Netskope Integration Guide (v1.0)

Prepared by: Bowei Chi, SecLytics
Date: 2023-08-22

Table of Contents

Overview

The intent of this document is to outline the steps and workflows for integration of the SecLytics threat feeds into Netskope CTE.

Services Installation

Prerequisites

Seclytics Account

Please request an organizational account by contacting support@seclytics.com. Seclytics will set up your organization. Minimum one admin user's email is required to enable the integration.

Netskope CTE Admin

Access to Netskope CTE portal with the ability to install and configure plugin is required.

Installation & Configuration Steps

Obtaining Seclytics Access Token

Login to the Seclytics Dashboard @ https://dashboard.seclytics.com/

1. Click on the left panel: "**Integrations**" > "**New Integration**".
2. Click under category: "**Cloud**".
3. Click on **"+Install**" on the **Netskope** tile.
4. Under "**Configure**", scroll down to **step 9** to find the access token string in red highlight.
5. Make note of the access token string to be used in Netskope CTE portal's plugin configuration.

Netskope's Seclytics CTE plugin configuration

Login to Netskope CTE admin portal

1. Click on **Threat Exchange**
2. Click on **Plugins**
3. Search for **Seclytics** in the search field and click on the resulting plugin.
4. Input Configuration Name: **Seclytics URL and CIDR**
5. Input Sync Interval: **360 (minutes)**
6. Click **Next**
7. Under **Default Endpoint Threat Data Types,** select **URL** and **CIDR Blocks**
8. Under Access Token, paste the Seclytics access token from the prior step.
9. (Optional) Select **High** for severity of IP indicators if you experience too many hits. **Keep it blank for the most coverage.**
10. Click **Save**
11. Threat data will populate on the next sync interval defined in step 5.