Securing the Decentralized Edge: An Integrated Approach to Endpoint Security Monitoring and Threat Detection

Victor Kipchirchir Bungei, Frank Johnfia, Esther Djan and Sara Sutton
Grand Valley State University, Allendale, USA

bungeiv@mail.gvsu.edu
johnfiaf@mail.gvsu.edu
djane@mail.gvsu.edu
suttosar@gvsu.edu

Abstract Modern IT infrastructure is undergoing a significant transformation, becoming increasingly complex and decentralized as organizations move away from centralized on premise data centers toward hybrid, multicloud, and edge computing models. This is a shift driven by the demand for higher resilience, lower latency, and the specialized requirements of modern AI workloads running on the edge. While this shift improves operational efficiency, it introduces significant challenges including limited visibility, legacy network bottlenecks, operational complexity, and a broadened attack surface as a result of the decentralized edge based infrastructure requiring new security approaches that go beyond traditional perimeter security. Adversaries increasingly exploit these decentralized environments for ransomware, espionage, or coscripting devices into botnets for large scale attacks. The resulting breaches carry severe consequences including financial loss, penalties from regulators, non-compliance and irreparable reputational damage. To address the aforementioned challenges, this paper proposes a zero Trust Architecture integrated with Wazuh. Using Wazuh's comprehensive monitoring and incident response capabilities, organizations can implement a "never trust, always verify" framework that protects the decentralized edge against modern threat vectors. This paper provides practical guidance for IT professionals and students seeking to implement modern endpoint security and defend infrastructure against evolving cyber threats.

Keywords: Wazuh, Malware, Threats, Detection, Response, Cybersecurity training

1. Introduction

As the threat landscape continues to evolve alongside emerging technological trends, organizations must continue to upgrade their IT infrastructure to remain competitive and efficient. However, many organizations prioritize infrastructure upgrades with little consideration for security, often treating it as an afterthought. These changes tend to introduce vulnerabilities into the environment, and without proper logging and monitoring of system activities, these vulnerabilities can create significant security risks, which could potentially lead to substantial losses if exploited by adversaries.

The absence of robust monitoring and detection capabilities creates major challenges for detection and response teams, making it extremely difficult to identify and mitigate sophisticated threats such as advanced persistent threats(APTs). A Security Information and Event Management (SIEM) system becomes essential in this situation. A SIEM provides real-time visibility into the organization's security posture regardless of whether your operations are on cloud or on premise, automates analysis of security events, and robust reporting to ensure the organization maintains compliance requirements and well covered during forensic investigations in the event of an incident.

Modern Security Information and Event Management (SIEM) solutions generally fall into two categories: high cost commercial platforms and flexible open-source tools. Although industry leaders such as Splunk, FortiSIEM, and IBM QRadar offer sophisticated automated capabilities as shown on Table 1, they carry significant licensing fees that often create a security gap for small-to-medium enterprises (SMEs). These organizations often operate without centralized monitoring, leaving them acutely vulnerable to cyber threats.

On the other hand, open source SIEM solutions provide robust functionalities for $0 in licensing. However, they typically require extensive time resources through manual configuration and specialized expertise to integrate it into existing IT infrastructures. In this paper, we explore Wazuh, an all in one open source security platform that bridges this gap by unifying Extended Detection and Response (XDR) with traditional SIEM capabilities. It provides enterprise grade features, including configuration assessment, malware detection, File Integrity Monitoring (FIM), and automated vulnerability & threat detection and response. Architecturally, the platform comprises the Wazuh Indexer, Server, Dashboard, and Agent, supporting modern deployment via Docker, Kubernetes, Ansible, and Puppet.

Wazuh also allows integration with various threat intelligence sources such as VirusTotal, YARA, CDB Lists, and AbuseIPDB which ensures realtime detection of threats with an element of automated response to the detected

threats, ensuring that your security team is always one step ahead of adversaries. This paper aims to show the deployment of Wazuh anIT infrastructure and the necessary configurations that can be made to the tool for malware detection , file integrity monitoring, threat and detection and response to suspect bruteforce attack attempts.

Table1: Comparative analysis of SIEM platforms

Platform	Architecture	Key Strength
Microsoft Sentinel	Cloud Native	Ecosystem Synergy: Near-zero configuration for Microsoft 365, Defender, and Entra ID logs
Splunk ES	Hybrid/Cloud	Data Maturity: Powerful search (SPL) and the ability to correlate almost any data source
IBM QRadar	On-Prem/ Cloud	Out-of-the-Box Rules: Excellent for compliance with stable, pretuned correlation engines
FortiSIEM	Physical/Virtual appliance	Unified NOC/SOC: Combines asset discovery (CMDB), performance monitoring, and security
Wazuh	Open-source (On-Prem/Cloud)	The Endpoint Edge: Native File Integrity Monitoring (FIM) and EDR-like capabilities for $0 licensing

2. Objective

The main objective of this paper is to show how to integrate Wazuh in an IT infrastructure environment, identify the recommended key configurations required for threat detection, monitoring endpoints, and automated incident response in the event of an attack. Our key focus will highlight the deployment of this critical tool and the necessary configurations that will enable your organization to stay ahead of adversaries, providing blue teams with more time to focus on actual threats, minimizing alert fatigue or danger of false negatives while at the same time saving the organization running costs that would have been incurred in the option of using the commercial tools.

3. Related Work

Endpoint protection plays a critical role as the first line of defense against cyber-attacks and remains a key priority in safeguarding an organization's assets from threats. Various efforts have been put to address and improve endpoint security. We see the work of A. Al Siam et al. (2025), where they developed a threat detection and response solution solely meant for Linux endpoints, unlike in our approach where we show how Wazuh caters not only for Linux endpoints but also endpoints running MacOS and Windows operating systems, which ensures a centralized approach to monitoring all endpoints. Recent comparative analyses emphasize the superiority of Wazuh among open source SIEM solutions (such as ELK and OSSIM) precisely due to this cross platform compatibility, along with its integrated File Integrity Monitoring (FIM) and native active response capabilities R. Amami et al.(2024).

We also see A. Al Siam et al.(2025) focusing on Extended Detection and Responses (EDRs) as a malware detection solution, which highlights some of the capabilities to consider for an EDR for effective detection and response to malware. This is indeed a great insight for organizations when sourcing an EDR, and they also go ahead to provide a list of available enterprise EDRs. In our approach with Wazuh, we highlight its Extended Detection and Response capabilities such as disrupting an ongoing brute force, slowing down the attacker, and providing the security team with an alert for investigation. This is actively supported by recent research demonstrating the effectiveness of Wazuh in instantly mitigating brute force attacks by deploying automated firewall drop actions to block offending IPs after a configured threshold of failed logins as shown by K. Z. Htet et al(2025). Furthermore, Wazuh drastically improves incident response times by allowing integration with messaging

platforms such as Telegram, ensuring that security teams receive automated, real time alerts for high severity threats through an experiment by C. Dhefanni et al.(2025).

Wazuh comes with out-of-the-box rules, the flexibility to create custom rules, and integration with threat intelligence platforms such as VirusTotal, YARA, and CDB lists, which increase the probability of detecting zero-day attacks and responding to them automatically based on your configurations. The integration of live threat intelligence feeds, such as VirusTotal and AbuseIPDB, into Wazuh's event pipeline has been empirically shown to achieve threat detection rates of 95.0% and high alert precision with very low mitigation delays (averaging 2.8 seconds) via dynamic Indicator of Compromise (IOC) querying. Beyond reactive threat detection, Wazuh also offers proactive endpoint defense using its Security Configuration Assessment (SCA) module to continuously validate OS system hardening and ensure compliance with CIS benchmarks (R. Doynov et al, 2025). All of this is available for free, offering a highly capable alternative compared to other commercial SIEMS, EDRs and XDRs such as Crowdstrike, Microsoft Sentinel, Splunk ES, IBM QRadar, FortiSIEM etc

4. Methodology

We deployed the Wazuh server on Google Cloud as a docker container. We then configured Wazuh for FIM, threat detection, and response as will be shown in the paper. We then deployed the agents on our endpoints which comprised a Windows OS, MacOS and Linux operating system. We then centralized our configurations to the respective OS type, which enabled us to create, modify, and push changes to our endpoints without the need to physically do so for each machine. This enabled us to get logs from agents for analysis, detection, and response in real time.

4.1 Wazuh Architecture

For this paper, we deployed Wazuh through the docker deployment option as a single-node stack, suitable for small organizations compared to the multi-node stack that offers scalability for large sized organizations. Our setup included Wazuh docker image on a Google Cloud Ubuntu 22.04 server instance, Cloudflare for our proxy, and Wazuh agent installed on three endpoints running Windows OS, MacOS and Linux respectively. These agents act as the first line of defense Host-Based Intrusion Detection system by detecting threats and forwarding the alerts to Wazuh server, which runs another check against the configured rules before it can determine if the detected threat is indeed positive and then apply the configured actions accordingly to contain it. Figure 1 shows the Wazuh docker deployment architecture on Google Cloud and how the various components of Wazuh come into play to enable it to monitor endpoints and detect malicious activities in real time.

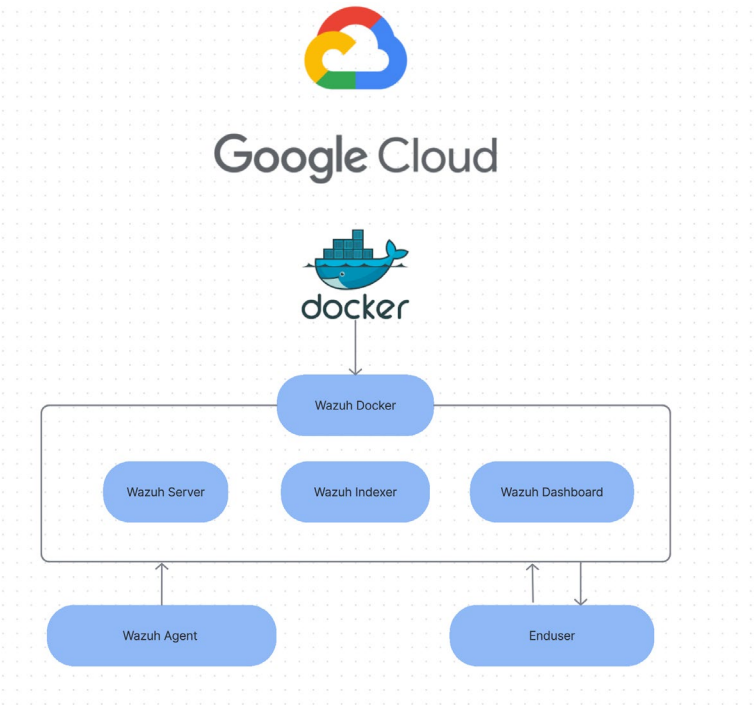

Figure 1: Wazuh docker deployment architecture on Google Cloud showing the various components that communicate with each other to make the platform work

4.2 How Wazuh Works

1. The Wazuh agents installed on endpoints in IT infrastructure collect logs from their respective endpoints and send the logs to the Wazuh server.
2. The Wazuh server parses the logs, decodes, and applies the configured rules to determine if there is any data from the decoded information that matches the rules and if any exists, an alert is raised with an id that specifies the kind of malicious activity detected for security analysts to review and analyze further to confirm if indeed there was a compromise.
3. Wazuh comes with out of the box default rules that are continuously updated and maintained by the Wazuh team to address emerging threats and ensure effectiveness of its detection capabilities which cover a wide range of security events and log sources, providing a great baseline for detecting common security threats. Wazuh also provides an advantage of flexibility through custom rules, either by creating new custom rules or modifying the default rules, which enable users to tailor Wazuh to meet their unique IT infrastructure's needs, greatly enhancing its capabilities and effectiveness.
4. Over time, Wazuh collects information from the alerts received, endpoints, and environments being monitored, and represents this information in dashboards and reports for review by security teams providing an overview of the security posture of your organization.

4.3 File Integrity Monitoring

Malware frequently targets the Windows Registry to achieve malicious objectives, such as establishing persistence and performing other malicious actions. The Wazuh file integrity monitoring module includes Windows Registry monitoring that monitors commonly targeted registry paths to detect modifications. VirusTotal integration uses the VirusTotal API to detect malicious content within files and directories monitored by the Wazuh file integrity monitoring capability. Wazuh allows users to define directories of interest that contain critical files such as system files and confidential information. Any changes made to files or directories of interest will create an alert as shown in Figure 2, where a new suspicious file, suspicious-file.exe, has been added to the monitored directory, Wazuh-test.

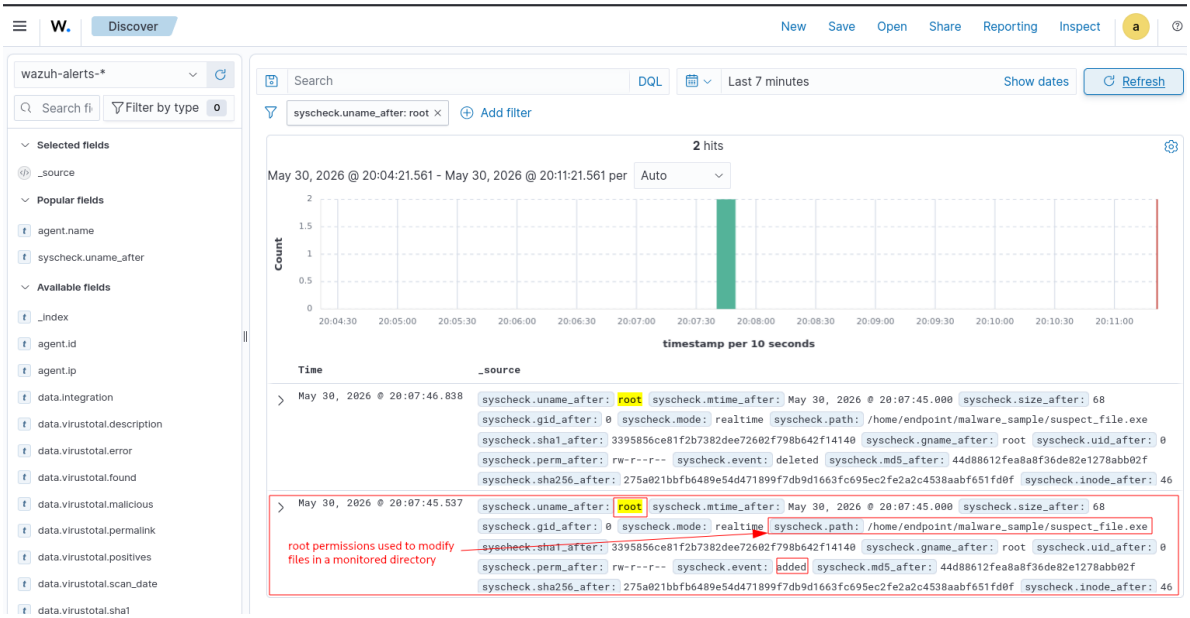

Figure 2: A suspicious file added to the monitored directories is detected by the FIM module

4.4 Threat Detection and Response

Wazuh uses the active response module to run scripts or executables on a monitored endpoint, acting on certain triggers. The data flow for threat detection and response is provided in Figure 3. In our use case, we simulated an ssh brute force attack against an Ubuntu endpoint and configured the active response module on the Wazuh server to block the IP address of the attacker endpoint. The main objective was to prevent brute force attacks from ssh. The active response module executed a script that blocked the IP address of the attacker when Rule 5763-sshd brute force trying to get access to the system got triggered.

Figure 4: Sample of Wazuh Manager configuration that disconnects connection to victim machine

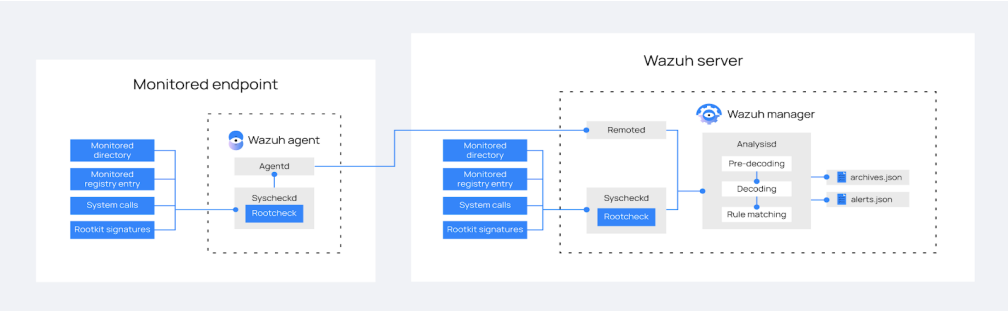

Figure 3: Wazuh threat detection and response workflow

Figure 4 provides a sample of Wazuh Manager configurations. This was followed by adding the active response configuration for response to brute-force attack attempts as shown in Figure 5.

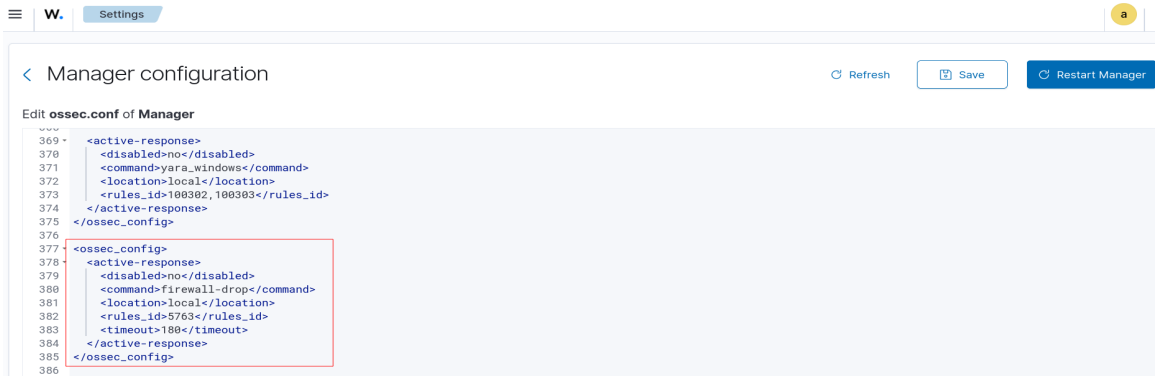

Figure 5: Wazuh Manager configurations for active response to brute-force attack attempts

The attacker and victim endpoints are shown in Figure 6. The adversary launched a ssh brute-force attack on the victim endpoint using a payload through hydra, as shown in Figure 7 Wazuh detected the brute-force attack and logged an alert as shown in Figure 8. After detection of this threat, Wazuh cut the connection between the victim machine and the adversary, as evidenced by the 100% packet loss as shown in Figure 9.

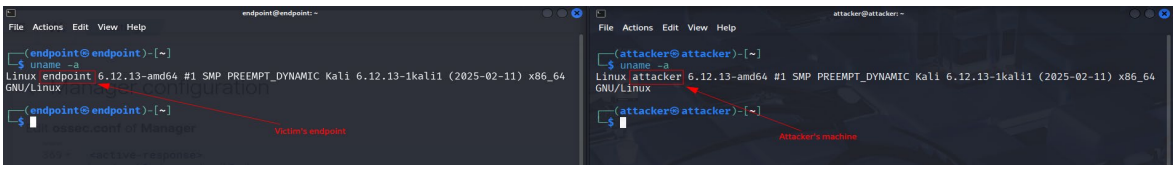

Figure 6: Attacker and Victim machine

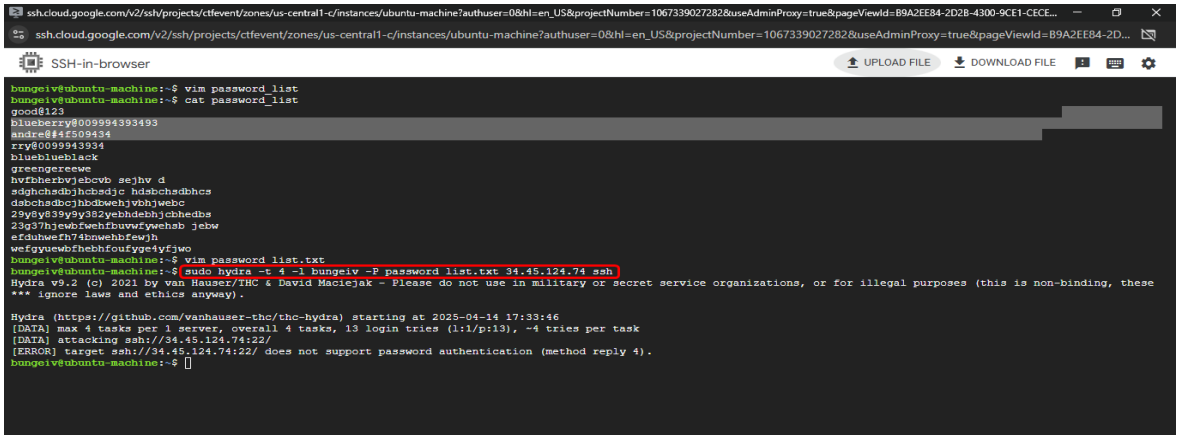

Figure 7: Attacker machine attempts a brute-force attack using hydra

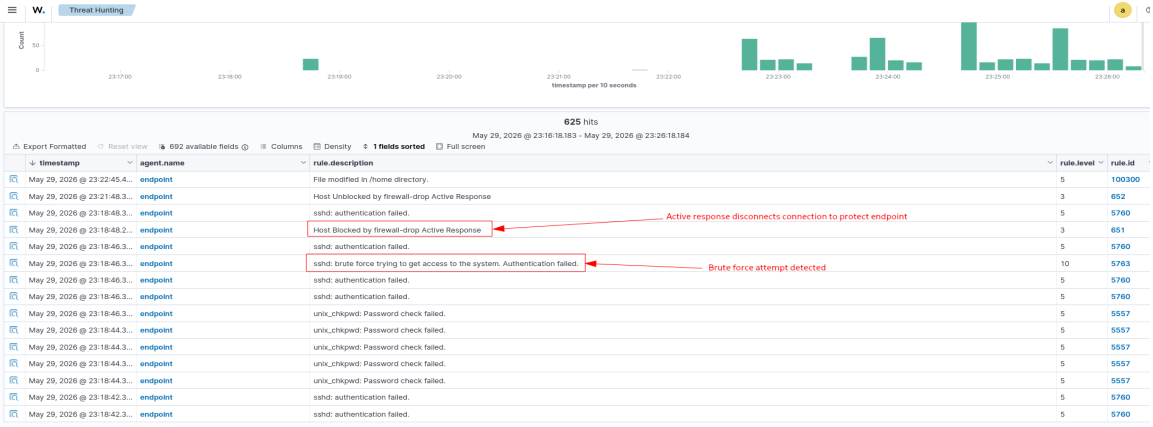

Figure 8: Brute-force attack is detected by Wazuh

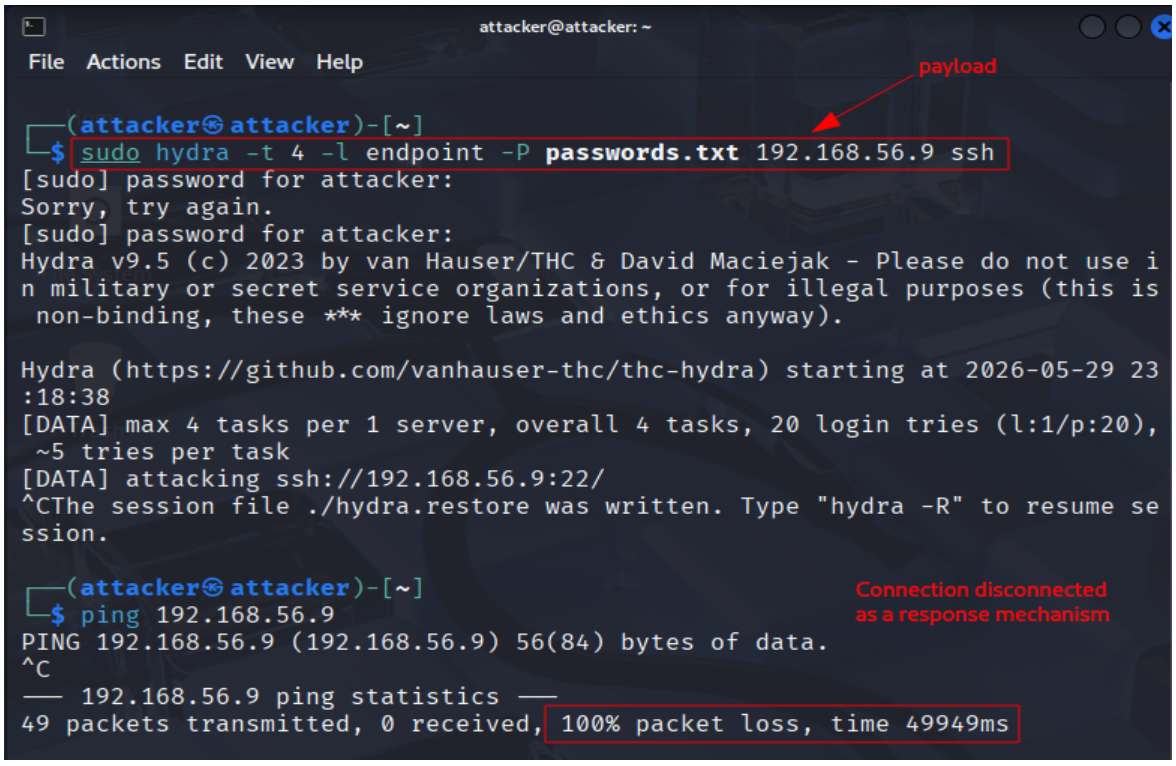

Figure 9: Wazuh responds to attack by disconnecting the connection between attacker machine and victim machine

4.5 Malware Detection

In recent emerging threats, traditional methods that rely solely on signature-based detections fail to capture new threats. Signature-based approaches struggle to detect zero-day attacks, polymorphic malware, and other evasion techniques used by threat actors. As a result, organizations are at risk of undetected data breaches and exfiltration. Having a SIEM in place with malware detection capabilities that not only rely on malware signatures for detection but use heuristics for user and entity behaviour analytics enables organizations to detect and respond to sophisticated and evasive threats effectively.

Our setup integrated threat intelligence sources such as VirusTotal which enabled Wazuh to detect malware in real time and raised alerts when it identified the malicious files by comparing the identified indicators of compromise with the information stored in the CDB lists (constant databases). These lists can store known malware indicators of compromise, including file hashes, IP addresses, and domain names. The screenshots shown in Figure 11 and Figure 12 show the process from the time a malicious file is downloaded to an endpoint to the time it is detected by Wazuh through the VirusTotal Threat intelligence integration.

Figure 11: The malicious file downloaded on the monitored endpoint is detected by Wazuh through VirusTotal threat intelligence integration

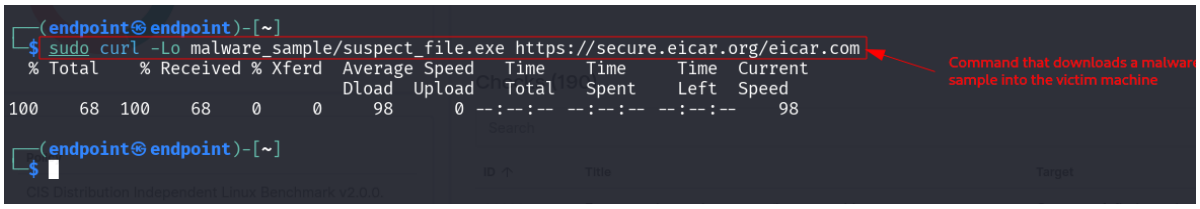

Figure 12: A malicious file is downloaded on the monitored endpoint

Wazuh Manager detected the malware and created an alert of the suspicious executable file as shown in Figure 11. From the alert received on Wazuh we were able to get a link to VirusTotal for this specific malicious file where we checked the threat intelligence sources that reported that it was indeed malicious, as shown on Figure 13.

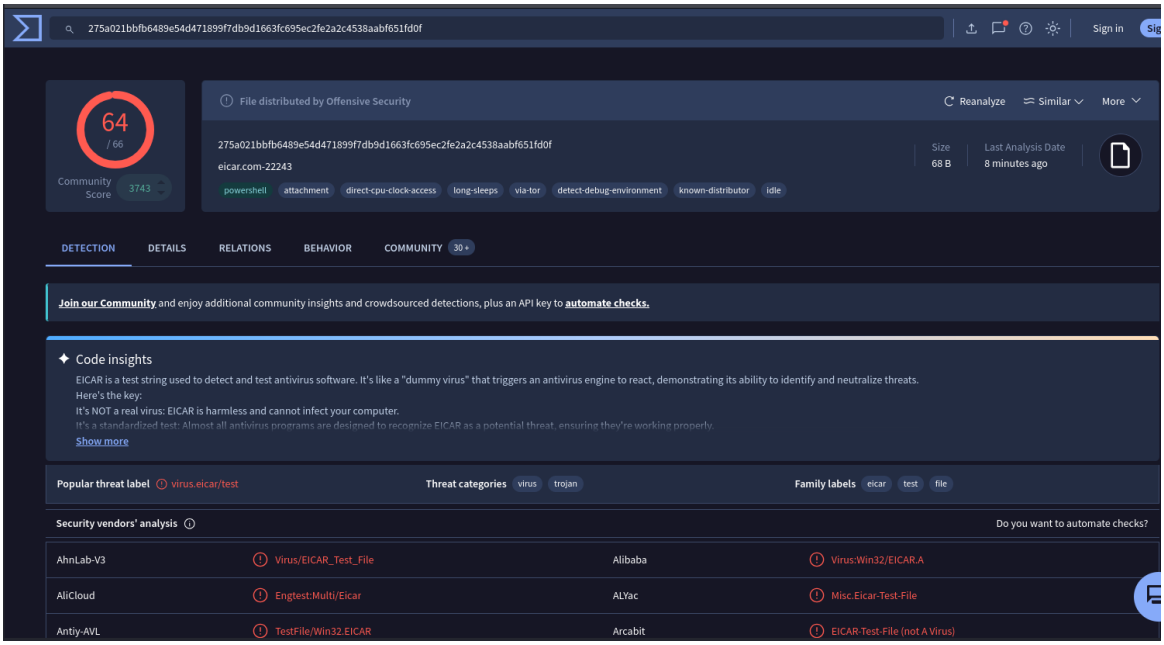

Figure 13: Malware score based on VirusTotal

4.6 Configuration Assessment

Wazuh gave an overview of endpoints based on the operating system running on the endpoint, it then checked this against the Centre for Internet Security benchmark for the specific operating system. This ensured that all endpoints in our experiment were hardened according to the standard.

Wazuh provided a view into the configuration assessment of all endpoints used in our experimental IT infrastructure, as shown in Figure 14. Endpoints are given a percentage score of compliance to the CIS benchmark as well as provide the list of checks that Wazuh ran against the endpoint and the result, making it easier and convenient for system administrators to patch up non-compliant endpoints, ensuring all critical assets are effectively hardened.

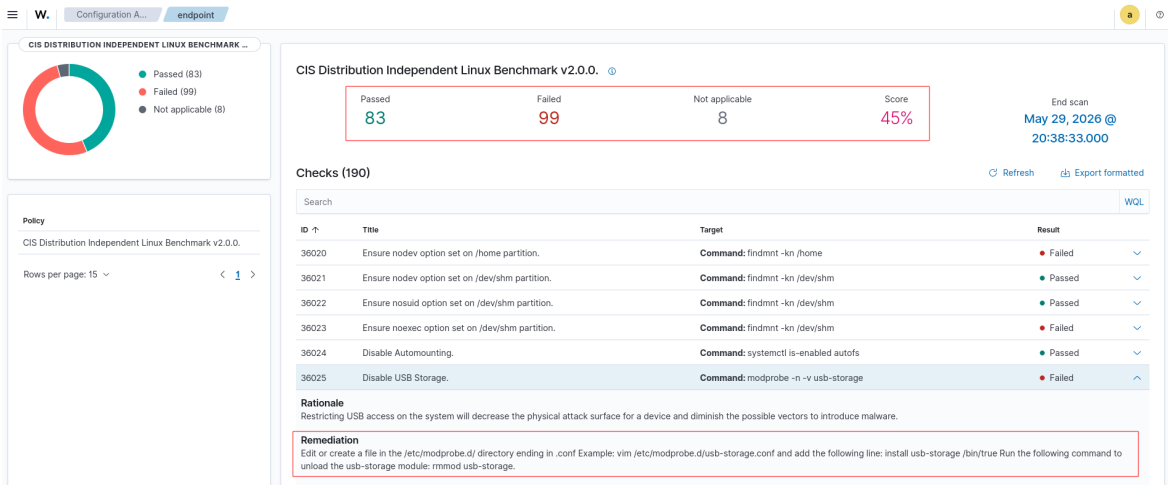

Figure 14: Onboarded endpoints configuration assessment with a score card based on passed and failed checks with recommendations to patch up

4.7 Limitations

Despite providing Extended Detection & Response(XDR) and SIEM capabilities at zero licensing costs, equating the free license with a zero cost or zero risk operation would be detrimental in evaluation of open source solutions. The open-source nature of the platform masks significant architectural, operational and security limitations that shift the burden of platform maturity and scaling efficiency onto the organization. Below are some of the limitations and tradeoffs to consider:

- The platform lacks a built-in load balancing mechanism which would require organization deploying Wazuh at scale to acquire a separate external load balancing solution
- High false positive burden if not properly tuned which necessitates expert level tuning to address false positives which can be time consuming and labor intensive
- Wazuh does not have internal integrity controls over its own alert data. If an attacker gains root access to the Wazuh Manager, logs and alerts can be manipulated. Organizations must implement a compensating control, such as shipping alerts to an immutable storage solution

5. Recommendations

False positives are security alerts incorrectly classified to suggest a threat when there is no threat. This poses a significant challenge in cybersecurity, as alerts often overwhelm security teams, leading to alert fatigue, potentially diverting their attention from detecting and responding to actual threats. Below are some of the recommendations to minimize false positives in your SIEM tool and enhance its effectiveness, as well as boost the productivity of your security team:

- Fine tune SIEM depending on how your IT infrastructure is set up, be it on premise or cloud to minimize false positives.
- Customize SIEM rule sets by enabling only the rules relevant to your environment to reduce noise and focus on genuine threats.
- Set appropriate alert thresholds on SIEM to balance between detecting suspicious activity and avoiding alert fatigue amongst your security teams.
- Use machine learning models for adaptive learning as seen in the evaluation on the use of Large Language Models (LLMs) to classify security alerts with the aim to reduce false positives in a Security Operations Center (J. Roy et al, 2026)

6. Conclusion

In an era defined by decentralized infrastructure and increasingly sophisticated adversarial tactics, a robust SIEM solution is no longer an enterprise luxury, but a strategic necessity for organizations of all sizes. However, the true efficacy of such a system lies not in its deployment alone, but in its customization to unique operational requirements of an organization. When properly tuned, a SIEM provides a vital "360-degree" visibility across hybrid, cloud, and edge environments, effectively bridging the visibility gaps that traditional security perimeters leave behind. By providing real time telemetry and identifying behavioral anomalies, the platform affords security teams the critical lead time necessary to disrupt the attack lifecycle before significant damage occurs.

Crucially, the open-source nature of platforms like Wazuh democratizes high tier security by eliminating the prohibitive licensing fees associated with commercial big data security tools. This accessibility allows small-to-medium businesses which often face the same threats as global corporations but with a fraction of the budget to implement enterprise grade monitoring and compliance frameworks. Furthermore, the integration of automated active response capabilities represents a paradigm shift in incident management. By delegating the mitigation of known commodity threats to automated workflows, organizations can significantly reduce their response time to security incidents. This automation empowers resource constrained security teams to move away from the fatigue of manual triage, allowing them to dedicate their expertise to high-level threat hunting and long-term strategic resilience. Ultimately, by marrying the principles of Zero Trust with the accessible power and customizability of open source monitoring, organizations can transform their security posture from a reactive, fragmented defense into a unified, proactive ecosystem capable of defending the modern digital frontier

Ethical Declaration: Ethical clearance was not required for this research.

AI Declaration: AI was used primarily to rectify grammatical errors and helped to formulate better structured sentences to improve readability.

References

S. Agarwal, A. Sable, D. Sawant, S. Kahalekar and M. K. Hanawal, "Threat Detection and Response in Linux Endpoints," 2022 14th International Conference on COMmunication Systems & NETworkS (COMSNETS), Bangalore, India, 2022

Al Siam, M. M. Hassan, A. K. M. Masum and T. Bhuiyan, "Automating Malware Detection and Response via Real-Time Threat Feed Integration with Wazuh SIEM," 2025 IEEE 2nd International Conference on Computing, Applications and Systems (COMPAS), Kushtia, Bangladesh, 2025

R. Amami, M. Charfeddine and S. Masmoudi, "Exploration of Open Source SIEM Tools and Deployment of an Appropriate Wazuh-Based Solution for Strengthening Cyberdefense," 2024 10th International Conference on Control, Decision and Information Technologies (CoDIT), Vallette, Malta, 2024

M. -M. Andronache, A. Vulpe and C. Burileanu, "A Comparative Study of Intrusion Events in Different SIEM Systems," 2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI), Stará Lesná, Slovakia, 2025

M. -M. Andronache, A. Vulpe and C. Burileanu, "A Comparative Study of Intrusion Events in Different SIEM Systems," 2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI), Stará Lesná, Slovakia, 2025

A. Arfeen, S. Ahmed, M. A. Khan and S. F. A. Jafri, "Endpoint Detection & Response: A Malware Identification Solution," 2021 International Conference on Cyber Warfare and Security (ICCWS), Islamabad, Pakistan, 2021

P. Bharti, S. S. Roy and A. Suresh, "Implementation of Yara Rules in Android," 2023 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2023.

C. Dhefanni, M. Suhartana and R. Hassan, "Real-time Attack Simulation and Detection Using WAZUH and Telegram Alerts," 2025 International Conference on Information Management and Technology (ICIMTech), Bandung, Jawa Barat, Indonesia, 2025

R. Doynov, M. Nenova and G. Sotirov, "Security Hardening of Ubuntu 22.04 LTS: Practical CIS Benchmark Implementation and Wazuh Monitoring," 2025 28th International Symposium on Wireless Personal Multimedia Communications (WPMC), Sofia, Bulgaria, 2025

EDRandThreatLocker,https://www.threatlocker.com/whitepaper/edr-and-threatlocker?d0ca0847_page=2&f508ed49_page=2

K. Z. Htet, H. T. Zaw and A. H. Maw, "Brute Force Detection and Active Response for Secure Web Login using Wazuh," 2025 6th International Conference on Advanced Information Technologies (ICAIT), Yangon, Myanmar, 2025

https://documentation.wazuh.com/current/getting-started/use-cases/malware-detection.html

https://documentation.wazuh.com/current/user-manual/ruleset/cdb-list.html

https://wazuh.com/platform/siem/

https://wazuh.com/resources/white-paper/

https://www.abuseipdb.com/

https://www.crowdstrike.com/en-us/resources/white-papers/endpoint-detection-and-response/

https://www.fortinet.com/products/siem/fortisiem

https://www.guardrails.io/blog/false-positives-and-false-negatives-in-information-security/

https://www.ibm.com/products/qradar-siem

https://www.siriusopensource.com/en-us/blog/problems-and-operational-limitations-wazuh

https://www.splunk.com/en_us/products/enterprise-security.html

Huntress Managed Endpoint Detection and Response(EDR), https://support.huntress.io/hc/en-us/categories/22524362006803-Huntress-Managed-Endpoint-Detection-and-Response-EDR

Kumari, D. Gupta and M. Uppal, "Enhanced Brute Force Attack Detection in Remote Access Security: Integrating ANN and SVM," 2024 Asia Pacific Conference on Innovation in Technology (APCIT), MYSORE, India, 2024

S. Moiz, A. Majid, A. Basit, M. Ebrahim, A. A. Abro and M. Naeem, "Security and Threat Detection through Cloud-Based Wazuh Deployment," 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), Tandojam, Pakistan, 2024

J. Roy and E. A. Balde, "Toward Context-Aware Alert Classification in Security Operations Centers Using LLMs," 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC), Houston, TX, USA, 2026

Sood G (2021). \textit{virustotal: R Client for the virustotal API}. R package version 0.2.2.

N. Tiwari and N. Hubballi, "Secure Socket Shell Bruteforce Attack Detection With Petri Net Modeling," in IEEE Transactions on Network and Service Management, vol. 20, no. 1, pp. 697-710, March 2023