

Windows Event Log Investigation using Splunk

Introduction:

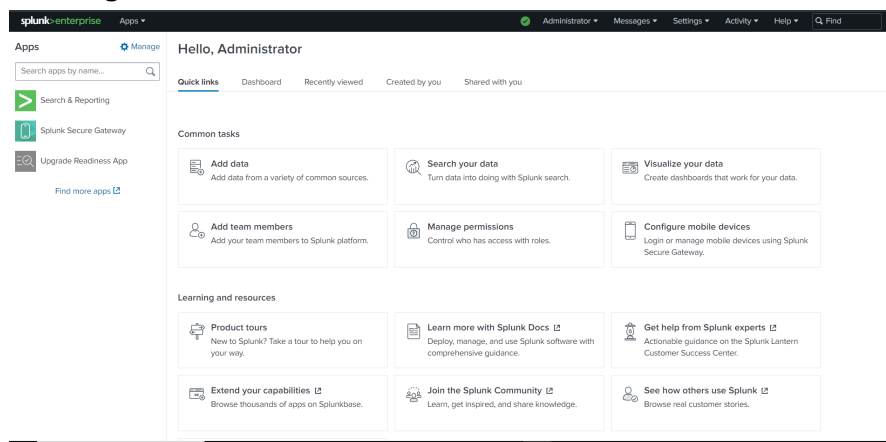
This report consists of Windows event log analysis using Splunk Enterprise SIEM. The analysis consists of data ingestion, field extraction, searching, statistical analysis, event correlation, and alerting.

Dataset:

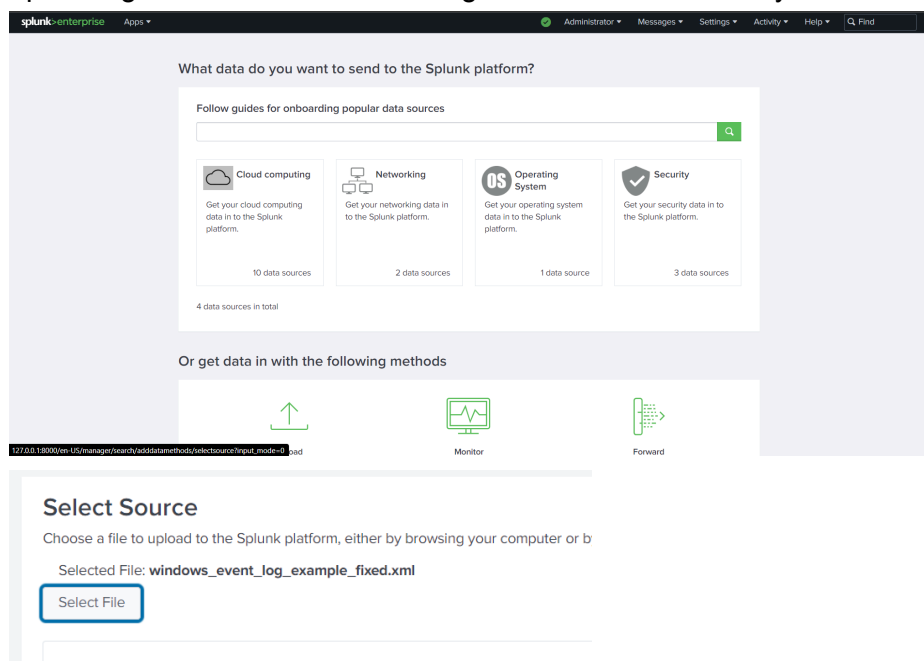
The dataset is a simulated Windows Event Log file in XML format, containing 100 entries. These entries simulate typical Windows system, application, and security events, including information on event sources, IDs, levels, and descriptions.

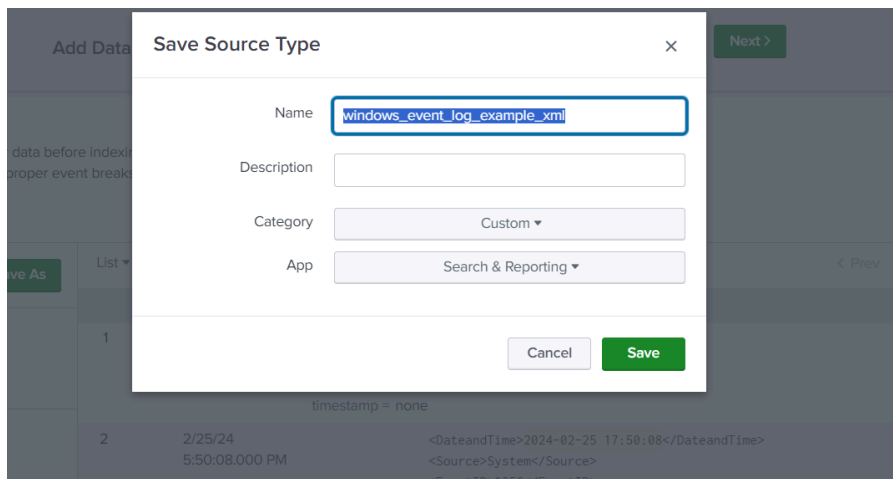
Tasks:

1. Data Ingestion and field extraction:

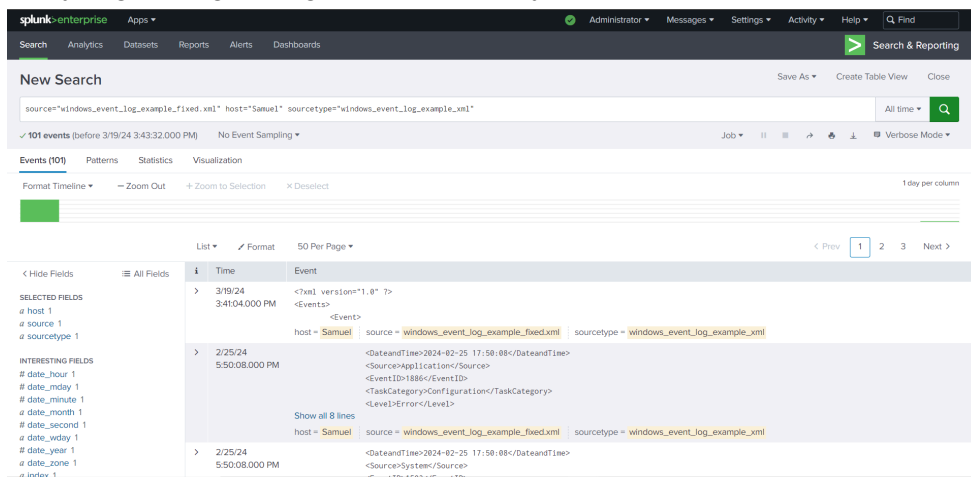


Uploading a .xml Windows event log file that is stored locally



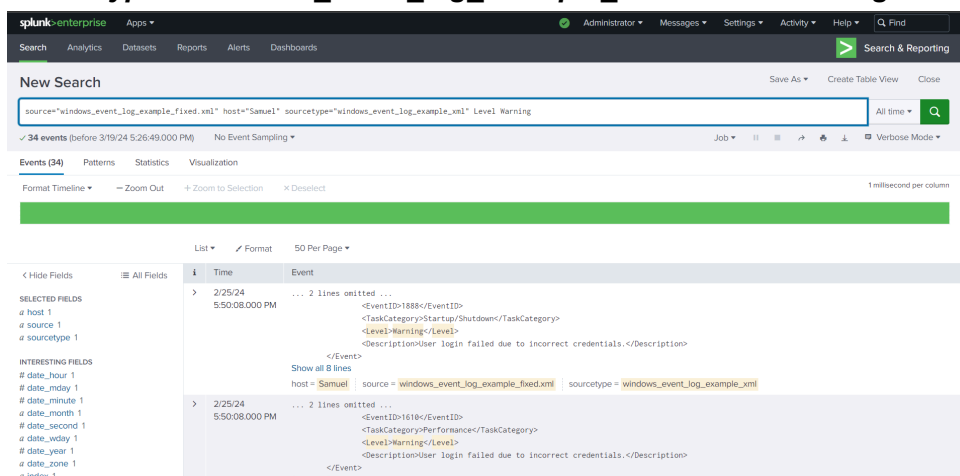


Analyzing the logs using the search query



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.***

The screenshot shows the Splunk Enterprise interface with a search query: `source="windows_event_log_example_fixed.xml" host="Samuel" sourcetype="windows_event_log_example_xml" | user login failed due to incorrect credentials.` The results show 22 events. The first event is expanded, showing XML data with a warning level and the description "User login failed due to incorrect credentials." The second event is also expanded, showing an error level and the same description.

The screenshot shows the Splunk Enterprise interface with a search query: `source="windows_event_log_example_fixed.xml" host="Samuel" sourcetype="windows_event_log_example_xml"` The results show 101 events. The interface includes a pattern view showing 4 patterns based on a sample of 101 events. The first pattern is highlighted, showing XML data with a warning level and the description "User login failed due to incorrect credentials." The second pattern is also highlighted, showing an error level and the same description.

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

The screenshot shows the Splunk Enterprise interface with a search query: `source="windows_event_log_example_fixed.xml" host="Samuel" sourcetype="windows_event_log_example_xml" error`. The search results show 52 events. The selected event is an error event with the following details:

Time	Event
2/25/24 5:50:08.000 PM	<pre><DateandTime>2024-02-25 17:50:08</DateandTime> ... 1 line omitted ... <EventID>1886</EventID> <TaskCategory>Configuration</TaskCategory> <Level>Error</Level> <Description>Security permissions were updated.</Description></pre>

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

The screenshot shows the Splunk Enterprise interface with a search query: `source="windows_event_log_example_fixed.xml" host="Samuel" sourcetype="windows_event_log_example_xml" information`. The search results show 24 events. The selected event is an information event with the following details:

Time	Event
2/25/24 5:50:08.000 PM	<pre><DateandTime>2024-02-25 17:50:08</DateandTime> ... 1 line omitted ... <EventID>1690</EventID> <TaskCategory>Performance</TaskCategory> <Level>Information</Level> <Description>Security permissions were updated.</Description></pre>

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`

splunkenterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

New Search

Save AsCreate Table ViewClose

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 > 10All time

22 events (before 3/19/24 8:50:42.000 PM)No Event Sampling

Job

Verbose Mode

Events (22)PatternsStatistics (1)Visualization

100 Per PageFormatPreview

_time

failed_logins

2024-02-25 17:0022

splunkenterpriseApps

AdministratorMessagesSettingsActivityHelpFind

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

New Search

Save AsCreate Table ViewClose

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 > 10All time

22 events (before 3/19/24 10:59:31.000 PM)No Event Sampling

Job

Verbose Mode

Events (22)PatternsStatistics (1)Visualization

100 Per PageFormatPreview

_time

failed_logins

2024-02-25 17:0022

Save As Alert

×

Settings

TitleFailed Windows Login Attempts

DescriptionThis alert is triggered when 10 failed login attempts are discovered due to incorrect credentials

PermissionsPrivateShared in App

Alert typeScheduledReal-time

Expires24hour(s)

Trigger Conditions

Trigger alert whenPer-Result

Throttle?

Trigger Actions

+ Add Actions

CancelSave

- Adding action to alert:

Throttle? ☐

Trigger Actions

+ Add Actions

When triggered

▼

Add to Triggered Alerts

Remove

Severity

Medium

CancelSave

SearchAnalyticsDatasetsReportsAlertsDashboards

Search & Reporting

Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

1 Alerts

AllYoursThis App'sfilter

Title

Failed Windows Login Attempts

Actions

Open in Search

Edit

Owneradmin

Appsearch

SharingPrivate

StatusEnabled