Perform a query with Splunk

**Scenario:**

You are a security analyst working at the e-commerce store Buttercup Games. You've been tasked with identifying whether there are any possible security issues with the mail server. To do so, you must explore any failed SSH logins for the root account.

**Background:** Splunk Cloud is an SIEM tool where the data can be accessed through queries.The Queries are written in SPL ( Search Programming Language)

In an organization the SIEM is connected with other tools such as OS/System, Security, Network and Application the query the pulled from the sources.As I have taken free Splunk cloud trail , I am importing data manually to Splunk using Add data from Apps

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Once the data is loaded , we search using search & reporting from Apps

The format of the query follows a Specific index and search term. We can also include logical operations to narrow down the search

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

To narrow down based on searching, we provide the details for restriction within query

A screenshot of a computer

Description automatically generated

* “\*” is a wildcard which is used to represent the value that starts with the fail will be considered . For Eg: they can be fail , failed, failed attempt …,

Observations:

* The Total events that are contained in the main index across all time are over 100,000
* Name of a network device or system from which an event originates can be identified from the field host and here the network device is vendor\_sales.
* The failed SSH logons for the root account on the mail server were over 300