**International Journal of Artificial Intelligence & Machine Learning (IJAIML)**
Volume 1, Issue 1, Jan-Dec 2022, pp. 10-14. Article ID: IJAIML_01_01_002
Available online at https://iaeme.com/Home/issue/IJAIML?Volume=1&Issue=1
Impact Factor (2022): 3.22 (Based on Google Scholar Citation)
Journal ID: 9339-1263



# AI AND MACHINE LEARNING IN SIEM: ENHANCING THREAT DETECTION AND RESPONSE WITH PREDICTIVE ANALYTICS

**ShivaDutt Jangampeta**
Senior Manager of Security Engineering,
JPMorgan Chase, Plano, USA

**ABSTRACT**

*In the modern digital world, many businesses are targets of cybercrime activities. Fortunately, organizations can stay ahead of cybercriminals and secure their sensitive, valuable data/networks by adopting advanced data security solutions like Security Information Event Management (SIEM). Contemporary SIEM systems leverage Artificial Intelligence (AI) and Machine Learning (ML) to enhance fast and effective detection of security threats while improving security capabilities through automated predictive analysis and response power. This study reviews how the adoption of AI and ML algorithms in SIEM solutions helps address threat detection and the key features and benefits that come with this adoption.*

**Keywords:** Security Information Event Management (SIEM), Artificial Intelligence (AI), Machine Learning (ML), Security Threats, AI-driven SIEM.

**Cite this Article:** ShivaDutt Jangampeta, AI and Machine Learning in SIEM: Enhancing Threat Detection and Response with Predictive Analytics International Journal of Artificial Intelligence & Machine Learning (IJAIML), 1(1), 2022, pp. 10-14. https://iaeme.com/Home/issue/IJAIML?Volume=1&Issue=1

## I. INTRODUCTION

Whereas conventional Security Information Event Management (SIEM) solutions have been an average part of the data security arsenal [1], threat actors are increasingly growing in complexity, devising more lethal attack mechanisms that can severely compromise computer systems/networks. Therefore, businesses are required to consider robust, highly powerful cybersecurity solutions to stay ahead of malicious actors. Artificial Intelligence (AI) and Machine Learning (ML) are emerging as potent technologies to address the limitations of conventional SIEM systems.

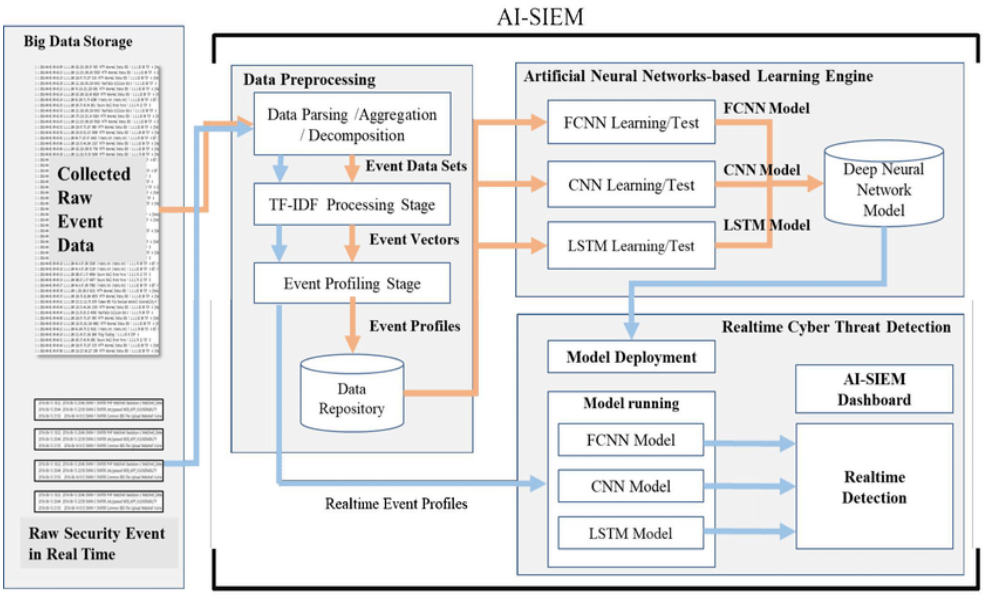


**Fig. 1.** The workflow and architecture for AI-powered SIEM system

Artificial Intelligence and Machine Learning have certainly transformed how businesses approach data security by leveraging the power of self-learning capacities and data-based algorithms. AI- and ML-powered SIEM systems can identify and respond to security incidents more effectively and more swiftly, as well as master and conform to the constantly changing nature of security threats.

Also, AI and ML-based SIEM software solutions can analyze voluminous amounts of data, effectively and quickly [2]. These technologies identify behaviors and anomalies that exhibit previously known threats. They are particularly revolutionary in enhancing real-time threat identification and mitigation, which is especially important as hackers have also started leveraging similar strategies and tools to execute their activities. Rapid threat detection and mitigation can substantially reduce potential data losses, financial losses, and reputational damages for enterprises.

## II. KEY FEATURES/BENEFITS OF AI- AND ML-POWERED SIEM SYSTEMS

### *A. Advanced Security Threat Identification*

AI-enabled SIEM systems leverage ML algorithms and state-of-the-art analytics to identify and monitor threats. These advanced tools analyze huge amounts of data, detect behavior patterns, and identify anomalies that may signal potential security events. By continually learning from available and new data, ML-powered SIEM systems enhance their threat identification capabilities and help organizations stay ahead of threat actors.

### *B. Real-Time Inspection and Alerting*

AI-enabled SIEM solutions provide real-time surveillance and notification of potential threats. They analyze security incidents in real-time, swiftly identify and correlate several signals of system/data compromise, and notify security personnel of potential security threats. This enables businesses to respond on time to security events, reducing the impact of attacks.

### *C. Predictive Analytics*

AI-powered SIEM solutions use predictive analysis tools/techniques to sport emerging security threats and predict future potential threat vectors. They analyze historical information, observe trends and behaviors, and leverage this information to project probable security risks. This helps organizations to bolster their information security defenses and prevent data breaches.

### *D. Adaptive Learning*

AI-driven SIEM solutions leverage the adaptive learning power of ML algorithms to learn how to counter new threats and adapt to the constantly evolving cybercrime landscape.

### *E. Automated Event Response*

AI-powered SIEM systems automate event response frameworks, enabling businesses to mitigate security threats swiftly and efficiently. The integration of SIEM solutions with AI and other security tools enables automated threat identification, containment, and remediation. This significantly reduces human errors, reduces response times, and allows the IT teams to endeavor in other tasks.

## III. USING AI AND ML IN SIEM SYSTEMS TO ADDRESS THREAT DETECTION AND MITIGATION CHALLENGES

Essentially, SIEM solutions are integrated systems that collect data from different sources across a computer system/network to provide a real-time view of probable security incidents [3]. The advanced version of SIEM systems leverages the power of AI to enhance threat identification, mitigation, and predictive analysis. This enables businesses to swiftly spot any anomaly or suspicious activity so they can respond if need be. AI has enabled advanced threat detection by automating many features/functions within the SIEM system using ML algorithms to enable learning to respond when similar incidents re-occur in the future. Some SIEM alternatives leveraging AI power include:

### *(a) Endpoint Detection and Response (EDR):*

Endpoint Detection and Response (EDR) systems are used to monitor and gather information from endpoints, including IoT devices, mobile phones, BYOD devices, etc. to detect security threats. Using AI and ML technologies, EDR solutions offer real-time inspection and mitigation of security threats. This enables organizations to secure their valuable data from cyber-attacks, in line with the present trend of increasing utilization of BYOD devices and remote-work models.

### *(b) User and Entity Behavior Analysis (UEBA):*

UEBA uses AI and ML tools to analyze user behaviors and other components across a business's digital environment. UEBA detects anomalies (deviations from standards) and thus can identify potential internal threats, compromised data, etc.

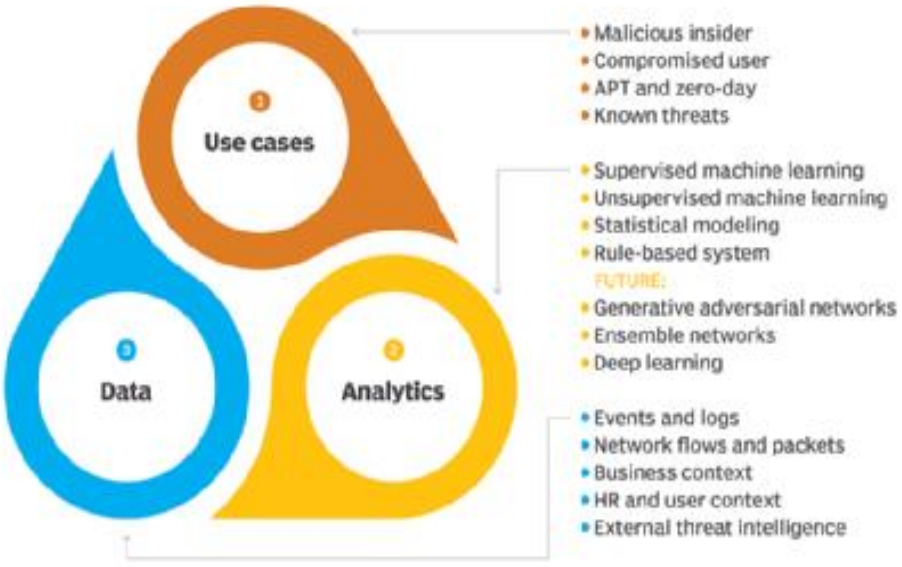


**Fig. 2.** Pillars of UEBA

### *(C) Security Orchestration, Automation, and Response (SOAR)*

SOAR systems use AI and ML solutions to automate monotonous tasks, streamline security event response processes, and empower businesses with evidence-based decision-making capabilities when responding to security incidents. Integrating the SOAR system with AI tools creates a holistic security architecture that can efficiently adapt to emerging security threats.

## IV. CHALLENGES ASSOCIATED WITH THE ADOPTION OF AI AND ML IN SIEM SYSTEMS

### *A. Architecture Complexity*

Incorporating AI and ML algorithms into SIEM systems may result in a complex security architecture. Effective execution requires sound planning, adequate understanding of the business's security requirements, and smooth collaboration between IT and security experts.

### *B. Compliance and Data Privacy*

The integration of AI in security solutions elicits compliance and data compliance concerns. To solve this problem, businesses must ensure the AI-enabled SIEM solutions they embrace comply with relevant standards and policies to secure sensitive data.

## V. CONCLUSION

Leveraging AI and ML solutions in SIEM solutions is both a technological advancement and a strategic technique to protect data in a growingly complex threat landscape. The adoption of AI-powered SIEM systems helps organizations fortify their cybersecurity defenses.

## REFERENCES

[1] David R. Miller, Shon Harris, Allen Harper, Stephen VanDyke, Chris Blask, Security Information and Event Management (SIEM) Implementation, McGraw Hill LLC, 2010.

[2] Dirk Schaefer, Lane Thames, Cybersecurity for Industry 4.0 Analysis for Design and Manufacturing, Springer International Publishing, 2017.

[3] Information Resources Management Association, Research Anthology on Artificial Intelligence Applications in Security, IGI Global.

**Citation:** ShivaDutt Jangampeta, AI and Machine Learning in SIEM: Enhancing Threat Detection and Response with Predictive Analytics International Journal of Artificial Intelligence & Machine Learning (IJAIML), 1(1), 2022, pp. 10-14

**Article Link:**
https://iaeme.com/MasterAdmin/Journal_uploads/IJAIML/VOLUME_1_ISSUE_1/IJAIML_01_01_002.pdf

**Abstract:**
https://iaeme.com/Home/article_id/IJAIML_01_01_002



✉ **editor@iaeme.com**