Windows Event Log Investigation using Splunk

Introduction:

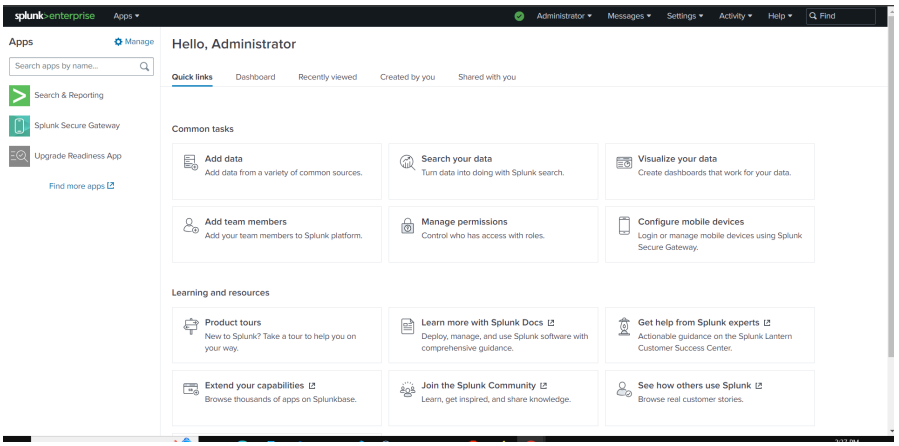
This report consists of Windows event log analysis using Splunk Enterprise SIEM. The analysis consists of data ingestion, field extraction, searching, statistical analysis, event correlation, and alerting.

Dataset:

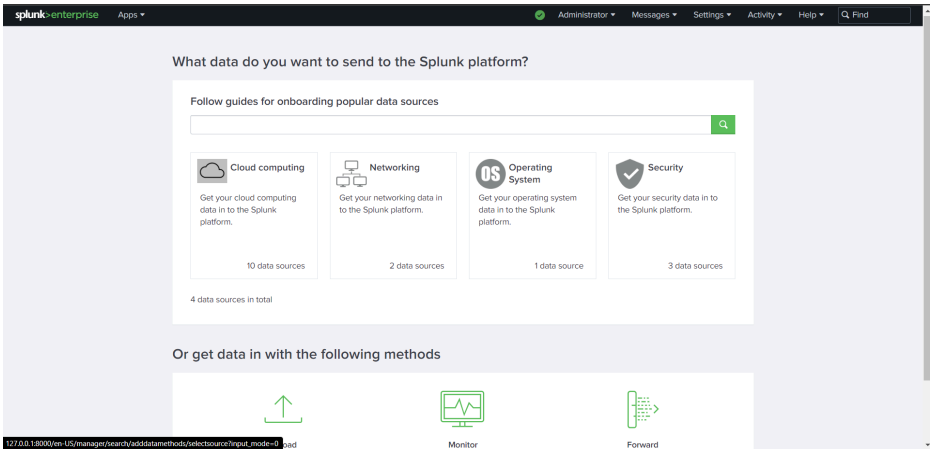
The dataset is a simulated Windows Event Log file in XML format, containing 100 entries. These entries simulate typical Windows system, application, and security events, including information on event sources, IDs, levels, and descriptions.

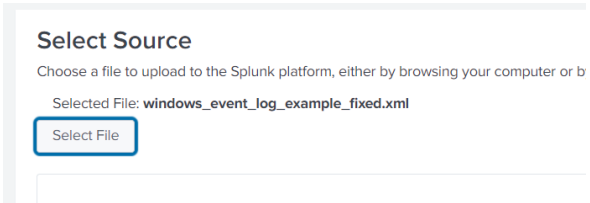
Tasks:

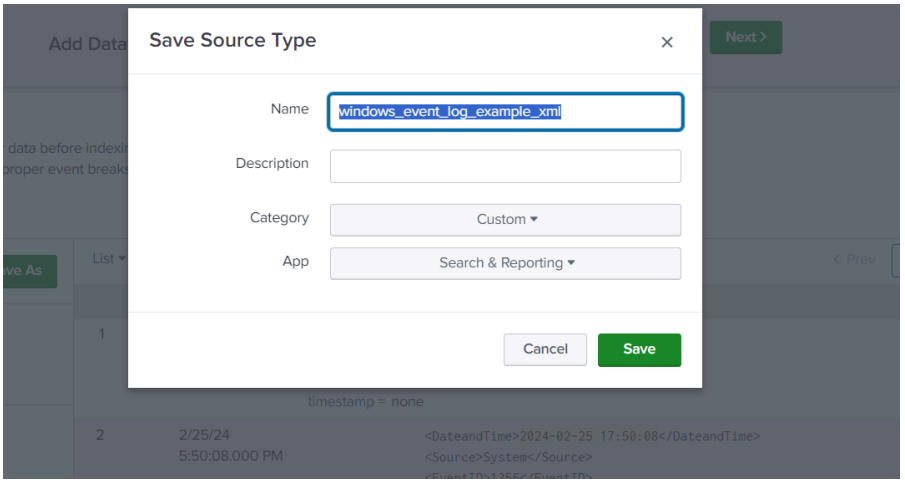
1. Data Ingestion and field extraction:



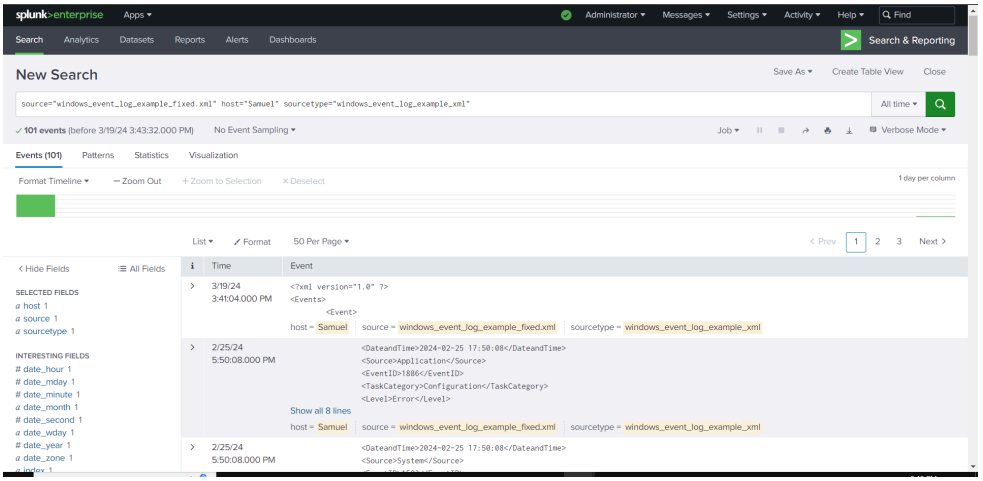
Uploading a .xml Windows event log file that is stored locally





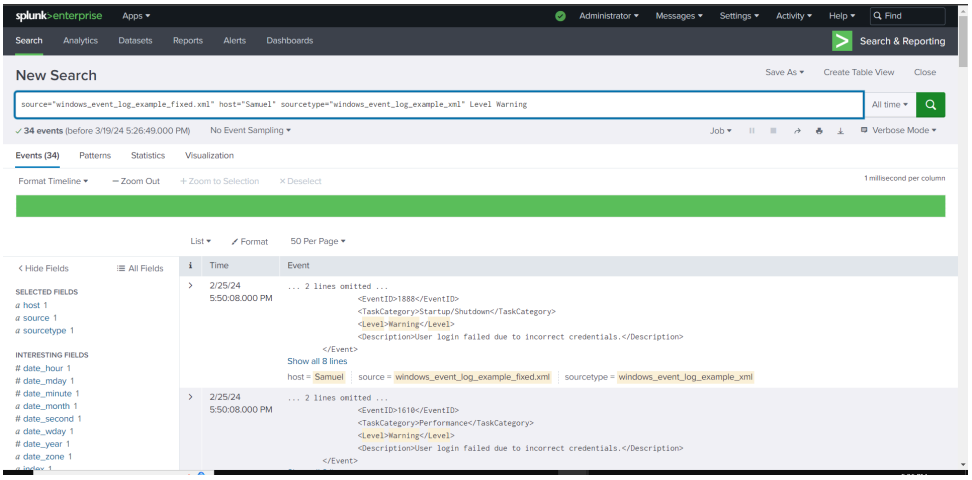


Analyzing the logs using the search query



2. Searching

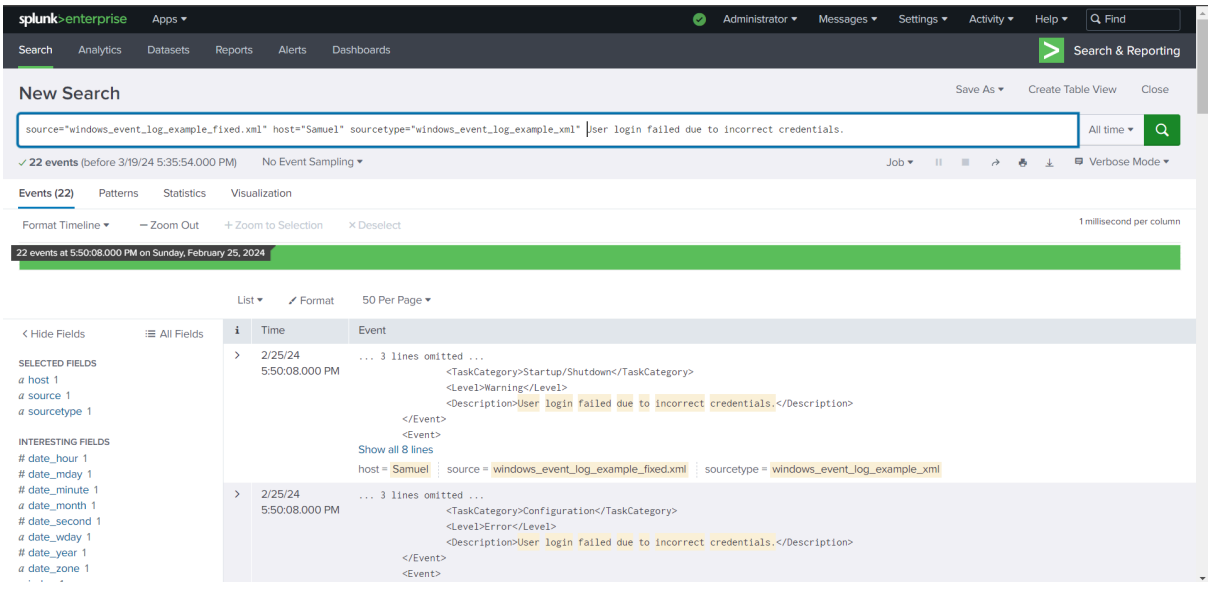
- Discovered 34 warnings using command ***source="windows_event_log_example_fixed.xml" host="Samuel" sourcetype="windows_event_log_example_xml" Level Warning***

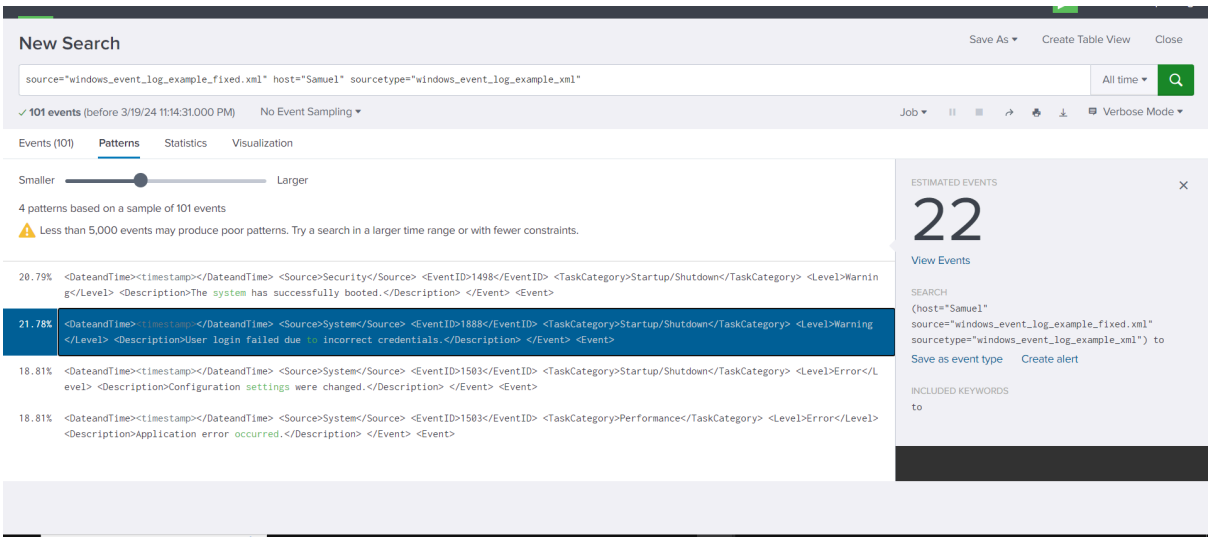


- Out of 34 warning
    - 8 events consist of success system boot

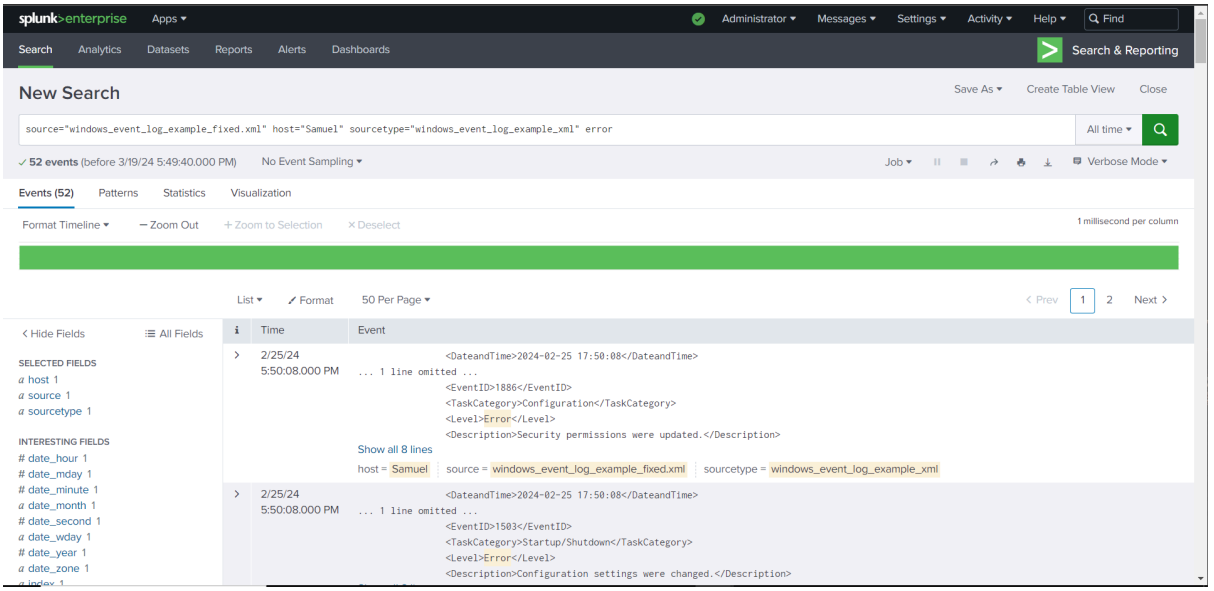
- 4 times security permissions were updated.

- 22 events indicate “Failed user login due to incorrect credentials” This indicates that there might be a brute force attack.
- The command used: ***source="windows_event_log_example_fixed.xml" host="Samuel" sourcetype="windows_event_log_example_xml" Level Warning User login failed due to incorrect credentials.***

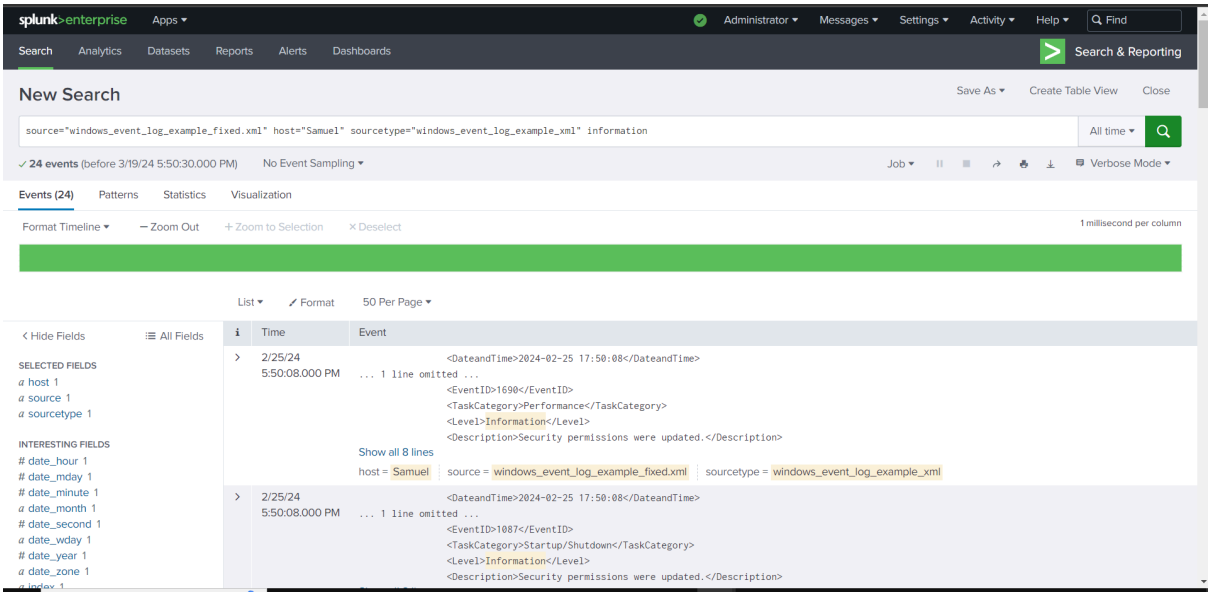




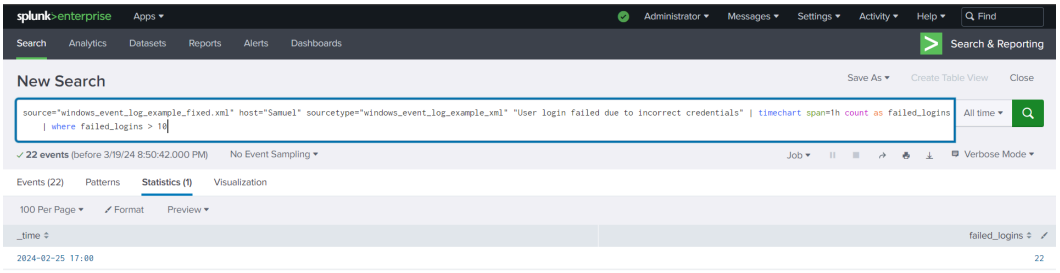
- Discovered 52 error events using command: ***source="windows_event_log_example_fixed.xml" host="Samuel" sourcetype="windows_event_log_example_xml" error***



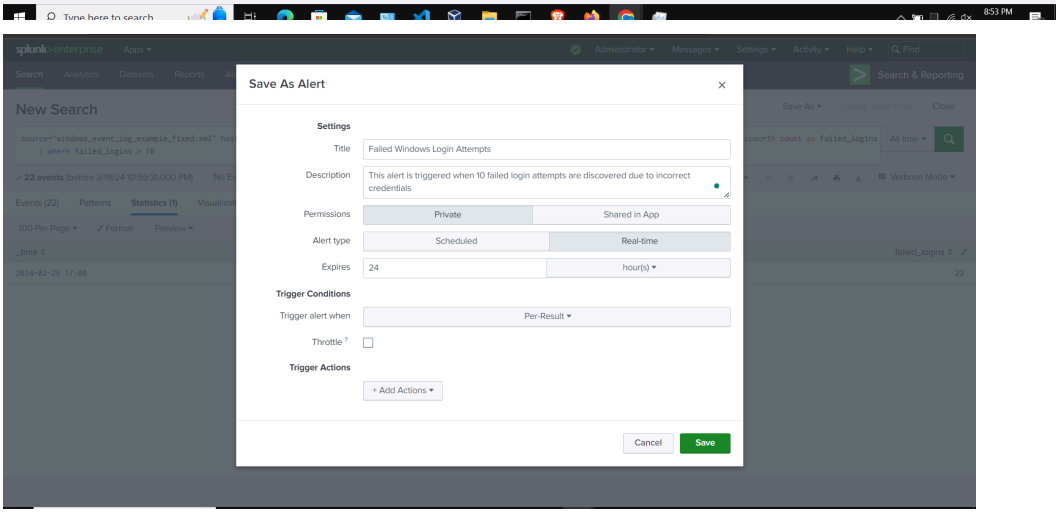
- There are 24 information-level events, command used: ***source="windows_event_log_example_fixed.xml" host="Samuel" sourcetype="windows_event_log_example_xml" information***



3. **Alerting:**
    - This step addresses setting up an alert. The alert is meant to be triggered when 10 failed login attempts occur due to wrong credentials in one hour.
    - The search query used is: ***source="windows_event_log_example_fixed.xml" host="Samuel" sourcetype="windows_event_log_example_xml" "User login failed due to incorrect credentials" | timechart span=1h count as failed_logins | where failed_logins > 10***

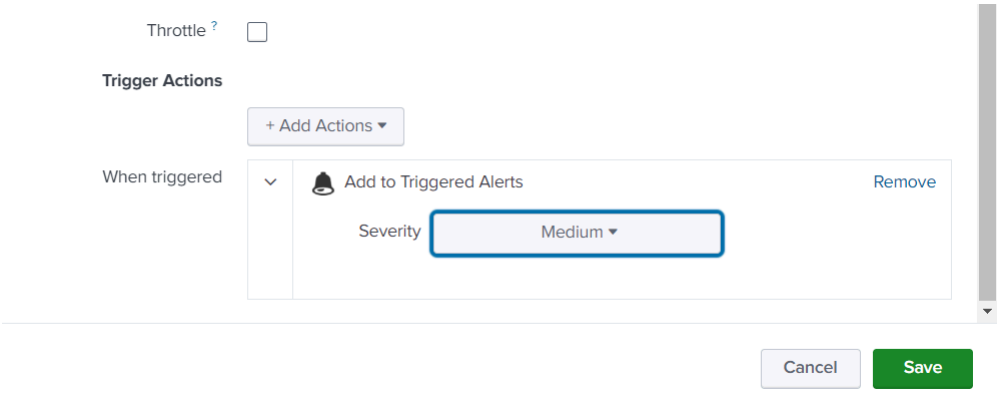


-



-

- Adding action to alert:



-