AI-Powered Network Intrusion Detection System (NIDS) Using Suricata and Machine Learning

# Project Summary

This project involved designing and implementing an AI-powered Network Intrusion Detection System (NIDS) leveraging Suricata for data collection and Python-based machine learning for real-time analysis and detection. The goal was to create a working demonstration of how cybersecurity monitoring can be augmented with intelligent classifiers to detect known malicious behaviors in network traffic.

# Key Contributions

While I do not have a formal background in machine learning or AI development, I managed to complete this end-to-end project by leaning heavily on guidance and iterative code generation with ChatGPT. This hands-on process gave me exposure to numerous technologies and processes relevant to cybersecurity and AI-powered systems.

The core responsibilities and work completed included:

• Setting up Suricata in a virtualized lab environment to collect realistic network data.

• Parsing large Suricata alert logs (over 1 million rows) using Python and pandas.

• Cleaning and transforming alert data to extract meaningful features (e.g., IPs, ports, flags).

• Building and training classification models (Random Forest and XGBoost) to identify malicious alert types.

• Creating an inference engine that can predict alert types from new Suricata events.

• Writing an evaluation script to benchmark model performance using accuracy, classification reports, and confusion matrices.

• Using GitHub to publish a working version of the project, while dealing with limitations around large files by hosting training datasets externally via Google Drive.

# Skills and Technologies

• Suricata IDS

• Python (pandas, scikit-learn, xgboost, joblib)

• Data preprocessing and feature engineering

• Classification models: RandomForestClassifier, XGBClassifier

• Git, GitHub, markdown, .gitignore, and handling large files

• Google Drive integration for file sharing

# Reflection

This project was an educational and empowering experience. Although I relied significantly on ChatGPT to learn and implement technical concepts, I gained a practical understanding of how AI can be applied to real-world cybersecurity use cases. The experience has deepened my interest in the intersection of AI and security and equipped me with skills I am eager to build upon in a professional setting.