer Science and Applications, vol. 15, no. 9, 2024
12. Uetz, R., Herzog, M., Hackländer, L., Schwarz, S., & Henze, M. (2023). You Cannot Escape Me: Detecting Evasions of SIEM Rules in Enterprise Networks. arXiv preprint arXiv:2311.10197.

13. Farrel, F.I.F., Mardianto, I. and Qamar, M.Ir.A.S. (2024) "Implementation of Security Information & Event Management (SIEM) Wazuh with Active Response and Telegram Notification for Mitigating Brute Force Attacks on The GT-I2TI USAKTI Information System," Intelmatics, 4(1), pp. 1–7. doi:10.25105/itm.v4i1.18529
14. R. Amami, M. Charfeddine and S. Masmoudi, "Exploration of Open Source SIEM Tools and Deployment of an Appropriate Wazuh-Based Solution for Strengthening Cyberdefense," 2024 10th International Conference on Control, Decision and Information Technologies (CoDIT), Vallette, Malta, 2024, pp. 1-7, doi: 10.1109/CoDIT62066.2024.10708476.
15. Alatise, T.I. and Nottidge, O.E. (2024) "Threat detection and response with SIEM system," International Journal of Communication and Information Technology, 5(1), pp. 36–38. doi:10.33545/2707661x.2024.v5.i1a.78.
16. Jumiaty and Soewito, B. (2024) "SIEM and Threat Intelligence: Protecting Applications with Wazuh and TheHive," International Journal of Advanced Computer Science and Applications, 15(9). doi:10.14569/ijacsa.2024.0150923.
17. Sufardy, D.B. and Widiasari, I.R. (2024) "The Use of PFSense and Suricata as a Network Security Attack Detection and Prevention Tool on Web servers," INOVTEK Polbeng - Seri Informatika, 9(2), pp. 765–777. doi:10.35314/shxy204.
18. Amin, R. and Hasan, D. (2023) "Comparative Analysis of Flexiwan, OPNSense, and pfSense Cybersecurity Mechanisms in MPLS / SD-WAN Architectures," passer, 6(1), pp. 27–32. doi:10.24271/psr.2023.390989.1295.
19. Analysis of Wazuh SIEM's Effectiveness in Cloud Security Monitoring" (2024) Journal of Cybersecurity and Information Management, 15(1). doi:10.54216/jcim.150119.