International Journal of Education, Science, Technology and Engineering
p-ISSN: 2685-1458, e-ISSN: 2684-9844

Original Research Paper

Automated Defense Against Application-Layer Attacks on Windows Systems Using Wazuh and Shuffle

Aastha Thakker[1], Aditya More[1*], Kapil Kumar[1]

[1] *Department of Biochemistry and Forensic Science, Gujarat University. Ahmedabad, India.*

Article History
Received:
29.04.2025

Revised:
21.05.2025

Accepted:
02.06.2025

***Corresponding Author:**
Aditya More
Email:
moreadityarajesh@gmail.com

Abstract: Application-layer attacks targeting Windows systems remain a significant threat due to their ability to bypass traditional perimeter defenses. These attacks often exploit vulnerabilities listed in the OWASP Top 10 for desktop applications, demanding proactive defense mechanisms. This paper proposes a unified approach that combines SIEM and SOAR capabilities to detect and respond to Windows-based application-layer threats with increased efficiency and automation. The framework integrates the open-source SIEM platform Wazuh with the SOAR engine Shuffle to automate threat detection and incident response. A layered defense strategy is implemented, involving log correlation, rule-based policy enforcement, and playbook-driven response automation. The integration reduces manual triage overhead and enhances response time compared to traditional SOC patterns. This framework demonstrates a scalable, open-source-based solution for defending Windows environments at the application layer. It sets the groundwork for future integration of AI-driven analytics, multi-OS support, and tamper-proof event lo event logging using blockchain technologies.

Keywords: Automated Security Orchestration, Log Correlation, SIEM, SOAR, Wazuh.

1. Introduction

As cyber threats evolve in sophistication and frequency, integrating detection and automated response mechanisms within Security Operations Centers (SOCs) has become critical. Modern-day SOCs are no longer confined to passive monitoring; they require dynamic systems capable of detecting, analyzing, and mitigating threats in real time. With increasing dependence on digital infrastructure, especially in enterprise environments, security teams face mounting challenges in responding swiftly to complex and multi-layered attacks. Traditional models relying heavily on human analysts are often unable to cope with the sheer volume of security alerts generated daily. This reactive posture creates latency, allowing attackers to exploit security gaps effectively. To overcome these limitations, the integration of Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) technologies has emerged as a proactive strategy. Windows remains the most common and widely used operating system globally, mostly across enterprise, government, and critical infrastructure environments. Its broad adoption makes it an easy target for cyber attackers, especially those exploiting application-layer vulnerabilities, including logic flaws, privilege escalation mechanisms, and insecure communications. Moreover, as enterprises rely heavily on legacy and modern Windows applications for daily operations, even minor vulnerabilities can become critical exploitation points. The OWASP Top 10 Desktop-Based Attacks represent a standardized threat model capturing the most critical security risks affecting Windows-based applications. From Injection attacks and Improper Authorization to Insecure Cryptography and Insufficient Logging, these vectors provide a roadmap for both attackers and defenders. Given the complexity and scope of these vulnerabilities, the security community increasingly recognizes the need for focused detection algorithms and automated playbooks to ensure timely identification and mitigation. The application layer is a critical domain for purple teaming and coordinated offensive-defense simulation.

Though the integration of SIEM and SOAR platforms has demonstrated potential in enhancing incident response, notable challenges remain, particularly within the Windows application layer. Many sophisticated attacks are capable of evading traditional endpoint security measures and often go undetected by standard telemetry. Security Operations Centers (SOCs) also continue to struggle with alert fatigue, as analysts are inundated with false positives and low-value alerts.

This research is scoped to focus on enterprise-level detection and mitigation strategies for application-layer attacks in Windows-based environments. Specifically, it investigates:

1) The integration of Wazuh (SIEM) and Shuffle (SOAR) to form a cohesive threat detection and response pipeline.
2) The identification, simulation, and analysis of attacks based on the OWASP Top 10 desktop application vulnerabilities.
3) The role of purple teaming exercises in refining detection logic and improving playbook effectiveness.
4) Real-time notification and response orchestration using Microsoft Teams as a human-in-the-loop collaboration tool.
5) Testing within both simulated and real-world SOC environments to validate the accuracy, performance, and scalability of the system.

2. Literature Review

Recent research by Waelchli and Walter [1] investigated SOAR deployments to mitigate social engineering threats. Their work identifies both the advantages of automated response and challenges such as cost and SIEM dependencies—issues directly related to this study's scope. Complementing this, Park et al. [2] evaluated open-source endpoint detection integrations using tools like Osquery and GRR, reinforcing the feasibility of combining modular tools for enhanced visibility. Erdivan [3] emphasized the importance of SOC frameworks grounded in international standards. This serves as a foundational reference for this study's human-tool integration. Further supporting this, Javid [4] tested Wazuh's on-premises deployment in real environments, showcasing its viability as an efficient SIEM/XDR system when integrated with threat intelligence platforms like VirusTotal. The role of Wazuh and TheHive in alert configuration was explored by Jumiaty and Soewito [5], where Telegram was used for notifications. This aligns with the use of Microsoft Teams in the current study, underscoring the adaptability of alert channels based on operational needs. Similarly, Bassey et al. [6] designed a scalable SOC architecture using open-source tools—validating the practicality of such setups in production environments. Abiade [7] proposes a hybrid model combining automation for routine incidents and human intervention for complex cases. This reflects the balanced incident

handling strategy advocated in this research. From an AI perspective, Kasturi et al. [8] demonstrated how neural networks could predict exploit paths from known vulnerabilities. Though exploratory, this supports future AI-SOAR integrations for proactive threat modeling. Nieminen [9] contributed insight into automated alert enrichment, reducing fatigue among Tier 1 analysts and accelerating triage—a concept directly applied in this project's SOAR workflow.

3. Methodology

the aim of this study is to develop and evaluate an integrated system that combines Security SIEM with SOAR to enhance the detection and mitigation of application-layer threats in Windows environments. The focus is on reducing detection-to-response times and improving alert precision using automated playbooks aligned with OWASP's Top 10 desktop application vulnerabilities. The study adopts an experimental research methodology, joining system design with controlled attack simulations to assess detection and response outcomes.

The methodology follows a phased approach:

1) System Integration Phase: Configuration of SIEM and SOAR tools, along with deployment of endpoint agents and notification systems.
2) Rule and Playbook Development: Creation of custom detection rules in Wazuh and corresponding response playbooks in Shuffle.
3) Simulation Phase: Execution of controlled attack scenarios aligned with OWASP Top 10 vulnerabilities in both real and virtualized Windows environments.
4) Evaluation Phase: Collection and analysis of metrics, including alert fidelity, response time, playbook execution accuracy, and analyst workload reduction.

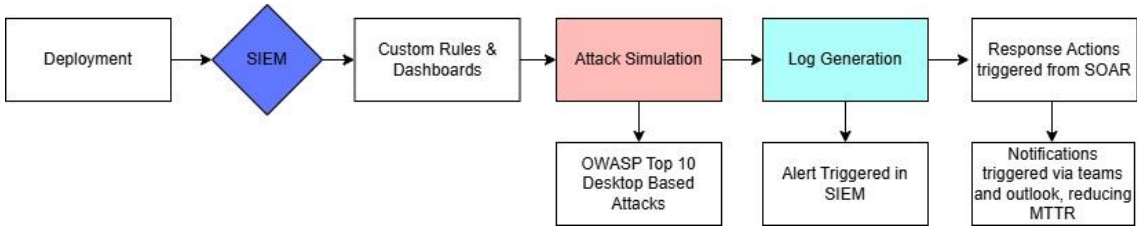


Figure 1. Architectural Overview of the Unified workflow for SIEM and SOAR

This architecture is composed of the following layers:

1) Endpoint Layer: Includes Windows systems with deployed Wazuh agents that monitor file changes, process activity, and user behavior.
2) Data Collection and Analysis Layer: Managed by the Wazuh manager, which aggregates logs, applies detection rules, and forwards high-priority alerts to the SOAR system.
3) Orchestration Layer: Operated by Shuffle, which parses incoming alerts and triggers automated playbooks. These may include host isolation, ticket creation, user notification, or blocking IP addresses.
4) Notification Layer: Real-time alerts are formatted and sent to Microsoft Teams channels, allowing analysts to monitor and intervene if necessary.

The workflow begins at the endpoint level, where Wazuh agents monitor for suspicious activity, such as abnormal script execution, unauthorized access attempts, or code injections. Upon identifying a potential threat, Wazuh evaluates the activity against its rule set. If the alert severity crosses a defined threshold, the alert is forwarded to Shuffle via a webhook integration. Shuffle receives the alert and initiates a predefined playbook.

4. Finding and Discussion

4.1. Purple Teaming Activities for Alert Generation and Detection Enhancement

Purple teaming integrates both offensive (red team) and defensive (blue team) approaches to evaluate the effectiveness of detection and response capabilities. In this study, I have focused on how purple

teaming is utilized to replicate realistic attack scenarios within a controlled environment. The red team simulates attack techniques that target Windows application-layer vulnerabilities, while the blue team, using Wazuh and Shuffle, monitors activity and responds through configured rules and automated playbooks.

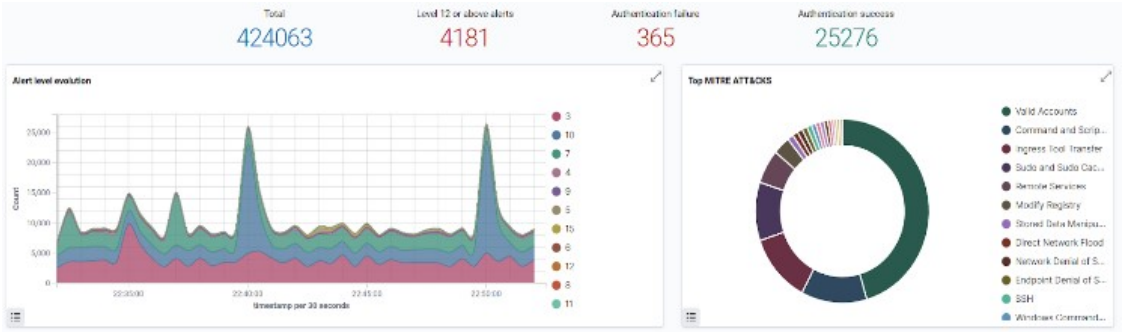


Figure 2. Dashboard of Wazuh

4.1.1. OWASP Top 10 - Desktop-Based Attack: Exploitation and Relevance

This section outlines simulated attack scenarios modeled on the OWASP Top 10 vulnerabilities for desktop applications, with an emphasis on Windows-based environments. Each scenario targets specific application-layer flaws—such as insecure deserialization, improper input validation, and broken access controls. For each simulated attack, a corresponding detection rule is crafted within the SIEM to identify malicious behavior, followed by the development of a targeted SOAR playbook to automate the appropriate response actions.

1) Injections

Detected repeated SQL injection attempts from the same source IP. Automated playbook checks IP, hash, and domain, and sends alerts to Microsoft Teams.

rule.description	rule.level	data.url	rule.mitre.technique	GeoLocation.region_name
Multiple SQL injection attempts from same source ip.	10	/scripts/calendar.php?month=%27%20UNION%20SELECT%201%2c1%2c%271744572564%27%2c%27calendarix_month_sql_injection.nasl%27%2c1%20%23	Process Injection	Washington
Multiple SQL injection attempts from same source ip.	10	/scripts/calendar.php?month=&year=%27%20UNION%20SELECT%201%2c1%2c%271744575798%27%2c%27calendarix_month_sql_injection.nasl%27%2c1%20%23	Process Injection	Washington

Figure 3. Wazuh Detection Log Showing Repeated SQL Injection Attempts from A Single Source IP

Figure 4. Playbook For Checking IP, Hash and Domain from The Log and Alerting on Teams

2) Broken Authentication and Session Management

Brute force attacks observed from a single source IP using the same username. Authentication logs are monitored, and suspicious patterns trigger instant alerts.

rule.description	rule.level	data.win.eventdata.ipAddress	data.win.eventdata.status	data.win.eventdata.subStatus	data.win.eventdata.targetUserName
Multiple Windows logon failures.	10	10.142.01.109	0xc000006d	0xc0000064	jnian
Multiple Windows logon failures.	10	10.142.01.109	0xc000005e	0x0	jnian
Multiple Windows logon failures.	10	10.142.01.109	0xc000005e	0x0	jnian
Multiple Windows logon failures.	10	10.142.01.109	0xc000005e	0x0	jnian
Multiple Windows logon failures.	10	10.142.01.109	0xc000006d	0xc0000064	jnian
Multiple Windows logon failures.	10	10.142.01.109	0xc000006d	0xc0000064	jnian
Multiple Windows logon failures.	10	10.142.01.109	0xc000005e	0x0	jnian

Figure 5. Brute Force attack from same source IP and Username

3) Sensitive Data Exposure

Sensitive files were shared via external drives, risking data leaks. Playbook monitors failed login attempts to detect unauthorized access patterns.

rule.description	rule.id	data.newdata.ruleViolationInfo.triggeredActionTypes	data.newdata.ruleViolationInfo.ruleInfo.resourceName	data.newdata.ruleViolationInfo.recipients
[redacted] Data Loss Prevention (DLP)	160014	DRIVE_WARN_ON_EXTERNAL_SHARING, ALERT	policies/akajj264aovp52hbb4	aditya[redacted]
[redacted] Data Loss Prevention (DLP)	160014	DRIVE_WARN_ON_EXTERNAL_SHARING, ALERT	policies/akajj264aovp52hbb4	krishna[redacted]
[redacted]: Data Loss Prevention (DLP)	160014	DRIVE_BLOCK_EXTERNAL_SHARING, ALERT	policies/akajj264apd4bfuha4	vaibhav[redacted]
[redacted] Data Loss Prevention (DLP)	160014	DRIVE_WARN_ON_EXTERNAL_SHARING, ALERT	policies/akajj264aovp52hbb4	vaibhav[redacted]

Figure 6. Sensitive File Sharing Over Drive

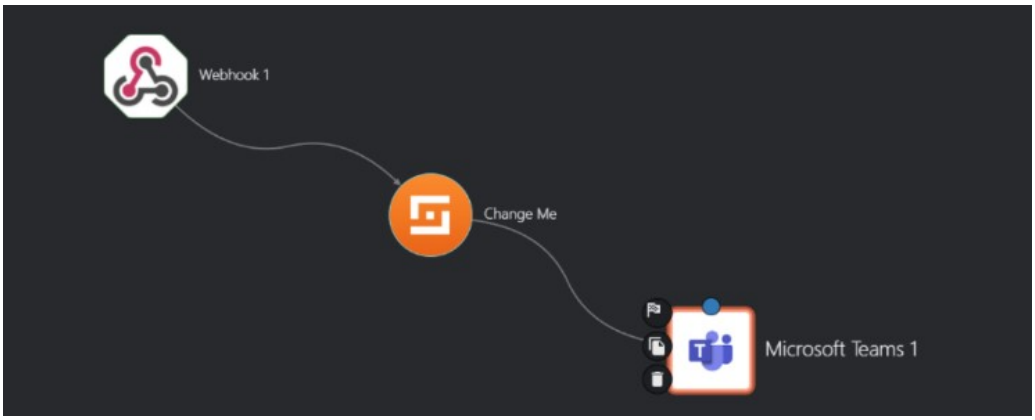


Figure 7. SOAR Playbook Configured to Respond to Multiple Failed Login Attempts

4) Improper Cryptography Usage

Credential dumping activity identified on the system. Such events are flagged for further forensic review and containment actions.

rule.description	decoder.name	data.win.eventdata.ruleName
[Potential LSASS dump found]	windows_eventchannel	technique_id=T1003,technique_name=Credential Dumping
[Potential LSASS dump found]	windows_eventchannel	technique_id=T1003,technique_name=Credential Dumping
[Potential LSASS dump found]	windows_eventchannel	technique_id=T1003,technique_name=Credential Dumping

Figure 8. Credential Dumping of The User with Specific Details

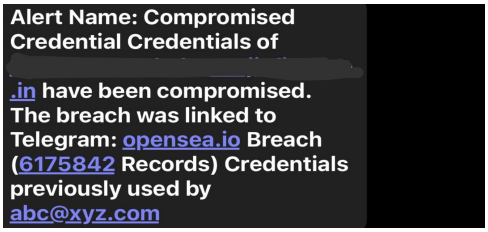


Figure 9. Notification Of Compromised Credentials of The User with Specific Details Obtained from The Log

5) Improper Authorization

Unauthorized changes to local security group membership were logged. Role-based access control checks are enforced to prevent privilege misuse.

rule.description	rule.mitre.tactic	rule.mitre.technique	data.win.system.eventID
Security enabled local group changed.	Defense Evasion, Privilege Escalation	Domain Policy Modification	4735
Security enabled local group changed.	Defense Evasion, Privilege Escalation	Domain Policy Modification	4735
Security enabled local group changed.	Defense Evasion, Privilege Escalation	Domain Policy Modification	4735
Security enabled local group changed.	Defense Evasion, Privilege Escalation	Domain Policy Modification	4735

Figure 10. Log for Security Enabled Local Group Changed in Windows

6) Security Misconfigurations

Windows Defender was found to be disabled, increasing system risk. Configuration drifts are detected, and alerts are raised for remediation.

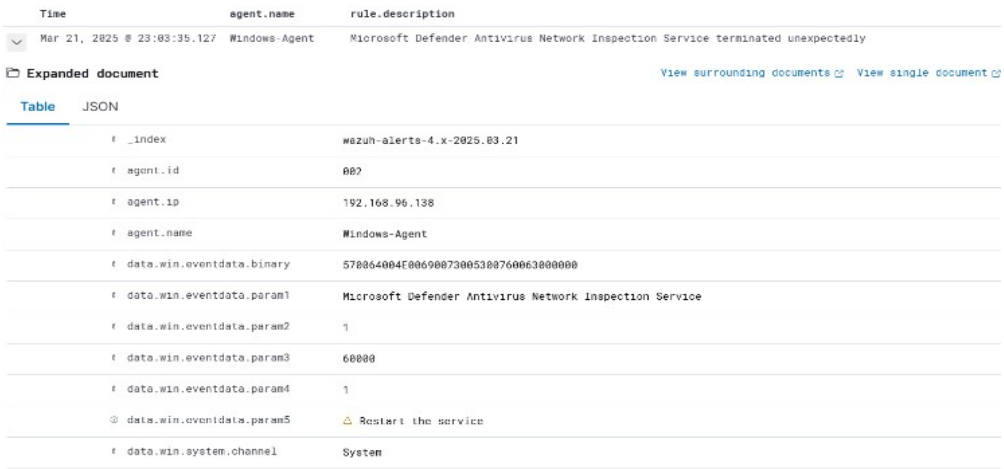


Figure 11. Alert Triggered by Wazuh Agent Detecting Disabled Windows Defender

7) Insecure Communication

Reconnaissance scans detected using unsecured communication protocols. Such network scans are auto-flagged and reported for blocking or quarantine.

data.parameters.alert.manager.name	wazuh-server
data.parameters.alert.rule.description	Nmap scripting engine detected.
data.parameters.alert.rule.firedtimes	17
data.parameters.alert.rule.groups	local
data.parameters.alert.rule.id	100201
data.parameters.alert.rule.level	12
data.parameters.alert.rule.mail	true
data.parameters.alert.rule.mitre.id	T1595
data.parameters.alert.rule.mitre.tactic	Reconnaissance
data.parameters.alert.rule.mitre.technique	Active Scanning

Figure 12. Reconnaissance Scanning on A Host

8) Poor Code Quality

Misconfigured disk-related code can lead to storage issues. Playbook identifies full partitions and notifies the admin team for action.

rule.description	rule.mitre.technique	decoder.name
System running out of memory. Availability of the system is in risk.	Endpoint Denial of Service	kernel
System running out of memory. Availability of the system is in risk.	Endpoint Denial of Service	kernel
System running out of memory. Availability of the system is in risk.	Endpoint Denial of Service	kernel

Figure 13. Poor Disk Code Configuration

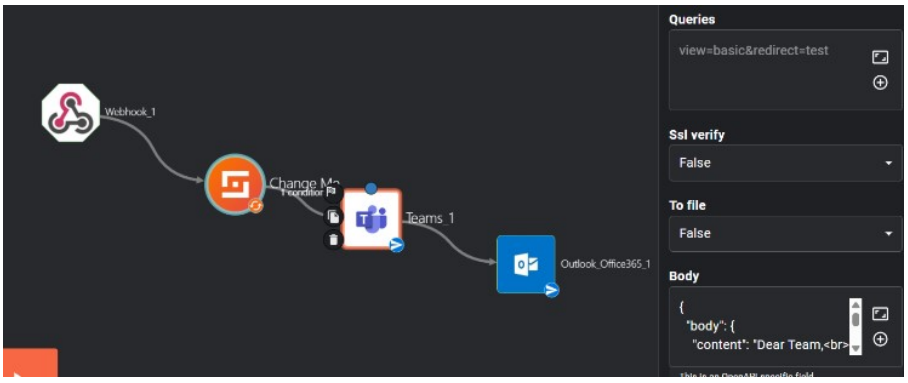


Figure 14. Playbook for Storage Partition Full

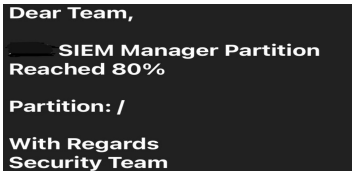


Figure 15. Notification for SIEM Manager 80% Partition Reached

9) Using Components with known Vulnerabilities

Outdated components were identified via the vulnerability dashboard. Automated patching or alerts are triggered based on severity level.

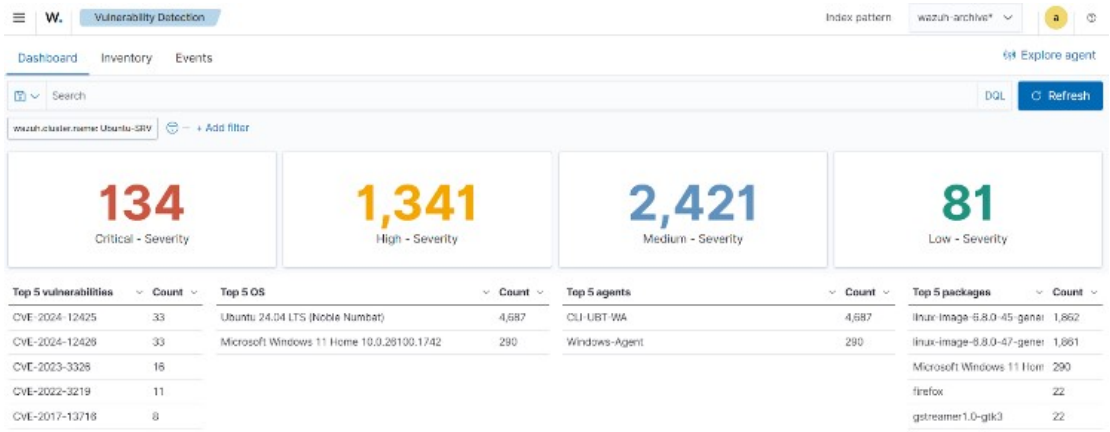
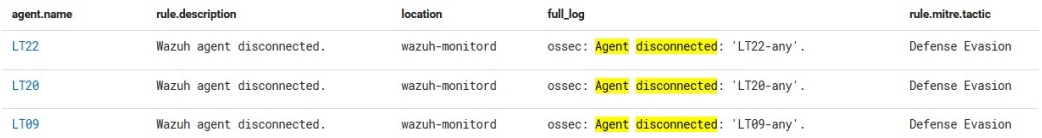


Figure 16. Dashboard Detecting Known Vulnerabilities

10) Insufficient Logging and Monitoring

Wazuh agent disconnections were flagged, risking visibility loss. Playbook automates alerting when logging agents stop or disconnect.



agent.name	rule.description	location	full_log	rule.mitre.tactic
LT22	Wazuh agent disconnected.	wazuh-monitord	ossec: Agent disconnected: 'LT22-any'.	Defense Evasion
LT20	Wazuh agent disconnected.	wazuh-monitord	ossec: Agent disconnected: 'LT20-any'.	Defense Evasion
LT09	Wazuh agent disconnected.	wazuh-monitord	ossec: Agent disconnected: 'LT09-any'.	Defense Evasion

Figure 17. Alert of Wazuh Agent Disconnected

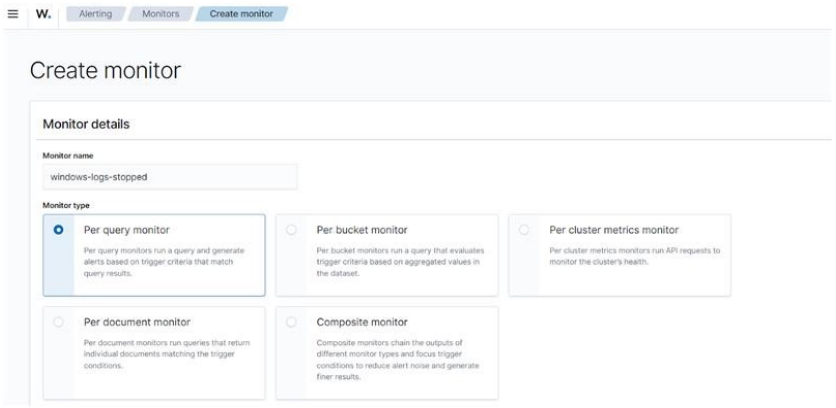


Figure 18. Automation of Alert Configuration for Logs Stopped

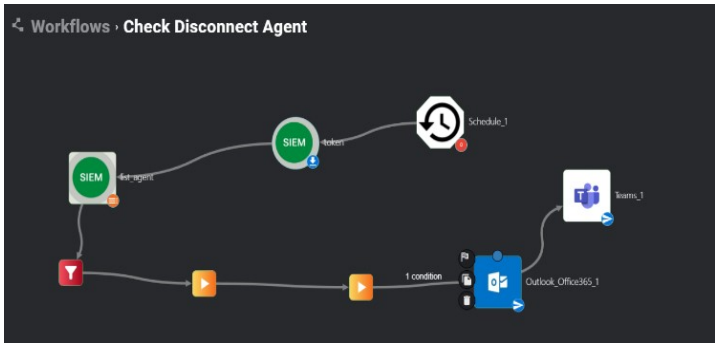


Figure 19. Playbook for SIEM Agent Disconnected

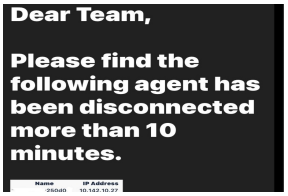


Figure 20. Notification of Wazuh Agent Disconnected

4.1.2. Mapping Attacks to MITRE ATT&CK

To ensure consistency with widely accepted adversarial behavior models, each attack scenario simulated in this study was mapped to relevant techniques from the MITRE ATT&CK Framework. This mapping provides structured visibility into the tactics employed by adversaries and enhances the interpretability of alerts generated by the SIEM-SOAR system.

The following table presents a structured mapping of each OWASP Top 10 desktop-based attack simulated during the study to corresponding MITRE ATT&CK techniques:

Table 1. MITRE ATT&CK Mapping Each OWASP Top 10 Desktop-Based Attack

No.	DA Category	Attack Performed	MITRE Tactic
DA1	Injections	SQL Injection from same source IP	Initial Access
DA2	Broken Authentication & Session Management	Brute Force attack from same IP and Username	Credential Access
DA3	Sensitive Data Exposure	Sensitive File sharing over drive	Exfiltration
DA4	Improper Cryptography Usage	Credential Dumping	Credential Access
DA5	Improper Authorization	Security enabled local group changed in Windows	Privilege Escalation
DA6	Security Misconfiguration	Disabled Windows Defender	Defense Evasion
DA7	Insecure Communication	Reconnaissance scanning on a host	Reconnaissance
DA8	Poor Code Quality	Poor disk code configuration	Impact
DA9	Using Components with Known Vulnerabilities	Dashboard detecting known vulnerabilities	Initial Access
DA10	Insufficient Logging & Monitoring	Alert of Wazuh agent disconnected	Defense Evasion

This mapping facilitates a comprehensive understanding of the attack lifecycle and allows security analysts to align detection and response mechanisms with well-defined threat behaviors. Integrating MITRE ATT&CK into detection logic also supports better threat hunting, response prioritization, and analyst training.

International Journal of Education, Science, Technology and Engineering, vol. 8, no. 1, pp. 45-57, June 2025. **DOI: 10.36079/lamintang.ijeste-0801.842**

4.2. Discussion

In this study, the key outcomes observed during the testing and evaluation of the integrated SIEM-SOAR system, focusing on detection efficiency, response automation, alerting mechanisms, and alignment with existing practices are mentioned. The experiments were conducted in both isolated and real-world test environments, using OWASP Top 10 desktop-based attack scenarios as the basis for validation.

1) Effectiveness of Automated SOAR Playbook

The deployment of automated SOAR playbooks showcased a substantial improvement in response velocity, precision, and standardization of incident handling. Each playbook was tightly coupled with detection rules within the SIEM platform, enabling real-time, rule-driven orchestration of incident response actions. Upon ingestion of a verified alert, the following automated tasks were triggered:

- Threat intelligence enrichment (IP, domain, and hash reputation checks)
- Real-time analyst notification via integrated channels (e.g., Teams, Slack, email, ticketing)
- Case documentation and summary generation for incident records

In controlled tests, playbooks executed consistently across diverse threat scenarios, containment of repetitive incidents (e.g., brute force, known malware hash detection). Manual intervention was only necessary for alerts exhibiting contextual ambiguity, such as low-confidence anomalies or multi-phase attacks that required lateral movement correlation.

These playbooks not only reduced the cognitive load on analysts by minimizing repetitive tasks but also ensured uniformity in response workflows, which is critical for maintaining consistency in SOC operations. The observed mean time to respond (MTTR) decreased when compared to manual triage methods.

2) SOAR-Driven Notifications

The alerting module within the SOAR platform was fine-tuned to prioritize actionable intelligence. Unlike traditional alerting systems that generate noise, the integrated pipeline filtered low-priority events and forwarded only correlated alerts with high-fidelity indicators of compromise (IOCs). This streamlined escalation process leveraged:

- Contextual enrichment from threat intelligence feeds
- Dynamic severity scoring based on MITRE ATT&CK tactics
- Role-based notification routing for rapid decision-making

The result was a marked reduction in alert fatigue, during the evaluation period. The system also demonstrated compliance alignment by ensuring alert traceability, audit logging, and structured reporting.

3) Pattern Visualization

The visualization of attack patterns revealed common trends in simulated attacker behavior. Several OWASP vulnerabilities were frequently exploited in sequential chains, often beginning with unauthorized access attempts and leading to data exposure or privilege escalation.

Using the data collected during simulations, recurring behaviors were identified across multiple attack vectors. These patterns were used to enhance detection logic and adjust the sensitivity of alert rules in the SIEM. Visualization tools helped map these trends over time, offering valuable insights for further tuning of the system. The ability to monitor and visualize these behavioral trends allowed the security team to understand not only individual threats but also their context within broader attack campaigns. This insight is critical for proactive defense, as it helps prioritize future response development and detection tuning.

Using advanced correlation rules and timeline visualization tools, the following trends were mapped:

- Frequently exploited chains: SQLi → Remote File Inclusion → Privilege Escalation
- Time-bound spikes in specific attack types
- Lateral movement paths and interdependency between compromised endpoints

In the Discussion section, the author explains how to finding are. The results obtained from the research have to be supported by sufficient data. The discussion must be the answers or the research hypothesis stated previously in the introduction part.

International Journal of Education, Science, Technology and Engineering, vol. 8, no. 1, pp. 45-57, June 2025. **DOI: 10.36079/lamintang.ijeste-0801.842**

The discussion of the research and test results obtained is presented in the form of theoretical descriptions, both qualitatively and quantitatively. In the discussion section, the author presents the results of data processing and research results logically.

5. Conclusion

The integration of Wazuh (SIEM) and Shuffle (SOAR) into a unified detection-response pipeline demonstrated clear improvements in operational efficiency, especially in the context of application-layer security for Windows-based environments. A series of simulated attack scenarios—mapped against OWASP Top 10 vulnerabilities—were executed to assess the system's ability to detect and respond to complex threats.

Key findings are as follows:

1) Effective Threat Detection: Custom rule sets in Wazuh successfully identified a range of attack behaviors at the application layer. These rules were fine-tuned based on iterative testing and feedback from purple teaming exercises.
2) Consistent Automated Response: SOAR playbooks execute predefined actions reliably, resulting in timely and standardized responses. Playbooks addressed analyst notification and were capable of operating with minimal manual oversight.
3) Improved Alert Clarity and Notification Efficiency: Integration with Microsoft Teams provided a clear and direct communication channel for SOC analysts. Real-time, context-rich alerts helped reduce decision-making time and promoted coordinated response efforts.
4) Pattern Recognition and Behavioral Insight: The system enabled identification of recurring attack patterns, which in turn supported proactive tuning of detection rules. Behavioral mapping against the MITRE ATT&CK framework added depth to incident classification and response prioritization.
5) Scalability Across Environments: The architecture was validated in both isolated virtual environments and real-world lab conditions, demonstrating adaptability to different deployment scales without compromising detection integrity or response speed.

The system can be enhanced by simulating advanced attacks using real-world data, expanding to cloud platforms for scalability, and supporting Linux, macOS, and IoT for broader coverage. AI/ML can improve threat prediction, while blockchain ensures tamper-proof event logs for audit and compliance.

While the current implementation demonstrates effective detection and response capabilities within Windows-based SOC environments, there are several areas for future expansion. These enhancements aim to increase the applicability, scalability, and intelligence of the system, supporting broader security needs across infrastructures and platforms.

- Expanding Use Cases for Refined Attack Scenarios

Future iterations of this system could benefit from the inclusion of more granular and evolving attack scenarios beyond the OWASP Top 10. These include simulations of ransomware operations, fileless malware execution, insider threat behavior, and persistence mechanisms observed in advanced persistent threats (APTs). Incorporating these attack chains would require the design of deeper detection rules and response playbooks capable of addressing multi-stage attacks.

Additionally, using datasets derived from real-world breach reports or MITRE's open-source ATT&CK evaluations would help ensure that detection logic remains current. Extending purple teaming efforts to test these scenarios continuously would further reinforce the adaptive nature of the defense stack.

- Porting to Cloud-Based Infrastructure

The rising adoption of hybrid and cloud-native architectures, porting the SIEM-SOAR integration to platforms such as AWS, Azure, or Google Cloud is a logical progression. This would involve rearchitecting components like Wazuh managers and Shuffle engines to operate in containerized or serverless environments.

Log ingestion would need to support cloud-native telemetry sources such as CloudTrail, Azure Monitor, and GCP Audit Logs. Playbooks would also be adapted to interact with cloud APIs for actions like revoking IAM roles, terminating cloud instances, or applying security group updates. Such portability ensures scalability, high availability, and dynamic resource allocation—key for large enterprises operating across multiple environments.

- Multi-OS Support: Linux, MacOS, IoT Devices

The current system focuses solely on Windows environments. Expanding support to include Linux distributions, macOS endpoints, and IoT devices would make the platform more versatile. Wazuh natively supports Linux agents, enabling file integrity monitoring, process auditing, and log analysis on Unix-like systems. For IoT environments, lightweight monitoring agents or network-level visibility would be required, given hardware and software constraints. This enhancement broadens the applicability of the system across industry verticals like healthcare, manufacturing, and smart infrastructure.

- Integration with AI/ML for Predictive Threat Detection

To further reduce manual analysis and improve detection accuracy, machine learning models could be integrated to identify emerging threat patterns. Unsupervised learning techniques (e.g., clustering, anomaly detection) may be employed to recognize deviations in system behavior that don't match existing rule sets.

- Blockchain for Event Integrity and Traceability

Ensuring the integrity and auditability of security events is critical in regulated industries. Introducing a blockchain-based ledger for storing alert data and playbook actions can enhance trust, transparency, and forensic reliability. Each event, detection rule match, and response action can be cryptographically recorded as a transaction, creating a tamper-evident chain of events. This ledger could be accessed by auditors or compliance officers to verify the authenticity of alerts and the appropriateness of response actions. This kind of system is valuable for incident response or compliance reporting, as immutable logs are key for legal and operational accountability.

Acknowledgment

At this significant juncture of my academic journey, I take the opportunity to express my gratitude to those who have supported and guided me throughout the completion of this dissertation.

I am deeply thankful to Dr. Kapil Kumar, Head of Department and my project guide, for placing his trust in me by allowing this work to take shape under his guidance. His constant support and for providing a platform where I could shape my ideas into meaningful outcomes have been invaluable.

I owe special thanks to my co-guide, Mr. Aditya More, whose consistent motivation and patient mentorship became the driving force behind this project. His clarity of thought and readiness to guide me at every stage helped transform initial ideas into structured execution.

I would also like to place on record my gratitude to Infopercept, where I interned as a SOC Analyst. The exposure and experience I gained there helped me align practical knowledge with academic concepts, and was a turning point that inspired me to choose this topic.

I wish to acknowledge the silent strength behind this journey, my mother, Hetal Thakker. Her belief in my potential and encouragement to pursue cybersecurity as a career laid the foundation for all that I have achieved today. Her support has played an irreplaceable role in helping me grow and complete this work with purpose and confidence.

References

[1] S. Waelchli and Y. Walter, "Reducing the risk of social engineering attacks using SOAR measures in a real-world environment: A case study," *Computers & Security*, vol. 148, p. 104137, Sep. 2024.

[2] S.-H. Park *et al.*, "Performance evaluation of open-source endpoint detection and response combining Google Rapid Response and Osquery for threat detection," *IEEE Access*, vol. 10, pp. 20259–20269, Feb. 2022.

[3] C. Erdivan, *Process, Technology and Human Aspects of a Security Operations Center*, METU/II-TR-2024, Technical Report, Informatics Institute, Middle East Technical University, Jan. 2024.

[4] H. Javid, "Practical applications of Wazuh in on-premises environments," Bachelor's thesis, School of Engineering, JAMK Univ. of Appl. Sci., Jyväskylä, Finland, 2024.

[5] Jumiaty and B. Soewito, "SIEM and threat intelligence: Protecting applications with Wazuh and TheHive," *Int. J. Adv. Comput. Sci. Appl. (IJACSA)*, vol. 15, no. 9, pp. 239–251, Sep. 2024.

[6] C. Bassey, E. T. Chinda, and S. Idowu, "Building a scalable security operations center: A focus on open-source tools," *J. Eng. Res. Rep.*, vol. 26, no. 7, pp. 196–209, 2024.
[7] O. Abiade, "Cybersecurity automation: Streamlining incident response," *EasyChair Preprints*, no. 14368, Aug. 2024.
[8] S. Kasturi, X. Li, P. Li, and J. Pickard, "Predicting attack paths from application security vulnerabilities using a multi-layer perceptron," *Am. J. Softw. Eng. Appl.*, vol. 12, no. 1, pp. 23–35, May 2024.
[9] A. H. Washo, "An interdisciplinary view of social engineering: A call to action for research," *Comput. Hum. Behav. Rep.*, vol. 4, p. 100126, 2021.
[10] S. Stanković, S. Gajin, and R. Petrović, "A review of Wazuh tool capabilities for detecting attacks based on log analysis," in *IX Int. Conf. IcETRAN*, Jun. 2022, pp. 6–9.
[11] Wazuh, "Installing the Wazuh central components." [Online]. Available: https://documentation.wazuh.com/current/installation-guide/index.html. [Accessed: Feb. 2025].
[12] M. Sheeraz *et al.*, "Effective security monitoring using efficient SIEM architecture," *Hum.-Centric Comput. Inf. Sci.*, vol. 13, p. 17, 2023.
[13] OWASP, "OWASP Top 10," 2021. [Online]. Available: https://owasp.org/www-project-desktop-app-security-top-10/. [Accessed: Jan. 2025].
[14] Reversing Labs, "How to evaluate threat intelligence feeds," *Reversing Labs*, [Online]. Available: https://www.reversinglabs.com/resources/how-to-evaluate-threat-intelligence-feeds
[15] NIST, "Framework for improving critical infrastructure cybersecurity." [Online]. Available: https://www.nist.gov/cyberframework. [Accessed: Feb. 2025].
[16] MITRE ATT&CK. [Online]. Available: https://attack.mitre.org/. [Accessed: Jan. 2025].
[17] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assessing MITRE ATT&CK risk using a cybersecurity culture framework," *Sensors*, vol. 21, no. 9, 2021.
[18] D. S. Mary, L. J. S. Dhas, A. R. Deepa, M. A. Chaurasia, and C. J. J. Sheela, "Network intrusion detection: An optimized deep learning approach using big data analytics," *Expert Syst. Appl.*, vol. 243, 2024.
[19] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures," *Sensors*, vol. 21, no. 14, p. 4759, Jul. 2021.
[20] S. A. Utari, V. Ardia, Jamiati, and D. Fitria, "How an organization should implement risk communication in response to cyber attack in Indonesia," *J. Educ.*, vol. 5, no. 4, pp. 14314–14328, 2023.