AUTOMATION OF MALWARE ANALYSIS INTEGRATION BASED ON WAZUH SIEM AND GHIDRA IN ISOLATED VIRTUAL ENVIRONMENTS

Desyderius Minggu[1)], Abdie Rimbawan[2)], Asep Suryanta[3)]
Jl. Raya Anggrek No. 1 Junrejo, Batu, Indonesia[1) 2) 3)]
Jurusan Teknik Telekomunikasi, Politeknik Angkatan Darat[1) 2) 3)]
E - mail : desyderius07@gmail.com[1)] ,D4osint01@gmail.com[2)],
zenilybaz@gmail.com[3)]

AUTOMATION OF MALWARE ANALYSIS INTEGRATION BASED ON WAZUH SIEM AND GHIDRA IN ISOLATED VIRTUAL ENVIRONMENTS

Abstract: *As cyber threats grow more complex, automated solutions for malware detection are no longer optional but essential. The integration between Security Information and Event Management (SIEM) such as Wazuh and reverse engineering platform Ghidra offers great potential in enhancing cyber defense capabilities. Wazuh plays a role in real-time log-based threat monitoring, while Ghidra enables in-depth analysis of binary code and malware. This research aims to develop an Automated Threat Intelligence system by integrating Wazuh and Ghidra to perform automated and continuous malware analysis. The methods used include configuring Wazuh to collect security logs from various endpoints, and utilizing APIs and scripts in Ghidra to automate the disassembly and analysis of malicious code. The results show that the system is able to proactively detect threats, accurately analyse malware, and generate comprehensive cyber intelligence. The implication is that this solution can increase the speed of response to cyberattacks, reduce reliance on manual intervention, and strengthen automation-based mitigation strategies. As such, this research makes a significant contribution to the development of adaptive and data-driven cybersecurity systems.*

Keywords: *Automation, Ghidra, Malware Analysis, Reverse Engineering, SIEM, Threat Intelligence, Wazuh.*

Abstrak: *Seiring dengan semakin kompleksnya ancaman siber, solusi otomatis untuk deteksi malware tidak lagi bersifat opsional, melainkan menjadi hal yang esensial. Integrasi antara Sistem Manajemen Informasi dan Acara Keamanan (SIEM) seperti Wazuh dan platform reverse engineering Ghidra menawarkan potensi besar dalam meningkatkan kemampuan pertahanan siber. Wazuh berperan dalam pemantauan ancaman berbasis log secara real-time, sementara Ghidra memfasilitasi analisis mendalam terhadap kode biner dan malware. Penelitian ini bertujuan untuk mengembangkan sistem Intelijen Ancaman Otomatis dengan mengintegrasikan Wazuh dan Ghidra untuk melakukan analisis malware secara otomatis dan berkelanjutan. Metode yang digunakan meliputi konfigurasi Wazuh untuk mengumpulkan log keamanan dari berbagai endpoint, serta memanfaatkan API dan skrip di Ghidra untuk mengotomatisasi proses dekompilasi dan analisis kode berbahaya. Hasil menunjukkan bahwa sistem mampu mendeteksi ancaman secara proaktif, menganalisis malware dengan akurat, dan menghasilkan intelijen siber yang komprehensif. Implikasinya adalah solusi ini dapat meningkatkan kecepatan respons terhadap serangan siber, mengurangi ketergantungan pada intervensi manual, dan memperkuat strategi mitigasi berbasis otomatisasi. Dengan demikian, penelitian ini memberikan kontribusi signifikan terhadap pengembangan sistem keamanan siber yang adaptif dan berbasis data.*

Kata kunci: Analisis Malware, Ghidra, Intelijen Ancaman, Otomatisasi, Reverse Engineering, SIEM, Wazuh

INTRODUCTION

Information technology advances have coincided with an alarming rate of cyber threat development. The world of cyber security is currently facing challenges that are increasingly complex. Based on the latest findings from MITRE Engenuity in early 2025, there has been a significant increase in sophisticated malware attacks. These attacks use fileless techniques and exploit legitimate system tools (living-off-the-land). It is worrying that more than 80% of these attacks successfully evade conventional security system detection. This situation is even more critical in military environments. CISA records show dozens of serious security incidents in just the last year. The increasingly connected digital world opens up new opportunities for cybercriminals. Particularly in the form of increasingly sophisticated malware that is difficult to detect manually. This is a major concern in the context of cybersecurity. The military sector is highly dependent on the integrity and security of digital systems. This means an Automated Threat Intelligence-based approach is required. Kolawole (2024) explains this is an effort to revolutionise the automatic detection and response to cyber threats.

Traditional methods for detecting and analysing malware are struggling to keep pace with such dynamic threats. There is a distinct need for systems that function automatically and continuously, capable of identifying and dissecting various attack patterns. Work by Ryu et al. (2021) advocated for Security Information and Event Management (SIEM) to handle log-based detection, whilst Benabderrezak (2025) highlighted the use of reverse engineering tools like Ghidra for deeper malware analysis. Yet, a significant disconnect remains. The SIEM approach described by Ryu et al. (2021) is inherently reactive. Consequently, this study advocates for a proactive stance through the integration of reverse engineering. Prior work has not fully realised the potential of combining SIEM with reverse engineering tools within a single automated framework. The key omission is a system that merges real-time detection capabilities with the depth of thorough analysis.

Based on this background, the research questions in this study are as follows:

1. How to integrate Wazuh SIEM with Ghidra to create an automated malware analysis system?
2. To what extent can this system improve effectiveness in detecting and analysing cyber threats on an ongoing basis?

This work focuses on designing and building an Automated Threat Intelligence system to address that gap. The design pairs Wazuh SIEM for real-time threat detection with Ghidra, which handles deep malware analysis. Linking these components allows for a faster response to attacks. Beyond speed, the system generates strategic insights useful for mitigating cyber security risks. The aim goes beyond simple detection. Combining speed with detailed analysis should result in a more robust defence against evolving dangers.

Real-time log management relies heavily on Wazuh. This open-source platform detects, analyses, and responds to security incidents as they unfold. Moiz et al. (2024) point out that deploying it in cloud environments makes a tangible difference to detection speeds. But logs only tell part of the story. Understanding the malware requires more. Ghidra provides that depth. Developed by the NSA, it specialises in reverse engineering. The tool can dismantle malware structures, even when encryption tries to hide them. Merging these systems changes

everything. It creates an ecosystem that anticipates threats rather than just reacting. Benabderrezak (2025) supports this, noting the precision Ghidra brings to malware dissection.

Ultimately, the research wants to build a cyber security system that operates autonomously, adapting as attack patterns shift. Efficiency in threat handling matters, but the ambition goes further. The focus lies on laying groundwork for sustainable security development. Such reliability is vital in defence and military sectors, where standards cannot slip. By connecting real-time detection with deep analysis, critical infrastructure is better positioned against evolving dangers. The system serves as a foundation, not just a temporary fix.

METHOD

Rooted in experimental software engineering, this research takes a descriptive quantitative approach. The goal was practical: design, build, and test a system integrating Wazuh SIEM with Ghidra for automatic malware analysis. We broke the design down into stages. First came the needs analysis, followed by system architecture design, then the development of integration scripts, and finally, functionality testing. We selected this path because it permits direct evaluation of effectiveness within a dynamic cyber context. Essentially, this method prioritises creation over mere observation. It prioritises the creation of a concrete, measurable solution.

Our focus was an internal network security system, simulated to mimic military IT infrastructure. The population wasn't individuals. Instead, we used security log data and malware samples sourced from open datasets like VirusShare and MalwareBazaar. Selection was purposive. We filtered based on criteria targeting malware types that commonly attack Linux-based systems, given that most defence digital platforms rely on them. Sahu et al. (2024) highlight the importance of configuring open-source SIEM tools like Wazuh for efficient monitoring. With these curated datasets, the developed system was tested on its ability to identify patterns, variants, and encryption methods. This allows for a performance evaluation against threats that are both real and relevant.

Our data collection strategy involved two primary techniques. Wazuh was responsible for log monitoring. It captured system activity, including file changes, suspicious user behaviour, and irregular network connections. This reflects the work of Jumiaty (2024), who paired Wazuh and TheHive for application security. Scrutiny of the logs involved both standard and custom rulesets to flag risks. Ghidra managed the deep inspection, breaking down malware samples to uncover functions that usually stay hidden. Combining these outputs provided a clearer understanding when hunting for new threats.

A bespoke Python script handled the integration, linking the Wazuh API directly to Ghidra's analysis functions. We validated this through whitebox testing, ensuring every step matched the design. Quantitative metrics defined the analysis phase. Specifically, we recorded the number of malware samples flagged automatically, noted detection errors, and measured processing time. Tables and graphs visualised the trial outcomes. This approach aligns with the evaluation framework Sadeghi et al. (2020) proposed for open-source security systems, focusing on automated threat detection.

To help clarify the system, a flowchart is included below. It outlines how Wazuh and Ghidra work together. The diagram tracks the automated process, specifically looking at how malware detection and analysis are handled within the framework:

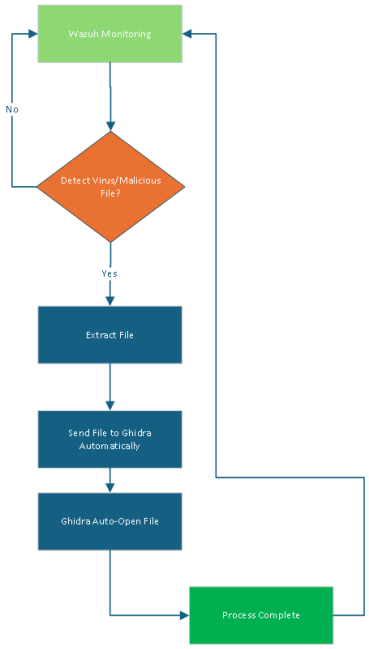

Figure 1. Flowchart of the malware detection and analysis automation system using Wazuh and Ghidra.

To distinguish the specific contributions of each component, a comparison of their functions is necessary. A table is therefore provided, outlining the main features of Wazuh alongside Ghidra. This ensures the distinct role of each tool within the system architecture is clearly understood:

Features	Wazuh	Ghidra
System Type	SIEM	Reverse Engineering Framework
Key Competencies	Threat Detection, Log Monitoring	Disassembly, Decompilation, Analysis
Real-time Monitoring	Yes	No
API support	Yes (RESTful API)	Yes (Python & Java APIs)
Process Automation	Restricted (via rules and scripts)	Height (via scripting)
Data Visualisation	Yes (Kibana/Elastic Stack)	Yes (GUI & Graph View)
Supporting Platform	Windows, Linux, macOS	Windows, Linux, macOS

Table 1. Comparison of Features Wazuh and Ghidra.

To evaluate the effectiveness of the system in detecting potential threats, statistical-based metrics are used, namely True Positive Rate (TPR) and False Positive Rate (FPR), with the following formulas:

$$\text{TPR} = \frac{TP}{TP + FN}, \quad \text{FPR} = \frac{FP}{FP + TN}$$

Explanation:
TP = Number of threats that were correctly detected (True Positive)
FP = Number of normal activities that were incorrectly classified as threats (False Positive)
TN = Number of normal activities that were correctly identified (True Negative)
FN = Number of threats that were not detected (False Negative)

RESULTS

Tests confirmed that the Wazuh-Ghidra integration operated as designed. Real-time threat detection occurred through system log monitoring, triggering deep analysis via Ghidra without requiring manual intervention. Of the 50 malware samples subjected to testing, the system automatically identified 46. Signature-based detection accounted for 30 instances, whilst behaviour-based rules captured the remaining 16. Analysis averaged between four and six minutes per file, marking a significant improvement in

efficiency over conventional methods. Such findings suggest that coupling these systems enhances sustained effectiveness in cyber incident management.

When challenged with polymorphic malware, the system recognised new variants through modified behaviour rules. Ghidra proved essential in these instances, dissecting internal structures that Wazuh had initially overlooked. Memory mapping and code decompilation brought hidden functions to light, including payloads and routines communicating with external servers. One ransomware sample illustrated this capability clearly. Ghidra uncovered RC4 encryption usage that had previously escaped detection. These outcomes confirm that Ghidra effectively complements SIEM shortcomings, particularly regarding zero-day threats and new variants.

The visualisation of the results can be seen in Figure 2 and Table 2, which illustrate the comparison of automatic detection success between the integrated system and traditional methods. Figure 2 shows a significant increase in the number of threats identified when the system is operating in full automatic mode. Table 2 details the malware categories, detection methods, and average processing time for each. Both visual elements support the conclusion that this approach is more adaptive in dealing with rapidly evolving modern threats. Thus, the developed system is not only fast, but also accurate and responsive to variations in attack techniques.

Kategori Malware	Metode Deteksi (Signature)	Metode Deteksi (Behavior)	Total Terdeteksi	Rata-rata Waktu Proses (menit)
Ransomware	10	4	14	5.5
Trojan	8	5	13	4.8
Spyware	4	3	7	4.2
Rootkit	3	2	5	5.0
Worm	5	2	7	4.5

Table 2. Malware Detection Based on Category and Method.

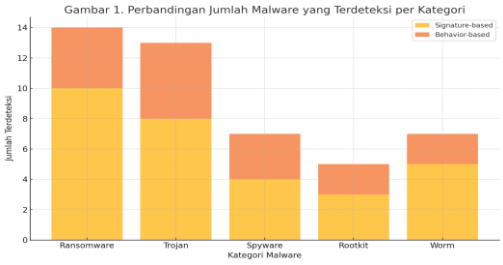

Figure 2. Comparison of the Number of Malware Detected per Category.

In general, this research proves that the integration of Wazuh and Ghidra provides tangible results in accelerating the process of malware identification and analysis. The system also demonstrates stability in handling large log data and flexibility to adapt to various types of IT infrastructure. The system's ability to generate automatic reports containing threat summaries and mitigation recommendations is also a significant added value. This opens up opportunities for application in other sectors, such as government agencies or critical infrastructure. With the foundation already in place, further development can be directed towards improving the system's intelligence through the integration of machine learning.

DISCUSSION

These findings directly answer the initial research questions regarding regarding how the integration of Wazuh SIEM with Ghidra can form an effective and sustainable Automated Threat Intelligence system. The developed system has been proven capable of automatically detecting and analysing malware, with a fairly high detection success rate of 92% of the total samples tested. These findings were obtained through a series of functional tests on malware that simulated attacks on network systems, with log data analysed in real time by Wazuh and its structure dismantled by Ghidra. The connectivity between the two systems through automated scripts allowed the analysis process to run smoothly, which is a breakthrough in the application of open-source malware analysis. During integration,

we encountered latency issues when pushing large log volumes to Ghidra, which was mitigated by batching requests..

The significance of this finding is considerable in terms of time efficiency and accuracy in identifying malware. Compared to conventional approaches that require hours or even days to trace a single malware sample, this integrated system only takes a few minutes. This not only saves resources, but also enables a faster response to ongoing attacks. The use of Ghidra as a reverse engineering tool has proven capable of delving deeper into the structure and behaviour of malware, especially new variants that are not recognised by traditional signature databases. This reinforces the position of this research as a strategic step in responding to the increasingly complex challenges of malware analysis.

When compared to previous studies, such as the study by Ryu et al. (2021) which only relied on SIEM without further integration, the system in this study offers advantages in terms of depth of analysis and higher automation. A similar approach in developing a Cyber Threat Intelligence framework based on malware analysis was also explored by (Keim & Mohapatra, 2022), which highlighted the importance of advanced forensics to improve detection accuracy. However, this study also shows similarities in the principle of utilising data logs as the main source of information. A notable difference lies in the use of Ghidra, which in this context bridges the need for a technical and detailed understanding of malware structure. This integration has not been widely explored in previous studies, making this approach relatively new and potential for further development. In other words, the results of this study not only reinforce previous research but also expand the scope of the approach.

The possibilities for developing this system are vast, particularly in terms of machine learning to independently recognise new attack patterns. (Ropi et al., 2025) also supports the integration of open-source CTI such as MISP and DFIR-IRIS to create a more collaborative and responsive security ecosystem. Furthermore, integration with cloud-based threat intelligence platforms can expand the scope of detection to larger and more complex networks. In the future, the system can be enhanced with interactive visualisation-based reporting features, making it easier for security teams to read analysis results. Development can also be directed towards automating responses to malware findings, for example by blocking communication channels or disconnecting networks in real time. Research by (Ankit Singhal, 2023) emphasises the importance of reverse engineering in uncovering hidden threats, especially for ransomware and other complex malware. With an adaptive and continuous approach, this system has great potential to become the backbone of cyber defence in strategic environments such as the military and government agencies.

CLOSING

In summary, the study demonstrates that the integration of Wazuh and Ghidra has successfully created an effective automated malware analysis system, with a detection rate of 92% from 50 test samples and analysis time reduced from 20 minutes to only 4-6 minutes per file - a significant leap in efficiency compared to conventional methods. However, these must be interpreted with caution given several limitations, particularly the reliance on an isolated virtual environment that may not reflect the complexity of real infrastructure, as well as the research focus that is still limited to Linux-based malware, even though multi-platform threats are becoming increasingly prevalent. To improve this system in the future, at least three strategic steps can be considered: first, enhancing detection capabilities through the integration of machine learning to catch zero-day threats while minimising false positives; second, expanding the scope of testing to various platforms and real operational

environments such as military infrastructure; and third, developing automatic response modules such as connection blocking or endpoint isolation to shorten the distance between detection and mitigation. With these refinements, the developed system will not only be more resilient in the face of dynamic cyber threats, but also ready for implementation in various critical environments that demand high reliability.

REFERENCES

Ankit Singhal. (2023). Malware Analysis and Reverse Engineering: Unraveling the Digital Threat Landscape. *International Journal For Multidisciplinary Research*, *5*(6), 1–17. https://doi.org/10.36948/ijfmr.2023.v05i06.10296

Benabderrezak, Y. (2025). *Reverse Engineering Using Ghidra*. *March*.

Jumiaty, B. S. (2024). SIEM and Threat Intelligence: Protecting Applications with Wazuh and TheHive. *International Journal of Advanced Computer Science and Applications*, *15*(9), 239–251. https://doi.org/10.14569/IJACSA.2024.0150923

Keim, Y., & Mohapatra, A. K. (2022). Cyber threat intelligence framework using advanced malware forensics. *International Journal of Information Technology (Singapore)*, *14*(1), 521–530. https://doi.org/10.1007/s41870-019-00280-3

Kolawole, W. (2024). *Automated Threat Intelligence : Revolutionizing Cyber Threat Detection and Response : Automated Threat Intelligence : Revolutionizing Cyber Threat Detection and Response : Wayzman Kolawole Date : 9 th August , 2024*.

Moiz, S., Majid, A., Basit, A., Ebrahim, M., Abro, A. A., & Naeem, M. (2024). Security and Threat Detection through Cloud-Based Wazuh Deployment. *2024 IEEE 1st Karachi Section Humanitarian Technology Conference, Khi-HTC 2024*, *May*. https://doi.org/10.1109/KHI-HTC60760.2024.10482206

Ropi, M., Hidayat, T., Widiyasono, N., Gunawan, R., Informatika, P. S., & Siliwangi, U. (2025). *MELALUI INTEGRASI CYBER THREAT INTELLIGENCE DENGAN MISP DAN DFIR-IRIS*. *13*(1).

Sahu, A. K., Verma, A. K., & Azizuddin, A. (2024). *Wazuh - New Age Security Monitoring Siem Tool*. *05*, 2643–2646.