Cyber Threat Intelligence (CTI) Dashboard

Intern Name: Athuljith P

Project Duration: 25-08-2025 – 05-09-2025

Abstract

This project focuses on building a Cyber Threat Intelligence (CTI) Dashboard that allows users to investigate suspicious IPs, domains, URLs, and file hashes. The application demonstrates the concept of threat intelligence aggregation, which is a critical part of modern cybersecurity operations. The tool integrates with VirusTotal, AbuseIPDB, and AlienVault OTX to provide insights into whether an indicator is benign, suspicious, or malicious. A simple risk scoring system summarizes the findings, while users can view both summarized results and raw JSON evidence. The tool also allows exporting reports for documentation and further analysis.

Introduction

Cyber Threat Intelligence (CTI) is the process of collecting and analyzing information about threats to support decision-making in cybersecurity. This project implements a Streamlit-based CTI dashboard in Python to demonstrate the practical use of threat intelligence APIs.

The tool provides core functionalities to:
- Lookup: Investigate IP addresses, domains, URLs, and file hashes.
- Risk Scoring: Classify indicators into Low, Medium, or High risk.
- Evidence View: Display raw intelligence data from external sources.
- Report Generation: Download structured JSON reports.

Tools Used

- Python 3.11+: Core programming language.
- Streamlit: Framework for creating interactive web apps.
- Requests: For making API calls.
- Pandas: For handling tabular summaries.
- APIs: VirusTotal, AbuseIPDB, AlienVault OTX.

Steps Involved in Building the Project

1. Project Setup: Created a structured directory including app.py, requirements.txt, and reports/.
2. Streamlit UI Design: Designed an interactive dashboard with input fields, lookup button, and results area.
3. API Integration: Connected the app with VirusTotal, AbuseIPDB, and OTX APIs to fetch intelligence data.
4. Indicator Type Detection: Implemented logic to detect whether input is IP, domain, URL, or hash.
5. Risk Scoring: Designed a heuristic to classify indicators into Low, Medium, or High risk.
6. Tabbed Results: Displayed findings in Summary (tabular) and Raw Evidence (JSON) views.
7. Report Download: Enabled JSON export of results for documentation.
8. Testing: Verified with safe IPs (Google DNS 8.8.8.8 → Low risk) and flagged IPs (Tor node 185.220.101.1 → High risk).
9. Evidence Capture: Screenshots of test lookups were saved in reports/.

Conclusion

The CTI Dashboard successfully demonstrates the integration of multiple cyber threat intelligence sources into a single interactive platform. By leveraging Streamlit, Python, and public APIs, it provides a practical way to enrich threat investigations. This project strengthens understanding of threat intelligence, risk scoring, and cybersecurity reporting. It also serves as a foundation for extending to more advanced applications like automated alerting and SIEM integration.