Integrating Wazuh and Snort for Enhanced

Security Monitoring

G C Divya

Department of Computer Science and Engineering

Jain Institute of Technology Davanagere divyagc10@gmail.com

Shwetha K M Department of Computer Science and

Engineering

Jain Institute of Technology Davanagere shwethakm791@gmail.com

Chandankumar K Department of Computer Science and

Engineering

Jain Institute of Technology Davangere chandankelur26@gmail.com

Karthik K G Department of Computer Science and

Engineering

Jain Institute of Technology Davangere kgkarthik3223@gmail.com

Pallavi M S

Department of Computer Science and Engineering

Jain Institute of Technology Davangere pallavims262@gmail.com

**Abstract: Integrating Wazuh and Snort IDS for Enhanced Monitoring In the face of increasingly sophisticated cyber threats, organizations require robust, real-time monitoring solutions to detect and respond to security incidents. Snort, a powerful open-source Intrusion Detection System (IDS), provides real-time network traffic analysis, while Wazuh, a comprehensive security monitoring platform, offers advanced log analysis, file integrity monitoring, and incident response capabilities. This project aims to integrate Wazuh and Snort to create a unified security monitoring solution that combines Snort’s real-time threat detection with Wazuh’s data aggregation and correlation features. By centralizing security events and automating responses, this integration enhances network visibility, accelerates threat identification, and improves incident management processes. The result is a more effective, scalable, and automated security framework that strengthens an organization’s defense against evolving cyber threats.**

**Keywords: Cyber Security, Wazuh, Snort, SIEM, IDS, IPS.**

# Introduction

The rapid growth of network-based threats requires robust mechanisms to protect sensitive data and infrastructure. Intrusion Detection Systems (IDS) play a pivotal role in identifying and mitigating these threats. Snort, a widely-used open-source IDS, excels in real-time traffic analysis and packet logging, allowing organizations to detect suspicious activities and potential attacks. Complementing this, Wazuh offers a comprehensive security monitoring solution with capabilities like log analysis, file integrity monitoring, and vulnerability assessment.

Integrating Snort with Wazuh enhances an organization's security by combining the strengths of network traffic analysis and centralized security management. This integration facilitates real- time threat detection, centralized alert correlation, and automated responses, providing a unified view of security incidents. The synergy between Snort and Wazuh ensures improved visibility into both network and endpoint activities, allowing for faster and more efficient incident response.

The project focuses on implementing the integration of Snort and Wazuh to demonstrate the practical benefits of enhanced threat detection, centralized monitoring, and scalability. By addressing the challenges of fragmented security monitoring, the integration provides a streamlined and effective approach to safeguarding organizational assets against evolving cyber threats.

# Related work

## Christian Bassey, Ebenezer Tonye Chinda, and Samson Idowu[1]

This paper focus on open-source tools, addresses the increasing frequency and sophistication of cyberattacks targeting organizations of various sizes. It emphasizes the importance of implementing scalable, cost-effective security operations centers (SOCs) using open-source tools. The authors propose a SOC architecture that integrates components for security information and event management (SIEM), extended detection and response (XDR), case management, and network intrusion detection. Tools such as Wazuh (for SIEM and XDR), TheHive (for case management), and Suricata (for network intrusion detection) are used to implement and validate this architecture.

The SOC architecture is tested against simulated cybersecurity threats, including brute force attacks, malware downloads, and denial-of-service (DoS) attacks. Results demonstrate effective detection, response, and threat mitigation. The paper also highlights the inclusion of compliance monitoring and automated incident response, offering a scalable solution for small and medium-sized enterprises. It concludes with recommendations for further research, particularly in automation and artificial intelligence integration within SOCs.

**Zeyad Safaa Younus and Mafaz Alanezi,** from the University of Mosul [2]

This paper explores the critical domain of network security monitoring, highlighting its importance in identifying and mitigating cybersecurity threats. It addresses how network devices produce vast quantities of logs, emphasizing the necessity for centralized log management and analysis to detect suspicious activities. The study examines traditional security tools, intrusion detection systems (IDS), intrusion prevention systems (IPS), and the advanced functionalities of Security Information and Event Management (SIEM) systems.

The authors detail how SIEM systems consolidate logs from diverse sources, normalize data, and apply correlation rules to identify anomalies in real time, enhancing an organization's ability to detect and respond to threats. The paper also categorizes commercial and open-source SIEM solutions, evaluating their effectiveness in addressing modern cybersecurity challenges. Additionally, it discusses the limitations of existing tools, such as high false-positive rates, and underscores the need for integrated approaches for more robust threat detection and management.

## Yi Anson Lam, Siu Ming Yiu, and K.P [3]

"A Three-Pronged Approach to Malicious APK: Combining Snort, Wireshark, and Wazuh for Advanced Threat Management".Chow,

introduces an integrated approach to combating malicious Android Package Kits (APKs). The authors propose a system that merges Snort’s intrusion detection, Wireshark’s network analysis, and Wazuh’s active response capabilities. This method allows real-time detection of malicious APKs through signature and anomaly-based detection while employing Wazuh for automated responses, such as isolating systems or removing threats. The experimental framework demonstrates high detection accuracy and response efficiency, providing a scalable, low-cost solution for mobile security, particularly for SMEs and individual users. This study emphasizes the importance of integrating detection tools and active response mechanisms to address the evolving threat landscape.

## Sudhanshu Sekhar Tripathy and Bichitrananda Behera [4]

This research paper investigates the integration of Wireshark and Snort as key components in Intrusion Detection Systems (IDS). Wireshark is celebrated for its detailed packet analysis and protocol investigation, while Snort excels in rule-based threat detection and alert generation. The study conducts experimental evaluations using live network traffic, emphasizing the complementary roles of these tools. By employing Snort for intrusion detection and exporting results to Wireshark for detailed packet-level analysis, the paper demonstrates the effectiveness of these tools in identifying network vulnerabilities, including malformed packets, DDoS attacks, and encrypted communication anomalies. The findings underscore the importance of continuous improvement and integration to adapt to the evolving landscape of cyber threats.

## Imdadul Karim, Quoc-Tuan Vien, Tuan Anh Le, and

**Glenford Mapp** [5]

This paper explores the performance of a Snort-based Network Intrusion Detection System (S-NIDS) in various practical network scenarios, including high-speed, heavy-traffic, and large-packet conditions. It introduces a Centralized Parallel Snort NIDS (CPS- NIDS), leveraging multi-core processors (MCPs) and operating systems to enhance packet analysis efficiency while minimizing packet drops. The study designs testbeds to compare the effectiveness of S-NIDS under different configurations, demonstrating that Linux outperforms other operating systems and that i7 processors achieve better performance than i5. The CPS-NIDS approach allows for real- time intrusion detection and centralized log management across multiple VLANs, significantly improving network security. The findings emphasize the need for optimized configurations to address modern cybersecurity challenges effectively.

## Akarshita Shankar and Vijay Madisetti [6]

This paper introduces ADRIAN (Alert Distribution and Response Network), a framework designed to enhance Security Information and Event Management (SIEM) platforms by integrating them with real-time collaboration tools like Slack. By leveraging a middleware-based architecture, ADRIAN addresses common challenges in SIEM operations, such as inefficient alert management, lack of real-time communication, and overwhelming low-priority alerts. The framework features bidirectional communication, enabling real-time alert customization, categorization, and system management through collaboration platforms. A case study integrating Wazuh (a SIEM tool) with Slack demonstrates ADRIAN’s capabilities, including improved incident response times, enhanced team collaboration, and operational efficiency. The paper concludes with discussions on future enhancements, such as AI-based alert prioritization and broader integration with other tools

# The objectives of this paper include:

* + Combine Snort’s real-time network traffic analysis with Wazuh’s advanced log analysis capabilities to improve the accuracy of threat detection.
	+ Integrate Snort and Wazuh to create a unified platform for monitoring network and endpoint activities in one centralized dashboard.
	+ Correlate Snort alerts with logs from various sources for a better understanding of security events.
* Enable automated responses to detected threats, reducing the time needed to mitigate risks.
* Utilize Wazuh’s dashboard for easy navigation and visualization of security alerts and logs.

# System Design

****

Figure 1: Wazuh Architectural Diagram

Wazuh is an open-source security platform designed for threat detection and response, with an architecture that includes various components working together to ensure efficient security monitoring. The system monitors multiple endpoints such as servers, desktops, laptops, cloud instances, and virtual machines, each running a Wazuh agent. These agents collect security data and transmit it to the Wazuh server cluster. The server cluster, which is the core of the platform, comprises a master node that manages the cluster and coordinates communication among worker nodes. Worker nodes process security data and perform analysis, with scalability achieved by adding more worker nodes. A network load balancer ensures that traffic is evenly distributed across these nodes.

The Wazuh indexer stores security data for future analysis and reporting, with high availability and scalability ensured through multiple nodes. The Wazuh dashboard provides an intuitive user interface for viewing security alerts and managing the platform. Security analysts and administrators, referred to as Wazuh users, utilize this dashboard to monitor and respond to potential threats. The data flow in Wazuh follows a systematic process. First, agents on each endpoint collect security logs, system events, and other relevant data. This data is then sent securely to the server cluster. The cluster processes the data to detect threats and anomalies, generating alerts when necessary. These alerts are displayed on the Wazuh dashboard for immediate attention. The processed data is also forwarded to the Wazuh indexer for storage and future analysis. Finally, security analysts use the dashboard to investigate and respond to alerts, ensuring effective threat mitigation.



Figure 2: Snort Architectural Diagram

Snort is a powerful intrusion detection system (IDS) that monitors network traffic for potential security threats. It begins with the network layer, representing the traffic that Snort monitors, and utilizes Libpcap, a library that captures network packets from the network interface. Once packets are captured, they are analyzed by

the packet decoder, which extracts relevant information such as source and destination IP addresses, ports, protocols, and payload data. The processed packets are then passed to the preprocessor, which performs essential operations to prepare the data for analysis. These operations include normalization, where fragmented packets are reassembled, and complex protocols are decoded; stream reassembly, which reconstructs TCP/UDP streams for comprehensive analysis; and anomaly detection, which identifies unusual network behavior.

The preprocessed data is then analyzed by the detection engine, the core component of Snort. This engine compares the data against a set of predefined rules designed to detect patterns of malicious activity, such as port scans, buffer overflows, or known malware signatures. When a rule is triggered, Snort generates an alert to indicate a potential security threat and logs the event for further examination. The alert and log output phase ensures that all packet information and detection events are systematically recorded for future analysis and reporting. Finally, these alerts and logs are stored, enabling security analysts to conduct investigations and reinforce security measures based on historical data.



Figure 3: Integration of Wazuh and Snort

The integrated intrusion detection system (IDS) architecture, combining **Wazuh** and **Snort**, offers comprehensive threat detection and response capabilities. The system is managed by an **administrator** who monitors and responds to security alerts. The **dashboard** serves as the primary user interface, providing a visual and interactive platform for administrators. It features **alert visualization**, presenting security alerts in a graphical format for easier analysis and quicker response.

The **Snort IDS** component is responsible for real-time **packet analysis**, scrutinizing network traffic to identify any malicious activity. Its **detection engine** processes the analyzed data to detect potential threats based on predefined rules. On the other hand, the **Wazuh server** plays a critical role in data monitoring and correlation. It conducts **file integrity mon-itoring (FIM)** to track changes to critical files and directories, while its **log analysis** module examines logs from various sources to identify security events. The **Snort integration module** ensures seamless incorporation of Snort-generated alerts into the Wazuh platform for advanced correlation and analysis. The **alert manager** within the Wazuh server manages and correlates alerts from multiple sources to provide a cohesive view of security incidents.

The **web server** component includes the **application layer**, offering a web-based interface for system management. The **Wazuh agent**, deployed on monitored endpoints, collects data such as log events and file changes and forwards this information to the Wazuh server. The **data flow** within the system starts with the Wazuh agent gathering security data from endpoints. Simultaneously, Snort IDS analyzes real-time network traffic and generates alerts upon detecting suspicious activity. Both the data from Wazuh agents and Snort alerts are transmitted to the Wazuh server, which performs

comprehensive log analysis, file integrity monitoring, and alert correlation. Finally, the **correlated alerts** are managed by the Alert Manager, which can trigger push notifications to inform the administrator of potential security incidents. This integrated approach ensures efficient and thorough threat detection and response.

# Result

****

Figure 4: Wazuh Dashboard

The Wazuh dashboard offers a consolidated view of security data, categorizing alerts based on severity—critical, high, medium, and low. This visual segmentation helps security analysts prioritize threats effectively. Additional insights such as configuration assessments, malware detections, and vulnerability reports are available, providing a holistic view of security posture. The inclusion of the MITRE ATT&CK framework aids in understanding adversary behaviors, while the timeline view helps track event occurrences over time, enhancing threat analysis.



Figure 5: Wazuh alerts

This figure illustrates the alerting mechanism of Wazuh, where potential security threats are categorized and displayed. The alerts cover a range of severities from low-level misconfigurations to high-severity active intrusions. This classification helps prioritize incident responses. Wazuh's alert system ensures that every suspicious activity is captured and flagged for review, enabling faster threat mitigation and improving overall security monitoring efficiency. Wazuh alerts are notifications generated by the Wazuh security platform when it detects potential security issues or suspicious activities on your systems. These alerts can range from low severity (like configuration issues) to high severity (like active intrusions), helping you prioritize and address security threats effectively.



Figure 6: Flood Attack

The figure demonstrates how a flood attack manifests and is detected within the integrated system. A flood attack involves overwhelming a network or server with excessive traffic, aiming to exhaust its resources. The detection capability of Snort, combined with Wazuh's alert correlation, helps identify these patterns early. Visualization of such attacks in the dashboard helps analysts understand the intensity and source of the attack, enabling prompt countermeasures.



Figure 7: Mitre Attack

This figure emphasizes the integration of the MITRE ATT&CK framework within Wazuh, allowing for structured categorization of adversary tactics and techniques. Mapping attacks to this framework enables security teams to understand attack vectors and develop appropriate defense strategies. The framework helps correlate observed activities with known attack patterns, thereby enhancing detection accuracy and response effectiveness.



Figure 8: Threat Hunting

Threat hunting is depicted as a proactive security measure where analysts actively seek hidden threats by analyzing various data sources such as network traffic and log files. The integration of Snort and Wazuh enhances this process by providing comprehensive data for analysis. This figure highlights the systematic approach of identifying anomalies that might evade automated detection systems, thereby strengthening security postures.

# Conclusion

Integrating Wazuh and Snort creates a comprehensive and robust solution for detecting and responding to cybersecurity threats by combining Wazuh’s capabilities in log management, SIEM, and file integrity monitoring with Snort’s real-time network intrusion detection. This integration enables holistic security monitoring by correlating host-based and network-based data to detect threats such as malware, brute force attacks, and denial-of-service (DoS) attempts with greater accuracy. Wazuh’s real-time event analysis and Snort’s active network traffic monitoring enhance detection precision and streamline incident investigation, allowing security analysts to quickly identify attack vectors and affected systems. Automated response capabilities further enable proactive mitigation of risks, while the solution’s efficiency and scalability ensure continuous monitoring with minimal system impact, even as networks expand. With a user-friendly interface, this integration empowers organizations to strengthen their security posture, effectively safeguarding against evolving cyber threats.

Integrating Wazuh and Snort offers a comprehensive and resilient approach to cybersecurity by leveraging the distinct strengths of both systems. Wazuh contributes advanced capabilities in log management, Security Information and Event Management (SIEM), and file integrity monitoring, which are essential for maintaining oversight over system activities and ensuring data security. On the other hand, Snort excels in real-time network intrusion detection, providing continuous surveillance of network traffic to identify suspicious or malicious activities as they occur. When combined, these tools enable holistic security monitoring that correlates both host-based data (from system logs and file monitoring) and network-based data (from packet analysis). This dual-layered approach significantly improves the detection of diverse cybersecurity threats, such as malware infections, brute-force login attempts, and denial-of-service (DoS) attacks. The integration not only enhances the precision of threat detection but also simplifies incident investigation, as security analysts can quickly trace attack vectors and identify compromised systems. Additionally, Wazuh’s automated response capabilities allow for proactive risk mitigation by triggering predefined actions like blocking IPs or sending alerts, thereby reducing the response time to threats. The solution is designed for scalability and efficiency, ensuring continuous protection with minimal system overhead, even as network demands grow. Moreover, its user-friendly interface ensures that security teams can easily navigate and manage alerts, enhancing operational efficiency. Overall, this integration empowers organizations to adopt a more robust security posture, effectively defending against the constantly evolving landscape of cyber threats.

# Reference

[1]. Bassey, Christian, Ebenezer Tonye Chinda, and Samson Idowu. (2024). "Building a Scalable Security Operations Center: A Focus on Open-Source Tools." Journal of Engineering Research and Reports 26 (7): 196-209. DOI: [https://doi.org/10.9734/jerr/2024/v26i71203.](https://doi.org/10.9734/jerr/2024/v26i71203)

[2]. Z. S. Younus and M. Alanezi. (2024). A Survey on Network Security Monitoring: Tools and Functionalities Department of Software, College of Computer Sciences and Mathematics, University of Mosul.

[3]. Tripathy, S. S., & Behera, B. (2024). Evaluation of Future Perspectives on Snort and Wireshark as Tools and Techniques for Intrusion Detection Systems. Industrial Engineering Journal, 53(10), 18–39.

[4]. Shankar, A., & Madisetti, V. (2024). A Framework for Cybersecurity Alert Distribution and Response Network (ADRIAN).

Journal of Software Engineering and Applications, 17(5), 396-420. doi:10.4236/jsea.2024.175022.

[5]. Tripathy, S. S., & Behera, B. (2023). Performance Evaluation of Machine Learning Algorithms for Intrusion Detection System. Journal of Biomechanical Science and Engineering, April Theme- II, 621–640.

[6]. Pramudya, P. B., & Alamsyah, A. (2022). Implementation of a Signature-Based Intrusion Detection System Using SNORT to Prevent Threats in Network Servers. Journal of Soft Computing Exploration, 3(2), 93–98.

[7]. Verma, N. (2022). Detect Network Threat Using SNORT Intrusion Detection System. International Research Journal of Engineering and Technology (IRJET), 9(1).

[8]. S. Kumar, S. Gupta, and S. Arora, “Research Trends in Network-Based Intrusion Detection Systems: A Review,” IEEE Access, vol. 9,pp. 157761–157779, 2021, doi: 10.1109/access.2021.3129775.

[9]. S. A. R. Shah and B. Issac, “Performance comparison of intrusion detection systems and application of machine learning to Snort system,”Future Generation Computer Systems, vol. 80, pp. 157–170, Mar.2018, doi: 10.1016/j.future.2017.10.016.

[10]. F. A. Vadhil, M. F. Nanne, and M. L. SALIHI, “Importance of Machine Learning Techniques to Improve the Open Source Intrusion Detection Systems,” Indonesian Journal of Electrical Engineering and Informatics (IJEEI), vol. 9, no. 3, Sep. 2021, doi:10.52549/ijeei.v9i3.3219.

[11]. A. Ghasempour, “HTTP based Network Intrusion Detection System by Using Machine Learning-Based Classifier,” Tallinn, 2021.

[12]. B. Subba, S. Biswas, and S. Karmakar, “Host Based Intrusion Detection System Using Frequency Analysis of N-Gram Terms,” in *IEEE Region 10 Conference (TENCON) Malaysia*, 2017.

[13]. I. Wahidah, Y. Purwanto, and A. Kurniawan, “Collaborative intrusion detection networks with multi-hop clustering for internet

of things,”International Journal of Electrical and Computer Engineering (IJECE),vol. 11, no. 4, p. 3255, Aug. 2021,

[14]. K. Farhana, M. Rahman, and Md. T. Ahmed, “An intrusion detection system for packet and flow based networks using deep neural network approach,” International Journal of Electrical and Computer Engineering (IJECE), vol. 10, no. 5, p. 5514, Oct. 2020, doi:10.11591/ijece.v10i5.pp5514-5525.

[15]. Podzins, O. and Romanovs, A., "Why SIEM is Irreplaceable in a Secure IT Environment?,," presented at *the 2019 Open Conference of Electrical, Electronic and Information Sciences (eStream)*, Vilnius, Lithuania, 2019.

[16]. Lif, P., Varga, S., Wedlin, M., Lindahl, D., and Persson, M., "Evaluation of Information Elements in a Cyber Incident Report," in *IEEE European S)ymposium on Security and Privacy Workshops (EuroS&PW*, Genoa, Italy, pp. 17-26, 2020.

[17]. González-Granadillo, G., González-Zarzosa, S. and Diaz, R., "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," *sensor* vol. 21, 2021. Muhammad, R., Irawati, I. and Iqbal, M., "Integrated Security

System Implementation for Network Intrusion," *Hunan University*（ *Natural Sciences*）*,* vol. 48, 2021.

[18]. Talukder S. and Talukder, Z., "A Survey on Malware Detection and Analysis Tools," *International Journal of Network Security & Its Applications (IJNSA),* vol. 12, pp. 37-57, 2020.

[19]. Kim, J. and Kwon, H., "Threat classification model for security information event management focusing on model efficiency," *Computers and Security,* vol. 120, 2022.