Cyber Threat Intelligence Dashboard Report

Introduction

In today's digital landscape, organizations face an increasing number of cyber threats that can compromise sensitive data and disrupt operations. The Cyber Threat Intelligence (CTI) Dashboard is designed to provide security analysts with a comprehensive tool for monitoring, analyzing, and responding to these threats in real-time. This dashboard aggregates data from various threat intelligence sources, enabling users to make informed decisions and take proactive measures against potential security incidents.

Abstract

The CTI Dashboard is a web-based application that consolidates real-time threat feeds, visualizes threat metrics, and allows users to perform threat lookups. Built using modern web technologies, the dashboard features a user-friendly interface that displays critical information such as threat levels, indicators of compromise (IOCs), and trends over time. The application also includes export functionality for generating reports in CSV format, facilitating data sharing and analysis. This report outlines the tools used, the steps involved in building the project, and the overall impact of the dashboard on cybersecurity operations.

Tools Used

- HTML5: For structuring the web application.
- CSS (Bootstrap 5): For responsive design and styling.
- JavaScript: For interactivity and dynamic content updates.
- Chart.js: For visualizing threat data through charts.
- Font Awesome: For icons and UI elements.
- Mock Data: Simulated threat intelligence data for demonstration purposes.

Steps Involved in Building the Project

1. Project Setup: Created a single HTML file structure, integrating necessary libraries (Bootstrap, Chart.js, Font Awesome).

2. Design Implementation: Developed a dark-themed, responsive layout using Bootstrap's grid system, ensuring compatibility across devices.

3. Dashboard Components: Implemented key features including threat metrics, real-time threat feed, and visual analytics through charts.

4. Threat Lookup Functionality: Enabled users to input IP addresses, domains, or hashes, with automatic detection and risk assessment.

5. Export Functionality: Developed CSV export capabilities for full reports, individual threat analyses, and current lookup results.

6. User Interaction: Enhanced user experience with responsive design, hover effects, and keyboard support for threat lookups.

7. Testing and Validation: Conducted manual testing across different browsers and devices to ensure functionality and performance.

Conclusion

The Cyber Threat Intelligence Dashboard serves as a vital tool for organizations seeking to enhance their cybersecurity posture. By aggregating real-time threat intelligence and providing actionable insights, the dashboard empowers security analysts to respond effectively to emerging threats. The project demonstrates the potential of web technologies in creating intuitive and powerful security solutions. Future enhancements could include real-time API integrations and advanced filtering options, further expanding the dashboard's capabilities.