CTI-Dashboard Project Report

Name: Yash Chandrashekhar Karnik
Date: 26-10-2025

---

1. Project Title

Cyber Threat Intelligence (CTI) Dashboard

---

2. Objective

To build a real-time CTI dashboard that aggregates threat feeds, analyzes Indicators of Compromise (IOCs), and visualizes threat trends to help security analysts monitor and respond to threats effectively.

---

3. Tools and Technologies

- Backend: Python, Flask
- Database: MongoDB
- Task Queue: Celery with Redis
- APIs: VirusTotal, AbuseIPDB, OTX
- Frontend: HTML, CSS, JavaScript, Chart.js, DataTables
- Deployment: Docker, Docker Compose
- Development OS: Kali Linux / Linux

---

4. Architecture

- Data Sources: Threat intelligence APIs (VirusTotal, AbuseIPDB, OTX)
- Database: MongoDB stores IOCs and threat events
- Workers: Celery handles scheduled ingestion tasks
- Backend: Flask serves API endpoints and dashboard
- Frontend: HTML/JS visualizes threat trends and lookup results

Folder Structure:
CTI-Dashboard/

- app.py
- requirements.txt
- static/

- templates/
- outputs/
- workers/
- services/
- docker-compose.yml

---

5. Features

- Aggregate real-time CTI feeds
- Lookup IPs, domains, URLs, file hashes
- Display threat levels and trends
- Tag and export IOCs
- Dashboard with charts and tables

---

6. Installation

Using Docker:

git clone https://github.com/yk47/Elevate-Labs-Projects.git

cd Elevate-Labs-Projects/CTI-Dashboard

docker compose up --build -d

Environment Variables (.env):

MONGO_URI=mongodb://mongo:27017/ctidb

CELERY_BROKER=redis://redis:6379/0

VT_API_KEY=<your_virustotal_key>

ABUSEIPDB_KEY=<your_abuseipdb_key>

OTX_API_KEY=<your_otx_key>

Access the dashboard: http://localhost:5000

---

7. Usage

- Perform threat lookups for IPs/domains
- Monitor threat trends on the dashboard charts
- Tag IOCs and export results for analysis

---

8. Future Enhancements

- Add more CTI sources
- Advanced analytics and alerts
- User authentication and roles
- AI/ML-based threat prediction

---

9. References

- VirusTotal API: https://www.virustotal.com/
- AbuseIPDB API: https://www.abuseipdb.com/
- OTX Open Threat Exchange: https://otx.alienvault.com/
- Flask Documentation: https://flask.palletsprojects.com/
- MongoDB Documentation: https://www.mongodb.com/docs/

Screenshots