RADemics

Security Event Correlation Using Graph Neural Networks for Threat Hunting and Response Automation

A. Johny, Punit Kumar Chaubey
KARPAGAVINAYAGA COLLEGE OF ENGINEERING AND TECHNOLOGY, BANSAL INSTITUTE OF ENGINEERING AND TECHNOLOGY

Security Event Correlation Using Graph Neural Networks for Threat Hunting and Response Automation

[1]A. Johny, Assistant Professor (Mathematics), Karpagavinayaga College of Engineering and Technology, GST Road, Chinnakolampakkam, Chengalpattu - 603308, Tamil Nadu, India. johny@kveg.in

[2]Punit Kumar Chaubey, Associate Professor, Department of Computer Science and Engineering (AI and AIML), Bansal Institute of Engineering and Technology, Lucknow, U.P., India. pkcmar@gmail.com

Abstract

This chapter explores the critical role of security event correlation in enhancing cybersecurity defenses, focusing on the integration of advanced techniques such as Graph Neural Networks (GNNs) to automate threat detection and response. As the complexity of modern network environments increases, traditional event correlation methods struggle to manage vast data volumes, leading to inefficiencies and increased vulnerability. By leveraging GNNs, this chapter demonstrates how correlated event data can improve anomaly detection, reduce false positives, and enhance the prioritization of threats. Additionally, it delves into the significance of machine learning and AI-driven approaches in optimizing the correlation process, ensuring real-time, adaptive responses. The chapter further emphasizes the value of correlated event data in post-incident forensics and recovery, providing insights into attack vectors, timelines, and overall system resilience. This comprehensive exploration offers valuable insights for researchers and practitioners aiming to strengthen their cybersecurity frameworks through advanced event correlation strategies.

Keywords: Security Event Correlation, Graph Neural Networks, Machine Learning, Anomaly Detection, Threat Prioritization, Post-Incident Forensics

Introduction

The rapid growth and complexity of modern cybersecurity environments present significant challenges in threat detection and response [1]. With the proliferation of connected devices, cloud infrastructures, and increasingly sophisticated cyberattacks, organizations face an overwhelming volume of security events [2]. These events, generated from various sources such as firewalls, intrusion detection systems, endpoints, and network traffic, must be effectively correlated to identify potential threats [3-7]. Traditional event correlation methods often struggle to keep up with the scale and complexity of modern systems, resulting in false positives, missed threats, and inefficient incident response processes [8-11]. This growing complexity necessitates advanced

techniques that can not only process vast amounts of security event data but also identify patterns and anomalies thatindicate potential security incidents [12].

Traditional event correlation methods primarily rely on rule-based systems, where predefined conditions or signatures trigger alerts when specific patterns are detected [13,14]. While effective for known threats, these methods struggle to detect novel or evolving attack vectors [15]. These systems often produce an overwhelming number of alerts, many of which are false positives [16]. Analysts are left sifting through large amounts of irrelevant data, wasting valuable time and resources [17-20]. The inability of traditional methods to dynamically adapt to new attack techniques further exacerbates this issue [21]. These limitations highlight the need for more advanced and automated approaches to event correlation that can handle complex, real-time data and provide more accurate threat detection [22].

In response to these challenges, machine learning (ML) and artificial intelligence (AI)-driven approaches have gained traction in the field of cybersecurity [23]. Machine learning algorithms can analyze vast amounts of data, identify patterns, and make predictions based on past experiences [24]. However, one promising innovation that has emerged was the use of Graph Neural Networks (GNNs) for security event correlation [25]. GNNs excel in capturing the relationships between different security events, entities, and network components, offering a more dynamic and scalable approach to detecting threats. By leveraging the graph structure, GNNs can identify hidden patterns that traditional methodsmiss, such as lateral movement within a network or multi-stage attack techniques. These capabilities make GNNs an ideal tool for automating threat detection and response in increasingly complex environments.