



Application for Splunk®

User Guide

Software Version 3.0 or Newer

November 5, 2018

©2018 ThreatConnect, Inc.

ThreatConnect® is a registered trademark of ThreatConnect, Inc.

UNIX® is a registered trademark of The Open Group.

Python® is a registered trademark of the Python Software Foundation.

Splunk® is a registered trademark of Splunk, Inc.



www.ThreatConnect.com

info@threatconnect.com

TOLL FREE: 1.800.965.2708

LOCAL: +1.703.229.4240

FAX: +1.703.229.4489

THREATCONNECT, INC.
3865 WILSON BLVD., SUITE 550
ARLINGTON, VA 22203

TABLE OF CONTENTS

- OVERVIEW5
 - Key Features 5
- GETTING STARTED.....5
 - Prerequisites..... 5
 - Installation 6
 - Upgrading..... 6
 - ThreatConnect API User Creation 7
- THE THREATCONNECT APP FOR SPLUNK9
 - App Setup and Configuration 9
 - Splunk REST Service SSL Verification 11
 - App Roles 11
 - Indicator Downloads..... 11
 - Setting Up Custom Searches..... 13
 - Setting up Data-Model Searches..... 16
 - The ThreatConnect Dashboard..... 19
 - The Indicator Dashboard..... 21
 - The Event Triage Dashboard 22
 - The Indicator Search Screen 23
 - The Indicator Review Dashboard 24
 - The Threat Indicator Download Report Screen 25

The Threat Indicators Menu	25
The Search Screen	27
Workflow: Event Actions	27
Workflow: Field Actions	28
The ThreatConnect App for Splunk Data	28
Administration Task	28
Clear Data (tcclear)	28
Enterprise Security Integration.....	29
Ingesting Indicators	29
KV Store (Collection) Index	30
Application Command Index	31
Software Dependencies.....	33
APPENDIX: SAMPLE DATA-MODEL SEARCHES.....	34

OVERVIEW

The ThreatConnect® Application (App) for Splunk gives Splunk users the ability to leverage customizable threat intelligence integrated into Splunk from their ThreatConnect accounts. ThreatConnect provides the ability to aggregate threat intelligence from multiple sources (i.e., open source, commercial, communities, and internally created), analyze and track identified adversary infrastructure and capabilities, and put that refined knowledge to work in Splunk, identifying threats targeting organizations.

Key Features

- Multi-source threat intelligence collection (open source, commercial, communities, internal research)
- Transparent threat intelligence aggregated, confidence weighted, and applied to triggered Splunk searches
- Customizable threat intelligence Indicator updates, custom searches, and [data-model](#) searches (Splunk CIM add-on required for data-model searches)
- Prioritized events based on criticality and confidence scores, relationships to known threat types and Groups, past Incidents, and Tags
- Insights on a threat's capability, infrastructure, and past Incidents affecting users or members of trusted communities represented using the Diamond Model for Intrusion Analysis

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 wish to start a trial of the ThreatConnect App for Splunk with a live connection to the latest customizable threat intelligence data, please inquire at <https://www.threatconnect.com/products/>.

Once an Organization has been licensed for API access, its users 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, please see the **API User Creation** section in the *ThreatConnect Application Programming Interface User Guide*.

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 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 can 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, the event data is 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** 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.

The data previously stored in the **tc_events** and **tc_events_data** collections is not modified or deleted. If this data is no longer required, it can be deleted manually by the Splunk Administrator.

ThreatConnect API User Creation

A ThreatConnect API User is created from within the ThreatConnect Web application for the instance being used. For the ThreatConnect Cloud edition, this application is located at <https://app.threatconnect.com>.

Follow these steps to create an API User:


- 1. On the top navigation bar (Figure 1), place the cursor on the **Settings**  icon and the **Settings** menu will appear (Figure 2).



Figure 1

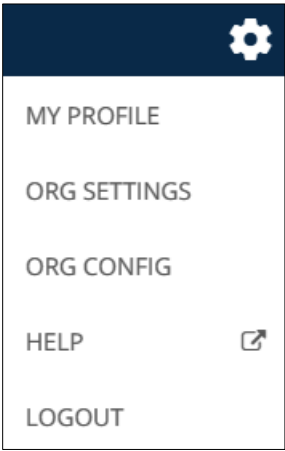


Figure 2

- 2. Select **ORG SETTINGS**, and the **Organization Settings** screen will appear (Figure 3).

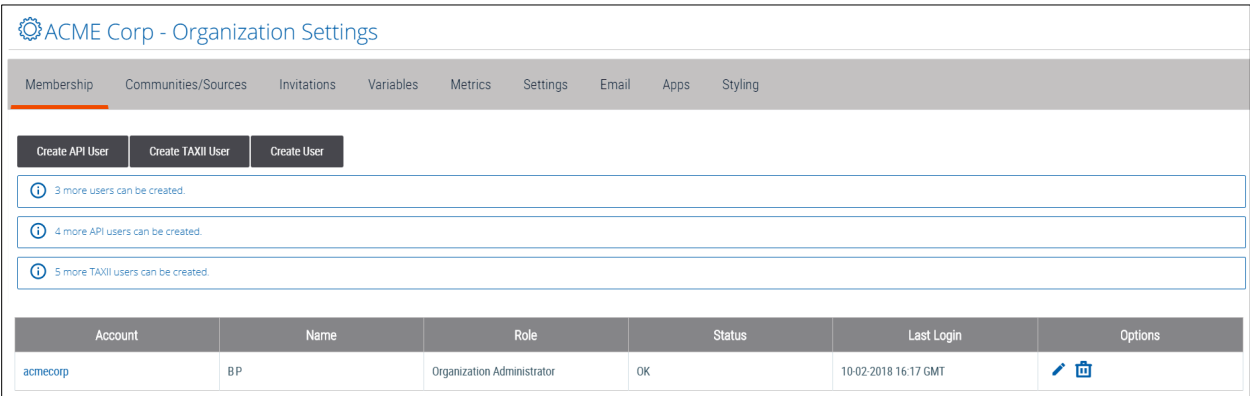
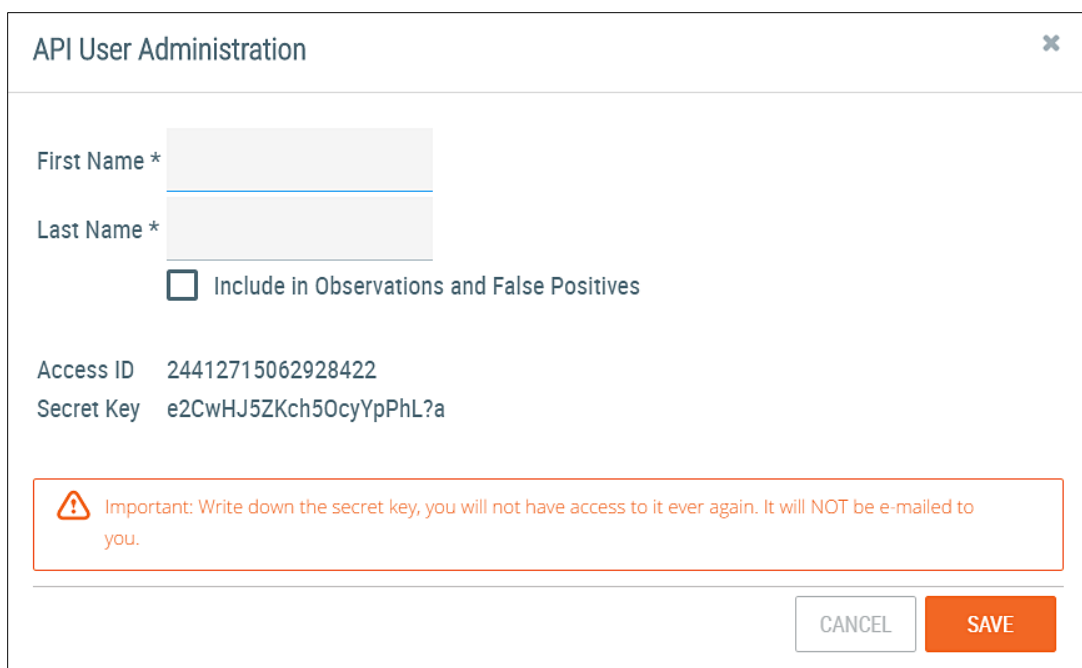


Figure 3

- 3. Click the **Create API User** button, and the **API User Administration** pop-up screen will appear (Figure 4).



The screenshot shows a web form titled "API User Administration" with a close button (X) in the top right corner. The form contains the following elements:

- Two text input fields for "First Name *" and "Last Name *".
- A checkbox labeled "Include in Observations and False Positives".
- Two lines of text: "Access ID 24412715062928422" and "Secret Key e2CwHJ5ZKch50cyYpPhL?a".
- A red-bordered warning box containing a warning icon and the text: "Important: Write down the secret key, you will not have access to it ever again. It will NOT be e-mailed to you."
- Two buttons at the bottom right: "CANCEL" and "SAVE".

Figure 4

4. Fill in the information requested, as described in Table 1, and copy the **Access ID** and **Secret Key** to a safe location.

NOTE: *It is recommended that an API User be created specifically for the ThreatConnect App for Splunk. Statistics are generated per API Key, which allows reporting per integration.*

Table 1

Parameter	Description
First Name	This parameter is the first name of the User that will appear in posts, data modifications, and data creation within ThreatConnect (e.g., Splunk).
Last Name	This parameter is the last name of the User that will appear in posts, data modifications, and data creation within ThreatConnect (e.g., App).
Pseudonym	This parameter is the pseudonym of the User that will appear in posts, data modifications, and data creation within ThreatConnect (e.g., splunk_app).

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 5. 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.

Figure 5

- **API Base URL:** The ThreatConnect Public Cloud API can be accessed at api.threatconnect.com. Users with a Private Cloud or On-Premises edition 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 a User's ThreatConnect API account's Access ID.
- **API Secret Key:** The API Secret Key corresponds with a User's ThreatConnect API account key, accessible during account creation within the User's ThreatConnect organization.
- **Activity Log:** The Activity Log checkbox enables activity logging in the ThreatConnect Platform for any API write actions.
- **Enable Proxy:** This checkbox enables proxy-server support.
- **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.
- **Logging Level:** This input enables the User to define the logging level for the ThreatConnect App for Splunk. A best practice is to set this to **info** or higher to prevent excessive logging to the Splunk KV Store.

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 does not verify the SSL certificates provided by the Splunk REST service (typically on localhost port 8089). To enable certificate checks, edit the file

\$SPLUNK_HOME/etc/apps/TA-threatconnect/local/tc_setup.conf and add **splunk_rest_ssl = 1** under the **[ta_threatconnect_settings]** section. If this setting is added, the certificate provided by the REST service must be trusted in order for the application to connect.

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 **tcclear**, and **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 user to update event status on the **Indicator 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 6) 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 the ThreatConnect platform. To edit a specific Owner configuration, click the **Edit** link in the row for the Owner, and the **Indicator Download Configuration** screen will appear (Figure 7). To run the Indicator download (optional), click the **Run** link in the row for the Owner in the **Indicator Downloads** screen. 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.

Dashboards ▾

Threat Lookup ▾

Reports ▾

Threat Indicators ▾

Configure ▾

Search

Support ▾

THREATCONNECT

Configure Indicator Downloads

Download Updates

Edit

Export ▾

...

i	Name	Id	Type	Minimum Threat Rating	Minimum Confidence Rating	Maximum False Positives	Status	Cron Schedule	Actions
>	abuse.ch Feodo Tracker	76	Source	<div><div></div><div></div><div></div><div></div><div></div></div>	<div><div>50</div><div></div></div>	10	✓ Enabled	20 6 * * *	Edit Run
>	abuse.ch Ransomware Tracker	77	Source	<div><div></div><div></div><div></div><div></div><div></div></div>	<div><div>50</div><div></div></div>	10	✓ Enabled	30 6 * * *	Edit Run
▼	abuse.ch Zeus Tracker	78	Source	<div><div></div><div></div><div></div><div></div><div></div></div>	<div><div>50</div><div></div></div>	10	✓ Enabled	40 6 * * *	Edit Run
<div><div><div>Indicator Types</div><div>URL, File, Mutex, Hashtag, Email Subject, Address, ASN, Registry Key, Host, CIDR, User Agent, EmailAddress</div><div>Filter Tag Includes</div><div>No Filter</div></div><div><div>Group Types</div><div>Adversary, Campaign, Document, Email, Event, Incident, Intrusion Set, Signature, Report, Threat, Task</div><div>Filter Tag Excludes</div><div>No Filter</div></div><div><div>Indicator Whitelists</div><div>None Selected</div><div>Last Download</div><div>2018-11-01T06:48:02+0000</div></div><div><div>Local Indicators</div><div>162</div><div>Remote Indicators</div><div>188</div></div></div>									
>	Accenture iDefense IntelGraph	132	Source	<div><div></div><div></div><div></div><div></div><div></div></div>	<div><div>50</div><div></div></div>	No Maximum	⚠ Disabled	20 9 * * *	Edit Run
>	Accenture iDefense IntelGraph - debug	131	Source	<div><div></div><div></div><div></div><div></div><div></div></div>	<div><div>50</div><div></div></div>	No Maximum	⚠ Disabled	10 9 * * *	Edit Run
>	Accenture iDefense IntelGraph - local	128	Source	<div><div></div><div></div><div></div><div></div><div></div></div>	<div><div>50</div><div></div></div>	No Maximum	⚠ Disabled	0 9 * * *	Edit Run
>	Bambenek	60	Source	<div><div></div><div></div><div></div><div></div><div></div></div>	<div><div>50</div><div></div></div>	No Maximum	⚠ Disabled	40 3 * * *	Edit Run
>	batch_local	118	Source	<div><div></div><div></div><div></div><div></div><div></div></div>	<div><div>50</div><div></div></div>	No Maximum	⚠ Disabled	0 8 * * *	Edit Run
>	batch_v1	115	Source	<div><div></div><div></div><div></div><div></div><div></div></div>	<div><div>50</div><div></div></div>	No Maximum	⚠ Disabled	40 7 * * *	Edit Run
>	batch_v2	116	Source	<div><div></div><div></div><div></div><div></div><div></div></div>	<div><div>50</div><div></div></div>	No Maximum	⚠ Disabled	50 7 * * *	Edit Run

Figure 6

Configure

Search

Support

THREATCONNECT

Edit

Export

...

Types Settings

Owner

abuse.ch Zeus Tracker

Group Types

Adversary X Campaign X

Document X Email X

Event X Incident X

Intrusion Set X

Signature X Report X

Threat X Task X

Indicator Types

URL X File X Mutex X

Hashtag X

Email Subject X

Address X ASN X

Registry Key X Host X

CIDR X User Agent X

EmailAddress X

Filter Settings

Tag Include Filters

The tag filter uses the AND operator by default.

Use OR operator for Tag include filters

Tag Exclude Filters

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

Threat Rating Minimum Filter

3 X

Confidence Rating Minimum Filter

50

False Positive Maximum Filter

10 X

Indicator whitelist

Select...

Global whitelist are automatically applied to download.

Options

Cron Schedule

40 6 * * *

Disabled

Cancel

Save

Figure 7

- **Owner:** The selected Owner to be configured is given here.
- **Group Types:** Select the ThreatConnect Group types to download for use in the Diamond Dashboard. Available options are Adversary, Campaign, Email, Incident, and Threat.
- **Indicator Types:** Select the Indicator types to download for use by the ThreatConnect App for Splunk.
- **Tag Filters Include:** 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.
- **Use Or Operator for Tag Include Filters:** Toggle this input to enable the Tag filter feature to Or tags instead of the default And. **Tag Filters Exclude:** 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 Rating Minimum Filter:** Select an Indicator threat-rating minimum threshold. In ThreatConnect, threat ratings have a value of 0–5 points. Only Indicators that meet the filter’s threshold will be downloaded into the App.
- **Confidence Rating Minimum Filter:** Select an Indicator confidence-rating minimum threshold. 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 an Indicator’s false positive maximum threshold. Indicators that have a false positive count higher than the provided value will be filtered during the download.
- **Indicator Whitelist:** Select one or more preconfigured Indicator whitelist. Global whitelists apply to all Indicator downloads.
- **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 <http://en.wikipedia.org/wiki/Cron>.
- **Disable:** Check this box to disable any further syncs of Indicators for this Owner. Checking this box 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 re-sync 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 8) to access the **Configure Custom Search** screen (Figure 9).

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

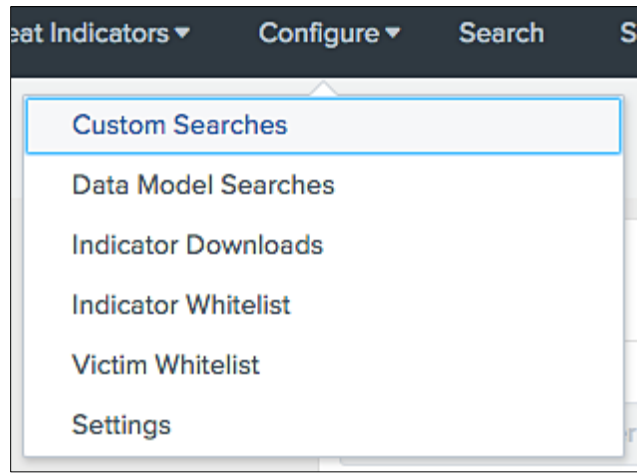


Figure 8

A screenshot of the ThreatConnect application's configuration page. The page is divided into three main sections: 'Search Settings', 'Filter Settings', and 'Search Options'.
Search Settings: Includes fields for 'Search Name' (Firewall Ingress), 'Simple Search' (index=sophos sourcetype=sophosutm), 'Indicator Field' (src_ip), 'Indicator Types' (Address), 'Victim Field' (dest_ip), and 'Victim Whitelist' (Select...). A note states: 'Global whitelist are automatically applied to search.'
Filter Settings: Includes 'Minimum Threat Rating Filter' (No Filter), 'Additional Minimum Confidence Rating Filter' (No Filter), and 'Tag Include Filters' (Select...). A note states: 'The tag filter uses the AND operator.'
Search Options: Includes 'Confidence Threshold' (80), 'Report Observations' (checked), 'Earliest' (-1h), 'Latest' (-1h), 'Cron Schedule' (0 * * * *), and a 'Disable' option.
At the bottom right, there are buttons for 'Cancel', 'Delete', and 'Save'.

Figure 9

- **Search Name:** Identifier for this job (e.g., Firefox Vulnerability).
- **Simple Search:** A properly formatted Splunk search expression that will return events with Indicators.
- **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**.
- **Victim Whitelist:** Select a Victim Whitelist filter for available options. Global filters will not be available.
- **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.
- **Tag Include Filter:** Provide one or more Tag Include filters for this search.
- **Confidence Threshold (Reset on Observation):** If a value is selected, this feature will allow the update of the Confidence Rating in the ThreatConnect platform to the selected value. This feature is intended to work with Indicator deprecation in the ThreatConnect platform. By changing the Confidence Rating, deprecation of the Indicator can be delayed.
- **Report Observations:** Check this box to enable the feedback loop to report observations back to ThreatConnect.
- **Earliest:** This represents the start window of time that should be searched (e.g., use **-75m@m** to start 75 minutes in the past).
See <http://docs.splunk.com/Documentation/Splunk/6.4.1/SearchReference/SearchTimeModifiers> for additional information.
- **Latest:** This represents the end window of time that should be searched (e.g., **-15m@m** to end 15 minutes in the past).
- **Cron Schedule:** This 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 switch to prevent this search from running.

To add a new search, click the **Add Search** button on the upper right of the screen (Figure 10). To edit a search, click the **Edit** link.

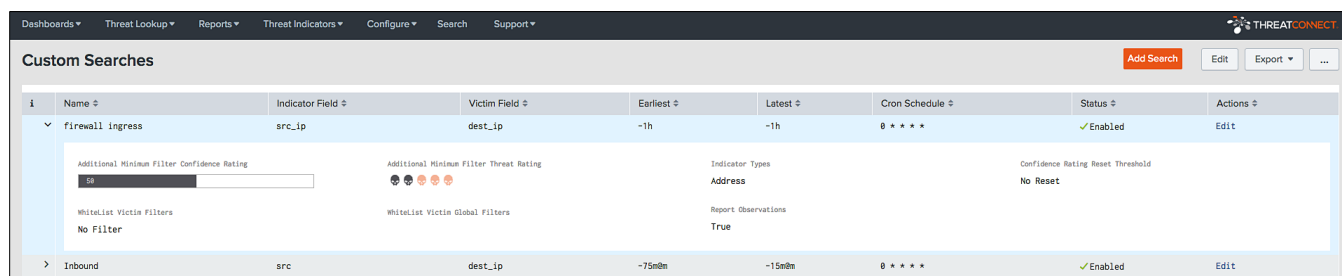


Figure 10

Setting up Data-Model Searches

To configure data-model searches, click the **Configure** menu and select the **DataModel Searches** option (Figure 11). To add a new data-model search, click the **Add Search** button on the top right of the screen (Figure 12). To edit an existing search, click the **Edit** link. Figure 13 shows the **Configure Data Model Search** screen.

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

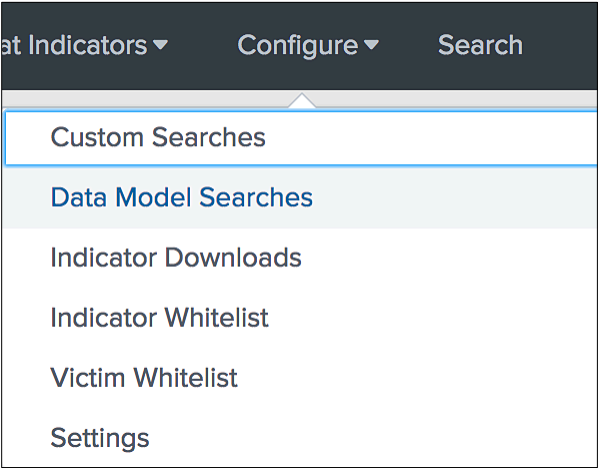


Figure 11

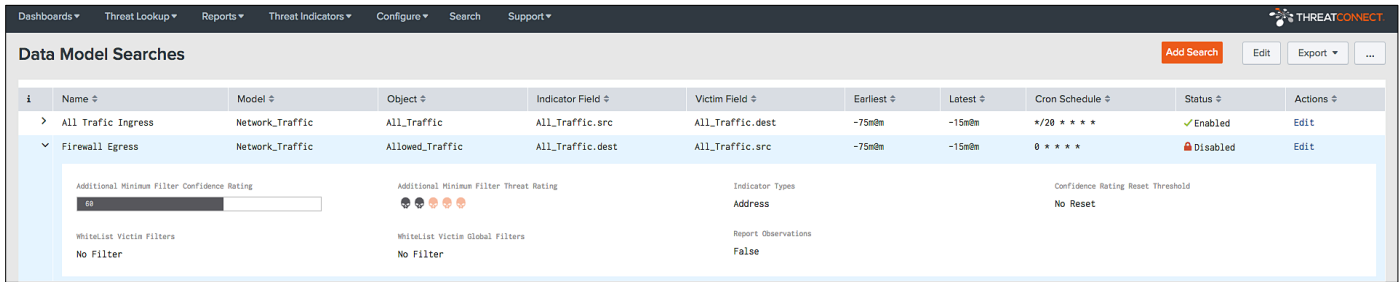


Figure 12

Dashboards

Threat Lookup

Reports

Threat Indicators

Configure

Search

Support

THREATCONNECT

Configure Data Model Search

EditExport...

Search Settings

Search Name

Firewall Egress

Data Model

Network_Traffic

Data Model Object

Allowed_Traffic

Indicator Field

All_Traffic.dest

Indicator Types

Address

Victim Field

All_Traffic.src

Victim Whitelist

Select...

Global whitelist are automatically applied to search.

Filter Settings

Additional Minimum Threat Rating Filter

2

Additional Minimum Confidence Rating Filter

60

Tag Include Filters

OSINTSplunkTest

The tag filter uses the AND operator.

Search Options

Confidence Threshold

No Reset

On observations reporting reset the confidence value.

Report Observations

Earliest

-75m@m

Latest

-15m@m

Cron Schedule

0 ****

Disable

CancelDeleteSave

Figure 13

- **Search Name:** Identifier for this search.
- **Data Model:** The name of the data model to be searched
- **Data Model Object:** The specific data-model object to search
- **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
- **Victim Whitelist:** Select a Victim Whitelist filter for available options. Global filters will not be available.
- **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.
- **Tag Include Filters:** Provide one or more Tag Include filters for this search.
- **Confidence Threshold (Reset on Observation):** If a value is selected, this feature will allow the update of the confidence value in the ThreatConnect platform to the selected value. This feature is intended to work with Indicator deprecation in the ThreatConnect platform. By changing the confidence value, deprecation of the Indicator can be delayed.
- **Report Observations:** Check this box to enable the feedback loop to report observations back to ThreatConnect.
- **Earliest:** This represents the start window of time that should be searched (e.g., use **-75m@m** to start 75 minutes in the past).
See <http://docs.splunk.com/Documentation/Splunk/6.4.1/SearchReference/SearchTimeModifiers> for additional information.
- **Latest:** This represents the end window of time that should be searched (e.g., **-15m@m** to end 15 minutes in the past).
- **Cron Schedule:** This 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 switch to prevent this search from running.

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 14).

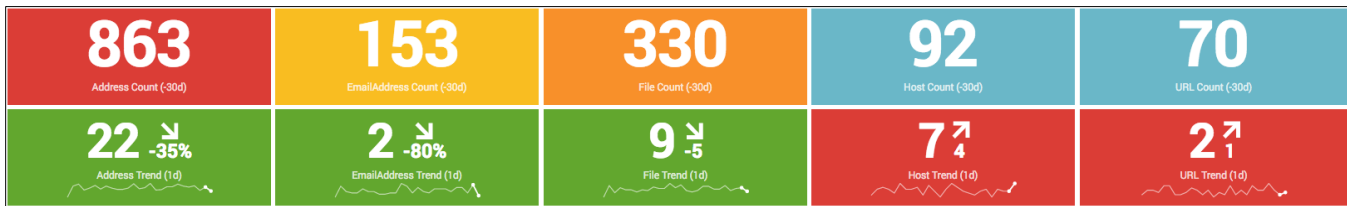


Figure 14

The third row provides a table with Custom Indicator counts and a chart of event activity (Figure 15). This table will include the **new** 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.

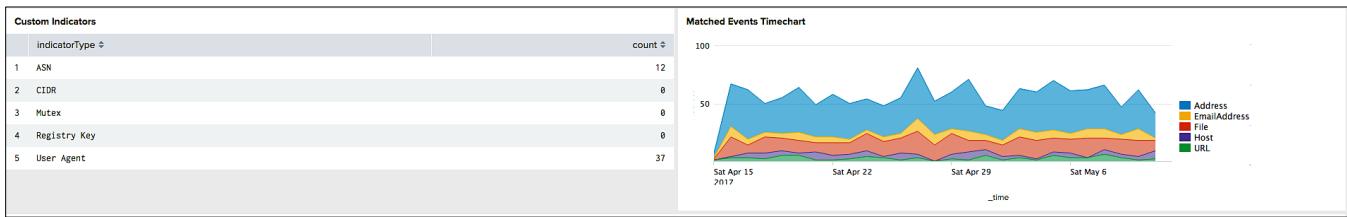


Figure 15

The view at the bottom displays the latest matched Indicators in a paginated table (Figure 16). 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.

Time	Indicator	Victim	Type	SourceType	SearchType
> 2018-11-01 20:01:44	77.72.85.27	66.23.241.204	Infrastructure	sophos:uts:firewall	auto
> 2018-11-01 20:01:44	176.119.7.22	66.23.241.206	Infrastructure	sophos:uts:firewall	auto
<div> <div> Owners <div>Blocklist.de Apache IPs</div> <div> <div> <div> <div></div> <div></div> <div></div> <div></div> </div> <div>80</div> </div> </div> </div> <div> Tags <div>No tags found.</div> </div> <div> Group Associations <div>No associations found.</div> </div> </div> <div> Event <div><30>2018:11:01-14:45:06 utm ulogd[2113]: id="2021" severity="info" sys="SecureNet" sub="packetfilter" name="Packet dropped (GEOIP)" action="drop" fwrule="60019" initf="eth0" srmac="cc:4e:24:f1:b0:80" dstmac="d4:ae:52:c0:3e:df" srcip="176.119.7.22" dstip="66.23.241.206" proto="6" length="40" tos="0x00" prec="0x00" ttl="245" sport="57079" dstop="51435" topflags="SYN"</div> </div>					
> 2018-11-01 20:01:44	176.119.7.22	66.23.241.200	Infrastructure	sophos:uts:firewall	auto
> 2018-11-01 20:01:43	77.72.85.27	66.23.241.199	Infrastructure	sophos:uts:firewall	auto
> 2018-11-01 20:01:43	78.128.112.62	66.23.241.202	Infrastructure	sophos:uts:firewall	auto
> 2018-11-01 20:01:43	200.54.86.59	66.23.241.206	Infrastructure	sophos:uts:firewall	auto

Figure 16

- **_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 on the ThreatConnect website.
- **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 criticality rating assigned by the Indicator's Owner within ThreatConnect. This value is on a scale of 0–5 points, 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 associated with 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 17) displays matched Indicators by Owners. A dropdown option is available to narrow down the window of time for the results.

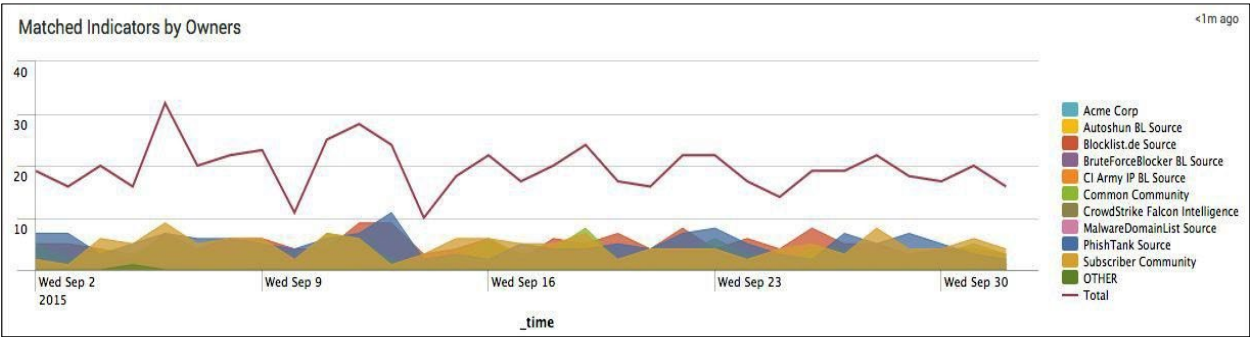


Figure 17

The second row displays additional paginated tables for matched Indicators (Figure 18). 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			Top Matched Tags		
Indicator ↕	count ↕	percent ↕	Tags ↕	count ↕	percent ↕
176.119.7.62	8306	3.28%	SSH	592	47.59%
78.128.112.14	7897	2.74%	OSINT	346	27.81%
5.188.206.14	7000	2.70%	Mail	284	16.40%
31.192.108.68	6596	2.54%	Splunk Testing	58	4.02%
122.228.10.51	6171	2.38%	Splunk Test	58	4.02%
176.119.7.6	6136	2.37%	Africa	2	0.16%
176.119.7.2	6134	2.37%			
176.119.7.58	6133	2.37%			
176.119.7.10	6052	2.33%			
78.128.112.30	5941	2.29%			

< prev 1 2 next >

Figure 18

The Event Triage Dashboard

The **Event Triage** dashboard (Figure 19) 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** and **Mark Reviewed** buttons/links in each row allow action on a specific event. When the **Mark False Positive** button/link is clicked, the state of the event is updated 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 the status of the events.

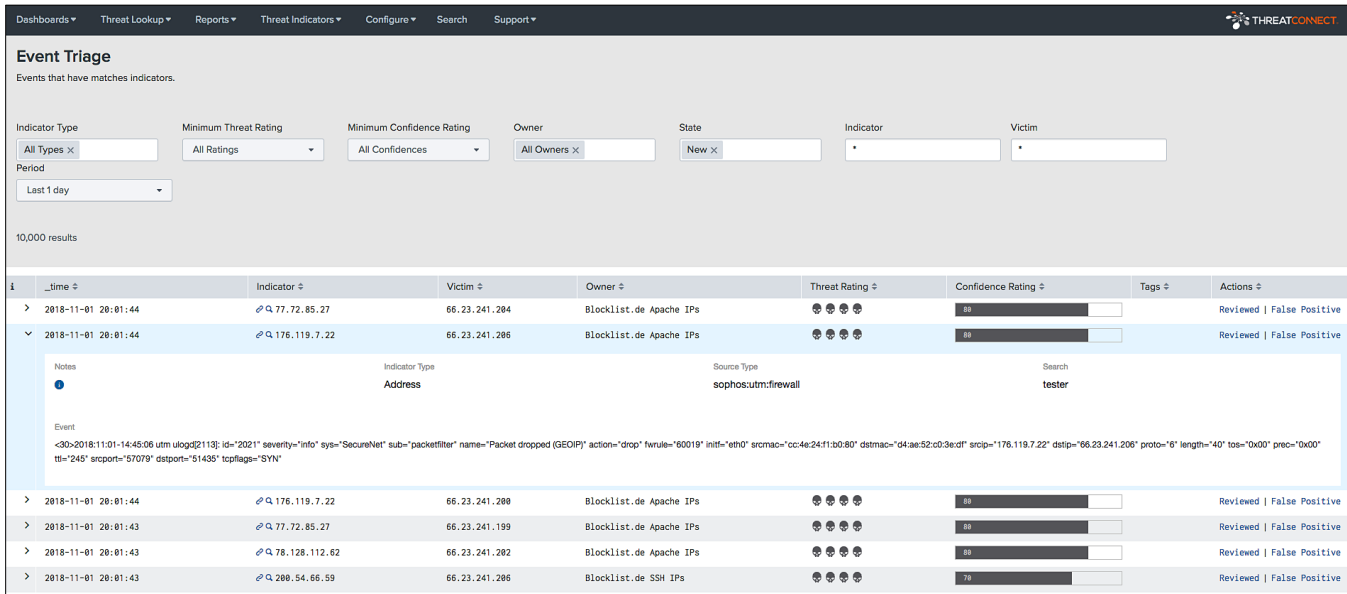


Figure 19

To add a comment on a matched event, click the **Notes** icon in the table row expansion, and the **Notes** pop-up screen will appear (Figure 20).

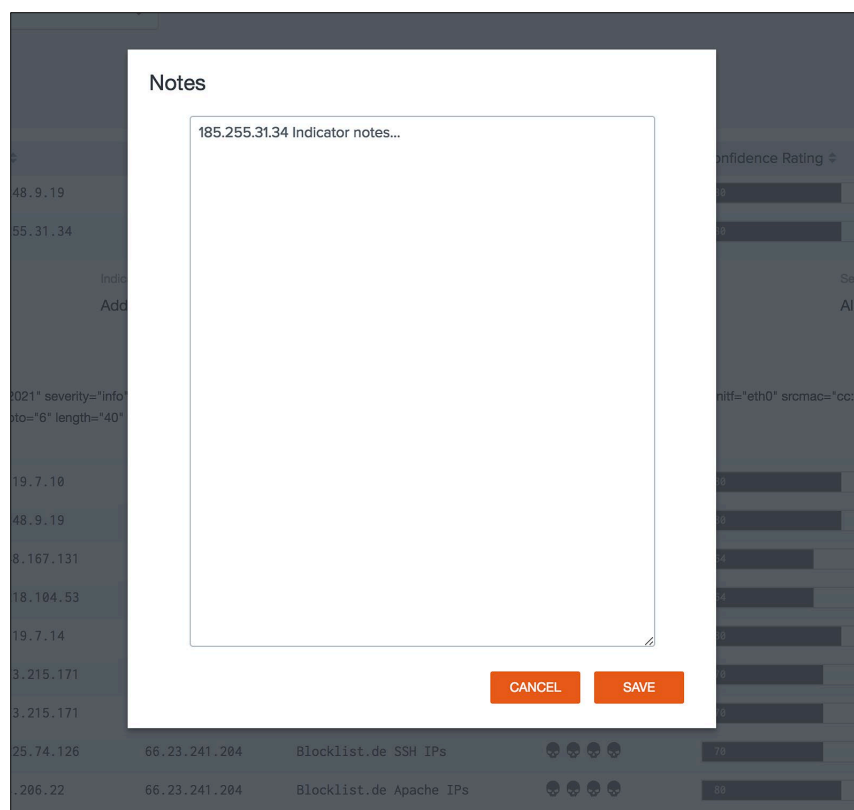


Figure 20

The **Indicator** column has two links in the form of icons. The first link redirects the user to threatconnect.com to view the Indicator's details. 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 21). The Indicator type is automatically detected.

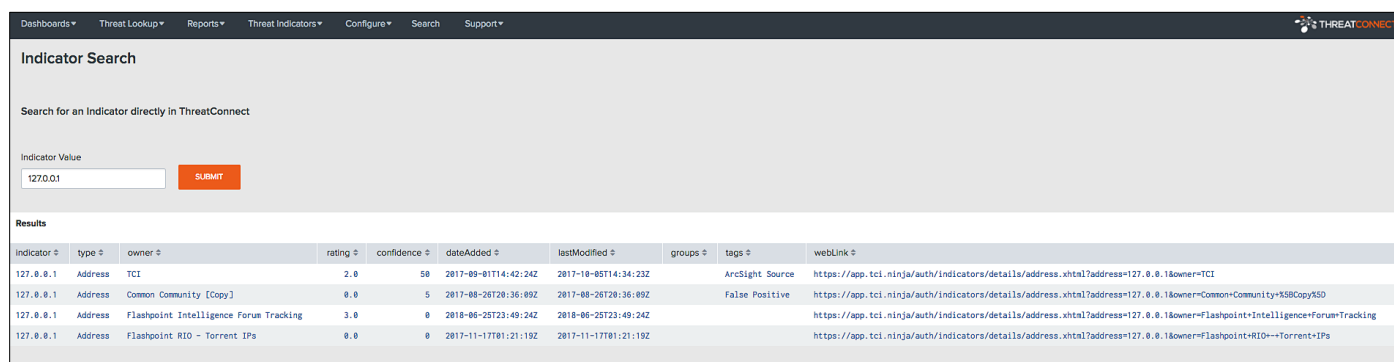


Figure 21

The Indicator Review Dashboard

The **Indicator Review** dashboard allows users to search for and filter Indicators (Figure 22).

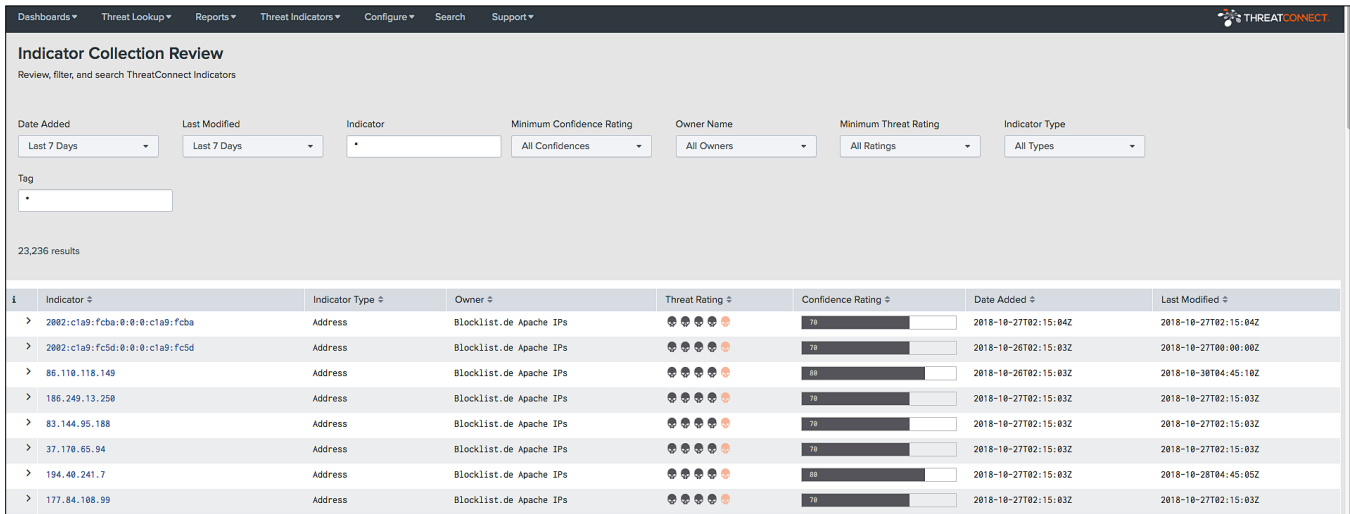


Figure 22

Each Indicator record expands and displays additional Indicator information, in real time, retrieved directly from the ThreatConnect API (Figure 23).

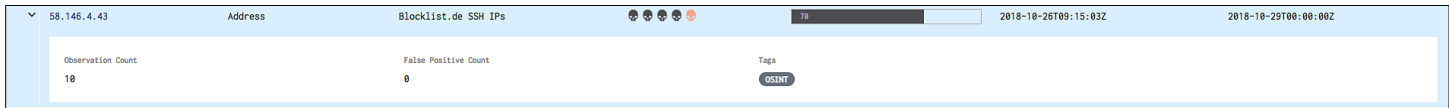


Figure 23

The Threat Indicator Download Report Screen

The **Threat Indicator Download Report** screen is used to create a few canned reports for monitoring ThreatConnect Alert queries and for tracking how many of those queries hit the ThreatConnect API (Figure 24). User-defined custom reports can be added for more detailed views into the ThreatConnect data.

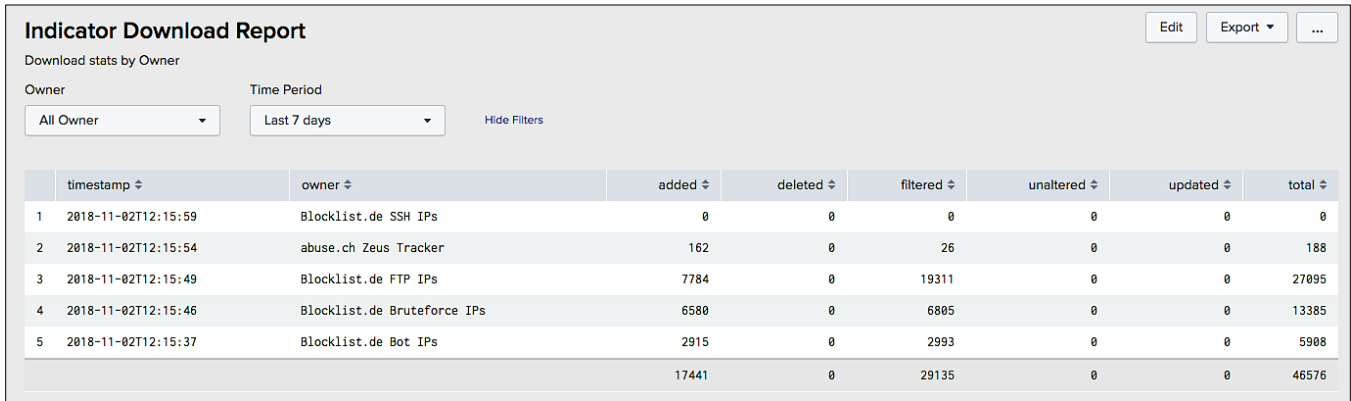


Figure 24

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 25). There are two charts: one for Indicator type by Owner and another for Indicator type by rating.



Figure 25

The second row contains two tables that display the last 10 created and updated Indicators, respectively (Figure 26).

Last 10 Added Address Indicators				Last 10 Updated Address Indicators			
dateAdded ↕	indicator ↕	rating ↕	ownerName ↕	lastModified ↕	indicator ↕	rating ↕	ownerName ↕
2018-11-01T02:02:12Z	125.64.94.200	5	TCI	2018-11-02T08:45:05Z	78.128.112.62	4	Blocklist.de Apache IPs
2018-11-01T01:56:56Z	78.128.112.14	5	TCI	2018-11-02T08:45:05Z	222.122.60.160	4	Blocklist.de Apache IPs
2018-10-31T20:20:06Z	176.119.7.50	3	TCI	2018-11-02T08:45:04Z	5.188.206.22	4	Blocklist.de Apache IPs
2018-10-27T02:15:04Z	202.40.182.246	4	Blocklist.de Apache IPs	2018-11-02T04:45:03Z	78.128.112.14	5	TCI
2018-10-27T02:15:04Z	45.192.39.251	4	Blocklist.de Apache IPs	2018-11-02T03:45:02Z	189.254.142.228	4	Blocklist.de Apache IPs
2018-10-27T02:15:04Z	177.105.155.124	4	Blocklist.de Apache IPs	2018-11-02T01:45:07Z	31.192.108.75	4	Blocklist.de Apache IPs
2018-10-27T02:15:04Z	49.65.204.20	4	Blocklist.de Apache IPs	2018-11-02T00:02:02Z	213.238.169.37	4	Blocklist.de Apache IPs
2018-10-27T02:15:04Z	82.63.112.47	4	Blocklist.de Apache IPs	2018-11-02T00:02:02Z	197.231.23.17	4	Blocklist.de Apache IPs
2018-10-27T02:15:04Z	114.109.128.146	4	Blocklist.de Apache IPs	2018-11-02T00:02:02Z	91.144.87.226	4	Blocklist.de Apache IPs
2018-10-27T02:15:04Z	170.81.60.254	4	Blocklist.de Apache IPs	2018-11-02T00:02:02Z	154.125.137.173	4	Blocklist.de Apache IPs

Figure 26

The final row displays a paginated table of all the Indicators of that type pulled from ThreatConnect (Figure 27).

Select a view: Address Indicators Address Indicators by Country Chart Address Indicators by Country Map						
indicator ↕	type ↕	rating ↕	confidence ↕	dateAdded ↕	lastModified ↕	webLink ↕
94.173.10.64	Address	3	50	2018-10-05T22:15:03Z	2018-10-07T00:00:00Z	https://app.tci.ninja/auth/indicators/details/address.xhtml?address=94.173.10.64&owner=abuse.ch+Feodo+Tracker
105.226.215.238	Address	3	50	2018-10-05T22:15:03Z	2018-10-07T00:00:00Z	https://app.tci.ninja/auth/indicators/details/address.xhtml?address=105.226.215.238&owner=abuse.ch+Feodo+Tracker
128.193.56.6	Address	3	50	2018-10-05T22:15:03Z	2018-10-07T00:00:00Z	https://app.tci.ninja/auth/indicators/details/address.xhtml?address=128.193.56.6&owner=abuse.ch+Feodo+Tracker
186.68.80.34	Address	3	50	2018-10-05T22:15:03Z	2018-10-07T00:00:00Z	https://app.tci.ninja/auth/indicators/details/address.xhtml?address=186.68.80.34&owner=abuse.ch+Feodo+Tracker
198.246.28.128	Address	3	50	2018-10-05T22:15:03Z	2018-10-07T00:00:00Z	https://app.tci.ninja/auth/indicators/details/address.xhtml?address=198.246.28.128&owner=abuse.ch+Feodo+Tracker
96.254.126.140	Address	3	50	2018-10-05T22:15:03Z	2018-10-07T00:00:00Z	https://app.tci.ninja/auth/indicators/details/address.xhtml?address=96.254.126.140&owner=abuse.ch+Feodo+Tracker
174.71.204.179	Address	3	50	2018-10-05T22:15:03Z	2018-10-07T00:00:00Z	https://app.tci.ninja/auth/indicators/details/address.xhtml?address=174.71.204.179&owner=abuse.ch+Feodo+Tracker
197.87.130.229	Address	3	50	2018-10-05T22:15:03Z	2018-10-07T00:00:00Z	https://app.tci.ninja/auth/indicators/details/address.xhtml?address=197.87.130.229&owner=abuse.ch+Feodo+Tracker
45.33.48.217	Address	3	50	2018-10-05T22:15:03Z	2018-10-07T00:00:00Z	https://app.tci.ninja/auth/indicators/details/address.xhtml?address=45.33.48.217&owner=abuse.ch+Feodo+Tracker
63.230.212.128	Address	3	50	2018-10-04T22:15:03Z	2018-10-07T00:00:00Z	https://app.tci.ninja/auth/indicators/details/address.xhtml?address=63.230.212.128&owner=abuse.ch+Feodo+Tracker
◀ PREV 1 2 3 4 5 6 7 8 9 10 next ▶						

Figure 27

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 28).

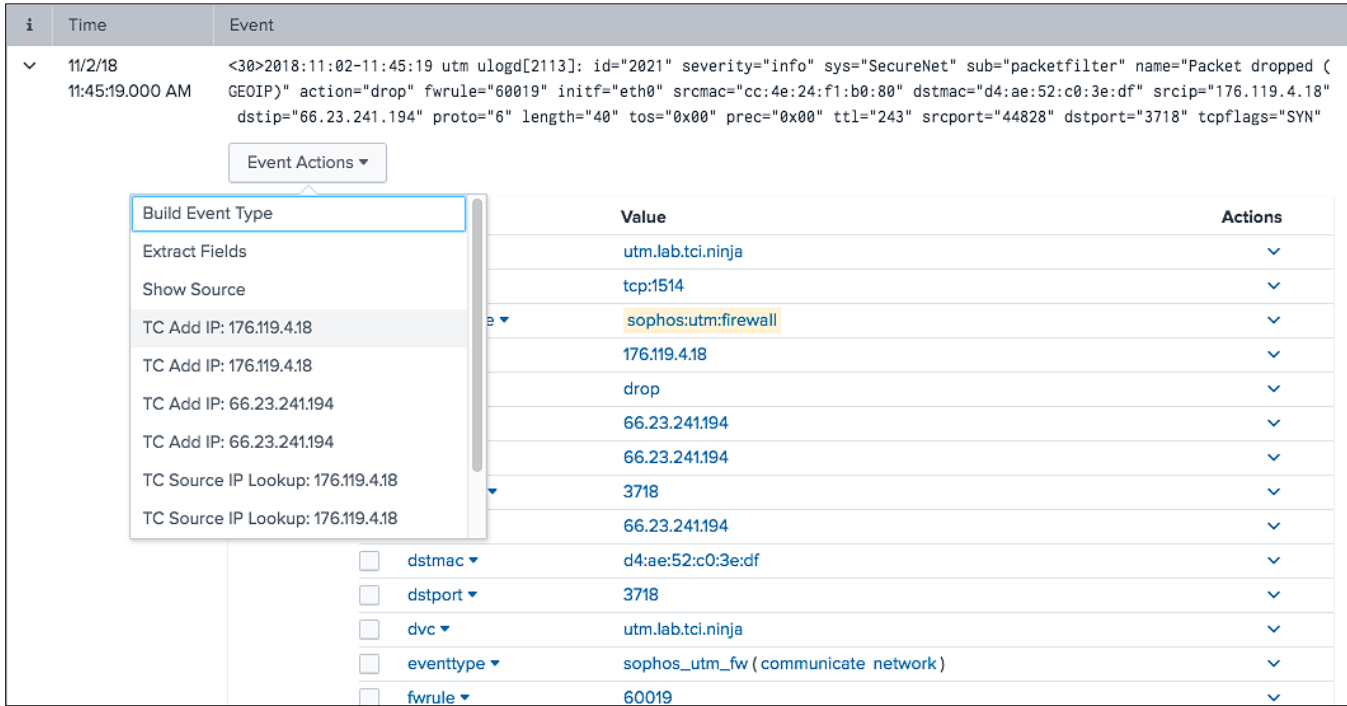


Figure 28

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 29).

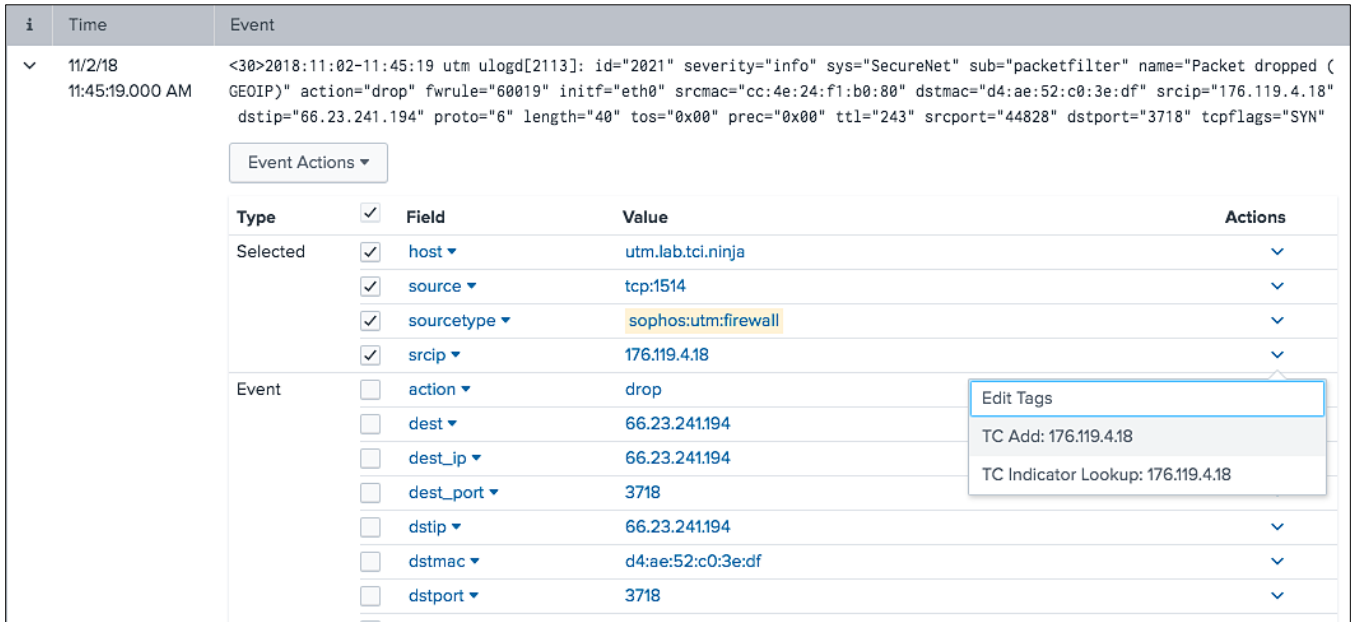


Figure 29

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** drop-down menu.

Administration Task

Clear Data (tcclear)

The ThreatConnect App for Splunk provides the tcclear command to clear out a collection of data from the KV Store. To use this tool, the **tc_admin** role must be assigned to the user.

NOTE: Once the tcclear command has been run, there is no way to recover the data. It is recommended to take backups of the KV store before clearing this data.

To clear all matched events, use the following search command:

```
| tcclear collection=tc_event_summaries
```

To clear all Indicators from the KV Store, use the following search command:

```
| tcclear collection=tc_indicators
```

To clear all Indicators for the “Example Community” Owner, use the following search command:

```
| tcclear collection=tc_indicators owner="Example Community"
```

To obtain a full list of all collections that can be cleared, see the [KV Store \(Collection\) Index](#).

Enterprise Security Integration

The latest version of the ThreatConnect App for Splunk provides support for Workflow actions in Enterprise Security, as well as 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

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 Permissions	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
tcclear	This command will clear data from the Splunk KV Store. See the Clear Data (tcclear) section.	admin, tc_admin	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
tcdstats	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
tciodownload	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 in the ThreatConnect Platform.	admin, tc_admin, tc_user	admin, tc_admin
tclog	This command is used to clear App log events from the Splunk KV Store.	admin, tc_admin, tc_user	admin, tc_admin
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	Data Model Object	Indicator Field	Victim Field	Indicator Types
Alerts	Alerts	Alerts	Alerts.src	Alerts.dest	Address
Email Outbound	Email	All_Email	All_Email.recipient	All_Email.src_user	EmailAddress
Email Inbound	Email	All_Email	All_Email.src_user	All_Email.recipient	EmailAddress
Email Attachment	Email	All_Email	All_Email.file_hash	All_Email.recipient	File
Intrusion_Detection	Intrusion_Detection	IDS_Attacks	IDS_Attacks.src	IDS_Attacks.dest	Address
Malware	Malware	Malware_Attacks	Malware_Attacks_file.hash	Malware_Attacks.dest	File
Network Resolution Answer	Network_Resolution	DNS	DNS.answer	DNS.src	Host
Network Resolution Query	Network_Resolution	DNS	DNS.query	DNS.src	Host
Network Sessions Inbound	Network_Sessions	All_Sessions	All_Sessions.src_jp	All_Sessions.dest_jp	Address
Network Traffic Inbound	Network_Traffic	All_Traffic	All_Traffic.src	All_Traffic.dest	Address
Network Traffic Outbound	Network_Traffic	All_Traffic	All_Traffic.dest	All_Traffic.src	Address
Web Outbound	Web	Web	Web.dest	Web.src	URL
Web Inbound	Web	Web	Web.src	Web.dest	URL
Web HTTP Referrer	Web	Web	Web.http_referrer	Web.src	URL
Web Site	Web	Web	Web.site	Web.src	URL
Web URL	Web	Web	Web.url_path	Web.src	URL
Web Url	Web	Web	Web.uri_path	Web.src	URL