GIJES
Greenation International Journal of Engineering Science
+62 81210467572 https://research.e-greenation.org/GIJES greenation.info@gmail.com
GREENATION RESEARCH

DOI: https://doi.org/10.38035/gijes.v3i3
https://creativecommons.org/licenses/by/4.0/

Analysis of the Effectiveness of Security Information and Event Management (SIEM) Detection Against Advanced Threats

Dilla Ghaisani Putri[1]
[1]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, dillaputri523@gmail.com

Corresponding Author: dillaputri523@gmail.com[1]

Abstract: Advanced Persistent Threats (APTs) pose a serious challenge to information systems security. APTs employ complex and persistent techniques to achieve their goal of infiltrating an organization's network. APTs often operate undetected for prolonged periods, which can last months or even years. The combination of intricate techniques and long-term persistence is what makes APTs so difficult to detect and counter. Security Information and Event Management (SIEM) is a type of security solution used for cyber threat detection and response. This research analyzed the effectiveness of SIEM in detecting APTs based on parameters such as detection speed, accuracy, and false positive rate. Simulations of repeated attacks demonstrate that SIEM expands security visibility and enhances the network's ability to respond to attacks rapidly. However, large log volumes present a challenge to the entire system, and optimal configuration incurs a high cost for such analysis.

Keyword: SIEM, Advanced Threat Detection, APT, Cybersecurity.

INTRODUCTION

Problem Background

In the digital age, information security has become critical as cyber threats grow increasingly complex, including *Advanced Persistent Threats (APT)*—targeted, sustained, and hard-to-detect attacks aimed at stealing data or compromising systems. To address these threats, organizations require advanced technologies such as *Security Information and Event Management (SIEM)*.

SIEM is a system that collects, analyzes, and manages security data to automatically detect and respond to threats. With the support of data analysis and AI, *SIEM* can identify suspicious activities such as *APTs*, reduce false positives, and help security teams focus on truly dangerous threats.

Given this situation, the purpose of this article is to develop hypotheses that can be used for future research, specifically to formulate: 1). Explain the concept and functions of *SIEM* in *APT* detection and response; 2). Evaluate the effectiveness *of SIEM* against *APT* threats; 3). Analyze the role *of SIEM* in improving security response; 4). Examine the utilization *of SIEM* in the industry and its challenges; 5).

Provide recommendations *for SIEM* optimization.

METHOD

Library Research and Systematic Literature Review (SLR) were used to write this Literature Review article. For qualitative analysis, web-based academic applications such as Google Scholar and Mendeley were utilized. The process of identifying, evaluating, and understanding all available research evidence to answer specific research questions is known as a systematic literature review (SLR) (Kitchenham et al., 2009). According to Ali et al. (2013), a literature review must be conducted consistently with the methodological assumptions of qualitative analysis. This method was chosen because this study is exploratory in nature.

RESULT AND DISCUSSION

Result

Considering the background, objectives, and methods discussed in this article, the results are as follows.

Information System Security

Information Security is the effort to protect information assets from various threats to maintain organizational operational continuity, reduce risks, and enhance value and trust in business activities (Susanto, 2020). Its core principles include confidentiality, integrity, and availability *(CIA)* as the foundation for maintaining information security (Rahayu & Prasetyo, 2021). Additionally, information privacy is a critical aspect encompassing individuals' rights

to personal data, the ability to control data usage, and restrictions on access to such information (Nugroho, 2022).

In its implementation, information security encompasses various interconnected aspects, ranging from physical protection of assets, environments, and facilities against risks such as disasters or unauthorized access, to the protection of individuals involved in the organization (Wibowo & Santoso, 2021). Furthermore, operational security plays a role in ensuring that all business processes run safely and under control (Hidayat, 2020).

Protection is also applied to communication systems and media to maintain the confidentiality and integrity of transmitted information (Pratama, 2021). Equally important, network security focuses on protecting network infrastructure and the data flowing through it to keep it safe from cyber threats (Kurniawan & Firmansyah, 2022). With this comprehensive approach, organizations can minimize potential disruptions and maintain the stability and continuity of information systems (Setiawan & Maghfiroh, 2022).

Definition and Characteristic of Advance Threats (APT Zero-Day Exploit)

An Advanced Persistent Threat (APT) is a sophisticated, targeted cyberattack that persists over an extended period, during which the attacker gains unauthorized access to a network and remains undetected (Chen & Hutchins, 2014). These attacks typically aim to steal sensitive data, monitor activities, or damage systems, with primary targets such as government agencies, the military, and large corporations (Rid & Buchanan, 2015).

APTs are characterized by specific targets, a persistent nature due to their ability to remain in a system for an extended period, and a multi-stage attack pattern that includes reconnaissance, infiltration via techniques such as spear phishing, establishing

a foothold, data exfiltration, and maintaining a presence (Hutchins, Cloppert, & Amin, 2011). Additionally, *APTs* utilize advanced techniques such as zero-day exploits—security vulnerabilities that are unknown and unpatched—allowing attackers to gain entry undetected (Bilge & Dumitras, 2012).

These attacks are typically carried out by organized groups or state-sponsored actors with strategic objectives, whether economic, political, or military (Rid & Buchanan, 2015). In practice, *zero-day exploits* are often used to infiltrate systems, plant malware such as *Remote Access Trojans (RATs)*, and achieve objectives before security systems are updated (Bilge & Dumitras, 2012).

Security Information and Event Management (SIEM)

SIEM (Security Information and Event Management) is a critical technology in information security that integrates the collection, analysis, and reporting of log data from various sources to detect and respond to threats in real-time (Bhatt et al., 2014). By combining log management and event correlation, *SIEM* is capable of monitoring system activity, identifying threats, and providing a rapid response to security incidents (Miloslavskaya & Tolstoy, 2016).

SIEM operates by collecting and analyzing logs to identify patterns or anomalies and generate decision-support reports (Chuvakin, Schmidt, & Phillips, 2013). Key functions *of SIEM* include centralized log collection, data correlation, and reporting for regulatory compliance, thereby aiding in the detection of threats within complex data (Bhatt et al., 2014).

Log management is a key component of *SIEM* because it provides an audit trail for incident investigations (Chuvakin, Schmidt, & Phillips, 2013). With effective log management, organizations can enhance the effectiveness of threat detection and response (Miloslavskaya & Tolstoy, 2016).

Discussion

Basic Concepts of *SIEM*

Security Information and Event Management (SIEM) is a monitoring system that detects attacks and a security response system that responds to those attacks by analyzing various event logs generated from real-time data (Bhatt et al., 2014). Logs are information recorded by devices that contain activity data, such as network traffic, device status, and other information (Chuvakin, Schmidt, & Phillips, 2013). A *SIEM* system operates by collecting data from every source within the network infrastructure—such as network sources, security sources, server sources, database sources, and application sources—to identify potential external and internal threats (Bhatt et al., 2014).

Input devices are considered sensors for *SIEM* because each device captures events occurring at its respective location (Miloslavskaya & Tolstoy, 2016). Data obtained from these devices is presented on a dashboard using graphs that make it easy to read, understand, and identify patterns within the system (Bhatt et al., 2014). *SIEM* offers long-term data storage, allowing for data correlation over extended periods (Chuvakin, Schmidt, & Phillips, 2013). This technology can perform integrated correlation processes with various data sources, and the processed data is transformed into an information overview (Miloslavskaya & Tolstoy, 2016).

How SIEM Works in Detecting Advance Threats

SIEM equipped with *machine learning (ML)* technology has the ability to detect advanced threats by examining patterns and anomalies in both historical and real-time

data (Alzahrani & Aldhahri, 2021). Unlike traditional systems that rely on static rules and known threat signatures, *ML-based SIEMs* can identify new attacks, such as *zero-day attacks* and *advanced persistent threats (APTs)*, through behavioral analysis, characteristic analysis, and anomaly detection (Ferrag et al., 2020). This system leverages continuous learning capabilities to constantly update its detection algorithms, enabling it to adapt to ever-evolving attack techniques (Alzahrani & Aldhahri, 2021). Additionally, modern *SIEM* systems can integrate data from various sources to detect complex, multi-stage patterns in cyberattacks (Vielberth, Bohm, & Pernul, 2020). *SIEM* now not only acts as a responder to events that have already occurred but is also capable of predicting and preventing incidents before they happen, thereby alerting security teams and providing the necessary reports for analysis (Alerting and Reporting), and taking action before an attack escalates (Vielberth, Bohm, & Pernul, 2020).

Modern *SIEM systems* no longer rely solely on static rules and existing attack signatures but also utilize machine learning algorithms such as *neural networks, support vector machines (SVM),* and random forests to identify attack patterns from both historical and real-time data (Ferrag et al., 2020). Additionally, *unsupervised learning* techniques such as *clustering* and *autoencoders* are used to detect anomalies or undefined suspicious behavior, such as *zero-day* attacks and *advanced persistent threats (APT)* (Abdulhammed et al., 2021). In practice, algorithms such as *k-means clustering* and principal component analysis *(PCA)* play a role in grouping and reducing the dimensions of the data, making it easier to analyze (Abdulhammed et al., 2021).

Meanwhile, the model uses *deep learning* methods *such as Long Short-Term Memory (LSTM)* to analyze sequential data, such as continuous network activity (Ferrag et al., 2020). This model is periodically updated through feedback from incident investigation results, enabling the system to learn from past events and adapt its detection strategies to evolving threats (Alzahrani & Aldhahri, 2021). Thus, integrating these algorithms into *SIEM* enables organizations to detect threats more quickly, accurately, and efficiently, while minimizing the risk of complex attacks (Vielberth, Bohm, & Pernul, 2020).

Implementing Security Information and Event Management (SIEM) to Enhance Security Response to Advanced Threats Such as APTs

Security Information and Event Management *(SIEM)* systems must be implemented methodically to fully leverage security responsiveness against advanced threats such as Advanced Persistent Threats *(APTs)* (Vielberth, Bohm, & Pernul, 2020). This includes accurate log entries, real-time automated data correlation, and in-depth internal reporting (Bhatt et al., 2021). A *SIEM* system can collect log data from various devices, such as firewalls, servers, and applications, and then analyze that data using algorithms to identify suspicious activity (Ferrag et al., 2020).

For detecting *APTs*, which are typically gradual and stealthy, correlation activities are crucial (Vielberth, Bohm, & Pernul, 2020). Platforms like *Splunk* are also renowned for their effectiveness in real-time data analysis and ease of use, with visual data and reports readily available (Alzahrani & Aldhahri, 2021). Consequently, *SIEM* is considered significant in supporting comprehensive detection and response to security threats (Ferrag et al., 2020).

How Effective Is SIEM in the Industry?

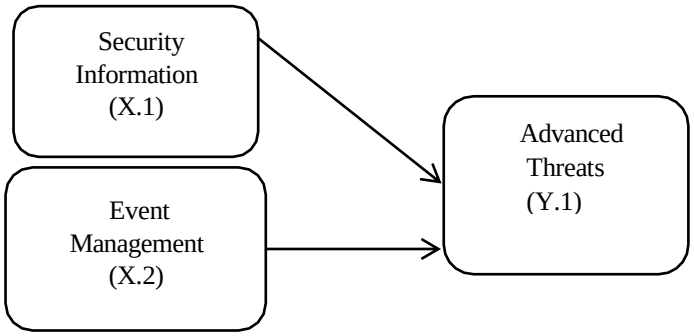
Overall, *SIEM* (Security Information and Event Management) is crucial in the

industry, particularly in terms of threat detection, incident response, and regulatory compliance (Vielberth, Bohm, & Pernul, 2020). This study reveals that *SIEM* is capable of integrating logs from various *IT* devices, detecting abnormal patterns in real time, and generating reports that support security audits (Ferrag et al., 2020). In a case study of implementation at a large organization, *SIEM* proved effective in accelerating incident response times and improving the efficiency of the information security team (Alzahrani & Aldhahri, 2021).

The use of *SIEM solutions* like Splunk can help industries achieve end-to-end visibility into network activity, which is critical for addressing sophisticated cyber threats such as *Advanced Persistent Threats (APTs)* (Vielberth, Bohm, & Pernul, 2020). Although there are technical complexities involved and a need for human resources, the benefits offered by *SIEM* make it a strategic area of expenditure in industries that rely on data security (Abdulhammed et al., 2021). Its successful implementation heavily depends on thorough planning, staff training, and full support from top management (Alzahrani & Aldhahri, 2021).

Conceptual Framework

Based on the problem formulation, discussion, and relevant research, the conceptual framework of this article is presented in Figure 1 below.



Source: Research Findings

Figure 1. Conceptual Framework

Thus, based on the conceptual framework above, the following factors influence Advanced Threats, Security Information, and Event Management. In addition to the three exogenous variables that affect a company's strength, there are many additional variables, including:

1. Network Security Monitoring: Situmorang & Hasibuan, 2021; Kurniawan & Firmansyah, 2022; Prasetyo & Nugroho, 2022).
2. Incident Response Management: (Hidayat & Santoso, 2021; Wibowo & Rahayu, 2022; Setiawan & Maghfiroh, 2022).
3. Cyber Threat Intelligence: (Nugroho & Pratama, 2021; Lestari & Wijaya, 2022; Ramadhan & Fauzi, 2023).

CONCLUSION

Based on the findings and discussion regarding this research topic, the authors conclude that *Security Information and Event Management (SIEM)* is an effective cybersecurity solution for detecting and responding to advanced threats, such as *Advanced Persistent Threats (APTs*). With technologies like machine learning, real-time data correlation, and log integration from various system sources, *SIEM* enhances network visibility and accelerates incident response times. These advantages are evident in reduced false positive rates, the identification of complex attack patterns, and

compliance reporting for information security regulations. Additionally, this study indicates that the use of a definitive *SIEM* platform, such as Splunk, offers advantages in visual analysis, real-time reporting, and the scalability of its security system. However, the success of *SIEM* implementation requires management support, thorough planning, human resource training, and periodic evaluations to ensure the system remains adaptive to evolving cyber threats. *SIEM* has proven to be a critical component of organizational security policies and an early detection system against terrorism, hidden, and persistent threats. Therefore, optimal *SIEM* integration into an organization's cybersecurity infrastructure is highly recommended to further enhance the organization's resilience and readiness against current and future digital.

REFERENCES

Abdulhammed, R., Faezipour, M., Abuzneid, A., & AbuMallouh, A. (2021). Deep and machine learning approaches for anomaly-based intrusion detection of imbalanced network traffic. *IEEE Sensors Letters, 5*(1), 1–4.

Alzahrani, A., & Aldhahri, E. (2021). A machine learning approach for security information and event management. *International Journal of Advanced Computer Science and Applications, 12*(6), 108–115.

Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The operational role of security information and event management systems. *IEEE Security & Privacy*, *12*(5), 35–41.

Bilge, L., & Dumitras, T. (2012). Before we knew it: An empirical study of zero-day attacks in the real world. *Proceedings of the 2012 ACM Conference on Computer and Communications Security (CCS)*, 833–844.

Chen, P., & Hutchins, E. (2014). Advanced persistent threat. *International Journal of Computer Science and Information Security, 12*(9), 1–9.

Chuvakin, A., Schmidt, K., & Phillips, C. (2013). *Logging and log management: The authoritative guide to understanding the concepts surrounding logging and log management*. Syngress/Elsevier.

Ferrag, M. A., Maglaras, L., Moschoyiannis, S., & Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications, 50*, 102419.

Hidayat, R., & Santoso, B. (2021). Analisis manajemen respons insiden keamanan siber pada sektor perbankan Indonesia. *Jurnal Keamanan Informasi dan Siber*, *3*(1), 22–30.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research, 1*(1), 80–106.

Kurniawan, Y., & Firmansyah, D. (2022). Analisis keamanan jaringan terhadap ancaman siber pada infrastruktur teknologi informasi. *Jurnal Keamanan Siber Indonesia, 2*(1), 14–22.

Lestari, D., & Wijaya, R. (2022). Pemanfaatan intelijen ancaman siber dalam sistem deteksi intrusi berbasis machine learning. *Jurnal Teknologi dan Sistem Informasi*, *8*(2), 55–63.

Miloslavskaya, N., & Tolstoy, A. (2016). Big data, fast data and data lake concepts. *Procedia Computer Science, 88*, 300–305.

Nugroho, A., & Pratama, I. (2021). Penerapan intelijen ancaman siber untuk mitigasi risiko keamanan informasi organisasi. *Jurnal Ilmu Komputer dan Informatika*, *7*(1), 44–52.

Prasetyo, D., & Nugroho, A. (2022). Implementasi manajemen respons insiden keamanan siber pada organisasi pemerintah. *Jurnal Sistem Informasi dan Teknologi*, *4*(1), 33–41.

Pratama, I. P. A. E. (2021). Keamanan sistem komunikasi data pada jaringan komputer. *Jurnal Ilmu Komputer dan Informatika*, *7*(1), 55–63.

Rahayu, S., & Prasetyo, A. (2021). Implementasi prinsip CIA dalam sistem keamanan informasi perusahaan. *Jurnal Informatika dan Komputer, 8*(1), 12–19.

Ramadhan, F., & Fauzi, A. (2023). Strategi intelijen ancaman siber dalam menghadapi advanced persistent threat pada infrastruktur kritis. *Jurnal Keamanan Siber Indonesia*, *4*(1), 10–18.

Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies, 38*(1–2), 4–37.