Cyber Threat Intelligence Dashboard Project Report

Introduction

This project develops a real-time Cyber Threat Intelligence (CTI) dashboard to aggregate and visualize threat data from open sources and APIs. It enables security professionals to monitor Indicators of Compromise (IOCs) like IPs and domains, assess threat levels, and track trends. The dashboard supports user-driven lookups, tagging, and data export, promoting proactive threat detection.

Abstract

The dashboard integrates APIs from VirusTotal and AbuseIPDB with MongoDB for storage. It pulls real-time data, displays threat metrics, and visualizes trends using Plotly. Key features include IOC verification, tagging for categorization, and CSV export. Built with Flask, it demonstrates practical CTI aggregation, though limited by free API tiers.

Tools Used

- **Flask**: Web framework for the dashboard.
- **VirusTotal API (Free Tier)**: For IOC analysis and threat scoring.
- **AbuseIPDB API (Free Tier)**: For IP reputation checks.
- **MongoDB**: NoSQL database for storing threats and trends.
- **APScheduler**: For background real-time data pulls.
- **Plotly**: JavaScript library for trend visualizations.
- **Requests/Pandas**: For API calls and data export.

Steps Involved in Building the Project

1. **Setup Environment**: Installed dependencies and configured MongoDB/API keys.
2. **Data Fetching**: Created scripts to pull data from VirusTotal and AbuseIPDB, storing in MongoDB.
3. **Dashboard Development**: Built Flask routes for displaying threats, lookups, and exports.
4. **Visualizations**: Integrated Plotly for trend charts based on historical data.
5. **Features Addition**: Added tagging (via AJAX) and export (to CSV).
6. **Real-Time Aggregation**: Used APScheduler for periodic API pulls (every 10 minutes).
7. **Testing**: Verified lookups, visualizations, and exports with sample IOCs.

Conclusion

The dashboard successfully aggregates CTI data, providing actionable insights into threats. It highlights the value of API integration for real-time monitoring. Future enhancements could include more sources (e.g., MISP) and advanced analytics. This project underscores the importance of CTI in cybersecurity