



# Application for Splunk®

## User Guide

Software Version 2.3 or Newer

September 26, 2017

©2017 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](http://www.ThreatConnect.com)

[info@threatconnect.com](mailto: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

OVERVIEW .....5

    Key Features ..... 5

GETTING STARTED.....5

    Prerequisites..... 5

    Installation ..... 6

    ThreatConnect API User Creation ..... 6

THE THREATCONNECT APP FOR SPLUNK .....8

    App Setup and Configuration ..... 8

    Splunk REST Service SSL Verification ..... 10

    App Roles ..... 10

    Indicator Downloads..... 10

    Setting Up Custom Searches..... 12

    Setting up Data-Model Searches..... 14

    The ThreatConnect Dashboard..... 16

    The Indicator Dashboard..... 18

    The Event Triage Dashboard ..... 19

    The Diamond Dashboard ..... 21

    The Indicator Search Screen ..... 23

    The Indicator Review Dashboard..... 23

    The IOC Download Report Screen..... 24

The Threat Indicators Menu .....	24
The Search Screen .....	26
Workflow: Event Actions .....	26
Workflow: Field Actions .....	27
The ThreatConnect App for Splunk Data .....	28
Administration Task .....	28
Clear Data (tcclear) .....	28
Demo Data (tcdemo) .....	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
- History of how a threat has affected users' networks, using the Diamond Dashboard and data models

## 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>.

## 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. Log in with an Organization Administrator account.
2. On the top navigation bar, place the cursor on the **USERNAME** drop-down menu and select **ORG SETTINGS** (Figure 1). The **Organization Settings** screen will appear with the **Membership** tab highlighted (Figure 2).

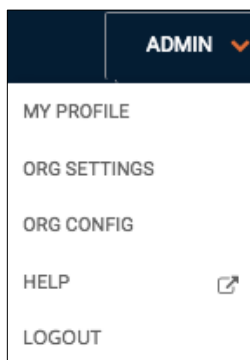



Figure 1

**NOTE:** The **USERNAME** in these examples is **ADMIN**, but it will be different for each user.


Grammatica - Organization Settings

Membership
Communities/Sources
Invitations
Variables
Settings
Email
Apps
Styling

Create API User
Create User

*i* 7 more users can be created.








Account	Name	Role	Status	Options
<a href="#">abr@threatconnect.com</a>	Chris Blair	User	OK	 
<a href="#">bk@threatconnect.com</a>	John Smith	Organization Administrator	OK	 
<a href="#">gs</a>	George Soo	Organization Administrator	OK	 

Figure 2

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

API User Administration 

First Name \*

Last Name \*

Pseudonym \*


☐ Include in Observations and False Positives

Access ID

892947

Secret Key

MemG8H1



Important: Write down the secret key, you will not have access to it ever again. It will NOT be e-mailed to you.

CANCEL

SAVE

Figure 3

- 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 4. 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.



**Settings**

**API Settings**

ThreatConnect API URL

API Access ID

API Secret Key

**Activity Log**

Enable ThreatConnect Activity Logging ☒

**Proxy**

Enable Proxy ☐

**Logging Level**

**SAVE**

**Figure 4**

- **API Base URL:** The ThreatConnect Public Cloud API can be accessed at <https://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**, **tcdemo**, 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 support on versions of Splunk lower than 6.5, a user must have the *admin\_all\_objects* capability. For versions 6.5 or higher, the *list\_storage\_passwords* capability will provide 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 5) 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 6). 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. In addition, to enable or disable Indicator downloads, click **Enabled** or **Disabled** in the **Status** column.



- **Owner:** The selected Owner to be configured is given here.
- **Use Bulk OnDemand:** Select this checkbox to enable the Bulk OnDemand download option. This feature must be enabled in the ThreatConnect platform before being used. This feature is not available on Public Cloud accounts and should not be enabled.
- **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.
- **“Or” Tag Filters (include):** Select this checkbox to enable the Tag filter feature to “Or” tags instead of the default “And.”
- **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.
- **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.
- **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.
- **Clear Indicator:** Click this button to remove all Indicators stored within the App for this particular Owner. This action is useful to prevent the Indicators for this Owner from matching any future events.

## Setting Up Custom Searches

Any 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 7) to access the **Configure Custom Search** screen (Figure 8).

**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.**

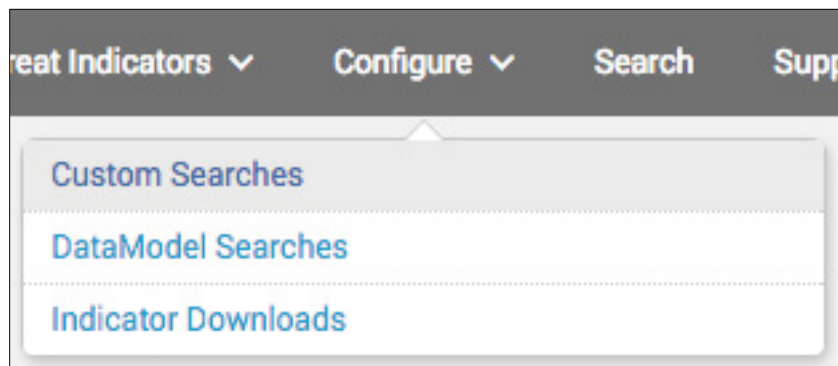


Figure 7

The screenshot displays the 'Configure Custom Search' form. The form includes the following fields and controls:

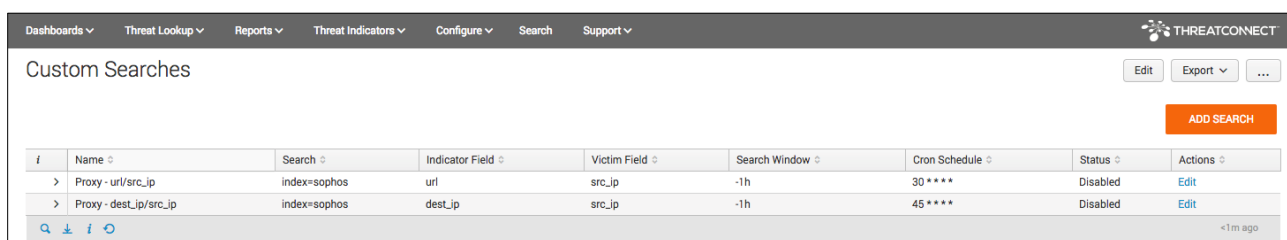
- Job Name:** A text input field containing 'Firewall Ingress'.
- Search:** A text input field containing 'index=sophos sourcetype=sophos:utm'.
- Indicator Field:** A text input field containing 'src\_ip'.
- Indicator Types:** A dropdown menu with 'Address' selected.
- Victim Field:** A text input field containing 'dest\_ip'.
- Victim Whitelist:** An empty text input field.
- Search produced no results.** A status message.
- Additional Minimum Threat Rating Filter:** A dropdown menu with 'No Filter' selected.
- Additional Minimum Confidence Rating Filter:** A dropdown menu with 'No Filter' selected.
- Confidence Threshold (Reset on Observations):** A dropdown menu with '80' selected.
- Report Observations:** A checkbox that is checked.
- Search Window (earliest):** A text input field containing '-1h'.
- Cron Schedule:** A text input field containing '0 \* \* \* \*'.
- Disable:** A checkbox that is unchecked.

At the bottom of the form, there are three buttons: 'CANCEL', 'DELETE', and 'SAVE'.

Figure 8

- **Job Name:** Identifier for this job (e.g., Firefox Vulnerability).
- **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**.
- **Search Window (earliest):** This represents the window of time, up to the present moment, that should be searched (e.g., use **-1h** for the past hour).  
See <http://docs.splunk.com/Documentation/Splunk/6.4.1/SearchReference/SearchTimeModifiers> for further information.
- **Cron Schedule:** 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.

To add a new search, click the **Add Search** button on the upper right of the screen (Figure 9). To edit a search, click the **Edit** link.



i	Name	Search	Indicator Field	Victim Field	Search Window	Cron Schedule	Status	Actions
>	Proxy - url/src_ip	index=sophos	url	src_ip	-1h	30 ****	Disabled	Edit
>	Proxy - dest_ip/src_ip	index=sophos	dest_ip	src_ip	-1h	45 ****	Disabled	Edit

Figure 9

## Setting up Data-Model Searches

To configure data-model searches, click the **Configure** menu and select the **DataModel Searches** option (Figure 10). To add a new data-model search, click the **Add Search** button on the top right of the screen (Figure 11). To edit an existing search, click the **Edit** link. Figure 12 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.**

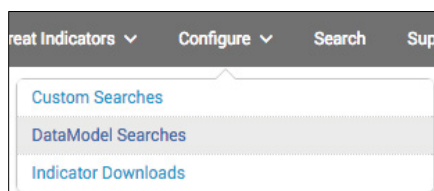


Figure 10

### Figure 11

### Figure 12

- **Job Name:** Identifier for this job
- **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.
- **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.
- **Search Window (earliest):** The window of time, up to the present moment, that should be searched (e.g., -use **-1h** for the past hour). See <http://docs.splunk.com/Documentation/Splunk/6.4.1/SearchReference/SearchTimeModifiers> for further information.
- **Cron Schedule:** 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.

## 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 13).

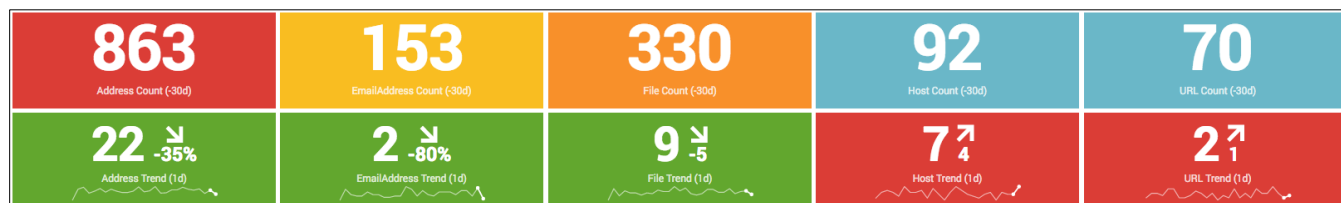


Figure 13



The third row provides a table with Custom Indicator counts and a chart of event activity (Figure 14). 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.

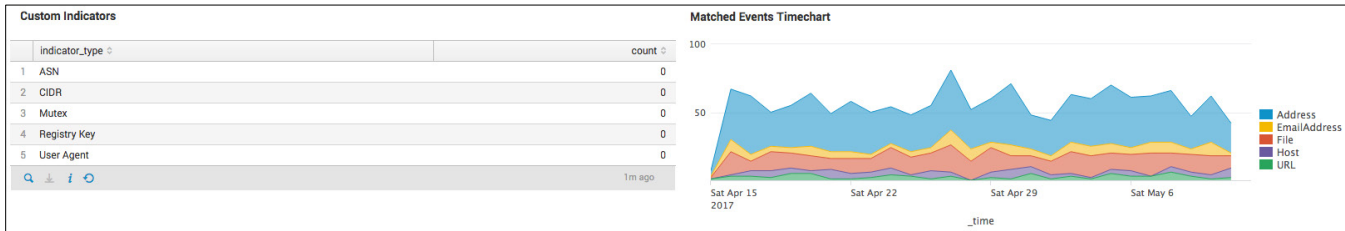


Figure 14

The view at the bottom displays the latest matched Indicators in a paginated table (Figure 15). 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.

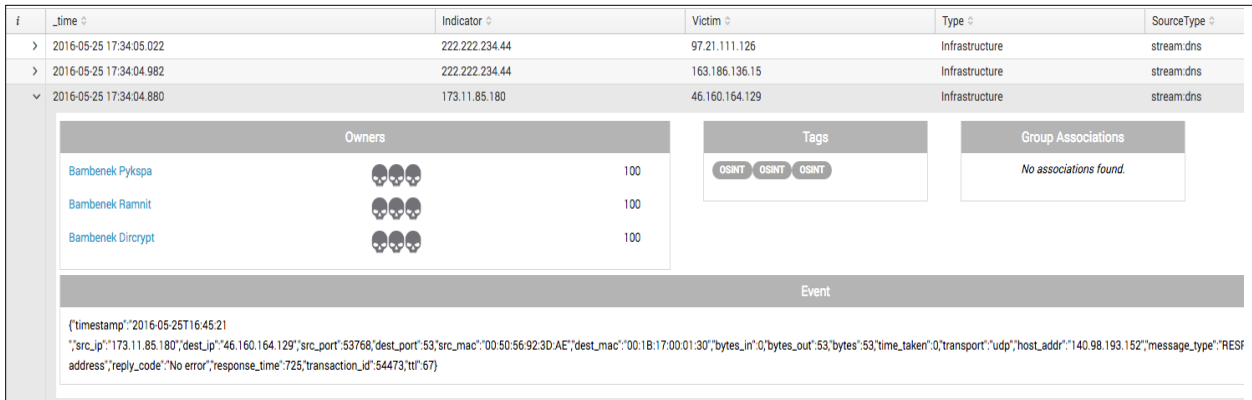


Figure 15

- **\_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 Alerts or automatically when searching the data models.
- **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 16) displays matched Indicators by Owners. A dropdown option is available to narrow down the window of time for the results.

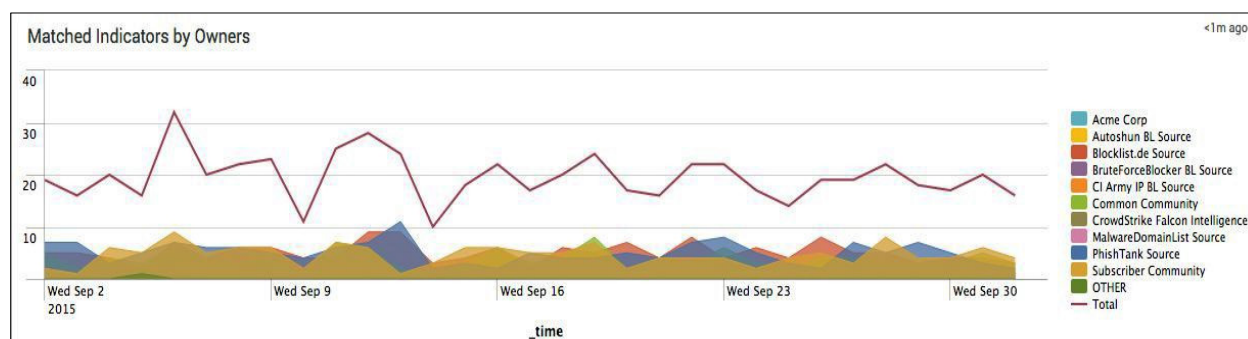


Figure 16

The second row displays additional paginated tables for matched Indicators (Figure 17). 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 <span>2m ago</span>			Top Matched Tags <span>2m ago</span>		
indicator.indicator ▾	count ▾	percent ▾	tag.name ▾	count ▾	percent ▾
http://youngstownchrysler.com/login.php	2	0.32%	Mail	152	16.45%
http://yensaongoctran.com/themes.php	2	0.32%	Apache	151	16.34%
http://www.yeefay.com/backback/ie/news.html	2	0.32%	Phishing	110	11.90%
http://www.yahoodaily.biz/norton/nfhostinfo.asp	2	0.32%	Aspxor	105	11.36%
http://www.winphonemi.com/backup/ietest/sport.html	2	0.32%	China	65	7.03%
http://www.winphonemi.com/backup/ie/calc.swf?happy=calc	2	0.32%	Advanced Persistent Threat	65	7.03%
http://www.tibetonline.info/conime.exe	2	0.32%	Spamming	62	6.71%
http://www.taomengx.com/backup/ietest/test.swf	2	0.32%	Crimeware	25	2.71%
http://vitagrafiastudio.com/list.php	2	0.32%	Upatre	22	2.38%
http://unikbrand.co/gallery.php	2	0.32%	Dyre	22	2.38%
<div> <div>« prev</div> <div>1</div> <div>2</div> <div>next »</div> </div> <div> <div>🔍</div> <div>⬇</div> <div>🔗</div> <div>🔄</div> </div>			<div> <div>« prev</div> <div>1</div> <div>2</div> <div>next »</div> </div>		

Figure 17

## The Event Triage Dashboard

The **Event Triage** dashboard (Figure 18) allows users to view and filter all matched events and take action on the events. The **Reviewed**, **False Positive**, and **Whitelist** buttons at the bottom of the screen allow bulk action on Indicators, while the **Mark False Positive**, **Mark Reviewed**, and **Whitelist** 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. When the **Whitelist** 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 add a tag of **SplunkWhitelisted**. This tag can be used to filter these Indicators from future downloads. The user must have the **tc\_user** role to update the status of the events.

**Event Triage**  
Events that have matches indicators.

Indicator Type: All Types | Minimum Threat Rating: All Ratings | Minimum Confidence Rating: All Confidences | Owner: All Owners | State: New

Indicator: \* | Victim: \* | Period: Last 7 Days

2,988 results

i	_time	Notes	Indicator	Indicator Type	Victim	Owner	Threat Rating	Confidence Rating	Tags	Source Type	Actions
>	2017-09-05 12:01:28.702		<a href="#">74.125.22.189</a>	Address	74.125.22.189	TC Integrations		0	Phishing Host	stream:ip	<a href="#">Reviewed</a>   <a href="#">False Positive</a>   <a href="#">Whitelist</a>
>	2017-09-05 12:01:26.601		<a href="#">127.0.0.1</a>	Address	127.0.0.1	TC Integrations		80	Flashpoint Torrent Tracking SplunkWhitelisted	stream:http	<a href="#">Reviewed</a>   <a href="#">False Positive</a>   <a href="#">Whitelist</a>
>	2017-09-05 12:01:26.601		<a href="#">127.0.0.1</a>	Address	127.0.0.1	yellow		80	Flashpoint Torrent Tracking SplunkWhitelisted	stream:http	<a href="#">Reviewed</a>   <a href="#">False Positive</a>   <a href="#">Whitelist</a>
>	2017-09-05 12:01:26.406		<a href="#">74.125.29.189</a>	Address	74.125.29.189	TC Integrations		0	Phishing Host	stream:ip	<a href="#">Reviewed</a>   <a href="#">False Positive</a>   <a href="#">Whitelist</a>
>	2017-09-05 12:01:26.209		<a href="#">2.2.2.2</a>	Address	2.2.2.2	TC Integrations		30		stream:smtp	<a href="#">Reviewed</a>   <a href="#">False Positive</a>   <a href="#">Whitelist</a>

Figure 18

To add a comment on a matched event, click the icon in the **Notes** column, and the **Notes** pop-up screen will appear (Figure 19).

**Event Triage**  
Events that have matches indicators.

Indicator Type: All Types | Minimum Threat Rating: All Ratings | Indicator: \* | Victim: \* | Period: Last 7 Days

2,988 results

**Notes**

74.125.22.189 notes...

Cancel
Save

i	_time	Notes	Indicator	Indicator Type	Victim	Owner	Threat Rating	Confidence Rating	Tags	Source Type	Actions
>	2017-09-05 12:01:28.702		<a href="#">74.125.22.189</a>	Address	74.125.22.189	TC Integrations		0	Phishing Host	stream:ip	<a href="#">Reviewed</a>   <a href="#">False Positive</a>   <a href="#">Whitelist</a>
>	2017-09-05 12:01:26.601		<a href="#">127.0.0.1</a>	Address	127.0.0.1	TC Integrations		80	Flashpoint Torrent Tracking SplunkWhitelisted	stream:http	<a href="#">Reviewed</a>   <a href="#">False Positive</a>   <a href="#">Whitelist</a>
>	2017-09-05 12:01:26.601		<a href="#">127.0.0.1</a>	Address	127.0.0.1	yellow		80	Flashpoint Torrent Tracking SplunkWhitelisted	stream:http	<a href="#">Reviewed</a>   <a href="#">False Positive</a>   <a href="#">Whitelist</a>
>	2017-09-05 12:01:26.406		<a href="#">74.125.29.189</a>	Address	74.125.29.189	TC Integrations		0	Phishing Host	stream:ip	<a href="#">Reviewed</a>   <a href="#">False Positive</a>   <a href="#">Whitelist</a>
>	2017-09-05 12:01:26.209		<a href="#">2.2.2.2</a>	Address	2.2.2.2	TC Integrations		30		stream:smtp	<a href="#">Reviewed</a>   <a href="#">False Positive</a>   <a href="#">Whitelist</a>

Figure 19

The **Indicator** column has two links in the form of icons. The first link redirects the user to [threatconnect.com](https://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 Diamond Dashboard

This screen allows users to look up an Adversary, Incident, or Threat group from a specified Owner in ThreatConnect. A Diamond Model profile of the group is given and includes all known capabilities, infrastructure, and related Incidents. Indicators associated to the group are matched using specified Common Information Model (CIM) data models. The first section of the dashboard allows the user to query a group with specified data models (Figure 20).

The screenshot shows the 'Diamond Dashboard' search interface. It features five dropdown menus: 'Data Models' (set to 'Network\_Traffic'), 'Owner' (set to 'Intel 471'), 'Type' (set to 'Incident'), 'Name' (set to 'Actor BuggiCorp is selling...'), and 'Time Period' (set to 'Last 1 day'). A green 'Submit' button is located to the right of the 'Time Period' dropdown.

Figure 20

The query parameters are specified by the following fields:

- **Data Models:** Select the CIM Data Model to match events against the group’s Indicators.
- **Owner:** Select the Owner (i.e., Source, Community, or Organization) in which the group exists.
- **Type:** Select the group Type (i.e., Adversary, Incident, or Threat).
- **Name:** Select the specific group by name.
- **Time Period:** Select the time period for the historical search.

The second section of the dashboard shows a Diamond Model breakout of the queried group (Figure 21). The **Adversary/Threat** table shows Adversary and Threat associations to the queried group. The **Associations** table shows all associated Documents, Emails, Incidents, and Signatures to the queried group. The **Capability** table shows all known associated Common Vulnerabilities and Exposures (CVE) and malware files by MD5 hash. The **Infrastructure** table shows all Address, Email, Host, and URL Indicators associated to the queried group.

Adversary / Threat		12m ago	Associations		12m ago
name	type		name	type	
Ge Xing aka GreenSky27	Adversary		20130712C: Teachings on Buddhism Doc Exploit	Incident	
Naikon	Threat		20130731B: SECRET Personal Doc Exploit	Incident	
			20120412A: Beware of what you download.	Incident	
			20130425A: Targeted Attack Campaign Hides Behind SSL Communication	Incident	
			20140309A: Search for MH370 Naikon APT	Incident	
			<a href="#">prev</a> <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> <a href="#">5</a> <a href="#">6</a> <a href="#">7</a> <a href="#">next</a>		

Capability: File Hashes CVE		12m ago	Infrastructure: Addresses Email Host URL		12m ago
indicator	type		indicator	type	
D92E68C488ADC372FA99C9B7F4F452D	File		113.10.220.215	Address	
8D5464F7C6C03FEEA5236931C8D4F05	File		113.10.220.54	Address	
FE2188F0F8FC3445D77876304428D71	File		208.77.46.251	Address	
BF178232711AC6EC28F38198B940E100	File		219.90.115.251	Address	
11253081BC4541FECF089A71506E56B7	File		175.45.208.114	Address	
			<a href="#">prev</a> <a href="#">1</a> <a href="#">2</a> <a href="#">3</a> <a href="#">4</a> <a href="#">5</a> <a href="#">6</a> <a href="#">7</a> <a href="#">8</a> <a href="#">9</a> <a href="#">10</a> <a href="#">next</a>		

Figure 21

The third section of the dashboard shows a timeline and table of CIM events matched to the queried group (Figure 22).

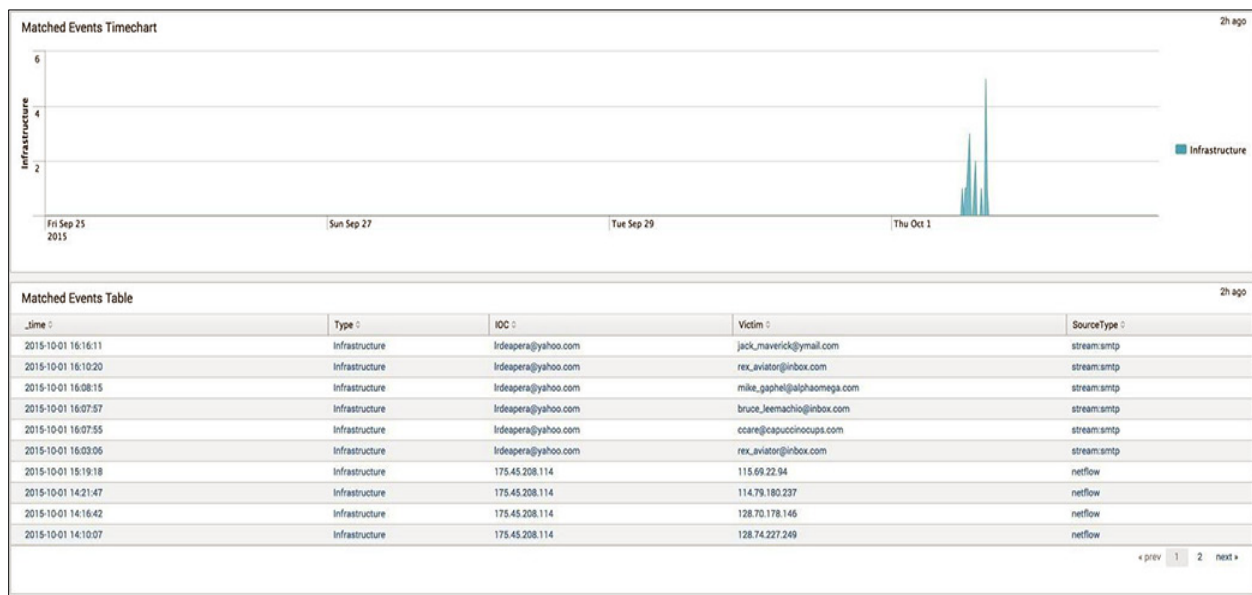


Figure 22

# The Indicator Search Screen

The **Indicator Search** screen allows manual lookup of Indicators against the ThreatConnect API (Figure 23). The Indicator type is automatically detected.

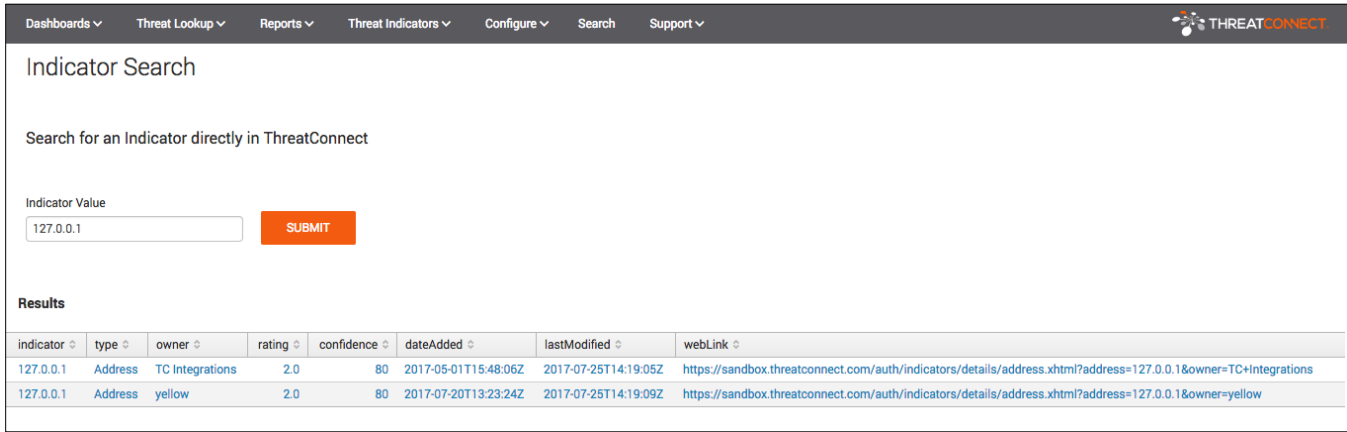


Figure 23

# The Indicator Review Dashboard

The **Indicator Review** dashboard allows users to search for and filter Indicators (Figure 24).

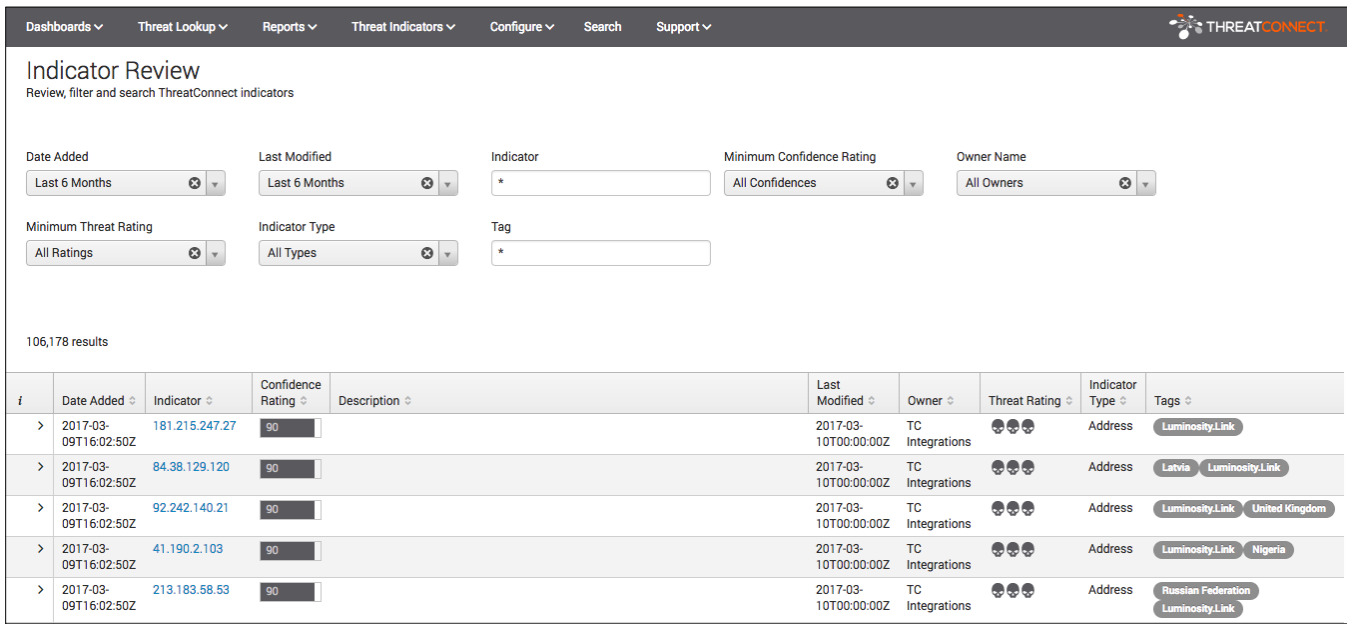


Figure 24

Each Indicator record expands and displays additional Indicator information, in real time, retrieved directly from the ThreatConnect API (Figure 25).



Figure 25

## The IOC Download Report Screen

The **IOC 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 26). User-defined custom reports can be added for more detailed views into the ThreatConnect data.

Daily download stats for each Owner.							Edit ▾	More Info ▾	Download	Print
date ▾	owner ▾	added ▾	deleted ▾	filtered ▾	updated ▾	total ▾	<1m ago			
2015-10-02	Acme Corp	11176	0	0	0	11176				
2015-10-02	Blocklist.de Source	55914	0	0	0	55914				
2015-10-02	Common Community	39117	0	3	0	39120				
2015-10-02	Demo Customer Community	2622	0	1	0	2623				
2015-10-02	MalwareDomainList Source	1025	0	0	0	1025				
2015-10-02	Subscriber Community	40433	0	0	0	40433				
2015-10-02	Test Community	131	0	0	0	131				
2015-10-02	abuse.ch Zeus Tracker Source	332	0	0	0	332				

Figure 26

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



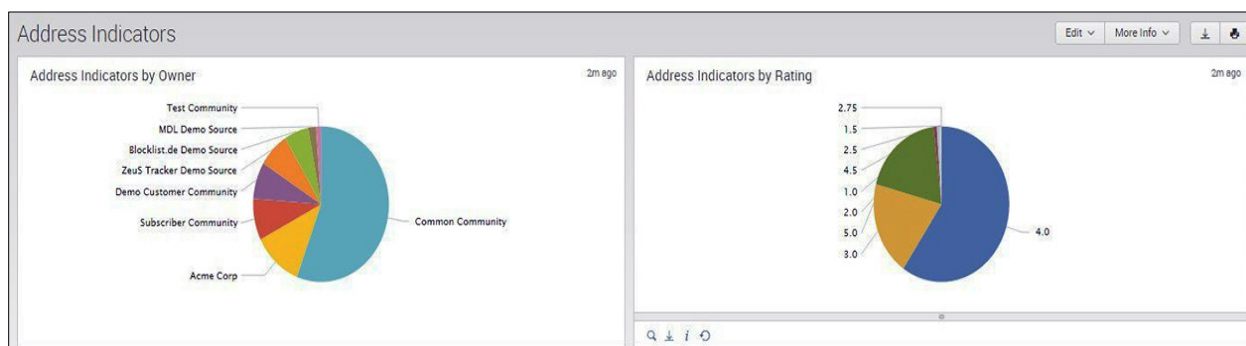


Figure 27

The second row contains two tables that display the last 10 created and updated Indicators, respectively (Figure 28).

Last 10 Added Address Indicators				Last 10 Updated Address Indicators			
dateAdded	Indicator	rating	ownerName	lastModified	Indicator	rating	ownerName
2014-10-10T11:51:33Z	50.63.202.95	4.0	Acme Corp	2014-10-10T15:22:05Z	50.63.202.95	4.0	Acme Corp
2014-10-09T19:39:12Z	198.55.119.125	4.0	Subscriber Community	2014-10-09T19:39:12Z	198.55.119.125	4.0	Subscriber Community
2014-10-09T17:01:45Z	11.38.113.138	1.0	Subscriber Community	2014-10-09T17:01:45Z	11.38.113.138	1.0	Subscriber Community
2014-10-08T01:36:45Z	89.207.135.125	5.0	Acme Corp	2014-10-08T01:36:45Z	89.207.135.125	5.0	Acme Corp
2014-10-08T01:36:45Z	75.127.84.182	5.0	Acme Corp	2014-10-08T01:36:45Z	75.127.84.182	5.0	Acme Corp
2014-10-08T01:36:45Z	42.120.145.23	5.0	Acme Corp	2014-10-08T01:36:45Z	42.120.145.23	5.0	Acme Corp
2014-10-08T01:36:45Z	67.229.128.88	5.0	Acme Corp	2014-10-08T01:36:45Z	67.229.128.88	5.0	Acme Corp
2014-10-08T01:36:45Z	153.121.58.243	5.0	Acme Corp	2014-10-08T01:36:45Z	153.121.58.243	5.0	Acme Corp
2014-10-08T01:36:45Z	82.99.57.32	5.0	Acme Corp	2014-10-08T01:36:45Z	82.99.57.32	5.0	Acme Corp
2014-10-08T01:36:45Z	114.96.140.114	5.0	Acme Corp	2014-10-08T01:36:45Z	114.96.140.114	5.0	Acme Corp

Figure 28

The final row displays a paginated table of all the Indicators of that type pulled from ThreatConnect (Figure 29).

Address Indicators							2m ago
confidence	dateAdded	id	ip	lastModified	ownerName	rating	webLink
79	2014-10-10T11:51:33Z	301131	50.63.202.95	2014-10-10T15:22:05Z	Acme Corp	4.0	https://app.threatconnect.com/tc/auth/indicators/details/address.xhtml?address=50.63.202.95&owner=Acme+Corp
100	2014-10-08T01:36:45Z	299776	89.207.135.125	2014-10-08T01:36:45Z	Acme Corp	5.0	https://app.threatconnect.com/tc/auth/indicators/details/address.xhtml?address=89.207.135.125&owner=Acme+Corp
100	2014-10-08T01:36:45Z	299777	75.127.84.182	2014-10-08T01:36:45Z	Acme Corp	5.0	https://app.threatconnect.com/tc/auth/indicators/details/address.xhtml?address=75.127.84.182&owner=Acme+Corp
100	2014-10-08T01:36:45Z	299778	42.120.145.23	2014-10-08T01:36:45Z	Acme Corp	5.0	https://app.threatconnect.com/tc/auth/indicators/details/address.xhtml?address=42.120.145.23&owner=Acme+Corp
54	2014-10-08T01:36:45Z	299779	67.229.128.88	2014-10-08T01:36:45Z	Acme Corp	5.0	https://app.threatconnect.com/tc/auth/indicators/details/address.xhtml?address=67.229.128.88&owner=Acme+Corp
100	2014-10-08T01:36:45Z	299780	153.121.58.243	2014-10-08T01:36:45Z	Acme Corp	5.0	https://app.threatconnect.com/tc/auth/indicators/details/address.xhtml?address=153.121.58.243&owner=Acme+Corp
100	2014-10-08T01:36:45Z	299781	82.99.57.32	2014-10-08T01:36:45Z	Acme Corp	5.0	https://app.threatconnect.com/tc/auth/indicators/details/address.xhtml?address=82.99.57.32&owner=Acme+Corp
100	2014-10-08T01:36:45Z	299782	114.96.140.114	2014-10-08T01:36:45Z	Acme Corp	5.0	https://app.threatconnect.com/tc/auth/indicators/details/address.xhtml?address=114.96.140.114&owner=Acme+Corp
0	2014-10-08T01:36:45Z	299792	185.31.209.84	2014-10-08T01:36:45Z	Acme Corp	5.0	https://app.threatconnect.com/tc/auth/indicators/details/address.xhtml?address=185.31.209.84&owner=Acme+Corp
100	2014-10-06T20:30:48Z	299132	128.199.223.129	2014-10-06T20:30:48Z	Acme Corp	3.0	https://app.threatconnect.com/tc/auth/indicators/details/address.xhtml?address=128.199.223.129&owner=Acme+Corp
							« prev 1 2 3 4 5 6 7 8 9 10 next »

Figure 29

## 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 30).

i	Time	Event
▼	2/22/16 7:59:41.000 PM	Feb 22 19:59:41 acmeapp1 vendor=Websense 9f product=Security product_version=7.7.0 - http_user_agent=- http_proxy_status_code=0 reason=- disposition=1060 policy=Unfi

Event Actions ▼

Add Event to Investigation  
 Build Event Type  
 Extract Fields  
 Show Source  
 TC Add IP: 10.64.144.88  
 TC Add IP: 1.165.156.121  
 TC Quick Add IP: 10.64.144.88  
 TC Quick Add IP: 1.165.156.121  
 TC Source IP Lookup: 10.64.144.88  
 TC Lookup Destination IP: 1.165.156.121

Value	Actions
ip-10-1-2-231	▼
/opt/splunk/var/spool/splunk/sample.websense	▼
websense	▼
allowed	▼
0	▼
1398	▼
72	▼
72	▼
1.165.156.121	▼
31.13.77.42	▼
1.165.156.121	▼
false	▼
31.13.77.42	▼
untrust	▼
80	▼
false	▼
false	▼
false	▼
1060	▼
0	▼

### Figure 30

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 31).

2/22/16

7:59:41.000 PM

Feb 22 19:59:41 acmeapp1 vendor= Websense 9f product=Security product\_version=7.7.0 action=p  
- http\_user\_agent=- http\_proxy\_status\_code=0 reason=- disposition=1060 policy=Unfiltered\_UR

Event Actions ▾

Type	Field	Value	Actions
Selected	<input checked="" type="checkbox"/> host ▾	ip-10-1-2-231	▾
	<input checked="" type="checkbox"/> source ▾	/opt/splunk/var/spool/splunk/sample.websense	▾
	<input checked="" type="checkbox"/> sourcetype ▾	websense	▾
Event	<input type="checkbox"/> action ▾	allowed	▾
	<input type="checkbox"/> bytes_in ▾	0	▾
	<input type="checkbox"/> bytes_out ▾	1398	▾
	<input type="checkbox"/> category ▾	72	▾
	<input type="checkbox"/> category_id ▾	72	▾
	<input type="checkbox"/> dest ▾	1.165.156.121	▾
	<input type="checkbox"/> dest_host ▾	31.13.77.42	▾
	<input type="checkbox"/> dest_ip ▾	1.165.156.121	▾
	<input type="checkbox"/> dest_is_expected ▾	false	▾
	<input type="checkbox"/> dest_nt_host ▾	31.13.77.42	▾
	<input type="checkbox"/> dest_pci_domain ▾	untrust	▾
	<input type="checkbox"/> dest_port ▾	80	▾
	<input type="checkbox"/> dest_requires_av ▾	false	▾
	<input type="checkbox"/> dest_should_timesync ▾	false	▾
	<input type="checkbox"/> dest_should_update ▾	false	▾
	<input type="checkbox"/> disposition_id ▾	1060	▾
	<input type="checkbox"/> duration ▾	0	▾
	<input type="checkbox"/> eventtype ▾	websense ( proxy web )	▾
	<input type="checkbox"/> host_is_expected ▾	false	▾
	<input type="checkbox"/> host_pci_domain ▾	untrust	▾
	<input type="checkbox"/> host_requires_av ▾	false	▾
	<input type="checkbox"/> host_should_timesync ▾	false	▾

Intrusion Search (as source)

Malware Search

Stream Capture

TC Add: 1.165.156.121

TC Indicator Lookup: 1.165.156.121

Traffic Search (as destination)

Traffic Search (as source)

Update Search

Vulnerability Search

Web Search (as destination)

Figure 31

## 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_events
```

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](#).

#### Demo Data (`tcdemo`)

For users who would like to evaluate the ThreatConnect App for Splunk in a staging environment, the App provides a method to generate demo data for the dashboards.

From the App’s search tab, run the search `| tcdemo`, and the dashboard data will be automatically generated. The command uses Indicators downloaded from ThreatConnect to generate the demo data, so the Indicator download script must be run before the demo data script is run. Ensure that there is an ample number of Indicators of each type in the ThreatConnect platform before downloading.

**NOTE: In order to remove the demo data, all matched events will have to be removed. Therefore, it is recommended to use the demo data generation only in a non-production environment.**

## 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_events	This collection stores the matched event-summary data.	admin, tc_admin, tc_user	admin, tc_admin, tc_user
tc_events_data	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_logs	This collection stores the temporary App logs.	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 the 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

## 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 <b>tcalert</b> 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 <b><i>Clear Data (tcclear)</i></b> 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 is used to collect 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
tcdemo	This command will generate sample event data. See the <b><i>Demo Data (tcdemo)</i></b> section.	admin, tc_admin	admin, tc_admin
tcdiamondsearch	This command is used to process searches from the Diamond Dashboard.	admin, tc_admin, tc_user	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 <b>owner_key</b> 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: 2.13.0
- Dateutil: 2.4.2
- Enum: 1.0.4
- Splunklib: 1.6.2
- 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