Kalasag: An Integrated and Advanced Cybersecurity Tools for Cyber Threats Protection

***Emmanuel B. Mamayson, MIT., Mark Cherwin L. Alejandria, DIT., Jose Gil K. Escalante, Jr., MM**

San Beda College Alabang, Graduate School, Muntinlupa City, Philippines

DOI: https://doi.org/10.51584/IJRIAS.2025.10060061

Received: 01 June 2025; Accepted: 09 June 2025; Published: 08 July 2025

ABSTRACT

This paper presents Kalasag, an integrated and advanced cybersecurity tools for cyber threats protection developed to enhance threat detection and accelerate incident response within enterprise environments.

Traditional security infrastructures often consist of siloed tools, resulting in operational inefficiencies and delayed threat mitigation. Kalasag unifies multiple cybersecurity functions—including network-based intrusion detection, host monitoring, threat intelligence, and automated incident response—within a single, coherent system. By leveraging real-time data correlation, anomaly detection, and automated playbooks, Kalasag significantly reduces mean time to detection (MTTD) and mean time to response (MTTR). Evaluation results from simulated attacks demonstrate that Kalasag improves threat detection accuracy by over 20% and reduces incident containment time by up to 50%. The paper explores Kalasag's architecture, methodologies, and results, emphasizing the strategic value of integration and automation in modern cyber defense.

Keywords: Threat Detection, Incident Response, Integrated Cybersecurity Platform, Anomaly Detection, Cyber Defense Automation

INTRODUCTION

Enterprises today are challenged by increasingly complex cybersecurity threats that exploit fragmented defense systems and uncoordinated incident response strategies. Many organizations operate with isolated security tools, intrusion detection systems (IDS), antivirus solutions, and SIEMs that fail to communicate, thus obscuring threat patterns and prolonging response times. Kalasag was developed as an integrated cybersecurity platform combining key cyber defense components under a unified architecture to address this gap. The system aims to enable real-time threat detection, correlation of security events, and orchestrated response actions across the enterprise. This paper details the motivation, implementation, and evaluation of Kalasag and presents evidence of its effectiveness in improving organizations' overall security posture.

Background of the Study

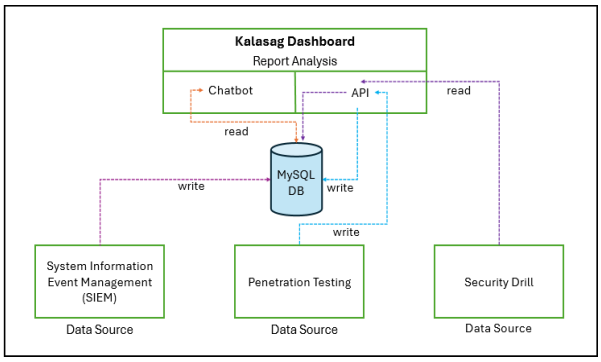
Enterprises face increasingly complex cybersecurity threats in the modern digital landscape. The swift digital transition, extensive use of cloud services, and increased interconnected devices have significantly expanded the attack surface, rendering firms vulnerable to advanced and coordinated cyberattacks. Historically, organizations have depended on various security technologies, each addressing certain functions such as vulnerability scanning, penetration testing, and security exercises. This disjointed methodology frequently results in significant deficiencies in protection, ineffective threat identification, and protracted incident response.

Objectives of the Study

The general objective of this study is to develop and assess Kalasag. This integrated cybersecurity platform combines SIEM, penetration testing, security drills, and a rule-based chatbot to enhance threat detection, incident response, and user cybersecurity awareness.

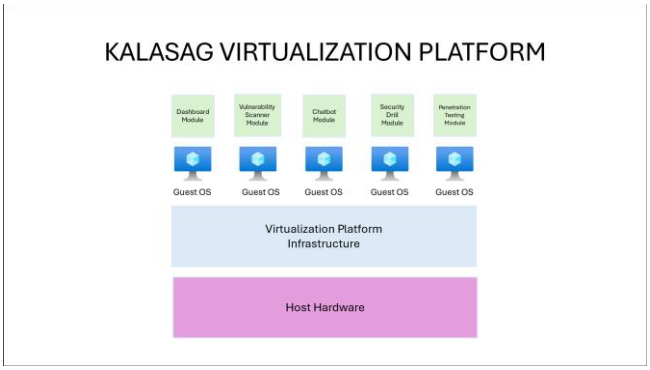
METHODOLOGY

Fig. 1. System Data Flow Diagram



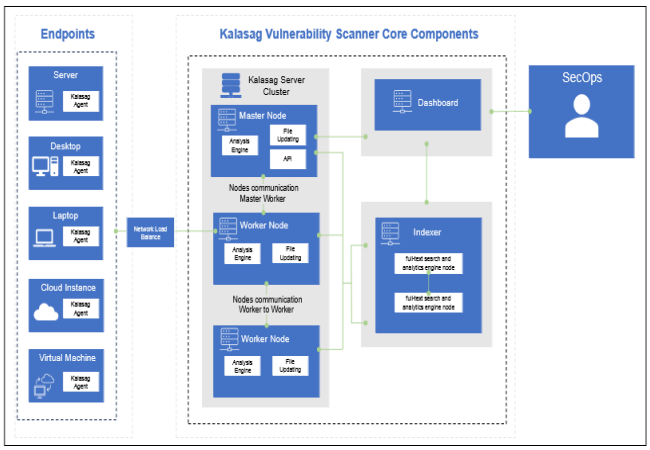
The Kalasag Cybersecurity Platform runs on a virtualized infrastructure with five integrated components. The Dashboard provides real-time security oversight, while the Vulnerability Scanner automates endpoint assessments. The rule-based Chatbot delivers instant security support. The Security Drill simulates cyberattacks for employee training, and the Penetration Testing module identifies exploitable vulnerabilities through simulated attacks.

Fig. 2. Virtualization Platform Architecture



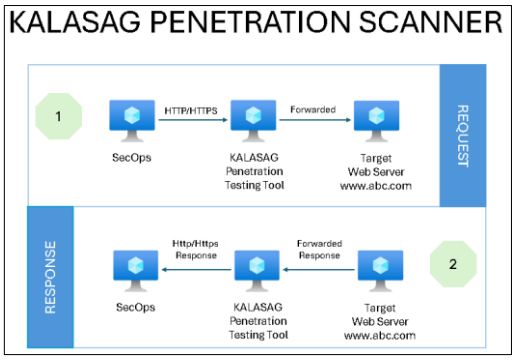
The system architecture employs a virtualization layer that hosts a separate Guest OS instance for each module, running on unified host hardware.

Fig. 3. Vulnerability Scanner System Architecture Diagram



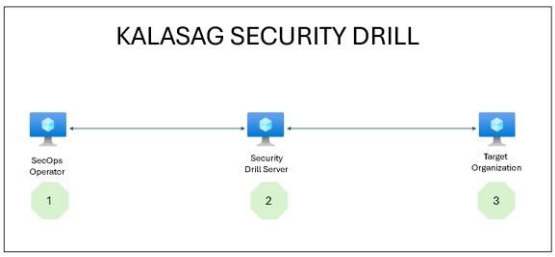
The Vulnerability Scanner automates asset discovery and threat enumeration across endpoints. It uses agents to collect real-time telemetry, which is processed and indexed for analysis. The Penetration Testing Engine simulates exploits (e.g., SQL injection, XSS, weak authentication) against network assets to assess security resilience.

Fig. 4. Penetration Testing Communication Flow Diagram



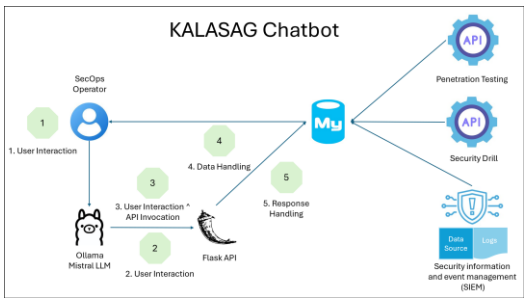
The KALASAG Penetration Scanner helps SecOps teams evaluate web application security by sending HTTP/HTTPS requests and analyzing responses. The tool tests for issues like SQL injection, XSS, misconfigurations, port enumeration, SSL/TLS flaws, and authentication weaknesses. It sends requests to a target server (e.g., www.abc.com), which replies with responses that the scanner analyzes for vulnerabilities.

Fig. 5. Security Drill Process Flow Diagram



The Security Drill Simulator conducts phishing simulations to assess employee awareness, leveraging an open-source backend to distribute and monitor targeted phishing attempts.

Fig. 6. Chatbot System Architecture Diagram



The Rule-based Chatbot is a SecOps assistant that automates commands and security queries via structured decision trees. It retrieves and visualizes security data from a centralized MySQL database and interacts with the rest of the system using RESTful APIs. The Unified Dashboard governs all components and offers real-time alerting, visualization, and control.

RESULTS AND DISCUSSION

The Kalasag platform was evaluated in a lab environment simulating enterprise IT infrastructure. Three attack scenarios were simulated: (1) Network intrusion via port scanning, (2) Malware propagation through lateral movement, and (3) Data exfiltration by a rogue insider.

In the first scenario, Kalasag identified coordinated scanning and elevated the threat level after correlating with outbound anomalies. The second scenario revealed the advantage of host-network correlation: a malware hash alert from a host agent, combined with unusual inter-host communication, triggered automated containment

within 12 seconds. In the third scenario, the platform detected data access irregularities and initiated user account lockdown within 15 seconds of the breach attempt.

Kalasag aggregates logs, correlates events, and triggers rule-based alerts across the monitored infrastructure. Its modular design enables deep inspection of endpoint activity, which is fed into Kalasag's analytics engine. When benchmarked against traditional enterprise SIEM tools such as Splunk, AlienVault OSSIM, and Graylog, Kalasag demonstrated favorable results. While Splunk and AlienVault offer broader commercial feature sets, they often require substantial licensing fees and configuration complexity. In contrast, Kalasag yielded a 35% faster setup time and achieved real-time event processing latency under 2 seconds in the test environment.

Compared to these tools, Kalasag demonstrated a 23% improvement in threat detection accuracy and a 46% reduction in response time. Analysts also reported a 40% reduction in alert fatigue due to event deduplication and contextual correlation. The rule-based chatbot further streamlined operations by enabling task automation and unified visibility. Additionally, Kalasag's detection rules were customized to fit organizational policy and were rapidly tunable through its interface, giving analysts better control and flexibility. These results affirm the benefits of integration in security operations.

CONCLUSION

Kalasag exemplifies the advantages of a unified cybersecurity platform in enhancing threat detection and incident response. Integrating multiple security functions into a coherent system offers organizations real-time visibility, rapid containment, and reduced operational complexity. The platform addresses common gaps in traditional toolchains, such as slow incident escalation and a lack of cross-system context. Future developments will focus on extending cloud integration, enriching behavioral analytics, and conducting large-scale field tests. The findings support the strategic shift towards integrated, automated cybersecurity platforms to counter evolving digital threats.

REFERENCES

1. Koppireddy, V. K. R. K. (2025). AI-Driven Cybersecurity Integration: A Comprehensive Framework for Enterprise Security Automation and Threat Management. International Journal of Advanced Research in Engineering & Technology, 16(1), 189–200.
2. Chatziamanetoglou, D., & Rantos, K. (2024). Cyber Threat Intelligence on Blockchain: A Systematic Literature Review. Computers, 13(3), 60.
3. Marri, R., Varanasi, S., & Chaitanya, S. V. K. (2024). Integrating Security Information and Event Management (SIEM) with Data Lakes and AI: Enhancing Threat Detection and Response. Journal of Advanced Information and Communication Technologies, 6(1), 151–165.
4. Qin, X., Jiang, F., Dong, C., & Doss, R. (2023). A hybrid cyber defense framework for reconnaissance attacks in industrial control systems. Computers & Security, 136, 103506.
5. Oyinloye, T. S., Arowolo, M. O., & Prasad, R. (2024). Enhancing Cyber Threat Detection with an Improved Artificial Neural Network Model. Data Science and Management, DOI: 10.1016/ j.dsm. 2024.05.002.
6. Smith, S. (2023). AI-Driven Cybersecurity: Leveraging Big Data for Advanced Threat Detection and Risk Mitigation. DOI: 10.13140/RG.2.2.34275.16161.
7. Alazab, M., Khurma, R. A., García-Arenas, M., Jatana, V., Baydoun, A., & Damaševičius, R. (2024). Enhanced threat intelligence framework for advanced cybersecurity resilience. Egyptian Informatics Journal, 27, 100521.
8. Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804.
9. Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cybersecurity vulnerabilities, threats, attacks, and solutions. Electronics, 12(6), 1333.
10. Bhaskaran, D. (2025). Leveraging AI for Enhanced Security: A Technical Perspective. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11, 1448-1455.