Name: Samrat Amit Sawant
Project: Cyber Threat Intelligence Dashboard

Project Report

Introduction

This project involved developing a comprehensive Cyber Threat Intelligence (CTI) Dashboard - a real-time web application designed to aggregate threat data from multiple external sources, visualize security trends, and enable security analysts to perform efficient threat lookups and analysis. The dashboard serves as a centralized platform for monitoring cybersecurity indicators and facilitating data-driven security decisions.

Abstract

The CTI Dashboard integrates multiple threat intelligence APIs including VirusTotal and AbuseIPDB to enrich threat indicators with contextual information. The system utilizes MongoDB for scalable data storage and caching, while Chart.js provides interactive frontend visualizations displaying threat trends over time. Real-time threat feed updates are delivered via WebSocket connections using Flask-SocketIO. The application supports data export functionality in both CSV and JSON formats, enabling further analysis and integration with external security tools. The dashboard provides a user-friendly interface for security operations center (SOC) analysts to efficiently monitor, analyze, and respond to emerging threats.

Tools Used

Backend Technologies:

- Python 3.13 with Flask framework for web application development
- Flask-PyMongo for MongoDB database integration
- Flask-SocketIO for real-time WebSocket communications
- Python-dotenv for secure environment variable management
- Requests library for external API integration

Frontend Technologies:

- HTML5, CSS3, and JavaScript for responsive user interface
- Chart.js library for interactive data visualizations
- Socket.IO client for real-time updates

Database & APIs:

- MongoDB for document-based data storage and indexing
- VirusTotal API for domain and IP reputation analysis
- AbuseIPDB API for IP abuse confidence scoring

Steps Involved in Building the Project

Environment Setup & Configuration

- Configured Python virtual environment and installed required dependencies
- Implemented secure API key management using environment variables
- Set up MongoDB database with proper indexing for performance optimization

Backend Development

- Developed Flask application with modular route structure
- Created REST API endpoints for threat statistics, trends, and recent threats
- Implemented threat lookup functionality with API enrichment from multiple sources
- Built data export capabilities supporting CSV and JSON formats with filtering options

Database Integration

- Designed MongoDB schema for threat indicator storage
- Implemented caching mechanism to reduce API calls and improve performance
- Created database indexes for efficient querying and data retrieval

Frontend Dashboard Development

- Designed responsive web interface with professional dark theme
- Integrated Chart.js for dynamic bar charts and doughnut visualizations
- Implemented interactive threat lookup form with real-time result display
- Added export controls with format selection and threat level filtering

Real-time Features Implementation

- Developed WebSocket communication using Flask-SocketIO
- Created background thread for threat feed simulation
- Implemented real-time dashboard updates and notifications

Testing & Quality Assurance

- Conducted comprehensive testing of all API integrations
- Validated data export functionality across different formats
- Performed responsive design testing across multiple devices

Conclusion

The Cyber Threat Intelligence Dashboard project successfully demonstrates the integration of modern web technologies with cybersecurity APIs to create a comprehensive threat monitoring platform. The application provides security analysts with real-time visibility into threat landscapes, interactive data visualization, and flexible data export capabilities. The dashboard's architecture supports scalability and extensibility, making it suitable for deployment in operational Security Operations Centers (SOCs).

This project showcases proficiency in full-stack development, API integration, database design, and cybersecurity domain knowledge. The resulting platform offers practical value for cybersecurity professionals while demonstrating technical expertise across multiple technology stacks. The dashboard serves as a foundation for more advanced threat intelligence operations and can be extended with additional APIs, machine learning capabilities, and enhanced analytical features.

Project Completion Date: August 20, 2025
Technologies: Python, Flask, MongoDB, Chart.js, VirusTotal API, AbuseIPDB API
Key Features: Real-time monitoring, Interactive visualizations, Data export, WebSocket updates