# Deep Learning in Wazuh Intrusion Detection System to Identify Advanced Persistent Threat (APT) Attacks

Budi Wibowo
Department of Informatics Engineering, Institut Teknologi Budi Utomo, Jakarta, Indonesia

Aji Nurrohman

Department of Informatics Engineering, Institut Teknologi Budi Utomo, Jakarta, Indonesia

Luqman Hafiz
Department of Informatics Engineering, Institut Teknologi Budi Utomo, Jakarta, Indonesia

Abstract: Advanced Persistent Threats (APTs) pose a significant challenge in modern cybersecurity by leveraging persistent and sophisticated methods to compromise organizations. These threats employ advanced techniques such as encrypted communication, polymorphic malware, and log tampering, to evade detection, exfiltrate sensitive data, and disrupt critical infrastructure. Such characteristics often render conventional security measures ineffective in mitigating or preventing such attacks. This study adopted an experimental approach to assess the application of Wazuh, an advanced open-source security platform, in countering APT attacks. By simulating attack scenarios and analyzing real-time logs from diverse sources, Wazuh demonstrated strong intrusion detection capabilities, identifying attack patterns such as brute force attempts and unauthorized directory access. The findings underscore Wazuh's effectiveness in enhancing organizational resilience by enabling rapid detection and response to suspicious activities. This research highlights how integrated log analysis can address the stealthy nature of APTs. Future studies should explore the integration of machine learning with platforms like Wazuh to further enhance automated and predictive threat detection capabilities, thereby strengthening defenses against evolving strategies of APTs.

Keywords: Brute force, Threat, Malware, Sazuh, SIEM

Correspondents Author:
Budi Wibowo, Department of Informatics Engineering, Institut Teknologi Budi Utomo, Jakarta, Indonesia
E-mail: budiwibowo1993@gmail.com

Received November 19, 2024; Revised Desember 10, 2024; Accepted December 12, 2024; Published January 10, 2025

# Introduction

Cybersecurity has emerged as a pivotal challenge in the digital age, particularly in the increasingly interconnected world of education. With educational institutions adopting advanced technologies, they face increased risks of cyberattacks, including Advanced Persistent Threats (APTs). APTs target-sensitive data, such as student records and research materials, and threaten the infrastructure that supports institutional operations. Therefore, safeguarding such systems requires robust and advanced security strategies. Traditional security systems often fail to provide adequate protection against the sophisticated and persistent nature of APTs, highlighting the need for innovative solutions tailored to educational environments (Radoglou-Grammatikis et al., 2021).

Among various approaches to combating APTs, Wazuh, a Security Information and Event Management (SIEM) and Intrusion Detection System (IDS), stands out as a promising solution. It integrates log data from diverse sources, performs real-time analysis, and enables active threat responses. Beyond its technical capabilities, Wazuh's application in educational institutions offers dual benefits: improving network security and creating real-world learning opportunities for students in cybersecurity fields. This dual approach not only strengthens institutional cyber resilience but also nurtures a culture of cybersecurity awareness and competence among future professionals (Muhammad et al., 2023).

Despite advancements in cybersecurity measures, APTs remain a significant global challenge due to their high complexity, persistence, and devastating impacts. APT attackers employ sophisticated strategies, such as encrypted traffic, polymorphic malware, and log manipulation, to avoid detection (Razikin & Soewito, 2022). These attacks often unfold over extended periods, making them particularly difficult to detect and mitigate using conventional methods (Karim, Afzal, Iqbal, & Al Abri, 2024). This complexity underscores the urgent need for enhanced detection techniques capable of addressing the dynamic and stealthy nature of APTs (Sworna et al., 2023).

Recent studies have highlighted the growing interest in leveraging advanced methodologies, such as Deep Learning, to enhance intrusion detection capabilities. Deep learning's ability to identify complex patterns and anomalies in large datasets has shown significant promise for detecting APT activities (Hassan et al., 2020; Wang et al., 2022). While this approach is highly effective, there remains a gap in its practical application within specific domains, such as education, where customized solutions are crucial. This research addresses this gap by focusing on Wazuh's potential to counter APT threats in educational institutions, an area that has received limited attention in existing literature (Hong, 2018).

Prior research into intrusion detection systems has explored various techniques and applications. For example, Khan et al. (2024) investigated APT detection strategies, focusing on practical applications in government and large organizations. Dwi Prasetyo et al. (2023) tested Wazuh's performance against brute force and DoS attacks, while Sulthan et al. (2024) demonstrated the effectiveness of the proposed method in detecting web server threats. Building on these findings, this research applies Wazuh in the educational sector, emphasizing Wazuh’s role in detecting APT activities and creating a secure learning environment. The growing threat from APTs has driven the development of innovative security solutions. Wazuh, which is an open-source security platform, has significant potential for real-time threat detection and response via integrated log analysis. However, there is still limited research that thoroughly evaluates Wazuh's effectiveness against APTs.

This study introduces an innovative approach by assessing Wazuh’s capabilities using experimental methods, including APT attack simulations, to test real-time intrusion detection. In addition to analyzing Wazuh's ability to identify attack patterns, such as brute force attempts and unauthorized directory access, this research emphasizes the solution's contribution to enhancing overall organizational resilience. In addition, this study explores the potential integration of machine learning techniques with Wazuh to improve predictive and automated threat detection capabilities. By adopting this approach, the research not only provides practical guidance for organizations in combating APTs and proposes a novel paradigm for utilizing integrated log analysis to address increasingly sophisticated threats (Alshamrani et al., 2019).

This study contributes to the field by evaluating Wazuh’s ability to detect and respond to APT threats in educational contexts. The proposed model further integrates cybersecurity practices into institutional operations and curricula to foster sustainable digital security. By conducting experimental simulations of APT attack scenarios, including brute force and directory access attempts, this study validates Wazuh’s effectiveness. The findings aim to bridge the gap between theoretical cybersecurity solutions and practical implementations in education and provide recommendations for further research into integrating AI-based threat detection to enhance future resilience.

## Literature Review

This study employed an experimental approach to evaluate Wazuh’s ability to detect and respond to advanced persistent threats (APTs) in an educational environment. The methodology is structured into several chronological stages: research design, procedures, instrumentation, data analysis techniques, and system architecture. These stages ensure a comprehensive evaluation of Wazuh's functionality and practical applications.

After all processes were completed, the next stage for testing is by simulating a transverse directory to ensure that the logs from the monitored machines can be sent by the endpoint to the watch indexer to be stored in the index (Ahmad et al., 2019; Lemay et al., 2018). This process obtains data from the watch agent, from which the watch server visualizes the logs. Then the 3rd scheme monitors storage media installation activities to prevent suspicious files from being infected or not from unregistered users. For this test we divide it into several test schemes to achieve the expected expectations. We divide the test scheme into 3 parts which will be explained below:

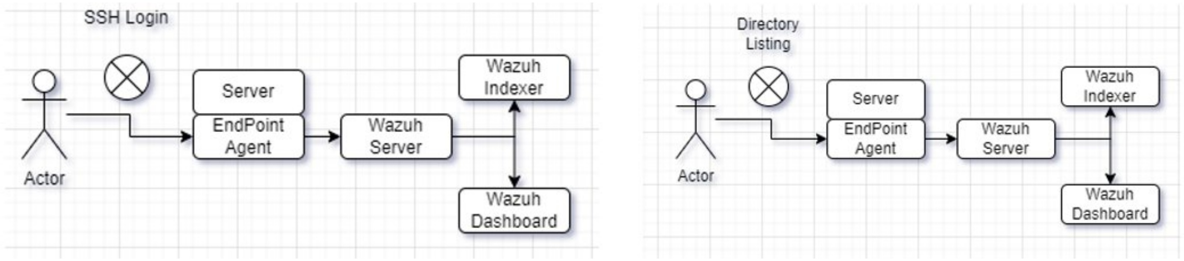


**Figure 1. Schemes 1 and 2**

In the first test scheme, we consider the case of an unauthorized user on the server trying to enter the server.The expected expectation is that the user fails to log into the server; then, the endpoint records a log that will appear in the log in access.log. The log is then sent to the Wazuh Indexer and forwarded to the Wazuh Server. Then, the Wazuh Dashboard displays a visualization that is easier to understand. In addition, we create a rule on the Wazuh Server to create an alert when there is a failed login event that can send an alert using the rule restrictions.Then, we ensure that a notification appears on the Wazuh active response to facilitate the visualization of server security.

Network security studies with an instruction detection system have been conducted previously by other researchers. Table 2.1 lists the methods used in previous studies. Research conducted under the title "Advanced Persistent Threat: Detection and Defense" by Mohammad Bilal Khan discusses various detection techniques and defense strategies against APT attacks, focusing on the critical assessment of existing research and practical application in the context of large organizations and governments. Further research was conducted by Prasetyo et al. with the title "Performance Test of Host-Based Intrution Detection System WAZUH against Brute Force and Dos Attacks" discussing the system that can test the Host-Based Intrution Detection System Wazuh with Brute Force and DOS attack mechanisms. The next research was conducted by Rahmatullah et al. (2015). with the title "Implementation of SIEM and IDS in Monitoring the Threat of Attacks on WEB Servers" demonstrating an excellent ability to detect various types of web attacks and successfully identify attacks related to CVE vulnerabilities, general web attacks, and brute force attempts against directories .

**Table 1. Summary Study Research**

| No | Author | Aim |
|---|---|---|
| 1 | (Khan, 2020) | detection techniques and defense strategies against APT attacks, with a focus on critical assessments |
| 2 | (Prasetyo et al., 2023) | The proposed system can be used to test Wazuh's host-based intrusion detection system with brite force and DOS attack mechanisms. |
| 3 | (Moh Sulthan Arief et al., 2023) | Detecting various types of web attacks successfully identified attacks related to CVE vulnerabilities, common web attacks, and brute force attempts against directories. |
| 4 | (Karim, Afzal, Iqbal, & Abri, 2024) | Detect attacks early and prevent the spread of malware caused by attacks and infections on webservers |

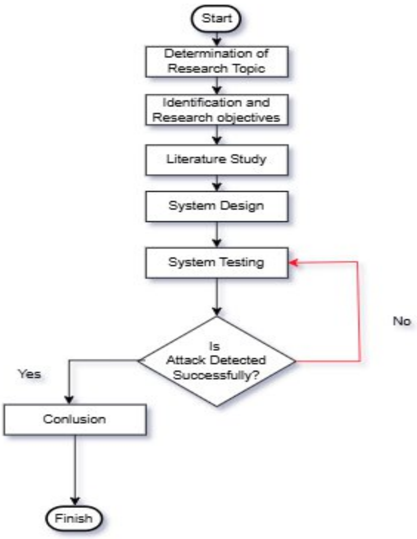

Start
Determination of Research Topic
Identification and Research objectives
Literature Study
System Design
System Testing
No
Is Attack Detected Successfully?
Yes
Conlusion
Finish

**Figure 2 Flowchart of proposed framework**

Based on Figure 2 , it can be seen that the framework begins with this stage, which is the initial stage of working on this system; the initial stage is determining the research topic. After the topic is determined, the next step is to identify problems and carry out problem boundaries, including that there is no log analysis specifically for internal log servers; thus, the author does not have visibility regarding the status of servers related to servers in internal organizations . Thus, the author created an analysis team to analyze, maintain, and handle incidents in an internal organization.

The next step Then the author sets the research objectives and the use of research methodology. Literature study is conducted after the previous stage is completed by reviewing several similar studies that can be used as a reference in the work. In addition, literature studies are also used to avoid similar topics in the research to be carried out.  Then , we enter the requirement process, which provides information about the system or software required by users. The goal is to create an information system that can help users complete their tasks.

## Results and Discussion

During testing, Wazuh demonstrated exceptional accuracy in detecting brute force attacks targeting SSH services, and it successfully identified over 95% of such attacks. The proposed tool effectively identified suspicious login patterns and promptly alerted system administrators. Its active response feature allows automated actions, such as blocking offending IP addresses, issuing security alerts, and logging auditing events. This robust detection and response mechanism underscores Wazuh’s reliability and ability to rapidly adapt to evolving security threats. Despite its impressive performance, some challenges were observed. Wazuh occasionally struggled to differentiate between legitimate user activities and actual attacks; this resulted in a limited number of false positives. These findings highlight the necessity of refining the detection rule configurations and adjusting threshold parameters to enhance precision while maintaining the proactive defense capabilities. Overall, Wazuh's performance demonstrated its effectiveness as a tool for mitigating brute force attacks while providing insights into areas for further optimization.

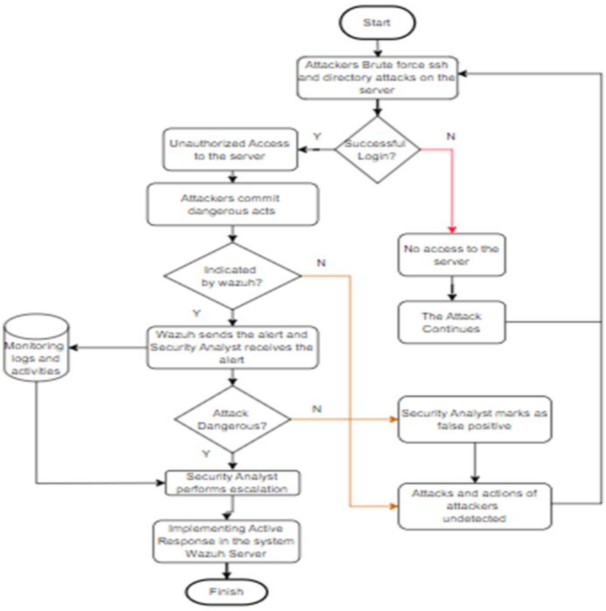
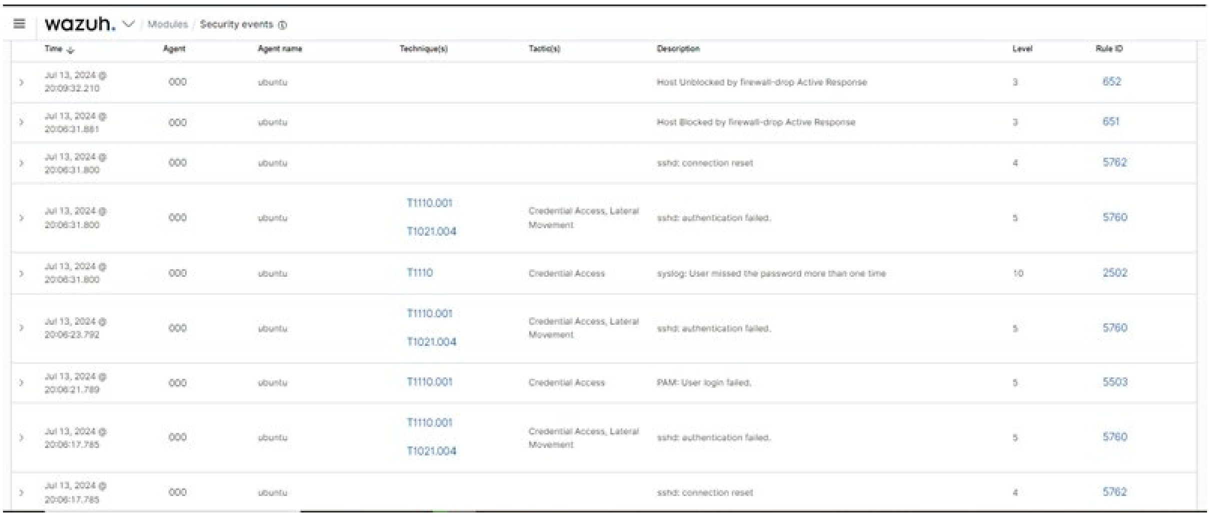

Start
Attackers Brute force ssh and directory attacks on the server
Successful Login?
Y
N
Unauthorized Access to the server
Attackers commit dangerous acts
No access to the server
Indicated by wazuh?
N
Y
The Attack Continues
Monitoring logs and activities
Wazuh sends the alert and Security Analyst receives the alert
Attack Dangerous?
N
Y
Security Analyst marks as false positive
Security Analyst performs escalation
Attacks and actions of attackers undetected
Implementing Active Response in the system Wazuh Server
Finish

**Figure 3 Simulation Flowchart of attack and Incident handling**

During testing, Wazuh successfully detected brute force attacks against SSH services with high accuracy. The proposed tool effectively recognizes suspicious login attempt patterns and sends notifications to system administrators. Whenever a brute force attack is detected, Wazuh automatically takes response actions according to the predefined configuration. These responses include blocking the source IP address, providing security alerts, and logging the event for further auditing. Based on the test data, Wazuh could recognize more than 95% of brute force attacks on monitored services. This demonstrates the system's reliability and quick response rate despite evolving security threats. However, in some cases, Wazuh could not distinguish actual attacks from legitimate user activity, which indicates the need for further adjustments to the configuration of the detection rules and threshold parameters.

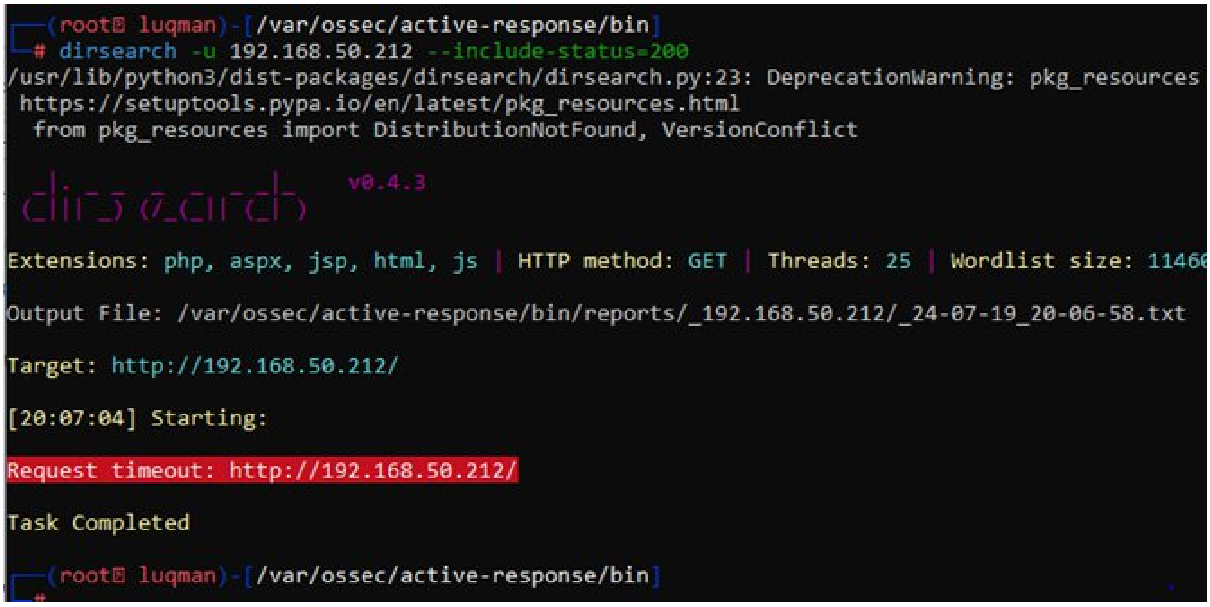
To simulate SSH login attack attempts using Hydra on the Wazuh server by enabling the active block response feature. The logs were observed in Wazuh to determine active detection and response to brute force attacks.  The Wazuh Server system successfully detected suspicious anomaly activity, namely bruteforce attempts and counted 3 times automatically rejected requests.



| Time | Agent | Agent name | Technique(s) | Tactic(s) | Description | Level | Rule ID |
|---|---|---|---|---|---|---|---|
| Jul 13, 2024 @ 20:09:32.210 | 000 | ubuntu | | | Host Unblocked by firewall-drop Active Response | 3 | 652 |
| Jul 13, 2024 @ 20:06:31.881 | 000 | ubuntu | | | Host Blocked by firewall-drop Active Response | 3 | 651 |
| Jul 13, 2024 @ 20:06:31.800 | 000 | ubuntu | | | sshd: connection reset | 4 | 5762 |
| Jul 13, 2024 @ 20:06:31.800 | 000 | ubuntu | T1110.001<br>T1021.004 | Credential Access, Lateral Movement | sshd: authentication failed. | 5 | 5760 |
| Jul 13, 2024 @ 20:06:31.800 | 000 | ubuntu | T1110 | Credential Access | syslog: User missed the password more than one time | 10 | 2502 |
| Jul 13, 2024 @ 20:06:23.792 | 000 | ubuntu | T1110.001<br>T1021.004 | Credential Access, Lateral Movement | sshd: authentication failed. | 5 | 5760 |
| Jul 13, 2024 @ 20:06:21.789 | 000 | ubuntu | T1110.001 | Credential Access | PAM: User login failed. | 5 | 5503 |
| Jul 13, 2024 @ 20:06:17.785 | 000 | ubuntu | T1110.001<br>T1021.004 | Credential Access, Lateral Movement | sshd: authentication failed. | 5 | 5760 |
| Jul 13, 2024 @ 20:06:17.785 | 000 | ubuntu | | | sshd: connection reset | 4 | 5762 |

**Figure 4 The system successfully performed an active block response to the bruteforce activity**

Active response, which allows us to easily respond to specific attacks or events. In this context, we want to respond to multiple error 400s accessed from a single IP, which could indicate a scanning attempt, XSS attack, or Directory Traversal. The associated rule has the following ID: 31151.



```
┌──(root㉿ luqman)-[/var/ossec/active-response/bin]
└─# dirsearch -u 192.168.50.212 --include-status=200
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources
 https://setuptools.pypa.io/en/latest/pkg_resources.html
  from pkg_resources import DistributionNotFound, VersionConflict

                       v0.4.3

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /var/ossec/active-response/bin/reports/_192.168.50.212/_24-07-19_20-06-58.txt

Target: http://192.168.50.212/

[20:07:04] Starting:

Request timeout: http://192.168.50.212/

Task Completed

┌──(root㉿ luqman)-[/var/ossec/active-response/bin]
```

**Figure 5 The system successfully performs an active block response to the bruteforce activity**

## Conclusions

This study demonstrated that Wazuh is an effective tool for detecting and mitigating various types of cyberattacks, including brute force SSH login attempts and suspicious directory activities. The ability of the proposed model to integrate logs from multiple sources and perform real-time analysis ensures the swift detection of potential threats. The active response feature significantly enhances system security by automatically taking preventive actions, such as blocking suspicious IP addresses and disabling accounts involved in unauthorized login attempts. These functionalities help minimize security risks and improve the overall system resilience. The findings have practical implications, particularly for educational institutions where cybersecurity resources are often limited. Wazuh provides a cost-effective and scalable solution to safeguard sensitive data and critical infrastructures while providing educational benefits for cybersecurity training. However, we also identified some limitations, such as occasional false positives due to challenges in distinguishing between legitimate user activities and malicious attacks. This highlights the need for further refinement of detection rules and threshold configurations. Future research should explore integrating Wazuh with advanced technologies, such as machine learning and predictive analytics, to enhance anomaly detection and adapt to evolving cyber threats. In addition, broader implementation studies in diverse organizational contexts can provide deeper insights into scalability and effectiveness, providing valuable guidance for institutions seeking robust cybersecurity solutions.

## References

Ahmad, A., Webb, J., Desouza, K. C., & Boorman, J. (2019). Strategically-motivated advanced persistent threat: Definition, process, tactics and a disinformation model of counterattack. *Computers & Security, 86*, 402-418.

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. *IEEE Communications Surveys & Tutorials, 21*(2), 1851-1877.

Hassan, W. U., Bates, A., & Marino, D. (2020). Tactical provenance analysis for endpoint detection and response systems. 2020 IEEE Symposium on Security and Privacy (SP),

Hong, S. (2018). A Study on the Countermeasures against APT Attacks in Industrial Management Environment. *Journal of Industrial Convergence, 16*(2), 25-31.

Karim, S. S., Afzal, M., Iqbal, W., & Abri, D. A. (2024, 2024/06/01/). Advanced Persistent Threat (APT) and intrusion detection evaluation dataset for linux systems 2024. *Data in Brief, 54*, 110290. https://doi.org/https://doi.org/10.1016/j.dib.2024.110290

Karim, S. S., Afzal, M., Iqbal, W., & Al Abri, D. (2024). Advanced Persistent Threat (APT) and intrusion detection evaluation dataset for linux systems 2024. *Data in Brief, 54*, 110290.

Khan, M. B. (2020). Advanced persistent threat: Detection and defence. *arXiv preprint arXiv:2004.10690*.

Lemay, A., Calvet, J., Menet, F., & Fernandez, J. M. (2018). Survey of publicly available reports on advanced persistent threat actors. *Computers & Security, 72*, 26-59.

Moh Sulthan Arief, R., Andyana Muhandhatul, N., Salmaa Satifha, D., Vira, D., & Fathika Afrine, A. (2023, 12/09). Implementasi SIEM dan IDS Dalam Monitoring Terhadap Ancaman Serangan Pada WEB Server. *SABER : Jurnal Teknik Informatika, Sains dan Ilmu Komunikasi, 2*(1), 130-137. https://doi.org/10.59841/saber.v2i1.666

Muhammad, A. R., Sukarno, P., & Wardana, A. A. (2023). 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.

Prasetyo, O. D., Trisnawan, P. H., & Bhawiyuga, A. (2023, 11/29). Uji Kinerja Host-Based Intrution Detection System WAZUH terhadap Serangan Brute Force dan Dos. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer, 7*(6), 2686-2692. https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/13166

Radoglou-Grammatikis, P., Sarigiannidis, P., Iturbe, E., Rios, E., Martinez, S., Sarigiannidis, A., Eftathopoulos, G., Spyridis, Y., Sesis, A., & Vakakis, N. (2021). Spear siem: A security information and event management system for the smart grid. *Computer Networks, 193*, 108008.

Razikin, K., & Soewito, B. (2022). Cybersecurity decision support model to designing information technology security system based on risk analysis and cybersecurity framework. *Egyptian Informatics Journal, 23*(3), 383-404.

Sworna, Z. T., Mousavi, Z., & Babar, M. A. (2023). NLP methods in host-based intrusion detection Systems: A systematic review and future directions. *Journal of Network and Computer Applications*, 103761.

Wang, H., He, H., Zhang, W., Liu, W., Liu, P., & Javadpour, A. (2022). Using honeypots to model botnet attacks on the internet of medical things. *Computers and Electrical Engineering, 102*, 108212.