Cyber Threat Intelligence (CTI) Dashboard Report

Project Title: Cyber Threat Intelligence (CTI) Dashboard

Subtitle: A Flask-Based Cyber Threat Intelligence Monitoring Tool

Prepared by: Aditya Kamble

Date: 27/07/2025, Friday

Tools: Flask/Django, VirusTotal API (free tier), AbuseIPDB, MongoDB

This report presents the design and implementation of a Cyber Threat Intelligence (CTI) Dashboard using Flask, MongoDB, and VirusTotal API. The dashboard enables IOC lookups, visualizes trends, and provides essential threat analytics in real-time. It aims to support cybersecurity analysts and researchers with minimal tools yet actionable intelligence.

Project Overview

Objective:

Build a real-time dashboard that collects, analyzes, and visualizes cyber threat intelligence data using public CTI feeds and user-submitted Indicators of Compromise (IOCs).

Technology Stack

Backend: Python + Flask

Database: MongoDB

APIs: VirusTotal (free tier)

Visualization: Matplotlib, Pandas

Frontend: HTML5, CSS3, Bootstrap 5

Security: Flask-Limiter, CSP headers

Core Features

- IOC Lookup: Analyze IPs/domains/hashes using VirusTotal.

- Threat Visualization: View IOC trends with matplotlib charts.

- Tagging System: Tag IOCs with labels like “APT29”, “Phishing”.

- Data Export: Export threat records as CSV.

- Threat Metrics: View total IOCs, high-risk stats, and tags.

- Security Measures: Rate limiting and CSP headers to prevent abuse.

UI Highlights

- Clean dark mode interface with Bootstrap 5

- Responsive layout for mobile and desktop

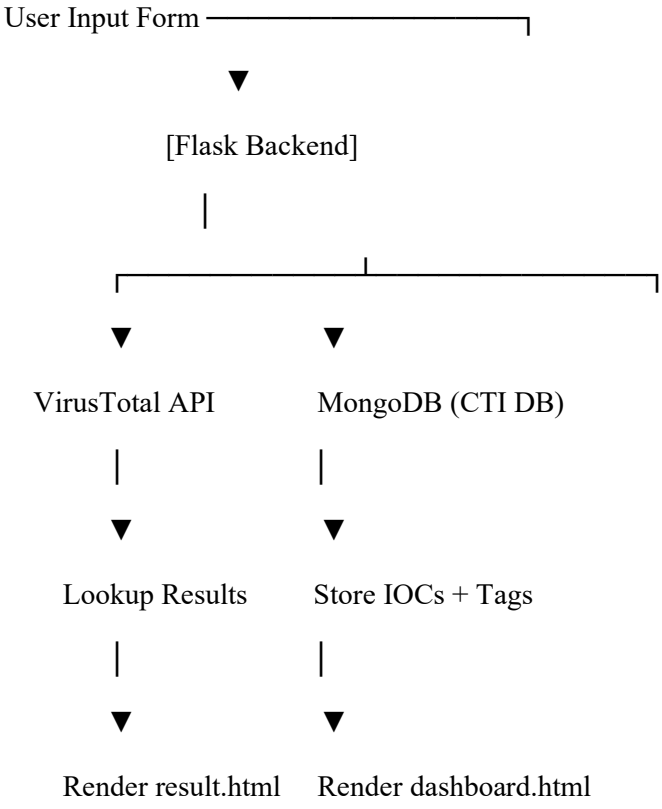
- Segoe UI typography for readability

- Trend graph with hover effects and export link

- Clear navigation between Dashboard, Trends, and Export

System Architecture & Flow

System Architecture Overview



Key Components

- `app.py`: Main Flask app with routes like /check, /dashboard, /trends, /export.

- `templates/`: Contains Jinja2 HTML templates.

- `utils/`: Handles IOC validation and API queries.

- `static/images/`: Stores trend graph images.

- `MongoDB`: Stores threat intelligence records with tags and metadata.

Example Use Case Flow

- 1. User submits IOC → validated in `/check`

- 2. VirusTotal queried → data returned

- 3. Data stored in MongoDB

- 4. Trend graph image updated

- 5. Dashboard shows new stats

Deliverables

- ✅ Flask-based CTI Dashboard

- ✅ IOC Lookup & Tagging

- ✅ Real-Time Metrics with Trend Graph

- ✅ Export to CSV

- ✅ Security Headers + Rate Limiting

- ✅ Modern UI