International Journal Software Engineering and Computer Science (IJSECS)
5 (3), 2025, 1070-1082
Published Online December 2025 in IJSECS (http://www.journal.lembagakita.org/index.php/ijsecs)
P-ISSN: 2776-4869, E-ISSN: 2776-3242. DOI: https://doi.org/10.35870/ijsecs.v5i3.5770.

RESEARCH ARTICLE Open Access

Advanced Persistent Threats Analysis and Intrusion Detection Systems Evaluation

Dedy Wibowo *
Postgraduate, Master of Informatics Engineering, Universitas Pamulang, South Tangerang City, Banten Province, Indonesia.
Corresponding Email: dedy.unpak06@gmail.com.

Taswanda Taryo
Postgraduate, Master of Informatics Engineering, Universitas Pamulang, South Tangerang City, Banten Province, Indonesia.
Email: dosen02234@unpam.ac.id.

Ferhat Aziz
Postgraduate, Master of Informatics Engineering, Universitas Pamulang, South Tangerang City, Banten Province, Indonesia.
Email: ferhat.aziz@brin.go.id.

Received: October 24, 2025; Accepted: November 10, 2025; Published: December 1, 2025.

Abstract: Advanced Persistent Threats are significant cybersecurity threats that employ covert and strategically planned operations to achieve long-term unauthorized access and data exfiltration. PT XYZ, a logistics company with considerable operational and customer data, is more susceptible to APTs, which is why the company decided to implement Wazuh as an open-source SIEM platform for improved intrusion detection capabilities. We assessed how effectively this IDS-SIEM implementation could detect and respond to APT scenarios by analyzing multi-source logs from Wazuh, Sysmon, and endpoint telemetry across PT XYZ's PC infrastructure between June 3-30, 2025—capturing 35,333 records in total. Simulated APT attacks were carried out using Atomic Red Team with detection mapping based on MITRE ATT&CK tactics. Most of the early stages of attack phases were identified by Wazuh particularly Initial Access and Execution phases where the system logged 1,060 true positives; 8,537 true negatives; 563 false positives; and 440 false negatives at an accuracy rate of 91%. Normal traffic detection results were good with a precision of 0.95, recall of 0.94 F1-score at the same value whereas attack detection had a precision value of 0.65 with a recall of 0.71 giving it an F1 score of 0.68 making macro-averaged metrics fall at values such as 0.80 for precision and 0.82 for recall which further brought the F1 score up to 0.81 while weighted averages peaked at 0.91.Our results indicate that an open-source SIEM like Wazuh can be used effectively for the detection of APTs in logistics operations when configured appropriately using MITRE ATT&CK-based threat simulations – hence having real-world applicability towards improving cybersecurity defenses within this sector.

Keywords: APT; SIEM; Wazuh; Advanced Persistent Threat; Intrusion Detection; Cybersecurity.

1. Introduction

Advanced Persistent Threats are advanced, sophisticated multi-stage cyberattacks designed with a specific target and long-term goal implemented in stealth mode. APT actors use advanced evasion techniques to circumvent organizational security perimeters, making detection and prevention exceptionally challenging. Organizations are required to adopt adaptive continuously evolving defense strategies against adversarial techniques that constantly shift in complexity and stealth [1]. One of the critical challenges is inconsistent detection rule labeling across vendors. Even though Endpoint Detection and Response (EDR) solutions may identify similar malicious behaviors, they oftentimes map them to different MITRE ATT&CK tactics or techniques. Two solutions can see the same events but classify them differently and therefore provide different analysis results depending on which product is being used [2].

Security Information and Event Management systems collect logs from many sources, correlate security events, and find potentially malicious behaviors based on their Tactics, Techniques, and Procedures [3]. Through log correlation analysis, PT XYZ uses the power of SIEM to try to find possible APT threats at early stages and suspicious behavior patterns in its enterprise network [4]. The research is an analysis of APT threats as well as the evaluation of an intrusion detection system that is currently running at PT XYZ. It then gives recommendations on how to improve policies concerning cybersecurity as well as operational defense strategies in order to be more resilient against ever-changing threats [5][6].

SIEM platform adoption has increased in number; however, there are existing limitations within current intrusion detection environments regarding APT attacks. Conventional IDS approaches cannot detect APT patterns because such attacks are very structured, stealthy, and prolonged. Poor integration between the implemented SIEM (Wazuh) and IDS components results in slower responses with reduced accuracy for detection. There is no optimal real-time threat analytics capability in the existing system; hence responses during active cyberattacks will be delayed. These limitations form large gaps of vulnerability in defense postures against adversaries who utilize temporal gaps between intrusion and detection.

This study aims to answer three fundamental questions. First, how much does the implementation of Wazuh-based SIEM improve the performance of detection at the APT stage in the operational environment of PT XYZ? Second, how effective is the existing SIEM-IDS integration in detecting multi-stage APT behavior through correlation based on MITRE ATT&CK? Third, what enhancement strategies would improve system accuracy, real-time detection capability, and overall cyber defense resilience for PT XYZ? Answering these questions requires a systematic evaluation of detection mechanisms, correlation rules, and response workflows against realistic APT scenarios reflecting actual threat actor behaviors observed in logistics sector operations.

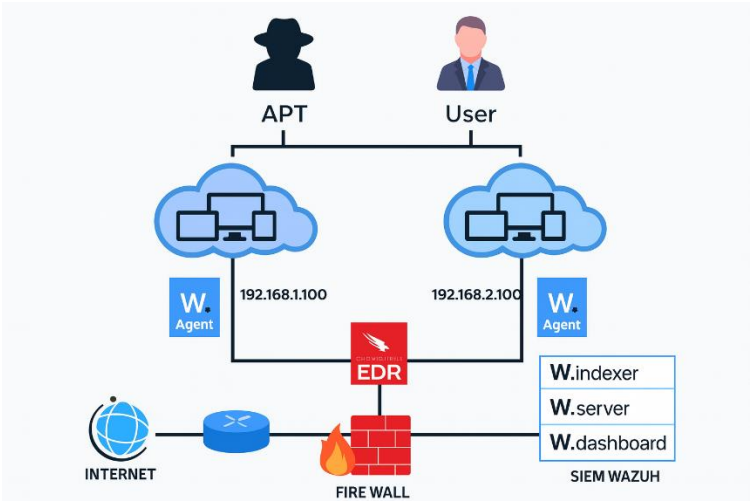


Figure 1. Cyberattack Handling Network Security Infrastructure.

2. Related Work

2.1 Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) systems record network events and identify potential threats or vulnerabilities. However, attackers frequently employ sophisticated evasion techniques to bypass predefined security rules, necessitating continuous refinement of detection mechanisms. Organizations typically deploy multiple security solutions in parallel, ensuring that attacks missed by one system can be caught by another [7]. Anomaly detection enhances network security by learning normal user patterns and

flagging packets that deviate from established baselines. The system categorizes unusual packets as anomalous, enabling rapid threat identification [8][9]. SIEM implementation plays a crucial role in strengthening information security through log collection, correlation, and analysis across diverse IT infrastructure sources. Open-source SIEM solutions offer particular advantages when addressing data privacy regulations such as the General Data Protection Regulation (GDPR) [11]. SIEM platforms function not only as security incident detection systems but also as monitoring tools for ensuring compliance with data protection policies. Evaluation results demonstrate that open-source SIEM solutions achieve effective performance in anomaly detection while providing visibility into network activities and maintaining regulatory compliance with data privacy requirements [12].

2.2 Advanced Persistent Threat (APT)

Advanced Persistent Threats (APTs) represent planned, continuous, and sophisticated attacks where adversaries gain unauthorized access to networks or systems and maintain prolonged presence without detection. APT attacks aim to steal sensitive data or disrupt target system operations, often causing significant impact on critical infrastructure. APT models target security diagnostic systems to simulate various cyberattack forms, including Denial of Service (DoS), brute force, man-in-the-middle (MITM), and ransomware [12]. APTs exhibit three defining characteristics. First, they are advanced—utilizing sophisticated exploitation techniques such as zero-day vulnerabilities, privilege escalation, and fileless attacks. Second, they are persistent—maintaining hidden and repeated access to target systems over extended periods. Third, they constitute genuine threats—conducted by highly capable actors, typically state-sponsored groups or organized criminal organizations, aiming to steal, spy on, or damage data and systems [13]. Research shows that technique coverage increased approximately 11.2% in interworking environments combining open-source threat detectors and threat log collectors. Coverage improvements were particularly notable during access domain expansion and session connection with final victims [14].

2.3 Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) solutions detect, analyze, and respond to security threats on endpoints such as computers, servers, and network devices [2]. EDR operates by continuously collecting activity data from endpoints and analyzing it to identify suspicious behavior or potential threats. Once threats are detected, EDR can execute automated response actions including isolating infected devices, blocking malicious processes, and providing forensic information for further investigation [15][16]. System-level monitors integrated with emulated IoT system algorithms identify malicious actions and determine corresponding network traffic or packets, enabling edge devices to block suspicious traffic effectively [17].

3. Research Method

Our study employs a mixed-methods case study approach combining qualitative description of the operational environment with quantitative performance evaluation of IDS-SIEM deployment. The qualitative aspect documents PT XYZ's network architecture, deployment decisions, rule engineering, and analyst workflows. The quantitative aspect measures detection performance using event-level classification metrics—confusion matrix, precision, recall, F1-score, and accuracy—while computing macro and weighted averages to address class imbalance.

3.1 Problem Identification

Advanced Persistent Threats (APTs) represent one of the most dangerous and complex forms of cyberattacks, often evading detection through structured, gradual, and covert operations. Attackers infiltrate organizational networks over extended periods to steal sensitive information or damage infrastructure. APT threats pose critical challenges because existing security systems struggle to identify suspicious activities that unfold gradually and persist over time. Current detection systems at PT XYZ—including Wazuh, Sysmon, and CrowdStrike EDR—lack optimal integration, resulting in fragmented information that fails to reveal complete APT attack patterns [18].

3.2 Research Object Selection

We selected three security tools currently operational in PT XYZ's information security infrastructure:

1) Wazuh (SIEM - Security Information and Event Management) version v4.10.1
2) Sysmon (IDS/IPS - Intrusion Detection and Prevention System)
3) CrowdStrike Falcon (EDR - Endpoint Detection and Response)

These tools were chosen because PT XYZ actively deploys them in production environments. However, no prior integrated study has evaluated their collective effectiveness in detecting stealthy, multi-layered, long-lasting APT attacks [19]. Our research addresses this gap by examining how these systems perform individually and collaboratively when confronting sophisticated threat scenarios.

3.3 Methodological Approach

We employ a descriptive qualitative approach aligned with our primary objective: understanding, describing, and evaluating APT attack phenomena and the effectiveness of intrusion detection systems deployed at PT XYZ. Our approach focuses on collecting narrative and contextual data obtained through security log documentation, alert reports from Wazuh, Sysmon [20], and CrowdStrike systems, alongside observations and analyses [21], from simulated attack processes conducted in controlled test environments. The descriptive method systematically explains how each system operates in detecting and responding to APT threats based on attack stages defined in the MITRE ATT&CK framework. Our approach enables detailed examination of system limitations, strengths, and synergies when addressing complex cyber threats. We document operational workflows, correlation rule effectiveness, and analyst response patterns to provide practical insights into real-world detection capabilities.

3.4 Dataset Description

Table 1 presents Wazuh SIEM log data collected during June 2025 as part of our APT detection research. The dataset [22], comprises daily CSV log files generated by the Wazuh SIEM system, capturing event data from monitored endpoints and network sources. File sizes vary significantly across days, reflecting fluctuations in system activity and event generation that correlate with different APT simulation and detection phases.

Table 1. Wazuh SIEM log dataset details for June 2025.

No.	Date	Record Name	Size (KB)
1	03 June 2025	3 June	1,600
2	04 June 2025	4 June	6,898
3	05 June 2025	5 June	9,058
4	09 June 2025	9 June	1,429
5	10 June 2025	10 June	1,048
6	11 June 2025	11 June	1,201
7	12 June 2025	12 June	8,351
8	13 June 2025	13 June	1,550
9	16 June 2025	16 June	161
10	17 June 2025	17 June	1,361
11	18 June 2025	18 June	1,857
12	19 June 2025	19 June	1,538
13	20 June 2025	20 June	1,413
14	23 June 2025	23 June	14,651
15	24 June 2025	24 June	17,347
16	25 June 2025	25 June	1,400
17	26 June 2025	26 June	1,755
18	30 June 2025	30 June	5,737

Notable activity peaks occur on June 23-24, with file sizes reaching 14,651 KB and 17,347 KB respectively, suggesting intensive security events during these periods. Lower activity days, such as June 16 (161 KB), indicate baseline operational levels. These variations provide valuable context for analyzing detection system behavior across different threat intensity scenarios.

4. Result and Discussion

4.1 Results

In this research phase, the intrusion detection system based on Security Information and Event Management (SIEM) Wazuh [23], was implemented to monitor and detect indications of Advanced Persistent Threat (APT) attacks within PT XYZ's system environment. The system was configured to receive logs from various infrastructure components, including Windows endpoints (via Sysmon), firewalls, and IDS [24]. The collected log data were then analyzed in real-time to identify complex and gradual attack patterns characteristic of APT activities.

4.1.1 SIEM Architecture and Configuration

Wazuh Manager serves as the main component for log collection, anomaly detection, and event correlation research.

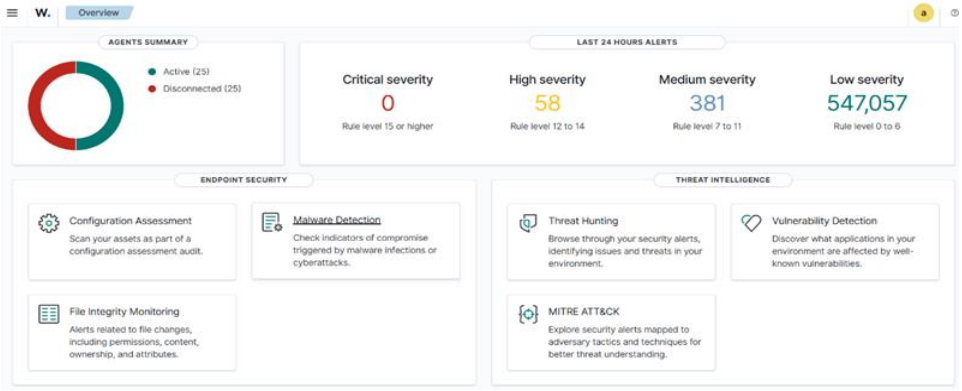


Figure 2. Dashboard Wazuh Manager.

4.1.2 Wazuh Agent

The Wazuh Agent is installed on client PCs to directly transmit system and security logs to the Wazuh Server.

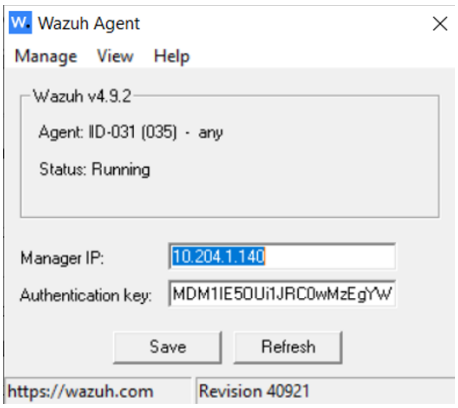


Figure 3. Setup Wazuh Agent.

4.1.3 Attack Simulation and Data Collection

To test Wazuh's detection effectiveness, an APT attack simulation was conducted using the Atomic Red. Team framework and PowerShell, with scenarios covering kill-chain stages such as [10]:

1) Initial Access: spear-phishing simulation employing macros or script-based payloads.
2) Execution: execution of PowerShell scripts and remote code execution on the target system.
3) Persistence & Privilege Escalation: addition of autorun registry entries and exploitation of system privileges.
4) Command and Control (C2): outbound connection established to a simulated C2 server.
5) Data Exfiltration: compression and transfer of sensitive files over an encrypted connection.

Data from this simulation were collected for analysis via the Kibana dashboard.

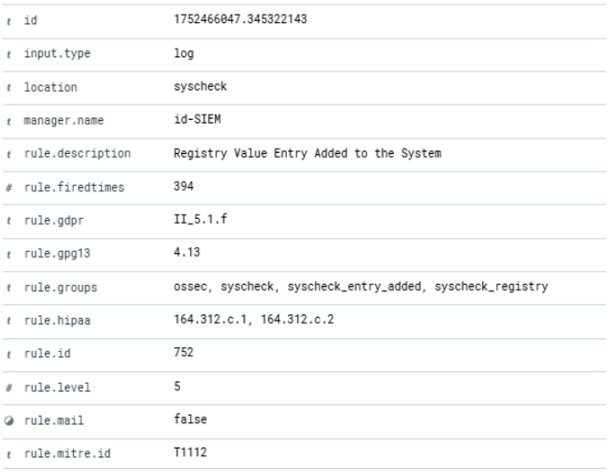
1) Penetration Simulation: Initial Access

   Initial Access is the stage in which an attacker executes malicious code [25], or exploitation commands on the victim's device after successfully obtaining initial access. The goal of this phase is to activate a payload such as malware, a backdoor, or a shell script that enables further system control.

```
CommandLine: "C:\Users\PCHR008\AppData\Local\IE Tab\17.1.25.1\ietabhelper.exe"
CurrentDirectory: C:\Users\PCHR008\AppData\Local\IE Tab\17.1.25.1\
User: ID-031\PCHR008
LogonGuid: {e725d783-50a9-686e-9000-170000000000}
LogonId: 0x170090
TerminalSessionId: 1
IntegrityLevel: Medium
Hashes: SHA256=45D211F3A85D54778A090B0B903FAE35E0EB043B13B01BE7A17447C8ACD1ABF5
ParentProcessGuid: {e725d783-da64-6870-fc2b-00000000c100}
ParentProcessId: 20572
ParentImage: C:\Windows\System32\cmd.exe
```

Figure 4. Macro attack detection from Wazuh.

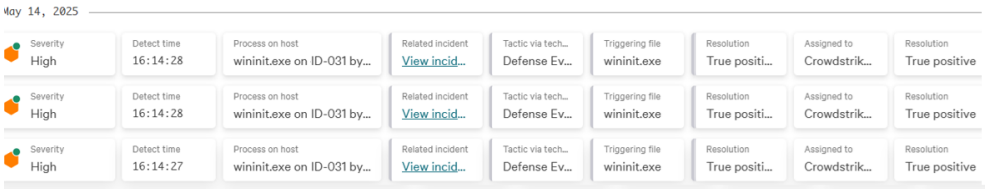
2) Penetration Simulation: Execution
Execution in the context of an Advanced Persistent Threat (APT) refers to the stage in which the attacker runs malicious code or commands on a compromised system to achieve their intended objectives. This phase typically involves the activation of malware, scripts, or legitimate tools that enable the attacker to establish control, perform reconnaissance, or prepare for subsequent actions such as privilege escalation or persistence.



id	1752466047.345322143
input.type	log
location	syscheck
manager.name	id-SIEM
rule.description	Registry Value Entry Added to the System
rule.firedtimes	394
rule.gdpr	II_5.1.f
rule.gpg13	4.13
rule.groups	ossec, syscheck, syscheck_entry_added, syscheck_registry
rule.hipaa	164.312.c.1, 164.312.c.2
rule.id	752
rule.level	5
rule.mail	false
rule.mitre.id	T1112

Figure 5. Execution attack detection from Wazuh.

3) Penetration Simulation: Persistence & Privilege Escalation
Persistence is a technique used by attackers to ensure continued access to the target system, even after a reboot, logout, or remediation attempts by the system owner. The primary objective of persistence is to maintain a long-term connection to the compromised system so the attacker can return at any time without needing to repeat the initial penetration process. Figure 6 shows detection results on CrowdStrike EDR [26]. The attack was automatically blocked before it could impact the system, and prior to being detected as an attack by the Wazuh client. Table 2 presents the detection log summary for May and June, showing how EDR protection prevented PT XYZ users from cyberattack issues using persistence techniques to access the system.



May 14, 2025

Severity	Detect time	Process on host	Related incident	Tactic via tech...	Triggering file	Resolution	Assigned to	Resolution
High	16:14:28	wininit.exe on ID-031 by...	View incid...	Defense Ev...	wininit.exe	True positi...	Crowdstrik...	True positive
High	16:14:28	wininit.exe on ID-031 by...	View incid...	Defense Ev...	wininit.exe	True positi...	Crowdstrik...	True positive
High	16:14:27	wininit.exe on ID-031 by...	View incid...	Defense Ev...	wininit.exe	True positi...	Crowdstrik...	True positive

Figure 6. Detection of persistence & privilege escalation on EDR.

Table 2. EDR detection log summary for May and June.

No	Severity	Tactic & Technique	Date	Host ID
1	High	Defense Evasion via Disable or Modify Security Tool	5/14/2025	ID-031
2	High	Defense Evasion via Disable or Modify Security Tool	5/14/2025	ID-031
3	High	Defense Evasion via Disable or Modify Security Tool	5/14/2025	ID-031
4	Informational	Execution via User Execution	5/14/2025	ID-031
5	Low	Malware via PUP	5/14/2025	ID-031
6	Medium	Machine Learning via Cloud-based Detection	5/14/2025	ID-031
7	Medium	Execution via Command and Scripting Interpreter	5/14/2025	ID-031
8	Medium	Execution via Command and Scripting Interpreter	5/14/2025	ID-031
9	High	Machine Learning via Cloud-based Detection	5/14/2025	ID-031
10	Low	Malware via PUP	5/14/2025	ID-031
11	High	Machine Learning via Cloud-based Detection	5/14/2025	ID-031
12	High	Machine Learning via Cloud-based Detection	5/14/2025	ID-031
13	Low	Malware via PUP	5/14/2025	ID-031
14	Low	Malware via PUP	5/14/2025	ID-031
15	Low	Malware via PUP	5/14/2025	ID-031
16	High	Machine Learning via Cloud-based Detection	5/14/2025	ID-031
17	High	Machine Learning via Cloud-based Detection	5/14/2025	ID-031
18	Low	Malware via PUP	6/18/2025	ID-033

4) Penetration Simulation: Command and Control (C2)
Command and Control (C2) is the phase in a cyberattack (particularly in APT attacks) when the compromised system communicates with the attacker's external infrastructure. The main objective is to provide remote control to the threat actor, enabling them to manage, monitor, and execute commands on the victim's system.

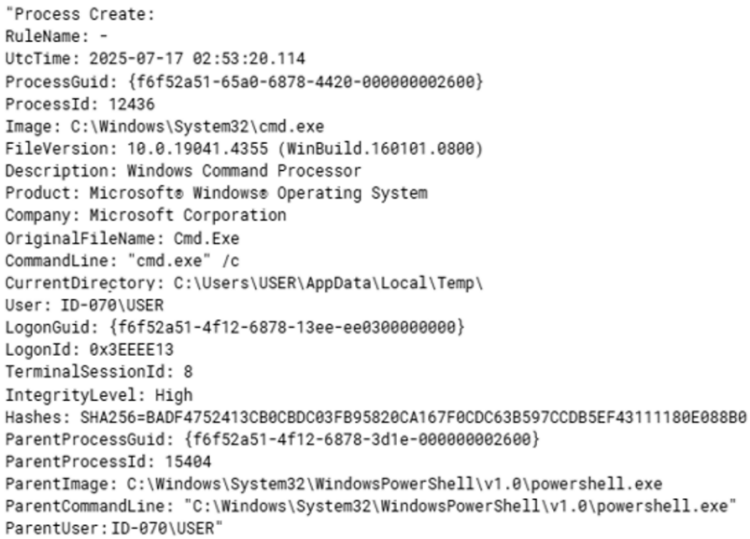


Figure 7. Custom beaconing attack detection from Wazuh.

5) Penetration Simulation: Data Exfiltration
Data Exfiltration is the process by which an attacker covertly steals and transmits data from a target system to an external location under their control. It represents one of the final stages of a cyberattack, typically carried out after the attacker has successfully gained access to the system and identified data deemed valuable.

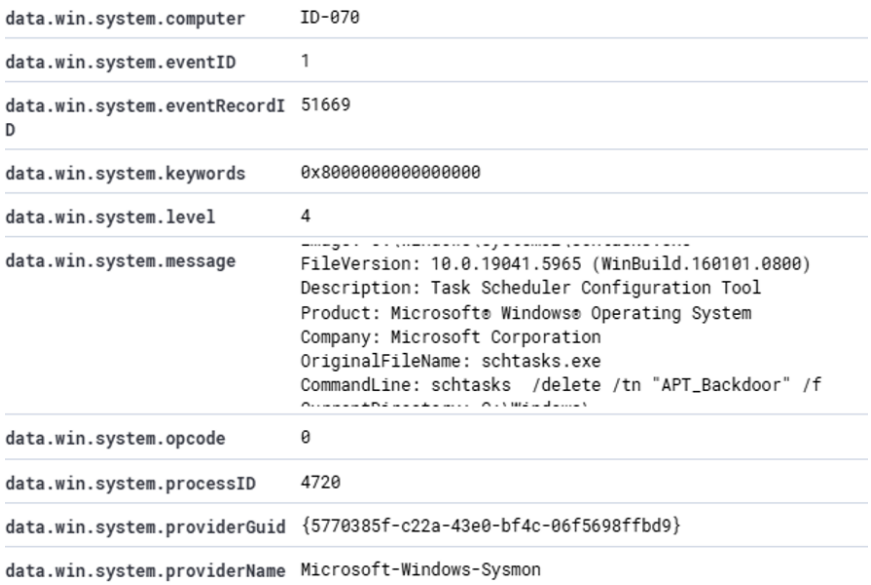


Figure 8. Data exfiltration detection from Wazuh.

4.1.4 Distribution Results of Attack Categories Based on MITRE ID

The testing results show that the Wazuh SIEM log data can detect attacks through the identification of attack contributions based on MITRE IDs.

Table 3. MITRE techniques log for June.

MITRE Techniques	Count
Modify Registry	24,112
File Deletion	12,033
Data Destruction	12,025
Stored Data Manipulation	7,151

Windows Command Shell	5,323
Account Discovery	4,039
Valid Accounts	2,555
Account Access Removal	2,360
Brute Force	318
Application Shimming	69
Domain Policy Modification	51
Domain Accounts	33
Remote Desktop Protocol	33
Pass the Hash	33
Disable or Modify Tools	22
PowerShell	13
Service Stop	7
Obfuscated Files or Information	6
System Shutdown/Reboot	5
Windows Service	4
Windows Management Instrumentation	1

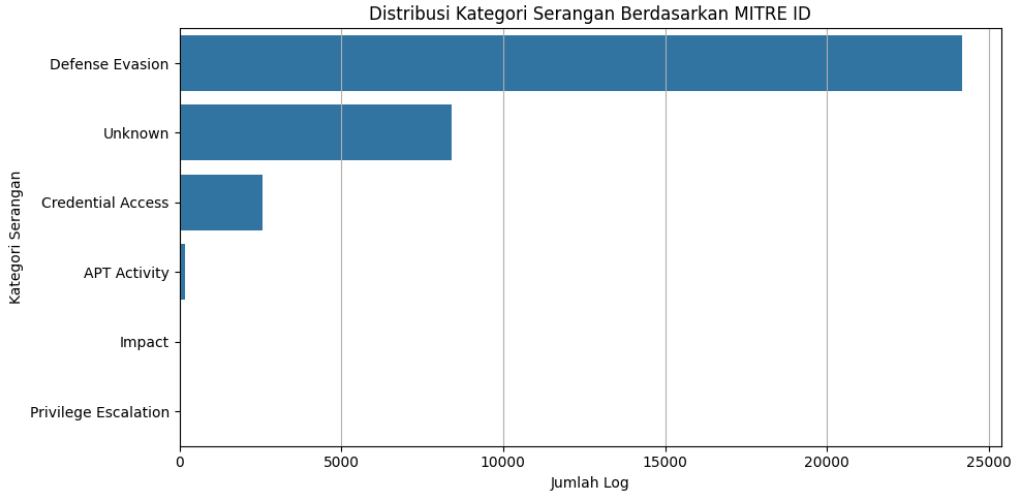


Figure 9. Distribution results of attack categories based on MITRE ID.

Further analysis of the attack distribution reveals distinct patterns in threat categorization. Table 4 presents the attack category distribution for June, highlighting the prevalence of specific attack types detected by the system.

Table 4. Attack category for June.

Attack Category	Count
Modify Registry	24,112
Defense Evasion	24,170
Unknown	8,424
Credential Access	2,555
APT Activity	173
Impact	7
Privilege Escalation	4

The evaluation results show that the attack prediction achieved a high level of accuracy in forecasting attacks based on the logs received by the Wazuh SIEM.

Table 5. Confusion matrix for attack prediction in June.

Matrix	Count
True Positive (TP)	1,060
True Negative (TN)	8,537
False Positive (FP)	563
False Negative (FN)	440

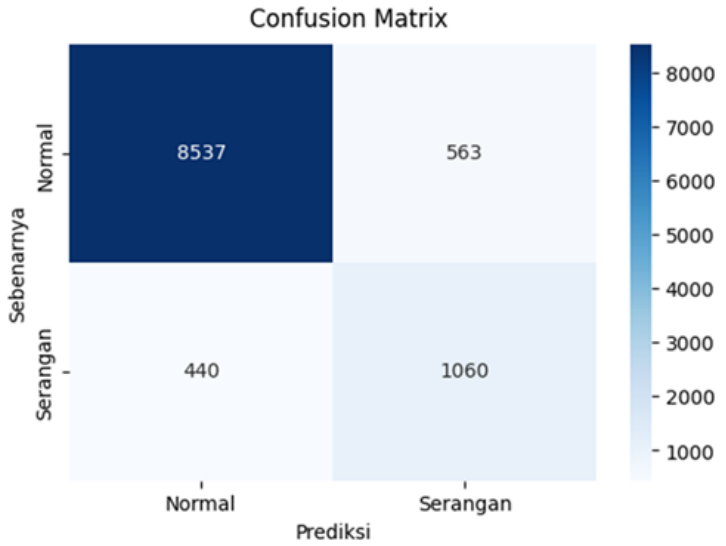


Figure 10. Confusion matrix for attack prediction in June.

Classification Report:

	precision	recall	f1-score	support
0	0.95	0.94	0.94	9100
1	0.65	0.71	0.68	1500
accuracy			0.91	10600
macro avg	0.80	0.82	0.81	10600
weighted avg	0.91	0.91	0.91	10600

Figure 11. Attack prediction results for June.

4.2 Discussion

As shown in Table 3, 173 logs were explicitly categorized as "APT Activity." The discrepancy between APT Activity (173) and Defense Evasion (24,170) represents the most prominent observation. Defense Evasion is a core MITRE ATT&CK tactic, frequently employed by APTs to evade detection. This strongly implies that Wazuh is detecting a high volume of activity consistent with APT behavior, but it is not classified under the specific "APT Activity" label. This indicates that the current rules for "APT Activity" are too narrow, or that the system lacks sophisticated multi-stage correlation capabilities to link individual tactical events (such as "Defense Evasion") into broader APT detection. This is a critical area for improvement. Given the low number of "APT Activity" detections and the high number of "Defense Evasion" and "Credential Access" logs, it is more beneficial to analyze the detection of tactics commonly used by APTs rather than relying on the generic "APT Activity" label. APTs achieve their objectives by identifying and exploiting existing system vulnerabilities, and Wazuh incorporates MITRE ATT&CK mapping. This suggests that Wazuh's strength in APT detection may lie more in its ability to identify specific TTPs (Tactics, Techniques, and Procedures) such as those under "Defense Evasion" or "Credential Access" which, when correlated, indicate an APT. This reframes the analysis from a simple count-based perspective to one of behavioral detection.

The performance data observed from Wazuh SIEM, particularly the number of False Positives (FP), False Negatives (FN), and the distribution of attack categories, provides critical insights when correlated with the known characteristics of APTs (stealth, persistence, and multi-stage nature). The high number of "Defense Evasion" logs (24,170), despite the relatively low number of "APT Activity" logs (173), indicates that Wazuh effectively detects tactics frequently employed by APTs, even if they are not explicitly classified as "APT." This suggests that Wazuh is capable of identifying individual components or tactics of APTs (such as defense evasion) rather than explicitly labeling the full attack chain as "APT Activity." This distinction highlights that while the system captures relevant indicators, higher-level classification rules or correlation mechanisms for full APT campaigns may require further refinement.The presence of 440 False Negatives (missed attacks) represents a significant vulnerability, particularly in the context of APTs, where even a single missed event can lead to severe and prolonged compromise. Since APTs are designed for long-term infiltration and data exfiltration, any undetected instance is likely to continue its operation, escalating privileges and moving laterally within the network. This underscores that although the overall accuracy (0.91) appears high, the

recall rate (0.71) for attack classes and the absolute number of FNs are the most critical metrics for APT defense, as they directly reflect the system's ability to capture these high-impact threats. The extremely low number of "APT Activity" logs (173) can be interpreted in two ways: either APTs are genuinely rare within the monitored environment, or, more concerningly, the current Wazuh configuration or rules are not optimized to identify the complete APT kill chain, allowing them to remain undetected or misclassified as less severe events. Given the stealthy and persistent nature of APTs, the latter explanation is highly plausible. This implies that while Wazuh is capable of detecting individual suspicious behaviors, it may lack the advanced correlation necessary to combine them into a recognizable APT narrative.

5. Conclusion and Recommendations

Advanced Persistent Threats are a high-level challenge in cybersecurity due to their complexity, continuity, and staged attack vectors designed to remain undetected and inflict damage over time. Intrusion Detection Systems and Security Information and Event Management play important roles in detection and response against such threats, with SIEM providing extensive log aggregation, advanced correlation, and behavioral analytics to reveal concealed activities of APTs. As an open-source SIEM/IDS platform [27], Wazuh has proven capabilities in log analysis, threat intelligence integration, and detection of attack patterns related to various APT tactics such as Defense Evasion and Credential Access. The performance data from June revealed high overall accuracy (0.91), primarily due to robust normal activity detection; however, further investigation indicated 440 false negatives (missed attacks) and lower performance on minority classes of attacks (recall 0.71), which is very critical within the context of high-impact APTs. The relatively small number of explicitly labeled "APT Activity" logs (173) as compared to the large volume for related APT tactics indicates a gap in multi-stage correlation for explicit APT classification. This gap highlights that Wazuh can detect individual APT tactics well but needs improvement in correlating these tactics into a full APT campaign. To improve Wazuh's effectiveness against APTs, continual enhancements in detection rules, advancements in behavioral analytics capabilities, and deeper integration of machine learning are necessary. More advanced APT-specific correlation rules should be created; alert triage should be optimized; deep learning for anomaly detection should be utilized [28][29]. Future research needs to bridge the practical implementation advancements with generalizability across different organizational contexts so that Wazuh may further improve its strength in resilience against an ever-evolving landscape of threats from APT.

Several recommendations follow from the results of this research in relation to improving PT XYZ's capability to detect APTs. Wazuh has shown a high level of accuracy (0.91); however, the large number of false negatives—440 undetected incidents—represents a critical security gap that needs attention at PT XYZ through rule tuning for better recognition of atypical patterns associated with an APT and development multi-stage correlation rules for staged tactics such as lateral movement, privilege escalation, and data exfiltration so that complete kill chains can be identified rather than isolated suspicious activities. Given the nature of APTs as dynamic and highly sophisticated threats, traditional systems may not be able to keep up with evolving attack techniques. Hence, integrating machine learning models—specifically deep learning—into anomaly-based detection is recommended for enhanced capabilities. Machine learning has the potential to discover subtle patterns and behavioral anomalies that a rule-based system would overlook, thereby minimizing false negatives and improving overall accuracy in detection. Furthermore, PT XYZ should leverage external threat intelligence feeds to enhance contextual information in logs analyzed by Wazuh [30]. Regular penetration testing and APT simulations should be performed at intervals to assess and continuously improve the effectiveness of detection, ensuring that the system stays robust against new threats. An interdisciplinary approach is very important for a complete defense against APTs. By combining methods from computer science with digital forensics, security policy, and psychology, this will give a better overall view of how APTs behave and what drives attackers. This kind of cross-discipline work should happen inside organizations to get access to real data and operational context, just like this study was done at PT XYZ. By mixing technical detection skills with smart threat intelligence and people-focused security practices, organizations can create stronger defenses against the ongoing and changing nature of APT attacks.

References

[1] Santoso, J. T., Hartono, B., Silalahi, F. D., & Muthohir, M. (2024). Transformers in cybersecurity: Advancing threat detection and response through machine learning architectures. *Journal of Technology Informatics and Engineering*, *3*(3), 382–396. https://doi.org/10.51903/jtie.v3i3.211

[2] Virkud, A., Inam, M. A., Riddle, A., Liu, J., Wang, G., & Bates, A. (2024). *How does endpoint detection use the MITRE ATT&CK framework?* https://www.usenix.org/conference/usenixsecurity24/presentation/virkud

[3] Artioli, P., Dentamaro, V., Galantucci, S., Magrì, A., Pellegrini, G., & Semeraro, G. (2025). SIEVE: Generating a cybersecurity log dataset collection for SIEM event classification. *Computer Networks*, *266*, 111330. https://doi.org/10.1016/j.comnet.2025.111330

[4] Lu, S., Chi, B., Zhou, T., Zhou, W., & Hu, H. (2025). STAE-APT: An APT detection method based on long-term behavioral features from provenance graphs. *2025 International Conference on Smart Computing and Artificial Intelligence Technology*, 1834–1841. https://doi.org/10.1109/iscait64916.2025.11010360

[5] Jang, S.-W., & Lee, Y.-J. (2023). A study on the APT attack scenario verification system. *Journal of the Korea Academia-Industrial Cooperation Society*, *24*(4), 610–615. https://doi.org/10.5762/kais.2023.24.4.610

[6] Mamun, A. Al, Al-Sahaf, H., Welch, I., & Camtepe, S. (2025). Genetic programming for enhanced detection of advanced persistent threats through feature construction. *Computers and Security*, *149*, 104185. https://doi.org/10.1016/j.cose.2024.104185

[7] Andronache, M.-M., Vulpe, A., & Burileanu, C. (2025). A comparative study of intrusion events in different SIEM systems. *2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI)*, 000065–000070. https://doi.org/10.1109/SAMI63904.2025.10883178

[8] Radoglou-Grammatikis, P., Sarigiannidis, P., Iturbe, E., Rios, E., Martinez, S., Sarigiannidis, A., Eftathopoulos, G., Spyridis, Y., Sesis, A., Vakakis, N., Tzovaras, D., Kafetzakis, E., Giannoulakis, I., Tzifas, M., Giannakoulias, A., Angelopoulos, M., & Ramos, F. (2021). SPEAR SIEM: A security information and event management system for the smart grid. *Computer Networks*, *193*, 108008. https://doi.org/10.1016/j.comnet.2021.108008

[9] Ayu, M. A., Erlangga, D., Mantoro, T., & Handayani, D. (2023). Enhancing security information and event management (SIEM) by incorporating machine learning for cyber attack detection. *2023 IEEE 9th International Conference on Computing, Engineering and Design, ICCED 2023*. https://doi.org/10.1109/ICCED60214.2023.10425288

[10] Nas, M., Ulfiah, F., Putri, U., Elektro, T., Negeri, P., & Pandang, U. (2023). Analisis sistem security information and event management (SIEM) aplikasi Wazuh pada Dinas Komunikasi Informatika Statistik dan Persandian Sulawesi Selatan. *Jurnal Teknologi Elekterika*, *20*(2). https://doi.org/10.31963/elekterika.v20i2.4536

[11] Vazão, A. P., Santos, L., Costa, R. L. de C., & Rabadão, C. (2023). Implementing and evaluating a GDPR-compliant open-source SIEM solution. *Journal of Information Security and Applications*, *75*, 103509. https://doi.org/10.1016/j.jisa.2023.103509

[12] Ahmad, S., Ahn, B., Alvee, S. R. B., Trevino, D., Kim, T., Youn, Y. W., & Ryu, M. H. (2022, April). Advanced persistent threat (APT)-style attack modeling and testbed for power transformer diagnosis system in a substation. *2022 IEEE Power and Energy Society Innovative Smart Grid Technologies Conference, ISGT 2022*. https://doi.org/10.1109/ISGT50606.2022

[13] Karim, S. S., Afzal, M., Iqbal, W., & Al Abri, D. (2024). *Advanced persistent threat (APT) and intrusion detection evaluation dataset for Linux systems 2024*. https://doi.org/10.17632/5x68fv63sh.2

[14] Park, N. E., Lee, Y. R., Joo, S., Kim, S. Y., Kim, S. H., Park, J. Y., Kim, S. Y., & Lee, I. G. (2023). Performance evaluation of a fast and efficient intrusion detection framework for advanced persistent threat-based cyberattacks. *Computers and Electrical Engineering*, *105*, 108548. https://doi.org/10.1016/j.compeleceng.2022.108548

[15] Sheng, C., & Gang, C. (2024). APT attack and detection technology. *IMCEC 2024 - IEEE 6th Advanced Information Management, Communicates, Electronic and Automation Control Conference*, 795–801. https://doi.org/10.1109/IMCEC59810.2024.10575432

[16] Ward, A. M., Bohacek, S., & Phillips, J. (2024). An evaluation study of endpoint detection and response systems across multi-vector attack scenarios. *Eastern-European Journal of Enterprise Technologies*, *2*(9), 182–191. https://doi.org/10.30837/2522-9818.2024.2.182

[17] Alexopoulos, A., & Daras, N. J. (2020). Mathematical study of advanced persistent threat (APT) hunting techniques. *Journal of Computations & Modelling*, *10*(2), 1–24. https://doi.org/10.47260/jcomod/1021

[18] Cheng, S. M., Lui, Y. C., Tsai, N. J., & Hong, B. K. (2024). Toward intelligent IoT endpoint detection and response using digital twins via firmware emulation. *IEEE Internet of Things Magazine*, *7*(6), 20–26. https://doi.org/10.1109/IOTM.001.2400070

[19] Gulbay, B., & Demirci, M. (2024). APT-scope: A novel framework to predict advanced persistent threat groups from enriched heterogeneous information network of cyber threat intelligence. *Engineering Science and Technology, an International Journal*, *57*, 101791. https://doi.org/10.1016/j.jestch.2024.101791

[20] Mahmoud, R. V., Anagnostopoulos, M., Pastrana, S., & Pedersen, J. M. (2024). Redefining malware sandboxing: Enhancing analysis through Sysmon and ELK integration. *IEEE Access*, *12*, 68624–68636. https://doi.org/10.1109/ACCESS.2024.3400167

[21] Muhammad, A. R., Sukarno, P., & Wardana, A. A. (2022). Integrated security information and event management (SIEM) with intrusion detection system (IDS) for live analysis based on machine learning. *Procedia Computer Science*, *217*, 1406–1415. https://doi.org/10.1016/j.procs.2022.12.339

[22] Artioli, P., Dentamaro, V., Galantucci, S., Magrì, A., Pellegrini, G., & Semeraro, G. (2025). SIEVE: Generating a cybersecurity log dataset collection for SIEM event classification. *Computer Networks*, *266*, 111330. https://doi.org/10.1016/j.comnet.2025.111330

[23] Chi, C. H., Ooi, S. Y., Binti, E. H., Pang, Y. H., Yan, M. K. B. A., & Sidin, K. I. B. (2023). Intelligent-based SIEM security email alert. *2023 11th International Conference on Information and Communication Technology, ICoICT 2023*, 481–486. https://doi.org/10.1109/ICoICT58202.2023.10262562

[24] Esseghir, A., Kamoun, F., & Hraiech, O. (2022). AKER: An open-source security platform integrating IDS and SIEM functions with encrypted traffic analytic capability. *Journal of Cyber Security Technology*, *6*(1–2), 27–64. https://doi.org/10.1080/23742917.2022.2058836

[25] Sinaga, Y. Y. (2024). *Analisis security information and event management (SIEM) berbasis Wazuh dalam mendeteksi malicious software pada sistem operasi Linux*. Universitas Sumatera Utara. https://repositori.usu.ac.id/handle/123456789/96053

[26] Cheng, S. M., Lui, Y. C., Tsai, N. J., & Hong, B. K. (2024). Toward intelligent IoT endpoint detection and response using digital twins via firmware emulation. *IEEE Internet of Things Magazine*, *7*(6), 20–26. https://doi.org/10.1109/IOTM.001.2400070

[27] Amami, R., Charfeddine, M., & Masmoudi, S. (2024). Exploration of open source SIEM tools and deployment of an appropriate Wazuh-based solution for strengthening cyberdefense. *10th 2024 International Conference on Control, Decision and Information Technologies, CoDIT 2024*, 2139–2145. https://doi.org/10.1109/CoDIT62066.2024.10708476

[28] Tharunika, V. S., Shridhar, T., Veeresh, K., Thangavel, S. K., Srinivasan, K., Vajipayajula, S., & Tibrewal, A. (2023). Detection and prevention of advanced persistent threat (APT) activities in heterogeneous networks using SIEM and deep learning. *2023 14th International Conference on Computing Communication and Networking Technologies, ICCCNT 2023*. https://doi.org/10.1109/ICCCNT56998.2023.10306968

[29] Saeed, N., Yaqub, M., Haider, A., Secureworks, D., Safdar, S., & Khan, H. (2025). An enhanced mechanism for advanced persistent threat (APT) detection based on deep learning. *Spectrum of Engineering Sciences*, *3*(1), 48–62. https://sesjournal.com/index.php/1/article/view/118

[30] Ren, W., Song, X., Hong, Y., Lei, Y., Yao, J., Du, Y., & Li, W. (2023). APT attack detection based on graph convolutional neural networks. *International Journal of Computational Intelligence Systems*, *16*(1), 168. https://doi.org/10.1007/s44196-023-00369-5