Team – 10.2

AI-Enhanced Security Analytics Dashboard That Provides Real-Time Insights Into Security Events, Trends, And Risks

Abstract

The exponential growth of the internet and online services has revolutionized communication, business, and society. However, this digital transformation has also expanded the threat landscape for cyber attacks that can cause severe reputational and financial damages. Verizon's 2021 Data Breach Investigations Report reveals that web application attacks have increased by 300% since 2020. Cybercriminals are rapidly innovating their techniques, making it impossible for manual monitoring alone to keep up.

According to industry surveys, security teams are flooded with more than 20,000 alerts each day and 80% of breaches take months to discover. The absence of real-time visibility into security events, anomalous behaviours, and vulnerability trends across networks, endpoints, cloud, and users has dangerous repercussions. Organizations urgently need AI-driven analytics that can synthesize intelligence from dispersed security tools and massive data silos.

Solution Overview

To address this need, our engineering team has developed an AI-enhanced security analytics dashboard that arms defenders with real-time insights and next-generation threat detection capabilities. The dashboard consolidates security events, user activity trails, network traffic, system audit logs, vulnerability feeds, and threat intelligence into a unified data lake. Cutting-edge AI algorithms are applied to identify suspicious patterns, derive contextual relationships, and surface early warnings of potential threats.

Key features include:

Risk-Based Prioritization: A continuously updated risk score associates each event with potential business impact, empowering analysts to focus on the most pertinent threats. Advanced analytics models determine risk levels by correlating events across multiple domains.

Anomaly Detection: Unsupervised ML algorithms profile normal behavior of users, devices, and networks to flag outliers and anomalies that deviate from baseline patterns. This facilitates proactive threat hunting.

Threat Forecasting: Time-series analysis on longitudinal event data predicts potential vulnerabilities that may be imminently or frequently targeted by adversaries.

Natural Language Processing: Unstructured data like security alerts and threat intel reports is parsed to extract entities, relationships, trends, and TTPs using NLP techniques.

Centralized Search: A lightning-fast search engine helps investigate incidents through evidence correlation across siloed tools. Analysts can pivot seamlessly between connected events.

Automated Response: Playbooks to contain detected threats can be initiated with a single click, accelerating incident response. Chatbots also facilitate human-machine collaboration.

Customizable Dashboard: An intuitive graphical interface offers customizable views, alerts, and drill-down reports to monitor security posture specific to one's role and needs.

Conclusion

Our AI-powered security analytics dashboard transforms how enterprises monitor, detect, investigate and respond to cyber risks in real-time. By integrating AI into the very foundation of security operations, we aim to successfully counter sophisticated threats and minimize business disruption for our customers.