Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Issue 1, Januari 2026
DOI : https://doi.org/10.33395/sinkron.v10i1.15616
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Hybrid Multilayer Architecture Integrating Suricata, Wazuh, and Cyber Threat Intelligence for Drive-by-Download Malvertising Detection

Aurell Zulfa Angger Adrian[1)*], Rama Aria Megantara[2)], Farrikh Al Zami[3)]
[1,2)]Teknik Informatika, Fakultas ilmu Komputer, Universitas Dian Nuswantoro
[3]Sistem Informasi, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
[1)]nairdareggna@gmail.com, [2)]aria@dsn.dinus.ac.id, [3)]alzami@dsn.dinus.ac.id

Submitted :Nov 22, 2025 | **Accepted** : Dec 9, 2025 | **Published** : Jan 02, 2026

Abstract: Malvertising has emerged as a serious cybersecurity threat, leveraging legitimate advertising networks to deliver malware through drive-by-download techniques without requiring user interaction. Existing standalone network- or host-based detection solutions provide limited protection because they lack integrated visibility and contextual validation across detection layers. However, no existing research has specifically evaluated the integration of Suricata, Wazuh, and VirusTotal for endpoint-focused malvertising detection, creating a critical gap in multi-layer defense strategies. This study proposes a hybrid multilayer architecture combining Suricata as a Network Intrusion Detection System, Wazuh as a Host-based Intrusion Detection and Prevention System, and VirusTotal as an external Cyber Threat Intelligence source to provide correlated threat detection and automated mitigation. The system was evaluated in a controlled virtual laboratory consisting of attacker, victim, and SIEM environments replicating real malvertising scenarios. The results show that the proposed architecture successfully detected malicious payloads and completed an end-to-end detection-to-mitigation cycle in approximately 5-7 seconds while maintaining zero false positives under non-malicious conditions. This research contributes a practical and reproducible architecture for endpoint-based malvertising detection, demonstrating effective multi-layer correlation and rapid autonomous response. The limitation of this study lies in its reliance on signature-based detection and external API communication, which may reduce effectiveness against zero-day threats or offline deployments.

Keywords: Suricata; Wazuh; Cyber Threat Intelligence; Drive-by-Download; Malvertising Detection

INTRODUCTION

The rapid growth of online advertising has transformed the digital marketing ecosystem into a multi-billion-dollar industry. However, this rapid expansion has also created opportunities for threat actors to exploit advertising supply chains and deliver malware through malicious advertising, known as malvertising (Bensaoud et al., 2024). Recent industry reports indicate that malvertising continues to be leveraged as a drive-by delivery vector, with threat actors embedding malicious scripts into seemingly legitimate advertisement placements, enabling infection without user interaction

Malvertising poses a unique risk because it does not require user interaction. Simply visiting a compromised website can automatically trigger a drive-by-download payload, resulting in ransomware infections, credential theft, or remote access compromise (Rehman et al., 2025). Threat reports also highlight that browser-based malware distribution remains among the most frequently observed vectors in modern cyberattacks, reflecting its persistence and operational effectiveness for adversaries across global digital environments.

Most attacks occur at the endpoint layer, where modern browsers serve as the primary gateway between users and the internet (Andreica et al., 2024). Traditional defenses such as antivirus and firewalls struggle with obfuscated payloads and encrypted channels, making early detection difficult (Waleed et al., 2022).

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Issue 1, Januari 2026
DOI : https://doi.org/10.33395/sinkron.v10i1.15616
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Prior studies have proposed improving visibility through SIEM-driven event correlation and rule-based IDS/IPS mechanisms (Abdulganiyu et al., 2023; Damanik & Anggraeni, 2024). Meanwhile, SIEM platforms such as Wazuh offer advantages in host-level monitoring, automated response, and log analysis (Hidayat et al., 2025). However, SIEM still produces excessive alerts and lacks global context for threat validation, resulting in noise and false positives (Singh & Agarwal, 2025).

Integrating SIEM with Cyber Threat Intelligence (CTI) services has shown promise, particularly in hash-based malware verification (Rizki Nurul et al., 2025). However, no existing research has specifically examined the integration of Suricata, Wazuh, and VirusTotal for endpoint-focused malvertising detection, leaving a significant gap in multi-layered defenses against drive-by-download attacks.

To address this gap, this study proposes a hybrid multi-layer architecture that combines Suricata for network-layer anomaly detection, Wazuh for host-level file monitoring and automated response, and VirusTotal for external threat reputation validation.

This study contributes by:
(1) Designing and implementing a hybrid Suricata–Wazuh–VirusTotal architecture tailored for endpoint malvertising detection;
(2) Demonstrating near real-time automated mitigation within controlled drive-by-download scenarios;
(3) Providing a practical, lightweight, and reproducible laboratory framework for further research and educational cybersecurity environments.

The objective of this work is to evaluate how multi-layer correlation enhances detection accuracy, reduces alert noise, and accelerates mitigation to counter modern web-based threats effectively.

LITERATURE REVIEW

The growing interest in hybrid intrusion detection systems (IDS) reflects the increasing complexity of modern cyber threats, where single-layer security controls are no longer sufficient to detect and mitigate attacks. Various studies have explored the combination of network-based IDS, host-based monitoring, and threat intelligence to enhance visibility, reduce alert noise, and provide more contextualized decisions during incident response. Table 1 presents a consolidated summary of key related works focusing on hybrid IDS architectures, SIEM-based monitoring, and CTI-enrichment mechanisms. The comparison highlights different technical approaches, their contributions, and the remaining limitations that motivate further research.

Table 1. Summary of Related Studies on Hybrid Intrusion Detection Architectures

Authors & Year	Focus Area	Method / System Used	Main Contribution	Limitation / Note
(Rehman et al., 2025)	Cyber-physical systems intrusion detection	Centralized IDS framework with event correlation	Demonstrated improved alert correlation to reduce redundancy and enhance detection efficiency	Not specifically designed for malvertising driven drive-by-download scenarios
(Waleed et al., 2022)	Comparative IDS performance	Snort, Suricata, and Zeek evaluation	Identified Suricata as superior in throughput and rule flexibility for real-time monitoring	Focused only on network layer performance without endpoint correlation
(Damanik & Anggraeni, 2024)	Hybrid IDS in heterogeneous	Suricata Wazuh integration with automated response	Implemented automated threat containment and anomaly detection in real-time	Did not incorporate external CTI for threat validation
(Hidayat et al., 2025)	SIEM optimization through CTI	Wazuh MISP integration	Improved IoC correlation and reduced false positives via threat intelligence enrichment	Focused on generalized malware, not malvertising attacks
(Andreica et al., 2024)	Real-time hybrid IDS implementation	Suricata Wazuh SIEM	Validated feasibility of hybrid IDS for real-time monitoring and alert correlation	Limited to DoS and generic intrusion scenarios

Hybrid IDS Architecture and Correlation

Hybrid IDS architectures combining NIDS and HIDS are crucial for enhanced security visibility. (Rehman et al., 2025) proposed a detection framework for cyber-physical systems that highlighted the importance of

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

centralized event correlation in reducing alert redundancy. This correlation mechanism is essential for effectively distinguishing anomalies from actual threats.

In terms of component performance, (Waleed et al., 2022) conducted a comparative study of open-source IDS platforms and demonstrated that Suricata achieved superior throughput and rule flexibility compared to Snort and Zeek, making it suitable for real-time network inspection. However, recent research indicates that modern web-based malware increasingly uses multi-stage redirection and payload obfuscation, challenging signature-only detection approaches (Guterres & Ashari, 2020). Additionally, (Bank et al., 2024) emphasized that modern digital advertising supply chains expand the attack surface through third-party ad networks, enabling silent compromise without direct user interaction reinforcing the need for endpoint-centric protection.
(Andreica et al., 2024) confirmed the feasibility of combining Suricata and Wazuh for real-time alert correlation and DoS detection.

In the Indonesian context, (Damanik & Anggraeni, 2024) implemented a similar hybrid system using Suricata and Wazuh to automate threat containment and improve network anomaly detection. (Zaini et al., 2025) also explored endpoint-focused intrusion scenarios but without SIEM-level correlation or external CTI validation, leaving gaps in contextual decision-making. Overall, combining rule-based detection with contextual analysis enhances detection accuracy and reduces false positives.

Integration with Cyber Threat Intelligence (CTI)

To address the high false-positive rates often associated with SIEM systems, recent research has focused on integrating SIEM with external Cyber Threat Intelligence (CTI) platforms. This integration enriches detection with real-time global indicators, thereby strengthening threat confidence.

(Hidayat et al., 2025) enhanced Wazuh SIEM performance through CTI enrichment using MISP, successfully improving IoC correlation. Similarly, (Rizki Nurul et al., 2025) integrated Wazuh with VirusTotal and ModSecurity to enable automated malicious file validation and response. This approach proved effective in endpoint-based systems, as confirmed by (Sholeh & Monalisa, 2024) in ransomware detection scenarios using Wazuh and VirusTotal. Complementing these approaches, (Mamatha et al., 2025) introduced hybrid deep-learning IDS models that show improved adaptability but require high computational resources and large datasets, limiting their applicability for lightweight endpoint deployments.
Similarly, (Anupama & Prasad, 2023) explored signature-assisted machine learning scoring, demonstrating potential improvements in intrusion classification, but highlighted stability challenges for real-time threshold-based decision-making.

Research Gap and Differentiation

While existing studies confirm the benefits of hybrid IDS architectures and CTI integration, most research has predominantly focused on generalized malware detection or server-side intrusion prevention. Limited attention has been given to malvertising-driven drive-by-download attacks that exploit trusted advertising channels to silently compromise endpoint systems.

Specifically, Suricata–Wazuh hybrid solutions presented by (Damanik & Anggraeni, 2024) and (Andreica et al., 2024) did not incorporate external CTI for critical validation of threat artifacts. Conversely, CTI-integrated approaches such as those by (Rizki Nurul et al., 2025) focused on web server intrusion and file verification, lacking a complete detection pipeline for the endpoint malvertising attack chain.

METHOD

Research Design

This study employs an Experimental Research Design using Scenario-Based Analysis. The primary goal is to evaluate the operational effectiveness and response consistency of the proposed hybrid architecture against *malvertising drive-by-download* attacks. The system's performance was tested under three controlled scenarios to ensure robust evaluation:

1. Malicious Drive-by-Download Scenario**:** Simulating an attack that successfully delivers a malicious payload (using the EICAR test file to guarantee consistent detection).
2. Benign Malvertising Scenario**:** Simulating a malicious redirection or page without an actual payload delivery (False Positive Check 1).
3. Control Condition**:** Simulating normal web browsing activity as a baseline (False Positive Check 2).

The entire experimental setup was conducted within an isolated virtual laboratory to ensure repeatability and control over external interference.

Testbed Spesifications

The testing environment was implemented within an isolated virtual laboratory consisting of three interconnected Virtual Machines (VMs). The systems communicated over an isolated virtual network (192.168.56.0/24). The detailed specifications of the VMs are presented in Table 2.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Issue 1, Januari 2026
DOI : https://doi.org/10.33395/sinkron.v10i1.15616
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Table 2. Virtual Laboratory Testbed Specifications

Component	Operating System	Processor	Memory	Storage	IP Address	Role	Key Components
Wazuh Server	Ubuntu Server 22.04	2vCPU	4096MB	92.16GB	192.168.56.10	Central SIEM, Log Aggregation, CTI Gateway	Wazuh Manager, Suricata NIDS
Victim Host	Windows 10 Enterprise	1vCPU	2048MB	50GB	192.168.56.40	Endpoint under attack	Wazuh Agent, Web Browser, Active Response script
Attacker Server	Ubuntu Server 22.04	2vCPU	4096MB	52.33GB	192.168.56.20	Malicious advertising source	Simulates malicious ad delivery and payload serving

System Implementation and Configuration

The implementation focused on configuring custom rulesets and correlation mechanisms to achieve the multi-layer defense flow. The system design ensures that the detection process is sequential across the network, host, and CTI layers, as illustrated in Figure 5 Workflow of Hybrid Malvertising Detection and Mitigation Process.

1. Network Layer (Suricata NIDS)**:** Suricata was deployed on the Wazuh Server to inspect network traffic. Custom rules were configured to detect suspicious outbound connections from the Victim Host (192.168.56.40) to the Attacker Server (192.168.56.20), generating an alert (e.g., SID 1000001) upon detection.
2. Host Layer (Wazuh HIDS/HIPS)**:** The Wazuh Agent on the Victim Host utilized the File Integrity Monitoring (FIM) module. FIM was specifically configured to monitor the Downloads directory. Upon detecting the creation of a new file (the malicious payload), the Wazuh Agent calculated its SHA-256 hash.
3. CTI and Mitigation (VirusTotal & Active Response)**:** The Wazuh Manager was integrated with the VirusTotal API. The hash calculated by the FIM module was sent for external validation. If VirusTotal returned a malicious verdict (triggering a specific rule ID), Wazuh automatically executed the Active Response script (remove-threat) to delete the file from the Victim Host.

The system design ensures that the detection process is sequential across the network, host, and CTI layers, as visually detailed in Figure 1.

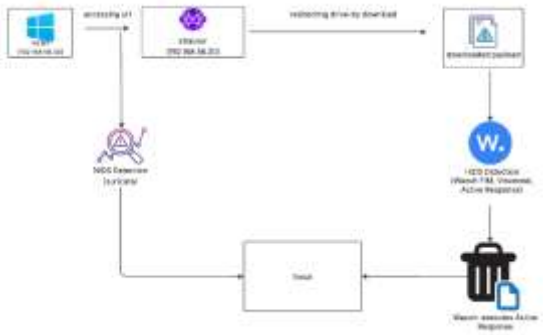

Fig. 1 Workflow of Hybrid Malvertising Detection and Mitigation Process

Metrics & Evaluation Criteria

To formally evaluate the effectiveness of the proposed detection architecture, this study adopts a set of performance metrics designed to measure both the functional behavior and operational efficiency of the multilayer detection pipeline. These metrics are selected to assess how each subsystem contributes to overall threat

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Issue 1, Januari 2026
DOI : https://doi.org/10.33395/sinkron.v10i1.15616
e-ISSN : 2541-2019
p-ISSN : 2541-044X

identification, validation, and automated mitigation. The evaluation criteria also consider the impact of layered correlation on accuracy and real-time responsiveness, which are critical in endpoint-focused drive-by-download scenarios. The primary metrics used in this study are detailed in Table 3 below.

Table 3. Evaluation Metrics Used in the Proposed Architecture

Metric	Definition and Evaluation Goal
Detection Accuracy	Measures the system's ability to correctly classify malicious events (True Positive) and non-malicious events (True Negative) across all scenarios
False Positive Rate	Measures the rate of erroneous alerts generated in non-malicious scenarios (Scenarios 2 and 3), aiming for a value of zero
Response Time	Measures the end-to-end time elapsed from the initial NIDS detection (Suricata alert) to the final Active Response execution (file deletion)
Multi-Layer Integration	Evaluates the seamless and proper correlation of alerts across the four key stages: Suricata, Wazuh FIM, VirusTotal CTI, and Active Response

Evaluation Procedure

The evaluation of the system was conducted through repeated executions of each scenario with five independent trials to minimize result variability. Detection timestamps were captured from three log sources: Suricata alert logs, Wazuh FIM event logs, and VirusTotal validation events. The response time was calculated by measuring the delta between the Suricata detection timestamp and the Active Response execution timestamp recorded within the Wazuh Manager logs. Each trial was executed under identical system conditions to ensure measurement consistency.

Validity and Reliability Assurance

To ensure internal validity, no additional background processes or network traffic were introduced during the experiment aside from those required for the simulated attack flows. The use of the standardized EICAR payload ensured repeatability of malicious events without risk of uncontrolled variables. Log records and timestamps were validated manually and cross-checked between Suricata and Wazuh Manager to prevent measurement deviation. Since VirusTotal reputation checks depend on external API services, the same hash was used repeatedly to eliminate variability caused by classification delay or internet routing factors.

RESULT

Detection Time Analysis

The proposed hybrid architecture demonstrated consistent detection-to-mitigation performance across repeated executions of the payload-based drive-by-download scenario. As shown in Figure 3, the end-to-end multilayer workflow beginning with Suricata's initial network anomaly alert, followed by Wazuh's File Integrity Monitoring (FIM) event, VirusTotal reputation validation, and concluding with automated file quarantine and removal was completed within approximately 5-7 seconds.

These results indicate that the introduction of multiple validation layers did not create disruptive latency, nor did it prevent the system from acting in near real time. Instead, the correlation of network, host, and CTI signals contributed to more confident decision-making without compromising responsiveness. The consistency of performance across repeated trials suggests that the proposed architecture remains operationally feasible for endpoint protection where threat response time is critical, particularly in attack patterns where payload execution may occur rapidly after download.

Furthermore, the relatively small detection gap between Suricata's initial alert and Wazuh's confirmation event reinforces the benefit of a synchronized pipeline rather than independent standalone components. This finding supports the viability of multilayer approaches for modern web-based threats that require rapid classification and immediate mitigation.

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Issue 1, Januari 2026
DOI : https://doi.org/10.33395/sinkron.v10i1.15616
e-ISSN : 2541-2019
p-ISSN : 2541-044X

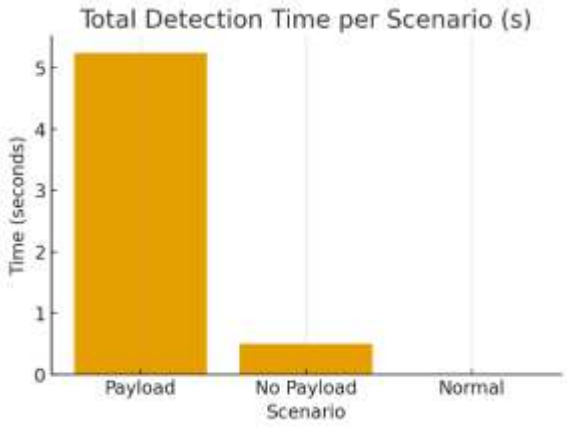

Fig. 2 Detection Time Comparison

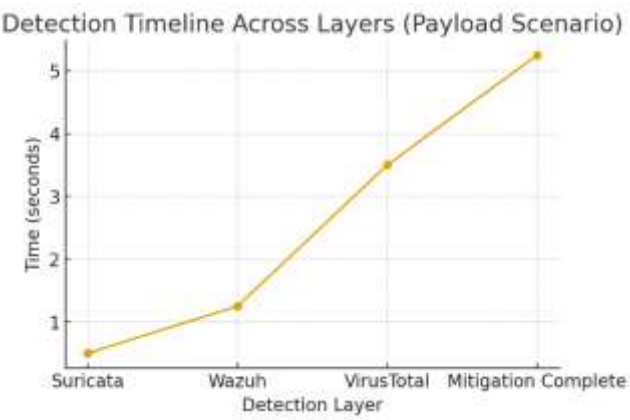

Fig. 3 Multi-Layer Detection Timeline

Layered Detection Behavior

The results demonstrate that each subsystem within the proposed architecture contributes a distinct, complementary function along the detection pipeline. Suricata consistently acted as the earliest alert trigger, identifying outbound connections to suspicious domains at the network layer before any payload was executed. Wazuh's File Integrity Monitoring (FIM) served as the second validation point by detecting the creation or modification of executable files on the host, providing concrete evidence of artifact presence beyond network anomalies. VirusTotal, functioning as the external Cyber Threat Intelligence (CTI) component, supplied global reputation verification to determine whether the observed file matched known malicious signatures prior to the execution of automated remediation.

This layered orchestration reflects a deliberate escalation model in which each subsystem corroborates the prior alert rather than acting independently. Such sequential validation supports more confident classification decisions and significantly reduces the likelihood of unnecessary or premature mitigation actions an acknowledged challenge in signature-only or SIEM-only detection strategies.

The complementary roles of each subsystem are summarized in Table 4, which illustrates the differentiated focus and contribution of the NIDS, HIDS/FIM, and CTI layers.

Table 4. Layered Detection Contributions of NIDS, HIDS, and CTI Components

Layer	Detection Focus	Result	Notes
Suricata NIDS	Outbound anomalous traffic	Detected	Earliest trigger
Wazuh FIM	Host file changes	Detected	Validates artifacts
VirusTotal CTI	Hash reputation	Verified	Confirms global threat

The integration of detection, validation, and response provides a more reliable decision-making foundation, minimizing false positives and reducing the operational burden commonly associated with SIEM platforms that generate single-layer, context-limited alerts. The structured escalation ensures that mitigation occurs only when corroborated across multiple indicators, thereby improving both system reliability and analyst confidence.

Performance Summary

To provide a consolidated overview of system performance across the evaluated scenarios, the key outcomes are summarized in Table 5. The results indicate that the multilayer architecture effectively balances detection speed, accuracy, and automated mitigation while maintaining low operational overhead. The consistent response time and the absence of false positives reinforce that the integration of network-level monitoring, host-based verification, and CTI-driven validation forms a reliable and efficient defensive pipeline for endpoint-focused threat prevention.

Table 5. Summary of Detection and Performance Outcomes

Metric	Result
Total Detection Time	5-7 seconds
False Positives	0
Automation Execution	100%
Detection Consistency	Stable
CTI Verification Reliability	100%

*name of corresponding author

Sinkron : Jurnal dan Penelitian Teknik Informatika
Volume 10, Issue 1, Januari 2026
DOI : https://doi.org/10.33395/sinkron.v10i1.15616
e-ISSN : 2541-2019
p-ISSN : 2541-044X

DISCUSSIONS

Detection Accuracy

The findings indicate that the proposed hybrid Suricata–Wazuh–VirusTotal architecture achieved consistent and reliable detection accuracy in identifying payload-based drive-by-download attacks. By correlating three independent indicators network anomaly, filesystem modification, and CTI confirmation the system forms a multi-perspective validation process that minimizes misclassification. This approach aligns with existing literature that highlights the importance of context-rich analysis in intrusion detection. However, unlike previous studies that rely solely on NIDS signatures or SIEM log patterns, this architecture demonstrates that accuracy improves significantly when endpoint artifacts are used as part of the evaluation sequence rather than as isolated events.

False Positive Avoidance

A critical advantage of the system is its ability to suppress unnecessary alerts. No false positives were generated in both benign malvertising and normal browsing scenarios, demonstrating a refined response escalation logic. Traditional SIEM environments frequently suffer from alert fatigue due to noisy rule sets and lack of contextual indicators. In contrast, this sequential validation ensures that action is only executed once evidence has been observed across all three layers. This contributes to operational efficiency and reduces the cognitive burden on security personnel, particularly in environments where security analysts are limited.

Performance & Latency

The system maintained an end-to-end detection and mitigation time of approximately 5-7 seconds, which is within acceptable thresholds for endpoint security responses. While additional CTI verification introduces measurable delay, the latency remains justified by improved threat confidence. Resource consumption within the virtual testbed showed no significant degradation, indicating that the architecture is viable for lightweight deployments. Nevertheless, latency tolerance may vary across industries, and organizations engaged in high-frequency trading, industrial control systems, or low-latency environments may require further optimization or localized CTI caching solutions.

Limitations

Several limitations should be considered when interpreting these results.
(1) The system relies on signature-based rules, making zero-day or behaviorally disguised payloads difficult to detect.
(2) External CTI verification introduces dependency on internet connectivity, API quotas, and cloud privacy policies.
(3) Performance has not been evaluated under enterprise-scale workloads, where alert volume, concurrent requests, and throughput could significantly alter behavior.
These limitations do not invalidate the approach but indicate that it currently serves best as a prototype for targeted endpoint protection rather than as a fully hardened enterprise solution.

Practical Implications

The architecture presents different implications depending on organizational context.
For small and medium enterprises, the solution offers a cost-effective mechanism for layered security without requiring dedicated security engineers. For cloud-centric environments, integration policies must consider whether external CTI validation conforms to compliance standards such as GDPR or internal data governance. For large-scale deployments, the architecture offers automation potential, but scaling factors such as event batching, load balancing, and rule optimization must be addressed to prevent performance bottlenecks in high-traffic networks.

Future Research Directions

Future development may explore combining signature-based detection with behavior-based or machine-learning models to improve adaptability against previously unseen threats. Offline or federated CTI repositories may reduce dependence on third-party APIs while maintaining intelligence relevance. Additionally, evaluating this architecture on cloud-native platforms, containerized microservices, or edge computing scenarios would provide deeper insight into deployment considerations across diverse digital ecosystems.

CONCLUSION

This study proposed and evaluated a hybrid multi-layer architecture integrating Suricata, Wazuh, and VirusTotal to detect and mitigate drive-by-download malvertising attacks. The experimental results demonstrated that the combination of network anomaly detection, host-level artifact monitoring, and CTI-based verification enables accurate discrimination of malicious payloads while avoiding unnecessary escalation during benign or normal browsing scenarios. The end-to-end detection cycle was completed within approximately 5-7 seconds with zero false positives, validating the feasibility of this lightweight and reproducible approach for endpoint-focused protection.

*name of corresponding author

e-ISSN : 2541-2019
p-ISSN : 2541-044X

However, several opportunities for future research remain open. Potential enhancements include the integration of machine-learning-based threat scoring to improve adaptability against zero-day attacks, the development of adaptive rule optimization mechanisms that evolve based on real-time threat telemetry, and the execution of real-world deployment scenarios in cloud or large-scale enterprise environments to evaluate scalability, throughput, and operational resilience. Addressing these directions may further advance the robustness and applicability of hybrid detection models for modern cybersecurity ecosystems.

REFERENCES

Abdulganiyu, O. H., Ait Tchakoucht, T., & Saheed, Y. K. (2023). A systematic literature review for network intrusion detection system (IDS). *International Journal of Information Security*, *22*(5), 1125–1162. https://doi.org/10.1007/s10207-023-00682-2

Andreica, G.-R., Ivanciu, I.-A., Zinca, D., & Dobrota, V. (2024). Integration of the Suricata intrusion detection system and the Wazuh security information and event management for real-time denial-of-service and data tampering detection and alerting. *ACTA TECHNICA NAPOCENSIS Electronics and Telecommunications, 64(2), 45–53.* Available at: https://users.utcuj.ro/~atn/papers/ATN_2_2024_1.pdf

Anupama, A., & Prasad, R. R. (2023). Hybrid Intrusion Detection System. In *Proceedings of the 2023 International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (IQ-CCHESS)*, (pp. 1–6). https://doi.org/10.1109/iQ-CCHESS56596.2023.10391328

Bank, M. R. I. B. C., Islam, M. R., & Rafique, R. (2024). Wazuh SIEM for Cyber Security and Threat Mitigation in Apparel Industries. *International Journal of Engineering Materials and Manufacture*, *9*(4), 136–144. https://doi.org/10.26776/ijemm.09.04.2020.02

Bensaoud, A., Kalita, J., & Bensaoud, M. (2024). A survey of malware detection using deep learning. *Machine Learning with Applications*, *16*, Article 100546. https://doi.org/10.1016/j.mlwa.2024.100546

Damanik, H. A., & Anggraeni, M. (2024). Sistem Deteksi Intrusi Hybrid dan Mitigasi Kerentanan Infrastruktur Jaringan Menggunakan Teknik Active Response (XDR) Wazuh dan Suricata. *Jurnal Pekommas*, *9*(2), 309–322. https://doi.org/10.56873/jpkm.v9i2.5829

Guterres, L. E. J., & Ashari, A. (2020). The Analysis of Web Server Security For Multiple Attacks in The Tic Timor IP Network. *IJCCS (Indonesian Journal of Computing and Cybernetics Systems)*, *14*(1), 103–112. https://doi.org/10.22146/ijccs.53265

Hidayat, M. R. T., Widiyasono, N., & Gunawan, R. (2025). Optimasi deteksi malware pada SIEM Wazuh melalui integrasi cyber threat intelligence dengan MISP dan DFIR-IRIS. *Jurnal Informatika Dan Teknik Elektro Terapan*, *13*(1). 1–10. https://doi.org/10.23960/jitet.v13i1.5686

Mamatha, P., Balaji, S., & Anuraghav, S. S. (2025). Development of Hybrid Intrusion Detection System Leveraging Ensemble Stacked Feature Selectors and Learning Classifiers to Mitigate the DoS Attacks. *International Journal of Computational Intelligence Systems*, *18*(1). 1–14. https://doi.org/10.1007/s44196-025-00750-6

Rehman, S. ur, Alhulayyil, H., Alzahrani, T., AlSagri, H., Khalid, M. U., & Gruhn, V. (2025). Intrusion detection system framework for cyber-physical systems. *Egyptian Informatics Journal*, *30*, 100600. https://doi.org/10.1016/j.eij.2024.100600

Rizki Nurul, F., Rudi, H., & Dede Syahrul, A. (2025). INTEGRASI WAZUH SIEM DENGAN MODSECURITY DAN VIRUS TOTAL MENGGUNAKAN NIST FRAMEWORK UNTUK MENDETEKSI SERANGAN WEBSITE. *JATI (Jurnal Mahasiswa Teknik Informatika)*, *9(4)*, 6578–6586. https://doi.org/10.36040/jati.v9i4.13804

Sholeh, M., & Monalisa, A. (2024). MEMBANGUN AGENT ENDPOINT DETECTION AND RESPONSE (EDR) MENGGUNAKAN WAZUH DAN VIRUSTOTAL SEBAGAI SISTEM DETEKSI SERANGAN RANSOMWARE LOCKBIT 3.0. *Infotech: Journal of Technology Information*, *10*(2), 279–288. https://doi.org/10.37365/jti.v10i2.320

Singh, N., & Agarwal, R. (2025). Hybrid net: enhanced DTL based intrusion detection system for electric vehicular network using hybrid architecture. *Peer-to-Peer Networking and Applications*, *19*(1), 1. https://doi.org/10.1007/s12083-025-02154-x

Waleed, A., Jamali, A. F., & Masood, A. (2022). Which open-source IDS? Snort, Suricata or Zeek. *Computer Networks*, *213*, 109116. https://doi.org/https://doi.org/10.1016/j.comnet.2022.109116

Zaini, M., Atthariq, A., & Anwar, A. (2025). Implementasi Intrusion Detection System Menggunakan Suricata Pada Jaringan Komputer. *Jurnal Teknologi Rekayasa Informasi Dan Komputer*, *8*(2), 30-39. https://doi.org/10.30811/jtrik.v8i2.7440

*name of corresponding author