Tool Reference: Security Onion

Accessing Security Onion

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

Using The Alerts Dashboard

The Alerts dashboard contains notable network events that matched the rule syntax for alerting

Step 1: Once logged in, click on the **"Alerts"** tab located on the left sidebar.

Step 2: To see the logs that created the alert, left click and select **drilldown**.

Step 3: To view the raw log and the fields extracted from them, click on the carrot located to the left of each log.

Using The Hunt Dashboard

*The Hunt dashboard allows you to explore network traffic and hunt for specified Indicators of Compromise (IOCs). * This can also be done via the **Kibanna application**.*

Step 1: Once logged in, click on the **"Hunt"** tab located on the left sidebar.

Step 2: Using the search bar, you are allowed to specify a search team and "hunt" for that term though the network logs