Log sources Onboarding

The log source onboarding process is a procedure of configuring and collecting security event logs from various systems, such as servers, endpoints, and cloud services, into one centralized SIEM for monitoring, alerting, and analysis purposes. In this walkthrough, I will demonstrate step by step how to connect a new device to an existing SIEM.

1. Create an installation Token

In the first step, you need to create an installation token. It is a text string that registers installed collectors to your SUMO Logic account. It is used to verify your SIEM instance.

2. Install Linux collector

The process of installing the Linux collector requires a couple of steps. First, you need to download the collector package. You can do it through the CLI. Use the command below to download the file.

Command - wget "https://collectors.sumologic.com/rest/download/linux/64" -O SumoCollector.sh && chmod +x SumoCollector.sh

Then you need to install the downloaded collector. During the installation, use the token key generated in step 1 of this walkthrough.

Command - sudo ./SumoCollector.sh -q -Vcollector.name=Training-admin- ***-<your initials>***

*Vsumo.token_and_url=****<your token>***

3. Add Source

To finish the SUMO Logic collector configuration, you need to add the source to it. I wrote about the different sources in the 1.1 walkthrough, but generally source “tells” the collector what kind of data it should expect. During the configuration process, you need to add the file path to the folder that contains different logs and messages, such as mail, kern, auth, cron, and daemon. In Linux OS, the file path to this folder is **/var/log/syslog**. You also need to specify the source category. For this type of data, the source category can be named **labs/Linux/messages**.