Engineering and Technology Journal e-ISSN: 2456-3358

Volume 10 Issue 07 July-2025, Page No.- 5738-5746

DOI: 10.47191/etj/v10i07.21, I.F. – 8.482

Advanced Persistent Threat (APT) Detection Using SIEM: A Review of Techniques and Tools

Vivek Sharma
Designation: System Analyst
MITS Deemed University

ABSTRACT*:* APTs are hard to fight in cybersecurity since they are difficult to spot, aimed at a single target and continue for a long time. Advanced threats evade traditional security solutions which is why it's important to use stronger defense systems. Because they centralize the collection of security events, security information and event management (SIEM) systems have grown in significance, compare them instantly and analyze them for large organizations. In this review paper, it analyzes existing ways and tools for finding APT threats using SIEM platforms. First, the article describes what APTs are and how SIEM works. Different ways to detect APTs, such as using signatures, abnormal behavior and machine learning, are looked at, and their pros and cons are presented. The document explains how well-known SIEM programs perform in terms of capabilities and how easily they can fetch information from third-party sources of threat intelligence. When performing a detailed literature review, the author summarizes current research, explores new frameworks and highlights the challenges that come with the lack of data, trouble measuring outcomes and limited resources. To finish, the paper highlights upcoming trends and research goals designed to boost SIEM's protection against APTs by urging the use of adaptive, smart and situation-aware security architectures. The main purpose of this study is to give researchers and practitioners advice on how to secure organizations against difficult cyber threats.

KEYWORDS: Advanced Persistent Threat (APT), APT Detection, Security Information and Event Management (SIEM), Cybersecurity, Threat Detection, Threat Intelligence Integration

I. INTRODUCTION

Cyber dangers in today's globally linked society are more sophisticated, common, and destructive than ever before. One of the struggle can be described as being engaged in shielding their networks, data, and digital assets against a wide variety of attacks, such as phishing, malware, Denial of Service (DoS), and APTs [1]. Out of these, APTs are specifically hazardous because they are covert, specific, and persistent [2]. In contrast to opportunistic attacks, APTs are aimed at particular entities, both in critical industries, which are energy, education, finance and defines sectors [3]. Such well-known cases as Stuxnet, Hydras, Titan Rain, and RSA SecureID breach demonstrate the harmful possibilities of the APTs' ability to stay hidden during long periods [4].

APT attacks are progressive and dynamic, since they can smoothly merge with normal operation of the systems hence becoming hard to diagnose [5]. The conventional security devices, like standalone Intrusion Detection Systems (IDS), are not up to this mark because they mostly use the rule-based approaches, which are event-centric. It makes them unhelpful against the complex and dynamic aspect of APTs [6].

The systems of modernization of the critical infrastructure, like Supervisory Control and Data Acquisition (SCADA) systems, deeper complicate the situation in the sphere of cybersecurity. Systems that used to be isolated are being introduced on a network that is interconnected, and the attack surface greatly expands accordingly [7]. Therefore, this leads to a rise in the demand for more complex and combined protection systems. To solve such a problem, companies are resorting to Security Information and Event Management (SIEM) systems, an advanced platform that centralizes gathering, processing, and disposing of security events within the IT environment of an enterprise [8]. SIEM solutions process information on a wide variety of sources such as firewalls, antivirus programs, IDS and network traffic logs, allowing real-time tracking and associated events. This is because this end-to-end viewing enables security teams to identify, study and act against multi-dimensional threats more efficiently [9].

Since they can match incidents across several systems and can detect advanced styles of attacks, the SIEM platforms have proven crucial when it comes to APT detection. All methods and solutions are reviewed in this paper to see the modern APT detection methods in use with SIEM systems [10]. It negatively assesses their advantages and shortcomings, along with presenting the main challenges and research recommendations on how to improve the detection of APT with the SIEM.

A. Structure of the Paper

This paper is organized as shown below: Section II describes the settings of the characteristics of APT. Section III describes SIEM platforms. Section IV discusses APT detection techniques using SIEM, and Section V reviews tools and platforms. Section

VI presents a literature review summarizing key research, and Section VII concludes with challenges and future directions for enhancing APT detection with SIEM technologies.

II. UNDERSTANDING ADVANCED PERSISTENT THREATS (APTS)

JavaScript, originally intended to augment the interactivity of online pages, has gone beyond its primary scope. The emergence
of contemporary JavaScript frameworks has facilitated its
transformation into a comprehensive programming language
that can drive both front-end and back-end development.
JavaScript, originally intended to augment the interactivity of online pages, has gone beyond its primary scope. The emergence
of contemporary JavaScript frameworks has facilitated its
transformation into a comprehensive programming language
that can drive both front-end and back-end development.

An APT is a tailored attack that derives unlawful access to information and communication systems to filter confidential data or to destroy a business. Ever since the announcement of Stuxnet, APTs have become more purposeful and devastating, demonstrating that it is easy to compromise familiar systems and succeed to dart many of the presumably more sophisticated security measures that are in place to protect the computing environment. Most of such threats have not yet been identified. These kinds of dangers, such as APT10, have been detected once it was found out and their operators have been caught with little or no effort at all, and APT41 make a triumphant return, this time armed with enhanced powers to accomplish their mission [11]. Damage to intellectual property, private data, and finances was substantial as a consequence of these assaults.

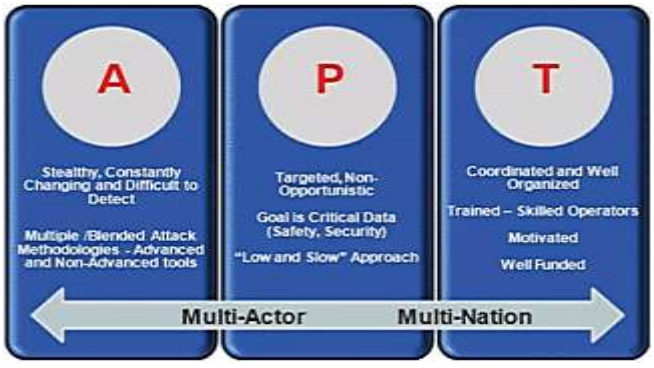

Fig. 1.Advanced Persistent Threat

Figure 1 shows three tell-tale signs of an APT assault. One, sophisticated: During the assault phase, the assailants use sophisticated instruments and strategies; 2. Determination: Attackers are hell-bent on destroying their objective. Throughout the assault cycle, attackers mimic the methodical procedure; 3. Danger: An intruder may get access to sensitive data.

The retrieval module in RAG typically leverages dense vector representations to identify relevant
documents from large datasets, such as Wikipedia or proprietary databases. Once retrieved, these
documents are passed to the generative module, often built using transformer-based architectures, to
generate responses grounded in the retrieved knowledge. This methodology helps mitigate the
hallucination problem and ensures that the generated text is more factual and contextually appropriate
(Thakur et al. 2021). Over the period, RAG models have seen applications in various domains, including
open-domain question answering (Karpukhin et al., 2020), conversational agents (Liu et al., 2021), and
personalized recommendations.
The retrieval module in RAG typically leverages dense vector representations to identify relevant
documents from large datasets, such as Wikipedia or proprietary databases. Once retrieved, these
documents are passed to the generative module, often built using transformer-based architectures, to
generate responses grounded in the retrieved knowledge. This methodology helps mitigate the
hallucination problem and ensures that the generated text is more factual and contextually appropriate
(Thakur et al. 2021). Over the period, RAG models have seen applications in various domains, including
open-domain question answering (Karpukhin et al., 2020), conversational agents (Liu et al., 2021), and
personalized recommendations.

APTs are a kind of coordinated and complex cyberattack. The hacker gains access to the network and proceeds to discreetly obtain information or accomplish the aim. To successfully penetrate a specific organization, APTs are meticulously planned and designed to circumvent security measures inside the target network environment [12]. One such target is the APT assault. The perpetrator learns as much as they can about the victim before launching an assault. Based on the data acquired, the attacker creates or develops the necessary tools to exploit the vulnerability. The assailant then moves on to the next stage of the assault by communicating with a remote server and relaying orders (command and control).

A. Characteristics of Advanced Persistent Threats (APTs)

Different from other types of cyberattacks, APTs persist over an extended period, have more specific goals, and use a wide range of tactics. Typically, very competent and well-funded actors put up APTs, resourced individuals or organizations and may benefit from state or criminal support. Here are several characteristics are as follows:

1) Persistence

These attacks are not carried out only for brief durations. Such games are meant to involve players for prolonged periods, which might last months or years. They never lose their access to the network and keep trying to hide their actions from security systems.

2) Stealth and Evasion

APTs are very secretive in their activities. To hide from simple security systems, attackers make use of encryption, rootkits, fileless malware and different evasion techniques.

3) Multi-Stage Attacks

APTs take several steps and are made up of various stages. Their methods usually consist of reconnaissance, initiation by using spear-phishing, access to different computers, collection of data and in rare situations, attacks aimed against the organization's infrastructure.

4) Targeted and Specific

APTs are not like opportunistic attacks, which are less focused on specific targets. Attackers tend to target certain organizations, whole industries or key infrastructure in support of their political, economic or strategic intentions.

5) Human-In-The-Loop

APT activities are seldom run without manual input. They have people operating them who oversee development, decide at any time and adapt using the target's movement.

B. APT Lifecycle (Kill Chain Model)

The Kill Chain Model is often used to depict each step of the APT Lifecycle that describes an attack. At the start, attackers use passive approaches to get information about the organization they are targeting. Next, malicious actors develop software that can attack computers and add it to files or links. At the delivery stage, criminals send malware by using emails with dangerous links or infected websites. When the payload is sent successfully, exploitation takes place, giving the attacker entry by using system flaws. Subsequently, the hacker implants a permanent access into the system in the form of back doors or remote applications. During the command and control (C2) step, the attacker executes his activities remotely on the target network and controls everything. In the final section, actions on objectives, the attacker completes the order by stealing information, monitoring systems or taking them offline. By being aware of the various stages of the APT attacks, the organizations can easily detect and prevent them to enhance their security.

C. Key Challenges in APT Detection

The presence of APTs poses several important problems in their detection because they are stealthy, targeted, and extended. The APTs commonly utilize zero-day vulnerabilities, encrypted communications channels, as well as multi-stage attack patterns, thus it hard to identify them through traditional security tools. Their capability of simulating normal users, which allows them to stay in systems unrecognized over a considerable amount of time, makes it hard to identify and react. Moreover, the sheer amount of logs and alerts Logs and alerts created by enterprise networks is so vast that it binds the hands of the analysts, making it hard to correlate threats in time [13]. The dynamism of APT techniques coupled with poor contextual threat information and the necessity to exert monitoring in real-time further complicates detection activities and requires such approaches as advanced analytics, threat hunting, and behaviour-based anomaly detection to be in corporate into cybersecurity models. Some key issues of APT Detection exist:

1) Stealthy and Persistent Nature

APTs take a long time to complete their goals by keeping their actions quiet and easy to overlook by traditional security methods.

2) Advanced Evasion Techniques

Hackers rely on encrypted communication, fileless malware and code that changes each time to avoid being detected by tools that scan or guess viruses.

3) Lack of Comprehensive Datasets

The effectiveness of using AI/ML for detecting APTs is limited because getting real-world, labelled datasets for training is hard.

4) High False Positive Rates

Many times, various detection systems generate alerts that are not real threats and make it tough for analysts to notice those that do matter.

5) Difficulty in Identifying Multi-Stage Attacks

Most detection tools concentrate on single events, which can make it tough to see the whole sequence that an APT use. Detecting APTs is challenging due to their stealthy, persistent behaviour, use of advanced evasion techniques like encrypted communication and fileless malware, and multi-stage attack strategies. Limited real-world datasets and high false positive rates further hinder effective detection, requiring advanced analytics and real-time monitoring.

III. SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM) SYSTEMS: AN OVERVIEW

Cyberattacks are still one of the biggest dangers for any organization. Most of the attacks in 2023 were related to cybercrime, and 50% or more of those attacks involved malware and the use of known flaws. One of the main ways to deal with these kinds of threats is to rely on Security Information and Event Management (SIEM). As the security research firm Gartner introduced it, SIEM brings together SIM and SEM abilities to offer round-the-clock monitoring, correlation of events and immediate response during incidents [14]. Modern SIEM tools scan a great deal of complex and changing log data and alerts from different parts of a company's network. For this reason, deploying a SIEM solution now means it needs to be customized, integrated and continuously managed to be useful.

A. Architecture of a SIEM System

A SIEM system is created to gather, process, review and take care of security information from every link in an organization's network. Starting with many sources such as servers, firewalls, intrusion detection systems, and endpoints, the system begins to acquire data by monitoring events and logs. After that, the information is normalized and adapted into a standard format for all processing operations [15]. The main part of the system is the correlation engine, which scans the data after normalization to look for suspicious behaviors, changes and security incidents. Any discovered threats trigger an alert which is automatically sent to security analysts. The platform stores all event data safely

to comply with regulations, attend audits and investigations, and it also provides real-time reports and analysis of trends. Nowadays, SIEM teams usually integrate with SOAR systems to automate actions and enhance the process of threat management. Because SIEM architecture is well-structured and can be updated, it can efficiently find, observe and handle threats happening right now.

B. SIEM Features and Capabilities

The events generated by the controlled infrastructure may be collected, stored, and linked by any SIEM [16]. In addition to these primary controls, the current systems often vary according to the market positioning of SIEMs. What follows is a discussion of the criteria that should be considered while evaluating SIEM systems [17]. Following a comparison of survey data from commercial and open-source SIEMs and an examination of several commercial SIEMs, it has assigned each SIEM feature to low (poor), average (partial) or high (complete) based on its effectiveness in the best solutions. Keep in mind that the assessment includes only the most essential parts of the purchased SIEM solutions; it does not take into account any further features (add-ons).

C. Benefits and Limitations of SIEM

SIEM systems offer centralized visibility, real-time threat detection, and compliance support by analyzing logs from various sources. However, they can be costly, require skilled personnel, and may produce many false positives. Traditional SIEMs also struggle to detect advanced threats without enhanced analytics. Here are the benefits and limitations are in below:

- **Benefits:** A SIEM system makes it easier to see how secure an organization is by reviewing logs and events from various systems. Such tools assist security teams in noticing threats right away and handling them without delay. It plays a role in helping with compliance by recording all data and producing detailed reports [18]. Likewise, they help connect happenings that may not be related to understand complex ways that cyberattacks are conducted, which makes cybersecurity more effective.
- **Limitations:** SIEM systems have strengths, but there are some things they cannot do. Such technologies usually require a lot of resources and knowledge to deploy, set up and look after properly. Many false alarms can result from analyzing large amounts of data, which can make security analysts exhausted and less attentive. Many SIEMs also find it difficult to catch advanced threats that avoid detection with signatures or work in a minor way for a long period, such as APTs. Moreover, problems with using various data sources and scaling the system can make it perform poorly in complex circumstances. Not monitoring and tuning the SIEM can cause its findings to be either wrong or difficult to use.

IV. APT DETECTION TECHNIQUES USING SIEM

Security software and tools called SIEM use several techniques together for APT detection, such as signature-based methods, behavior analysis, artificial intelligence and threat research. Security systems that use signatures can detect malware cases that are already recognized, but they fail to catch those that appear unexpectedly or change. This issue is resolved by behaviour-based detection, which monitors user and network activities, but sometimes leads to many false alarms. Nearly 99.89% accuracy can be reached by Belts and CNN-LSTM systems, which can find complicated APT patterns in a huge amount of network traffic. The inclusion of real-time information about dangers and shared strategies between organizations improves how quickly and strongly threats are identified and handled. The latest SIEM tools can benefit from using blockchain, honeypots and honeytokens as well as federated learning models [19]. As a result, detection is made possible in many locations, privacy is protected, and the system monitors, responds automatically and takes action against constant APT threats.

A. Current APT Detection Techniques

APT detection combines signature-based methods, AI/ML models, threat intelligence, and anomaly detection. While signatures miss new threats, AI and SIEM detect unusual behaviour, and shared threat data improves accuracy. Together, they enhance APT defense.

1) Signature-Based Detection

Network events are checked against a collection of threat and malware signatures using this strategy. Although these solutions can detect different threats such as malicious software, compromised data, rootkits, and the attacker's Internet Protocol addresses, they run into several issues dealing with APTs. Malicious actors can use advances in technology to sneak past, as the main weakness is that these security tools do not spot unknown attacks. In addition, this approach doesn't work well against APTs since they can change their appearance and signature over 60% of the time.

2) Machine Learning and AI-Based Detection

Machine learning and artificial intelligence have applied several approaches to improve the detection of APts. According to existing research, an approach that includes the Bead model and Belts, attention, and DGCNN techniques achieves superior detection performance for APT threats. Currently, analysis of a network's characteristics using Artificial Intelligence leads to a detection accuracy of almost 99.89%. CNN-LSTM models offer a higher level of accuracy when it comes to assessing network activity and detecting complex APT attack methods, as compared to other DL models [20]. They can thoroughly monitor traffic on automobile networks while looking for possible breaches and hints of APts.

3) Threat Intelligence

catching APTs, supported by the use of iOS and shared defined approaches (Figure 2). Using distributed audit models at the network level helps to cost-effectively identify and stop lateral attacks, as well as to pinpoint evading actions of attackers [21]. They help make APT defence services stronger and improve how well the detection systems work.

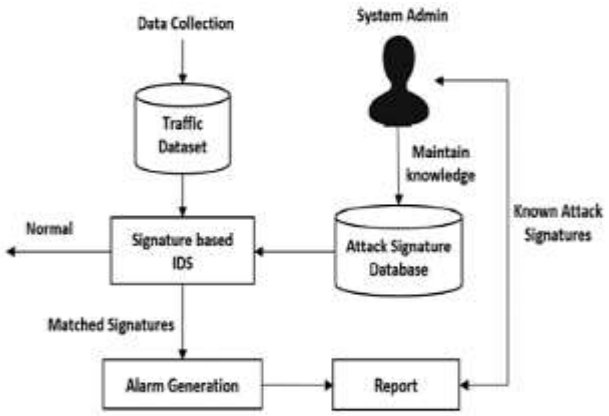

Fig. 2.APT Detection

A signature-based IDS where traffic data is compared with known attack signatures. Matches trigger alarms and reports, while unmatched traffic is marked normal. A system admin updates the signature database to maintain detection accuracy.

4) Anomaly-Based Detection:

SIEM makes use of anomaly detection to find APTs by marking behavior that is not typical. Signature-based approaches identify threats based on familiar attacks, but anomaly detection finds out about odd behavior by studying network traffic, how people use devices and the contents of packets. SIEM systems collect and connect different logs to learn about normal user and system actions which helps in finding subtle changes that might point to APT attacks [22]. Advanced anomaly detection makes use of machine learning so that it can recognize new dangers that are not caught by older security systems. Even though it works well, the approach might result in many false positives and needs very powerful computers to operate in large organizations. But when used along with other methods, it greatly helps an organization spot these difficult and changing APT attacks.

B. Behaviour-Based Detection

This technique monitors and checks user, system and network actions to spot any APTs that act differently from ordinary users. As opposed to relying on known attack patterns, the technique in question creates a pattern of normal activity and identifies any behavior that stands out as potentially hazardous. SIEM systems use behaviour-based detection by closely inspecting network packets, reviewing traffic patterns and bringing together logs to catch signs of lateral movement, use of more privileges or unapproved access [23]. This approach is useful for detecting threats that go past conventional security methods, such as zero-day attacks [24]. Taking advantage of UEBA, the software creates an understanding of user and system actions and identifies cyberattacks spreading across any number of devices. However, since behaviour-based systems detect threats better and earlier, they may report false suspicious activity frequently and need heavy computing, along with a skilful setup to work properly.

C. Challenges in APT Detection and Mitigation

The adaptability and stealthies of APTs make them difficult to detect and counter. SIEM systems help by correlating and analyzing logs to detect anomalies and threats. Techniques like behavior analytics, ML, and advancements in danger detection with threat intelligence [25], but challenges remain due to false positives, encrypted traffic, and attacker evasion tactics.

- **Stealth Techniques:** APTs employ methods of sophisticated evasion, and thus they are hard to intercept using conventional protection methods.
- **Persistence:** The delayed nature of APTs implies that although an attack may be detected, it is quite difficult to secure complete elimination of the malicious attack.
- **Adaptive Behaviour:** APT actors continually evolve their tactics in response to improved defences.
- **Resource Intensity:** The APT attack is quite expensive to defend against and needs major technological and human resources Investment.
- **Data Volume:** The sheer amount of information in modern networks cannot allow easy detection of even minor APT activities as it is similar to finding a needle in a haystack.
- **Supply Chain Vulnerabilities:** As recent attacks such as SolarWinds have shown, APTs can use the context of trust in official software and updates and circumvent a lot of classical security mechanisms.

APTs are hard to detect due to stealth, persistence, and adaptive tactics. Challenges include encrypted traffic, high data volume, resource demands, and supply chain risks.

V. TOOLS AND PLATFORMS FOR APT DETECTION WITH SIEM

APTs are best detected by strong systems that can handle lots of security data, recognize common behaviors and connect findings from various networks. SIEM is the foundation for making this ability possible within an organization. Using firewall, intrusion detection data, servers and endpoint data, they manage to detect long-lasting, hard-to-notice cyber threats. Being armed with new technologies and methods, SIEMs can recognize the soft signs APTs often leave behind [26]. It is important for SIEM in APT detection to connect with third-party threat databases, find unusual activities through anomaly detection and let users customize how data is shown and automated actions are triggered. Open-source and commercial SIEM products differ in terms of how well they work, how much they can grow with needs and how adjustable they are, as mentioned in the upcoming subsections.

Commercial SIEM Solutions: Businesses adopt commercial SIEM solutions mainly because of their strong abilities, scalability and available support. Because of its indexing, search and machine learning systems, Splunk can easily identify the signs of APTs [17]. With their log and flow data matched with threat intelligence, Radar can detect both lateral actions and attempts to control a network. Micro Focus designed ArcSight which is focused on discovering threats and responding to them through sophisticated analysis and reporting. They are also able to use security tools and threat feeds from outside sources which helps them notice complicated APT efforts. SOC operations are

improved and the response time is lowered, thanks to the group's user-friendly dashboards and automated incident actions.

Open-Source SIEM Tools: Open-source SIEM tools are a smart choice for businesses that have to work with limited budgets. ELK Stack makes it easy to gather logs, store them for indexing and analyze them using charts, plus it can merge anomaly detection tools and threat intelligence [27]. With intrusion detection, vulnerability discovery and file integrity watch, Wazuh on the ELK Stack ensures more effective APT detection. By bringing together multiple open-source programs, OSSIM (Open Source SIEM by AT&T) supports complete security management, covering asset detection, vulnerability assessment and event grouping. While these tools might be more complicated to use and understand, they help with both flexibility and clear understanding when spotting and analyzing threats.

Comparative Analysis of SIEM Tools: There are major differences between the two types of SIEM when it comes to setting up the system, how it performs, its scalability, how reliably it detects threats and what support is offered [28]. Because they have polished interfaces, business support and features for big businesses, Splunk and QRadar are the right choice for handling complex tasks. On the other hand, using Wazuh or ELK Stack means you can adjust them more and spend less, but you need to have technical skills and perform manual steps. If a company is to detect an APT, it needs to analyze events across various systems, merge threat feeds and do advanced analytics. Having these features in a commercial SIEM is common, but you can achieve them with open-source tools when you configure them and download appropriate plugins.

Integration of Third-Party Threat Feeds: The inclusion of threat intelligence from external sources in SIEM platforms greatly increases the ability to detect APT threats, by supplying the latest suspicious data, IP addresses, domain names and behaviors [29]. By unifying SIEM with MISP, it becomes easier to find and respond to threats promptly. Most commercial SIEMs are designed to work smoothly along with premium threat intelligence tools such as IBM X-Force, FireEye and Recorded Future. You can connect open-source SIEMs to free or open-source-driven feeds with the help of tools like MISP (Malware Information Sharing Platform) or TAXII. Automating the process of receiving feeds and finding related threats allows organizations to quickly spot APTs, address dangers more rapidly and boost their defines against cybercrime.

VI. LITERATURE REVIEW

They study SIEM-based APT detection techniques, discuss the use of ML with SIEM, analyze what makes detection difficult, suggest CDT and game theory models and highlight effective detection ways using SIEM rules.

Buchta et al. (2024) performing a literature review that covers the different APT attack detection systems and methods and categorizing them based on the threat model to which they apply, as well as how they apply the detection method. In their results, they found some shared challenges in detecting the APT attacks, which include the proper attribution of the abnormal event to APT attack operation, inadequate public datasets and insufficient evaluation methods, flaws in the APT attack detection process, and inaccurate understanding of requirements [30].

AL-Aamri et al. (2023) carry out a thorough examination of the existing research and defines their advantages, weaknesses, and the points where they can be improved. Moreover, there are standardized methods that have been improved to facilitate their efficiency against APT attack detection. The learning process is dependent on datasets that are obtained through multiple avenues, and such avenues include journal logs, traceability audits and monitoring statistics of systems. Then, it has developed an effective APT recognizable and preventable system named the composition-based decision tree (CDT) to work in complicated environments. The results that are acquired illustrate that the suggested method has always been more effective and high-level compared to other algorithms in accuracy and performance of detection [31].

Kadhimi, Singh and Khalid (2023) offer a review of pieces of art carried out in the period 2012-2023. The initial search of 1351 papers has been carried out. After that, these articles were handled based on their titles, abstracts, and contents. The papers that came up as a result of such a search were chosen to answer the research questions. A theoretical framework has been suggested in which the situational awareness model is considered, according to implementing the game theory as an AI method to create both APT-based tactics, techniques, and procedures (TTPs) and standard TTPs and cognitive decision making. The framework increases the awareness of security and helps to detect APT attacks on smartphone sensors, applications, and user behavior [32].

Pulyala (2023) highlights the future of SIEM tools in light of the rapidly changing field of cybersecurity and explains how organizations cannot just be ready to implement ML-enhanced SIEM systems, but also optimize their use to achieve positive results. Organizations should build an intensive data policy, invest in talent, and simply improve ML-powered SIEM implementations to gain the most benefits of the promised opportunities of the technologies [33].

Jeffrey, Tan and Villar (2023) determining the major obstacles that still exist in the field, such as resource limitation, absence of normalized communication procedures, severe heterogeneity, which disrupts industry consensus, and various levels of information security between the Operational Technology (OT) and the IT networks. There is also the listing of potential solutions and/or opportunities to research to meet these challenges, selected [34].

Şimşek and Koltuksuz (2023) made an effort to review the research on APT detection and to shed light on the challenges associated with doing so. Furthermore, a novel method for APT detection using the SIEM solution is introduced in this study. Here, you should use the signs that were left behind by the assaults to build up APT rulesets in SIEM systems. The rule sets

take into account three primary categories of indicators and provide examples of each [35].

This Table I summarizes key literature on APT detection using SIEM, highlighting focus areas such as CDT models, game theory, ML integration, and rule-based methods. It identifies major challenges and showcases each study's unique contributions to improving APT detection effectiveness.

TABLE I. LITERATURE OF REVIEW ON ADVANCED PERSISTENT THREAT (APT) DETECTION USING SIEM

Reference	Focus Area	Key Findings	Challenges	Key Contribution
Buchta et al. (2024)	APT Detection Techniques and Classification	Reviewed and classified APT detection systems by threat models and methods	Misattribution of anomalies, lack of datasets, and poor evaluation methods	Provided structured classification of APT detection systems
AL-Aamri et al. (2023)	The CDT Model, Which is Based on Composition	CDT outperforms existing methods in detecting APTs using diverse datasets	Need for improved effectiveness and dataset diversity	Proposed CDT for APT detection with higher accuracy
Al-Kadhimi et al. (2023)	Game Theory and Situational Awareness Framework	Integrated game theory to detect APT behavior via sensors and applications	Difficulty in modelling cognitive behavior and context awareness	Developed a conceptual AI-based framework for APT detection
Pulyala et al. (2023)	Machine Learning in SIEM	The ability of SIEM systems to detect and respond is improved by ML.	Organizational readiness and gradual adoption	Advocated strategic adoption of ML-enabled SIEM tools
Jeffrey et al. (2023)	Challenges in APT Detection	Identified gaps in standardization, OT/IT integration, and resources	Heterogeneity and lack of standard protocols	Outlined future research directions and industry gaps
Şimsek et al. (2023)	Rule-Based Detection via SIEM	Introduced APT rulesets based on attacker indicators	Difficulties in generalizing indicators	Proposed practical ruleset examples for integration into SIEM

VII. CONCLUSION AND FUTURE WORK

Advanced Persistent Threats (APTs) constitute a strong cybersecurity problem with their covertness, strategic pursuit and attack schemes. These high-tech threats are not always interrupted or caught by traditional systems of security on their own. Security Information and Event Management (SIEM) tools are important when it comes to increasing the level of detection, in that, they amalgamate, track-down and scrutinize a variety of security data in real-time. Some detection methods have been mentioned in this review and these are behavior approaches, anomaly based and rule based methods of detection within SIEM. It also mentioned the advantages of incorporating machine learning in the reduction of false positives and enhancing accuracy in detection. The results of testing both commercial and open-source SIEM led to the conclusion that the organizations need to deploy the SIEM solutions that suit their requirements and integrate external sources of threat intelligence to strengthen security.

Even with these developments, there are some butterflies, which include scarcity of available publicly shared information, resource constraints, and complications in the development of effective and stable threat detection rules. There is more that needs to be done to scale the performance of SIEM by enhancing data sharing ability among systems, developing standard threat information sharing processes, and using AI to detect APTs fast. Along with that, the establishment of large-scale public datasets and the improvement of the evaluation methods can make the SIEM-based APT detection more reliable and efficient. There is a need to strengthen counter measures against the evolving APT by continually increasing defences through togetherness.

REFERENCES

1. H. Okamoto, "The Role of Information Security Event Management (SIEM) in Enhancing Intrusion Detection and Cybersecurity Through Machine Learning Technology." 2021. doi: 10.13140/RG.2.2.35096.00003.
2. N. K. Prajapati, "Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection," *Int. J. Adv. Res. Sci. Commun. Technol.*, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.
3. G. Wang, Y. Cui, J. Wang, L. Wu, and G. Hu, "A Novel Method for Detecting Advanced Persistent Threat Attack Based on Belief Rule Base," *Appl. Sci.*, vol. 11, no. 21, 2021, doi: 10.3390/app11219899.
4. B. Stojanović, K. Hofer-Schmitz, and U. Kleb, "APT datasets and attack modeling for automated detection methods: A review," *Comput. \& Secur.*, vol. 92, p. 101734, 2020.
5. A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities," *IEEE Commun. Surv. Tutorials*, vol.

21, no. 2, pp. 1851–1877, 2019, doi: 10.1109/COMST.2019.2891891.
6. A. R. Muhammad, P. Sukarno, and A. A. Wardana, "Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning," *Procedia Comput. Sci.*, vol. 217, pp. 1406–1415, 2023, doi: 10.1016/j.procs.2022.12.339.
7. B. Genge, P. Haller, and A.-S. Roman, "E-APTDetect: Early Advanced Persistent Threat Detection in Critical Infrastructures with Dynamic Attestation," *Appl. Sci.*, vol. 13, no. 6, 2023, doi: 10.3390/app13063409.
8. S. B. Shah, "Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure," *J. Glob. Res. Electron. Commun.*, vol. 2, no. 2, pp. 1–7, 2025, doi: 10.5281/zenodo.14955016.
9. A. Singla, E. Bertino, and D. Verma, "Preparing network intrusion detection deep learning models with minimal data using adversarial domain adaptation," in *Proceedings of the 15th ACM Asia conference on computer and communications security*, 2020, pp. 127–140.
10. V. Prajapati, "Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics : A Review Study," *J. Glob. Res. Math. Arch.*, vol. 12, no. 4, pp. 1–6, 2025.
11. S. Chatterjee, "Risk Management in Advanced Persistent Threats (APTs) for Critical Infrastructure in the Utility Industry," *Int. J. Multidiscip. Res.*, vol. 3, no. 4, pp. 1–10, 2021.
12. S. Krishnapriya and S. Singh, "A Comprehensive Survey on Advanced Persistent Threat (APT) Detection Techniques.," *Comput. Mater. \& Contin.*, vol. 80, no. 2, 2024.
13. A. K. Polinati, "AI-Powered Anomaly Detection in Cybersecurity: Leveraging Deep Learning for Intrusion Prevention," *Int. J. Commun. Networks Inf. Secur.*, vol. 17, no. 3, 2025.
14. L. Hase, "The Path to Choosing a SIEM System – A Systematic Literature Review," *Semin. IT-Management Digit. Age*, no. Summer, pp. 1–12, 2024.
15. M. Sheeraz *et al.*, "Effective Security Monitoring Using Efficient SIEM Architecture," *Human-centric Comput. Inf. Sci.*, vol. 13, 2023, doi: 10.22967/HCIS.2023.13.023.
16. M. Aymard, "Security Monitoring System Applied to IoT," Universidad Politécnica de Madrid, 2019.
17. G. Granadillo, S. González-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," *Sensors*, vol. 21, p. 4759, 2021, doi: 10.3390/s21144759.
18. H. Kali, "The Future of HR Cybersecurity: AI-Enabled Anomaly Detection in Workday Security," *Int. J. Recent Technol. Sci. Manag.*, vol. 8, no. 6, pp. 80–88, 2023.
19. W. Ahmed, "Advanced Persistent Threats (APTs) Analysing: Current Detection Techniques and Emerging Countermeasures," *Prem. J. Artif. Intell.*, 2025, doi: 10.70389/PJAI.100011.
20. A. Meliboev, J. Alikhanov, and W. Kim, "Performance Evaluation of Deep Learning Based Network Intrusion Detection System across Multiple Balanced and Imbalanced Datasets," *Electronics*, vol. 11, no. 4, p. 515, Feb. 2022, doi: 10.3390/electronics11040515.
21. S. R. Pulyala, "From Detection to Prediction: AI-powered SIEM for Proactive Threat Hunting and Risk Mitigation," *Turkish J. Comput. Math. Educ.*, 2024, doi: 10.61841/turcomat.v15i1.14393.
22. Z. Oughannou, Z. EL Rhadiouini, H. Chaoui, and S. Bourekkadi, "Anomaly-Based Intrusion Detection System To Detect Advanced Persistent Threats: Environmental Sustainability," *E3S Web Conf.*, vol. 412, pp. 1–6, 2023, doi: 10.1051/e3sconf/202341201106.
23. A. Bhardwaj, K. Kaushik, A. Alomari, A. Alsirhani, M. M. Alshahrani, and S. Bharany, "BTH: Behavior-Based Structured Threat Hunting Framework to Analyze and Detect Advanced Adversaries," *Electronics*, vol. 11, no. 19, 2022, doi: 10.3390/electronics11192992.
24. S. Murri, "Data Security Challenges and Solutions in Big Data Cloud Environments," *Int. J. Curr. Eng. Technol.*, vol. 12, no. 06, Jun. 2022, doi: 10.14741/ijcet/v.12.6.11.
25. V. Malik, A. Khanna, N. Sharma, and S. Nalluri, "Advanced Persistent Threats (APTs): Detection Techniques and Mitigation Strategies," *Int. J. Glob. Innov. Solut.*, 2024, doi: 10.21428/e90189c8.91e89a3e.
26. S. Arora and S. R. Thota, "Ethical Considerations and Privacy in AI-Driven Big Data Analytics," *Int. Res. J. Eng. Technol.*, vol. 11, no. 05, 2024.
27. J. Manzoor, A. Waleed, A. F. Jamali, and A. Masood, "Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," *PLoS One*, vol. 19, no. 3, Mar. 2024, doi: 10.1371/journal.pone.0301183.
28. K. Bezas and F. Filippidou, "Comparative Analysis of Open Source Security Information & Event Management Systems (SIEMs)," *Indones. J. Comput. Sci.*, vol. 12, pp. 443–468, 2023, doi: 10.33022/ijcs.v12i2.3182.
29. A. Elkosairy, N. Abdelbaki, and H. K. Aslan, "A Survey on the Integration of Cyber Threat Feeds and Blockchain Technology," *Int. J. Saf. Secur. Eng.*, vol. 14, no. 5, Oct. 2024, doi: 10.18280/ijsse.140502.
30. R. Buchta, G. Gkoktsis, F. Heine, and C. Kleiner, "Advanced Persistent Threat Attack Detection

Systems: A Review of Approaches, Challenges, and Trends," *Digit. Threat. Res. Pract.*, vol. 5, no. 4, pp. 1–37, Dec. 2024, doi: 10.1145/3696014.

31. A. S. AL-Aamri, R. Abdulghafor, S. Turaev, I. Al-Shaikhli, A. Zeki, and S. Talib, "Machine Learning for APT Detection," *Sustainability*, vol. 15, no. 18, 2023, doi: 10.3390/su151813820.
32. A. A. Al-Kadhimi, M. M. Singh, and M. N. A. Khalid, "A Systematic Literature Review and a Conceptual Framework Proposition for Advanced Persistent Threats (APT) Detection for Mobile Devices Using Artificial Intelligence Techniques," *Appl. Sci.*, vol. 13, no. 14, 2023, doi: 10.3390/app13148056.
33. S. R. Pulyala, "The Future of SIEM in a Machine Learning-Driven Cybersecurity Landscape," *Turkish J. Comput. Math. Educ.*, vol. 14, no. 03, pp. 1309–1314, Jul. 2023, doi: 10.61841/turcomat.v14i03.14392.
34. N. Jeffrey, Q. Tan, and J. R. Villar, "A Review of Anomaly Detection Strategies to Detect Threats to Cyber-Physical Systems," *Electron.*, vol. 12, no. 15, pp. 1–34, 2023, doi: 10.3390/electronics12153283.
35. A. Şimşek and A. Koltuksuz, "Detection of Advanced Persistent Threats Using Siem Rulesets," *Int. J. 3D Print. Technol. Digit. Ind.*, vol. 7, no. 3, pp. 471–477, Dec. 2023, doi: 10.46519/ij3dptdi.1353341.