Cyber Threat Intelligence Dashboard - Summary Report

Introduction

This project focuses on building a real-time Cyber Threat Intelligence (CTI) Dashboard using open-source tools and threat intelligence APIs. The dashboard allows users to input IP addresses or domain names and retrieve real-time threat intelligence data from public CTI sources.

Abstract

The CTI Dashboard is a web-based application designed to assist security analysts in identifying, verifying, and visualizing Indicators of Compromise (IOCs) using real-time threat feeds. It integrates AbuseIPDB and VirusTotal APIs to fetch intelligence and stores the results in a MongoDB database for trend analysis and historical lookups.

Tools Used

- Python (Flask)
- MongoDB
- AbuseIPDB API (Free Tier)
- VirusTotal API (Free Tier)
- HTML, CSS (for UI)
- Bootstrap (optional for styling)

Steps Involved in Building the Project

1. Set up the Flask backend and define routes for dashboard and lookups.
2. Integrate AbuseIPDB and VirusTotal APIs for threat intelligence queries.
3. Configure MongoDB to store IOC lookup history.
4. Build HTML templates to display results and recent IOC activity.
5. Add .env support for secure API key storage.
6. Start Flask development server and test the dashboard functionality.

Conclusion

The CTI Dashboard successfully provides real-time insights into IP/domain threats using open APIs. It is scalable, modular, and can be enhanced with additional sources, charting, or automation for broader threat visibility and faster incident response.