SNMP data

The simple network management protocol (SNMP) is one of the oldest, most flexible, and most broadly adopted IP protocols used for managing or monitoring networking devices, servers, and virtual appliances. This includes network devices such as routers and switches, as well as non-networking equipment such as server hardware or disk arrays. SNMP supports two different methods of obtaining data.

- SNMP Traps are essentially alerts, set to send an alert on a state change, critical threshold, hardware failure and more. Traps are initiated by the SNMP device, and the trap is sent to an SNMP collector.
- SNMP Polling is an interactive query/response approach. Unlike traps, polling is initiated by the SNMP collector in the form of a request for certain—or all—SNMP data available on the SNMP device.

Although many now provide vendor-specific APIs for remote management and data collection, SNMP is still valuable in troubleshooting due to its ubiquity (nearly every device supports it) and inherently centralized design (a single instance of SNMP management software can collect data from every device on an internal network, even across route domains).

SNMP data can provide current information about performance, configuration, and current state. This could include current speed of all of the ports on a switch, the number of bytes sent (per port or in aggregate) through a router, the CPU temperature of a server, and any other information made available by the vendor per the SNMP MIBs for that device.

SNMP Polling helps a security analyst to see the data transmission rates for a network-connected device that is suspected of malicious activity. The data can also help identify abnormal amounts of traffic to a certain site or domain, an abnormal amount of specific SNMP traps from a certain host, and an abnormal number of unique SNMP traps from hosts compared to normal profiles. In the Common Information Model, SNMP data is typically mapped to the Alerts data model.

Application

When your Splunk deployment is ingesting SNMP data, you can use it to accomplish security observability use cases.

- Recovering lost visibility of IT infrastructure

Sources

Guidance for onboarding data can be found in the Splunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud).


The information provided in Splunk Lantern is intended for informational and educational purposes only. All information is provided in good faith, however, Splunk disclaims any and all representations and warranties, express and implied, regarding the information provided, including without limitation any warranties and representations regarding the completeness, adequacy or accuracy of the information. You agree to take full responsibility for the results arising from the use of the information provided.