# Cyber Threat Intelligence Dashboard — Project Report

---

## Abstract

The **Cyber Threat Intelligence Dashboard** is an open-source platform designed to provide a unified view of malicious or suspicious IP addresses using multiple OSINT (Open Source Intelligence)sources. By integrating APIs from **Shodan, VirusTotal, and AlienVault OTX**, the dashboard assists security analysts and SOC teams in quickly assessing risks associated with a target IP.

The dashboard supports both **Live API Mode** and **Cached Data Mode**, making it usable even under API limitations. Future work includes full support for **automated PDF report exports**.

---

## Introduction

The Cyber Threat Intelligence Dashboard is a security-focused project developed to assist analysts, SOC teams, and cybersecurity professionals in investigating IP addresses. It integrates multiple threat intelligence sources (Shodan, VirusTotal, and AlienVault OTX) into a single unified dashboard, making it easier to visualize and analyze threat data.

---

## Objectives

- Centralize IP threat intelligence data from different APIs
- Provide visual insights for open ports, detections, and threat categories
- Store results locally for offline access and reusability
- Highlight potential threats with a calculated Threat Score
- (In Progress) Export professional PDF reports for SOC/analyst usage

---

## Key Features

1. **Integration of APIs**: Fetches live data from Shodan, VirusTotal, and AlienVault OTX.
2. **Cached Data Mode**: Enables usage of stored JSON data to avoid API limits during demos.
3. **Visualization**: Uses Streamlit to display metrics, charts, and maps.

4. **Threat Scoring**: Calculates a simple score (0–100) based on detections, pulses, and open ports.
5. **Data Storage**: Saves every query in JSON format inside the `data/` directory.
6. (**Planned Feature**): Export detailed PDF reports summarizing findings.

## Limitations

- Shodan host lookups require a paid Membership plan, limiting results to popular networks.
- Free-tier API keys have rate limits (especially VirusTotal).
- The Threat Score is a simplified model and should not be treated as a full risk assessment.
- PDF export feature is currently under development.

---

## Usefulness for SOC Teams

The dashboard is valuable for SOC (Security Operations Center) workflows because it:
- Aggregates intelligence from multiple sources into one view.
- Helps in quick triage of suspicious IP addresses.
- Provides both visual context and raw JSON data for deeper analysis.
- Can serve as a lightweight, customizable internal tool.

---

## Conclusion

The **Cyber Threat Intelligence Dashboard** is a practical, analyst-focused project that integrates OSINT threat feeds into a single interface. While some features are constrained by free API plans, the system demonstrates a **realistic SOC workflow** and can be expanded with premium APIs or additional OSINT sources.

This project highlights the importance of **automation in cyber threat intelligence** and serves as a **showcase project** for both learning and professional demonstration.

---

📌 **Repository**: https://github.com/shashank181034/CyberThreatIntel-Dashboard
📌 **Demo Video**: [https://www.linkedin.com/in/shashank-mvs-115630266](https://www.linkedin.com/in/shashank-mvs-115630266)