Chapter 7
Revolutionizing Security Information and Event Management (SIEM) Systems:
Harnessing Deep Learning for Advanced Threat Detection

Vijay B. Gadicha
https://orcid.org/0009-0006-4939-9026
P.R. Pote College of Engineering and Management, India

Ajay B. Gadicha
https://orcid.org/0000-0002-5496-3334
P.R. Pote College of Engineering and Management, India

Mohammad Zuhair
P.R. Pote College of Engineering and Management, India

Zeeshan I. Khan
P.R. Pote College of Engineering and Management, India

Mayur S. Burange
P.R. Pote College of Engineering and Management, India

ABSTRACT

This chapter explores various deep learning methods for enhancing Security Information and Event Management (SIEM) systems. As cyber threats become in-

DOI: 10.4018/979-8-3373-0700-8.ch007

creasingly sophisticated, traditional SIEM approaches often fall short in efficiently processing and analyzing vast amounts of security data. We investigate the application of deep learning techniques, such as convolutional neural networks (CNNs), recurrent neural networks (RNNs), and autoencoders, to improve threat detection, anomaly detection, and incident response capabilities. CNNs are leveraged for feature extraction from complex datasets, enabling the identification of intricate patterns in security events. RNNs are utilized for sequential data analysis, effectively capturing temporal dependencies in attack vectors.

INTRODUCTION

In today's rapidly evolving digital landscape, organizations face an unprecedented array of cybersecurity threats that demand innovative and adaptive security solutions. Traditional Security Information and Event Management (SIEM) systems, while valuable, often struggle to keep pace with the sheer volume and complexity of data generated by modern IT environments. Enter AI-enhanced SIEM, a transformative approach that harnesses the power of artificial intelligence and machine learning to revolutionize how security events are monitored, analysed, and responded to. By integrating advanced algorithms and automated processes, AI-enhanced SIEM solutions provide organizations with the ability to detect threats in real-time, reduce response times, and ultimately bolster their overall security posture.

At the core of AI-enhanced SIEM is the capability to analyze vast amounts of security data from diverse sources, including network devices, servers, applications, and user activity logs. Traditional SIEM systems often rely on predefined rules and signatures to identify threats, which can lead to missed detections or overwhelming numbers of false positives. In contrast, AI algorithms can identify patterns and anomalies that may indicate malicious activity, even when such behavior does not match known attack signatures. This adaptive approach enables organizations to uncover sophisticated threats that might otherwise go unnoticed, including zero-day exploits and insider threats.

One of the most significant advantages of AI-enhanced SIEM is its ability to automate incident response. In an environment where every second counts, the speed of response can be the difference between a contained incident and a full-blown data breach. AI-driven automation allows for predefined actions to be taken immediately upon detection of a threat, such as isolating affected systems, blocking malicious IP addresses, or even alerting security personnel. This automation not only reduces the burden on overworked security teams but also ensures a more consistent and rapid response to incidents.