Develop an AI-enhanced security analytics dashboard that provides real-time insights into security events, trends, and risks.

By Team 10.1
(Siddharth, Pushya, Adithya, Sameer)

Abstract

As artificial intelligence (AI) transforms the security landscape, AI-enhanced security analytics dashboards emerge as a promising application to detect, prevent, and respond to threats. This project proposes to develop a customized AI-enhanced security analytics dashboard that leverages the latest AI and machine learning algorithms to analyze security data from diverse sources and provide real-time insights into security events, trends, and risks. The dashboard is to be user-friendly and interpretable, empowering security analysts to identify and understand the insights quickly and easily.

Objectives

1. Collect and normalize security data from a variety of sources. This may include security logs, network traffic data, and threat intelligence feeds.
2. Use AI and machine learning algorithms to analyze the security data. This can be used to identify patterns and anomalies, detect threats, and predict future risks.
3. Develop a security analytics dashboard that visualizes the insights from the AI and machine learning analysis. The dashboard should be easy to use and interpretable, so that security analysts can quickly identify and respond to threats.

4. The dashboard should be able to:

   Detect threats in real time and alert security analysts.

   Provide security analysts with the tools they need to investigate security incidents.

   Identify and track security trends over time.

   Assess the security risk of different assets and systems.

Scope

The scope of AI-enhanced security analytics dashboards is relatively vast. They can help security teams to:

1. Improve their ability to detect and respond to threats in real time.
2. Reduce the time it takes to investigate and resolve security incidents.
3. Identify and track security trends over time.
4. Prioritize security resources and mitigate risks.
5. Gain a better understanding of their security landscape and identify areas for improvement.