Proceedings of the International Conference on Industrial Engineering and Operations Management

Publisher: IEOM Society International, USA DOI: 10.46254/AU04.20250027
Published: November 25, 2025

AI with Data Science for Advanced Cyber Risk and Threat Analytics

Thiru Pandian
The University of Texas at Dallas
United States
thiru.pandian@utdallas.edu

Abstract

In today's rapidly changing threat landscape, traditional cybersecurity tools often fail to detect and respond effectively to complex attacks. This paper introduces a comprehensive framework that combines Artificial Intelligence (AI) with Data Science to improve cyber risk assessment and threat analysis. By utilizing machine learning, anomaly detection, and predictive modeling, organizations can move from reactive defense to proactive threat mitigation. The integration of big data techniques allows for scalable analysis of various security logs, network traffic, and user behavior. AI models continually learn from past incidents, enabling real-time detection of emerging threats. The proposed approach also employs risk scoring and prioritization using advanced statistical and AI-based methods. This helps security teams better allocate resources and reduce dwell time. Case studies show how AI-driven analytics improve detection accuracy and lower false positive rates. The framework encourages automation, agility, and intelligence in security operations, closing the gap between data abundance and actionable cyber defense.

Keywords

AI, Data science, Advanced cyber risk and threat, security operation, cyber defense.