CIS 542-01: Digital Forensics (Fall 2023)

Project Report

SIEM Data Analysis Web Application

Project Overview & Goal:

The project aimed to create a user-friendly web application focusing on critical aspects of Security Information and Event Management (SIEM) data analysis. The objectives included:

1. **Log Collection:** Collected System, Security, and Application Windows logs and with download csv option.

2. **Event Impact Analysis:** Analyzing data to identify crucial events by prioritizing events and analyzing anomalous logs.
3. **Log Percentage Visualization:** Providing clear visualizations of log distribution using Pie chart.

Project Outcome:

The web app performs the following tasks:

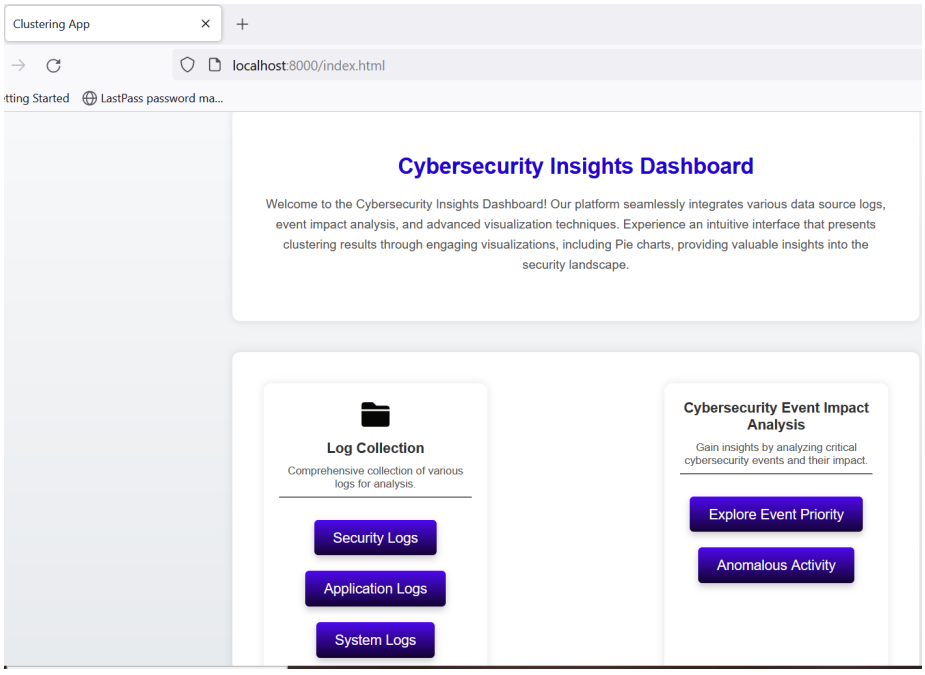
1. **Data Collection & Analysis**: Gathers and analyzes Windows System, Security, and Application logs, enabling easy CSV downloads.
2. **Log Analysis:** Ranks critical events using event prioritization, analyzes anomalous activities.
3. **Visualization Features:** Presents log percentage distributions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

Project Implementation:

The project's implementation involved:

1. **Web Application Creation:** Developing an intuitive interface for seamless user interaction. Web application is accessible on below URL. http://localhost:8000/index.html

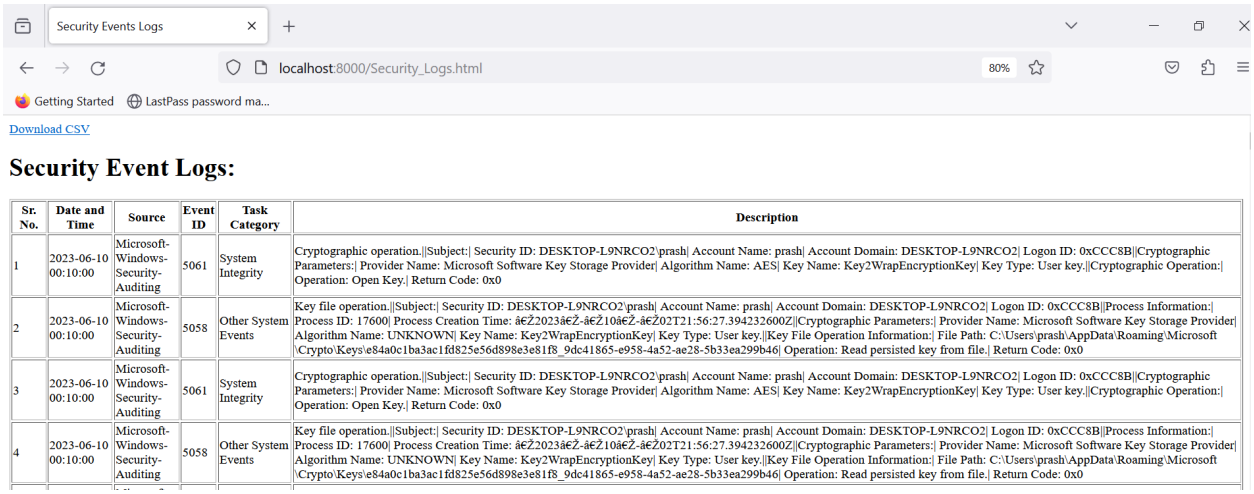
Screenshot:



2. **Log Collection:** Collected Security, System and Application Windows logs with download CSV option.

1. **Windows 'Security logs':**
   http://localhost:8000/Security_Logs.html

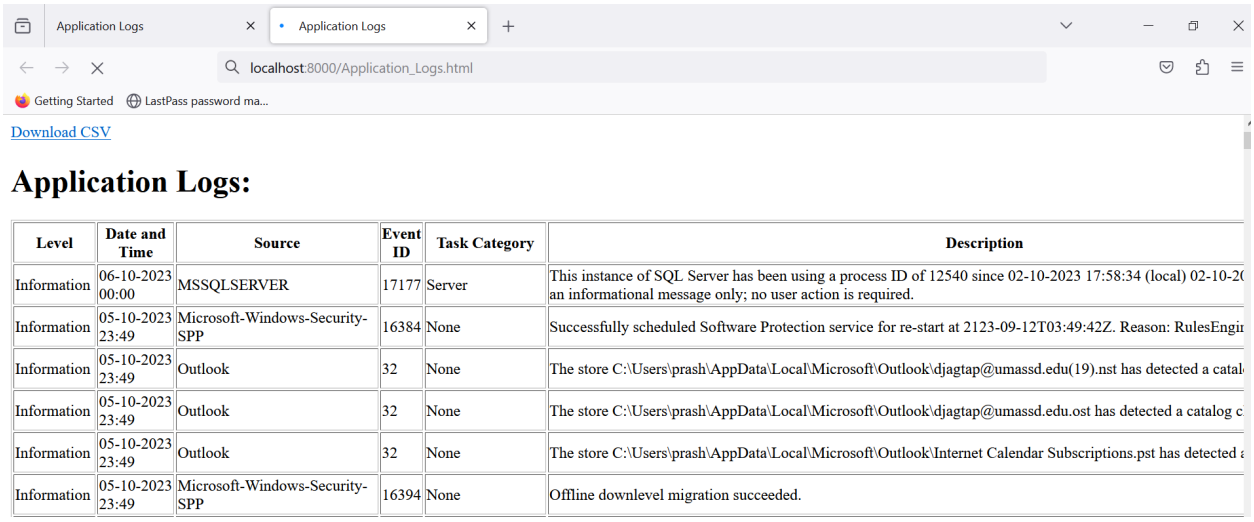
   Screenshot:



2. Application Logs:

http://localhost:8000/Application_Logs.html

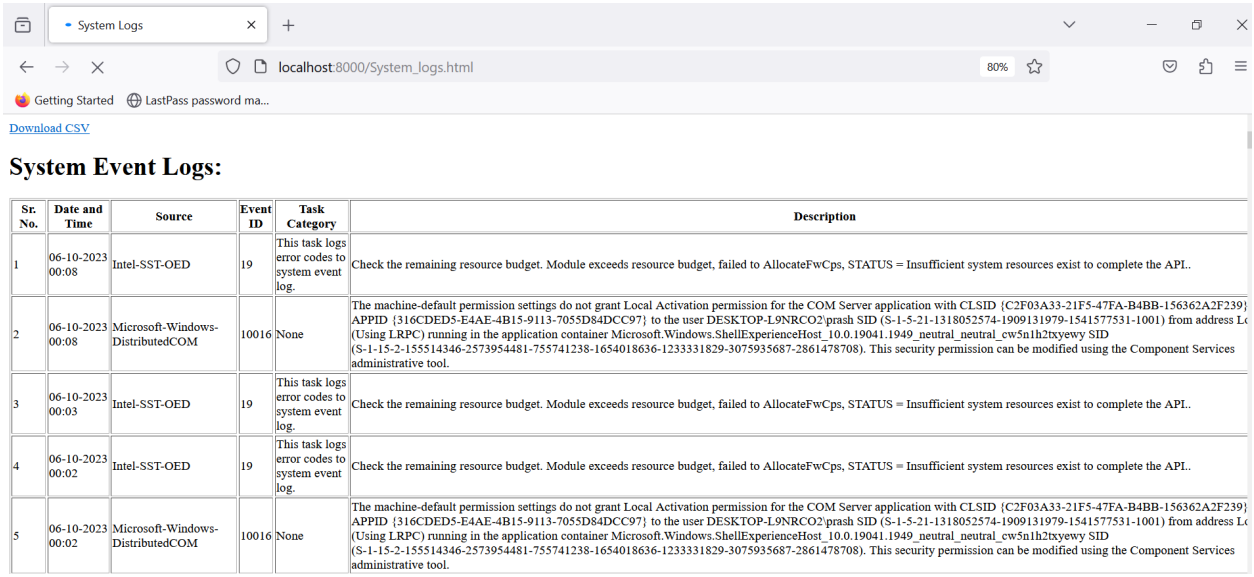
Screenshot:



3. Windows System Logs:

http://localhost:8000/System_logs.html

Screenshot:

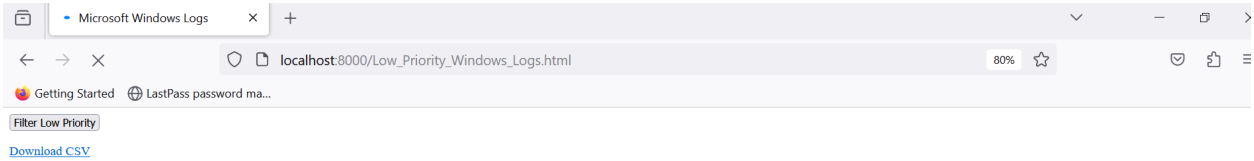


Sr. No.	Date and Time	Source	Event ID	Task Category	Description
1	06-10-2023 00:08	Intel-SST-OED	19	This task logs error codes to system event log.	Check the remaining resource budget. Module exceeds resource budget, failed to AllocateFwCps, STATUS = Insufficient system resources exist to complete the API..
2	06-10-2023 00:08	Microsoft-Windows-DistributedCOM	10016	None	The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A33-21F5-47FA-B4BB-156362A2F239} APPID {316CDED5-E4AE-4B15-9113-7055D84DCC97} to the user DESKTOP-L9NRCO2\prash SID (S-1-5-21-1318052574-1909131979-1541577531-1001) from address Lo (Using LRPC) running in the application container Microsoft.Windows.ShellExperienceHost_10.0.19041.1949_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-755741238-1654018636-1233331829-3075935687-2861478708). This security permission can be modified using the Component Services administrative tool.
3	06-10-2023 00:03	Intel-SST-OED	19	This task logs error codes to system event log.	Check the remaining resource budget. Module exceeds resource budget, failed to AllocateFwCps, STATUS = Insufficient system resources exist to complete the API..
4	06-10-2023 00:02	Intel-SST-OED	19	This task logs error codes to system event log.	Check the remaining resource budget. Module exceeds resource budget, failed to AllocateFwCps, STATUS = Insufficient system resources exist to complete the API..
5	06-10-2023 00:02	Microsoft-Windows-DistributedCOM	10016	None	The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID {C2F03A33-21F5-47FA-B4BB-156362A2F239} APPID {316CDED5-E4AE-4B15-9113-7055D84DCC97} to the user DESKTOP-L9NRCO2\prash SID (S-1-5-21-1318052574-1909131979-1541577531-1001) from address Lo (Using LRPC) running in the application container Microsoft.Windows.ShellExperienceHost_10.0.19041.1949_neutral_neutral_cw5n1h2txyewy SID (S-1-15-2-155514346-2573954481-755741238-1654018636-1233331829-3075935687-2861478708). This security permission can be modified using the Component Services administrative tool.

3. **Critical Event Identification:** Implementing algorithms to prioritize and visualize critical events impacting cybersecurity decisions.

   a. **Event Priority:**

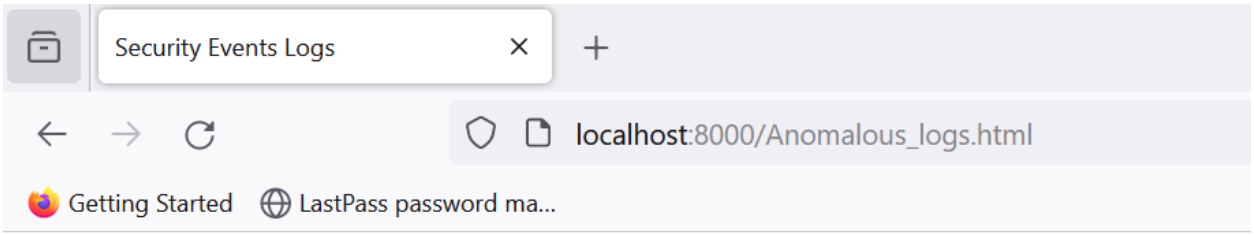
Screenshot:



ï»¿Level	Date and Time	Source	Event ID	Task Category	Description	Priority
Information	06-10-2023 00:00	MSSQLSERVER	17177	Server	This instance of SQL Server has been using a process ID of 12540 since 02-10-2023 17:58:34 (local) 02-10-2023 21:58:34 (UTC). This is an informational message only; no user action is required.	Low
Information	05-10-2023 23:49	Microsoft-Windows-Security-SPP	16384	None	Successfully scheduled Software Protection service for re-start at 2123-09-12T03:49:42Z. Reason: RulesEngine.	Low
Information	05-10-2023 23:49	Outlook	32	None	The store C:\Users\prash\AppData\Local\Microsoft\Outlook\djagtap@umassd.edu(19).nst has detected a catalog checkpoint.	Low
Information	05-10-2023 23:49	Outlook	32	None	The store C:\Users\prash\AppData\Local\Microsoft\Outlook\djagtap@umassd.edu.ost has detected a catalog checkpoint.	Low
Information	05-10-2023 23:49	Outlook	32	None	The store C:\Users\prash\AppData\Local\Microsoft\Outlook\Internet Calendar Subscriptions.pst has detected a catalog checkpoint.	Low
Information	05-10-2023 23:49	Microsoft-Windows-Security-SPP	16394	None	Offline downlevel migration succeeded.	Low
Information	05-10-2023 23:49	SecurityCenter	15	None	Updated Windows Defender status successfully to SECURITY_PRODUCT_STATE_ON.	Low
Information	05-10-2023 23:49	nssm	1040	None	Service ExpressVPNService received POWEREVENT control, which will be handled.	Low
Information	05-10-2023 23:49	igccservice	0	None	PowerEvent handled successfully by the service.	Low

b. Anomalous Events:

Screenshot:



Anomalous Windows Events:

Date and Time	Source	Event ID	Task Category	Anomaly
06-10-2023 00:09:37	Microsoft-Windows-Security-Auditing	4672	Special Logon	Anomalous
06-10-2023 00:09:37	Microsoft-Windows-Security-Auditing	4624	Logon	Anomalous
06-10-2023 00:09:36	Microsoft-Windows-Security-Auditing	4672	Special Logon	Anomalous
06-10-2023 00:09:36	Microsoft-Windows-Security-Auditing	4624	Logon	Anomalous
05-10-2023 23:55:40	Microsoft-Windows-Security-Auditing	4799	Security Group Management	Anomalous
05-10-2023 23:55:35	Microsoft-Windows-Security-Auditing	4672	Special Logon	Anomalous
05-10-2023 23:55:35	Microsoft-Windows-Security-Auditing	4624	Logon	Anomalous
05-10-2023 23:54:06	Microsoft-Windows-Security-Auditing	4672	Special Logon	Anomalous
05-10-2023 23:54:06	Microsoft-Windows-Security-Auditing	4624	Logon	Anomalous
05-10-2023 23:49:13	Microsoft-Windows-Security-Auditing	4799	Security Group Management	Anomalous
05-10-2023 23:49:09	Microsoft-Windows-Security-Auditing	4798	User Account Management	Anomalous
05-10-2023 23:49:09	Microsoft-Windows-Security-Auditing	4798	User Account Management	Anomalous
05-10-2023 23:49:09	Microsoft-Windows-Security-Auditing	4798	User Account Management	Anomalous
05-10-2023 23:49:09	Microsoft-Windows-Security-Auditing	4798	User Account Management	Anomalous
05-10-2023 23:49:09	Microsoft-Windows-Security-Auditing	4672	Special Logon	Anomalous
05-10-2023 23:49:09	Microsoft-Windows-Security-Auditing	4624	Logon	Anomalous
05-10-2023 23:49:09	Microsoft-Windows-Security-Auditing	5382	User Account Management	Anomalous
05-10-2023 23:49:07	Microsoft-Windows-Security-Auditing	4672	Special Logon	Anomalous
05-10-2023 23:49:07	Microsoft-Windows-Security-Auditing	4624	Logon	Anomalous
05-10-2023 23:48:27	Microsoft-Windows-Security-Auditing	5382	User Account Management	Anomalous
05-10-2023 23:47:54	Microsoft-Windows-Security-Auditing	4672	Special Logon	Anomalous
05-10-2023 23:47:54	Microsoft-Windows-Security-Auditing	4624	Logon	Anomalous
05-10-2023 23:47:54	Microsoft-Windows-Security-Auditing	4634	Logoff	Anomalous
05-10-2023 23:47:54	Microsoft-Windows-Security-Auditing	4634	Logoff	Anomalous
05-10-2023 23:47:54	Microsoft-Windows-Security-Auditing	4634	Logoff	Anomalous

4. **Log Percentage Visualization:** Presented log percentage distributions via pie charts.

Conclusion:

The SIEM Data Analysis Web Application successfully achieves its objectives by providing essential functionalities for event impact analysis and log percentage visualization. It empowers users to make informed decisions based on critical event insights and log distribution representations.