NG SIEM - CISCO Umbrella Integration

Introduction

Cisco Umbrella is a cloud-delivered security platform that provides an additional layer of defense against malicious threats on the internet using Cisco’s threat intelligence. It helps block access to:

- **Malware**
- **Adware**
- **Botnets**
- **Phishing attacks**
- **Known malicious websites**

Assumptions

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

Prerequisites

- Full Admin access to Cisco Umbrella to create and manage Umbrella API keys.
- Umbrella API KeyAdmin access (if managing API key scopes and expirations).

Requirements

This integration supports log ingestion from Cisco Umbrella. Data is collected from:

- AWS S3 buckets using an SQS notification queue
- Cisco-managed S3 buckets without SQS

Supported Dataset

- log dataset: Collects Cisco Umbrella logs.

Umbrella Logs

When using Cisco-managed S3 buckets without SQS:

- Load balancing across multiple agents is not supported.
- A single agent must be configured to poll the S3 bucket.
- Vertical scaling can be applied by configuring the number of workers.

The log dataset is responsible for collecting all Cisco Umbrella logs.

Advantages of the Umbrella API Integration

The Umbrella API introduces several improvements over older versions (v1 and Reporting v2 APIs):

- Intuitive base URI
- API paths defined by top-level scopes
- Granular, intent-based API key scopes
- API key expiration support
- Updated API administration dashboard
- Programmatic API key administration
- Authentication & authorization via OAuth 2.0 client credentials flow
- Portable, programmable API interface for integrations

Before sending requests to the Umbrella API, create Umbrella API credentials and generate an access token.

More details: **Cisco Umbrella API Authentication**

Authentication

- The Umbrella API provides a **REST interface**.
- Supports **OAuth 2.0 client credentials flow**.

Steps:

1. Log in to Umbrella at: **https://dashboard.umbrella.com**
2. Create a new **API Key (ID + Secret)**.
   - Keys can only be copied once at creation.
   - Lost secrets cannot be retrieved.
3. Generate an **API Access Token** using your credentials.

> **Important:** API keys, passwords, and tokens grant access to private customer data. **Never share them** with external users or organizations.

Managing Umbrella API Keys

Create a New API Key

1. Navigate to **Admin > API Keys**
   - For MSP/MSSP: **Console Settings > API Keys**
2. Click **Add Key**.

3. Enter a **Name** (≤256 characters) and optional **Description**.
4. Select **Scopes** (Read-Only or Read/Write).
5. Configure an **Expiry Date** (or select *Never Expire*).
6. (Optional) Add **Network Restrictions** (up to 10 public IPs or CIDRs).
7. Click **Create Key** → Copy and save **Key + Secret**.

Refresh an API Key

1. Go to **Admin > API Keys**.
2. Expand the target key → Click **Refresh Key**.
3. Copy and save the new **Key + Secret**.

Update an API Key

1. Expand an existing key.
2. Update **Name, Description, Scopes, Expiry, or Network Restrictions**.
3. Click **Save**.

> To integrate Cisco Umbrella logs into AQUILA, provide the following details to **CyTech Support**:

- **Queue URL**
  - AWS SQS queue URL where messages will be received.
  - For Cisco-managed S3 without SQS, use **Bucket ARN** instead.
- **Bucket ARN**
  - Required for Cisco-managed S3.
  - Example: `arn:aws:s3:::cisco-managed-eu-central-1`
  - **List of Cisco-managed S3 buckets**
- **Bucket Region**
  - The AWS region where the bucket is located.
- **Bucket List Prefix**
  - The root folder of the S3 bucket to be monitored (visible in the S3 UI).
  - Example: `1235_654vcasd23431e5dd6f7fsad457sdf1fd5`
- **Number of Workers**
  - Number of workers to process S3 objects (min = 1).
- **Bucket List Interval**
  - Time interval for polling the S3 bucket. Default = 120s.
- **Access Key ID**
- **Secret Access Key**

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

Revision #4
Created 23 September 2025 08:08:00 by Richmond Abella
Updated 3 October 2025 13:33:52 by Richmond Abella