Cyber Threat Intelligence Dashboard – Project Report

Student Name: Chandana Devarakonda

Program: MBA (Cybersecurity focus)

Tools: Flask, MongoDB, Chart.js, VirusTotal API, AbuseIPDB API, APScheduler, Docker

Objective

To design and implement a real-time Cyber Threat Intelligence (CTI) Dashboard that aggregates open threat feeds, visualizes Indicators of Compromise (IOCs), and enables interactive lookups for IPs and domains using external threat intelligence APIs.

Architecture Overview

Frontend (Bootstrap + Chart.js) connects to Flask backend via REST APIs. MongoDB stores IOC data, while VirusTotal and AbuseIPDB APIs provide enrichment. A scheduler automates CTI feed ingestion.

Key Features

1. IOC Lookup with real-time API enrichment.
2. Threat feed aggregation and visualization.
3. Tagging and CSV export capabilities.
4. Automated scheduling of data pulls.
5. Simple Dockerized deployment.

Results & Future Enhancements

The dashboard successfully aggregates and visualizes IOCs, improving security visibility. Future work includes integration with STIX/TAXII feeds, user authentication, and geo-IP threat maps.

Conclusion

The Cyber Threat Intelligence Dashboard effectively centralizes and visualizes multi-source threat data, demonstrating practical cybersecurity data engineering and analytics capabilities.