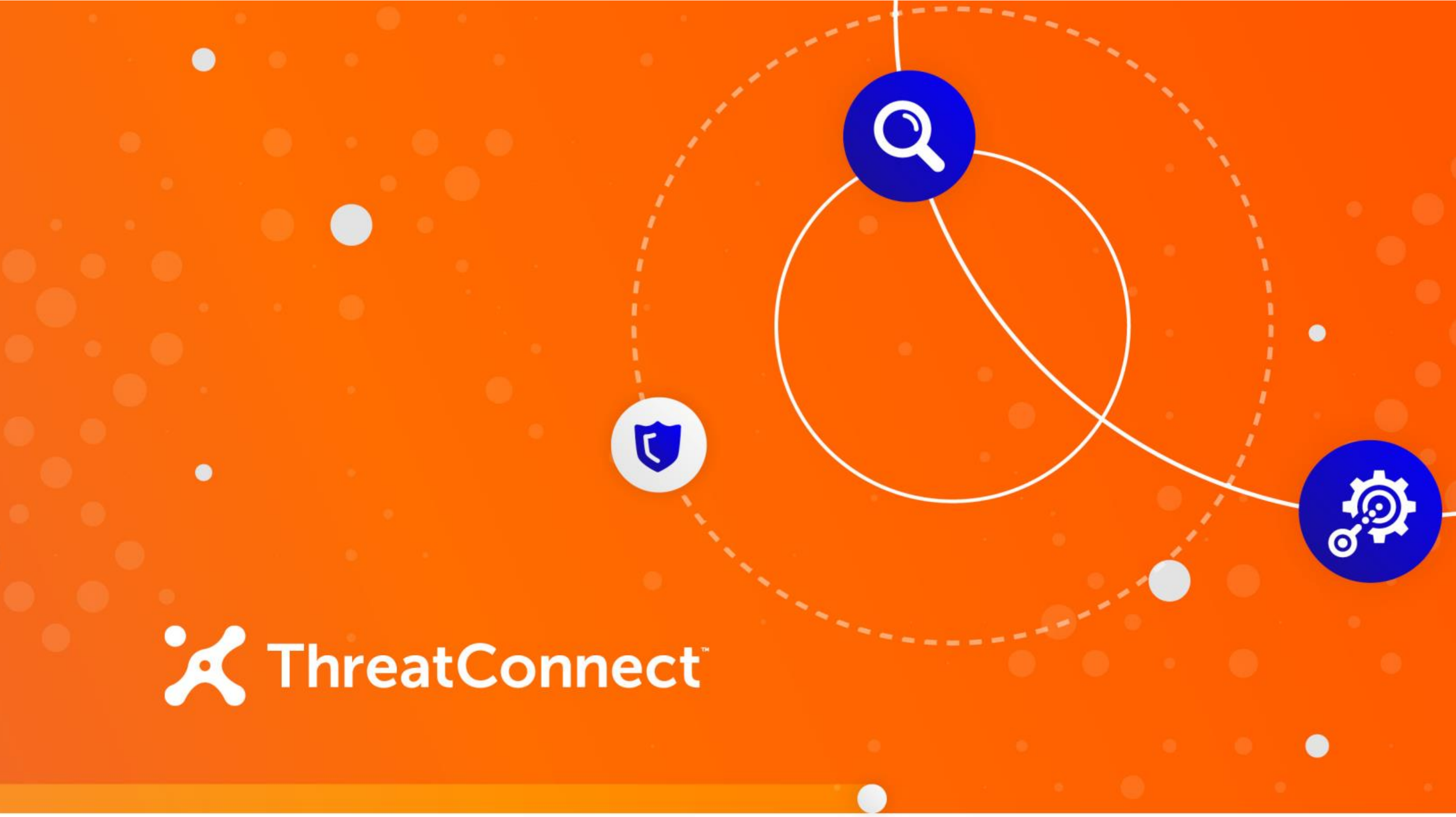


Application for Splunk®

User Guide

SOFTWARE VERSION 3.2

MARCH 3, 2022

30011-09 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: 1.703.229.4489
www.ThreatConnect.com

TABLE OF CONTENTS

OVERVIEW

The ThreatConnect® Application (App) for Splunk gives users the ability to integrate ThreatConnect's intelligence, automation, analytics, and workflows into Splunk. Users can centralize their intelligence, establish process consistency, scale operations, measure their effectiveness in one place, and put that refined knowledge to work in Splunk, identifying threats targeting their organization and taking action to contain and remediate them with automations and workflows.

KEY FEATURES

- Aggregate all sources of intel, such as data feeds and technology blogs, as well as logs from endpoint technologies to identify correlations and achieve actionable insights
- Reduce false positives by providing relevant and actionable intelligence to Splunk searches for alerting
- Customizable threat-intelligence downloads, custom searches, and data-model searches (Splunk CIM add-on required for data-model searches)
- Prioritize events based on Criticality and Confidence scores, relationships to known Threat types and Groups, past Incidents, and Tags
- Establish a feedback loop that allows for increased threat-intelligence insight and relevance to a user's organization.
- Trigger complex, automated workflows for consistent, repeatable, and faster decision making across a user's team.

GETTING STARTED

Prerequisites

Users will need an active ThreatConnect Application Programming Interface (API) account to leverage the ThreatConnect App for Splunk. Users without a current subscription to ThreatConnect who would like a live demonstration of the ThreatConnect App for Splunk, please inquire at sales@threatconnect.com.

Once an Organization in ThreatConnect has been licensed for API access, an Organization Administrator will need to create an API User within the Organization prior to Splunk interfacing with the ThreatConnect API. For detailed steps on creating an API User, see the "Creating an API User" section of *Creating User Accounts*.

Installation

Users can download the ThreatConnect App for Splunk from https://splunkbase.splunk.com/, or they can directly install the App from the **Find more apps online** link by going to the **Apps** and then the **Manage Apps** menu choices. For more information on installing Splunk Apps, refer to the Splunk documentation located at http://docs.splunk.com/Documentation.

The 3.0, and later, version of the App requires that two indexes be created. The App ships with an **indexes.conf** file; however, in a clustered environment the indexes should be created manually on the indexers.

The following is an example index configuration:

```
[tc_app_logs]
coldPath = $SPLUNK_DB/tc_app_logs/colddb
enableDataIntegrityControl = 0
enableTsidxReduction = 0
homePath = $SPLUNK_DB/tc_app_logs/db
maxTotalDataSizeMB = 20
thawedPath = $SPLUNK_DB/tc_app_logs/thaweddb

[tc_event_data]
coldPath = $SPLUNK_DB/tc_event_data/colddb
enableDataIntegrityControl = 1
enableTsidxReduction = 0
homePath = $SPLUNK_DB/tc_event_data/db
maxTotalDataSizeMB = 512000
thawedPath = $SPLUNK_DB/tc_event_data/thaweddb
```

Upgrading

When upgrading the ThreatConnect Splunk App from 2.*x* to 3.*x*, there are several different migrations that could be needed.

Migration 0.0.1:

The event data are not automatically migrated to the new collection and index. If migrating the data is a requirement, the app has a migration script that can be run to move the data. Running the

| tcmigration VERSION=0.0.1 command in a search will move the data from the **tc_events** collection to the **tc_event_summaries** collection, as well as the data from the **tc_events_data** collection to the **tc_event_data** index. During the migration, the data will be converted to a new **schema** required for the 3.0.0 version of the App.

Migration 0.0.2: (*required)

With the addition of **labels** to the **tc_event_summaries** collection, the state is not automatically transferred over. To update the collection with the appropriate value, the command **| tcmigration VERSION=0.0.2** is required. During the migration, the state will be removed from the collection and the labels attribute will be added and populated.

Migration 0.0.3:

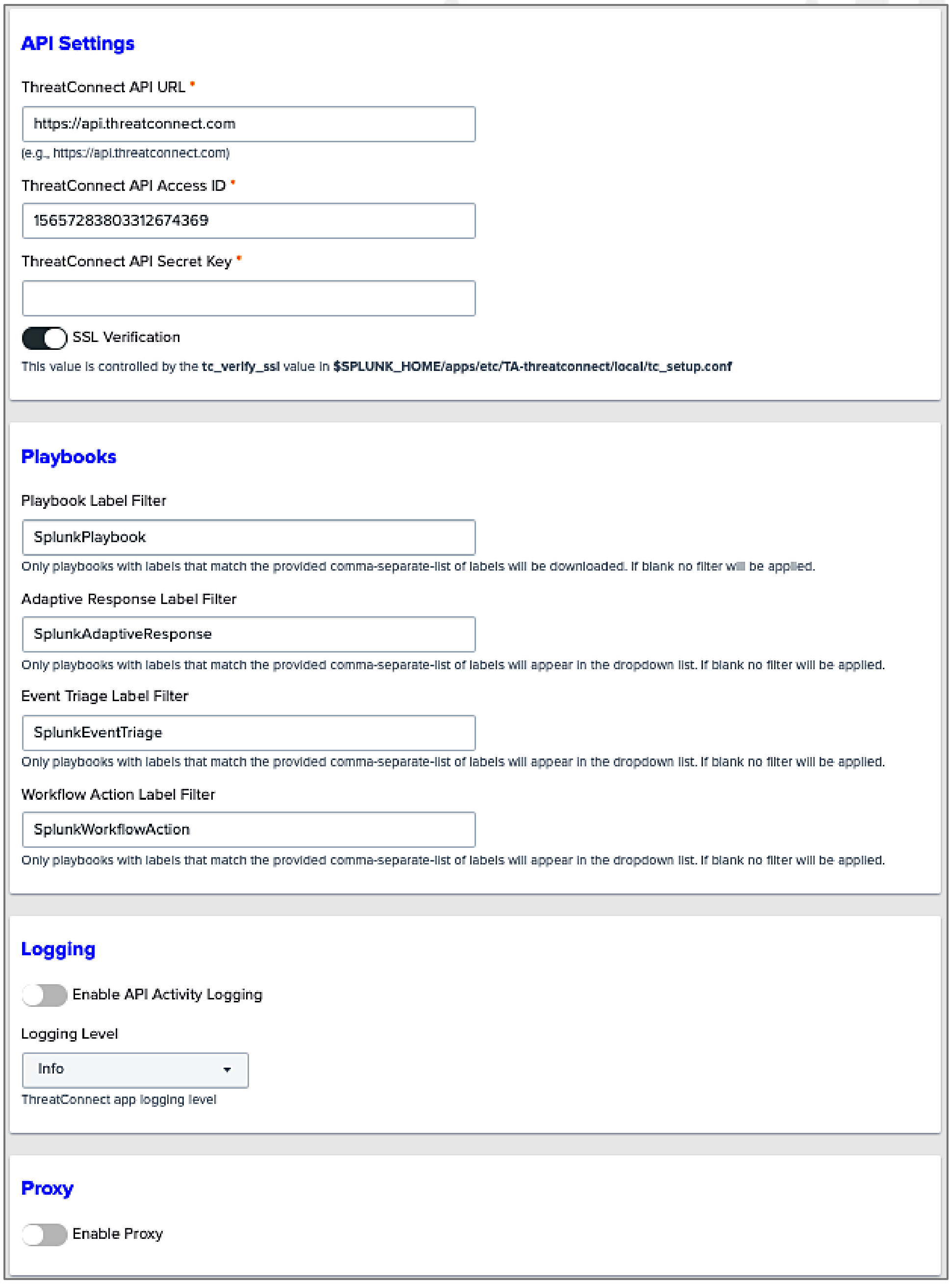
With the enhanced capabilities of the Data Model Search, an additional field, **whereClause**, has been added and the **objectName** field has been removed. To update the collection with the appropriate value, the command **| tcmigration VERSION=0.0.3** is needed. This migration will populate the **whereClause** attribute with the search previously applied using the **objectName** attribute.

NOTE: It is possible to skip to specific migration versions without applying the previous versions. For example, if migration 0.0.1 is not applicable, the user can skip to version 0.0.2 using the *|tcmigration VERSION=0.0.2* ***command. However, if this is done, the user will no longer be able to perform the*** *|tcmigration VERSION=0.0.1* ***command. Furthermore, migration versions noted with an asterisk (*) must be applied before the user is allowed to perform higher migration versions. For example, users currently on migration version 0.0.1 that attempt to perform the command*** *| tcmigration VERSION=0.0.3* ***will be notified that the minimum required version in order to upgrade to version 0.0.3 is version 0.0.2.***

THE THREATCONNECT APP FOR SPLUNK

App Setup and Configuration

After installing the ThreatConnect App for Splunk, the application setup must be completed before using the App. The **Settings** screen can be accessed from within the App by choosing **Configure** and then **Settings** from the menu. To properly configure the App, fill in each of the text boxes in the form with the appropriate data from the **API User Creation** section, as shown in Figure 1. This step requires a user to have the **admin** role in Splunk. The **admin** role is required in Splunk in order to edit the password endpoint. This is the only part of the App that requires this role.



API Settings

ThreatConnect API URL *

https://api.threatconnect.com

(e.g., https://api.threatconnect.com)

ThreatConnect API Access ID *

15657283803312674369

ThreatConnect API Secret Key *

● SSL Verification

This value is controlled by the **tc_verify_ssl** value in **$SPLUNK_HOME/apps/etc/TA-threatconnect/local/tc_setup.conf**

Playbooks

Playbook Label Filter

SplunkPlaybook

Only playbooks with labels that match the provided comma-separate-list of labels will be downloaded. If blank no filter will be applied.

Adaptive Response Label Filter

SplunkAdaptiveResponse

Only playbooks with labels that match the provided comma-separate-list of labels will appear in the dropdown list. If blank no filter will be applied.

Event Triage Label Filter

SplunkEventTriage

Only playbooks with labels that match the provided comma-separate-list of labels will appear in the dropdown list. If blank no filter will be applied.

Workflow Action Label Filter

SplunkWorkflowAction

Only playbooks with labels that match the provided comma-separate-list of labels will appear in the dropdown list. If blank no filter will be applied.

Logging

○ Enable API Activity Logging

Logging Level

Info ▾

ThreatConnect app logging level

Proxy

○ Enable Proxy

Figure 1

- **API Base URL**: The ThreatConnect Public Cloud API can be accessed at https://app.threatconnect.com/api. Users with a Dedicated Cloud or On-Premises instance of ThreatConnect were provided with their instance URL during their initial setup and installation and must append **/api** to the URL.
- **API Access ID**: The API Access ID corresponds to the Access ID of a user's ThreatConnect API account.
- **API Secret Key**: The API Secret Key corresponds to the Secret Key of a user's ThreatConnect API account, which is accessible during account creation within the user's ThreatConnect Organization.

- **SSL Verification**: This toggle is now controlled by a setting in the **$SPLUNK_HOME/etc/apps/TA-threatconnect/local/tc_setup.conf** file. The value on this page is only to indicate the current setting and cannot be changed in the UI.
- **Playbook Label Filter**: Use this filter to limit the Playbooks downloaded to Splunk. Only Playbooks that contain a label in the provided comma-separated list will be downloaded. If the input is left blank, then no filters will be applied.
- **Adaptive Response Label Filter**: Use this filter to limit the Playbooks in the dropdown input on the Adaptive Response screen. Only Playbooks that contain a label in the provided comma-separated list will be displayed. If the input is left blank, then no filters will be applied.
- **Event Triage Label Filter**: Use this filter to limit the Playbooks in the dropdown input on the Event Triage screen. Only Playbooks that contain a label in the provided comma-separated list will be displayed. If the input is left blank, then no filters will be applied.
- **Workflow Action Label Filter**: Use this filter to limit the Playbooks in the dropdown input on the Workflow Action screen. Only Playbooks that contain a label in the provided comma-separated list will be displayed. If the input is left blank, then no filters will be applied.
- **Enable API Activity Logging**: Toggle this slider on to enable activity logging in ThreatConnect for any API write actions.
- **Logging Level**: Select the logging level for the ThreatConnect App for Splunk. A best practice is to set this parameter to **info** or higher to prevent excessive logging.
- **Enable Proxy**: Toggle this slider on to enable proxy-server support. When this slider is toggled on, the following fields will be displayed:
  - **Proxy Host (Optional)**: This is the hostname or IP of the internal proxy server.
  - **Proxy Port (Optional)**: This is the port number for the proxy server.
  - **Proxy User (Optional)**: This is the authentication user name for the proxy server, if required.
  - **Proxy Pass (Optional)**: This is the authentication password for the proxy server, if required.

NOTE: After the setup is complete, the ThreatConnect App for Splunk will be usable. When accessing the App,the default dashboard will not show any populated results, which is expected until matched data are available.

Splunk REST Service SSL Verification

By default, the ThreatConnect App for Splunk does not verify the SSL certificates provided by the Splunk REST service (typically on localhost port 8089). If this setting is added, the certificate provided by the REST service must be trusted in order for the application to connect.

NOTE: To enable certificate checks, edit the following file under the *[ta_threatconnect_settings]* ***section:*** *$SPLUNK_HOME/etc/apps/TA-threatconnect/local/tc_setup.conf*. ***When editing this file, add*** *splunk_rest_ssl =* ***to it.***

App Roles

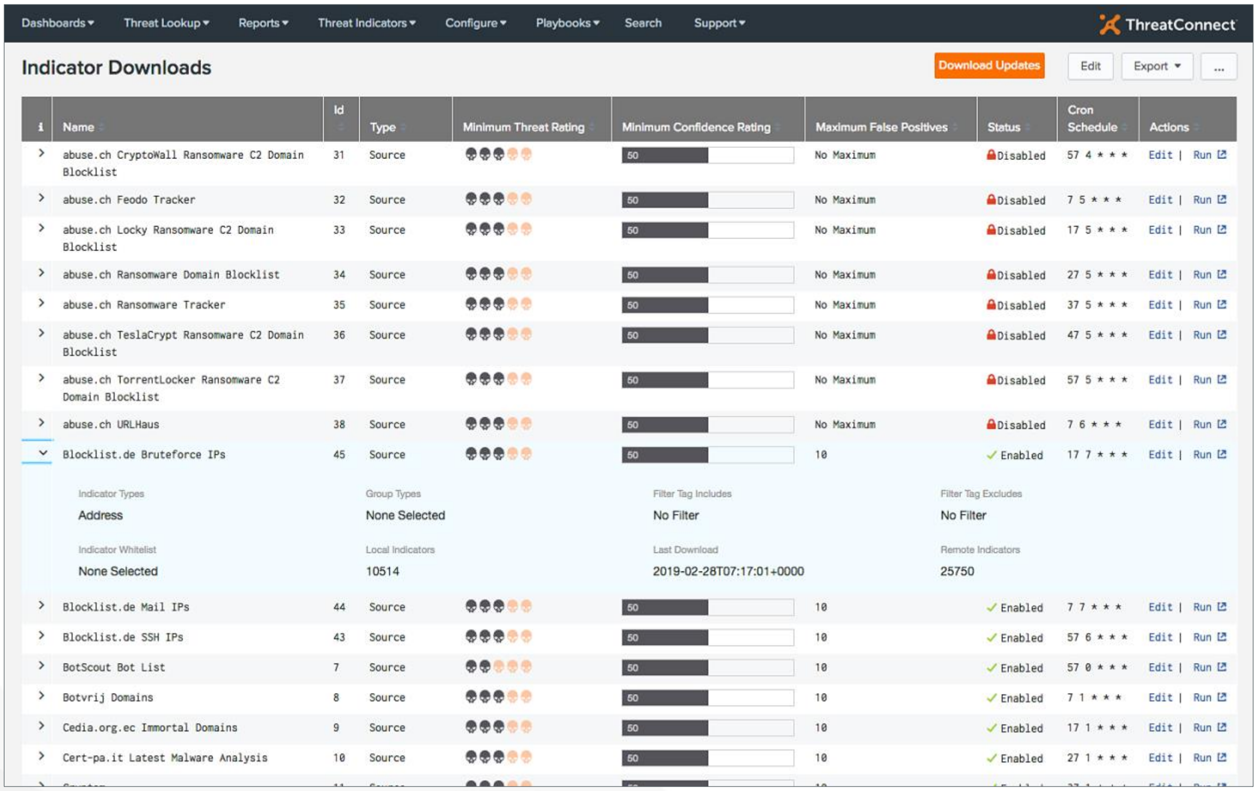
The App provides two roles: **tc_admin and tc_user**. The **tc_admin** role allows a user to execute key commands, such as `tcowners`. The Splunk administrator will have to add this role to any user requiring access in order to execute these commands. The **tc_user** role allows users to update event status on the **Event Triage** dashboard.

NOTE: For Splunk version 6.5 or higher, the** list_storage_passwords **capability provides the required permissions.

Indicator Downloads

After setting up the App, users may want to specify filters for the Groups and Indicators imported from ThreatConnect. The **Indicator Downloads** screen (Figure 2) allows users to choose what is imported into Splunk for alerting and context and how often it is updated. To load the owner's information for the first time, click the **Download Updates** button. This button can also be used to sync changes to owners in ThreatConnect.

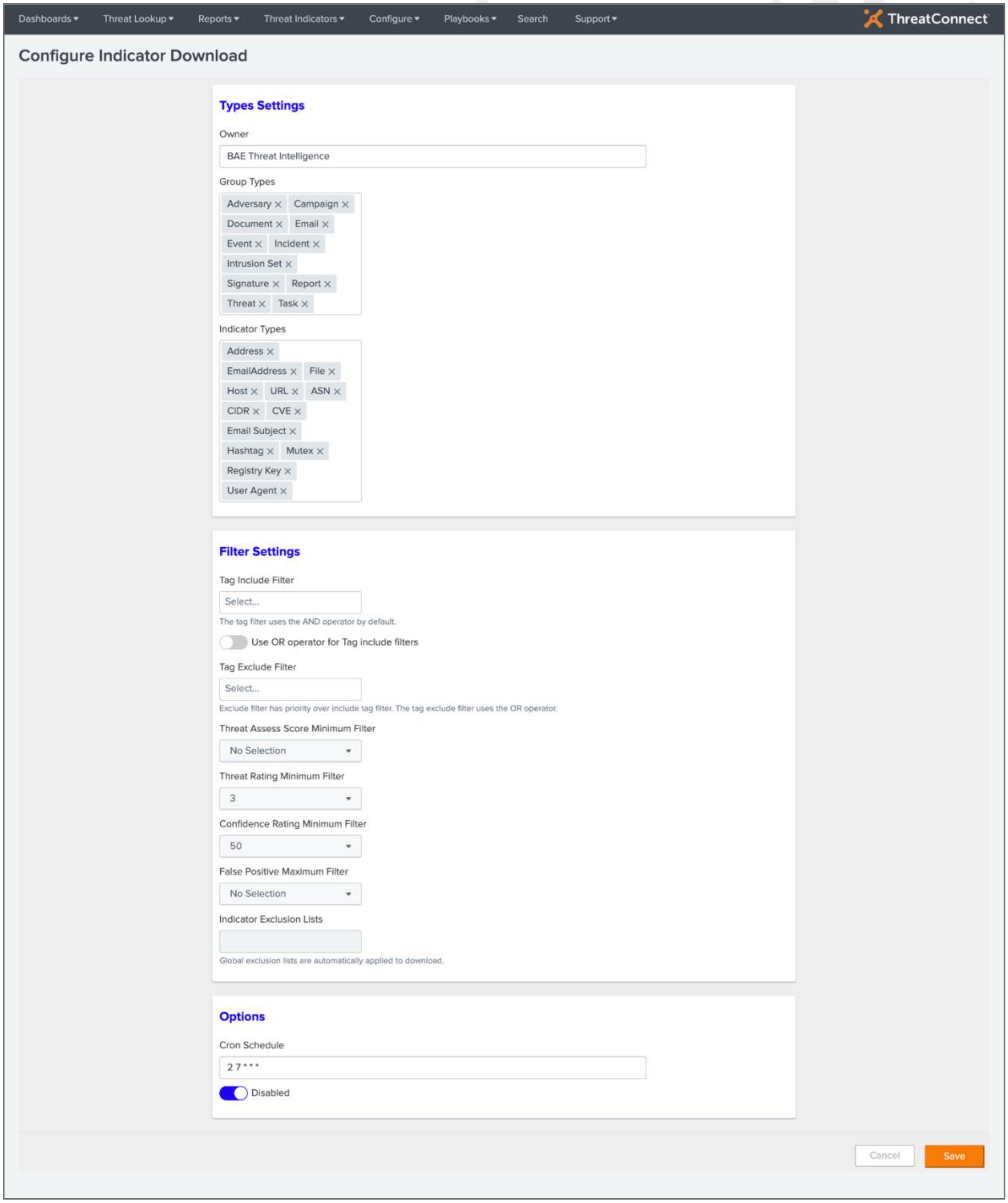
To edit a specific owner configuration, click **Edit** in the **Actions** column for the owner. The **Indicator Download Configuration** screen will be displayed (Figure 3). To run the Indicator download (optional), click **Run** in the **Actions** column for the owner. A new tab will open and execute the Indicator downloaded for the owner listed in the selected row. The download can take a while on initial run, as it syncs Indicators to the Splunk instance. For the duration of the download, the search will remain in **Finalizing Results** status.



Indicator Downloads

i	Name	Id	Type	Minimum Threat Rating	Minimum Confidence Rating	Maximum False Positives	Status	Cron Schedule	Actions
›	abuse.ch CryptoWall Ransomware C2 Domain Blocklist	31	Source	●●●○○	50	No Maximum	Disabled	57 4 * * *	Edit | Run
›	abuse.ch Feodo Tracker	32	Source	●●●○○	50	No Maximum	Disabled	7 5 * * *	Edit | Run
›	abuse.ch Locky Ransomware C2 Domain Blocklist	33	Source	●●●○○	50	No Maximum	Disabled	17 5 * * *	Edit | Run
›	abuse.ch Ransomware Domain Blocklist	34	Source	●●●○○	50	No Maximum	Disabled	27 5 * * *	Edit | Run
›	abuse.ch Ransomware Tracker	35	Source	●●●○○	50	No Maximum	Disabled	37 5 * * *	Edit | Run
›	abuse.ch TeslaCrypt Ransomware C2 Domain Blocklist	36	Source	●●●○○	50	No Maximum	Disabled	47 5 * * *	Edit | Run
›	abuse.ch TorrentLocker Ransomware C2 Domain Blocklist	37	Source	●●●○○	50	No Maximum	Disabled	57 5 * * *	Edit | Run
›	abuse.ch URLHaus	38	Source	●●●○○	50	No Maximum	Disabled	7 6 * * *	Edit | Run
⌄	Blocklist.de Bruteforce IPs	45	Source	●●●○○	50	10	✓ Enabled	17 7 * * *	Edit | Run
	Indicator Types Address Indicator Whitelist None Selected		Group Types None Selected Local Indicators 10514		Filter Tag Includes No Filter Last Download 2019-02-28T07:17:01+0000	Filter Tag Excludes No Filter Remote Indicators 25750			
›	Blocklist.de Mail IPs	44	Source	●●●○○	50	10	✓ Enabled	7 7 * * *	Edit | Run
›	Blocklist.de SSH IPs	43	Source	●●●○○	50	10	✓ Enabled	57 6 * * *	Edit | Run
›	BotScout Bot List	7	Source	●●○○○	50	10	✓ Enabled	57 0 * * *	Edit | Run
›	Botvrij Domains	8	Source	●●●○○	50	10	✓ Enabled	7 1 * * *	Edit | Run
›	Cedia.org.ec Immortal Domains	9	Source	●●●○○	50	10	✓ Enabled	17 1 * * *	Edit | Run
›	Cert-pa.it Latest Malware Analysis	10	Source	●●●○○	50	10	✓ Enabled	27 1 * * *	Edit | Run

Figure 2



Configure Indicator Download

Types Settings

Owner: BAE Threat Intelligence

Group Types: Adversary ×, Campaign ×, Document ×, Email ×, Event ×, Incident ×, Intrusion Set ×, Signature ×, Report ×, Threat ×, Task ×

Indicator Types: Address ×, EmailAddress ×, File ×, Host ×, URL ×, ASN ×, CIDR ×, CVE ×, Email Subject ×, Hashtag ×, Mutex ×, Registry Key ×, User Agent ×

Filter Settings

Tag Include Filter: Select...

The tag filter uses the AND operator by default.

○ Use OR operator for Tag include filters

Tag Exclude Filter: Select...

Exclude filter has priority over include tag filter. The tag exclude filter uses the OR operator.

Threat Assess Score Minimum Filter: No Selection ▾

Threat Rating Minimum Filter: 3 ▾

Confidence Rating Minimum Filter: 50 ▾

False Positive Maximum Filter: No Selection ▾

Indicator Exclusion Lists:

Global exclusion lists are automatically applied to download.

Options

Cron Schedule: 2 7 * * *

● Disabled

Figure 3

- **Owner**: The selected owner to be configured is given here.
- **Group Types**: Select the ThreatConnect Group types to download. The Group data are not currently used in the App, but made available in the KV Store for custom use cases.

- **Indicator Types**: Select the Indicator types to download for use by the ThreatConnect App for Splunk.
- **Tag Include Filter**: Add any Tags to filter Indicators that are available to the ThreatConnect App for Splunk. If Tags are provided, only Indicators that have all those Tags (And operator) present will be downloaded into the App.

  NOTE: Tag names are case sensitive.

- **Use OR Operator for Tag include filters:** Toggle this slider on to enable the Tag filter feature to use **OR** tags instead of the default **AND.**
- **Tag Exclude Filter**: Add any Tags to filter Indicators that are available to the ThreatConnect App for Splunk. If Tags are provided, Indicators that have any listed Tag(s) present will *not* be downloaded into the App.

  NOTE: *Tag Filters Exclude* ***will override*** *Tag Filters Include.*
- **Threat Assess Score Minimum Filter:** Select a minimum threshold for an Indicator's ThreatAssess score. In ThreatConnect, ThreatAssess scores have a value of 0–1000. Only Indicators that meet the filter's threshold will be downloaded into the App.
- **Threat Rating Minimum Filter**: Select a minimum threshold for an Indicator's Threat Rating. In ThreatConnect, Threat Ratings have a value of 0–5 skulls. Only Indicators that meet the filter's threshold will be downloaded into the App.
- **Confidence Rating Minimum Filter**: Select a minimum threshold for an Indicator's Confidence. In ThreatConnect, Confidence Ratings have a value of 0–100. Only Indicators that meet the filter's threshold will be downloaded into the App.
- **False Positive Maximum Filter**: Select a maximum threshold for an Indicator's false positive count. Indicators that have a false positive count higher than the provided value will be filtered during the download.
- **Indicator Exclusion Lists**: Select one or more preconfigured Indicator exclusion lists. Global exclusion lists apply to all Indicator downloads.

  NOTE: If an Indicator exclusion list has been created or updated, the changes will not convey for pre-existing Indicator data until the option to Clear and Save the source has been invoked.
- **Cron Schedule**: The schedule for the Indicator download is defined here. The recommended download period is once every 24 hours. More information on Cron settings can be found at: https://docs.splunk.com/Documentation/Splunk/latest/Alert/CronExpressions.
- **Disable**: Toggle this slider on to disable any further syncs of Indicators for this owner. Toggling this slider on will not remove existing downloaded Indicators from the App and will not prevent matches of those Indicators.

When saving the Indicator download configuration, an option for Clear and Save is presented to allow Indicators to be removed from the system while saving. This feature allows for the removal of Indicators when the download for the owner is disabled. This feature is also useful when filter values have changed and a resync of the Indicator data is required.

Setting Up Custom Searches

Any simple search that returns a set of Indicators can be used with the ThreatConnect App for Splunk to search for known Indicators. The App provides a form to create custom searches that will use the Indicators downloaded from ThreatConnect. Select **Custom Searches** from the **Configure** menu (Figure 4) to access the **Configure Custom Search** screen (Figure 5).

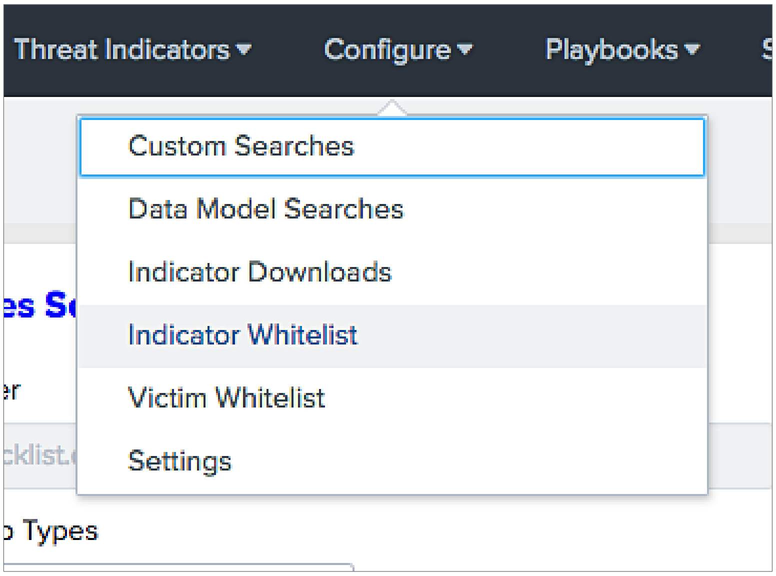
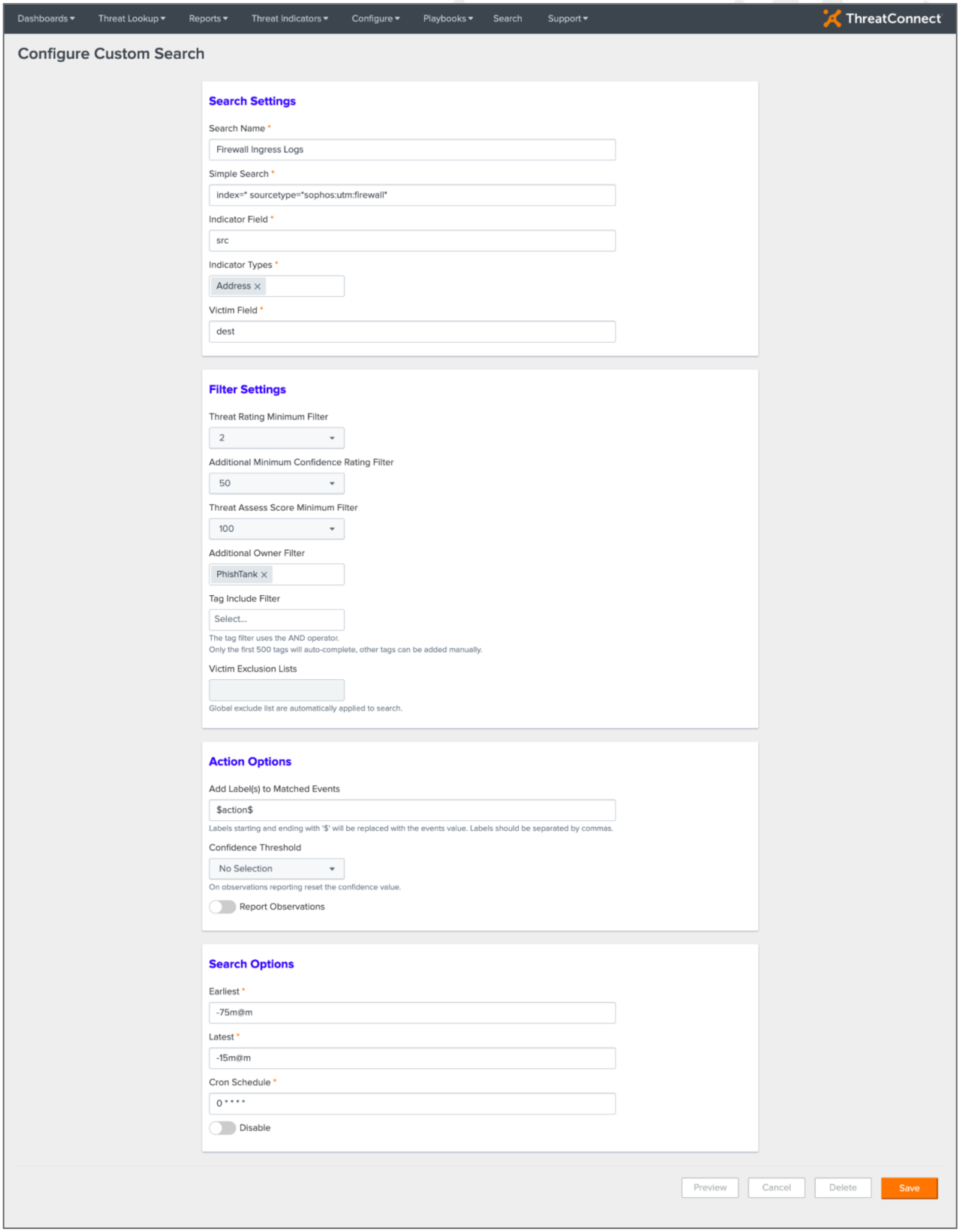


Figure 4



Configure Custom Search

Search Settings

Search Name *

Firewall Ingress Logs

Simple Search *

index=" sourcetype="sophos:utm:firewall"

Indicator Field *

src

Indicator Types *

Address ×

Victim Field *

dest

Filter Settings

Threat Rating Minimum Filter

2 ▾

Additional Minimum Confidence Rating Filter

50 ▾

Threat Assess Score Minimum Filter

100 ▾

Additional Owner Filter

PhishTank ×

Tag Include Filter

Select...

The tag filter uses the AND operator.
Only the first 500 tags will auto-complete, other tags can be added manually.

Victim Exclusion Lists

Global exclude list are automatically applied to search.

Action Options

Add Label(s) to Matched Events

$action$

Labels starting and ending with '$' will be replaced with the events value. Labels should be separated by commas.

Confidence Threshold

No Selection ▾

On observations reporting reset the confidence value.

○ Report Observations

Search Options

Earliest *

-75m@m

Latest *

-15m@m

Cron Schedule *

0 * * * *

○ Disable

Figure 5

- **Search Name**: The identifier for this job (e.g., Firefox Vulnerability).

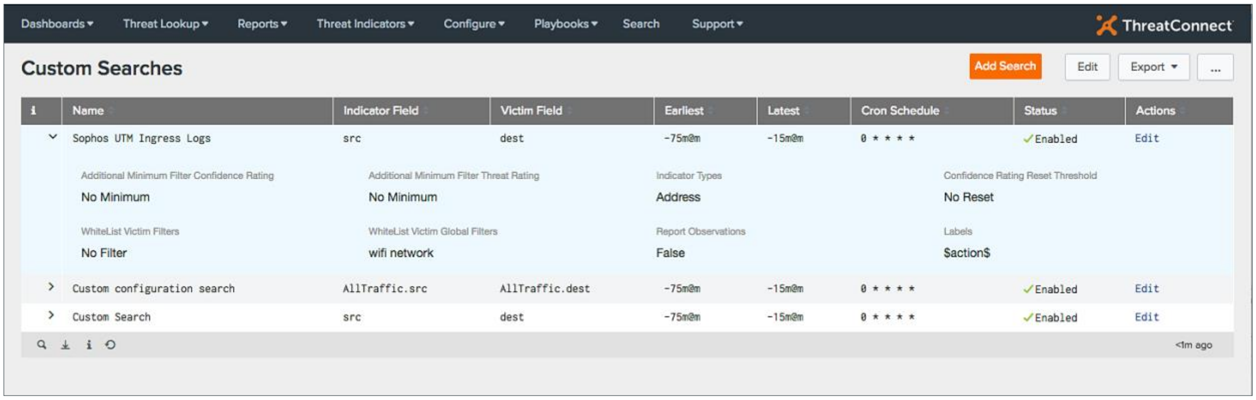
- **Simple Search**: A properly formatted Splunk search expression that will return events with Indicators. This can be validated using the **Preview** button at the lower-right corner of the screen.
- **Indicator Field**: The results field name that contains the Indicator to be checked.
- **Indicator Types**: The type of Indicators against which the Indicator Field should be checked. Multiple Indicator types can be selected.
- **Victim Field**: The results field name that contains the victim for this event. For example, if the Indicator Field is **url**, then the Victim Field might be **src_ip**.
- **Additional Minimum Threat Rating Minimum Filter**: This option allows each search to narrow the Indicator pool by adding further filtering on Threat Rating. It is important to note that this filter is above the filters in the Indicator download configuration.
- **Additional Minimum Confidence Rating Filter**: This option allows each search to narrow the Indicator pool by adding further filtering on Confidence Rating. It is important to note that this filter is above the filters in the Indicator download configuration.
- **Threat Assess Score Minimum Filter**: This option allows each search to narrow the Indicator pool by adding further filtering on ThreatAssess score. It is important to note that this filter is above the filters in the Indicator download configuration.
- **Additional Owner Filter**: This option allows each search to narrow the Indicator pool by further filtering on additional owners. It is important to note that this filter is above the filters in the Indicator download configuration.
- **Tag Include Filter**: Provide one or more Tag Include filters for this search.
- **Victim Exclusion Lists**: Select one or more pre-configured Victim exclusion lists. Global exclusion lists will not be available.
- **Add Label(s) to Matched Events**: Two types of labels can be added automatically to an event. The first type is a static value (e.g., **fw-event**), which will be added to the event as entered by the user. The second type is a dynamic value (e.g., **$action$**), which will cause the search to look up the matching field name in the event and write the value for that field as a label. Note that a label of **New** is added to all events by default.
- **Confidence Threshold**: If a value is selected, this feature will allow the update of the Confidence Rating in ThreatConnect to the selected value. This feature is intended to work with Indicator deprecation in ThreatConnect. By changing the Confidence Rating, deprecation of the Indicator can be delayed.
- **Report Observations**: Toggle this slider on to enable the feedback loop to report observations back to ThreatConnect.
- **Earliest:** This parameter represents the start window of time that should be searched (e.g., use **-75m@m** to start 75 minutes in the past). See the following link for additional information: http://docs.splunk.com/Documentation/Splunk/6.4.1/SearchReference/SearchTimeModifiers

- **Latest:** This parameter represents the end window of time that should be searched (e.g., **15m@m to end 15 minutes in the past**).
- **Cron Schedule**: This parameter represents the cron schedule for this search. Note that if the search is run every hour, then **Search Window (earliest)** should be **-1h**.
- **Disable**: Toggle this slider on to prevent this search from running.

Preview

The **Preview** button allows the user to view a sample result set that is returned from the current search. This feature is helpful to ensure that the search is valid and returns the expected Indicator and Victim values.

To add a new search, click the **Add Search** button at the top right of the screen (Figure 6). To edit a search, click **Edit** in the **Actions** column.



Custom Searches

i	Name	Indicator Field	Victim Field	Earliest	Latest	Cron Schedule	Status	Actions
⌄	Sophos UTM Ingress Logs	src	dest	-75m@m	-15m@m	0 * * * *	✓Enabled	Edit
›	Custom configuration search	AllTraffic.src	AllTraffic.dest	-75m@m	-15m@m	0 * * * *	✓Enabled	Edit
›	Custom Search	src	dest	-75m@m	-15m@m	0 * * * *	✓Enabled	Edit

Additional Minimum Filter Confidence Rating: No Minimum
Additional Minimum Filter Threat Rating: No Minimum
Indicator Types: Address
Confidence Rating Reset Threshold: No Reset
WhiteList Victim Filters: No Filter
WhiteList Victim Global Filters: wifi network
Report Observations: False
Labels: $action$

Figure 6

Setting up Data-Model Searches

To configure data-model searches, click the **Configure** menu and select **Data Model Searches** (Figure 7). To add a new data-model search, click the **Add Search** button at the top right of the screen (Figure 8). To edit an existing search, click **Edit** in the **Actions** column. Figure 9 shows the **Configure Data Model Search** screen.

NOTE: The ThreatConnect App for Splunk supports only searches that use the Splunk Common Information Model (CIM). Although other data models can be used, they are not supported.

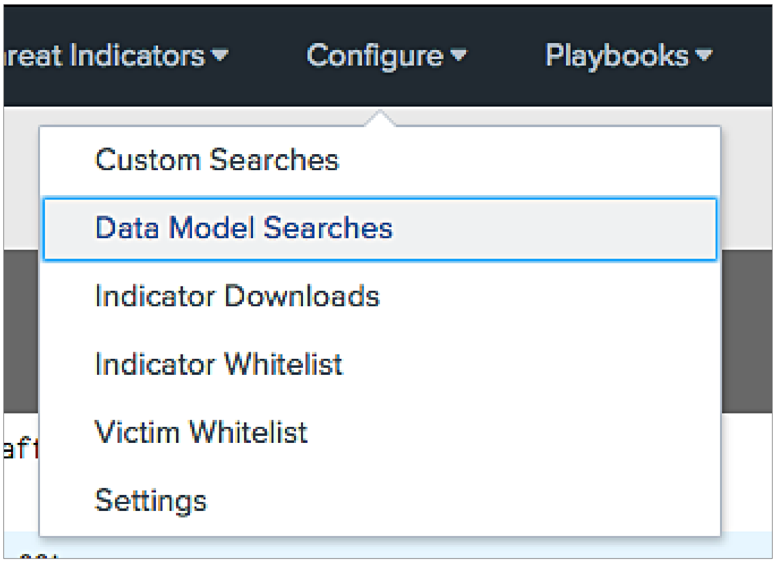
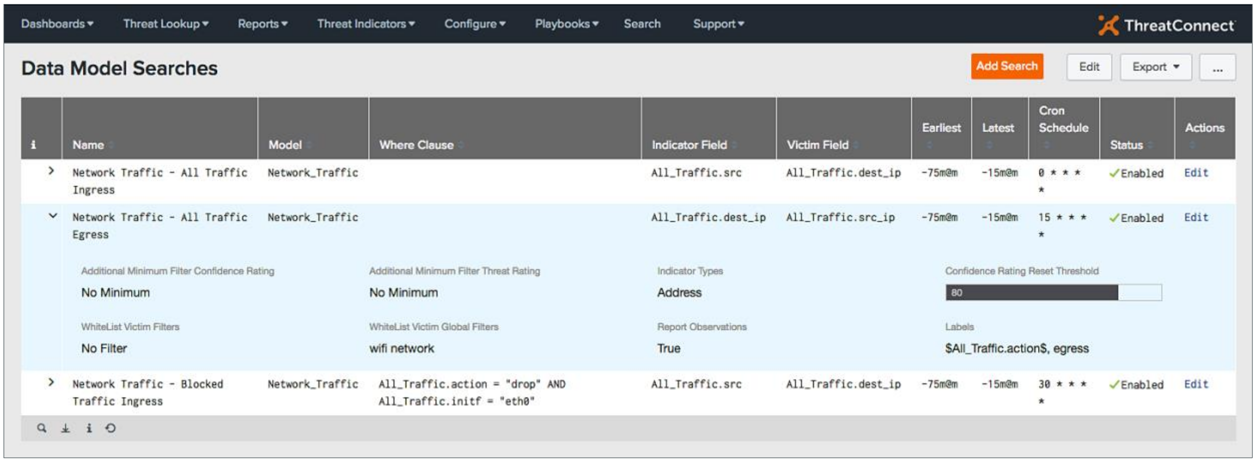


Figure 7

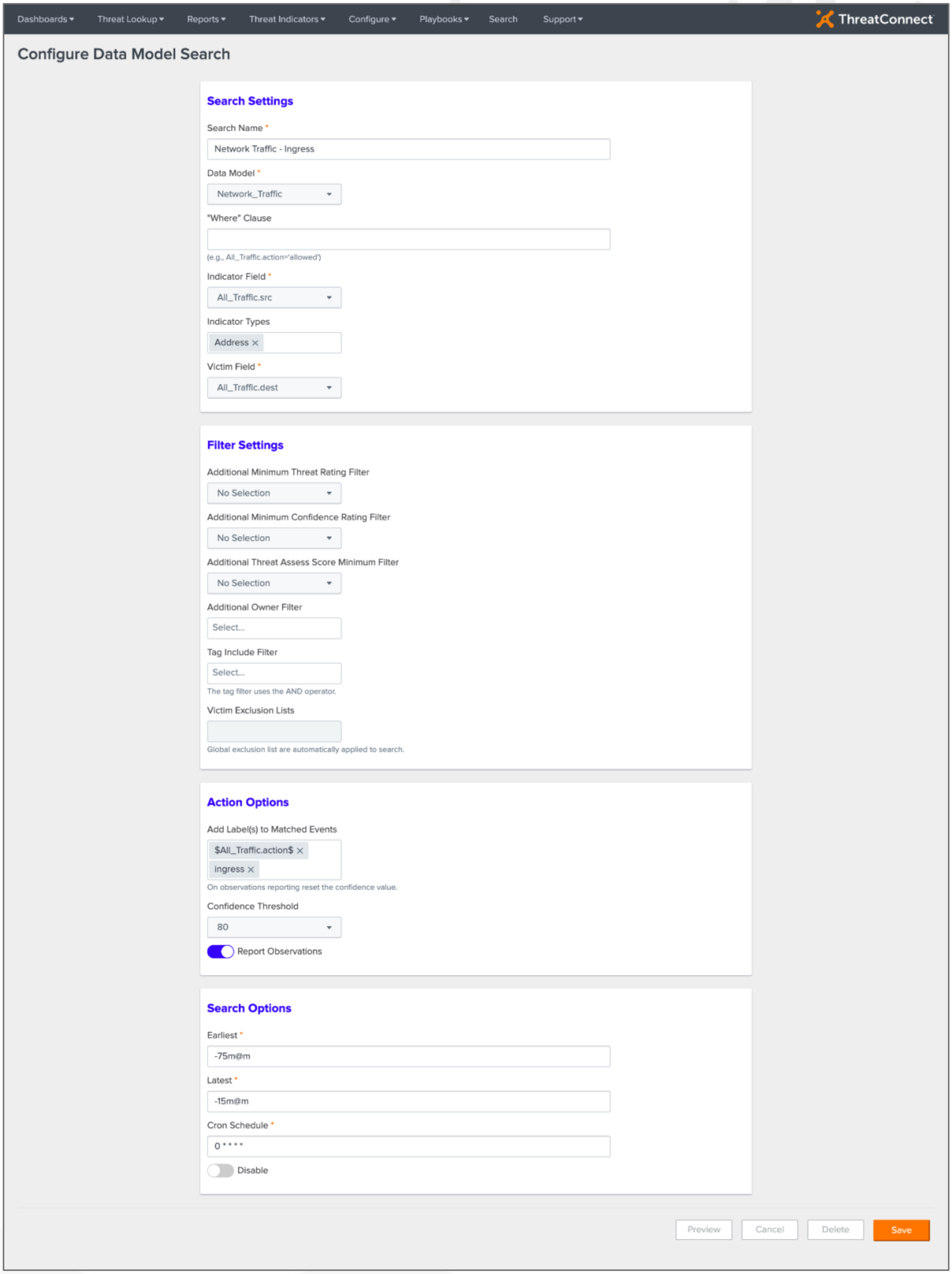


Data Model Searches

i	Name	Model	Where Clause	Indicator Field	Victim Field	Earliest	Latest	Cron Schedule	Status	Actions
>	Network Traffic - All Traffic Ingress	Network_Traffic		All_Traffic.src	All_Traffic.dest_ip	-75m@m	-15m@m	0 * * * *	✓Enabled	Edit
˅	Network Traffic - All Traffic Egress	Network_Traffic		All_Traffic.dest_ip	All_Traffic.src_ip	-75m@m	-15m@m	15 * * * *	✓Enabled	Edit
>	Network Traffic - Blocked Traffic Ingress	Network_Traffic	All_Traffic.action = "drop" AND All_Traffic.initf = "eth0"	All_Traffic.src	All_Traffic.dest_ip	-75m@m	-15m@m	30 * * * *	✓Enabled	Edit

Additional Minimum Filter Confidence Rating: No Minimum
Additional Minimum Filter Threat Rating: No Minimum
Indicator Types: Address
Confidence Rating Reset Threshold: 80
WhiteList Victim Filters: No Filter
WhiteList Victim Global Filters: wifi network
Report Observations: True
Labels: $All_Traffic.action$, egress

Figure 8



Configure Data Model Search

Search Settings

Search Name *: Network Traffic - Ingress

Data Model *: Network_Traffic

"Where" Clause:

(e.g., All_Traffic.action='allowed')

Indicator Field *: All_Traffic.src

Indicator Types: Address ×

Victim Field *: All_Traffic.dest

Filter Settings

Additional Minimum Threat Rating Filter: No Selection

Additional Minimum Confidence Rating Filter: No Selection

Additional Threat Assess Score Minimum Filter: No Selection

Additional Owner Filter: Select...

Tag Include Filter: Select...

The tag filter uses the AND operator.

Victim Exclusion Lists:

Global exclusion list are automatically applied to search.

Action Options

Add Label(s) to Matched Events: $All_Traffic.action$ × ingress ×

On observations reporting reset the confidence value.

Confidence Threshold: 80

● Report Observations

Search Options

Earliest *: -75m@m

Latest *: -15m@m

Cron Schedule *: 0 * * * *

○ Disable

Figure 9

- **Search Name**: The identifier for this search.
- **Data Model**: The name of the data model to be searched.
- **Where Clause**: This input allows the user to configure additional filters for the search (e.g., **All_Traffic.action==”blocked”** or (**All_Traffic.action==”blocked”** AND **All_Traffic.initf==”eth0”**). The syntax of this input must be valid SPL and can be validated using the **Preview** button at the bottom of the page.
- **Indicator Field**: The data-model field containing the Indicator.
- **Indicator Types**: The type of Indicators against which the **Indicator Field** should be checked. Multiple Indicator types can be selected.
- **Victim Field**: The data-model field containing the victim.
- **Additional Minimum Threat Rating Filter**: This option allows each search to narrow the Indicator pool by adding further filtering on Threat Rating. It is important to note that this filter is above the filters in the Indicator download configuration.
- **Additional Minimum Confidence Rating Filter**: This option allows each search to narrow the Indicator pool by adding further filtering on Confidence Rating. It is important to note that this filter is above the filters in the Indicator download configuration.
- **Additional Threat Assess Score Filter**: This option allows each search to narrow the Indicator pool by adding further filtering on ThreatAssess score. It is important to note that this filter is above the filters in the Indicator download configuration.
- **Additional Owner Filter**: This option allows each search to narrow the Indicator pool by adding further filtering on owners. It is important to note that this filter is above the filters in the Indicator download configuration.
- **Tag Include Filter**: Provide one or more Tag Include filters for this search.
- **Victim Exclusion Lists**: Select one or more pre-configured Victim exclusion lists. Global exclusion lists will not be available.
- **Add Label(s) to Matched Events**: Two types of labels can be added automatically to an event. The first type is a static value (e.g., **fw-event**) that will be added to the event as entered by the user. The second type is a dynamic value (e.g., **$action$)**, which will cause the search to lookup the matching field name in the event and write the value for that field as a label. Note that a label of **New** is added to all events by default.
- **Confidence Threshold**: If a value is selected, this feature will allow the update of the Confidence Rating in ThreatConnect to the selected value. This feature is intended to work with Indicator deprecation in ThreatConnect. By changing the Confidence Rating, deprecation of the Indicator can be delayed.
- **Report Observations**: Toggle this slider on to enable the feedback loop to report observations back to ThreatConnect.
- **Earliest**: This parameter represents the start window of time that should be searched (e.g., use **-75m@m** to start 75 minutes in the past). See the following link for additional information:

http://docs.splunk.com/Documentation/Splunk/6.4.1/SearchReference/SearchTimeModifiers

- **Latest:** This parameter represents the end window of time that should be searched (e.g.,-15m@m to end 15 minutes in the past).
- **Cron Schedule**: This parameter represents the cron schedule for this search. Note that if the search is run every hour, then **Search Window (earliest)** should be **-1h.Disable**: Check this box to prevent this search from running.
- **Disable**: Toggle this slider on to prevent this search from running.

Preview

The **Preview** button allows the user to view a sample result set that is returned from the current search. This feature is helpful to ensure that the search is valid and returns the expected Indicator and Victim values.

To add a new search, click the **Add Search** button at the upper right of the screen (Figure 6). To edit a search, click **Edit** in the **Actions** column.

Playbooks

Users may wish to incorporate their Playbooks from ThreatConnect into Splunk. To do so, click the **Playbooks** menu and select **Playbooks** (Figure 10). The **Playbooks** screen will be displayed, which is where users can import Playbooks that use a WebHook Trigger from ThreatConnect into Splunk (Figure 11). The **Downloaded Update** button uses the filters provided on the **Settings** screen.

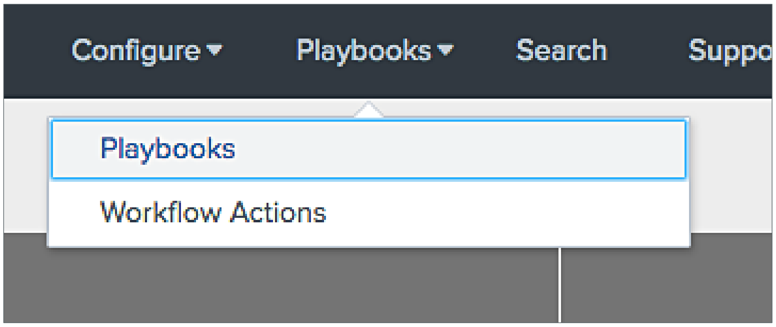
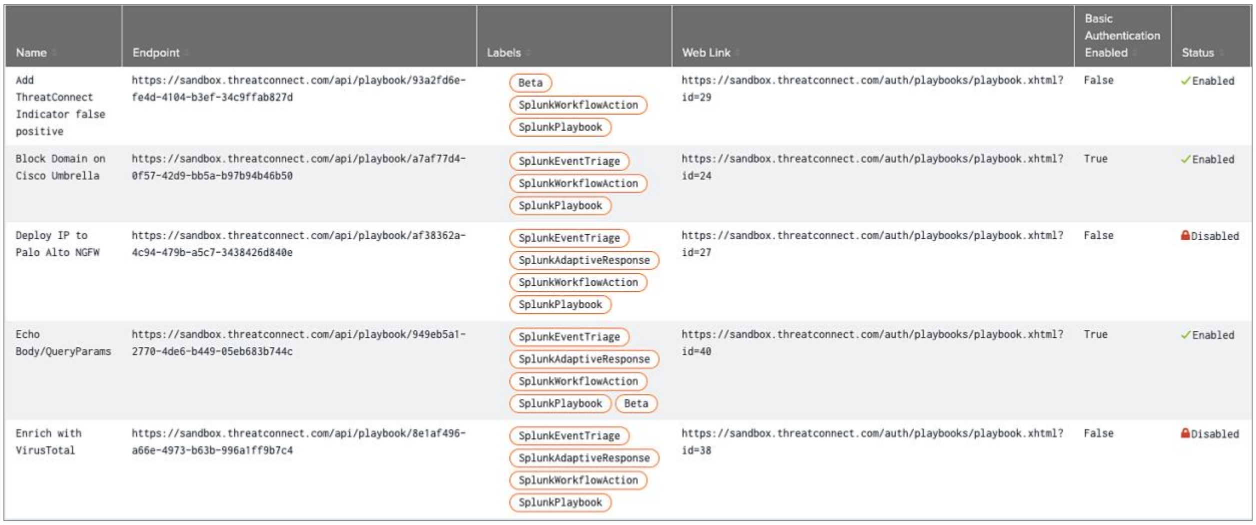


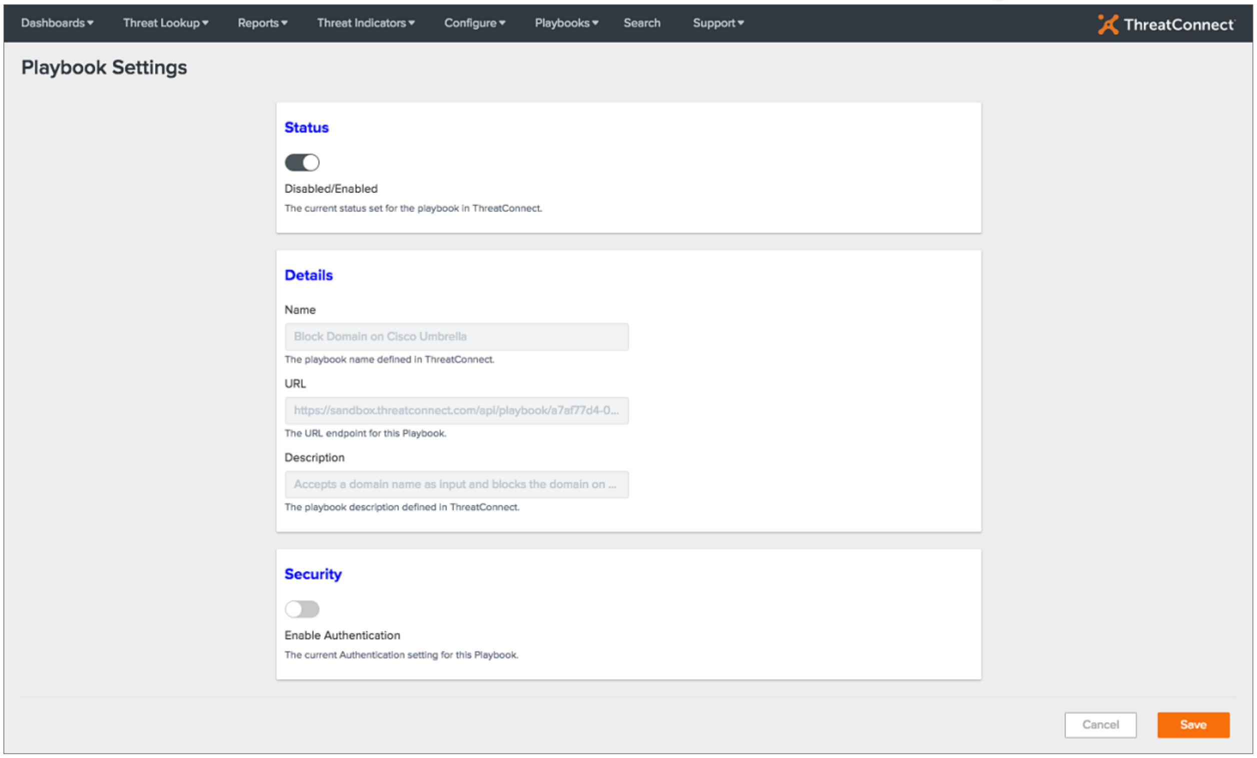
Figure 10



Name	Endpoint	Labels	Web Link	Basic Authentication Enabled	Status
Add ThreatConnect Indicator false positive	https://sandbox.threatconnect.com/api/playbook/93a2fd6e-fe4d-4104-b3ef-34c9ffab827d	Beta SplunkWorkflowAction SplunkPlaybook	https://sandbox.threatconnect.com/auth/playbooks/playbook.xhtml?id=29	False	✓Enabled
Block Domain on Cisco Umbrella	https://sandbox.threatconnect.com/api/playbook/a7af77d4-0f57-42d9-bb5a-b97b94b46b50	SplunkEventTriage SplunkWorkflowAction SplunkPlaybook	https://sandbox.threatconnect.com/auth/playbooks/playbook.xhtml?id=24	True	✓Enabled
Deploy IP to Palo Alto NGFW	https://sandbox.threatconnect.com/api/playbook/af38362a-4c94-479b-a5c7-3438426d840e	SplunkEventTriage SplunkAdaptiveResponse SplunkWorkflowAction SplunkPlaybook	https://sandbox.threatconnect.com/auth/playbooks/playbook.xhtml?id=27	False	🔒Disabled
Echo Body/QueryParams	https://sandbox.threatconnect.com/api/playbook/949eb5a1-2770-4de6-b449-05eb683b744c	SplunkEventTriage SplunkAdaptiveResponse SplunkWorkflowAction SplunkPlaybook Beta	https://sandbox.threatconnect.com/auth/playbooks/playbook.xhtml?id=40	True	✓Enabled
Enrich with VirusTotal	https://sandbox.threatconnect.com/api/playbook/8e1af496-a66e-4973-b63b-996a1ff9b7c4	SplunkEventTriage SplunkAdaptiveResponse SplunkWorkflowAction SplunkPlaybook	https://sandbox.threatconnect.com/auth/playbooks/playbook.xhtml?id=38	False	🔒Disabled

Figure 11

When a Playbook in ThreatConnect is deleted and the user reimports the Playbook, all Workflow Actions corresponding to that Playbook will be marked as **Disabled**. To view or configure the Playbook, or to edit its basic authentication credentials, click **Edit** in the **Actions** column. The **Playbook Configuration** screen will be displayed (Figure 12).



Playbook Settings

Status

Disabled/Enabled

The current status set for the playbook in ThreatConnect.

Details

Name: Block Domain on Cisco Umbrella

The playbook name defined in ThreatConnect.

URL: https://sandbox.threatconnect.com/api/playbook/a7af77d4-0...

The URL endpoint for this Playbook.

Description: Accepts a domain name as input and blocks the domain on ...

The playbook description defined in ThreatConnect.

Security

Enable Authentication

The current Authentication setting for this Playbook.

Figure 12

- **Status**: The current status set for the Playbook in ThreatConnect.
- **Name**: The Playbook name defined in ThreatConnect.
- **URL**: The URL endpoint for the Playbook.
- **Description**: The Playbook description defined in ThreatConnect.
- **Enable Authentication**: The current Authentication Setting for this Playbook. Toggling this slider on will display the following fields:
    - **Username**: The username needed to launch this Playbook.
    - **Password**: The password needed to launch this Playbook.

Playbook Workflow Actions

Users may want to launch specific Playbooks from the Workflow Event Actions or Workflow Events, which are discussed further in the "The Search Screen" section of this document. To do so, click the **Playbooks** menu and select **Workflow Actions**. The **Workflow Actions** screen will be displayed, which is where users can view and edit the Workflow Actions they have created (Figure 14).

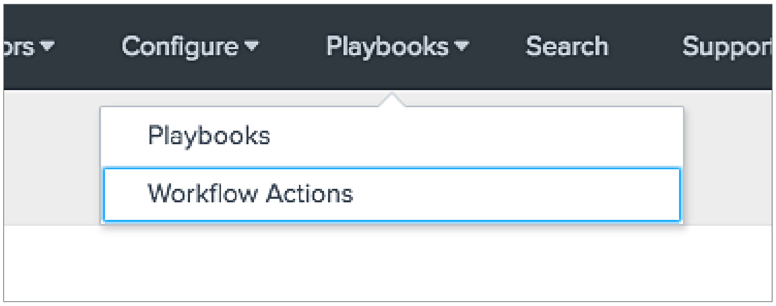
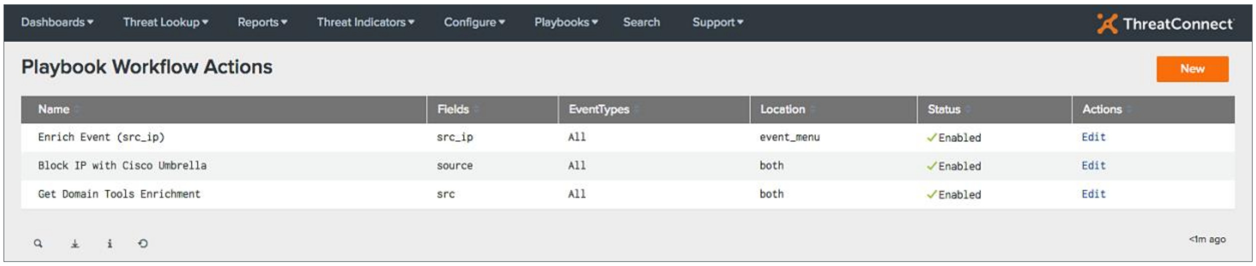


Figure 13

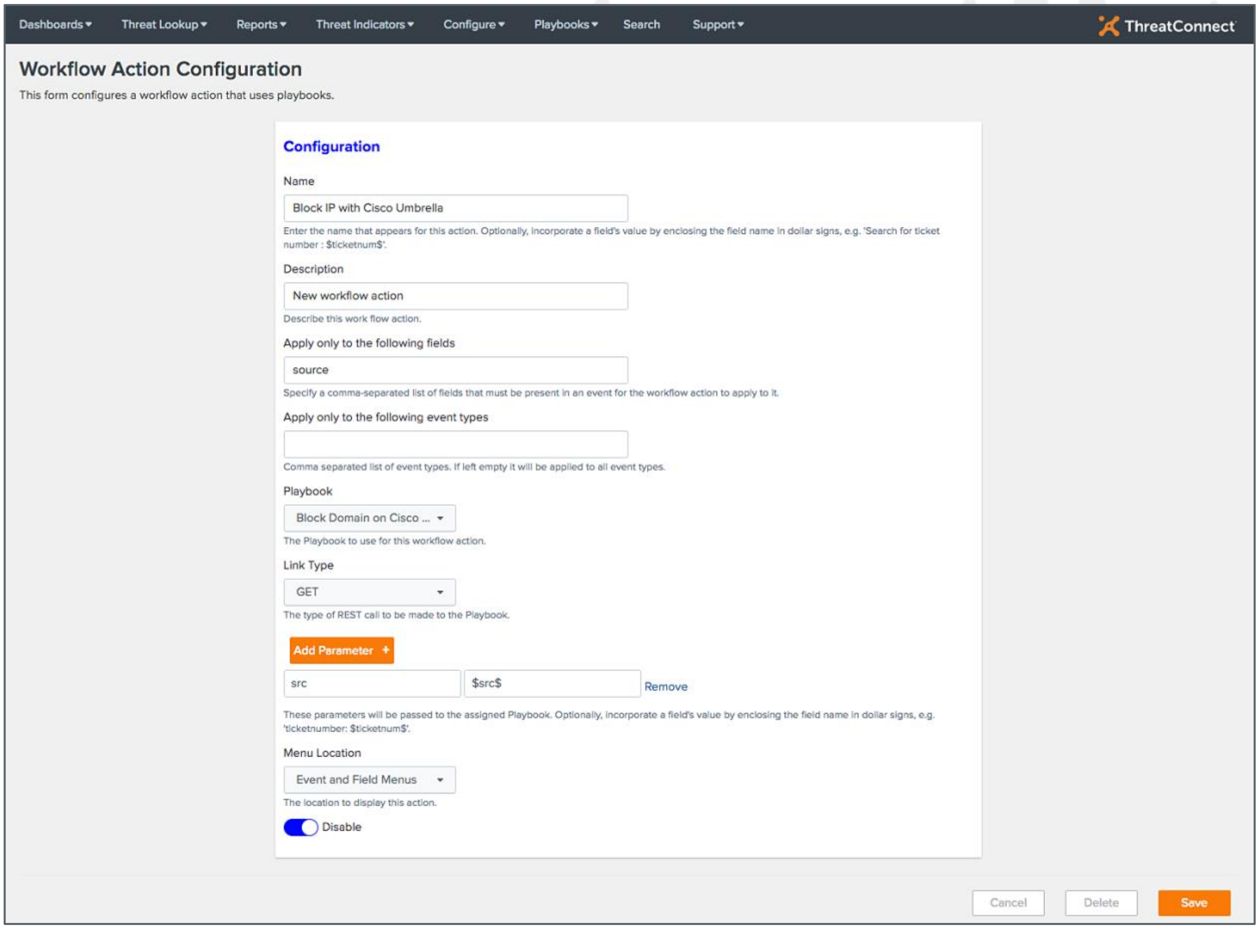


Playbook Workflow Actions

Name	Fields	EventTypes	Location	Status	Actions
Enrich Event (src_ip)	src_ip	All	event_menu	✓Enabled	Edit
Block IP with Cisco Umbrella	source	All	both	✓Enabled	Edit
Get Domain Tools Enrichment	src	All	both	✓Enabled	Edit

Figure 14

To view a specific Workflow Action configuration, click **Edit** in the **Actions** column. The **Workflow Action Configuration** screen will be displayed (Figure 16).



Workflow Action Configuration

This form configures a workflow action that uses playbooks.

Configuration

Name: Block IP with Cisco Umbrella

Enter the name that appears for this action. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'Search for ticket number : $ticketnum$'.

Description: New workflow action

Describe this work flow action.

Apply only to the following fields: source

Specify a comma-separated list of fields that must be present in an event for the workflow action to apply to it.

Apply only to the following event types:

Comma separated list of event types. If left empty it will be applied to all event types.

Playbook: Block Domain on Cisco ...

The Playbook to use for this workflow action.

Link Type: GET

The type of REST call to be made to the Playbook.

src: src

These parameters will be passed to the assigned Playbook. Optionally, incorporate a field's value by enclosing the field name in dollar signs, e.g. 'ticketnumber: $ticketnum$'.

Menu Location: Event and Field Menus

The location to display this action.

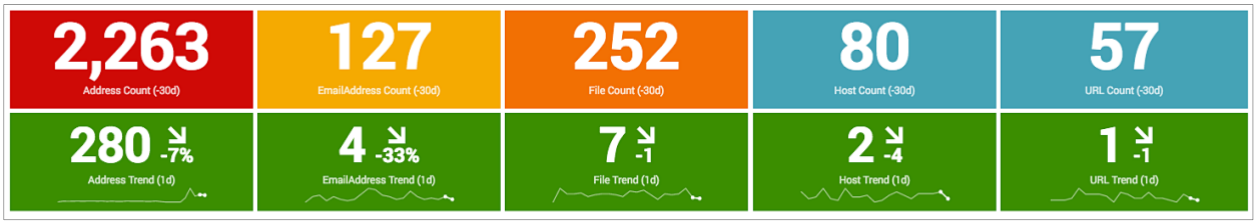
Disable

Figure 15

- **Name**: The name that is displayed for this Workflow Action. Optionally, incorporate the fields value by enclosing the field name in dollar signs (e.g., **Search for ticket number:$ticketnum$**).
- **Description**: The description of this Workflow Action.
- **Fields List**: A comma-separated list of fields that must be present in an event for a Workflow Action to apply to it.
- **Event Type List**: A comma-separated list of Event Types to which the Workflow Action will apply. If left empty, it will be applied to all Event Types.
- **Playbook**: The Playbook that will be launched for this Workflow Action. Only **Playbooks** that match the filter in the **Settings** screen will be displayed.
- **Link Type**: The type of REST call to be made to the Playbook.
- **Parameters**: The parameters that will be passed to the assigned Playbook. Optionally, incorporate a field value by enclosing the field name in dollar signs (e.g., **ticketnumber: $ticketnum$**').
- **Menu Location**: The location to display this Workflow Action.
- **Disable**: Toggle this slider on to disable the Playbook.

The ThreatConnect Dashboard

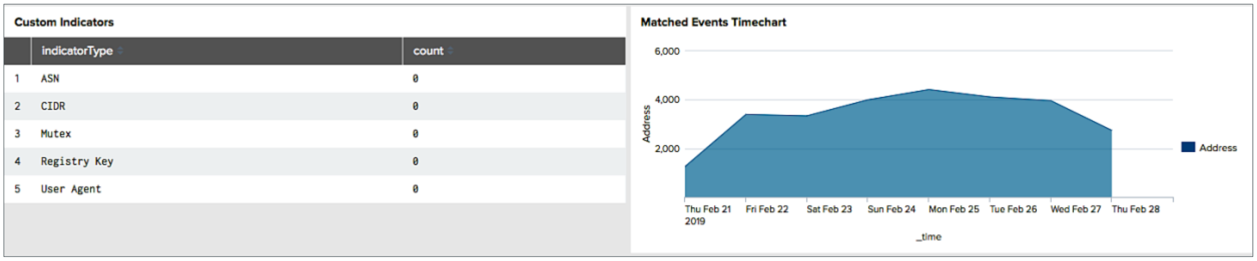
The **ThreatConnect** dashboard provides an overview of matches between events in Splunk and Indicator data in ThreatConnect. The first row of Single Value results provides a count of matched Indicators. The second row provides trending for the selected Time Period and Time Span. These Indicators are separated by type (Figure 16).



2,263 Address Count (-30d)	127 EmailAddress Count (-30d)	252 File Count (-30d)	80 Host Count (-30d)	57 URL Count (-30d)
280 ↘ -7% Address Trend (1d)	4 ↘ -33% EmailAddress Trend (1d)	7 ↘ -1 File Trend (1d)	2 ↘ -4 Host Trend (1d)	1 ↘ -1 URL Trend (1d)

Figure 16

The third row provides a table with Custom Indicator counts and a chart of event activity (Figure 17). This table includes the ASN, CIDR, Mutex, Registry Key, and User Agent standard Indicator types and any custom defined Indicator types with a count greater than zero. The chart will display all Indicator types with a non-zero value using a span defined in the Time Span input.



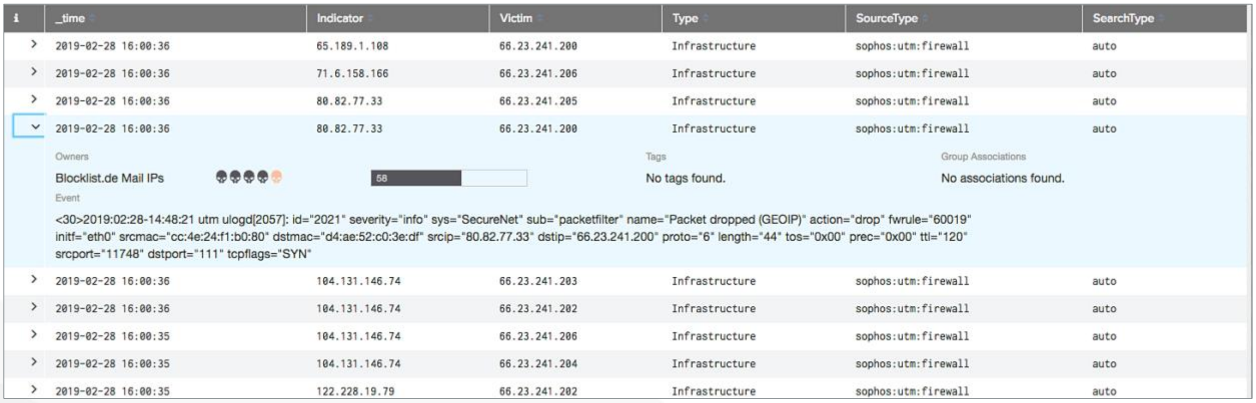
Custom Indicators

	indicatorType	count
1	ASN	0
2	CIDR	0
3	Mutex	0
4	Registry Key	0
5	User Agent	0

Matched Events Timechart

Figure 17

The view at the bottom displays the latest matched Indicators in a paginated table (Figure 18). This table has a built-in form that allows dynamic filtering on Indicator data. The table, by default, shows summary information for all the matched Indicators. Each row can be expanded to view more detailed data.



i	_time	Indicator	Victim	Type	SourceType	SearchType
>	2019-02-28 16:00:36	65.189.1.108	66.23.241.200	Infrastructure	sophos:utm:firewall	auto
>	2019-02-28 16:00:36	71.6.158.166	66.23.241.206	Infrastructure	sophos:utm:firewall	auto
>	2019-02-28 16:00:36	80.82.77.33	66.23.241.205	Infrastructure	sophos:utm:firewall	auto
⌄	2019-02-28 16:00:36	80.82.77.33	66.23.241.200	Infrastructure	sophos:utm:firewall	auto

Owners			Tags	Group Associations
Blocklist.de Mail IPs	●●●●○	58	No tags found.	No associations found.

Event

```
<30>2019:02:28-14:48:21 utm ulogd[2057]: id="2021" severity="info" sys="SecureNet" sub="packetfilter" name="Packet dropped (GEOIP)" action="drop" fwrule="60019"
initf="eth0" srcmac="cc:4e:24:f1:b0:80" dstmac="d4:ae:52:c0:3e:df" srcip="80.82.77.33" dstip="66.23.241.200" proto="6" length="44" tos="0x00" prec="0x00" ttl="120"
srcport="11748" dstport="111" tcpflags="SYN"
```

i	_time	Indicator	Victim	Type	SourceType	SearchType
>	2019-02-28 16:00:36	104.131.146.74	66.23.241.203	Infrastructure	sophos:utm:firewall	auto
>	2019-02-28 16:00:36	104.131.146.74	66.23.241.202	Infrastructure	sophos:utm:firewall	auto
>	2019-02-28 16:00:35	104.131.146.74	66.23.241.206	Infrastructure	sophos:utm:firewall	auto
>	2019-02-28 16:00:35	104.131.146.74	66.23.241.204	Infrastructure	sophos:utm:firewall	auto
>	2019-02-28 16:00:35	122.228.19.79	66.23.241.202	Infrastructure	sophos:utm:firewall	auto

Figure 18

- **_time:** This column is stored internally in UTC format. It is translated to human-readable UNIX® time format when Splunk renders the search results (the very last step of search-time event processing).
- **Indicator**: This column lists the Indicator that matched between local logs and ThreatConnect. This value is a hyperlink that will open a screen to the Indicator's **Details** screen in ThreatConnect.
- **Victim:** This column represents the bottom vertex of the Diamond Model. This value is determined by the user while setting up custom or Data Model searches.
- **Type:** This column specifies whether the Indicator is part of an Infrastructure or a Capability, as defined in the Diamond Model.
- **SourceType:** This column provides the sourcetype for the event for which the Indicators were matched.
- **Owners**: This section displays the Owners of the Indicator within ThreatConnect. Owners are typically a particular Source, Community, or an Organization (e.g., the Indicator belongs to the Owner's private Organization).
- **Rating (skulls)**: This value displays the Threat Rating assigned by the Indicator's owner within ThreatConnect. This value is on a scale of 0–5 skulls, with 5 being the most critical.
- **Confidence**: This value displays the Confidence Rating assigned by the Indicator's owner within ThreatConnect. This value is on a scale of 0–100.
- **Tags**: This column displays any Tags applied to the matched Indicator by the owner. If multiple owners exist for a matched Indicator, only Tags created by the owner listed in the same row will be displayed in this column.
- **Group Associations**: This column display any Groups associated with the matched Indicator by the owner.
- **Event**: This section shows the raw data for the matched event.

The Indicator Dashboard

The **Indicator** dashboard provides an additional view of the matched-Indicator data. This dashboard focuses on the groupings of the matched Indicators. The first row of this timeline view (Figure 19) displays matched Indicators by Owners. A dropdown option is available to narrow down the window of time for the results.

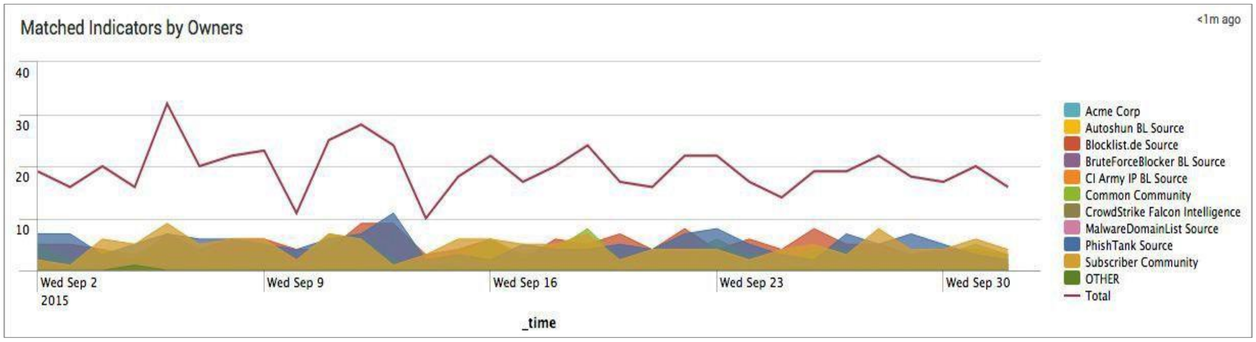
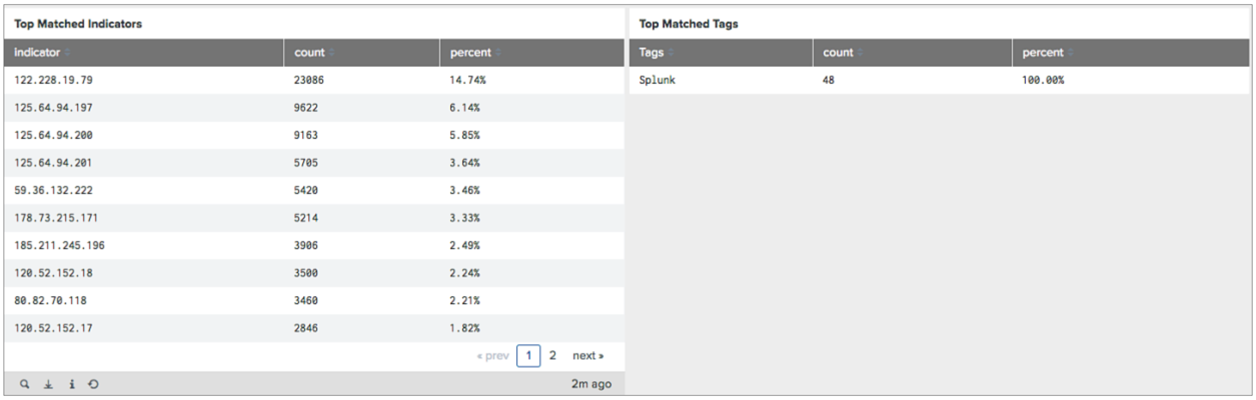


Figure 19

The second row displays additional paginated tables for matched Indicators (Figure 20). From left to right, these tables are for the top matched Indicators (with a count of times observed for each Indicator) and the top matched Tags.



Top Matched Indicators

indicator	count	percent
122.228.19.79	23086	14.74%
125.64.94.197	9622	6.14%
125.64.94.200	9163	5.85%
125.64.94.201	5705	3.64%
59.36.132.222	5420	3.46%
178.73.215.171	5214	3.33%
185.211.245.196	3906	2.49%
120.52.152.18	3500	2.24%
80.82.70.118	3460	2.21%
120.52.152.17	2846	1.82%

Top Matched Tags

Tags	count	percent
Splunk	48	100.00%

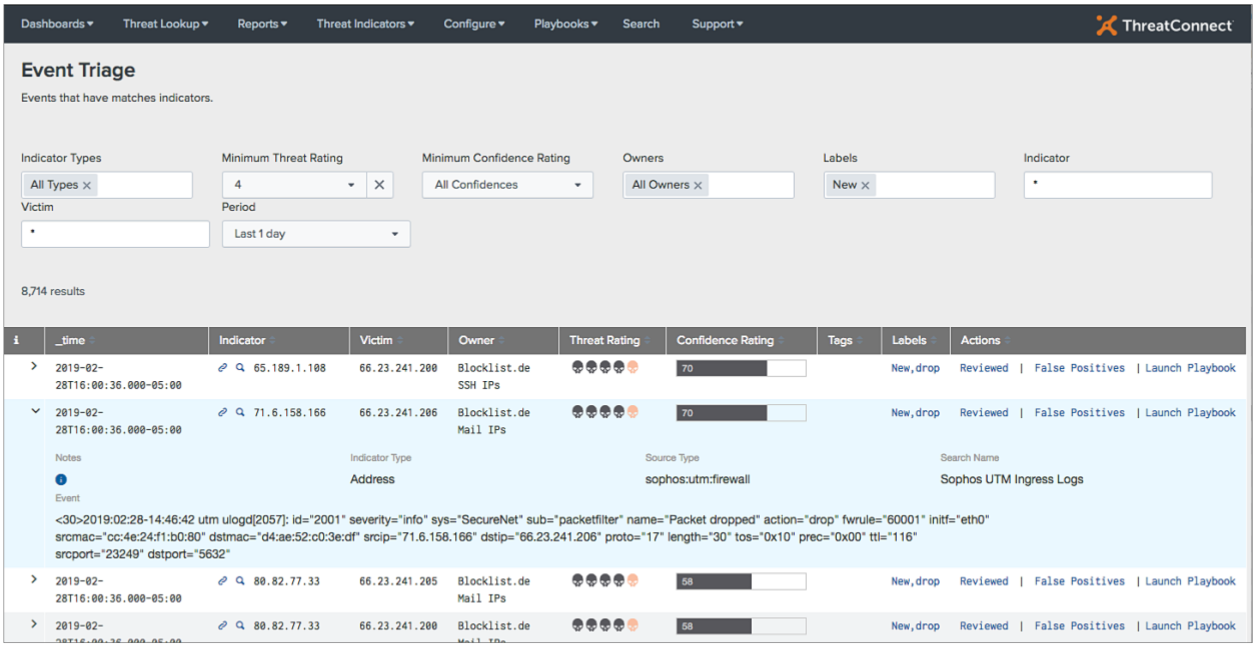
Figure 20

The Event Triage Dashboard

The **Event Triage** dashboard (Figure 21) allows users to view and filter all matched events and act on the events. The **Reviewed** and **False Positive** buttons at the bottom of the screen allow bulk action on Indicators, while the **Mark False Positive**, **Mark Reviewed**, and **Launch Playbook** buttons or links in each row allow action on a specific event.

When the **Mark False Positive** button or link is clicked, a **False Positive** label is added to the event and, if present, the **New** label is removed from the event in the Splunk KV Store, and a request is made to the ThreatConnect API to report a false positive for this Indicator. The user must have the **tc_user** role to update labels on events.

When the **Mark Reviewed** button or link is clicked, a **Reviewed** label is added to the event and, if present, the **New** label is removed from the event in the Splunk KV Store.



Event Triage

Events that have matches indicators.

Indicator Types: All Types ✕
Minimum Threat Rating: 4
Minimum Confidence Rating: All Confidences
Owners: All Owners ✕
Labels: New ✕
Indicator: *
Victim: *
Period: Last 1 day

8,714 results

i	_time	Indicator	Victim	Owner	Threat Rating	Confidence Rating	Tags	Labels	Actions
>	2019-02-28T16:00:36.000-05:00	65.189.1.108	66.23.241.200	Blocklist.de SSH IPs	●●●●○	70		New,drop	Reviewed | False Positives | Launch Playbook
⌄	2019-02-28T16:00:36.000-05:00	71.6.158.166	66.23.241.206	Blocklist.de Mail IPs	●●●●○	70		New,drop	Reviewed | False Positives | Launch Playbook

Notes: ●
Indicator Type: Address
Source Type: sophos:utm:firewall
Search Name: Sophos UTM Ingress Logs

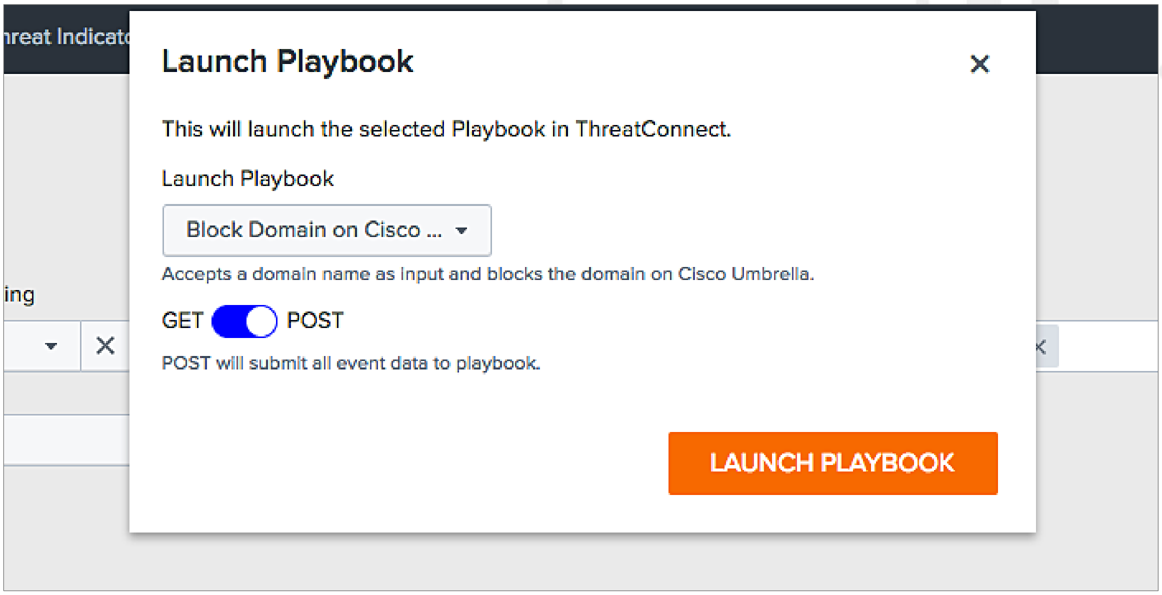
Event

```
<30>2019:02:28-14:46:42 utm ulogd[2057]: id="2001" severity="info" sys="SecureNet" sub="packetfilter" name="Packet dropped" action="drop" fwrule="60001" initf="eth0"
srcmac="cc:4e:24:f1:b0:80" dstmac="d4:ae:52:c0:3e:df" srcip="71.6.158.166" dstip="66.23.241.206" proto="17" length="30" tos="0x10" prec="0x00" ttl="116"
srcport="23249" dstport="5632"
```

i	_time	Indicator	Victim	Owner	Threat Rating	Confidence Rating	Tags	Labels	Actions
>	2019-02-28T16:00:36.000-05:00	80.82.77.33	66.23.241.205	Blocklist.de Mail IPs	●●●●○	58		New,drop	Reviewed | False Positives | Launch Playbook
>	2019-02-	80.82.77.33	66.23.241.200	Blocklist.de	●●●●○	58		New,drop	Reviewed | False Positives | Launch Playbook

Figure 21

If there are any configured Playbooks in your system that can be launched (view the “Playbooks” section for additional information), then the **Launch Playbook** button or link will be displayed for events. When this button or link is clicked, the **Launch Playbook** window will be displayed (Figure 22).



This will launch the selected Playbook in ThreatConnect.

Launch Playbook: Block Domain on Cisco ...

Accepts a domain name as input and blocks the domain on Cisco Umbrella.

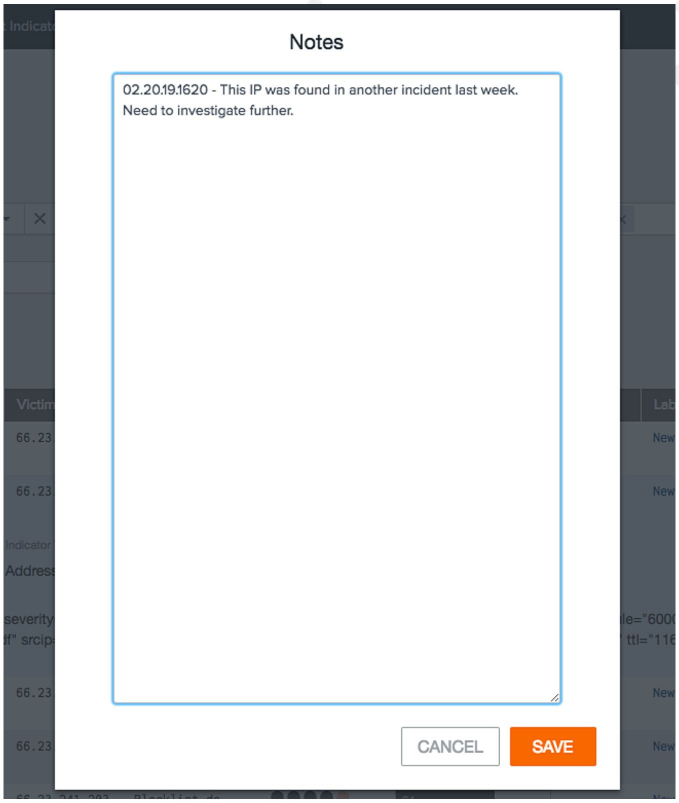
GET POST

POST will submit all event data to playbook.

Figure 22

- **Launch Playbook**: This dropdown menu provides a list of available Playbooks to be launched. . Only Playbooks that match the filter in the Settings screen will be displayed.
- **GET/POST Slider**: Toggle this slider to **GET** or **POST** to indicate that the Playbook will perform a GET or POST request, respectively. If the data in the event are parsable, then users will be able to perform either a GET request, through which they specify the fields to be sent to the Playbook, or a POST request, through which all the fields present in the event are sent to the Playbook.
- Click the **LAUNCH PLAYBOOK** button. A new window will open that displays the return value of the selected Playbook.

To add a comment on a matched event, click the **Notes** icon in the table row expansion (Figure 21). The **Notes** window will be displayed (Figure 23).



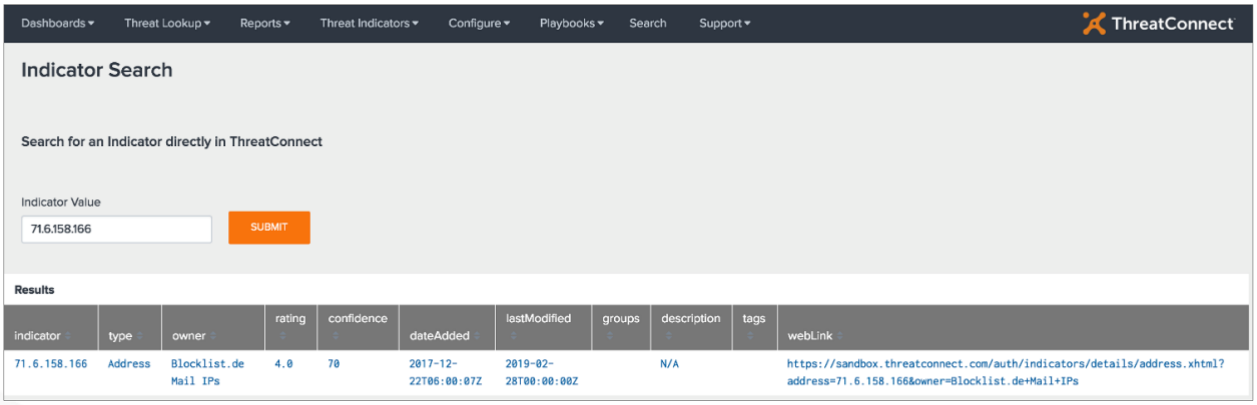
02.20.19.1620 - This IP was found in another incident last week. Need to investigate further.

Figure 23

The **Indicator** column has two links in the form of icons. The first link redirects the user to the Indicator's **Details** screen in ThreatConnect. The second link redirects the user to the **Indicator Review** dashboard to view the Indicator's details.

The Indicator Search Screen

The **Indicator Search** screen allows manual lookup of Indicators against the ThreatConnect API (Figure 24). The Indicator type is automatically detected.



Indicator Search

Search for an Indicator directly in ThreatConnect

Indicator Value: 71.6.158.166

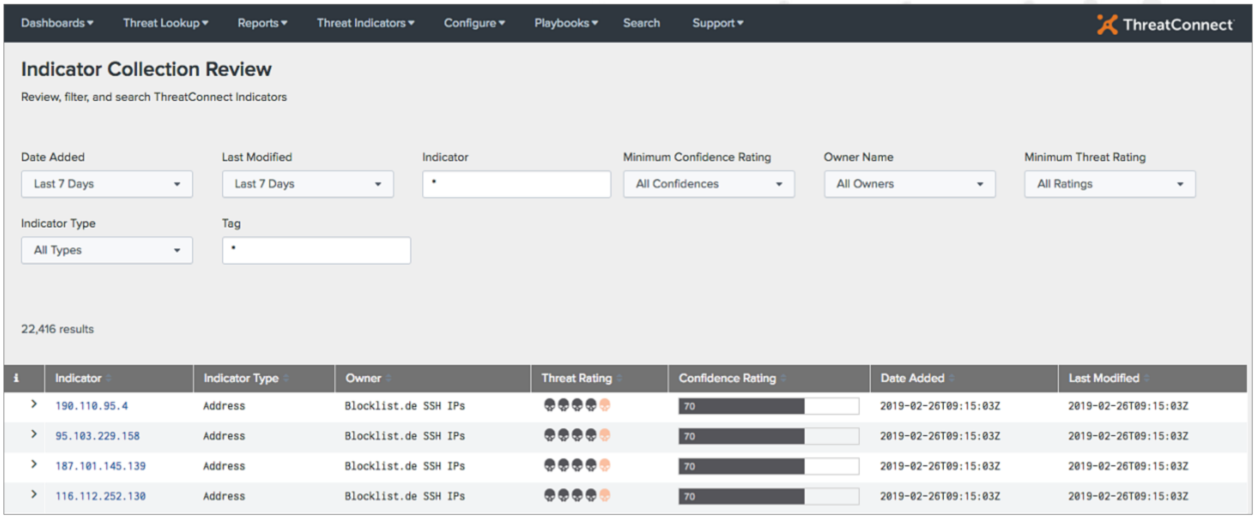
Results

indicator	type	owner	rating	confidence	dateAdded	lastModified	groups	description	tags	webLink
71.6.158.166	Address	Blocklist.de Mail IPs	4.0	70	2017-12-22T06:00:07Z	2019-02-28T00:00:00Z		N/A		https://sandbox.threatconnect.com/auth/indicators/details/address.xhtml?address=71.6.158.166&owner=Blocklist.de+Mail+IPs

Figure 24

The Indicator Review Dashboard

The **Indicator Review** dashboard allows users to search for and filter Indicators (Figure 25).



Indicator Collection Review

Review, filter, and search ThreatConnect Indicators

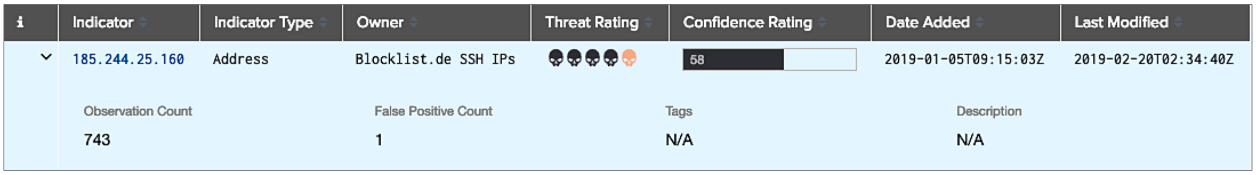
Date Added: Last 7 Days
Last Modified: Last 7 Days
Indicator: *
Minimum Confidence Rating: All Confidences
Owner Name: All Owners
Minimum Threat Rating: All Ratings
Indicator Type: All Types
Tag: *

22,416 results

i	Indicator	Indicator Type	Owner	Threat Rating	Confidence Rating	Date Added	Last Modified
›	190.110.95.4	Address	Blocklist.de SSH IPs	●●●●○	70	2019-02-26T09:15:03Z	2019-02-26T09:15:03Z
›	95.103.229.158	Address	Blocklist.de SSH IPs	●●●●○	70	2019-02-26T09:15:03Z	2019-02-26T09:15:03Z
›	187.101.145.139	Address	Blocklist.de SSH IPs	●●●●○	70	2019-02-26T09:15:03Z	2019-02-26T09:15:03Z
›	116.112.252.130	Address	Blocklist.de SSH IPs	●●●●○	70	2019-02-26T09:15:03Z	2019-02-26T09:15:03Z

Figure 25

Each Indicator record expands and displays additional Indicator information, in real time, retrieved directly from the ThreatConnect API (Figure 26).



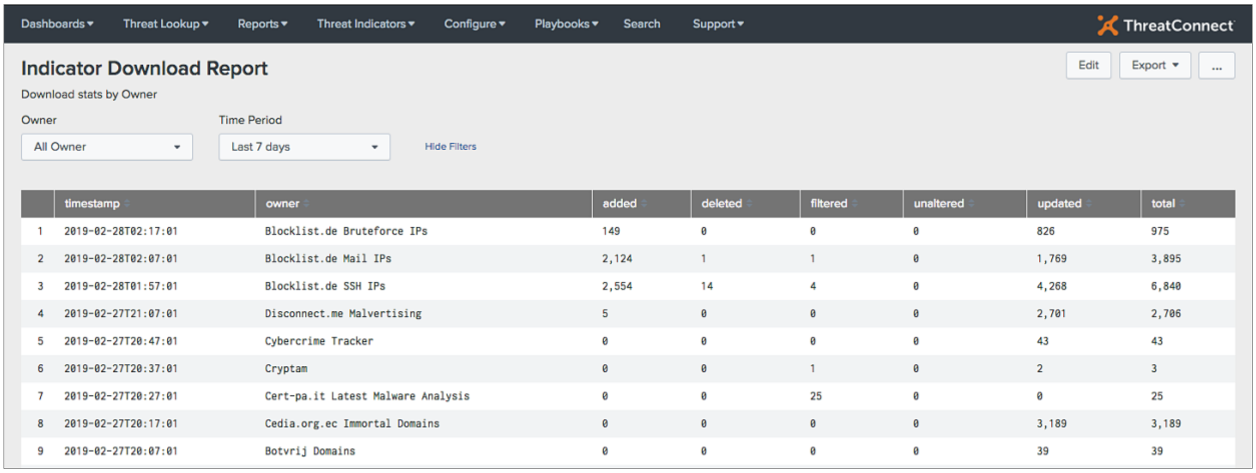
i	Indicator	Indicator Type	Owner	Threat Rating	Confidence Rating	Date Added	Last Modified
⌄	185.244.25.160	Address	Blocklist.de SSH IPs	●●●●○	58	2019-01-05T09:15:03Z	2019-02-20T02:34:40Z

Observation Count	False Positive Count	Tags	Description
743	1	N/A	N/A

Figure 26

The Threat Indicator Download Report Screen

The **Threat Indicator Download Report** screen is used to create reports for monitoring ThreatConnect Alert queries and for tracking how many of those queries hit the ThreatConnect API (Figure 27). User-defined custom reports can be added for more detailed views into the ThreatConnect data.



Indicator Download Report

Download stats by Owner

Owner: All Owner

Time Period: Last 7 days

	timestamp	owner	added	deleted	filtered	unaltered	updated	total
1	2019-02-28T02:17:01	Blocklist.de Bruteforce IPs	149	0	0	0	826	975
2	2019-02-28T02:07:01	Blocklist.de Mail IPs	2,124	1	1	0	1,769	3,895
3	2019-02-28T01:57:01	Blocklist.de SSH IPs	2,554	14	4	0	4,268	6,840
4	2019-02-27T21:07:01	Disconnect.me Malvertising	5	0	0	0	2,701	2,706
5	2019-02-27T20:47:01	Cybercrime Tracker	0	0	0	0	43	43
6	2019-02-27T20:37:01	Cryptam	0	0	1	0	2	3
7	2019-02-27T20:27:01	Cert-pa.it Latest Malware Analysis	0	0	25	0	0	25
8	2019-02-27T20:17:01	Cedia.org.ec Immortal Domains	0	0	0	0	3,189	3,189
9	2019-02-27T20:07:01	Botvrij Domains	0	0	0	0	39	39

Figure 27

The Threat Indicators Menu

The **Threat Indicators** menu provides additional screens containing statistics for each ThreatConnect Indicator type, independent of matches to events or logs within Splunk. The screens are formatted similarly, and one screen exists for each Indicator type.

The first row in the screen displays graphical representations for the total number of Indicators from ThreatConnect of the specified type (Figure 28). There are two charts: one for Indicator type by owner and another for Indicator type by rating.

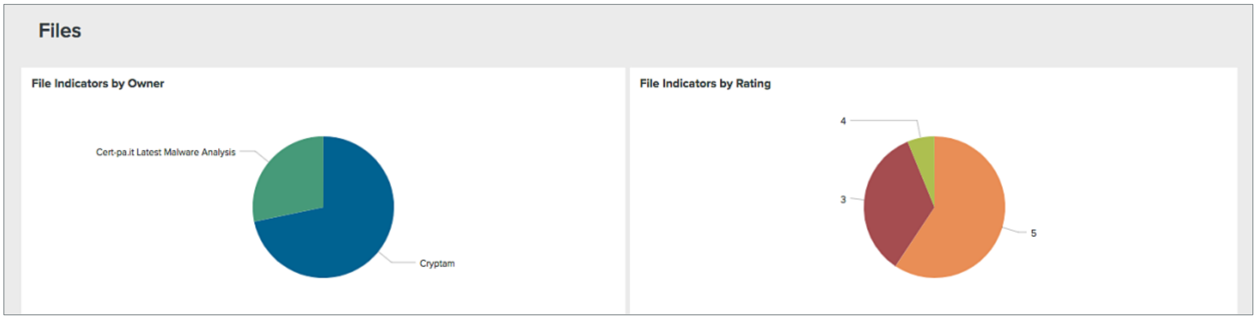
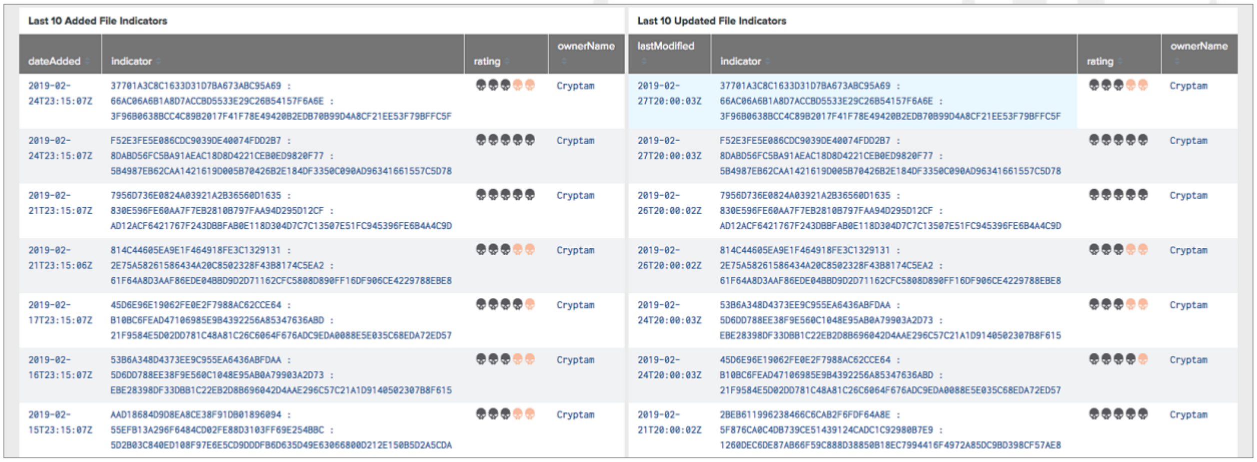


Figure 28

The second row contains two tables that display the last 10 created and updated Indicators, respectively (Figure 29).



Last 10 Added File Indicators

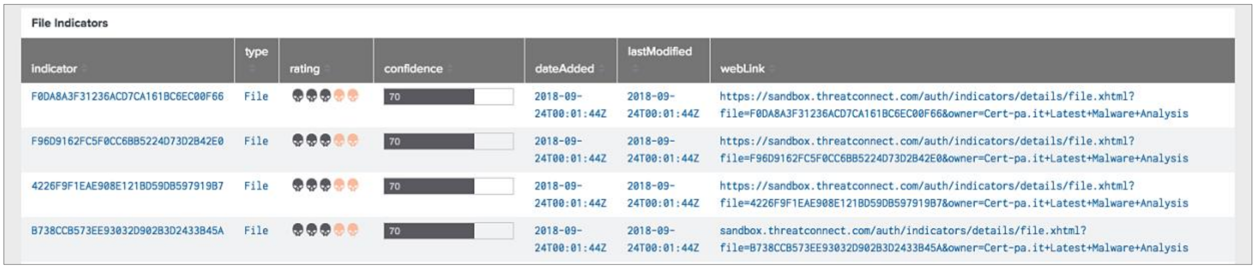
dateAdded	indicator	rating	ownerName
2019-02-24T23:15:07Z	37701A3C8C1633D31D7BA673ABC95A69 : 66AC06A6B1A8D7ACCBD5533E29C26B54157F6A6E : 3F96B0638BCC4C89B2017F41F78E49420B2EDB70B99D4A8CF21EE53F79BFFC5F	●●●○○	Cryptam
2019-02-24T23:15:07Z	F52E3FE5E086CDC9039DE40074FDD2B7 : 8DABD56FC5BA91AEAC18D8D4221CEB0ED9820F77 : 5B4987EB62CAA1421619D005B70426B2E184DF3350C090AD96341661557C5D78	●●●●●	Cryptam
2019-02-21T23:15:07Z	7956D736E0824A03921A2B36560D1635 : 830E596FE60AA7F7EB2810B797FAA94D295D12CF : AD12ACF6421767F243DBBFAB0E118D304D7C7C13507E51FC945396FE6B4A4C9D	●●●●●	Cryptam
2019-02-21T23:15:06Z	814C44605EA9E1F464918FE3C1329131 : 2E75A58261586434A20C8502328F43B8174C5EA2 : 61F64A8D3AAF86EDE04BBD9D2D71162CFC5808D890FF16DF906CE4229788EBE8	●●●○○	Cryptam
2019-02-17T23:15:07Z	45D6E96E19062FE0E2F7988AC62CCE64 : B10BC6FEAD47106985E9B4392256A85347636ABD : 21F9584E5D02DD781C48A81C26C6064F676ADC9EDA0088E5E035C68EDA72ED57	●●●●○	Cryptam
2019-02-16T23:15:07Z	53B6A348D4373EE9C955EA6436ABFDAA : 5D6DD788EE38F9E560C1048E95AB0A79903A2D73 : EBE28398DF33DBB1C22EB2D8B696042D4AAE296C57C21A1D9140502307B8F615	●●●○○	Cryptam
2019-02-15T23:15:07Z	AAD18684D9D8EA8CE38F91DB01896094 : 55EFB13A296F6484CD02FE88D3103FF69E254BBC : 5D2B03C840ED108F97E6E5CD9DDDFB6D635D49E63066800D212E150B5D2A5CDA	●●●○○	Cryptam

Last 10 Updated File Indicators

lastModified	indicator	rating	ownerName
2019-02-27T20:00:03Z	37701A3C8C1633D31D7BA673ABC95A69 : 66AC06A6B1A8D7ACCBD5533E29C26B54157F6A6E : 3F96B0638BCC4C89B2017F41F78E49420B2EDB70B99D4A8CF21EE53F79BFFC5F	●●●○○	Cryptam
2019-02-27T20:00:03Z	F52E3FE5E086CDC9039DE40074FDD2B7 : 8DABD56FC5BA91AEAC18D8D4221CEB0ED9820F77 : 5B4987EB62CAA1421619D005B70426B2E184DF3350C090AD96341661557C5D78	●●●●●	Cryptam
2019-02-26T20:00:02Z	7956D736E0824A03921A2B36560D1635 : 830E596FE60AA7F7EB2810B797FAA94D295D12CF : AD12ACF6421767F243DBBFAB0E118D304D7C7C13507E51FC945396FE6B4A4C9D	●●●●●	Cryptam
2019-02-26T20:00:02Z	814C44605EA9E1F464918FE3C1329131 : 2E75A58261586434A20C8502328F43B8174C5EA2 : 61F64A8D3AAF86EDE04BBD9D2D71162CFC5808D890FF16DF906CE4229788EBE8	●●●○○	Cryptam
2019-02-24T20:00:03Z	53B6A348D4373EE9C955EA6436ABFDAA : 5D6DD788EE38F9E560C1048E95AB0A79903A2D73 : EBE28398DF33DBB1C22EB2D8B696042D4AAE296C57C21A1D9140502307B8F615	●●●○○	Cryptam
2019-02-24T20:00:03Z	45D6E96E19062FE0E2F7988AC62CCE64 : B10BC6FEAD47106985E9B4392256A85347636ABD : 21F9584E5D02DD781C48A81C26C6064F676ADC9EDA0088E5E035C68EDA72ED57	●●●●○	Cryptam
2019-02-21T20:00:02Z	2BEB611996238466C6CAB2F6FDF64A8E : 5F876CA0C4DB739CE51439124CADC1C92980B7E9 : 1260DEC6DE87AB66F59C888D38850B18EC7994416F4972A85DC9BD398CF57AE8	●●●●●	Cryptam

Figure 29

The final row displays a paginated table of all the Indicators of that type pulled from ThreatConnect (Figure 30).



File Indicators

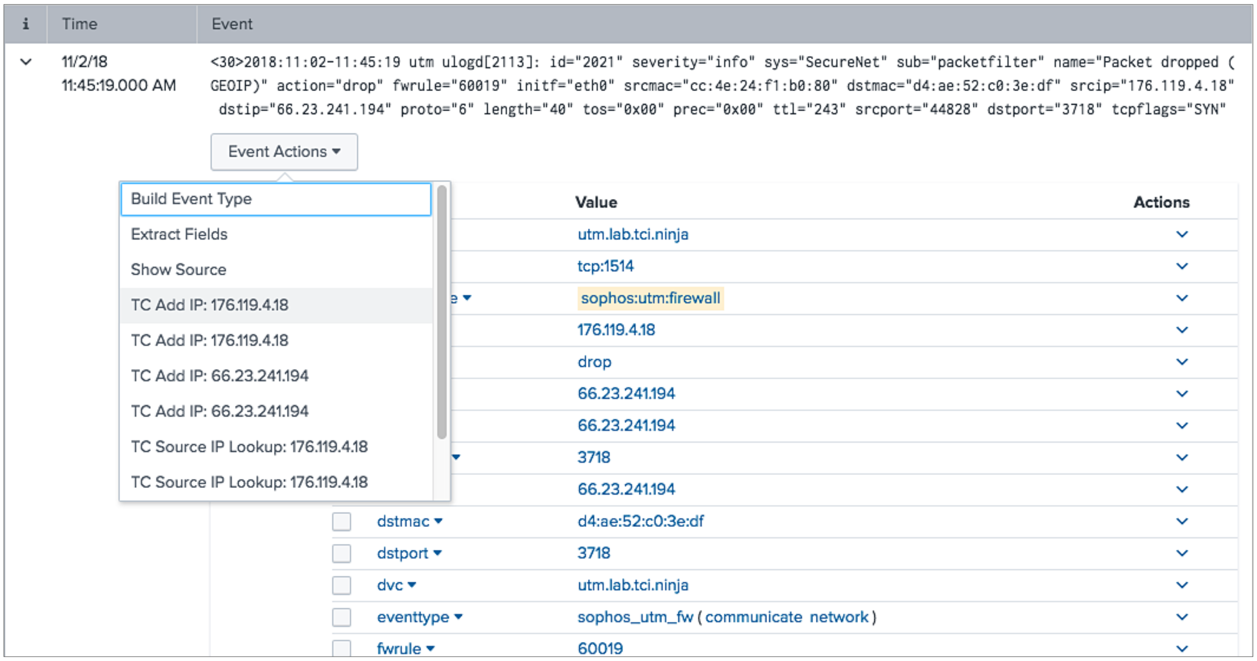
indicator	type	rating	confidence	dateAdded	lastModified	webLink
F0DA8A3F31236ACD7CA161BC6EC00F66	File	●●●○○	70	2018-09-24T00:01:44Z	2018-09-24T00:01:44Z	https://sandbox.threatconnect.com/auth/indicators/details/file.xhtml?file=F0DA8A3F31236ACD7CA161BC6EC00F66&owner=Cert-pa.it+Latest+Malware+Analysis
F96D9162FC5F0CC6BB5224D73D2B42E0	File	●●●○○	70	2018-09-24T00:01:44Z	2018-09-24T00:01:44Z	https://sandbox.threatconnect.com/auth/indicators/details/file.xhtml?file=F96D9162FC5F0CC6BB5224D73D2B42E0&owner=Cert-pa.it+Latest+Malware+Analysis
4226F9F1EAE908E121BD59DB597919B7	File	●●●○○	70	2018-09-24T00:01:44Z	2018-09-24T00:01:44Z	https://sandbox.threatconnect.com/auth/indicators/details/file.xhtml?file=4226F9F1EAE908E121BD59DB597919B7&owner=Cert-pa.it+Latest+Malware+Analysis
B738CCB573EE93032D902B3D2433B45A	File	●●●○○	70	2018-09-24T00:01:44Z	2018-09-24T00:01:44Z	sandbox.threatconnect.com/auth/indicators/details/file.xhtml?file=B738CCB573EE93032D902B3D2433B45A&owner=Cert-pa.it+Latest+Malware+Analysis

Figure 30

The Search Screen

Workflow: Event Actions

Using the **Search** screen while in the ThreatConnect App enables one to access additional features for threat analysis. The built-in Splunk **Event Actions** feature will display multiple links for any Indicator field that follows the CIM standard naming convention (Figure 31).



i	Time	Event
⌄	11/2/18 11:45:19.000 AM	`<30>2018:11:02-11:45:19 utm ulogd[2113]: id="2021" severity="info" sys="SecureNet" sub="packetfilter" name="Packet dropped (GEOIP)" action="drop" fwrule="60019" initf="eth0" srcmac="cc:4e:24:f1:b0:80" dstmac="d4:ae:52:c0:3e:df" srcip="176.119.4.18" dstip="66.23.241.194" proto="6" length="40" tos="0x00" prec="0x00" ttl="243" srcport="44828" dstport="3718" tcpflags="SYN"`

		Value	Actions
		utm.lab.tci.ninja	⌄
		tcp:1514	⌄
	e ▾	sophos:utm:firewall	⌄
		176.119.4.18	⌄
		drop	⌄
		66.23.241.194	⌄
		66.23.241.194	⌄
	▾	3718	⌄
		66.23.241.194	⌄
□	dstmac ▾	d4:ae:52:c0:3e:df	⌄
□	dstport ▾	3718	⌄
□	dvc ▾	utm.lab.tci.ninja	⌄
□	eventtype ▾	sophos_utm_fw (communicate network)	⌄
□	fwrule ▾	60019	⌄

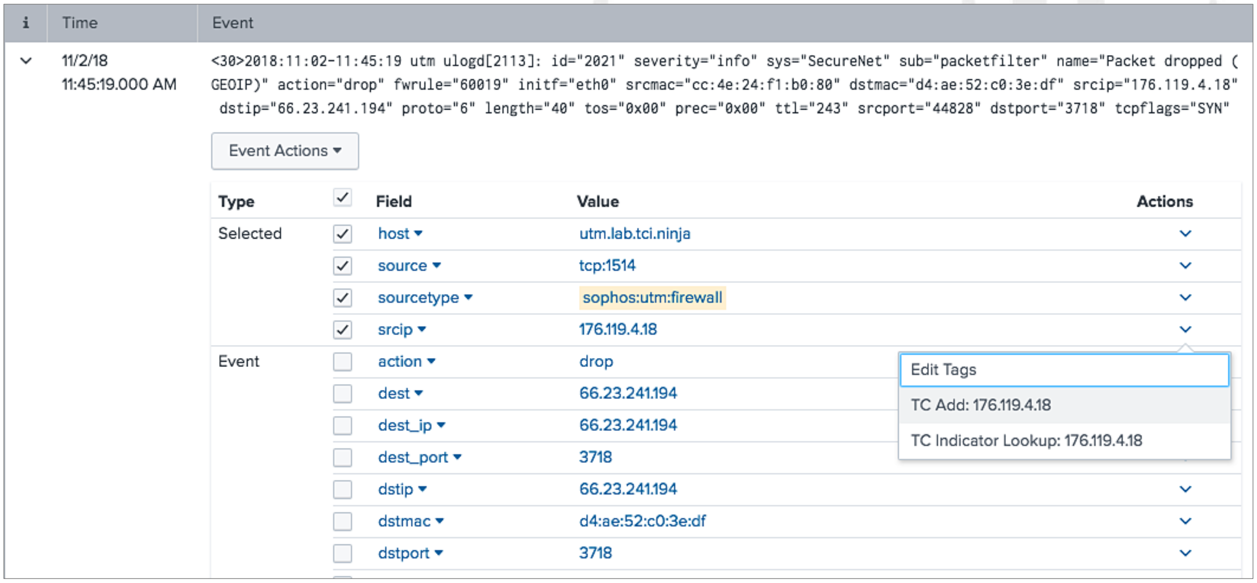
Figure 31

The **Workflow** actions provided by the App are **TC Add** and **TC Lookup**:

- The **TC Add** action will open a new browser tab and allow the user to select the appropriate metadata before submitting the Indicator to ThreatConnect.
- The **TC Lookup** action will perform an API query to see if the Indicator is known to ThreatConnect.

Workflow: Field Actions

If the results fields do not follow the CIM naming convention, the **Workflow** actions are still available via the **Actions** menu for a given field, which supports only the **TC Add** and **TC Indicator Lookup** Workflow actions (Figure 32).



i	Time	Event
⌄	11/2/18 11:45:19.000 AM	`<30>2018:11:02-11:45:19 utm ulogd[2113]: id="2021" severity="info" sys="SecureNet" sub="packetfilter" name="Packet dropped (GEOIP)" action="drop" fwrule="60019" initf="eth0" srcmac="cc:4e:24:f1:b0:80" dstmac="d4:ae:52:c0:3e:df" srcip="176.119.4.18" dstip="66.23.241.194" proto="6" length="40" tos="0x00" prec="0x00" ttl="243" srcport="44828" dstport="3718" tcpflags="SYN"`

Type	☑	Field	Value	Actions
Selected	☑	host ▾	utm.lab.tci.ninja	⌄
	☑	source ▾	tcp:1514	⌄
	☑	sourcetype ▾	sophos:utm:firewall	⌄
	☑	srcip ▾	176.119.4.18	⌄
Event	□	action ▾	drop	
	□	dest ▾	66.23.241.194	
	□	dest_ip ▾	66.23.241.194	
	□	dest_port ▾	3718	
	□	dstip ▾	66.23.241.194	⌄
	□	dstmac ▾	d4:ae:52:c0:3e:df	⌄
	□	dstport ▾	3718	⌄

Figure 32

The ThreatConnect App for Splunk Data

All of the ThreatConnect App for Splunk data are stored in the Splunk KV Store and are available via predefined lookups using the `inputlookup` Splunk command. To view a list of available lookup definitions, navigate to **Settings** > **Lookups** > **Lookup Definitions**, and select **ThreatConnect** from the **App Context** dropdown menu.

Enterprise Security Integration

The latest version of the ThreatConnect App for Splunk provides support for Workflow Actions in Enterprise Security, invoking ThreatConnect Playbooks on notable events via Adaptive Responses, ingestion of Indicators into Splunk Enterprise Security.

Ingesting Indicators

The ThreatConnect App for Splunk provides five saved searches configured to run once daily. These saved searches generate Comma-Separated Values (CSV) files that can be ingested into Splunk Enterprise Security. To configure these Indicators for ingestion, navigate to **Configure** > **Data Enrichment** > **Threat Intelligence Downloads** in the Enterprise Security App. Splunk packages contain a local list for each Indicator type (e.g., `local_domain_intel`, `local_email_intel`, `local_file_intel`, `local_http_intel`, and `local_ip_intel`). Click the **Clone** link on the far right of the row to create a new intelligence download using the Splunk CSV files. See the following mapping to determine which lookup to use:

- local_domain_intel > lookup://threatconnect_domain_indicators
- local_email_intel > lookup://threatconnect_email_indicators
- local_file_intel > lookup://threatconnect_file_indicators
- local_http_intel > lookup://threatconnect_http_indicators

- local_ip_intel > lookup://threatconnect_ip_indicators

Splunk Enterprise Security Adaptive Response with Playbook

The **Send Event to ThreatConnect Playbook** Adaptive Response can be used to send notable event data to a ThreatConnect Playbook. Splunk Enterprise Security Adaptive Response actions can now trigger a ThreatConnect Playbook using manual or automated actions.

Send Notable Event Data to Playbook with Ad Hoc Adaptive Response

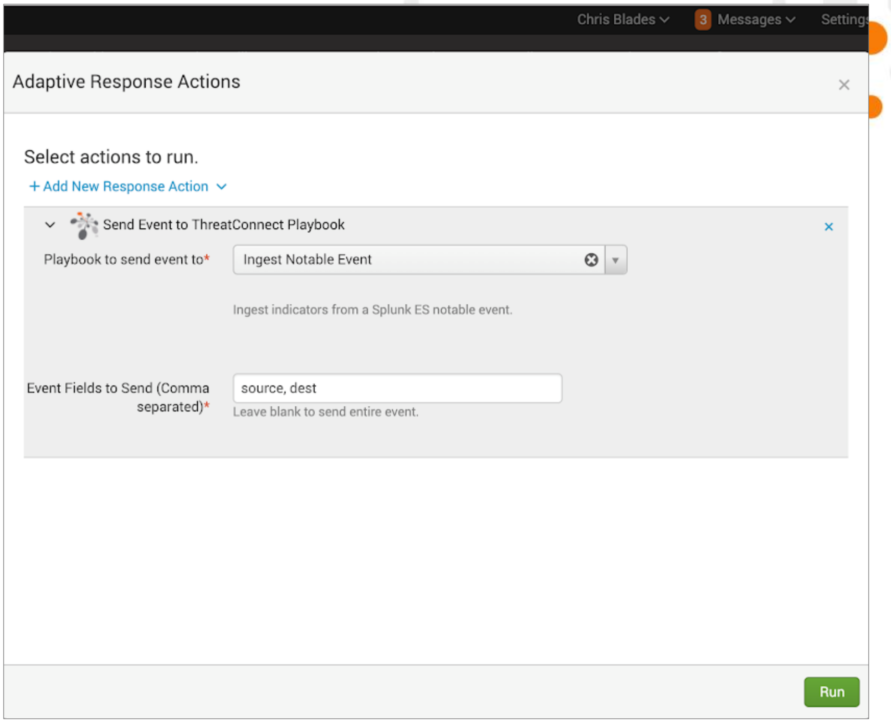
From the **Incident Review** screen of the Splunk Enterprise Security application, choose **Run Adaptive Response** from the **Actions** menu of any notable event. In the **Adaptive Response Actions** dialog, click **+ Add New Response Action,** and from the resulting menu select **Send Event to ThreatConnect Playbook**.

Automatically Send Notable Event Data to Playbook with Adaptive Response

While editing any Correlation Search, click **+ Add New Response Action**, and from the resulting menu select **Send Event to ThreatConnect Playbook**.

Configuring the Send Event to ThreatConnect Playbook Adaptive Response

The **Send Event to Playbook** dropdown selects the Playbook that will receive the notable event data. Only Playbooks that match the filter in the **Settings** screen will be displayed. It is populated with Playbooks from the **Playbooks** screen in ThreatConnect. If the selected Playbook requires authentication, credentials must be configured from the **Playbooks** screen in the ThreatConnect. When a Playbook is selected, its description will be displayed (Figure 33).



Adaptive Response Actions

Select actions to run.

+ Add New Response Action

Send Event to ThreatConnect Playbook

Playbook to send event to*: Ingest Notable Event

Ingest indicators from a Splunk ES notable event.

Event Fields to Send (Comma separated)*: source, dest

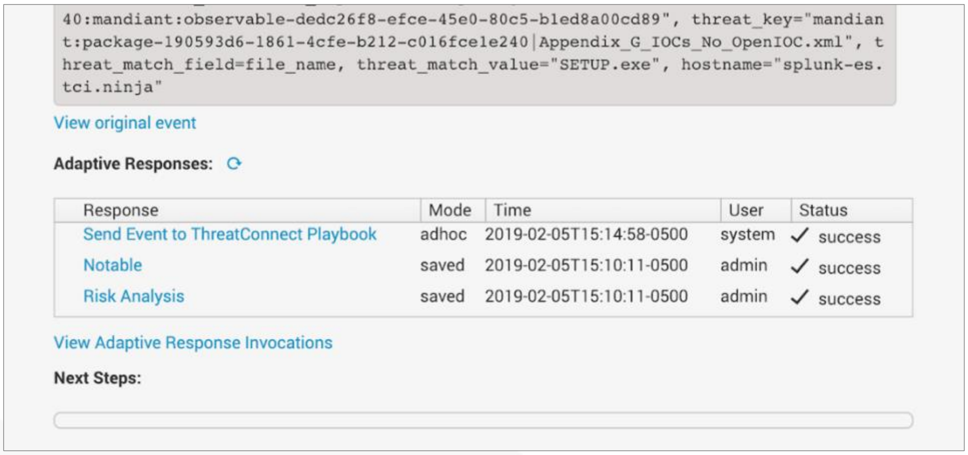
Leave blank to send entire event.

Figure 33

The **Event fields to send** input allows users to define which fields from the notable event are submitted to the Playbook. If left empty, all notable event data will be sent.

Viewing Responses from the Send Event to ThreatConnect Playbook Adaptive Response

From the **Incident Review** screen of the Splunk Enterprise Security application, expand a notable event on which the **Send Event to ThreatConnect Playbook** Adaptive Response has been invoked. Under the **Adaptive Responses** section, click **Send Event to ThreatConnect Playbook** to view the result of the Adaptive Response (Figure **34**).



```
40:mandiant:observable-dedc26f8-efce-45e0-80c5-bled8a00cd89", threat_key="mandian
t:package-190593d6-1861-4cfe-b212-c016fcele240|Appendix_G_IOCs_No_OpenIOC.xml", t
hreat_match_field=file_name, threat_match_value="SETUP.exe", hostname="splunk-es.
tci.ninja"
```

Adaptive Responses:

Response	Mode	Time	User	Status
Send Event to ThreatConnect Playbook	adhoc	2019-02-05T15:14:58-0500	system	✓ success
Notable	saved	2019-02-05T15:10:11-0500	admin	✓ success
Risk Analysis	saved	2019-02-05T15:10:11-0500	admin	✓ success

Next Steps:

Figure 34

KV Store (Collection) Index

Collection	Description	Read Permission	Write Permission
tc_custom_search_settings	The collection stores the configuration for custom searches.	admin, tc_admin, tc_user	admin, tc_admin
tc_db_stats	This collection stores the stats on the current Indicator counts by Type and Owner.	admin, tc_admin, tc_user	admin, tc_admin, tc_user
tc_dm_data	This collection stores the Data Model name, objects, and fields for quick access in forms.	admin, tc_admin, tc_user	admin, tc_admin
tc_dm_search_settings	This collection stores the configuration for Data Model searches.	admin, tc_admin, tc_user	admin, tc_admin
tc_download_stats	This collection stores the download Indicator statistics.	admin, tc_admin, tc_user	admin, tc_admin, tc_user
tc_event_summaries	This collection stores the matched event-summary data.	admin, tc_admin, tc_user	admin, tc_admin, tc_user
tc_events (legacy)	This collection stores the matched event-summary data.	admin, tc_admin, tc_user	admin, tc_admin, tc_user
tc_events_data (legacy)	This collection stores the matched event-detail data.	admin, tc_admin, tc_user	admin, tc_admin, tc_user
tc_groups	This collection stores the Group data download from ThreatConnect.	admin, tc_admin, tc_user	admin, tc_admin, tc_user

tc_indicators	This collection stores the Indicator data downloaded from ThreatConnect.	admin, tc_admin, tc_user	admin, tc_admin, tc_user
tc_observations	This collection stores the temporary observation data.	admin, tc_admin, tc_user	admin, tc_admin
tc_owners	This collection stores the Indicator download configuration for each Owner.	admin, tc_admin, tc_user	admin, tc_admin
tc_settings	This collection stores App configuration.	admin, tc_admin, tc_user	admin, tc_admin
tc_victim_whitelist	This collection stores the Victim Whitelist configuration.	admin, tc_admin, tc_user	admin, tc_admin
tc_indicator_whitelist	This collection stores the Indicator Whitelist configuration.	admin, tc_admin, tc_user	admin, tc_admin

Application Command Index

Command	Description	Read Permission	Write Permission
tcaddindicator	This command is used to add an Indicator to ThreatConnect.	admin, tc_admin, tc_user	admin, tc_admin
tc_alert	This command is the alias to the **tcalert** command.	admin, tc_admin	admin, tc_admin
tcalert	This command is for legacy searches created in the App. It should no longer be used for creating new search alerts.	admin, tc_admin	admin, tc_admin
tcascg2i	This command is used by the App to download Indicators associated with the provided Group.	admin, tc_admin, tc_user	admin, tc_admin
tcasci2g	This command is used by the App to download Groups associated with the provided Indicator.	admin, tc_admin, tc_user	admin, tc_admin
tccustomsearch	This command is used to process custom search results and match Indicators downloaded from ThreatConnect. Any match results are stored in the Splunk KV Store.	admin, tc_admin	admin, tc_admin
tcdbstats	This command collects statistics on Indicator counts from the KV Store.	admin, tc_admin, tc_user	admin, tc_admin

tcdebug	This command will test all network connectivity that the App requires in order to function.	admin, tc_admin	admin, tc_admin
tcdmsearch	This command is used to run data-model searches and match Indicators downloaded from ThreatConnect. Any match results are stored in the Splunk KV store.	admin, tc_admin	admin, tc_admin
tcfalsepositive	This command is used to mark events as false positives in the ThreatConnect App and report the false positives to ThreatConnect.	admin, tc_admin, tc_user	admin, tc_admin
tcgroupdownload	This command is used by the App to download Group data from the ThreatConnect API and store the data in the Splunk KV Store.	admin, tc_admin, tc_user	admin, tc_admin
tcgrouptypes	This command returns all Group Types supported by the App.	admin, tc_admin, tc_user	admin, tc_admin
tciocdownload	This command is used by the App to download Indicator data from the ThreatConnect API and store the data in the Splunk KV Store. It requires the **owner_key** argument, with the key for the ThreatConnect Owner.	admin, tc_admin, tc_user	admin, tc_admin
tcioctypes	This command returns all Indicator Types defined	admin, tc_admin, tc_user	admin, tc_admin

	in the ThreatConnect Platform.		
tclookup	This command is used to search for an Indicator in ThreatConnect via the ThreatConnect API.	admin, tc_admin, tc_user	admin, tc_admin
tcobservations	This command is used to report Indicator observations to the ThreatConnect platform.	admin, tc_admin	admin, tc_admin
tcowners	This command is used by the App to download all Owner data from ThreatConnect and store the data in the Splunk KV Store.	admin, tc_admin	admin, tc_admin
tcreport	This command is used by the App to report bulk observations, false positives or whitelist.	admin, tc_admin, tc_user	admin, tc_admin
tcreportsingle	This command is used by the App to report observations, false positives, or whitelist.	admin, tc_admin, tc_user	admin, tc_admin
tctags	This command is used to retrieve all tags for a specified owner from the ThreatConnect API.	admin, tc_admin, tc_user	admin, tc_admin
tcworkflowaddindicator	This command is used to add an Indicator to ThreatConnect through the Splunk Workflow process.	admin, tc_admin, tc_user	admin, tc_admin

Software Dependencies

The following Python® modules come packaged with the App and are required for the App to function properly:

- Requests: 2.18.4
- Dateutil: 2.7.0
- Splunklib: 1.6.3
- Six: 1.10.0
- ThreatConnect Splunk: 1.0.0

APPENDIX: SAMPLE DATA-MODEL SEARCHES

Name	Data Model	Indicator Field	Victim Field	Indicator Types
Alerts	Alerts	Alerts.src	Alerts.dest	Address
Blocked Traffic	Network_Traffic	All_Traffic.src	All_Traffic.dest	Address
Email Outbound	Email	All_Email.recipient	All_Email.src_user	EmailAddress
Email Inbound	Email	All_Email.src_user	All_Email.recipient	EmailAddress
Email Attachment	Email	All_Email.file_hash	All_Email.recipient	File
Intrusion_Detection	Intrusion_Detection	IDS_Attacks.src	IDS_Attacks.dest	Address
Malware	Malware	Malware_Attacks_file.hash	Malware_Attacks.dest	File
Network Resolution Answer	Network_Resolution	DNS.answer	DNS.src	Host
Network Resolution Query	Network_Resolution	DNS.query	DNS.src	Host
Network Sessions Inbound	Network_Sessions	All_Sessions.src_jp	All_Sessions.dest_jp	Address
Network Traffic Inbound	Network_Traffic	All_Traffic.src	All_Traffic.dest	Address
Network Traffic Outbound	Network_Traffic	All_Traffic.dest	All_Traffic.src	Address
Web Outbound	Web	Web.dest	Web.src	URL
Web Inbound	Web	Web.src	Web.dest	URL
Web HTTP Referrer	Web	Web. http_referrer	Web.src	URL
Web Site	Web	Web.site	Web.src	URL