*nix: Security logs

*nix security logs are a source of data that records information related to login attempts (success and failure), elevated privileges, and other security events as defined by the system's audit policy. Security data is collected and written to the plain text log files hosted within the operating system. These logs are one of the primary tools used by security analysts to detect and investigate unauthorized activity and to troubleshoot access problems.

The *nix security logs contain important events relating to applications, system services, and the operating system. The events describe errors, warnings or details about activity taking place on each system. This information is used to monitor and troubleshoot each system. In the Common Information Model, *nix security logs can be mapped to any of the following data models, depending on the field: Endpoint, Network Sessions, Inventory, Updates, Change, Performance.

Configuration

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). Refer to the documentation, and note the following:

- Source type: This source type includes many identifiers, all listed here.
- Input type: OS Logs, syslog, and scripted
- Add-on or app: Splunk Add-on for Unix and Linux
- Sizing estimate: The best way to estimate sizing is to send the data to Splunk and use the monitoring console to get ingest sizing by index or sourcetype. Data ingest will vary widely, but an estimated baseline is 250/MB per day per item.

Validation

The first step in validating the logs is to run a search and confirm that the index is getting data in the proper time frame and that the source types and sources are as expected. Further validation is done by inspecting the events and making sure the needed fields are seen.

A search similar to the following is a good starting point. You can limit the search to the index you configured by replacing index=* with your choice of name e.g., index=foo.

```
| tstats values(sourcetype) WHERE index=* group by index
```
Application

When your Splunk deployment is ingesting *nix security logs, you can use the data to achieve the following:

- Securing a work-from-home organization
- Investigating a ransomware attack
- Managing *nix system user account behavior