International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

Enhancing Wazuh SIEM Capabilities through SOAR Integration for Automated Threat Response

K P Sangeetha, Assistant Professor
Department Of CSE – Cyber Security
ACS College Of Engineering
Bengaluru, India
kpsangeetha20@gmail.com

Ananya S Nadig, Bachelor of Engineering
Department Of CSE – Cyber Security
ACS College Of Engineering
Bengaluru, India
ananyaswamy14@gmail.com

S Anu Nadig, Bachelor of Engineering
Department Of CSE – Cyber Security
ACS College Of Engineeringng
Bengaluru, India
anunadig58@gmail.com

Vignesh C, Bachelor of Engineering
Department Of CSE – Cyber Security
ACS College Of Engineering
Bengaluru, India
nyctophile.dark21@gmail.com

***Abstract*—The cybersecurity world today faces challenges such as rapidly evolving attacks, overwhelming log volumes, delayed incident response, and the lack of centralized monitoring across diverse systems. These issues make it difficult for security teams to detect threats early and respond before damage occurs. To address these gaps, this project integrates Wazuh SIEM with Shuffle SOAR to build an automated security monitoring and response environment using open-source technologies. The main goal of the project is to create a mini-SOC that can collect logs from Windows and Linux endpoints, analyze them in real time, and automate responses using SOAR workflows. Key technologies used include VirtualBox-based virtual machines, Kali Linux, Docker containers, Wazuh Manager, Wazuh agents, Kibana dashboards, webhooks, and Shuffle SOAR. The system implements custom detection rules, file integrity monitoring, MITRE ATT&CK mapping, vulnerability scanning, and network traffic analysis. By connecting Wazuh alerts to Shuffle through webhooks, the setup enables automated analysis and faster response actions. The final outcome demonstrates that combining SIEM visibility with SOAR automation significantly improves detection accuracy, reduces manual workload, and enhances overall security posture in a scalable and cost-effective way.**

***Keywords*—SIEM, SOC, SOAR, Analysis, Threat Response.**

I. INTRODUCTION

Cybersecurity has become one of the most important areas of IT today. Every year, attacks are becoming more advanced, and even normal organizations and individuals are becoming targets. Attacks like phishing, ransomware, brute-force logins, and man-in-the-middle (MITM) are now very common. According to Cybersecurity Ventures, the cost of cybercrime is expected to reach around $10.5 trillion annually by 2025. In India, CERT-In reported more than 1.3 million incidents in 2022 alone. These numbers show why stronger monitoring and response systems are needed.

One of the most popular solutions used by organizations is SIEM (Security Information and Event Management). SIEMs collect logs from different devices like servers, firewalls, and intrusion detection systems. They combine all this data, normalize it, and then apply rules to find suspicious behaviour. With dashboards and alerts, SIEM gives a central place for monitoring. SIEM is also used for compliance because companies can store logs for auditing.

But there are challenges. Traditional SIEM platforms like Splunk, ArcSight, and Q-Radar are very costly, require skilled analysts. Our project tries to address this gap by using Wazuh SIEM, which is open-source, and integrating it with SOAR. This way, we aim to build a system that is affordable, automated, and more effective.

A. Background on SIEM and Wazuh

SIEM stands for Security Information and Event Management. It is basically a platform that brings together logs from different systems in one place and helps security teams detect suspicious activity.

Main Features includes the following:

a) Log collection**:** Takes logs from servers, firewalls, IDS, etc.

b) Normalization**:** Converts different log formats into one standard.

c) Alerts and dashboards: Shows warnings and graphs for analysts.

d) Compliance: Helps in meeting regulations like ISO standards.

Organizations use SIEM to detect threats, analyse past incidents, and have real-time visibility of what is happening in their networks. It also makes auditing easier since all logs are collected centrally.

Traditional SIEM systems have several limitations that affect their overall effectiveness. They are often very expensive to purchase and maintain, which can be a barrier for many organizations. Additionally, they tend to generate a large number of false positives, overwhelming security analysts and making it difficult to focus on genuine threats. Most traditional SIEMs do not offer automated blocking or response mechanisms, requiring manual intervention for incident handling.

When deciding which SIEM platform to use for our project, we looked at both commercial and open-source options. Splunk and Q-Radar are among the most popular commercial SIEMs, while Wazuh, Elastic SIEM, and OSSEC are some well-known open-source choices.

Splunk is powerful and widely used in the industry. It provides excellent dashboards, correlation rules, and even has SOAR integration. However, Splunk is extremely costly, and its free version has strict limitations. For a student project or even for small organizations, Splunk is not practical because of its licensing fees and heavy resource usage.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

Other open-source SIEMs like Elastic SIEM are flexible but require complex setup and tuning. OSSEC, which is actually the predecessor of Wazuh, has become outdated and lacks many of the features needed for modern security operations.

Wazuh is an open-source SIEM that is built on top of the Elastic Stack. It collects logs from endpoints using lightweight agents, sends them to the Wazuh manager, and then stores and visualizes them in Elasticsearch and Kibana. Wazuh includes intrusion detection, compliance check, vulnerability scanning.

a) It is free and open-source, unlike Splunk or Q-Radar.
b) It allows us to create custom rules and scripts.
c) It can integrate with SOAR tools like Hive and Cortex.
d) It has strong community support with a lot of tutorials and documentation.

II. WAZUH SETUPS

Wazuh environment for this project was deployed in the controlled virtual laboratory to replicate a typical small-network use case. The host environment consists of an Oracle VirtualBox virtual machine running a Kali Linux guest, where initial installation and testing were performed. The Wazuh Manager and visualization components were deployed as Docker containers on the Kali VM to simplify service orchestration and to allow rapid teardown and replication. Wazuh agents were installed on target systems (including the host VM and additional test endpoints) and configured to forward logs and events to the Wazuh Manager over the agent-manager channel. During setup, administrative accounts (dashboard user accounts and notification addresses) were created and secured with strong passwords; authentication and email parameters were stored in configuration files and handled according to best-practice access controls (no plaintext credentials in shared locations). This virtualized, containerized deployment provided a portable and reproducible testbed for validating detection rules and downstream automation with SOAR. A system with 8–16 GB RAM, 4–8 vCPUs, and at least 50–100 GB storage is required to run the VirtualBox VMs, Wazuh stack, Docker containers, and Shuffle SOAR smoothly.

III. SOAR SETUP AND INTEGRATION

Shuffle is an open-source SOAR (Security Orchestration, Automation, and Response) platform that allows security teams to automate repetitive tasks and build incident-response workflows without coding. It provides a visual workflow builder where different applications can be connected through drag-and-drop blocks. Since Wazuh generates a large number of alerts, Shuffle is used in this project to automate the processing of those alerts, reduce manual workload, and speed up response actions.

To deploy Shuffle, a separate Linux virtual machine was created in VirtualBox to isolate the SOAR environment from the Wazuh SIEM setup. This VM was configured with both NAT and Bridged network adaptors so that it could access the internet for installation while also communicating with the Wazuh Manager. After setting up the operating system, Docker was installed to host Shuffle inside containers.

Shuffle was deployed using the official Docker image, which automatically starts the required backend services and the web user interface. A .env file was created before running the container to define important settings such as admin credentials, internal API keys, allowed ports, and the URLs for HTTP and HTTPS access. In this project, two modes were used: an HTTP mode for testing workflows during development, and an HTTPS mode for production-level execution with secure communication. Once the container was running, the Shuffle dashboard became accessible through a browser, where workflows and applications could be configured.

IV. METHODOLOGY

The methodology for this project followed an implementation-driven approach, where Wazuh SIEM and Shuffle SOAR were deployed, configured, and integrated inside a controlled virtualized environment. Each component was built to perform a specific function in the security pipeline: data collection, analysis, automation, and visualization which allow the system to operate like a small-scale SOC.

A. System Architecture

The system architecture was designed to establish a continuous flow from data generation at endpoints to automated responses using SOAR. Windows and Linux endpoints formed the foundation of the architecture, acting as primary data sources for events such as process executions, file changes, logins, and vulnerabilities.At the center of the architecture sits the Wazuh Manager, responsible for log correlation, rule matching, MITRE ATT&CK mapping, and vulnerability analysis. This central placement ensures standardized alert generation and efficient communication with the SOAR engine.

Shuffle SOAR was placed above the Wazuh Manager, since automation only occurs after an alert is generated. Webhook-based communication between Wazuh and Shuffle created an event-driven architecture where alerts are sent instantly.

Kibana was positioned alongside Wazuh to function as the visualization layer, helping analysts understand trends.

This layered structure endpoints, Wazuh Manager, Shuffle SOAR, Visualization, creates a modular, scalable, and easily extendable security monitoring ecosystem.

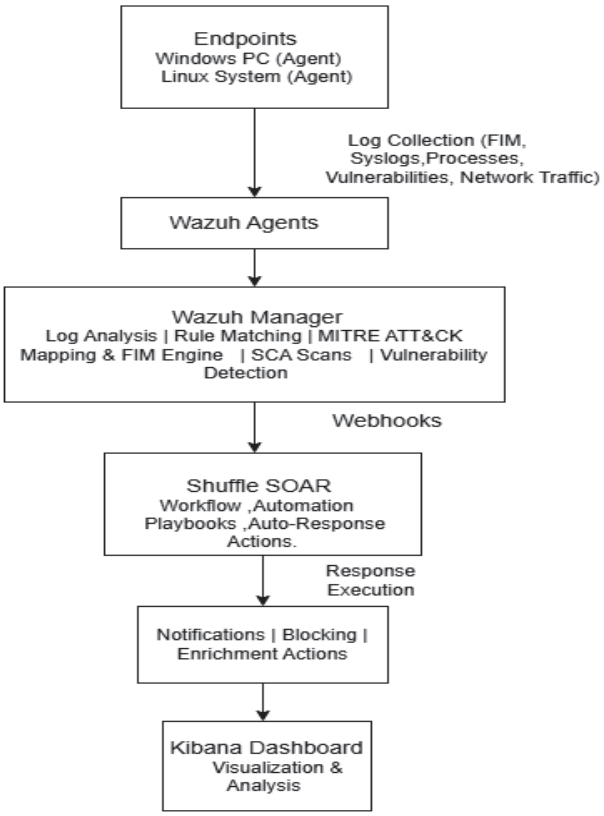

Fig 1. System Architecture

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

B. Log collection and Monitoring

The Data collection in this project is carried out using Wazuh agents installed on Windows and Linux endpoints. These agents continuously gather essential security telemetry and forward it to the Wazuh Manager for centralized processing. The collected data includes operating system logs, authentication events, process activity, file changes, software inventory, and basic network information. This provides complete visibility into endpoint behavior and forms the foundation for all further analysis.

Wazuh's File Integrity Monitoring (FIM) records any modification to critical files or directories, detecting changes in content, ownership, or permissions. Configuration Assessment is performed through scheduled scans that evaluate system settings against security baselines, helping identify weak configurations or policy deviations.

Through continuous Log Data Analysis, the Wazuh Manager correlates incoming logs to identify system errors, unauthorized access attempts, suspicious processes, policy violations, and other anomalies. The software inventory collected from endpoints enables Vulnerability Detection, where package versions are compared against updated vulnerability feeds to identify outdated or risky components.

Monitoring also supports advanced Malware Detection and Threat Hunting. Behavioural indicators, unusual system modifications, and rule-matched events are mapped to MITRE ATT&CK techniques, helping identify malicious activity that may not be immediately obvious. This enhances the ability to investigate patterns or attacker techniques across the environment.

Based on the severity and rule evaluations, Wazuh triggers Incident Response actions. These may include generating high-severity alerts, executing active responses, or forwarding events to Shuffle SOAR via webhook for automation. This ensures suspicious activity is not only detected but also acted upon quickly and consistently.

Through this combined data collection and monitoring framework, the system maintains continuous situational awareness, supports vulnerability and threat analysis, and enables end-to-end detection and response across all monitored endpoints.

V. IMPLEMENTATION

A. Wazuh & SOAR Capabilities

During implementation, Wazuh effectively monitored Windows and Linux endpoints and detected multiple categories of security events in real time. Using its agent-based collection and rule engine, the system identified file tampering, suspicious processes, configuration weaknesses, unusual network activity, and software vulnerabilities across the monitored environment.

- Real-Time Endpoint Monitoring

Wazuh captured continuous endpoint activity, including system logs, running processes, authentication attempts, installed software, and network events. The process monitoring dashboard clearly shows process names, parent processes, execution paths, and command-line arguments enabling detection of abnormal or unexpected executions.

- Vulnerability Detection

Software inventory collected from endpoints was matched with updated CVE data.

- Network Activity Monitoring

Wazuh monitored active ports, inbound/outbound connections, protocol usage, and network flow patterns. Screenshots from the network tab highlight unique networks, top ports, and protocol distribution, helping identify scanning, probing, or unusual traffic spikes often associated with reconnaissance or lateral movement.

- MITRE ATT&CK Technique Mapping

Detected events were mapped to MITRE ATT&CK tactics. The Top Tactics chart recorded techniques such as Defence Evasion, showing Wazuh's ability to classify events based on attacker behaviour and tactics rather than raw logs.

- File Integrity Monitoring (FIM)

The FIM module captured real-time file modifications,

content changes, deletions, and permission updates. The FIM panel shows recent tampering events generated during testing, confirming Wazuh's ability to detect unauthorized or suspicious file changes immediately.

- Configuration & Compliance Assessment

Security Configuration Assessment (SCA) scanned system configurations using benchmarks like CIS Windows 11. The results revealed misconfigurations and compliance failures, which represent potential privilege escalation or system-hardening gaps attackers commonly exploit. Based on the severity and rule evaluations, Wazuh triggers Incident Response actions. These may include generating high-severity alerts, executing active responses, or forwarding events to Shuffle SOAR via webhook for automation.

- Automated Incident Response and Detection

The integration of Wazuh with Shuffle SOAR enabled automated incident response for high-severity alerts, allowing workflows to execute instantly through webhook-based communication. Actions such as sending notifications, enriching alert data, creating tickets, or running containment scripts were triggered automatically, reducing response time and improving consistency. During testing, Wazuh also detected several attack-like behaviors, including unauthorized file modifications, abnormal or high-risk process executions, unusual network activity, weak system configurations, and outdated software vulnerabilities. These detections align with common attacker techniques and validate the system's ability to identify early indicators of compromise effectively.

B. Snapshots of the System

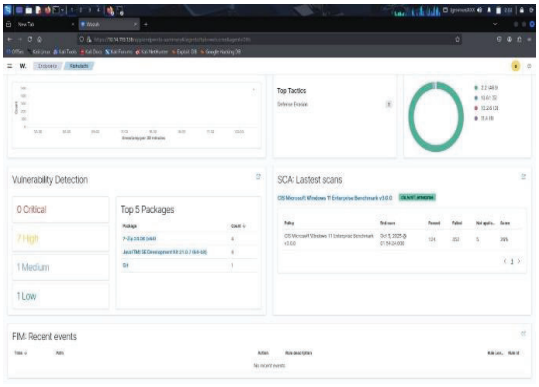

Fig 2. Screenshot 1: SCA Scans.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

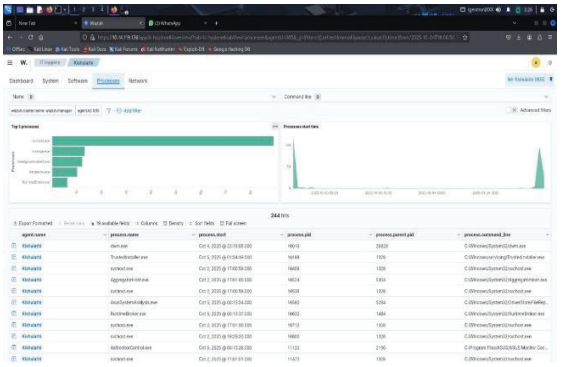

Fig 3. Screenshot 2: Process detections.

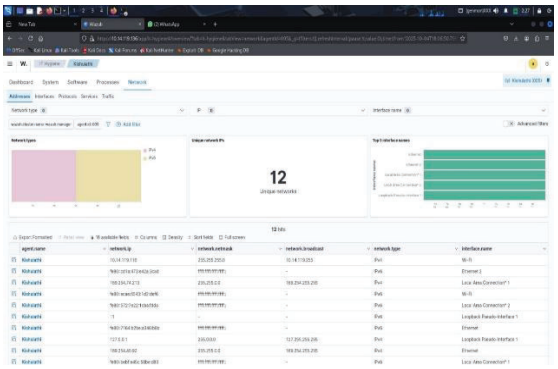

Fig 4. Screenshot 3: Network detections.

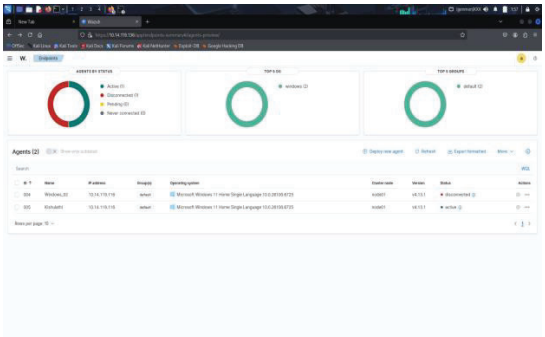

Fig 5. Screenshot 4: Dashboard overview.

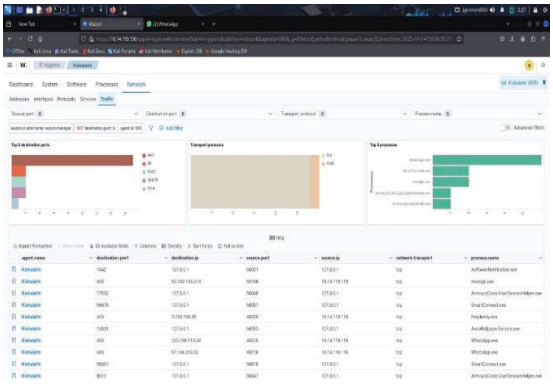

Fig 6. Screenshot 5: Traffic overview.

VI. RESULTS AND FUTURE OUTCOMES

A. Result and Discussions

The implemented system successfully monitored Windows and Linux endpoints and detected key security events in real time. Wazuh identified vulnerabilities, configuration weaknesses, suspicious processes, file tampering, and abnormal network activity, all of which were visible through the Kibana dashboards. MITRE ATT&CK mappings and FIM alerts validated the system's ability to capture attack-like behavior effectively. The integration with Shuffle SOAR further improved response time by automating actions for high-severity alerts, showing a clear reduction in manual effort and ensuring consistent incident handling across repeated threats. Overall, the results confirmed that combining Wazuh SIEM with Shuffle SOAR provides a practical, automated, and scalable approach to endpoint security monitoring.

Future Scope

This work can be extended by adding more endpoints, integrating advanced threat-intelligence feeds, and expanding SOAR workflows for deeper automation. Future improvements could include cloud security monitoring, container security at scale, machine-learning-based anomaly detection, and full ticketing system integration for complete SOC lifecycle management. The system can also be deployed on larger networks to test its performance and effectiveness in enterprise-grade environments.

VII. CONCLUSION

This project successfully implemented a functional SIEM–SOAR environment by integrating Wazuh with Shuffle in a virtualized setup. Wazuh effectively monitored Windows and Linux endpoints, detecting file changes, suspicious processes, vulnerabilities, misconfigurations, and unusual network activity, all visualized through Kibana dashboards. The webhook-based integration with Shuffle SOAR enabled automated workflows for high-severity alerts, reducing response time and improving incident handling. Overall, the system proved to be a scalable, efficient, and cost-effective solution for real-time monitoring and automated response, demonstrating the practical value of open-source tools in building a mini-SOC.

REFERENCES

[1] Catescu, Georgeta. "Detecting insider threats using security information and event management (SIEM)." University of Applied Sciences Technikum Wien, 2018. Available at: shorturl.at/dtzOT

[2] González-Granadillo, Gustavo, Susana González-Zarzosa, and Rodrigo Diaz. "Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures."Sensors 21, no. 14 (2021): 4759.

[3] Coppolino, Luigi, Luigi Sgaglione, Salvatore D'Antonio, Mario Magliulo, Luigi Romano, and Roberto Pacelli. "Risk assessment driven use of advanced SIEM technology for cyber protection of critical e-health processes."SN Computer Science 3 (2022): 1-13.

[4] Muhammad, AdabiRaihan, Parman Sukarno, and AuliaArifWardana. "Integrated security information and event management (SIEM) with intrusion detection system (IDS) for live analysis based on machine learning."Procedia Computer Science 217 (2023): 1406-1415.

[5] Zaidan, MustaghfirNaufal, Parman Sukarno, and AuliaArifWardana. "Collaborative Detection of SQL Injection Attacks using SIEM, Multi-Wazuh Agents, and Diverse Web Application Firewalls." In 2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), pp. 1-6. IEEE, 2024.

[6] Maliki, M. Akmal, Parman Sukarno, and AuliaArifWardana. "Integration of Heterogeneous IDS with SIEM for DDoS Attack

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14, Issue 06, ACSCON - 2026

Detection in Computer Networked Multi-Organizational Environments." In 2024 5th International Conference on Communications, Information, Electronic and Energy Systems (CIEES), pp. 1-7. IEEE, 2024.

[7] Ahmed, WasanSaad, and Ziyad Tariq Mustafa AL-Ta'I. "Analysis of Wazuh SIEM's Effectiveness in Cloud Security Monitoring."Journal of Cybersecurity& Information Management 15, no. 1 (2025).

[8] Andronache, Maria-Mădalină, AlexandruVulpe, and CorneliuBurileanu. "A Comparative Study of Intrusion Events in Different SIEM Systems." In 2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI), pp. 000065-000070. IEEE, 2025.

[9] Lee, Jong-Hoon, Young Soo Kim, Jong Hyun Kim, and Ik Kyun Kim. "Toward the SIEM architecture for cloud-based security services." (In 2017 IEEE Conference on Communications and Network Security (CNS), pp. 398-399. IEEE, 2017).

[10] Schölzel, Markus, Evren Eren, and Kai-Oliver Detken. "A viable SIEM approach for Android." (In 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), vol. 2, pp. 803-807. IEEE, 2015).

[11] Serckumecka, Adriano, Ibéria Medeiros, and Alysson Bessani. "Low-cost serverless SIEM in the cloud." (In 2019 38th Symposium on Reliable Distributed Systems (SRDS), pp. 381-3811. IEEE, 2019).

[12] Mokalled, Hassan, Rosario Catelli, Valentina Casola, Daniele Debertol, Ermete Meda, and Rodolfo Zunino. "The applicability of a SIEM solution: Requirements and evaluation." (In 2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE), pp. 132-137. IEEE, 2019).

[13] Singh, S., and A. Kumar. "Detect and Mitigate Cyberattacks Using SIEM." IEEE Xplore, 2022.

[14] Sridharan, Anish, and V. Kanchana. "SIEM integration with SOAR."