SLASHNEXT

USER GUIDE V1.0

SlashNext Threat Intelligence Guide for ThreatConnect

TABLE OF CONTENTS

1 | INTRODUCTION

This document outlines the process to integrate SlashNext Threat Intelligence feeds into the ThreatConnect platform and provides details on how to efficiently use the integrated Threat Intelligence to get a specific list of Indicators of Compromise (IoCs).

SlashNext Threat Intelligence provides three types of feeds as per the corresponding type of IoCs which are listed below:

1. SlashNext Intel – Phishing IPs as the name indicates contains IPv4 IoCs and are represented in ThreatConnect under **Address** type of Indicators.
2. SlashNext Intel – Phishing FQDNs as the name indicates contains domain IoCs and are represented under **Host** type of Indicators.
3. SlashNext Intel – Phishing Wildcard URLs as the name indicates contains wildcard URL IoCs and are also represented under **URL** type of Indicators.

All the IoCs within SlashNext threat feeds have four attributes which are also updated in the ThreatConnect Platform to facilitate the filtering of feed to get a list of more desired IoCs as per threat nature or as per usage which are as follows:

1. **SlashNext Threat Type** as the name indicates contains the broad threat nature posed by the IoC.
2. **SlashNext Threat Name** as the name indicates contains the exact threat name posed by the IoC.
3. **First Seen** as the name indicates contains the timestamp when the IoC was first observed to be active threat.
4. **Last Seen** as the name indicates contains the timestamp when the IoC was last observed to be active threat.

2 | CONFIGURATION

The following section provides details on how to configure **SlashNext Phishing Threat Intelligence** app developed for the ThreatConnect Platform, as a job to download and ingest IoCs from SlashNext threat feeds into the platform.

2.1 | REQUIREMENT

The above requirements must be met to ingest SlashNext feeds into the ThreatConnect Platform:

1. Access to ThreatConnect instance
2. At least one ThreatConnect API user (See Creating User Accounts)
3. SlashNext API Key provisioned by SlashNext to authenticate requests to SlashNext cloud
4. **SlashNext Phishing Threat Intelligence** app installed in ThreatConnect Instance. (See **App Installation** section)
5. SlashNext Threat feed attributes properly configured in your ThreatConnect instance (See **Attributes Configuration** section)

2.2 | APP INSTALLATION

SlashNext Phishing Threat Intelligence app for ThreatConnect is available on Github at: Github Link. Download the app package with **tcx** extension and install it in your instance. To install the app in your ThreatConnect instance, refer to the ThreatConnect System Administration Guide (Install an App and Feed Deployer) for more information or contact your ThreatConnect Customer Success Engineer.

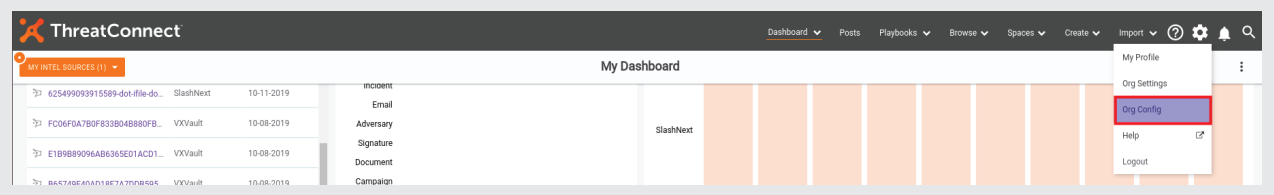
Also, download the **attributes.json** file in the Github repository which is required for attributes configuration step (See **Attributes Configuration**)

2.3 | ATTRIBUTES CONFIGURATION

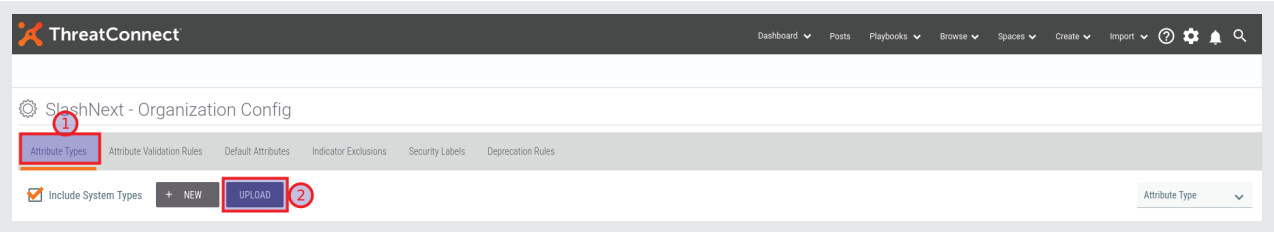
> **Note**
> This step is not required for customers who use Feed Deployer as it is automatically performed by the Feed Deployer Wizard.

As mentioned above, indicators ingested in the ThreatConnect Platform have four types of attributes to represent different characteristics of the threat posed by it. All of these attribute types must be available in your ThreatConnect instance to be able to display and update them accordingly. By default, in any ThreatConnect instance, only First Seen and Last Seen attribute types are present and the rest (**SlashNext Threat Type** and **SlashNext Threat Name**) have to be imported by the users themselves. In order to import these attributes in your instance, follow the steps below:

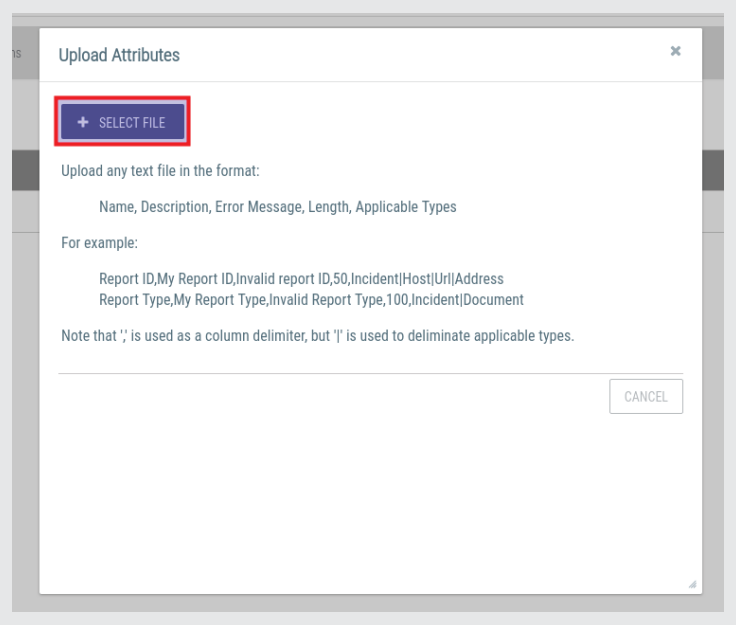
1. Login to your ThreatConnect instance and hover your mouse cursor over the gear icon on the top menu-bar. From the drop-down menu, Click on **Org Config** (highlighted by the red rectangle below) to go to your Organization Configuration page.



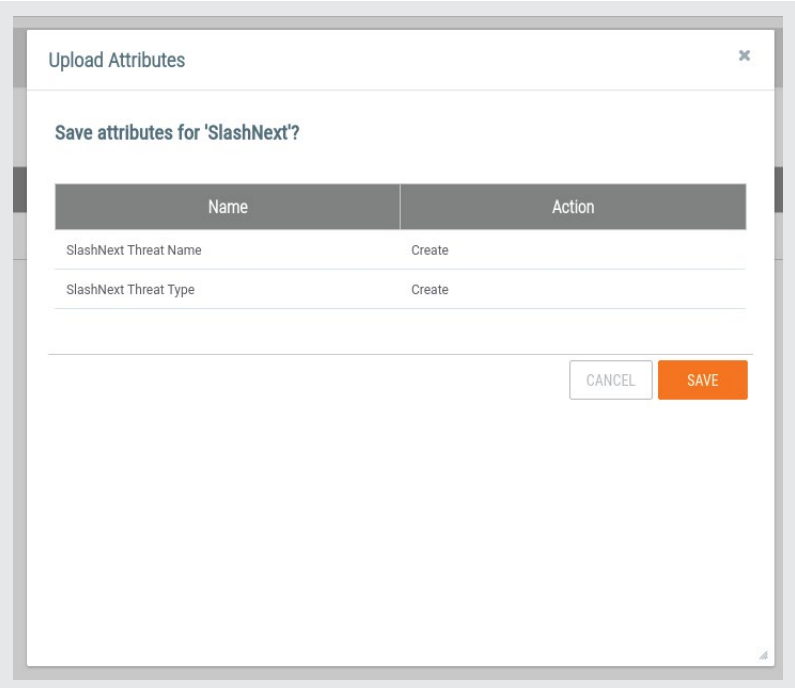
2. Click on **Attribute Types** tab on the Organization Config page, which is selected by default. Also, click on the **Upload** button and the **Upload Attributes** dialog box will appear.



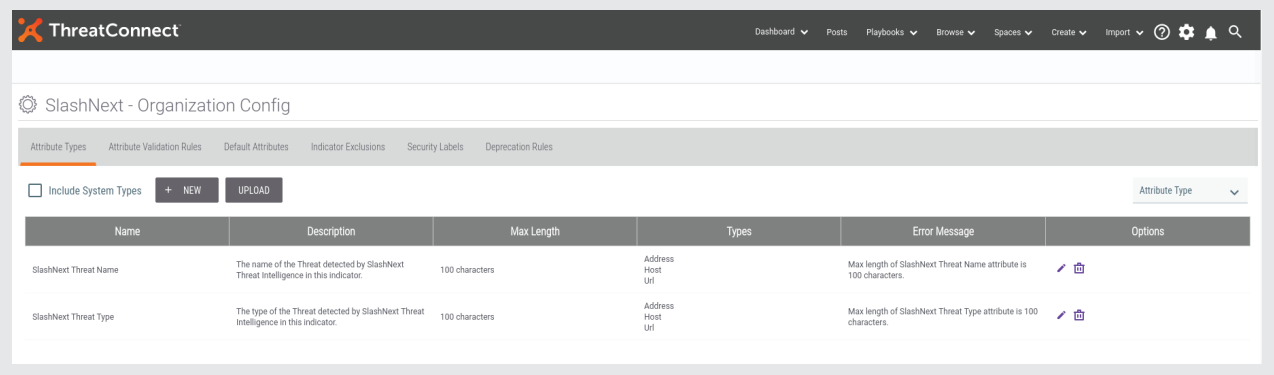
3. On the **Upload Attributes** dialog box, click on + **SELECT FILE** button shown below and upload the file **attributes.json** (present in the Github Repository), that contains the configuration metadata of the required attributes.



4. The dialog box will then show you the attributes to be uploaded and ask for confirmation. Click on **Save** button to confirm.



5. Once the file is uploaded, the attributes along with their corresponding metadata will start appearing in your instance as shown below. The attributes configuration step is completed at this stage.

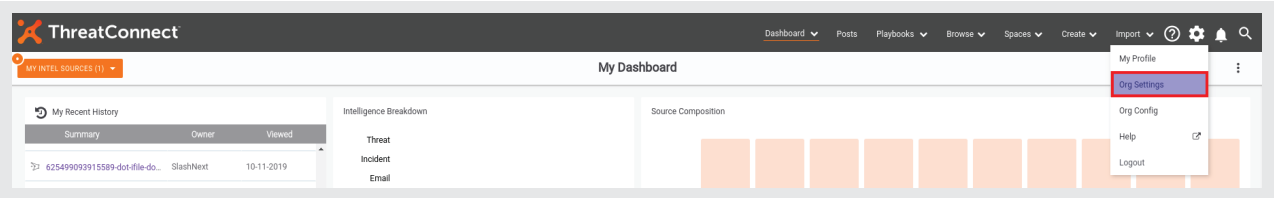


2.4 | THREATCONNECT JOB CONFIGURATION

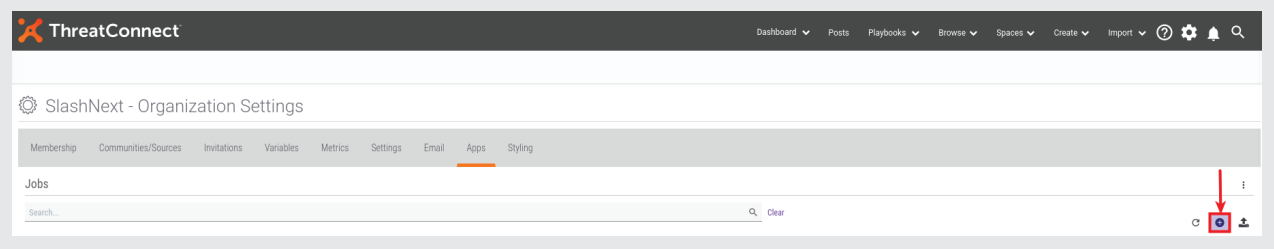
> **Note**
> This step is not required for customers who use Feed Deployer as it is automatically performed by the Feed Deployer Wizard.

The ThreatConnect Platform provides the ability for customers to schedule applications as jobs, specifically known as Job apps, that can be run at configured intervals. SlashNext, Inc has developed a Job app for ThreatConnect customers by the name of **SlashNext Phishing Threat Intelligence** that handles the complete process of downloading and ingesting the threat feed into the ThreatConnect Platform. In order to configure the SlashNext threat feed ingestion job app, follow the steps mentioned below:

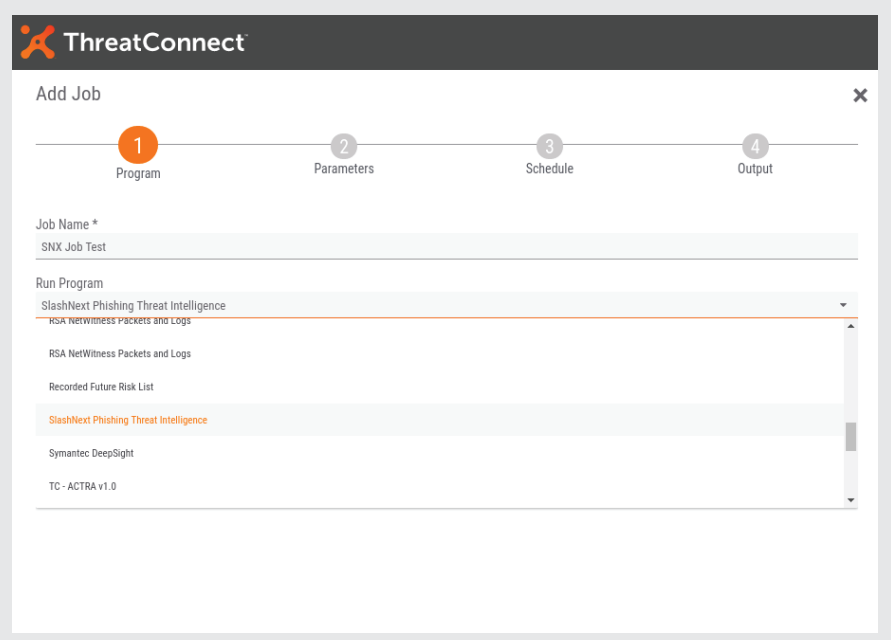
1. Hover your mouse cursor over the gear icon present on the top menu-bar. From the drop-down menu, Click on **Org Settings** to go to your Organization Settings page.



2. Click on the **Apps** tab to configure **Jobs**. Also, click on the small + button (shown in the image below) to show the **Add Job** panel.

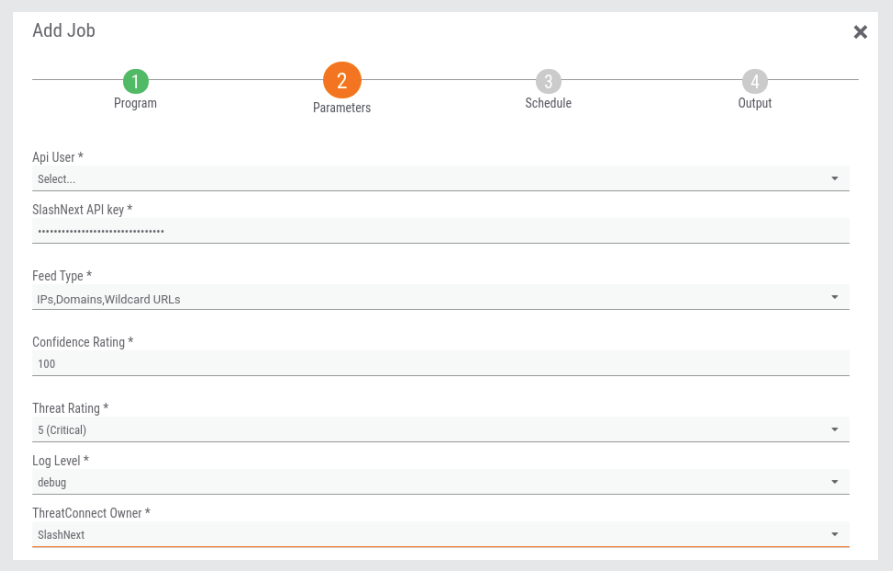


3. In the **Add Job** panel, choose a suitable name for your Job in the **Job Name** option. Also select **SlashNext Phishing Threat Intelligence** from the **Run Program** drop-down list.



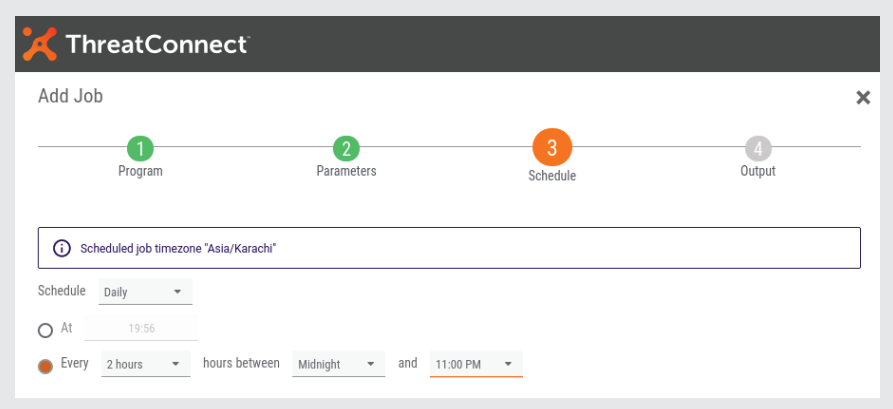
Note
If you cannot see **SlashNext Phishing Threat Intelligence** in the drop-down list, please follow the **App Installation** step above or contact your Customer Success Engineer.

4. Click **Next** to configure the parameters of the Job app then select a suitable **Api User** configured in your instance. For the **SlashNext API Key** parameter, insert the 32 character API key provided to you by SlashNext or contact at support@slashnext.com if you do not have a valid API key. Under the **Feed Type** parameter, select the type of feeds from the multi-choice drop-down menu, that you want to ingest in your instance. Optionally, you can also set the **Confidence Rating** and **Threat Rating** parameter values for all the indicators ingested from SlashNext feeds other than the default values. Select the appropriate **Log Level** and finally, choose an owner for the ingested feed from the **ThreatConnect Owner** drop-down menu.

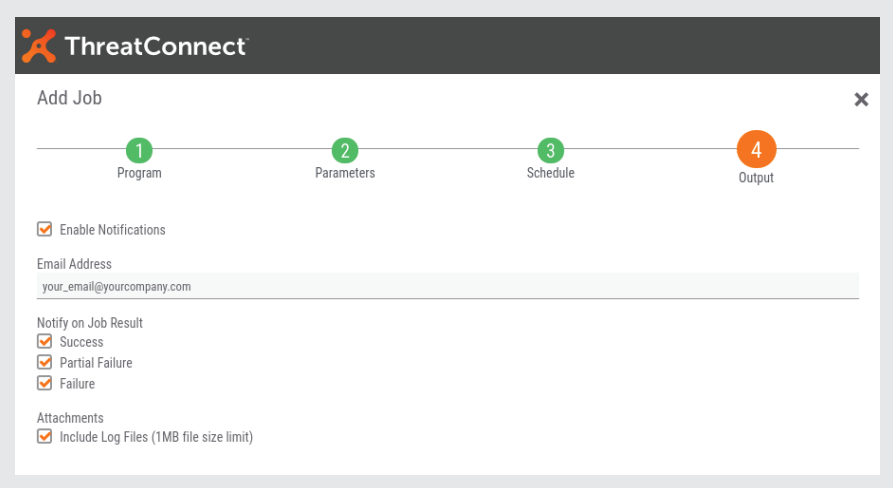


5. Click **Next** button to configure the schedule of running the job app, at which the feed will be ingested in your instance. Select the suitable period from the **Schedule** drop-down menu.

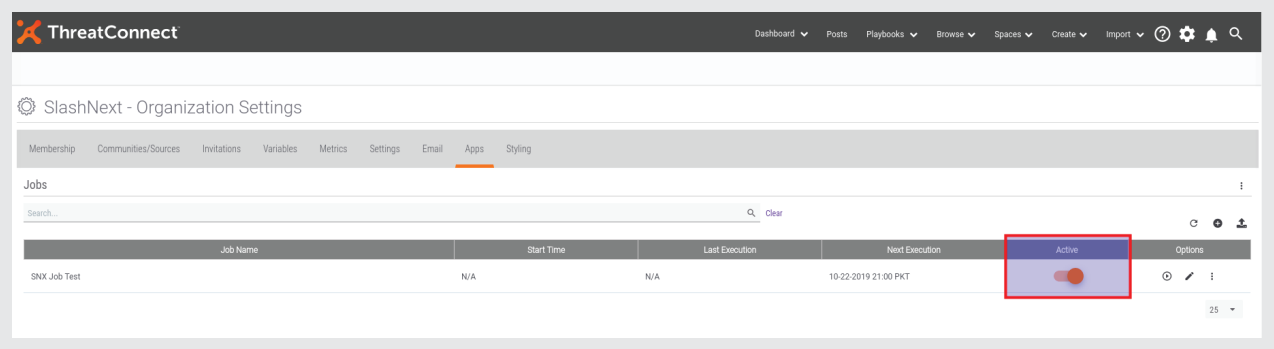
Note
SlashNext recommends that the job is executed after every two hour interval daily, as set in the figure below, for best syncing with the latest feed.



6. Finally, click **Next** to setup the **Output** of the job app. Optionally, you can check the **Enable Notifications** checkbox to enable email notifications upon completion of the Job and provide the receiving **Email Address**. Under the **Notify on Job Result** option, check all the required scenarios at which email notifications are desired to be received. Also, click on **Include Log Files** checkbox under the **Attachments** option to receive job execution logs as attachments in the email notifications.



7. Click on **Save** button to save the job configuration. At this point, the job app is configured but is currently not active for execution. Click on the toggle button under **Active** as shown below to activate the job for running. The job configuration step is now complete.



3 | INDICATOR DEPRECATION CONFIGURATION

From time to time, SlashNext retires indicators in its threat feed that it estimates are, no longer malicious and pose any significant threat. These indicators previously ingested into the ThreatConnect Platform should also be deleted accordingly to avoid false-positives. ThreatConnect provides the ability for users to configure an indicator deprecation policy to allow ThreatConnect indicators to drop in confidence rating if their confidence rating is not being maintained and updated. Once the indicator rating reaches a minimum value (i.e. 0%), it can either be set to inactive or delete. To configure an indicator deprecation policy depending upon the type of your ThreatConnect instance, please refer to the detailed knowledge-base article from ThreatConnect: CONFIGURING INDICATOR CONFIDENCE DEPRECATION (See sections **Configuring Indicator Confidence Deprecation for an Organization** and **Configuring Indicator Confidence Deprecation for a Community or Source**)

The recommended indicator deprecation rule settings for SlashNext threat feed are as follows:

- **Action at Minimum** selected to be **Delete** so that indicators are deleted as soon as they reach minimum confidence
- **Percentage** checkbox checked which means that indicator confidence will be dropped as a percent of its previous value
- **Confidence** amount set to **100** so that 100% of an indicator's confidence is dropped
- **Interval** value set to **1 day** which is the period after which the confidence will be dropped
- **Recurring** checkbox also selected so that deprecation is performed on a recurring basis

In simple words the recommended deprecation rule can be stated as, **"After every day, drop the confidence of each indicator by 100% of its previous value and when any indicator's confidence reaches the minimum value, delete it from ThreatConnect".**

4 | LIST SPECIFIC IOCS

ThreatConnect provides the ability to filter and display indicators from a number of sources. We can filter different types of indicators from the feed by applying a filter on either indicator tags or attributes.

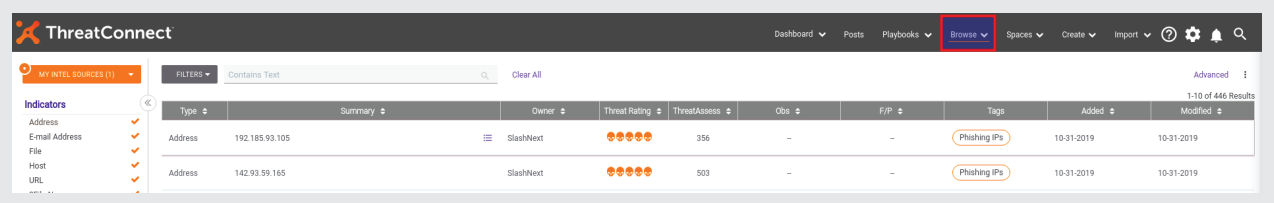
4.1 | FILTER FEED TYPES

In order to filter indicators by their types, we can apply a filter on indicator tags. SlashNext threat feed indicators can have three types of tags:

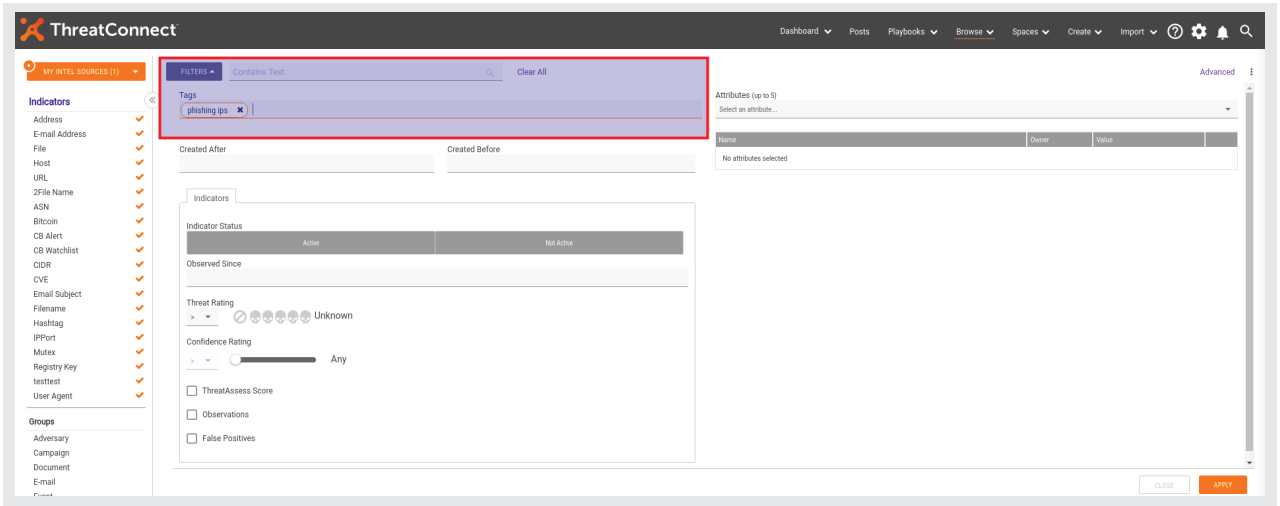
FEED TYPE	INDICATORS TYPE	TAG
SlashNext Intel – Phishing IPs	Address	"Phishing-IPs"
SlashNext Intel – Phishing FQDNs	Host	"Phishing-FQDNs"
SlashNext Intel – Phishing Wildcard URLs	URL	"Phishing-Wildcard-URLs"

To filter all the indicators with one of these tags, follow the steps below:

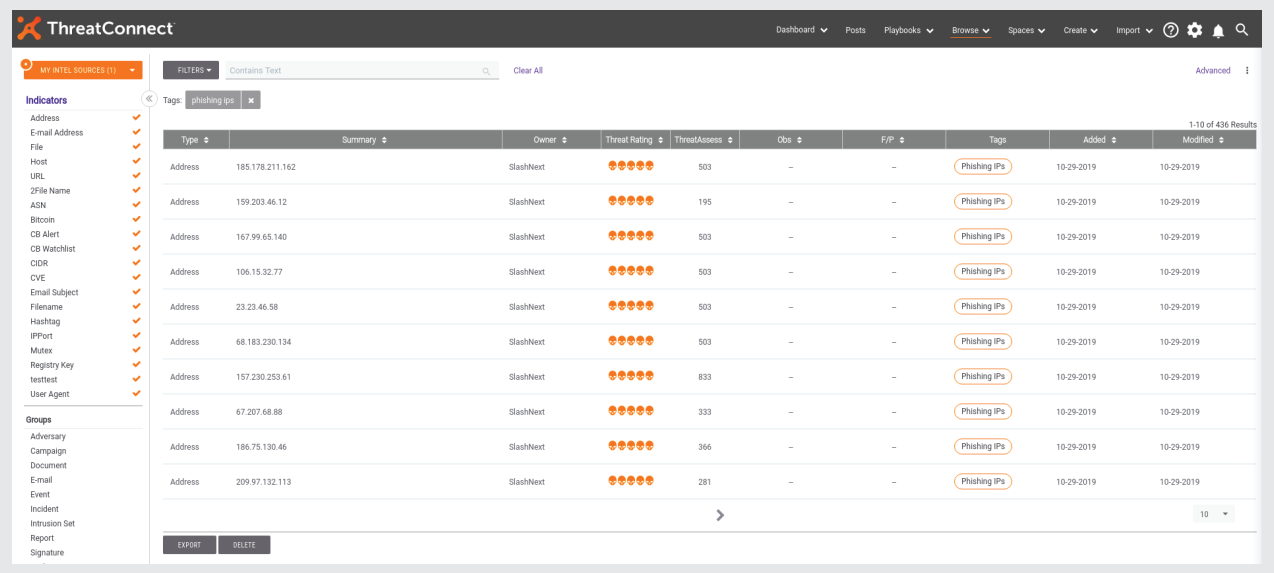
1. Click on **Browse** from the top menu-bar to go to the ThreatConnect Browse page that displays indicators from all the sources.



2. Click on **FILTERS** button shown in the figure below to expand the Filters panel. In the **Tags** textbox, write **phishing** and a drop-down auto completion list will appear with all SlashNext tags. Select the required tag according to the table given above. Let's filter all the indicators which have a tag of **"Phishing-IPs"** representing Phishing IPs in SlashNext feed.



3. The **Browse** page will then start showing all the indicators with **"Phishing-IPs"** tag as shown in the figure below:



4.2 | FILTER ATTRIBUTES

Each indicator in the SlashNext feeds has the following four attributes:

1. SlashNext Threat Type
2. SlashNext Threat Name
3. First Seen (First Seen time)
4. Last Seen (Last Seen time)

SlashNext Threat Type attribute has one of the following values:

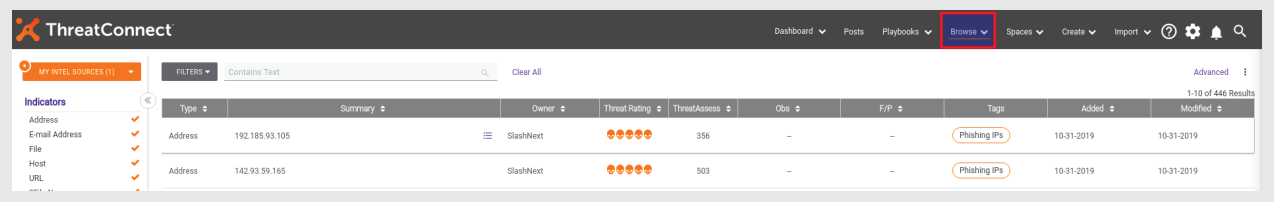
1. Phishing & Social Engineering
2. Malware & Exploit
3. Callback/C2s

SlashNext Threat Name attribute can have the following values:

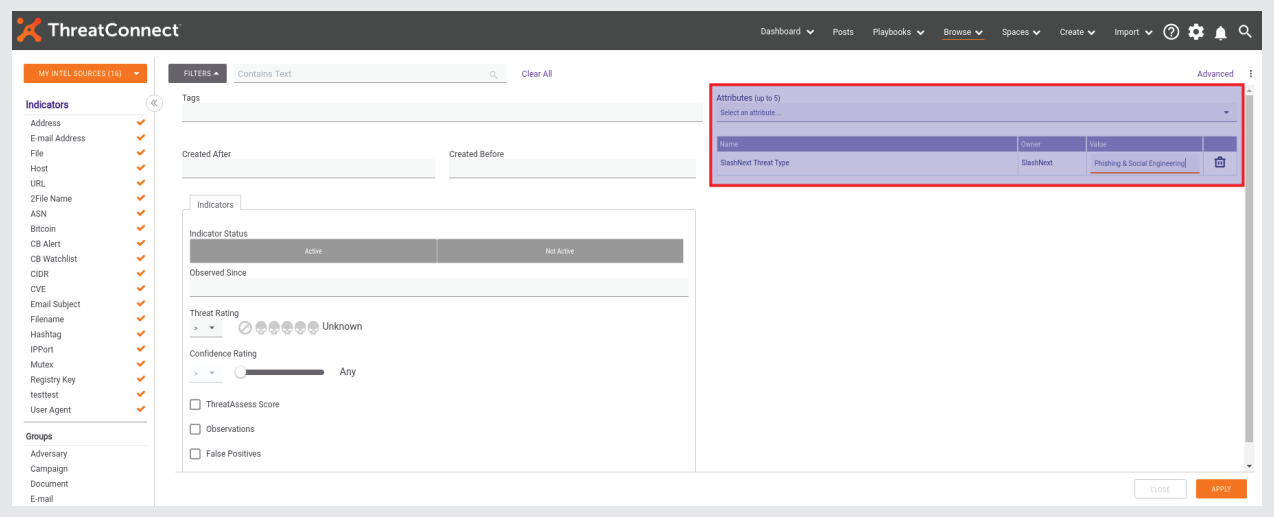
1. Fake Login Page
2. Scareware
3. Rogue Software
4. Internet Scam
5. Exploit:Win32/MSDocs
6. BadObject:Multi/RogueBinary
7. BadObject:Win32/InstallCore
8. Trojan:OSX/SearchJack
9. Trojan:Win32/Hijacker
10. Trojan:Multi/RogueExtension
11. Trojan:Win32/Spigot
12. BankingTrojan:Win32/Zbot

Indicators in the ingested SlashNext threat feed can be filtered by any specific value of the above indicators. Let us demonstrate how to filter all the indicators with **SlashNext Threat Type** of **Phishing & Social Engineering**:

1. Click on **Browse** from the top menu-bar to go to the ThreatConnect Browse page that displays indicators from all the sources.



2. Click on **FILTERS** button shown in the figure below to expand the Filters panel. From the **Attributes** drop-down list select **SlashNext Threat Type** and it will appear below. Next to it, write the value in the **Value** textbox, against which you want to filter the indicators as shown below in the highlighted section:



3. All the indicators in the threat feed with **SlashNext Threat Type** attribute equal to **Phishing and Social Engineering** will now appear on the Browse page: