

# USE SPLUNK CLOUD TO PERFORM A SEARCH AND INVESTIGATE LOG DATA

Pedro Osorio Lopez.

## 1. High-Level Project Description:

\*In this activity, we'll upload sample log data, and use Splunk Cloud to perform a search and investigate this data.

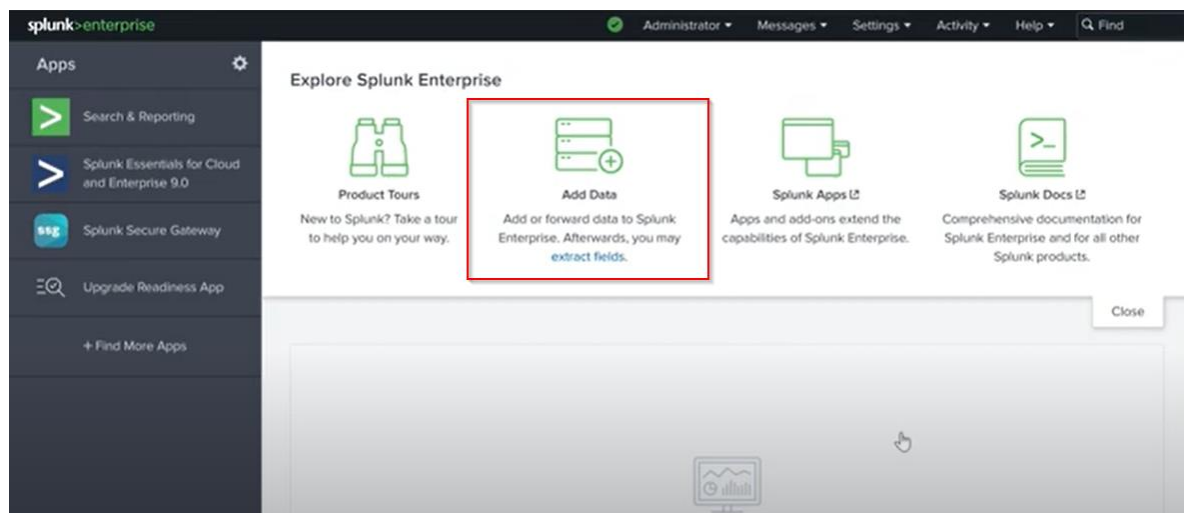
## 2. Project Setup and Required Tools:

\*All we need to complete this activity is a Splunk account, so we can use this extremely popular SIEM tool on any device.

## 3. Step by Step Project Walkthrough

\*In this lab, we will: Upload sample log data, search through indexed data, evaluate search results, identify different data sources, and locate failed SSH login(s) for the root account.

\*The first step is pretty straightforward, since one logged in into Splunk, in the main interface we just need to click "Add Data" and proceed to upload it and fill out the necessary information. Note that Splunk can ingest zip data; Google already provided sample files to us, but these can be downloaded from Splunk as well if necessary.



\*Once successfully uploaded, we can proceed to search through all the indexed data included in the imported file. For example:

The screenshot shows the Splunk Enterprise interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below this is a 'Search & Reporting' section with a 'New Search' button. The search query is entered in a text box: `source="tutorialdata.zip:*" host="DESKTOP-P567QIR" index="test" fail*`. Below the query, it shows '33,253 events (before 2/2/23 7:15:53.000 PM)' and 'No Event Sampling'. The interface includes a timeline visualization and a table of results. The table has columns for 'Time' and 'Event'. The results show failed password attempts for 'appserver' and 'root' users.

Time	Event
2/1/23 9:44:26.000 AM	Thu Feb 01 2023 09:44:26 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2
2/1/23 9:44:26.000 AM	Thu Feb 01 2023 09:44:26 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2
2/1/23 9:44:26.000 AM	Thu Feb 01 2023 09:44:26 mailsv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2

\*In this query, we are using a source (the uploaded zip file), a host, and an index to get a series of results. In we add the keyword “fail\*), we will be checking for all the entries that contain words which start with fail (including fail, failed failure, etc), to check for anomalies such as failed login attempts.

\*Lastly, if we want to locate failed SSH login(s) for the root account, we can do so with the following search query:

The screenshot shows the Splunk Cloud interface. At the top, there's a navigation bar with 'splunk>cloud' and various menu items like 'Apps', 'Messages', 'Settings', 'Activity', and 'Find'. Below this is a 'Search & Reporting' section with a 'New Search' button. The search query is entered in a text box: `index=main host=mailsv fail* root sourcetype=ssh`. Below the query, it shows '692 events (before 10/3/23 8:17:13.000 PM)' and 'No Event Sampling'. The interface includes a timeline visualization and a table of results. The table has columns for 'Time' and 'Event'. The results show failed password attempts for the 'root' user.

Time	Event
2/1/23 9:44:26.000 AM	Thu Feb 01 2023 09:44:26 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2

## 4. Summary and/or Recommendations:

\*In this activity, we learned how to use Splunk, a SIEM tool of extreme popularity used by many major companies to safeguard and monitor their data.