Cyber Threat Intelligence Dashboard – Project Report

Introduction

The cybersecurity landscape is constantly evolving, with organizations facing an increasing number of threats from malicious actors. Timely detection, enrichment, and analysis of Indicators of Compromise (IOCs) such as malicious IPs, domains, and URLs are essential for proactive defense. To address this, a Cyber Threat Intelligence (CTI) Dashboard was developed during my internship. The dashboard aggregates threat data from open feeds and APIs, enriches it with contextual intelligence, and presents actionable insights through visualizations and reports.

Abstract

The CTI Dashboard project focuses on building a real-time, lab-safe environment that demonstrates ingestion, enrichment, and visualization of cyber threat intelligence data. It is designed for analysts to quickly assess threat levels, identify related incidents, and export results for reporting. Unique features such as Adaptive Threat Scoring (merging multiple API signals into a normalized score) and Threat Attribution & Story-Builder (clustering related IOCs into incident narratives) elevate the project beyond basic dashboards. The solution was built with Flask, SQLite, Chart.js, and Leaflet, emphasizing simplicity, modularity, and explainability.

Tools Used

- Programming Language: Python (Flask Framework)
- Database: SQLite (lightweight, local persistence)
- Frontend Libraries: Jinja2 templates, Chart.js (charts), Leaflet.js (maps)
- APIs Integrated: AbuseIPDB (IP reputation), IP-API (geolocation), mock data for safe testing
- Environment Management: Virtualenv, Python-Dotenv
- Version Control & Documentation: GitHub, Markdown, PDF reporting

Steps Involved in Building the Project

1. Project Initialization: Set up a Flask project with SQLite database schema (iocs and enrichments tables). Created homepage with IOC upload form and data table.
2. IOC Ingestion: Enabled CSV upload of IOCs (IP, domain, type, first seen). Stored parsed IOCs with ingestion timestamp into the database.
3. Threat Enrichment: Integrated AbuseIPDB API (with safe mock fallback). Created a /lookup route to test enrichment per IOC. Stored enrichment results in the database.
4. Visualizations: Time-series chart of IOC ingestions per day, Geolocation map plotting malicious IPs by country, Threat Scores bar chart showing computed risk values per IOC.
5. Unique Features: (a) Adaptive Threat Scoring (multi-source fusion with explainability), (b) Threat Attribution & Story-Builder (clusters related IOCs and auto-generates stories).
6. Export & Filters: Added CSV export for IOCs and enrichments, plus client-side filtering by IOC type, score, and date window.

Conclusion

The Cyber Threat Intelligence Dashboard successfully demonstrates the full cycle of threat intelligence handling — from ingestion and enrichment to visualization and contextual storytelling. By implementing unique features like adaptive scoring and automated story generation, the project not only meets internship requirements but also showcases advanced skills in security analysis, data fusion, and dashboard development. This project can be extended with more feeds, authentication, and automation to serve as a practical SOC (Security Operations Center) tool.