CIS 542-01: Digital Forensics

SIEM Data Analysis Web Application

Group Member: Dnyaneshwari Jagtap
StudentID: 02097835
Email: djagtap@umassd.edu
Date: 3 December 2023

Content

1. Goal
2. Scope
3. Technique
4. Result
5. Demo
6. Conclusion

Goal

The goal of our project was to create a user-friendly web application focusing on critical aspects of Security Information and Event Management (SIEM) data analysis.

Objectives:

- Log Collection: Collected System, Security, and Application Windows logs with a download CSV option.
- Event Impact Analysis: Analyzing data to identify crucial events by prioritizing and analyzing anomalous logs.
- Log Percentage Visualization: Providing clear visualizations of log distribution using a Pie chart.

Scope

1. **Project Focus:** Creation of a user-friendly SIEM Data Analysis Web Application focused on SIEM Log analysis.
2. **Key Objectives:**
    - Log Collection: Gathered System, Security, and Application Windows SIEM logs with a downloadable CSV option.
    - Event Impact Analysis: Identified crucial events through prioritization and analysis of anomalous logs.
    - Log Percentage Visualization: Provided clear visualizations of log distribution using Pie charts.
3. **Scope Highlights:**
    - In-depth analysis of Windows logs for cybersecurity insights.
    - Emphasis on essential functionalities: Data Collection, Log Analysis, and Visualization.

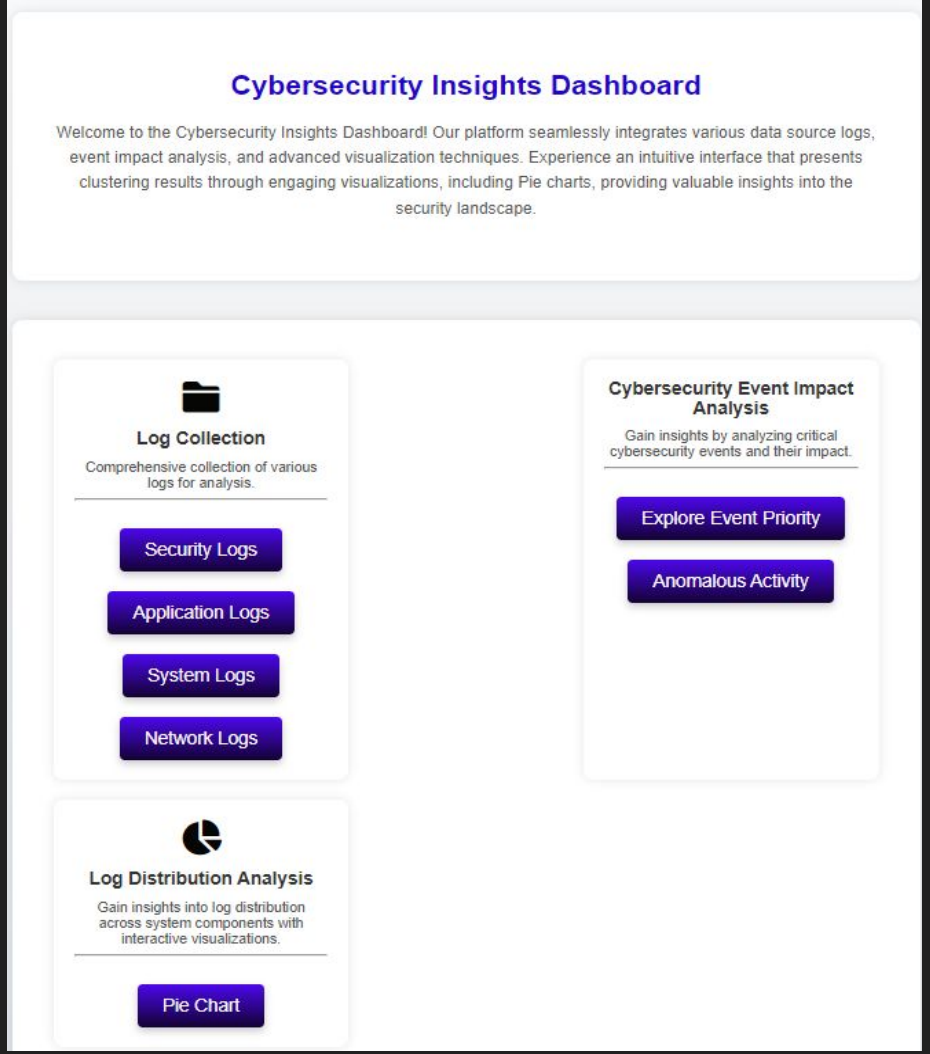
Technique/Methodology

1. Programming Language: Python
2. Libraries Used: pandas, csv, plotly, matplotlib, sklearn
3. Log Collection : Analyzed a CSV file containing Windows SIEM logs. Collected Windows Application, Security, and System events. Displayed logs on a web page with CSV download option.
4. Event Prioritization : Identified critical cybersecurity events, prioritized based on event ID.
5. Anomalous activity Detection: Detected anomalous activity within collected logs using sklearn's Isolation Forest for anomaly detection.
6. Visualizations : Created an interactive Pie Chart using plotly to visualize aggregated counts(Level, Source, Event ID, Task Category) attributes.

Result

The web application performs the following tasks:

1. **Log Collection:** Gathers and analyzes Windows System, Security, and Application logs, enabling easy CSV downloads.
2. **Cybersecurity Event Impact Analysis:** Ranks critical events using event prioritization, analyzes anomalous activities.
3. **Visualization:** Presents log percentage distributions via pie charts, helps in understanding log contribution by system components.



Demo

Conclusion

The SIEM Log Analysis Web Application has successfully implemented and achieved its primary objectives of Data Collection & Analysis, Log Analysis, and Visualization.