Splunk is a platform that collects, manages, organizes, and analyzes machine data. This assists cybersecurity professionals with the ability to record and monitor large scale events in bite size pieces. Splunk allows users to monitor, search and index data from various sources. Also, while searching through large data blocks, users can set up alerts to alert them of specific actions that have taken place.

A screenshot of a computer

Description automatically generated with medium confidence

1. After downloading Splunk, log into the application.

A screenshot of a computer

Description automatically generated with medium confidence

1. After logging into the Splunk Dashboard, open your settings to configure your logs for ingestion. Select Data Inputs under the Data section.

A screenshot of a computer

Description automatically generated

1. To only analyze events for your local system instead of remote workstations, select Edit under the “Local event log collection” option.

Graphical user interface

Description automatically generated

1. The Event Log Collections screen will populate, and this is where you will select which logs you would like Splunk to ingest. The common logs are Application, Security and System logs.

A screenshot of a computer

Description automatically generated

1. After saving your log settings, you will need to navigate to the Search and Reporting page of Splunk.

A screenshot of a computer

Description automatically generated with medium confidence

1. When adding an “\*” to the search bar and selecting the magnify glass, you will see all events from your local system within the determined scope.

Graphical user interface

Description automatically generated

1. Splunk will show your preselected log events in real time. For example, search for Event Viewer within Windows and open it.

Graphical user interface

Description automatically generated

1. Under Window Logs, right click on Security and select Clear Logs. This will clear all security logs.

A screenshot of a computer

Description automatically generated

1. Going back to Splunk, you can narrow down your search for this particular event by adding parameters to your search.

Text

Description automatically generated

1. Searching for the parameters “\* host=WINDOWS11 source=winEventLog:Security EventCode=1102”, you will find the exact clear log event you performed.

A screenshot of a computer

Description automatically generated with medium confidence

1. You can also place your findings in a table to better review the events.

A screenshot of a computer

Description automatically generated

1. Another option you can create is a Dashboard.

Graphical user interface

Description automatically generated

1. When you select “Create New Dashboard”, this window populates. You will need to title the Dashboard and select Create.

A screenshot of a computer

Description automatically generated

1. Once the Dashboard is created you will need to input the same query used to find the initial security clear log event. Select Apply and close once that is completed.

A screenshot of a computer

Description automatically generated

1. A Dashboard will be created with the tile Clear Logs. Anytime a security clear log event occurs within the time scope of the last 24 hours on this device it will populate within this Dashboard.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated with medium confidence

1. The Dashboard is now available within the Dashboard section of your Administrator home screen.