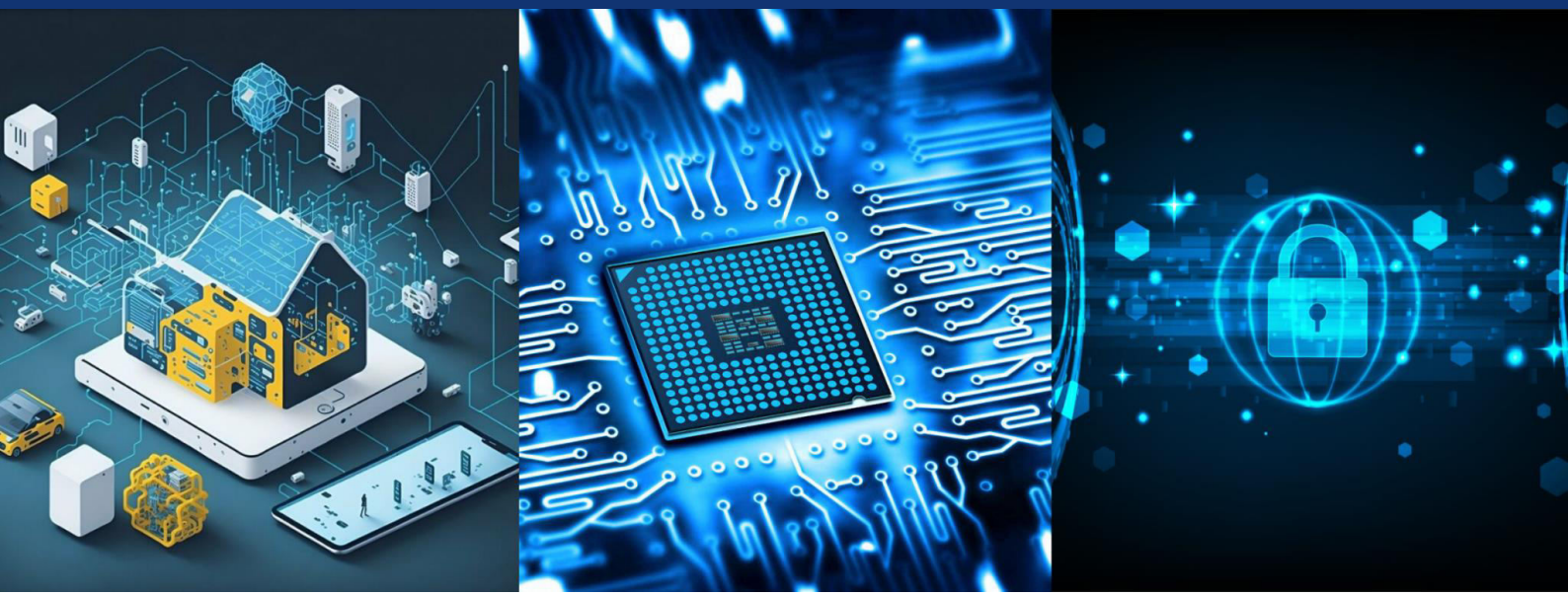
IJIRCCE

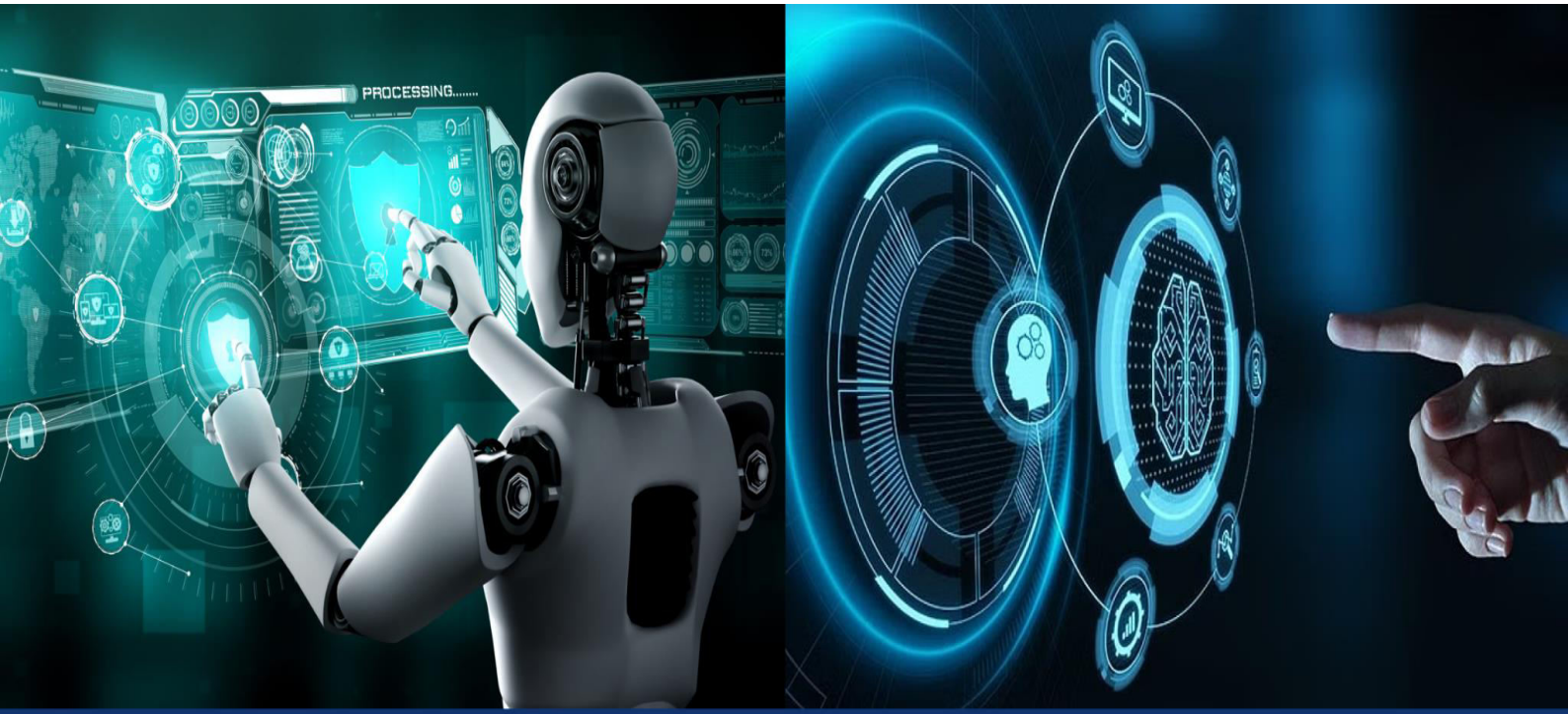
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 6, June 2026

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406046

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Design and Implementation of an Enhanced SIEM (Wazuh) Framework with SOAR, XDR, and ARP Spoofing Detection

Medha C Chalageri[1], G. Chidambaram[2], A.Sudhakar[3]

PG Student, Department of Computer Science and Engineering, Bharathidasan Engineering College, Vellore, Tamil Nadu, India[1]

Assistant Professor, Department of Computer Science and Engineering, Bharathidasan Engineering College, Vellore, Tamil Nadu, India[2]

Head of the Department, Department of Computer Science and Engineering, Bharathidasan Engineering College, Vellore, Tamil Nadu, India[3]

ABSTRACT: Cyber threats are continuously evolving, making traditional security monitoring insufficient for modern organizations. Security Information and Event Management (SIEM), Extended Detection and Response (XDR), Intrusion Detection Systems (IDS), and Security Orchestration, Automation and Response (SOAR) technologies play a crucial role in identifying, analyzing, and responding to cyberattacks. This project presents the design and implementation of a cybersecurity monitoring laboratory using Wazuh SIEM, Suricata IDS, and Ubuntu Linux. The environment simulates real-world attacks from a Kali Linux attacker machine and demonstrates centralized log collection, threat detection, alert generation, attack visibility, and automated notification capabilities. The project also explores ARP spoofing attacks, network monitoring, active response concepts, and email-based alerting mechanisms. The implemented solution provides a cost-effective open-source security monitoring platform suitable for learning, research, and small-scale enterprise environments. The results demonstrate the effectiveness of combining multiple security technologies in a unified monitoring framework to detect and respond to modern cyber threats in real time.

KEYWORDS: SIEM, XDR, Wazuh, Suricata, SOAR, IDS, Cybersecurity Monitoring, ARP Spoofing, Threat Detection, Security Operations Center.

I. INTRODUCTION

In the digital age, organizations face an ever-increasing volume and sophistication of cyber threats. From nation-state actors conducting espionage to ransom ware groups targeting critical infrastructure, the threat landscape has grown dramatically in both complexity and scale. Security monitoring — the continuous observation and analysis of an organization's information systems — has become a foundational pillar of modern cyber security strategy.

Cybersecurity monitoring involves collecting, aggregating, and analysing logs, events, and alerts from disparate sources across an IT environment. These sources include endpoint devices, servers, network appliances, applications, databases, and cloud services. Without centralized visibility, security analysts struggle to detect threats, correlate events, and respond effectively. As organizations increasingly adopt hybrid and cloud-based infrastructures, maintaining comprehensive visibility across distributed environments has become both more challenging and more critical.

Security Information and Event Management (SIEM) platforms emerged as a solution to this challenge by providing centralized log collection, correlation, and alerting capabilities. Modern SIEM solutions have evolved beyond simple log management to incorporate advanced analytics, machine learning, threat intelligence integration, and automated response workflows. These capabilities enable security teams to identify anomalous behavior, detect sophisticated attack patterns, and reduce the time required to investigate incidents.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Another significant driver for security monitoring is regulatory compliance. Standards and frameworks such as GDPR, HIPAA, PCI-DSS, ISO 27001, and NIST require organizations to maintain audit trails, monitor security events, and demonstrate effective incident detection and response capabilities. SIEM platforms help organizations meet these requirements by providing centralized logging, reporting, and evidence collection

Objective of the Work:

The primary objective of this project is to design, implement, and validate a comprehensive cyber security monitoring laboratory using open-source tools. The system aims to provide security analysts, researchers, and students with a practical platform for learning threat detection, incident analysis, security monitoring, and Security Operations Center (SOC) workflows. The project focuses on demonstrating how integrated security technologies can improve organizational visibility, accelerate threat detection, and enhance incident response capabilities in modern IT environments. The specific objectives of the project are as follows:

- To implement a SIEM platform using Wazuh for centralized log collection, event correlation, and threat detection.
- To integrate Suricata IDS for network traffic analysis and signature-based intrusion detection.
- To simulate real-world cyber attacks using Kali Linux, including Nmap reconnaissance and ARP spoofing.
- To demonstrate Extended Detection and Response (XDR) capabilities through unified endpoint and network monitoring.
- To generate and visualize security alerts through the Wazuh Dashboard for incident investigation.
- To implement email-based alert notifications as a foundational SOAR capability.
- To explore automated response mechanisms for critical security events.
- To analyze the performance and effectiveness of the monitoring solution in detecting simulated attacks.

II. LITERATURE REVIEW

Security Information and Event Management (SIEM) and Extended Detection and Response (XDR) are widely used technologies for modern cybersecurity monitoring. SIEM systems collect, analyze, and correlate security logs from multiple sources, while XDR extends visibility across endpoints, networks, cloud environments, and identity systems. These technologies help organizations detect threats more accurately, reduce response times, and improve overall security operations.

Intrusion Detection Systems (IDS) play a vital role in identifying malicious activities within networks and hosts. Network-based IDS solutions such as Wazuh monitor endpoint activities and system events. The integration of these technologies provides comprehensive threat detection and enhanced incident investigation capabilities through correlated security monitoring.

Security Orchestration, Automation, and Response (SOAR) improves cybersecurity operations by automating repetitive tasks and accelerating incident response. Open-source platforms such as Wazuh and Suricata offer cost-effective security monitoring, intrusion detection, log analysis, and automation features. Their combined use provides an efficient and scalable security solution for modern cybersecurity environments.

III. EXISTING MODEL

Existing security monitoring systems rely on technologies such as SIEM, XDR, IDS, and SOAR to detect and respond to cyber threats. Traditional solutions collect and analyze security logs, monitor network and endpoint activities, and generate alerts for suspicious behavior. Open-source platforms such as Wazuh and Suricata are widely used to provide centralized log management, intrusion detection, threat correlation, and automated response capabilities. However, existing systems often face challenges such as high alert volumes, false positives, and the need for continuous configuration and rule tuning to maintain effective security monitoring.

IV. PROPOSED METHODOLOGY

The proposed system implements an integrated cybersecurity monitoring framework using Wazuh and Suricata to provide SIEM, XDR, IDS, and SOAR functionalities within a unified environment. The objective is to achieve real-time threat detection, event correlation, security monitoring, and automated incident response across network and endpoint infrastructures.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

In the first stage, Wazuh agents are deployed on monitored endpoints such as servers and workstations. These agents continuously collect security-related information including system logs, authentication events, file integrity changes, process activities, and vulnerability data. The collected information is forwarded to the Wazuh Manager for centralized analysis and correlation.

Simultaneously, Suricata is deployed as a Network Intrusion Detection System (NIDS) to monitor network traffic. Suricata inspects packets traversing the network and detects malicious activities such as port scanning, malware communication, brute-force attacks, and known exploit attempts using predefined threat detection rules.

The security events generated by both Wazuh and Suricata are aggregated and processed through the Wazuh Manager. Event correlation mechanisms analyze host-based and network-based alerts together to identify complex attack patterns and provide a comprehensive view of security incidents. This integration enhances threat visibility and improves detection accuracy.

The analyzed security data is stored and indexed within the OpenSearch database, enabling efficient searching, reporting, and historical analysis. The Wazuh Dashboard provides visualization of alerts, security events, compliance status, and threat intelligence information, allowing administrators to monitor the security posture of the environment in real time.

To improve response efficiency, the system incorporates SOAR-based automation through Wazuh Active Response. When predefined threats are detected, automated actions such as blocking malicious IP addresses, generating alerts, executing response scripts, and sending email notifications are performed. This approach reduces response time, minimizes analyst workload, and strengthens the overall security monitoring capability of the proposed system.

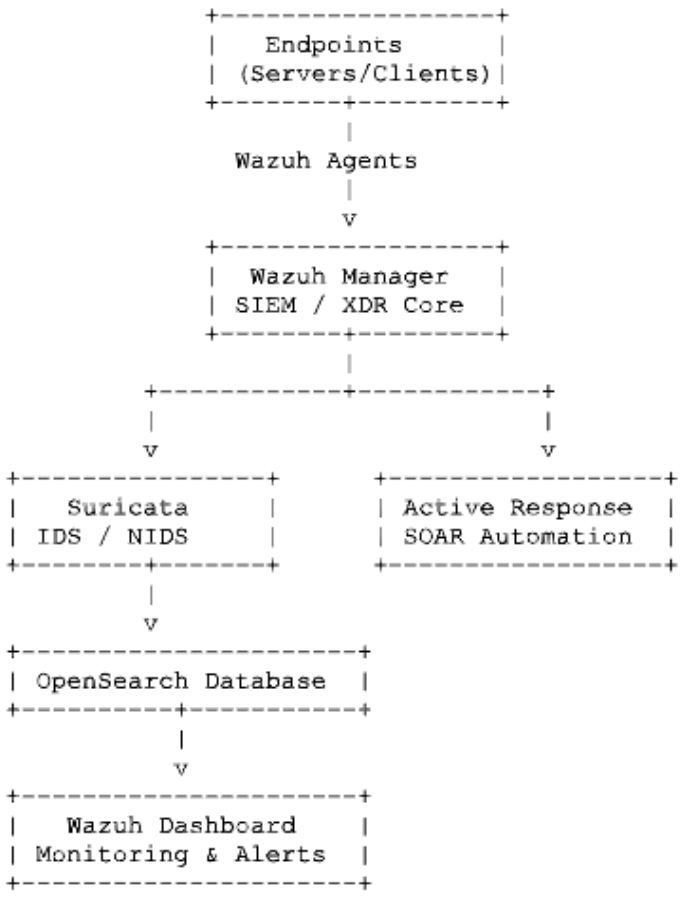


Fig. 1 Proposed Architecture

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406046

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. IMPLEMENTATIONS

The implementation of the proposed security monitoring system was carried out in a controlled laboratory environment using Wazuh and Suricata to achieve integrated SIEM, XDR, IDS, and SOAR functionalities. The main objective of the implementation was to design a centralized security monitoring framework capable of collecting, analyzing, correlating, and responding to security events generated from both host-based and network-based sources.

1. Wazuh Manager Setup

The implementation began with the installation and configuration of the Wazuh Manager, which serves as the core component of the system. The Wazuh Manager is responsible for receiving security data from multiple endpoints and performing log analysis, event correlation, and alert generation. It acts as the central processing unit of the entire security monitoring architecture, enabling unified visibility of all security events.

2. Wazuh Agent Deployment on Endpoints

Wazuh agents were installed on all monitored endpoint systems, including servers and client machines. These agents continuously collect system-level information such as authentication logs, process activities, file integrity changes, and vulnerability data. The collected data is securely transmitted to the Wazuh Manager for analysis. This setup enables host-based intrusion detection and supports continuous endpoint monitoring.

3. Suricata IDS Configuration

Suricata was deployed as a Network Intrusion Detection System (NIDS) to monitor real-time network traffic. It analyzes packets flowing through the network and detects malicious activities such as port scanning, denial-of-service attempts, brute-force attacks, malware communication, and exploit attempts. Suricata uses rule-based detection mechanisms along with deep packet inspection to identify suspicious network behavior effectively.

4. Integration of Suricata with Wazuh

To achieve a unified security monitoring system, Suricata was integrated with the Wazuh platform. This integration allows network-based alerts generated by Suricata to be forwarded to the Wazuh Manager, where they are correlated with host-based logs. This correlation enables the system to detect complex attack patterns that span across multiple systems and network layers, improving overall threat detection accuracy.

5. OpenSearch and Wazuh Dashboard Configuration

OpenSearch was used as the backend data storage and indexing engine for all security events. It enables fast searching, querying, and analysis of large volumes of log data. The Wazuh Dashboard was configured on top of OpenSearch to provide a user-friendly interface for real-time monitoring, visualization of alerts, incident investigation, and security reporting. This helps administrators easily analyze security posture and identify threats.

6. Attack Simulation and System Testing

To validate the effectiveness of the implemented system, various attack scenarios were simulated in the laboratory environment. These included port scanning, unauthorized login attempts, suspicious network communication, and brute-force attacks. The system successfully detected and generated alerts for these activities, demonstrating the effectiveness of both Suricata and Wazuh in identifying security threats.

7. SOAR-Based Active Response Implementation

Wazuh Active Response was configured to provide automation and incident response capabilities. When specific security events are detected, the system automatically executes predefined actions such as blocking malicious IP addresses, generating alerts, terminating suspicious connections, and sending email notifications to administrators. This automation reduces response time and minimizes the need for manual intervention.

Overall, the implementation demonstrates a fully functional cyber security monitoring system that integrates SIEM, XDR, IDS, and SOAR capabilities using open-source tools. The combination of Wazuh and Suricata provides comprehensive visibility across endpoints and networks, enabling efficient threat detection, correlation, and automated response.

© 2026 IJIRCCE | Volume 14, Issue 6, June 2026 DOI: 10.15680/IJIRCCE.2026.1406046

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

V. CLASSIFICATION

Security monitoring systems are classified based on functionality, deployment type, and detection techniques. Based on functionality, they include detection systems like Intrusion Detection Systems (IDS), prevention systems like Intrusion Prevention Systems (IPS), and response systems such as Security Orchestration, Automation, and Response (SOAR), which automate incident handling. Based on deployment, systems are divided into network-based solutions, such as Suricata which monitors network traffic for malicious activity, and host-based solutions like Wazuh agents which monitor logs, processes, and system events on individual machines. Based on detection techniques, systems use signature-based detection for identifying known threats and anomaly-based detection for detecting unusual behavior. In the proposed model, Wazuh functions as a SIEM and XDR platform for centralized monitoring and correlation, while Suricata acts as an IDS/IPS for network security, together forming an integrated and efficient cybersecurity monitoring framework.

VI. RESULT

The implemented cyber security monitoring system using Wazuh and Suricata successfully demonstrates an integrated approach to SIEM, XDR, IDS, and SOAR functionalities. The system effectively collects and analyzes logs from endpoints through Wazuh agents while simultaneously monitoring network traffic using Suricata IDS. The correlation of host-based and network-based events enables accurate detection of malicious activities and improves overall threat visibility. The Wazuh Dashboard provides real-time visualization of security events, allowing efficient monitoring and analysis of system behavior. Furthermore, the implementation of Active Response automates critical security actions such as alert generation, IP blocking, and notifications, thereby reducing response time and minimizing manual intervention. Overall, the system proves to be effective in detecting, analyzing, and responding to cyber threats in a centralized and efficient manner.

VII. CONCLUSIONS

The proposed cybersecurity monitoring system successfully integrates Wazuh and Suricata to implement a unified framework combining SIEM, XDR, IDS, and SOAR capabilities. The system provides centralized log collection, real-time network and host-based intrusion detection, event correlation, and automated incident response. By combining Wazuh for endpoint monitoring and Suricata for network traffic analysis, the solution enhances visibility across the entire infrastructure and improves the accuracy of threat detection. The use of Open Search and the Wazuh Dashboard enables efficient storage, visualization, and analysis of security events, making it easier for administrators to monitor system activity and respond to threats.

Additionally, the implementation of Active Response introduces automation into the security workflow, reducing manual effort and improving response time during security incidents. The system successfully demonstrates how open-source tools can be leveraged to build a cost-effective and scalable cyber security monitoring environment. Overall, the proposed model strengthens organizational security posture by improving threat detection, analysis, and response capabilities, and it provides a strong foundation for future enhancements such as advanced machine learning integration, cloud security expansion, and improved SOAR functionalities.

VIII. FUTURE WORK

Future enhancements of the proposed system can focus on integrating artificial intelligence and machine learning techniques to improve anomaly detection, reduce false positives, and identify unknown threats more effectively. The system can also be extended to support cloud-native and hybrid environments for broader security visibility across modern infrastructures. Additionally, advanced SOAR capabilities such as automated ticketing, chatbot-based incident response, and intelligent security playbooks can be incorporated to improve automation and response efficiency. Integration with real-time threat intelligence feeds and predictive analytics can further strengthen detection accuracy and enable proactive threat hunting. Overall, these improvements will help evolve the current system into a more intelligent, scalable, and fully automated cybersecurity framework aligned with advanced SOC requirements.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

REFERENCES

[1] L. Fachruddin and S. Neyman, "Analisis Integrasi Security Information and Event Management (SIEM) Wazuh dengan Suricata pada Azure Cloud Web Server," *Repository IPB University*, 2023. [Online]. Available: https://repository.ipb.ac.id/handle/123456789/136766

[2] G.-R. Andreica, I.-A. Ivanciu, D. Zinca, and V. Dobrota, "Integration of the Suricata Intrusion Detection System and of the Wazuh Security Information and Event Management for Real-Time Denial-of-Service and Data Tampering Detection and Alerting," *Technical University of Cluj-Napoca*, 2024. [Online]. Available: https://oasis.utcluj.app/items/06fe9ec4-df09-48aa-a00a-b2419a3e3eb4

[3] M. Vasilakis, M. G. Tampouratzis, and A. Dimitriadis, "Integrated Threat Intelligence and Event Correlation with Wazuh, Suricata, and MISP," in *Proc. 6th Int. Conf. Communications, Information, Electronic and Energy Systems (CIEES)*, 2025, doi: 10.1109/CIEES66347.2025.11300009.

[4] R. S. Chouhan, Y. S. Bisht, and V. Rawat, "A Fuzzy Logic-Based Intrusion Detection and Prevention System Using Suricata, Wazuh and MITRE ATT&CK Framework for Virtualized Network Environments," *IJRASET*, vol. 14, no. 4, 2026. doi: 10.22214/ijraset.2026.81227.

[5] M. S. R. Setyo, "Implementasi SIEM (Security Information & Event Management) Menggunakan Wazuh & Suricata Untuk Monitoring Dalam Lingkup Departemen Teknologi Informasi," *ITS Repository*, 2023. [Online]. Available: https://repository.its.ac.id/101897/.

[6] B. Alboushy et al., "Context-Aware Web Attack Detection in Open-Source SIEM Systems via MITRE ATT&CK-Enriched Behavioral Profiling," *arXiv preprint arXiv:2605.13337*, 2026. [Online]. Available: https://arxiv.org/abs/2605.13337

[7] H. A. Damanik and M. Anggraeni, "Hybrid Intrusion Detection System and Network Infrastructure Vulnerability Mitigation using Active Response (XDR) Technique Wazuh and Suricata," *Jurnal Pekommas*, vol. 9, no. 2, 2024. doi: 10.56873/jpkm.v9i2.5829.

[8] H. A. Damanik and M. Anggraeni,
"Hybrid Intrusion Detection System and Network Infrastructure Vulnerability Mitigation using Active Response (XDR) Technique Wazuh and Suricata," *Jurnal Pekommas*, vol. 9, no. 2, pp. 309–322, Dec. 2024, doi: 10.56873/jpkm.v9i2.5829.

[9] G.-R. Andreica, I.-A. Ivanciu, D. Zinca, and V. Dobrota,
"Integration of the Suricata Intrusion Detection System and of the Wazuh Security Information and Event Management for Real-Time Denial-of-Service Detection," in *Proc. CIEES*, 2024, doi: 10.1109/CIEES66347.2025.11300009.

[10] B. Alboushy et al.,
"Context-Aware Web Attack Detection in Open-Source SIEM Systems via MITRE ATT&CK-Enriched Behavioral Profiling," *arXiv preprint arXiv:2605.13337*, 2026.

[11] R. A. Bridges et al.,
"Testing SOAR Tools in Use," *arXiv preprint arXiv:2208.06075*, 2022.

[12] M. Vasilakis, M. G. Tampouratzis, and A. Dimitriadis,
"Integrated Threat Intelligence and Event Correlation with Wazuh, Suricata, and MISP," in *2025 6th Int. Conf. Communications, Information, Electronic and Energy Systems (CIEES)*, 2025.

[13] H. Kim et al.,
"Enhancing Security Operations Center: Wazuh Security Event Response with Retrieval-Augmented Generation-Driven Copilot," *Sensors*, vol. 25, no. 3, p. 870, 2025, doi: 10.3390/s25030870.

[14] J. M. P. Silva et al.,
"Modeling Wazuh Rules with Weighted Timed Automata," *Procedia Computer Science*, vol. 251, pp. 75–82, 2024, doi: 10.1016/j.procs.2024.11.086.

[15] M. Al-Siam et al.,
"Improving Threat Detection in Wazuh Using Machine Learning Techniques," *J. Cybersecur. Priv.*, vol. 5, no. 2, 2025.

[16] A. A. Katresna,
"Integrasi Wazuh dan Suricata (IDS) untuk Deteksi Medusa Ransomware," *Polibatam Repository*, 2025.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details