VulnScope – A Cyber Threat Intelligence Dashboard

INTRODUCTION:

In today's evolving cybersecurity landscape, it is essential to have visibility into malicious threats in real-time. VulnScope is a lightweight and responsive Cyber Threat Intelligence (CTI) dashboard designed to help analysts assess risks by collecting, displaying, and visualizing intelligence on domains or IPs. The system supports tagging, historical tracking, and exporting reports.

ABSTRACT:

VulnScope is a web-based CTI dashboard developed using Flask, which integrates with the VirusTotal API to collect intelligence on domains and IPs in real time. The application allows users to input targets, retrieve structured threat data, view detection metrics visually, assign custom threat tags, and export the results in a professional PDF format. It also maintains a persistent scan history for future reference. The project emphasizes accessibility, simplicity, and real-time feedback, making it suitable for use in both academic and operational security environments

TOOLS USED:

- Frontend: HTML, CSS, JavaScript, Chart.js
- Backend: Python (Flask)
- APIs: VirusTotal (Free Tier)
- Data Storage: JSON file-based logs (can be extended to MongoDB)
- Reporting: jsPDF + html2canvas

STEPS INVOLVED IN BUILDING THE PROJECT:

1. User Interface Design:

A responsive and intuitive user interface was developed using standard web technologies. The dashboard includes navigation controls, a scanning form, and sections for visualizations and lookup history.

2. Backend and API Integration:

The Flask server processes user-submitted input and queries the VirusTotal API for intelligence data. Responses are parsed and displayed in a structured format, highlighting key threat indicators.

3. Threat Intelligence Rendering:

Extracted details include analysis statistics, detection engine results, timestamps, and certificate information. These are presented in a tabular format and visualized using a donut chart for better comprehension.

4. Tagging and Persistence:

Users can assign custom tags to each scan (e.g., "Malicious", "Suspicious", "Safe"), which are stored alongside the lookup results in a local JSON file. This enables consistent classification across sessions.

5. Report Generation:

The dashboard includes functionality to export scan results and threat metrics into a downloadable PDF file. This aids in documentation, auditing, and incident reporting.

CONCLUSION:

VulnScope provides a streamlined, interactive, and intelligent way to monitor IoCs. Its modular design and minimal resource usage make it ideal for security learners, small teams, or threat research. With real-time lookups, visual summaries, tagging, and export capabilities, VulnScope stands out as an educational and functional cyber threat analysis tool.

Submitted by : PRIYANSHI PAWAR

Internship : Elevate Labs