CIS 542-01: Digital Forensics (Fall 2023)

Project Proposal: SIEM Data Analysis Web Application

Project Goals Statement:

The project aimed to develop a user-friendly web application focused on crucial aspects of Security Information and Event Management (SIEM) data analysis. Its objectives included collecting and analyzing Windows System, Security, and Application logs, conducting event impact analysis to identify critical events, and providing clear log distribution visualizations through pie charts.

Scope Statement:

This project primarily focused on creating a web application specifically tailored for Windows-based log analysis (System, Security, and Application) and providing visualization features like pie charts for log distribution. However, it did not extend to building a comprehensive SIEM tool nor addressed broader network security concerns beyond log analysis within SIEM tools. Integration with logs from other operating systems was outside the project scope.

Deliverables Statement:

The project delivered a functional web application capable of:

- **Data Collection & Analysis:** Gathering and analyzing Windows-based logs with an option for easy CSV downloads.
- **Log Analysis:** Prioritizing critical events and analyzing anomalous activities within the collected logs.
- **Visualization Features:** Presenting log percentage distributions through pie charts, aiding in understanding the contribution of system components to log generation.

The program created included functionalities to:

1. Develop a user-friendly web application interface.
2. Log Collection(Windows - System, Security, Application)
3. Identify and visualize critical events impacting cybersecurity decisions.
4. Visualize log percentage distributions.