NG SIEM - CISCO Secure Endpoint Integration

Introduction

Cisco **Secure Endpoint** is a cloud-delivered, advanced **endpoint detection and response (EDR)** solution. It provides visibility and protection across multiple control points, enabling organizations to rapidly detect, contain, and remediate advanced threats.

Assumptions

The procedures in this guide assume that a **Log Collector** has already been set up.

Requirements

This integration is designed for collecting **Cisco Secure Endpoint logs**.

Supported Dataset

- **event dataset** → Supports Cisco Secure Endpoint **event logs**, either:
  - Received over **syslog**
  - Read from a **file**

Generating Client ID and API Key

To collect logs via the **Secure Endpoint API**, you must first generate API credentials:

1. Log in to your **AMP for Endpoints Console**.
2. Navigate to **Accounts > Organization Settings**.
3. Under **Features**, click **Configure API Credentials**.
4. Generate and copy the **Client ID** and **Secure API Key**.

> **Important:** You can only copy your **API Key** at the time of creation. It cannot be retrieved later. Store it securely.

Secure Endpoint Logs

- The **event dataset** collects Cisco Secure Endpoint event logs.

Secure Endpoint API Capabilities

The **Secure Endpoint API** can be used to retrieve and manage detailed information, including:

- Generate a list of **organizations** a user has access to.
- Generate a list of **policies** for a specified organization.
- Retrieve detailed information about a specific policy, such as:
  - General policy data
  - Associated network control lists
  - Associated computers
  - Associated groups
  - Proxy settings
  - Policy XML
- Generate a list of all **policy types** and supported **operating systems** for an organization.

Top Use Cases

- **Reporting:** Generate reports on policy settings across an organization.
- **Inspection:** Review a particular policy's detailed settings.
- **Policy Auditing:** Query for policies that match specific criteria to determine which should be updated.

API Response Format

The Secure Endpoint API provides responses in three key objects:

- **Data** → Requested content.
- **Meta** → Metadata describing the request/response.
- **Errors** → Error details if the request fails.

> To enable log collection from the Cisco Secure Endpoint API, provide the following information to **CyTech Support**:

- **Client ID** → Cisco Secure Endpoint Client ID
- **API Key** → Cisco Secure Endpoint API Key

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

Revision #2
Created 23 September 2025 08:08:50 by Richmond Abella
Updated 3 October 2025 13:42:41 by Richmond Abella