CISCO Meraki Integrations

Introduction

Cisco Meraki offers a centralized cloud management platform for all Meraki devices such as MX Security Appliances, MR Access Points and so on. Its out-of-band cloud architecture creates secure, scalable, and easy-to-deploy networks that can be managed from anywhere. This can be done from almost any device using web-based Meraki Dashboard and Meraki Mobile App. Each Meraki network generates its own events.

Assumptions

The procedures described in Section 3 assumes that a Log Collector has already been setup.

Compatibility

A syslog server can be configured to store messages for reporting purposes from MX Security Appliances, MR Access Points, and MS switches. This package collects events from the configured syslog server. The integration supports collection of events from "MX Security Appliances" and "MR Access Points". The "MS Switch" events are not recognized.

Requirements

Cisco Meraki Dashboard Configuration

SYSLOG

Cisco Meraki dashboard can be used to configure one or more syslog servers and Meraki message types to be sent to the syslog servers. Refer to Syslog Server Overview and Configuration page for more information on how to configure syslog server on Cisco Meraki.

API ENDPOINT (WEBHOOKS)

Cisco Meraki dashboard can be used to configure Meraki webhooks. Refer to the Webhooks Dashboard Setup section.

Configure the Cisco Meraki integration

SYSLOG

Depending on the syslog server setup in your environment check one/more of the following options "Collect syslog from Cisco Meraki via UDP", "Collect syslog from Cisco Meraki via TCP", "Collect syslog from Cisco Meraki via file".

Enter the values for syslog host and port OR file path based on the chosen configuration options.

API Endpoint (Webhooks)

Check the option "Collect events from Cisco Meraki via Webhooks" option.

1. Enter values for "Listen Address", "Listen Port" and "Webhook path" to form the endpoint URL. Make note of the Endpoint URL https://{AGENT_ADDRESS}:8686/meraki/events.

2. Enter value for "Secret value". This must match the "Shared Secret" value entered when configuring the webhook from Meraki cloud.

3. Enter values for "TLS". Cisco Meraki requires that the webhook accept requests over HTTPS. So you must either configure the integration with a valid TLS certificate or use a reverse proxy in front of the integration.

Log Events

Enable to collect Cisco Meraki log events for all the applications configured for the chosen log stream.

Logs

Syslog

The cisco_meraki.log dataset provides events from the configured syslog server. All Cisco Meraki syslog specific fields are available in the cisco_meraki.log field group.

API Endpoint (Webhooks)

Cisco Meraki Integration Procedures

Please provide the following information to CyTech:

1. Collect syslog from Cisco Meraki via UDP

- Listen Address - The bind address to listen for UDP connections. Set to 0.0.0.0 to bind to all available interfaces.
- Listen Port - The UDP port number to listen on.

2. Collect syslog from Cisco Meraki via TCP

- Listen Address - The bind address to listen for TCP connections. Set to 0.0.0.0 to bind to all available interfaces.
- Listen Port - The UDP port number to listen on.

3. Collect syslog from Cisco Meraki via file

- Paths

4. Collect syslog from Cisco Meraki via Webhooks

- Listen Address - Bind address for the listener. Use 0.0.0.0 to listen on all interfaces.
- Listen Port

Revision #3
Created 23 April 2024 11:03:28
Updated 19 June 2024 06:54:01