CYBER THREAT INTELLIGENCE DASHBOARD

Introduction

With the increasing frequency and complexity of cyber threats, cybersecurity professionals need a centralized system to monitor incidents, investigate threats, and streamline the response process. CTI OPS PANEL addresses this challenge by offering a comprehensive, hacker-style dashboard that aggregates threat intelligence, provides actionable analytics, and supports SOC workflows through real-time updates and automation.

Abstract

The Cyber Threat Intelligence Dashboard (CTI OPS PANEL) is a web-based platform designed to centralize, analyze, and visualize real-time cyber threat data for security operations centers (SOC). It provides live threat feeds, search functionality, automated reporting, incident response playbooks, and a user friendly interface for SOC analysts to detect and respond to security incidents efficiently.

Tools Used

• Backend: Python (Flask), FPDF for PDF export • Frontend: HTML, CSS, JavaScript • Libraries: Chart.js (visualization), Leaflet.js (geolocation maps) • APIs/Utilities: Mock data with option for live integration, REST/AJAX for feed updates • Other: Role-based login, activity log, export to CSV, JSON, and PDF

Steps Involved in Building the Project

1. Backend Setup: Initialized Flask app, built out routes for dashboard, threat feed, lookup, login/logout, and exports. 2. User Authentication: Added session-based login for analyst/admin roles, controlling access to features.

3. Threat Feed & Live Ingestion: Integrated mock data, enabled live feed auto-refresh, and allowed manual/additional threat submission via the UI.

4. Visualization: Used Chart.js for threat summaries and Leaflet.js to plot threat locations on a map.

5. Search & Incident Response: Implemented real-time threat search; showed contextual incident response playbooks in modals for each new threat.

6. Export & Reporting: Enabled exports of report data in PDF, CSV, and JSON formats using dedicated Flask routes.

7. Audit/SOC Log: Tracked all user actions in a SOC log, viewable as a dashboard section for accountability/traceability.

8. Recommendations & UI: Displayed security recommendations and ensured a responsive, dark-mode hacker UI.

Conclusion

The CTI OPS PANEL project demonstrates a modern, extensible approach to cyber threat intelligence operations. By blending live data visualization, threat lookup, incident response planning, and SOC logging into a single dashboard, the platform empowers SOC analysts to respond to attacks faster and more effectively. This project also serves as a foundation for future integrations with real-world threat intelligence APIs, user management improvements, and advanced analytics capabilities.