NG SIEM - CISCO Meraki Integration

Cisco Meraki provides a centralized cloud management platform for devices like MX Security Appliances, MR Access Points, and more. Its cloud-based architecture enables secure, scalable networks manageable from anywhere via the Meraki Dashboard or Mobile App. Each Meraki network generates events that can be collected and analyzed.

Integration Overview

This integration supports event collection through:

- **Syslog** messages from Meraki devices
- **API Reporting Webhooks** via the Meraki cloud

Events can be searched, observed, and visualized.

Compatibility

- Supports event collection from **MX Security Appliances** and **MR Access Points** via syslog.
- **MS Switch** events are **not supported** and will not be recognized.

Cisco Meraki Dashboard Configuration

Syslog Setup:
Configure one or more syslog servers and specify Meraki message types to send to those servers.

For details, refer to the **Syslog Server Overview and Configuration guide**.

API Endpoint (Webhooks):

Configure Meraki webhooks from the dashboard. See the **Webhooks Dashboard Setup** for detailed instructions.

Configuring the Cisco Meraki Integration

Syslog Collection:

- Select one or more of these options based on your syslog server setup:
  - Collect syslog via **UDP**
  - Collect syslog via **TCP**
  - Collect syslog from a **file**
- Enter the appropriate **Syslog Host**, **Port**, or **File Path** based on your selection.

API Webhooks Collection:

- Enable **Collect events from Cisco Meraki via Webhooks**.
- Enter the following values to configure the webhook listener endpoint:
  - **Listen Address**
  - **Listen Port**
  - **Webhook Path**
- The endpoint URL will be: `https://{AGENT_ADDRESS}:8686/meraki/events`
- Enter the **Secret Value** matching the “Shared Secret” set in your Meraki webhook configuration.
- Provide **TLS configuration**: Meraki requires HTTPS for webhook endpoints, so configure a valid TLS certificate or use a reverse proxy with HTTPS in front of the integration.

Log Events

Enable this option to collect Cisco Meraki log events across all applications configured for the selected log stream.

Logs Dataset

- The `cisco_meraki.log` dataset contains events collected from the configured syslog server.
- All Cisco Meraki specific syslog fields are available under the `cisco_meraki.log` field group for detailed analysis.

*If you need further assistance, kindly contact **support@cytechint.com** for prompt assistance and guidance.*

Revision #8
Created 23 September 2025 08:08:30 by Richmond Abella
Updated 26 November 2025 05:33:08