



# Leveraging Machine learning for Security Operations

Duke  
UNIVERSITY

Code<>

Brandon Cheng, Dalia Alasmari, Hams Almansori, Joey Sun,  
Raghad Alharbi, Uzziel Avalos

## OVERVIEW

This project streamlines Security Operations Center (SOC) analyst workflows by automating key alert enrichment processes.

## DEMO



## FEATURES

- Ingests JSON-formatted alerts and extracts key metadata such as IP address, hostname, operating system, and subnet.
- Simple front-end interface to submit JSON alerts and view all stored threat data in a readable format.
- Automatically classifies incoming alerts based on predefined rules (e.g., login, mail, SASL, etc.).

## TECH STACK

 FastAPI



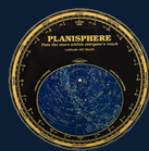
python



HTML



CSS



PostgreSQL



podman



docker

## WHAT'S NEXT?

- Incorporate machine learning to auto-filter out alerts.
- Expand the number of types of alerts our application can enrich.