Tool Reference: Splunk

Accessing Splunk

Step 1: Open the Microsoft Edge browser on the desktop of your SOC workstation and click the bookmark to access Splunk. **Login credentials are saved in the browser.**

Step 2: Once logged in, click on the **"Search & Reporting"** app located on the left side of the window.

Step 3: From here, enter your query into the search box at the top and either hit enter or click on the magnifying glass on the right side of the search bar. The results will be displayed below, click on an arrow to the left of a result to expand it and see more information.

Splunk Example Queries

"192.168.1.1" - Shows all results that contain the IP address in quotes

"192.168.1.1" AND "192.168.1.2" - Shows all results that contain both IPs

"192.168.1.1" OR "192.168.1.2" - Shows all results that at least one of the IPs

host="webserver" | head 1000 - Shows the most recent 1000 results with webserver in the host field

"192.168.1.*" - Wildcards can be used while searching, avoid using them at the start for faster searches.

search "terms" - Another way to specify if you wish to search for a particular string.

search srcip="192.168.1.1" - Searches for events where the string 'srcip="192.168.1.1"' is present

search "4625" - A rudimentary way to search for failed logons from Windows Event Viewer. This will return events that contain the string "4625" anywhere in them, which could include ones that are unrelated.