CISCO Umbrella Integrations

Introduction

Cisco Umbrella is a cloud security platform that provides an additional line of defense against malicious software and threats on the internet by using threat intelligence. That intelligence helps prevent adware, malware, botnets, phishing attacks, and other known bad Websites from being accessed.

Assumptions

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

Prerequisites

- You must have Full Admin access to Umbrella to create and manage Umbrella API keys or Umbrella KeyAdmin API keys.

Requirements

This integration is for Cisco Umbrella. It includes the following datasets for receiving logs from an AWS S3 bucket using an SQS notification queue and Cisco Managed S3 bucket without SQS:

- log dataset: supports Cisco Umbrella logs.

Logs

Umbrella

When using Cisco Managed S3 buckets that does not use SQS there is no load balancing possibilities for multiple agents, a single agent should be configured to poll the S3 bucket for new and updated files, and the number of workers can be configured to scale vertically.

The log dataset collects Cisco Umbrella logs.

Advantages of Integrating with the Umbrella API

The Umbrella API features a number of improvements over the Umbrella v1 APIs and the Umbrella Reporting v2 API.

- Intuitive base URI
- API paths defined by top-level scopes
- Intent-based, granular API key scopes
- API key expiration
- Updated API key administration dashboard views
- Programmatic API key administration
- API authentication and authorization supported by OAuth 2.0 client credentials flow
- Portable, programmable API interface for client integrations

Before you send a request to the Umbrella API, you must create new Umbrella API credentials and generate an API access token. For more information, see Umbrella API Authentication.

Authentication

The Umbrella API provides a standard REST interface and supports the OAuth 2.0 client credentials flow. To get started, log in to Umbrella and create an Umbrella API key. Then, use your API credentials to generate an API access token.

Note: API keys, passwords, secrets, and tokens allow access to your private customer data. You should never share your credentials with another user or organization.

Log in to Umbrella

- Log in to Umbrella with the following URL: https://dashboard.umbrella.com

- You can find your username after Admin in the navigation tree. Confirm that your organization appears under your username.

Cisco Secure Endpoint Integration Procedures

Please provide the following information to CyTech:

Collect logs from the Cisco Umbrella

1. Queue URL - URL of the AWS SQS queue that messages will be received from. For Cisco Managed S3 buckets or S3 without SQS, use Bucket ARN.

2. Bucket ARN - Required for Cisco Managed S3. If the S3 bucket does not use SQS, this is the address for the S3 bucket, one example is arn:aws:s3:::cisco-managed-eu-central-1

   For a list of Cisco Managed buckets, please see https://docs.umbrella.com/mssp-deployment/docs/enable-logging-to-a-cisco-managed-s3-bucket.

3. Bucket Region - Required for Cisco Managed S3. The region the bucket is located in.

4. Bucket List Prefix - Required for Cisco Managed S3. This sets the root folder of the S3 bucket that should be monitored, found in the S3 Web UI. Example value: 1235_654vcasd23431e5dd6f7fsad457sdf1fd5.

5. Number of Workers - Required for Cisco Managed S3. Number of workers that will process the S3 objects listed. Minimum is 1.

6. Bucket List Interval - Time interval for polling listing of the S3 bucket. Defaults to 120s.

7. Access Key ID

8. Secret Access Key

9. Preserve original event

Revision #2
Created 23 April 2024 11:16:32
Updated 19 June 2024 06:54:01