

ThreatSTOP Integration for ThreatConnect Version 1.0.4

This document describes the integration between ThreatSTOP and ThreatConnect.

Introduction	2
Features	2
Data Mapping	2
Policy Action	5
Exceptions	5
Browsing ThreatSTOP IOCs in the ThreatConnect Platform	5
Maximum Policy Size and Deprecation	5
Configuration	6
Requirements	6
Setup	6
Schedule setting	9
Configuration changes	9
Integration status	10
Threat Types	11
ThreatSTOP Support	11
Release notes	11

Introduction

ThreatSTOP is a security platform which aggregates Threat Intelligence from hundreds of sources to define custom policies loaded on Firewalls and DNS Servers to block malicious connections and DNS lookups.

The “**Active IOCs**” integration between ThreatSTOP and ThreatConnect automates the import of the IOCs from ThreatSTOP Policies into the ThreatConnect TIP. This provides users with the ability to:

Browse the IOCs in their current ThreatSTOP policies and view their meta data.
Leverage their ThreatSTOP Policies in ThreatConnect playbooks.

Features

The integration allows users of both platforms to select one or multiple ThreatSTOP policies and import their IOCs in the ThreatConnect Platform. The IOCs are imported hourly as ThreatSTOP policies are updated.

Data Mapping

Targets are ThreatSTOP's atomic building blocks for policies, typically grouping IOCs by the associated threat. Each IOC is imported with the following data:

ThreatSTOP Field	ThreatConnect Field	Description
Target name	Associated Intel	
Threat Type	Tags	The Threat Type associated with the target
Severity	Threat Rating	The ThreatSTOP severity score (0 to 5)
Confidence Level	Confidence Rating	The ThreatSTOP scale (1-5) is translated to a range from 20 to 100
First and Last Seen	First and Last Seen	The first and last time the IOC was in ThreatSTOP targets preset in the exported policies

ThreatSTOP Field	ThreatConnect Field	Description
N/A	Added	The first time the IOC was imported
N/A	Last Modified	The last time the IOC was imported


Example of IOCs imported from ThreatSTOP into the ThreatConnect Platform:



The screenshot shows the ThreatConnect web interface. The top navigation bar includes links for Dashboard, Workflow, Posts, Playbooks, Browse, Spaces, Create, Import, and a search icon. The left sidebar lists various indicators and groups. The main content area displays a table of indicators imported from ThreatSTOP.

Type	Summary	Owner	Version	Threat Rating	ThreatAssess	Cbs	F/P	Tags	Added	Modified
Address	125.186.73.24	ThreatStop Source	IPv4	513	--	--	Gen...	01-11-20...	01-15-20...	
Address	151.106.13.150	ThreatStop Source	IPv4	449	--	--	Gen...	01-11-20...	01-15-20...	
Address	109.73.39.195	ThreatStop Source	IPv4	513	--	--	Gen...	01-11-20...	01-15-20...	
Address	117.84.214.144	ThreatStop Source	IPv4	513	--	--	Gen...	01-11-20...	01-15-20...	
Address	134.119.213.127	ThreatStop Source	IPv4	440	--	--	Gen...	01-11-20...	01-15-20...	
Address	134.119.218.49	ThreatStop Source	IPv4	449	--	--	Gen...	01-11-20...	01-15-20...	
Address	100.1.117.74	ThreatStop Source	IPv4	513	--	--	Gen...	01-11-20...	01-15-20...	
Address	105.104.10.115	ThreatStop Source	IPv4	520	--	--	Gen...	01-11-20...	01-15-20...	
Address	115.22.73.96	ThreatStop Source	IPv4	513	--	--	Gen...	01-11-20...	01-15-20...	
Address	151.106.13.154	ThreatStop Source	IPv4	449	--	--	Gen...	01-11-20...	01-15-20...	


At the bottom of the table, there are buttons for 'EXPORT' and 'DELETE'. The interface also shows a search filter 'Contains Text' and a 'Clear All' button.


IOC Details:


 117.84.214.144

 Status set by 

Type	Owner	Added	Last Modified
Address	ThreatStop Source	01-11-2021	01-15-2021

ThreatAssess
 513 High
Recent False Positive Reported
Impacted by Recent Observations

Threat Rating
 Critical


Confidence Rating
 100% Confirmed

Tags
General


Attributes

Type	Last Modified	Value
First Seen	01-15-2021	2019-09-24T11:22:11Z
Last Seen	01-15-2021	2021-01-15T16:24:28Z

Associated Intel

Type	Owner	Date Added
 Threat TS Originated - Core Threats - IPs	ThreatStop Source	12-08-2020

Associated Indicators

Type	Owner	Date Added
 Address 100.1.117.74	ThreatStop Source	01-11-2021

IOCs are imported as one of three ThreatConnect IOC types:

- Addresses (v4 IP addresses).
- CIDR (v4 subnets).
- Host (FQDN and domains).

An IOC can be present in multiple ThreatSTOP Targets; the IOC will show meta data for each target. The highest severity and confidence scores across all targets are used.

Policy Action

For IP policies, the IOCs exported to the ThreatConnect Platform are the **Block** section of the policies; the **Allow** section is not exported. For RPZ policies, IOCs are exported for every RPZ action except **Passthru**.

Exceptions

The following elements of a ThreatSTOP policy are not imported into the ThreatConnect TIP:

ThreatSTOP IOCs for wildcard DNS domains (e.g. *.example.com).
ThreatSTOP targets with a severity score of 0 (used for whitelisting and Geographical targets). IP addresses and domains from User-defined lists.

Browsing ThreatSTOP IOCs in the ThreatConnect Platform

IOCs are displayed by following the Browse > Indicators menu and selecting Address, CDIR or Host. Types can be combined using the Indicators list in the left menu.

- If you are using ThreatConnect's shared environment, the IOCs imported are attached to a source named 'ThreatSTOP'. In a private instance (cloud or on-premise), the source name is set by the user during the installation.
- In the details tab of the IOC, the **Associated Intel** section will show the targets that the IOC is (or was) present in. You can click on each of the target to access a page with the description of the target and the list of IOCs in it.
- The associated indicators section lists the IOCs in the same ThreatSTOP target.
- The list of targets can be accessed by following **Browse > Groups > Threat**. The integration only includes targets present in the ThreatSTOP policy.

The list of Threat Types can be accessed from the **Tags** left menu of the **Browse IOC** page. Only Threat Types associated with IOCs in the policy are imported.

Maximum Policy Size and Deprecation

IOCs imported using the integration will be deleted according to the deprecation rules set for the ThreatSTOP source. Deprecation rules must be configured to avoid

reaching the maximum number of IOCs allowed in the ThreatConnect Platform (500,000 per source). If an IOC remains in the ThreatSTOP targets, it will be refreshed and its deprecation value reset. ThreatSTOP recommends deprecating the IOCs to be deprecated overnight days, i.e. deprecating IOCs by 100 points daily.

The integration module will stop importing IOCs if the combined size across the policies reaches 500,000. Users should consider this limit and the size of the ThreatSTOP policies they choose to import when customizing deprecation rule, so as to avoid reaching the limit.

Configuration

Requirements

ThreatSTOP accounts require two features to be enabled on the account:

- Custom policies
- ThreatConnect integration

Please contact support@threatstop.com if you wish to use the integration but your account doesn't have the required feature. The ThreatConnect Platform requires an API user to install the application.

Setup

The integration is configured into three steps: first selecting policies to import using the ThreatSTOP Portal, download the TCEX application and finally configuring the integration key in the ThreatConnect Platform.

- ThreatSTOP Portal
 - Login to your ThreatSTOP Account.
 - Browse to the Integrations > ThreatConnect page.
 - You will be presented with a list of your custom policies.
 - Click **Add** to add a policy to the list of policies to be imported. The policy must be a custom policy; pre-defined policies can't be exported.
 - It will take a few minutes (less than 5) for the policy to be available to ThreatConnect.
 - The **Integration Key** which is used in the next step is shown at the top of the page.

ThreatConnect Integration

This is where you will manage your integration with your ThreatConnect Module. You will be able to select policies to activate for integration and learn the status of your integration. For more information about implementing this feature, please see <https://docs.threatstop.com/threatconnect.html>.

Integration Key
(Click to toggle):

Currently Integrated Policies

These are the policies currently being generated for integration from ThreatSTOP into ThreatConnect

Show 10 entries
Showing 1 to 3 of 3 entries

Previous 1 Next

Policy Name	Policy Type	Policy Size	Last Import	Actions
policy4	DNS Defense	7629	Ok at 2020-12-08 16:50:17 UTC. Imported 3665 indicators	Remove
policy1	IP Defense	1921	Ok at 2020-12-08 16:49:58 UTC. Imported 1904 indicators	Remove
policy3	IP Defense	8717	Ok at 2020-12-08 16:50:25 UTC. Imported 8603 indicators	Remove

Previous 1 Next

Other Policies

These are your ThreatSTOP policies not currently being integrated with ThreatConnect

Show 10 entries
Showing 1 to 6 of 6 entries

Previous 1 Next

Policy Name	Policy Type	Policy Size	Actions
Policy2	DNS Defense	84016	Add
policy5	IP Defense	0	Add

- Download the application
 - Retrieve the TCEx file from ThreatConnect's GitHub repository: <https://github.com/ThreatConnect-Inc/threatconnect-jobs/tree/master/apps>
- ThreatConnect Dashboard
 - For general documentation about adding an application, please refer to the ThreatConnect System Administration Guide (Install an App). For more information, contact your ThreatConnect Customer Success representatives.
 - **Step 1:** enter the ThreatConnect Owner (ThreatStop source), API Key (retrieved from the ThreatSTOP Admin Portal) and log level (recommended value: info)

Edit Job ✕

1 2 3 4
Program Parameters Schedule Output

ThreatConnect Owner *
ThreatStop Source

ThreatSTOP Policy Token *
YOUR_API_KEY

Log Level *
info

CANCEL PREVIOUS NEXT

- **Step 2:** select how often the integration will run (i.e. check for new data and import it). The default value is every two hours.

Edit Job ✕

1 2 3 4
Program Parameters Schedule Output

ThreatConnect Owner *
ThreatStop Source

ThreatSTOP Policy Token *
YOUR_API_KEY

Log Level *
info

- **Step 3:** set the desired notifications. The recommended setting is to alert on failure and partial failure.

Edit Job
×

1
Program
2
Parameters
3
Schedule
4
Output

☒ Enable Notifications

Email Address

user@example.com

Notify on Job Result

☐ Success
☒ Partial Failure
☒ Failure

Attachments

☒ Include Log Files (1MB file size limit)

Schedule setting

The default schedule setting for importing the latest policy is every two hours. This setting controls how often the ThreatConnect Platform will check for updated policies. Imports are performed only if at least one of the selected policies has been updated.

The frequency can be increased based on the policy sizes. The following table lists recommended frequencies based on the total size of the selected policies.

Combined size of policies	Recommended frequency
50k to 100k records	Every 15 minutes
100k to 200k records	Every 30 minutes
200k to 400k records	Every 45 minutes
400k to 600k records	Hourly

Configuration changes

- Additional policies can be added to the list of exported policies.

- Policies can be removed from the list as well. IOCs will be deleted from the ThreatConnect database according to the deprecation rules.
- Policies are refreshed hourly by the ThreatSTOP system; the ThreatConnect application will import the policy based on the frequency selected in step 2 above.

Integration status

- The configuration page in the ThreatSTOP will display the update time for every exported policy and the number of IOCs in the last export. It will also warn if a policy has not been retrieved in more than one day or if the combined size of the policies exceed the maximum import size.

In the ThreatConnect Dashboard:

- The status of the last import attempt (Completed or failed) is shown on the Application list page as show below.

Jobs					
Search... Clear					
Job Name	Start Time	Last Execution	Next Execution	Active	Options
ThreatSTOP - ActiveIOC	01-28-2021 13:45 PST	Completed	01-28-2021 14:00 PST	<input checked="" type="checkbox"/>	⏸ ✎ ⋮
25					

- The Log for the integration can be viewed or downloaded by selecting **View Log** on the ThreatSTOP Integration entry as shown below.

Jobs					
Search... Clear					
Job Name	Start Time	Last Execution	Next Execution	Active	Options
ThreatSTOP - ActiveIOC	01-28-2021 13:45 PST	Completed	01-28-2021 14:00 PST	<input checked="" type="checkbox"/>	⏸ ✎ ⋮ <div> Delete Job Environment Export Job Kill Job Published Files View Details View Log </div>

- Possible errors include an incorrect Integration Key or exceeding the maximum number of IOCs that can be imported.

Threat Types

The ThreatSTOP Threat Types associated with targets are mapped to Tags in the ThreatConnect Platform. The possible values are:

- Anon Proxies
- Botnet
- C2
- Cryptomining
- Exfiltration
- Exploit Kits
- General
- Geo
- Inbound Attacks
- Infection Sites
- Malware
- Phishing
- Policy Violations
- Ransomware
- Scams
- Scanners
- Sinkholes
- Spam
- Test Target
- Whitelists
- APT
- Crawlers

ThreatSTOP Support

Please contact ThreatSTOP support (support@threatstop.com) for assistance with using the integration.

Release notes

Version	Date	Changes
1.0.4	February 2021	Initial Release