Tharushi Jayasuriya, 2018, 6:1
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

The impact of AI-integrated SIEM systems on real-time threat correlation

Tharushi Jayasuriya
University of Peradeniya, Sri Lanka

Abstract - Security Information and Event Management (SIEM) systems play a critical role in modern cybersecurity, enabling organizations to aggregate, monitor, and analyze security events across diverse IT infrastructures. However, traditional SIEM solutions often face limitations in handling high volumes of heterogeneous security data, leading to delayed threat detection, false positives, and inefficient incident response. The integration of Artificial Intelligence (AI) into SIEM platforms represents a transformative advancement, allowing for automated, intelligent threat correlation in real time. AI techniques, including machine learning, deep learning, natural language processing, and reinforcement learning, enhance the ability of SIEM systems to identify complex attack patterns, correlate multi-source events, and prioritize alerts based on risk and context. This review examines the impact of AI-enhanced SIEM systems on real-time threat correlation, highlighting improvements in detection accuracy, response speed, and predictive analytics. It also discusses challenges related to data quality, computational requirements, adversarial attacks, and integration with existing systems. Finally, the article explores future directions, including hybrid SIEM approaches, federated learning, and autonomous security operations. By leveraging AI, organizations can transform SIEM platforms from reactive monitoring tools into proactive, intelligent cybersecurity frameworks capable of addressing increasingly sophisticated and dynamic threats.

Keywords - AI, SIEM, Threat Correlation, Real-Time Security, Machine Learning, Cybersecurity Analytics, Anomaly Detection, Predictive Threat Intelligence.

I. INTRODUCTION

The Growing Complexity of Cybersecurity Threats

In today's digital landscape, organizations face an unprecedented volume and sophistication of cybersecurity threats. The rapid proliferation of connected devices, cloud-based services, and remote work infrastructures has exponentially increased the attack surface for cybercriminals. Threats range from simple malware infections to advanced persistent threats (APTs) and multi-stage intrusions that exploit vulnerabilities across multiple systems. As the frequency and complexity of attacks grow, traditional security measures often struggle to keep pace, leaving organizations vulnerable to financial losses, operational disruption, and reputational damage. Detecting and responding to threats in real time has become a critical priority for enterprises, requiring innovative approaches that go beyond conventional cybersecurity tools.

Role of SIEM Systems in Modern Security

Security Information and Event Management (SIEM) systems are central to contemporary cybersecurity strategies, providing organizations with a platform for collecting, aggregating, and analyzing security events from diverse IT assets. By correlating logs from network devices, servers, endpoints, and applications, SIEM systems help security teams detect suspicious activity, generate alerts, and investigate incidents. Traditional SIEM solutions, however, rely heavily on static rule-based correlation and predefined signatures. While effective in identifying known threats, these systems often produce high volumes of alerts, many of which are false positives. Manual analysis and incident response processes can further delay mitigation,

reducing the system's ability to address real-time threats effectively.

Limitations of Conventional Threat Correlation

The conventional SIEM approach faces several significant challenges in the context of modern cybersecurity. First, the sheer volume of security data generated across large organizations can overwhelm traditional correlation engines, making it difficult to identify critical events promptly. Second, sophisticated attacks, such as multi-stage intrusions or lateral movement within networks, may bypass signature-based detection or evade predefined correlation rules. Third, static SIEM systems lack the adaptability to learn from new threat patterns, making them reactive rather than proactive. These limitations underscore the need for enhanced intelligence and automation in real-time threat correlation.

Emergence of AI in SIEM

Artificial Intelligence (AI) offers a promising solution to overcome these limitations by introducing automated, adaptive, and predictive capabilities into SIEM systems. AI techniques, including machine learning, deep learning, natural language processing, and reinforcement learning, enable SIEM platforms to analyze complex, high-dimensional datasets in real time, recognize anomalous patterns, and correlate events across multiple sources. By learning from historical data and continuously updating models based on new threats, AI-integrated SIEM systems improve detection accuracy, reduce false positives, and prioritize critical alerts efficiently. Additionally, AI allows SIEM to perform predictive analytics, anticipating potential attacks and enabling proactive mitigation strategies.

Purpose and Scope of the Study

This article aims to explore the impact of AI integration on real-time threat correlation within SIEM systems. It examines the key AI techniques employed, their influence on detection accuracy, alert prioritization, and operational efficiency, and the challenges associated with deploying AI-enhanced SIEM platforms. Furthermore, the study investigates emerging trends, including hybrid correlation models, autonomous SIEM systems, and predictive threat analytics. By evaluating both the advantages and limitations of AI in SIEM, this paper provides a comprehensive perspective on how AI-driven intelligence can transform traditional security monitoring into a proactive, real-time cybersecurity framework capable of addressing the growing complexity of digital threats.

II. BACKGROUND AND LITERATURE REVIEW

Traditional SIEM Systems

Traditional SIEM systems serve as centralized platforms that collect, normalize, and analyze security events from multiple sources, including network devices, servers, applications, and endpoints. These systems rely on predefined correlation rules, signature databases, and heuristics to identify potential threats. While effective against known attacks, these approaches struggle with the increasing complexity of modern cyber threats. High volumes of heterogeneous data can overwhelm SIEM systems, resulting in delayed detection, excessive false positives, and missed attacks.

Challenges in Threat Correlation

Real-time threat correlation involves analyzing and linking events from multiple sources to identify malicious activities. Manual or rule-based correlation faces significant limitations, including the inability to process large-scale data efficiently, poor adaptability to unknown attack patterns, and the requirement for extensive expert input. As attacks become more sophisticated, the inadequacy of traditional SIEM systems underscores the need for adaptive intelligence in threat detection.

AI in Cybersecurity

AI and machine learning have been increasingly applied to cybersecurity, enabling automated threat detection, anomaly recognition, and predictive analytics. Supervised learning models classify events based on historical data, while unsupervised learning methods detect novel threats through anomaly detection. Reinforcement learning enables systems to optimize response strategies iteratively, and deep learning models identify complex, multi-stage attacks across high-dimensional datasets. These

techniques allow SIEM systems to correlate events intelligently and adaptively, improving overall situational awareness.

Prior Studies on AI-Enhanced SIEM

Recent research demonstrates the advantages of AI integration in SIEM. Studies report improvements in detection accuracy, reduction in false positives, and faster response times. AI models can prioritize critical alerts, identify previously unseen threats, and detect attack chains spanning multiple systems. By leveraging machine learning and AI-driven analytics, SIEM platforms transition from reactive monitoring tools to proactive, intelligence-driven security frameworks.

AI Techniques in SIEM Systems

The integration of Artificial Intelligence (AI) into Security Information and Event Management (SIEM) systems represents a significant advancement in cybersecurity. Traditional SIEM platforms rely on static rules and signatures, which often fail to detect sophisticated or novel attacks. AI enhances SIEM by enabling automated, adaptive, and predictive analysis of large-scale security data. By leveraging machine learning, deep learning, natural language processing, and reinforcement learning, AI-driven SIEM systems can identify complex threats, correlate events across heterogeneous sources, and prioritize alerts in real time.

Machine Learning Models

Machine learning (ML) forms the foundation of AI-enhanced SIEM systems. Supervised learning algorithms, such as decision trees, support vector machines (SVM), and random forests, classify events by learning from historical labeled datasets. These models are particularly effective for detecting known attack patterns, phishing attempts, and malware signatures.

Unsupervised learning methods, including clustering, principal component analysis, and autoencoders, are designed to detect anomalies in network behavior without prior knowledge of attack signatures. This capability allows SIEM systems to identify novel threats, including zero-day exploits, lateral movements, and unusual user behaviors. ML models continuously refine their decision-making capabilities by incorporating feedback from newly observed data, reducing false positives and improving threat detection over time.

Real-world deployments of ML in SIEM have demonstrated substantial improvements in event classification and alert prioritization. For example, enterprise SIEM platforms now use ML algorithms to automatically cluster related events, identifying suspicious activity that might otherwise go unnoticed in high-volume log data.

Deep Learning Approaches

Deep learning, a subset of machine learning, uses multi-layered neural networks to analyze high-dimensional data. Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) are commonly applied to security analytics. CNNs excel at identifying structured patterns in large datasets, such as network traffic flows or system logs, while RNNs are ideal for sequential and temporal analysis, detecting multi-stage or time-dependent attacks.

Deep learning models can uncover sophisticated threats, such as Advanced Persistent Threats (APTs) or coordinated attacks that span multiple network nodes. By processing millions of events in real time, these models provide SIEM systems with enhanced pattern recognition capabilities, allowing the detection of complex attack chains that static rule-based approaches would miss.

Natural Language Processing (NLP) and Knowledge Graphs

NLP techniques are increasingly integrated into SIEM systems to process textual threat intelligence feeds, security reports, and incident logs. NLP enables automated extraction of entities, indicators of compromise (IOCs), and attack relationships from unstructured data.

Knowledge graphs complement NLP by representing the relationships among threats, vulnerabilities, assets, and events in a structured format. They enable SIEM systems to enrich event correlation with contextual information, improving the understanding of complex attacks. For instance,

a knowledge graph can link an unusual network login to a known malware campaign, helping analysts prioritize critical threats effectively.

Reinforcement Learning for Adaptive Response

Reinforcement learning (RL) allows SIEM systems to learn optimal response strategies through continuous interaction with the network environment. In RL-based SIEM, the system receives feedback on the effectiveness of its actions, such as blocking traffic, quarantining devices, or generating alerts. Successful mitigation is reinforced, while ineffective actions are penalized.

RL is particularly effective for adaptive threat management, enabling SIEM systems to prioritize alerts, automate response policies, and continuously improve over time. By learning from both historical and real-time events, reinforcement learning enhances the system's ability to respond to dynamic and evolving threats without constant human intervention.

Integration Frameworks for AI-Enhanced SIEM

Integrating AI techniques into SIEM requires robust frameworks that combine data ingestion, normalization, model training, and real-time analytics. AI-enhanced SIEM platforms must handle multi-source log data from network devices, endpoints, cloud services, and applications. These frameworks ensure seamless integration of AI models, real-time event processing, and scalable performance for high-volume enterprise environments.

Additionally, AI frameworks provide visualization tools and alert dashboards for security analysts, enabling them to interpret AI-generated insights, validate detections, and make informed decisions. Hybrid frameworks that combine AI-driven analytics with traditional rule-based correlation offer the best balance between automation and human oversight.

Impact on Real-Time Threat Correlation

AI integration has significantly transformed the ability of SIEM systems to perform real-time threat correlation, improving both the speed and accuracy of security operations. Traditional SIEM platforms often rely on static rules and predefined signatures to link events, which can result in delayed detection and high false-positive rates. In contrast, AI-enhanced SIEM systems leverage machine learning, deep learning, NLP, and reinforcement learning to correlate complex events from diverse data sources dynamically. This enables organizations to identify sophisticated threats more effectively and respond proactively, rather than reactively, to cyber incidents.

Improved Detection Accuracy

One of the most notable impacts of AI on SIEM is the improvement in detection accuracy. AI models can analyze large volumes of multi-source security data to uncover subtle patterns indicative of malicious activity. Supervised learning algorithms classify known attack patterns efficiently, while unsupervised models detect anomalies in network behavior that may signal zero-day attacks or emerging threats. By continuously learning from historical and real-time data, AI-enhanced SIEM platforms reduce false positives, ensuring that analysts focus on genuine incidents rather than sifting through irrelevant alerts. This accuracy is particularly valuable in complex enterprise environments, where thousands of events occur every second.

Accelerated Response and Mitigation

Real-time correlation enabled by AI significantly reduces the mean time to detect (MTTD) and mean time to respond (MTTR). Automated alert prioritization and risk scoring allow security teams to address critical threats immediately, while reinforcement learning models can suggest or implement optimal mitigation actions without human intervention. This rapid response capability limits the potential damage from attacks, containing malware propagation, data exfiltration, or system compromise before they escalate.

Detection of Sophisticated, Multi-Stage Attacks

AI-enhanced SIEM systems excel at identifying complex attack chains that span multiple network nodes and timeframes. Deep learning models, such as recurrent neural networks (RNNs), are particularly effective in recognizing temporal correlations between sequential events. Knowledge graphs and NLP techniques enrich event data with contextual

intelligence, linking seemingly isolated incidents into coherent attack narratives. As a result, multi-stage intrusions, lateral movements, and coordinated attacks that would otherwise go undetected can be identified in near real time.

Case Studies and Operational Evidence

Empirical studies and industry reports demonstrate measurable improvements in SIEM performance through AI integration. Organizations implementing AI-driven SIEM report higher detection rates, faster incident triage, and reduced alert fatigue among analysts. For example, the application of machine learning models in enterprise environments has shown a reduction of false positives by up to 40%, while detection of complex threats improved by 30–50%, highlighting the operational benefits of AI-enhanced event correlation.

In summary, AI integration in SIEM systems has fundamentally improved real-time threat correlation by enhancing detection accuracy, accelerating response, and enabling the identification of sophisticated multi-stage attacks. By automating complex event analysis and providing predictive insights, AI-driven SIEM platforms empower organizations to respond to threats proactively, strengthening their cybersecurity posture against an increasingly dynamic and sophisticated threat landscape.

Challenges and Limitations

Despite the substantial benefits of AI integration in SIEM systems, several challenges and limitations remain that can affect their effectiveness and adoption. One of the primary concerns is data quality and consistency, as AI models rely heavily on accurate, normalized, and comprehensive input from diverse sources, including network devices, endpoints, applications, and cloud services; incomplete or inconsistent data can lead to misclassifications, missed threats, or false positives. Computational complexity and resource requirements also pose significant challenges, particularly for deep learning models and real-time analytics, which demand high-performance processing power and memory to handle the volume, velocity, and variety of security events in large-scale enterprise networks. Additionally, AI models are vulnerable to adversarial attacks, where malicious actors deliberately manipulate input data to evade detection or mislead the system, potentially undermining automated threat correlation and response.

Biases in training data may further impact model accuracy, disproportionately prioritizing certain threats while overlooking others, which can create security blind spots. Integration with existing SIEM platforms and legacy systems can be complex, requiring careful architecture planning to ensure compatibility, scalability, and operational continuity, while balancing automation with human oversight. Another consideration involves regulatory and compliance requirements, as automated decision-making must be auditable and explainable to meet legal and organizational standards for data privacy and accountability.

Furthermore, maintaining AI models over time requires continuous monitoring, retraining, and validation to adapt to evolving attack techniques, which introduces ongoing operational overhead. Collectively, these challenges highlight the need for hybrid approaches that combine AI-driven analytics with traditional rule-based detection, human expertise, and robust data governance practices to ensure reliable, efficient, and secure real-time threat correlation within modern SIEM deployments.

III. CONCLUSION

AI-integrated Security Information and Event Management (SIEM) systems have emerged as a transformative advancement in the field of cybersecurity, fundamentally altering how organizations detect, correlate, and respond to threats. Traditional SIEM platforms, while effective at aggregating logs and applying predefined rules, often struggle to keep pace with the increasing volume, complexity, and sophistication of modern cyber-attacks. By embedding artificial intelligence techniques such as machine learning, deep learning, natural language processing (NLP), and reinforcement learning SIEM systems can now analyze vast amounts of heterogeneous security

data in real time, identify complex attack patterns, and correlate events across multiple sources automatically. This integration significantly enhances detection accuracy, enabling the identification of both known and previously unseen threats while reducing false positives that traditionally overwhelm security analysts.

AI-driven threat correlation also improves operational efficiency and accelerates incident response. Automated prioritization and risk scoring allow security teams to focus on high-impact alerts, while predictive analytics and reinforcement learning models provide guidance for optimal mitigation strategies. These capabilities are particularly valuable for detecting multi-stage attacks, lateral movements, and coordinated threats that span multiple network nodes and timeframes scenarios where traditional SIEM systems often fail. By providing comprehensive, contextualized insights, AI-integrated SIEM systems enhance situational awareness across diverse IT environments, from on-premises infrastructure to cloud-based platforms, enabling organizations to proactively defend against emerging threats.

REFERENCE

1. Battula, V. (2014). A new era for CRM: Salesforce automation on a scalable, cloud-native Red Hat foundation. International Journal of Science, Engineering and Technology, 2(8), 5.
2. Battula, V. (2014). Beyond legacy: Modernizing with Red Hat and the open-source stack on hybrid platforms. International Journal of Science, Engineering and Technology, 2(2), 5.
3. Battula, V. (2015). Next-generation LAMP stack governance: Embedding predictive analytics and automated configuration into enterprise Unix/Linux architectures. International Journal of Research and Analytical Reviews (IJRAR), 2(3), 47.
4. Battula, V. (2016). Adaptive hybrid infrastructures: Cross-platform automation and governance across virtual and bare metal Unix/Linux systems using modern toolchains. International Journal of Trend in Scientific Research and Development, 1(1), 47.
5. Battula, V. (2017). Unified Unix/Linux operations: Automating governance with Satellite, Kickstart, and Jumpstart across enterprise infrastructures. International Journal of Creative Research Thoughts (IJCRT), 5(1), 66.
6. Gowda, H. G. (2016). Container intelligence at scale: Harmonizing Kubernetes, Helm, and OpenShift for enterprise resilience. International Journal of Scientific Research & Engineering Trends, 2(4), 1–6.
7. Hong, Z., & Xue-na, P. (2005). A Network Security Information Fusion Based Security Event Analysis and Prediction Model. Journal of Northeastern University.
8. Illa, H. B. (2013). Optimization of data transmission in wireless sensor networks using routing algorithms. International Journal of Current Science (IJCSPUB), 3(4), 17–25.
9. Illa, H. B. (2014). Design and simulation of low-latency communication networks for sensor data transmission. International Journal of Research and Analytical Reviews (IJRAR).
10. Illa, H. B. (2015). Secure cloud connectivity using IPsec and SSL VPNs: A comparative study. TIJER – International Research Journal, 2(5), a12–a35.
11. Illa, H. B. (2016). Bridging academic learning and cloud technology: Implementing AWS labs for computer science education. International Journal of Science, Engineering and Technology, 4(3), 9.
12. Illa, H. B. (2016). Comparative study of wired vs. wireless communication protocols for industrial IoT networks. International Journal of Scientific Research & Engineering Trends, 2(6).
13. Illa, H. B. (2016). Dynamic resource allocation for cloud-based applications using machine learning. International Journal of Scientific Development and Research (IJSDR).
14. Illa, H. B. (2016). Performance analysis of routing protocols in virtualized cloud environments. International Journal of Science, Engineering and Technology, 4(5).
15. Jingxin, W., Wang, Z., & Dai, K. (2007). Security Event Management System based on Mobile Agent Technology. 2007 IEEE Intelligence and Security Informatics, 166-171.
16. Kota, A. K. (2017). Cross-platform BI migrations: Strategies for seamlessly transitioning

dashboards between Qlik, Tableau, and Power BI. International Journal of Scientific Development and Research (IJSDR), 2(63).
17. Liu, L., Li, Z., Xu, L., & Chen, H. (2006). A Security Event Management Framework Using Wavelet and Data-Mining Technique. 2006 International Conference on Communications, Circuits and Systems, 3, 1566-1569.
18. Madamanchi, S. R. (2014). Solaris to Kubernetes: A practical guide to containerizing legacy applications on Linux. International Journal of Science, Engineering and Technology, 2(2), 6.
19. Madamanchi, S. R. (2014). The UNIX-to-Linux journey: A strategic guide for enterprise IT and cloud transformation. International Journal of Science, Engineering and Technology, 2(4), 5.
20. Madamanchi, S. R. (2015). Adaptive Unix ecosystems: Integrating AI-driven security and automation for next-generation hybrid infrastructures. International Journal of Science, Engineering and Technology, 3(2), 47.
21. Madamanchi, S. R. (2017). From compliance to cognition: Reimagining enterprise governance with AI-augmented Linux and Solaris frameworks. International Journal of Scientific Research & Engineering Trends, 3(3), 49.
22. Maddineni, S. K. (2016). Aligning data and decisions through secure Workday integrations with EIB Cloud Connect and WD Studio. Journal of Emerging Technologies and Innovative Research (JETIR), 3(9), 610–617.
23. Maddineni, S. K. (2017). Comparative analysis of compensation review deployments across different industries using Workday. International Journal of Trend in Scientific Research and Development (IJTSRD).
24. Maddineni, S. K. (2017). Dynamic accrual management in Workday: Leveraging calculated fields and eligibility rules for precision leave planning. International Journal of Current Science (IJCSPUB), 7(1), 50–55.
25. Maddineni, S. K. (2017). From transactions to intelligence by unlocking advanced reporting and security capabilities across Workday platforms. TIJER – International Research Journal, 4(12), a9–a16.
26. Maddineni, S. K. (2017). Implementing Workday for contractual workforces: A case study on letter generation and experience letters. International Journal of Trend in Scientific Research and Development (IJTSRD).
27. Müller, R. (2007). Developing a Security Event Management System for Intermodal Transport. GI Jahrestagung.
28. Mulpuri, R. (2014). The Sales Cloud evolution: Salesforce and the power of hybrid infrastructure for business growth. International Journal of Science, Engineering and Technology, 2(5), 5.
29. Mulpuri, R. (2016). Conversational enterprises: LLM-augmented Salesforce for dynamic decisioning. International Journal of Scientific Research & Engineering Trends, 2(1), 47.
30. Mulpuri, R. (2016). Enhancing customer experiences with AI-enhanced Salesforce bots while maintaining compliance in hybrid Unix environments. International Journal of Scientific Research & Engineering Trends, 2(5), 5.
31. Mulpuri, R. (2017). Sustainable Salesforce CRM: Embedding ESG metrics into automation loops to enable carbon-aware, responsible, and agile business practices. International Journal of Trend in Research and Development, 4(6), 47.