Use Case:

Missing Log Source/Host

Description:

Log sources are the feeds for any SIEM solution. Most of the SIEM solution these days comes with an agent-manager deployment model, which means that on all the log sources, light weight SIEM agent software is installed to collect logs and pass them to a manager for analysis. An attacker, after gaining control over a compromised machine/account, tends to stop all such agent services, so that their unauthorized and illegitimate behavior goes unnoticed.

To counter such malformed actions, SIEM should be configured to raise an alert if a host stops forwarding logs after a threshold limit. For example, the below search query (SPL) in Splunk will raise an alert if a host has not forwarded the logs for more than one hour.

Log Source:

All

Splunk Query:

| metadata type=hosts| where recentTime < now() -3600 | convert cTime(recentTime) as "Last time the log source reported" | rename host as "Log Sources" | table "Log Sources" "Last time the log source reported"