Volume 12, No. 11, November 2025

Journal of Global Research in Mathematical Archives

ISSN 2320 – 5822

RESEARCH PAPER

Available online at http://www.jgrma.com

MACHINE LEARNING IN SIEM A SURVEY ON INTELLIGENT EVENT CORRELATION AND ANOMALY DETECTION

Mrs. Neha Upadhyay[1]

[1] Assistant Professor, Department of Computer Applications IIS University, Bhopal (M.P.)
neha.upadhyay887@gmail.com

Abstract: Security Information and Event Management (SIEM) platforms are vital for identifying, analyzing, and responding to security incidents in complex IT infrastructures. However, traditional SIEM systems often struggle to handle massive event volumes, generate false positives, and efficiently correlate diverse data sources. Machine learning, a subset of artificial intelligence, offers promising solutions for enhancing the intelligence and adaptability of SIEM systems. This paper presents a comprehensive survey of the integration of machine learning techniques into SIEM, with a particular focus on intelligent event correlation and anomaly detection. It explores a wide spectrum of approaches including supervised, unsupervised, and hybrid learning models that aim to detect complex threats, reduce false alerts, and uncover hidden attack patterns in real time. Key advancements such as clustering, neural networks, ensemble models, and deep learning-based anomaly detectors are critically analyzed in terms of their strengths, limitations, and application scope. Furthermore, the paper highlights the challenges in deploying ML-enabled SIEM such as data quality, model interpretability, scalability, and adversarial threats. It emphasizes the importance of combining domain expertise with automated learning to develop robust and context-aware systems. This survey aims to guide researchers and security practitioners by offering insights into the current landscape, ongoing gaps, and future directions in intelligent SIEM development.

Keywords: Security Information and Event Management (SIEM), Machine Learning, Event Correlation, Anomaly Detection, Cybersecurity, Machine Learning.

1 INTRODUCTION

In today's digital environment, organizations face a constant barrage of cyber threats that are becoming more intricate, focused, and enduring. By collecting, standardizing, and scrutinizing security logs and events from IT infrastructures, Security Information and Event Management (SIEM) systems have become a key element of enterprise security operations. These systems enable centralized monitoring and streamline incident response by correlating events from various sources, including firewalls, intrusion detection systems [1], servers, and endpoints. However, traditional SIEM systems rely heavily on static rule-based correlation, manual configurations, and predefined thresholds. These limitations greatly hinder their ability to detect sophisticated or previously unseen attacks [2]. fundamental constraint of traditional SIEM systems is their reliance on pre-established correlation rules and on detection based on signatures [3]. This method is fundamentally reactive and does not adapt to evolving attack vectors. In addition, it results in a large number of false positives, heightened alert fatigue among analysts, and delays in incident response. With the increasing complexity of enterprise environments and the massive amounts of heterogeneous log data they produce, there is an urgent requirement for more intelligent and automated approaches to efficiently and accurately detect malicious behavior [4].

By analyzing time-series data, network traffic, user behavior, and system logs, ML models can correlate events across different layers of the infrastructure and provide actionable insights in real time. Machine Learning (ML) has proven to be an effective answer for dealing with the limitations of conventional SIEM platforms. ML techniques improve the accuracy, scalability, and responsiveness of security monitoring processes by allowing SIEM systems to learn from historical data, recognize complex patterns, and adapt to new threats [5]. Event correlation based on ML surpasses static rules by employing supervised, unsupervised, and deep learning models to cluster related security events and extract valuable insights from data that would otherwise remain unnoticed. In the same way, models for detecting anomalies can spot divergences from typical conduct, thereby aiding in the discovery of covert assaults like insider threats, zero-day exploits, and advanced persistent threats (APTs) [6]. Current research and real-world applications highlight improved threat detection [7], automated analysis, and the growing need for scalable, explainable, and data-driven SIEM solutions [8].

1.1 Structure of the paper

The structure of this paper is as follows: Section 2 explains the SIEM architecture. Section 3 discusses machine learning techniques for intelligent event correlation and anomaly detection. Section 4 Present Event Correlation Section 5 presents a literature review of recent advancements. Section 6 concludes with insights and recommendations for future research directions.

2 FUNDAMENTAL OF SIEM ARCHITECTURE

Security Information and Event Management (SIEM) systems play a central role in detecting and responding to cybersecurity threats by collecting, correlating, and analyzing security events across enterprise networks. Traditional SIEM architectures rely on rule-based event correlation and predefined workflows, which often lead to high false-positive rates and limited adaptability to evolving threats.

The architecture of a SIEM system involves a set of agents installed on hosts throughout an organization's infrastructure. The agent represents a software component deployed on individual hosts or endpoints within an organization's network. Their main function consists of continuous monitoring, ensuring that they capture every relevant activity on the host. Agents monitor files and logs generated on respective hosts, in real-time, collecting data relevant to information security (for example, successful or unsuccessful logins, unauthorized user behaviours, modification of system files, etc.). After the data is collected by the agent, it is transferred to the server, where it is correlated and analyzed in real-time using detection rules. Figure 1, architecture enables robust monitoring, allowing identification of potential security threats and anomalies:

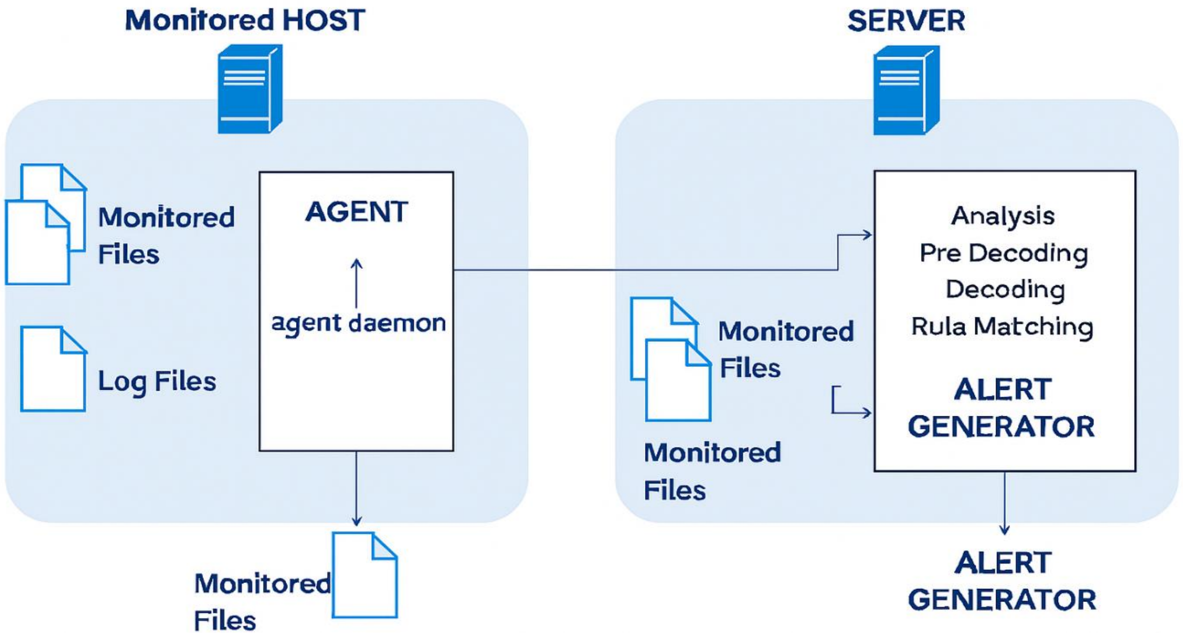

Figure 1: SIEM Architecture

The operational progression of the SIEM architecture workflow as follows:

- **Distributed Data Collection:** Software agents on "Monitored HOSTs" continuously collect real-time [6]security data from "Monitored Files" and "Log Files" (e.g., login attempts, system changes) via their "Log Collector" and "agent daemon."
- **Secure Data Transmission:** The collected data is then securely transferred from the host-based "agent daemon" to the central "SERVER."
- **Centralized Data Processing and Analysis:** On the "SERVER," the "server daemon" manages incoming data, which undergoes "Analysis," "Pre-Decoding," "Decoding" for normalization, and "Rule Matching." This real-time correlation and analysis against detection rules identifies potential security threats.
- **Automated Threat Identification and Notification:** Upon detecting threats or anomalies through rule matching, the ALERT GENERATOR" activates, creating and disseminating notifications to security personnel for prompt response [9].

2.1 Traditional Event Correlation Techniques

Traditional event correlation techniques are foundational to early SIEM systems, enabling security analysts to detect potential threats by identifying patterns within log and event data. These methods typically rely on rule-based logic, where predefined conditions are used to trigger alerts [10]. The primary techniques include:

- **Rule-Based Correlation:** This approach uses manually defined rules to detect specific attack patterns or policy violations. For example, multiple failed logins attempt from a single IP within a short time frame might trigger a brute-force attack alert.
- **Threshold-Based Correlation:** Alerts are generated when event frequencies exceed predefined thresholds. For instance, if traffic to a port exceeds normal levels, the system flags it as anomalous.
- **Time-Based Correlation:** Events are correlated based on their temporal relationships. Sequences of related events occurring within a specific time window may indicate a coordinated attack.
- **Event Aggregation and Deduplication:** To reduce alert fatigue, similar or repetitive events are grouped, preventing the system from generating redundant alerts and overwhelming analysts.
- **Hierarchical Correlation:** This technique involves grouping events by system components, users, or assets to understand the broader impact of isolated events.

While these traditional techniques offer structured analysis, they suffer from limitations such as high false-positive rates, inflexibility to unknown attack patterns, and the need for constant rule updates. These challenges have prompted a shift toward machine learning-based correlation to enhance adaptability and threat detection capabilities.

2.2 Challenges in Existing SIEM Systems

Despite their critical role in cybersecurity, existing Security Information and Event Management (SIEM) systems confront several significant challenges that can impede their effectiveness [11]. These issues are summarized as follows:

2.2.1 Data Volume and Velocity

SIEM systems frequently struggle with the immense volume and high velocity of log and event data generated across contemporary IT environments [12]. This can lead to difficulties in real-time ingestion, processing, and storage, potentially causing data loss or delayed threat detection due to system overload.

2.2.2 Complexity of Data Correlation and Contextualization

A primary limitation is the inability to effectively correlate disparate events from diverse sources into a cohesive and actionable security narrative. The lack of adequate context often results in a high prevalence of false positives, diminishing the value of generated alerts and contributing to analyst fatigue.

2.2.3 Significant Operational Overhead

SIEM deployments typically entail substantial operational burdens. This includes considerable effort for initial setup, continuous maintenance, and the constant tuning of detection rules and use cases. The demand for specialized cybersecurity expertise to manage and interpret SIEM outputs imposes a notable resource strain on organizations.

2.2.4 Limited Adaptability to Evolving Threats

Existing SIEM solutions often exhibit a reactive posture against the dynamic and increasingly sophisticated cyber threat landscape. While rule updates can be applied, their inherent reliance on predefined patterns can render them less effective against novel attack techniques, polymorphic malware, and zero-day exploits, necessitating continuous adaptation and integration of advanced analytical capabilities.

3 MACHINE LEARNING FOR SECURITY ANALYTICS

Machine Learning (ML) significantly enhances the analytical power of SIEM systems by enabling intelligent event correlation and robust anomaly detection [13]. Supervised and unsupervised learning models help classify known threats and detect previously unseen patterns, while deep and reinforcement learning expand capabilities for processing complex data and adapting to evolving attack behaviours. Effective integration of ML into SIEM involves structured data pipelines, model training, and continuous tuning to maintain relevance. These intelligent models reduce false positives, improve threat detection accuracy, and streamline incident response, making ML an essential component for modern, adaptive SIEM solutions in dynamic cybersecurity environments [14][15].

3.1 Machine Learning Categories Used in SIEM

Machine Learning (ML) techniques applied within Security Information and Event Management (SIEM) systems typically fall into distinct categories, each offering unique advantages for threat detection and analysis. The predominant categories include Supervised Learning, Unsupervised Learning, and the emerging applications of Reinforcement and Deep Learning [16]:

3.1.1 Supervised Learning

Supervised learning models are extensively utilized in SIEM for tasks involving labelled historical data. Algorithms learn a mapping from input features to known output outcomes, enabling the classification or prediction of new events. In a SIEM context, this involves training models on events explicitly marked as malicious or benign to detect known threats, classify network traffic, or identify specific attack types (e.g., phishing, brute-force). Common algorithms include Support Vector Machines, Decision Trees, and Random Forests, effective for recognizing previously observed attack patterns.

3.1.2 Unsupervised Learning

Unsupervised learning techniques are particularly valuable in SIEM, where labelled data is scarce or the objective is to uncover novel threats. These algorithms identify hidden patterns, structures, or anomalies in unlabelled datasets without prior knowledge of the output. Their primary application in SIEM is for anomaly detection and clustering. By learning normal behavioural baselines for users, applications, or network segments, unsupervised models can flag significant deviations as potential indicators of insider threats, compromised accounts, or sophisticated, unknown attack techniques. Techniques like K-Means Clustering and Isolation Forests are frequently used for identifying outliers or grouping similar events.

3.1.3 Reinforcement Learning

RL involves an agent learning optimal actions through interaction with an environment to maximize a reward. In SIEM, RL could potentially enable adaptive defensive strategies, optimize alert correlation rules, or facilitate autonomous responses by learning from the outcomes of past actions. While largely in research for direct response, its potential for dynamic security policy management is significant.

3.1.4 Deep Learning

DL, a subset of ML using deep neural networks, excels at learning complex representations from high-dimensional and sequential data. In SI [17]EM, DL models (e.g., CNNs, RNNs) are highly effective for processing raw log entries, network packets, and event streams. They automatically extract intricate features for advanced malware detection, sophisticated anomaly detection in network traffic, and analyzing unstructured threat intelligence, making them powerful for complex pattern recognition in cybersecurity.

3.2 Integration Of ML Models Into SIEM

Integrating Machine Learning (ML) models into SIEM systems is a multi-stage process designed to enhance analytical capabilities. The initial step involves establishing robust data pipelines to ensure all heterogeneous security data (from various sources) is properly ingested, parsed, normalized, and enriched. This meticulous pre-processing is crucial for providing the high-quality data necessary for accurate ML model training and inference. Subsequently, the process focuses on the selection, training, and deployment of appropriate ML models based on specific security use cases. Models are rigorously trained on historical data, refined for accuracy, and then deployed, either directly within the SIEM or as integrated external modules. Finally, successful integration requires a continuous feedback loop and operationalization. ML models need ongoing tuning and retraining to adapt to environmental and threat changes. Alerts generated by ML must seamlessly integrate into SIEM's incident response workflows, allowing analysts to validate findings and provide feedback, ensuring continuous effectiveness and actionable intelligence.

4 INTELLIGENT EVENT CORRELATION AND ANOMALY DETECTION IN SIEM

Intelligent event correlation and anomaly detection are at the core of machine learning-driven SIEM enhancements. Traditional detection methods struggle to handle the complexity, scale, and evolving nature of modern cybersecurity threats [18]. The event correlation process is the process of finding the relationships between events. Correlation creates context between individual events and information previously collected in real-time, and also normalizes it for subsequent processing [19]. The primary purpose of alert correlation is to identify the most significant events in the security dataset. Security event correlation should increase the quality of information about events while decreasing their number and interpreting multiple alarms. Figures 2-3 show diagrams for a better understanding of the relationships between the terms.

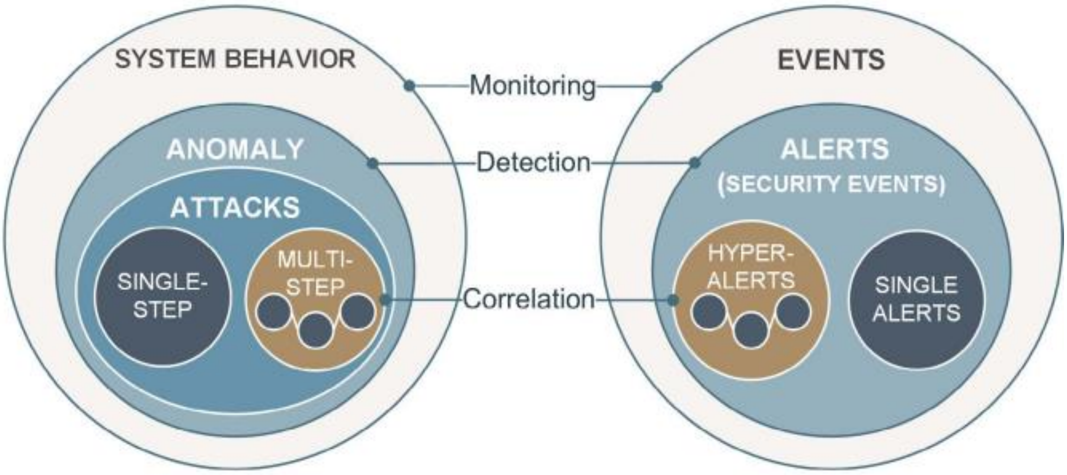

Figure 2: Role of correlation in security event management [10]

In Figure 2, events are the result of system behaviour monitoring, and alerts or security events are the results of abnormal activity detection, which also include single-step and multi-step attacks. The correspondences between concepts are indicated by color. The security event correlation process, in turn, allows one to define relationships between single alerts, at the same time the related alerts can be combined into a meta-event or a hyper-alert and categorized in different ways.

The Figure 3 shows the relationships between the main concepts in the security event management [20]. We can trace the relationships between the previously mentioned terms of intrusion detection, SIEM and alert correlation (indicated by colour) [21].Intrusion detection is the source of security events. These events are monitored by SIEM system and then correlated in the management process [22].

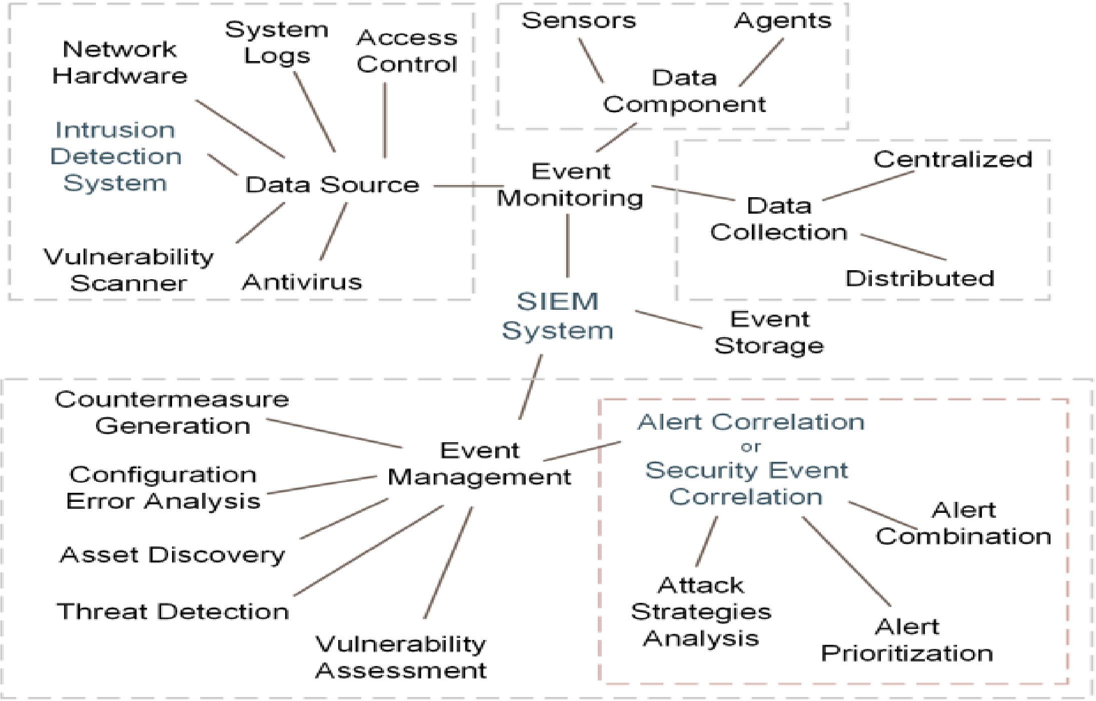

Figure 3: Security event management relations [10]

4.1 Anomaly Detection Models and Techniques

Anomaly Detection has been known as the process of detecting abnormalities and outliers in data. Essentially anomaly detection aims to recognize data instances that differ considerably from the bulk of data instances, hence the name anomaly detection or sometimes novelty discovery [23]. A collective or group anomaly occurs when a group of comparable data examples deviates from the predicted behavior of the entire dataset. Figure 4 shows the types of anomalies [24].

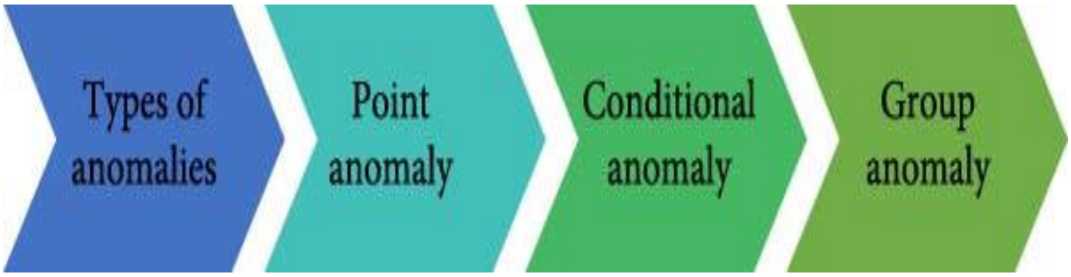

Figure 4: Types of anomalies [24]

Anomaly detection can therefore be split into three broad categories based on the training data function used to build the model. The three broad classes are:

- **Supervised anomaly detection:** In this class, both the normal and anomalous training datasets contain labelled instances. In this model, the approach is to build a predictive model for both anomaly and normal classes and then compare these two models.
- **Semi-supervised anomaly detection:** Semi-supervised techniques presume that training data have labelled instances for the normal class alone. Since they do not need anomaly class labels, they are more common than supervised methods.
- **Unsupervised anomaly detection:** those methods imply that normal instances are much more common than anomalies in test datasets. However, if the assumption fails, it leads to a high false alarm rate for this technique [25].

4.2 Real-World Applications and Use Cases

Real-world usage of machine learning integration in SIEM platforms has grown, especially in sectors with high data volumes and frequent cyberthreats. Businesses in industries like government, healthcare, energy, and finance are using machine learning (ML) to improve their SIEM systems in order to discover anomalies early and correlate events more precisely [26]. These features are especially helpful in detecting advanced persistent attacks (APTs), insider threats, and zero-day vulnerabilities that are difficult to detect using signatures. Key real-world use cases include:

- **Financial Institutions:** Detecting fraudulent transactions, account takeovers, and unusual user behavior through anomaly detection models like Isolation Forests and autoencoders [27].
- **Healthcare Systems:** Monitoring medical devices, EHR access logs, and user behaviors to detect policy violations and insider threats in compliance with HIPAA regulations.
- **Cloud-Based Environments:** Implementing ML-enhanced SIEMs to detect cross-tenant attacks, data exfiltration, and privilege escalations in multi-cloud or hybrid infrastructures.
- **Security Operation Centres (SOCs):** Automating alert triage and correlating dispersed alerts to form a coherent attack narrative, reducing alert fatigue and enhancing analyst efficiency [28][29].

5 LITERATURE REVIEW

The section provides an overview of recent advancements in SIEM systems, emphasizing their integration with Zero Trust Architecture and machine learning. It highlights key functionalities, correlation methods, and challenges in enhancing threat detection and cybersecurity effectiveness.

Ahuja, Vashisth and Thakur (2025) explores the core principles of Zero Trust, examines the key functions and roles of SIEM systems, and outlines effective integration strategies. Through real-world case studies and the lessons learned from various implementations, the paper provides insights into how organizations can leverage this integration to enhance threat detection, streamline incident response, and improve overall security posture [30].

Thorat et al. (2025) gives a broad look at where ML-driven SIEM solutions stand right now, focusing on their main parts, pros, and cons. Unlike standard SIEM systems, ML-driven SIEMs can learn from data on their own and get better at detecting things over time without having to change their rules by hand. ML techniques like supervised learning, unsupervised learning, and reinforcement learning also help SIEM systems find complex attack trends, zero-day threats, and more accurately tell the difference between normal and hostile activity. ML-driven SIEMs can also process and analyze huge amounts of security data quickly and efficiently when big data technologies are added [31].

Tech, Kumar and Asst (2024) used Isolation Forest Algorithm which is best to separate the normal instances and anomalies. This Machine learning approach reduces the false positive rates and increases anomaly detection. this paper aims to reveal the possible changes in the cybersecurity sphere due to the implementation of machine learning and promote further development of the technology as an addition to the existing SIEM systems. Adopting these advancements is an effective way of strengthening the security of any organization, thus providing a safer and more secure digital environment [32].

Ehis (2023) hereby strikes a compromise between lowering false positive alerts and not ignoring any potential abnormalities that could indicate a cyberattack when establishing SIEM correlation rules. In order to decide which data is pertinent and which data is irrelevant in an event pipeline, this research employs the use of filters. Through this examination, it can be inferred that the conditions are advantageous for promoting investment in the growth and enhancement of this technology as an essential component of industrial control systems with security operation centres, as well as offering cybersecurity management for small and medium-sized enterprises (SMEs) with restricted security expertise and capabilities [33].

Kotenko, Gaifulina and Zelichenok (2022) presents a systematization of security event correlation methods into several categories, applied correlation methods, knowledge extraction methods, used data sources, architectural solutions, and quality evaluation of correlation methods. The research method is a systematic literature review, which includes the formulation of research questions, the choice of keywords and criteria for inclusion and exclusion. The review corpus is formed by using search queries in Google Scholar, IEEE Xplore, ACM Digital Library, ScienceDirect, and selection criteria. The final review corpus includes 127 publications from the existing literature for 2010-2021 and reflects the current state of research in the security event correlation field [10].

Okamoto (2021) integrating machine learning (ML) technology, SIEM systems can significantly improve the accuracy, speed, and adaptability of intrusion detection mechanisms, allowing for proactive cybersecurity measures. Machine learning brings a data-driven, adaptive approach to threat detection in SIEM systems. Traditional SIEM setups, while capable of aggregating logs and alerts from various network components, can be limited by the predefined rules and static models [34].

Despite these advancements, existing studies reveal several limitations in the integration of machine learning with SIEM systems. Current approaches often focus on isolated algorithms or conceptual frameworks without providing scalable, real-time validation across diverse environments. Challenges such as high false positives, lack of adaptive rule learning, limited empirical benchmarks, and difficulties in cloud-native deployment remain unresolved. As summarized in Table 1, while prior research demonstrates promising improvements in anomaly detection, event correlation, and Zero Trust integration, there is still a clear need for comprehensive, adaptive, and benchmarked ML-driven SIEM frameworks that can operate effectively in dynamic cybersecurity landscapes.

TABLE I. SUMMARY OF THE STUDY ON MACHINE LEARNING IN SIEM INTELLIGENT EVENT CORRELATION AND ANOMALY DETECTION

Reference	Study On	Approach	Key Findings	Challenges	Future Work
Ahuja, Vashisth, and Thakur (2025)	Integration of SIEM with Zero Trust Architecture	Conceptual with case studies	Enhances threat detection and incident response through combined strengths	Limited technical detail and scalability issues	Develop scalable frameworks for SIEM-ZTA integration in cloud-native environments

Thorat et al. (2025)	ML-driven SIEM components and workflows	Overview of ML in SIEM operations	Automates threat detection and handles large datasets efficiently	Lacks real-time validation and performance benchmarks	Explore adaptive ML models with real-time training capabilities
Tech, Kumar, and Asst (2024)	Anomaly detection using Isolation Forest	Algorithm-based implementation	Reduces false positives and improves anomaly detection	Focuses on a single method without system-wide evaluation	Extend evaluation using hybrid and ensemble models within SIEM
Ehis (2023)	Optimization of SIEM correlation rules	Filtering techniques in event pipelines	Reduces false alerts while maintaining detection accuracy	Does not integrate adaptive rule learning	Implement intelligent, self-adjusting rule systems
Kotenko, Gaifulina, and Zelichenok (2022)	Event correlation methods in SIEM	Systematic literature review	Categorizes methods by architecture and evaluation metrics	Absence of empirical performance assessments	Establish benchmark datasets for comparative testing of correlation methods
Okamoto (2021)	ML-enhanced SIEM for intrusion detection	Comparative analysis	ML improves detection accuracy, speed, and adaptability	Real-time application and generalization limitations	Study adversarial robustness and real-time ML deployment strategies

6 CONCLUSION AND FUTURE WORK

Harnessing advanced analytics and adaptive learning capabilities, modern SIEM platforms are evolving into intelligent security solutions that can detect and respond to dynamic threats. Enhanced by machine learning, these systems deliver deeper insights, real-time correlation, and proactive anomaly detection to tackle the complexity of modern cybersecurity challenges. As cyber threats become more sophisticated, automation and intelligence in event management are no longer optional but essential. This review highlighted how machine learning significantly improves traditional SIEM functionalities by reducing false positives, increasing detection accuracy, and streamlining response workflows. Various ML techniques—including supervised, unsupervised, and deep learning models—enable contextual analysis and robust event correlation, addressing key limitations of static rule-based systems. Additionally, the integration of ML models has demonstrated effective real-world applications across critical sectors such as finance, healthcare, and cloud infrastructure. Going forward, future SIEM advancements must prioritize model explain ability, scalability, and continuous learning to ensure resilient and adaptive cybersecurity defences. Future research should focus on enhancing the explain ability and transparency of machine learning models within SIEM systems to build trust and support informed decision-making. Integrating federated learning and edge-based analytics can improve data privacy and scalability. Additionally, continuous model adaptation and the fusion of threat intelligence with real-time analytics will be crucial for developing more autonomous, resilient, and context-aware cybersecurity solutions.

REFERENCES

[1] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large- Scale Cybersecurity Networks Data Analysis : A Comparative Study," *TIJER – Int. Res. J.*, vol. 11, no. 12, pp. 922–928, 2024.

[2] S. Tatineni, "Machine Learning Approaches For Anomaly Detection In Cybersecurity: A Comparative Analysis," *Int. J. Comput. Eng. Technol.*, vol. 12, pp. 42–50, 2021.

[3] P. Nutalapati, J. R. Vummadi, S. Dodda, and N. Kamuni, "Advancing Network Intrusion Detection: A Comparative Study of Clustering and Classification on NSL-KDD Data," in *2025 International Conference on Data Science and Its Applications (ICoDSA)*, IEEE, Jul. 2025, pp. 880–885. doi: 10.1109/ICoDSA67155.2025.11157595.

[4] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," *Sensors*, vol. 21, no. 14, 2021, doi: 10.3390/s21144759.

[5] H. Maosa, K. Ouazzane, and M. C. Ghanem, "A Hierarchical Security Event Correlation Model for Real-Time Threat Detection and Response," *Network*, vol. 4, no. 1, pp. 68–90, 2024, doi: 10.3390/network4010004.

[6] N. Miloslavskaya, "Analysis of SIEM Systems and Their Usage in Security Operations and Security Intelligence Centers," in *2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, vol. 1, 2018, pp. 282–288. doi: 10.1007/978-3-319-63940-6_40.

[7] R. Patel, "Automated Threat Detection and Risk Mitigation for ICS (Industrial Control Systems) Employing Deep Learning in Cybersecurity Defence," *Int. J. Curr. Eng. Technol.*, vol. 13, no. 06, pp. 584–591, 2023, doi: 10.14741/ijcet/v.13.6.11.

[8] A. Nurusheva, N. Medelbayeva, D. Satybaldina, and N. Goranin, "Machine learning algorithms in SIEM systems for enhanced detection and management of security events," *Bull. L.N. Gumilyov Eurasian Natl. Univ. Math. Comput. Sci. Mech. Ser.*, vol. 148, pp. 6–17, 2024, doi: 10.32523/bulmathenu.2024/3.1.

[9] G. Sarraf, "Behavioral Analytics for Continuous Insider Threat Detection in Zero-Trust Architectures," *Int. J. Res. Anal. Rev.*, vol. 8, no. 4, pp. 596–602, 2021.

[10] I. Kotenko, D. Gaifulina, and I. Zelichenok, “Systematic Literature Review of Security Event Correlation Methods,” *IEEE Access*, vol. 10, pp. 43387–43420, 2022, doi: 10.1109/ACCESS.2022.3168976.

[11] P. Shirazi and A. Padyab, “Discerning Challenges of Security Information and Event Management (SIEM) Systems in Large Organizations,” in *International Symposium on Human Aspects of Information Security and Assurance*, 2025, pp. 339–354. doi: 10.1007/978-3-031-72559-3_23.

[12] A. Omoseebi, D. Jonson, and D. Robert, “Challenges of integrating various data sources in SIEM.,” 2022.

[13] V. Thangaraju, “Enhancing Web Application Performance and Security Using AI-Driven Anomaly Detection and Optimization Techniques,” *Int. Res. J. Innov. Eng. Technol.*, vol. 9, no. 3, 2025, doi: 47001/IRJIET/2025.903027.

[14] H. Kali, “The Future Of Hr Cybersecurity: Ai-Enabled Anomaly Detection In Workday Security.,” *Int. J. Recent Technol. Sci. Manag.*, vol. 8, no. 6, 2023, doi: 10.10206/IJRTSM.2025803096.

[15] N. K. Prajapati, “Federated Learning for Privacy-Preserving Cybersecurity: A Review on Secure Threat Detection,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 4, pp. 520–528, Apr. 2025, doi: 10.48175/IJARSCT-25168.

[16] R. Dattangire, R. Vaidya, D. Biradar, and A. Joon, “Exploring the Tangible Impact of Artificial Intelligence and Machine Learning: Bridging the Gap between Hype and Reality,” in *2024 1st International Conference on Advanced Computing and Emerging Technologies (ACET)*, IEEE, 2024, pp. 1–6. doi: 10.1109/ACET61898.2024.10730334.

[17] S. Amrale, “A Novel Generative AI-Based Approach for Robust Anomaly Identification in High-Dimensional Dataset,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, no. 2, pp. 709–721, 2024, doi: 10.48175/IJARSCT-19900D.

[18] E. Krzysztoń, I. Rojek, and D. Mikołajewski, “A Comparative Analysis of Anomaly Detection Methods in IoT Networks: An Experimental Study,” *Appl. Sci.*, vol. 14, no. 24, 2024, doi: 10.3390/app142411545.

[19] D. Levshun and I. Kotenko, “A survey on artificial intelligence techniques for security event correlation: models, challenges, and opportunities,” *Artif. Intell. Rev.*, vol. 56, no. 8, pp. 8547–8590, Aug. 2023, doi: 10.1007/s10462-022-10381-4.

[20] V. Shewale, “Demystifying the MITRE ATT&amp;amp;CK Framework: A Practical Guide to Threat Modeling,” *J. Comput. Sci. Technol. Stud.*, vol. 7, no. 3, pp. 182–186, May 2025, doi: 10.32996/jcsts.2025.7.3.20.

[21] D. Patel, “Leveraging Blockchain and AI Framework for Enhancing Intrusion Prevention and Detection in Cybersecurity,” *Tech. Int. J. Eng. Res.*, vol. 10, no. 6, pp. 853–858, 2023, doi: 10.56975/tijer.v10i6.158517.

[22] S. Narang and A. Gogineni, “Zero-Trust Security in Intrusion Detection Networks: An AI-Powered Threat Detection in Cloud Environment,” *Int. J. Sci. Res. Mod. Technol.*, vol. 4, no. 5, pp. 60–70, Jun. 2025, doi: 10.38124/ijsrmt.v4i5.542.

[23] S. Natha, “A Systematic Review of Anomaly detection using Machine and Deep Learning Techniques,” *Quaid-e-Awam Univ. Res. J. Eng. Sci. Technol.*, vol. 20, pp. 83–94, 2022, doi: 10.52584/QRJ.2001.11.

[24] S. Kumari, C. Prabha, A. Karim, M. M. Hassan, and S. Azam, “A Comprehensive Investigation of Anomaly Detection Methods in Deep Learning and Machine Learning: 2019–2023,” *IET Inf. Secur.*, vol. 2024, no. 1, Jan. 2024, doi: 10.1049/2024/8821891.

[25] J. Ogundiran, E. Asadi, and M. da Silva, “A Systematic Review on the Use of AI for Energy Efficiency and Indoor Environmental Quality in Buildings,” *Sustainability*, vol. 16, no. 9, 2024, doi: 10.3390/su16093627.

[26] R. Q. Majumder, “A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems,” *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 10, pp. 101–110, Apr. 2025, doi: 10.48175/IJARSCT-25619.

[27] S. B. Shah, “Advancing Financial Security with Scalable AI: Explainable Machine Learning Models for Transaction Fraud Detection,” in *2025 4th International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE)*, IEEE, Apr. 2025, pp. 1–7. doi: 10.1109/ICDCECE65353.2025.11034838.

[28] V. Panchal, “Mobile SoC Power Optimization : Redefining Performance with Machine Learning Techniques,” *IJIRSET*, vol. 13, no. 12, pp. 1–17, 2024, doi: 10.15680/IJIRSET.2024.1312117.

[29] A. Ahmed, “Advancements in Anomaly Detection: A Review of Machine Learning Applications in Cyber-Physical System Networks,” May 22, 2024. doi: 10.21203/rs.3.rs-4412375/v1.

[30] L. Ahuja, S. Vashisth, and A. Thakur, “Integrating SIEM with Zero Trust Architecture,” in *2025 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, IEEE, Jan. 2025, pp. 1–6. doi: 10.1109/IITCEE64140.2025.10915422.

[31] S. Thorat, S. S. Dari, K. Ahuja, A. Ingle, J. P. Dhamone, and S. H. Lavate, “Machine Learning-Driven Security Information and Event Management (SIEM),” in *Innovations in Information and Decision Sciences*, V. Bhateja, M. Dey, and R. Senkerik, Eds., Singapore: Springer Nature Singapore, 2025, pp. 525–542.

[32] R. Arora and V. K. Kharbas, “Machine Learning-Driven Anomaly Detection : Strengthening Siem Tools For Robust Cyber Defense,” vol. 45, no. 3, pp. 823–836, 2024.

[33] A.-M. T. Ehis, “Optimization of Security Information and Event Management (SIEM) Infrastructures, and Events Correlation/Regression Analysis for Optimal Cyber Security Posture,” *Arch. Adv. Eng. Sci.*, no. July, pp. 1–10, Jul. 2023, doi: 10.47852/bonviewAAES32021068.

[34] 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.