Security Alerts Processing Challenge

April 2025
Artificial Intelligence & Data Science

Project Overview

This project focuses on transforming raw cybersecurity alert data into actionable intelligence. The dataset, provided in CSV format, contains a high volume of security alerts automatically generated by detection tools. However, these alerts need significant refinement to be useful for cybersecurity analysts.

The main goals are :

- **Data Cleaning**
  Deduplicate records, fix inconsistencies, and organize the data into a structured, usable format.
- **Alert Contextualization**
  Enrich the alerts by integrating external threat intelligence, vulnerability databases, and historical information to add valuable context.
- **False Positive Management**
  Develop methods to distinguish real threats from noise, reducing unnecessary workload and focusing attention on genuine incidents.
- **Classification and Prioritization**
  Design a scoring model to assess the criticality and impact of each alert, helping teams prioritize their responses efficiently.
- **Visualization and Reporting**
  Create a concise report or an interactive dashboard to allow rapid understanding and navigation of the processed alerts.

This challenge blends **data science**, **cybersecurity**, and **automation** skills to build a smarter, more efficient alert management system.

This challenge is brought by Algosecure.