CISCO Secure Endpoint Integrations

Introduction

Secure Endpoint offers cloud-delivered, advanced endpoint detection and response across multidomain control points to rapidly detect, contain, and remediate advanced threats.

Assumptions

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

Requirements

This integration is for Cisco Secure Endpoint logs. It includes the following datasets for receiving logs over syslog or read from a file:

- event dataset: supports Cisco Secure Endpoint Event logs.

Logs

Secure Endpoint

The event dataset collects Cisco Secure Endpoint logs.

What can the Secure Endpoint API be used for?

- Generate a list of organizations a user has access to
- Generate a list of policies for a specified organization
- Generate specific information about a specified policy such as:
    - General policy data
    - Associated network control lists
    - Associated computers
    - Associated groups

    - Proxy settings
    - Policy XML

- Generate all policy types and operating systems available for a specified organization

Top Use Cases

- Generating reports on policy settings across an organization
- Inspecting a particular policy's settings
- Querying to find policies matching certain criteria in order to detect which policies should be edited

Response Format

- Data
- Meta
- Errors

Cisco Secure Endpoint Integration Procedures

Please provide the following information to CyTech:

Collect logs from the Cisco Secure Endpoint API.

1. Client ID - Cisco Secure Endpoint Client ID

2. API Key - Cisco Secure Endpoint API Key

Revision #2
Created 23 April 2024 11:11:17
Updated 19 June 2024 06:54:01