ThreatQuotient

ThreatQ User Guide

Version 4.16

February 26, 2019

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Last Updated: Friday, May 10, 2019

Contents

Introduction

The following provides an introduction to the ThreatQ platform.

ThreatQ Introduction

ThreatQ is a cyber threat intelligence platform that focuses on centralizing, structuring, and strengthening a security organization's intelligence-driven defensive posture against attacks.

Concept Overview

The following describes how ThreatQ helps organizations manage threat intelligence, allowing them to defend against sophisticated cyber-attacks.

Threat Library

A central repository combining global and local threat data to provide relevant and contextual intelligence that is customized for your unique environment. Over time, the library becomes more and more tuned to your environment and fills in the intelligence gaps created by different sources, all providing only some pieces of the puzzle.

Adaptive Workbench

An open and extensible work area for security experts across the organization to work within your processes and tools. A customizable workflow and customer-specific enrichment streamlines investigations and analysis, and automates the intelligence life cycle.

Open Exchange

ThreatQ is the only threat intelligence platform specifically designed for customization to meet the requirements of your unique environment. Get more from your existing security investments by integrating your tools, teams and workflows through standard interfaces and an SDK/API for customization.

System Access

The following describes how to login and log out of the platform.

System Access Overview

To access the ThreatQ web UI, you must authenticate yourself with a username and password. You can use the main menu to access ThreatQ functionality.

System Login

When you installed ThreatQ, you set up the default user account, *Maintenance Account*, which you can use to log into the web UI.

Using this account, you can create additional user accounts.

Passwords must be 15 characters or longer. There is no limit on the character type.

Logging into ThreatQ

When you installed ThreatQ, you defined an IP address for the web UI, and set up the *Maintenance Account* and password.

1. In your web browser, navigate to `https://your-ThreatQ-web-ip-address`.

2. Enter your username (email address) and password.
3. Optionally, if you have 2-step verification enabled, complete the following steps:
    - Enter your verification code from Google Authenticator.
    - Optionally, choose to **Remember this computer for 30 days**.
4. Click **Login** or **Submit**.

Session Timeout

User sessions time out after 30 minutes of inactivity.

Managing your User Account

When you choose the **Settings icon > My Account**, the system directs you to the Edit User page for your current login. From here, you can edit your user account, set up 2-step verification, or view your login history.

Procedure

1. Choose the **Settings icon > My Account**.

   Users that have upgraded to **ThreatQ 4.1** will see an avatar icon in place of the **My Account** link. Click on the icon and select **My Account**.

2. On the User Profile tab, you can edit the following settings of your user account:
   - Name
   - Title
   - Email
   - Password
3. You can update your user avatar; see Update User Avatar.

   The User Avatar feature is only available with ThreatQ 4.1 and later.

4. Optionally, you can set up 2-step verification; see 2 Step Verification.
5. Optionally, on the Login Activity tab, you can view:
   - The last date and time you logged in.
   - The IP Address where you logged in.
   - Whether the login was successful or not.
6. Click **Save**.

User Avatar Icons

The User Avatar feature is only available with ThreatQ 4.1 and later.

User avatar icons provide a personalized look to your ThreatQ dashboard. Clicking on the avatar icon will reveal the **My Account** and **Log out** options.

Users can update their avatars by clicking on the avatar and selecting **My Account**.

- Update User Avatar Graphic

Update User Avatar Graphic

> The User Avatar feature is only available with ThreatQ 4.1 and later.

1. Click on avatar icon located to the top-right on the screen and select **My Account**.

   The *Edit User* form will load.

2. Click on the green **Add User Avatar** button and select the icon graphic to upload.

   > Users can also click and drag the new icon graphic onto the page

3. Click on **Save** at the bottom of form.

2 Step Verification

When you enable 2-Step Verification (also known as two-factor authentication), you add an extra layer of security to your account. After 2-Step Verification is active, you sign in with your password and a code sent to your mobile device.

- Enabling 2 Step Verification

Enabling 2 Step Verification

Procedure:

1. Choose the **Settings icon> My Account**.

Users that have upgraded to **ThreatQ 4.1** will see an avatar icon in place of the **My Account** link. Click on the icon and select **My Account**.

2. Under Enable 2-Step Verification, click **Turn On**.
3. In the Enable 2 Step Verification dialog box, complete the following:
   - Scan the qr code using your Google Authenticator mobile app.
   - Enter the validation code delivered to your mobile device via Google Authenticator.
   - Click **Submit**.
4. Click **Save**.

What to do next

The next time you log in, you must use the newest verification code.

Licensing

The following provides an overview of licensing for the ThreatQ platform.

Licensing Overview

Your ThreatQ deployment requires a license to initialize the platform. ThreatQ Support provides the initial license and any subsequent licenses provided to maintain the platform. You apply the initial ThreatQ license during first boot, as described in the ThreatQ Getting Started Guide. Any subsequent license updates can be applied in the ThreatQ user interface.

Viewing the License Status

ThreatQ licenses are not perpetual. To view the license expiration date, complete the following steps:

Procedure

Choose the Help icon **>About** .

Updating a License

If you receive a new license from Support, apply the new license by accessing the About page.

Procedure

1. Choose the Help icon **>About** .
2. Choose **Update License**.
3. Enter the new license key.
4. Click **Submit**.

User Management

The following describes how to manage user accounts.

User Management Overview

ThreatQ uses role-based access control to manage user accounts. The system provides several user roles, each containing a set of permissions for accessing system functionality. You create user accounts, and assign them to a user role. The user role determines each account's set of permissions.

After you create a user account, you can modify the user role group, full name, and email address.

User Roles

The following details the user roles and their associated permissions.

User Role	Permissions
Maintenance Account	Members have access to the entire ThreatQ user interface and can edit all data.

User Role	Permissions
	Note: This account can not be deleted
Administrative Access	Members have access to the entire ThreatQ user interface and can edit all data.
Primary Contributor Access	Members have access to most of the ThreatQ user interface, except for: • User Management • Incoming Feeds • Exports • Operations Management • OAuth Management • System Configurations Members can edit: • Their own user info • Whitelist Management • Operations Management • Object meta data • Saved Searches

User Role	Permissions
Read Only Access	Members have access to most of the ThreatQ user interface, except for: • User Management • Incoming Feeds • Indicator Management • Whitelist Management • Exports • Operations Management • OAuth Management • System Configurations Members cannot edit any data. Members can export search results.

User Account Creation

When you first install ThreatQ, the system creates a default user account, the Maintenance Account. You cannot delete this account, and you can use it to initially create other user accounts. Each user account must have a unique username.

Only the Maintenance Account and Administrative Access user role have permissions to access user management functionality. You can only create new user accounts if logged in as one of these roles.

User Account Properties

Property	Description	Validation
Name	full name of the user associated with this account	any alphabetic character and spaces
Title	optional user title	any alphabetic character and spaces
Group	roles which this user account belongs to	at least one role selected
Email	email address associated with this account	valid email address, such as user-@domain.com
Password	initial password associated with the username	all characters

Adding a User

1. From the main menu, choose the **Settings icon > User Manangement**.
2. Click **Add User**.
3. Enter the user's **Name**.
4. Optionally, enter the user's **Title**.
5. Select the level of access for the user from the **Group** drop-down menu.

   Choose from the following options:

- Maintenance Account
- Administrative Access
- Primary Contributor Access
- Read Only Access

6. Enter the user's **Email** address.
7. Enter a password for the user.
8. Retype the password.
9. Click **Add User**.

User Account Modification

After you create a user account, you can modify the account's role group, full name, title, email address, and password.

- Editing a User
- Resetting User Passwords from the Command Line
- Deleting a User

Editing a User

1. From the main menu, choose the **Settings icon > User Manangement**.
2. Click the name of the user whose profile you wish to edit.

   The Edit User page appears.

3. Edit the user fields as desired; see User Account Properties.
4. To change the password, click **Change Password**.
5. Click **Save**.

Resetting User Passwords from the Command Line

If you have root access to your ThreatQ installation, you can reset any user's password from the command line.

1. Login to the ThreatQ command line as root.
2. Navigate to the api directory:

   ```
   cd /var/www/api
   ```

3. Run the following command:

   ```
   sudo php artisan threatq:password-reset
   ```

4. At the prompt, enter the email address for the user whose password you are resetting.
5. At the prompt, enter the new password.
6. At the prompt, re-enter the new password to confirm.

Deleting a User

Deleting a user cannot be undone.

1. From the main menu, choose the **Settings icon > User Manangement**.
2. Select the user(s) you wish to delete.
3. Click the **Delete.** icon.
   A confirmation dialog box appears, asking if you are sure.
4. Click **Delete Users**.

System Configurations

The following describes how to manage various system configurations in ThreatQ.

- System Configuration: Indicator Statuses
- System Configuration: Indicator Types
- System Configuration: Event Types
- System Configuration: Proxy
- LDAP Authentication
- System Configuration: Date and Time Format

System Configuration: Indicator Statuses

The System Configuration: Indicator Statuses page allows you to view, duplicate, add, edit, and delete available system-wide indicator statuses. You cannot edit and delete indicator statuses provided by ThreatQ, but you can add new statuses and edit or delete your custom statuses.

Indirect Indicator Status

For feeds that set multiple statuses, A status of *Indirect* is assigned to indicators that meet the following criteria:

- Indicators created from the relations array are imported with a status of *Indirect*.
- If an indicator already exists, its original status value will remain the same. However, if the status is *Indirect*, and it is received as a parent indicator, its value will be updated as defined in the connector configuration.

Currently, this status only applies to CrowdStrike and iSight feeds, where:

- For CrowdStrike, *Indirect* indicates that ThreatQ received the indicator from the relations list for the parent indicator.
- For iSight Partners, *Indirect* indicates that ThreatQ received an indicator that does not have an attribute of *Attack* or *Compromised*.

Viewing Indicator Statuses

To view existing indicator statuses, complete the following procedure.

Procedure:

1. Choose the **Settings icon > System Configurations**.

   The System Configurations page opens to the Indicator Statuses tab.

   Statuses found within ThreatQ are listed by status, number, and description within the Indicator Statuses table.

2. Optionally, to sort the table by a column, click the column header. To reverse the column sorting order, click the header a second time.

Adding an Indicator Status

To add an indicator status that can be applied to any system indicator, complete the following procedure.

Procedure:

1. Choose the **Settings icon > System Configurations**.

   The System Configurations page opens to the Indicator Statuses tab.

2. Click **Add New Status**.
3. Enter a **Status Name**.
4. Optionally, enter a **Status Description**.
5. Click **Add Status**.

Editing an Indicator Status

To edit an existing indicator status, complete the following procedure. You cannot edit indicator statuses provided by ThreatQ.

Procedure:

1. Choose the **Settings icon > System Configurations**.

   The System Configurations page opens to the Indicator Statuses tab.

2. Determine the indicator you want to edit and click **Edit** in the far right column.
3. Optionally, enter a new **Status Name**.
4. Optionally, enter a new **Status Description**.
5. Click **Save Changes**.

Deleting an Indicator Status

To delete an indicator status, complete the following procedure. You cannot edit and delete indicator statuses provided by ThreatQ. Custom statuses can only be deleted if there are no indicators using that status.

Procedure:

1. Choose the **Settings icon > System Configurations**.

   The System Configurations page opens to the Indicator Statuses tab.

2. Determine the indicator you want to delete and select the corresponding checkbox in the first column.
3. Click the **Delete icon** in the upper right hand corner.
4. Click **Delete Statuses**.

System Configuration: Indicator Types

The Indicator Types table allows you to view a list of indicator types found in ThreatQ and the number of those indicators within the system.

To view Indicator Types found within ThreatQ:

1. Go to **ThreatQ Configuration** > **System Configurations**.

   The System Configurations page opens.

2. Click the **Indicators** sub-tab.

   The Indicator Types page opens.

From the Indicators sub-tab, the following functions are available:

- *Viewing existing indicators by type and number*

  Indicators found within ThreatQ are listed by type and number in the Indicator Types table.

System Configuration: Event Types

The System Configuration: Events page allows you to view, add, and delete system events. Event types provided by ThreatQ cannot be edited or deleted, but you can add new event types and edit or delete your event types.

Custom statuses can only be deleted if there are no indicators using that event type.

To view Event Types found withing ThreatQ:

1. Go to **ThreatQ Configuration** > **System Configurations**.

   The System Configurations page opens.

2. Click the **Events** sub-tab.

   The Event Types page opens.

From the Events sub-tab, the following functions are available:

- ***Viewing existing events by type and number***

  Events found within ThreatQ are listed by type and number in the Event Types table.

- ***Adding an event type***

  At the top right of the Event Types table, click **+ Add**, and follow the steps.

- **Editing an event type**

  Editable events have an edit option in the Event Types table. Click **edit**, and follow the steps.

- ***Deleting an event type***

  Select the event type(s) you wish to delete, and click **Delete** at the top right of the Statuses table.

- ***Changing the number of entries displayed in the table***

  Click the dropdown menu at the top right of the table and select the desired option.

- ***Sorting the table by a column***

  Click the column header. To reverse the column sorting order, click the header a second time.

System Configuration: Proxy

The System Configuration: Proxy page allows you to enable or disable proxies.

Users are required to set their proxy server settings to use http: for their https: traffic. The ThreatQ **Proxy Configuration** page can be found by navigating to **Settings > System Configuration > Proxy**.

Access Proxies

To access proxies:

1. Go to **ThreatQ Configuration** > **System Configurations**.

   The System Configurations page opens to the Statuses sub-tab.

2. Click the **Proxy** sub-tab.

   The Proxy Configuration table appears.

From the Proxy sub-tab, the following functions are available:

- ***Enabling a proxy for HTTP or HTTPS traffic***

  Check the correct proxy type and enter configuration details. Click **Save Changes**. ThreatQ will check that the proxy has been configured properly.

- ***Disabling a proxy for HTTP or HTTPS traffic***

  Uncheck the proxy you wish to disable, and click **Save Changes**.

LDAP Authentication

ThreatQ allows you to configure system access via LDAP, the Lightweight Directory Access Protocol. You can configure a basic LDAP or configure a secure connection to your LDAP server.

When configuring LDAP, it is important to note the following:

- Local users and LDAP users may exist on the same system.
- ThreatQ will check the LDAP user table first for any attempted login, then fall back to the local user table if no entry is found in the LDAP directory.

Note: Currently, ThreatQ supports LDAP authentication on LDAP servers running OpenLDAP 2.4, Active Directory 2008, and Active Directory 2012. If you are using a different configuration, please contact ThreatQ Support.

Required Information for Creating LDAP Authentication

Before you configure a connection to your LDAP server, you should work with your LDAP administrator to collect, at minimum, the following information:

- the server name or IP address for the server where you plan to connect
- the server type of the server where you plan to connect, typically LDAP for basic and LDAPS for secure LDAP
- if possible, the base distinguished name for the server directory where the user names reside

Configuring LDAP

For ThreatQ to identify different user types, your LDAP server should include groups under an organizational unit, OU, for each user role:

- Maintenance Account
- Administrative Access

- Primary Contributor Access
- Read Only Access

> **Note:** Only users with an Administrative or Maintenance account can access LDAP settings.

Procedure:

1. Choose the **Settings icon > System Configurations**.
2. Choose **LDAP** from the System Configurations toolbar.
3. Configure the following server settings:

Server Address	Enter the name of the server where LDAP is hosted. For example, ldap://[servername]
Port #	Typically, enter 389 for LDAP.
LDAP Domain	Enter the domain for which LDAP is configured to authenticate. For example: threatq.com
Append Domain to Username	Choose from the following options: • Yes for most Active Directory servers • No for most Open Ldap servers
Filter Field Name	This field is specific to your LDAP directory configuration. For example:

	• memberuid • uid
Group Field Name	This field is specific to your LDAP directory configuration. For example: • cn • memberof
Use RDN?	Choose from the following options: • Yes to use Relative Distinguished Names. • No to use full Distinguished Names
Organizational Unit (OU)	This field is specific to your LDAP directory configuration. Your LDAP administrator should provide the correct value for this field.
User Lookup Name	This field is specific to your LDAP directory configuration. For example: • memberUid, for Active Directory • uid, for Open LDAP

4. Next, **Map Your Permission Levels to LDAP**, using the user groups that your LDAP administrator established for each user role. For roles not mapped, you should enter a hyphen: "-." You cannot save the configuration without entering a

value in each field.

> **Note:** You can not list the same LDAP User Group for multiple permission levels.

- For OpenLDAP, consider the following example:

Maintenance Account	ldapSuper
Administrative Access	administrator
Read Only Access	ldapObserver
Primary Contributor Access	ldapAnalyst

- For Active Directory, consider the following example:

Maintenance Account	CN=read-only,CN=Builtin,DC=yourdomain,DC=com
Administrative Access	CN=linux-admins,CN=Builtin,DC=yourdomain,DC=com
Read Only Access	CN=tq-maintenance,CN=Builtin,DC=yourdomain,DC=com

Primary Contributor Access	CN=primary-contributor,CN=Builtin,DC=yourdomain,DC=com

5. Click the **LDAP** toggle switch to enable your LDAP configuration.
6. Click **Save Changes**.

If your LDAP fails to enable or fails to function properly, validate your inputs. If the configuration continues to fail, please contact ThreatQ Support.

Configuring Secure LDAP

To configure secure LDAP, you must complete the following steps:

1. Enter your LDAP settings in the ThreatQ user interface.
2. Access the ThreatQ appliance command line as root and edit openldap.conf.
3. If necessary, run the ThreatQ LDAP utility, to retrieve your LDAP binding strings.

For ThreatQ to identify different user types, your LDAP server should include groups under an organizational unit, OU, for each user role:

- Maintenance Account
- Administrative Access
- Primary Contributor Access
- Read Only Access

> **Note:** Only users with an Administrative or Maintenance account can access LDAP settings.

Procedure:

1. Choose the **Settings icon > System Configurations**.
2. Choose **LDAP** from the System Configurations toolbar.
3. Configure the following server settings:

LDAP Domain	Enter the domain for which LDAP is configured to authenticate. For example: threatq.com
Server Address	Enter the name of the server where LDAP is hosted. For example, ldaps://[servername]
Port #	Typically, enter 636 for ldaps
Organizational Unit (OU)	This field is specific to your LDAP directory configuration. Your LDAP administrator should provide the correct value for this field.
User Lookup Name	This field is specific to your LDAP directory configuration. For example: • memberUid, for Active Directory • uid, for Open LDAP
Use RDN?	Choose from the following options: • Yes to use Relative Distinguished Names. • No to use full Distinguished Names

Append Domain to Username	Choose from the following options: • Yes for most Active Directory servers • No for most Open Ldap servers
Group Field Name	This field is specific to your LDAP directory configuration. For example: • cn • memberof
Filter Field Name	This field is specific to your LDAP directory configuration. For example: • memberuid • uid

4. Next, **Map Your Permission Levels to LDAP**, using the user groups that your LDAP administrator established for each user role. For roles not mapped, you should enter a hyphen: "-." You cannot save the configuration without entering a value in each field.

> **Note:** You can not list the same LDAP User Group for multiple permission levels.

- For OpenLDAP, consider the following example:

Maintenance Account	ldapSuper
Administrative Access	administrator
Read Only Access	ldapObserver
Primary Contributor Access	ldapAnalyst

- For Active Directory, consider the following example:

Maintenance Account	CN=read-only,CN=Builtin,DC=yourdomain,DC=com
Administrative Access	CN=linux-admins,CN=Builtin,DC=yourdomain,DC=com
Read Only Access	CN=tq-maintenance,CN=Builtin,DC=yourdomain,DC=com
Primary Contributor Access	CN=primary-contributor,CN=Builtin,DC=yourdomain,DC=com

5. Click the **LDAP** toggle switch to enable your LDAP configuration.
6. Click **Save Changes**.
7. Access the ThreatQ command line as root.

8. Use vi to edit /etc/openldap/ldap.conf. Make sure that your settings are as follows:

```
#
# LDAP Defaults
#
```

```
# See ldap.conf(5) for details
# This file should be world readable but not world writable.
```

```
BASE    dc=[your domain],dc=com
URI ldap://[your servername]:389 ldaps://[your servername]:636
```

```
#SIZELIMIT  12
#TIMELIMIT  15
#DEREF      never
```

```
TLS_CACERTDIR   /etc/openldap/certs
```

```
# Turning this off breaks GSSAPI used with krb5 when rdns =
false
SASL_NOCANON    on
TLS_REQCERT allow
```

> **Caution:** ThreatQ recommends that you edit ldap.conf on the appliance, rather than editing off box and uploading it. If you do edit the file off box, ensure that you use a linux editor. Windows and Mac editors may corrupt the file.

If your LDAP fails to enable or fails to function properly, validate your inputs. If the configuration continues to fail, please contact ThreatQ Support.

System Configuration: Date and Time Format

You can configure the date and time format of your choice system-wide within the ThreatQ platform.

Note: If you make changes to the date and time format while another user is working concurrently in the same ThreatQ installation, that user must refresh their browser for the changes to take effect.

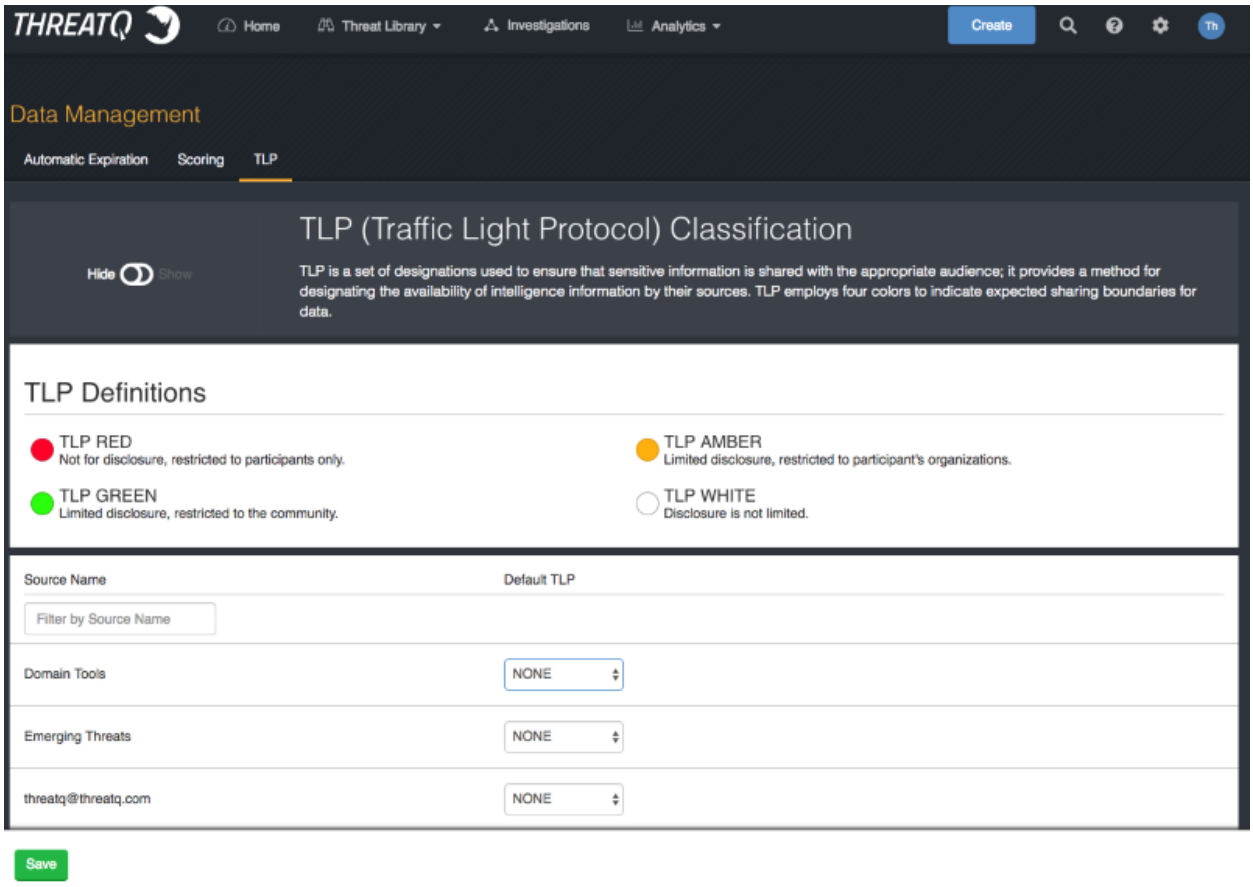
Configuring Date and Time Format

1. From the navigation menu, choose the gear icon > **System Configurations**.
2. From the System Configurations menu, choose **General**.
3. Select the desired **Date Format**.
4. Select the desired **Time Format**.
5. Click **Submit** to save your settings.

Traffic Light Protocol (TLP)

Traffic Light Protocol (TLP) classification provides a set of designations used to ensure that sensitive information is shared with the appropriate audience. ThreatQ provides a method for designating the availability of intelligence information by their sources. Users can also use TLP classifications to filter objects when creating an export - see the Adding an Export topic for more details.

Administrators have the ability to configure TLP visibility settings for the ThreatQ application.



TLP employs four colors to indicate the expected sharing boundaries for data:

Color	Classification	Description
	Red	Not for disclosure, restricted to participants only.

	Amber	Limited disclosure, restricted to participant's organizations.
	Green	Limited disclosure, restricted to the community.
	White	Disclosure is not limited.

TLP Assignment Hierarchy

The ThreatQ TLP assignment hierarchy is as follows (highest to lowest precedence):

Method	Details
Manually Set	Using the Add New Source option when creating an object will allow you to select a TLP classification.
Source Provided Data	TLP information received from ingested data.
Source Default	Administrators can set a source's default TLP classification. See the Apply TLP Classification to Source topic for more details.
No TLP	A TLP classification has not been set for the source.

Access TLP Settings

Users can manage TLP settings for system sources by accessing the **TLP** tab under the **Data Management** page.

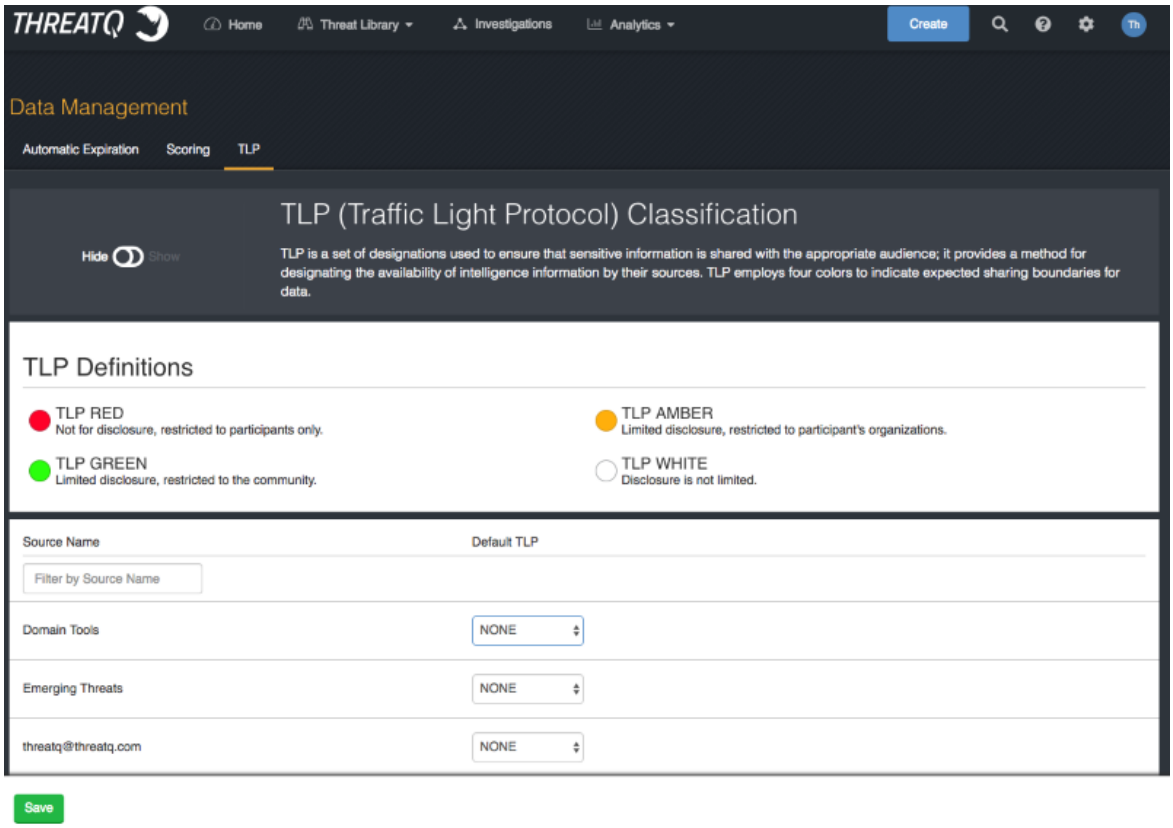
The Indicator Management option is now Data Management.

1. From the navigation menu, click on the **gear icon** and select **Data Management**.

   The Data Management page will load with Automatic Expiration tab selected by default

2. Click on the **TLP** tab.

   The TLP Setting page will open.

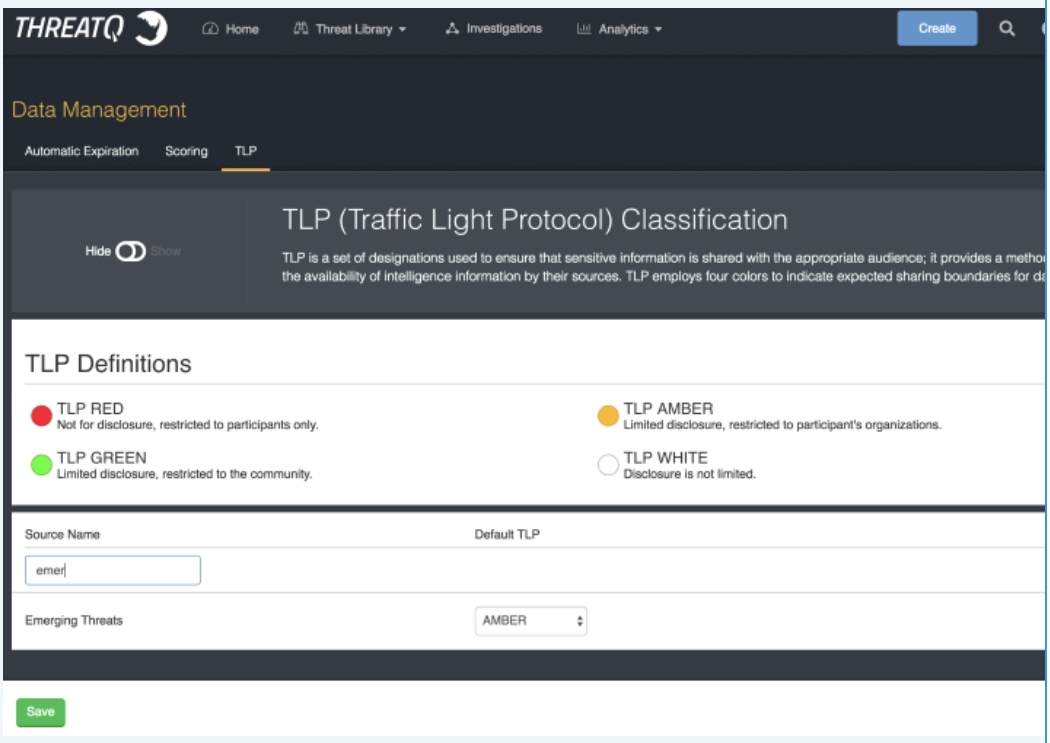


Apply TLP Classification to Source

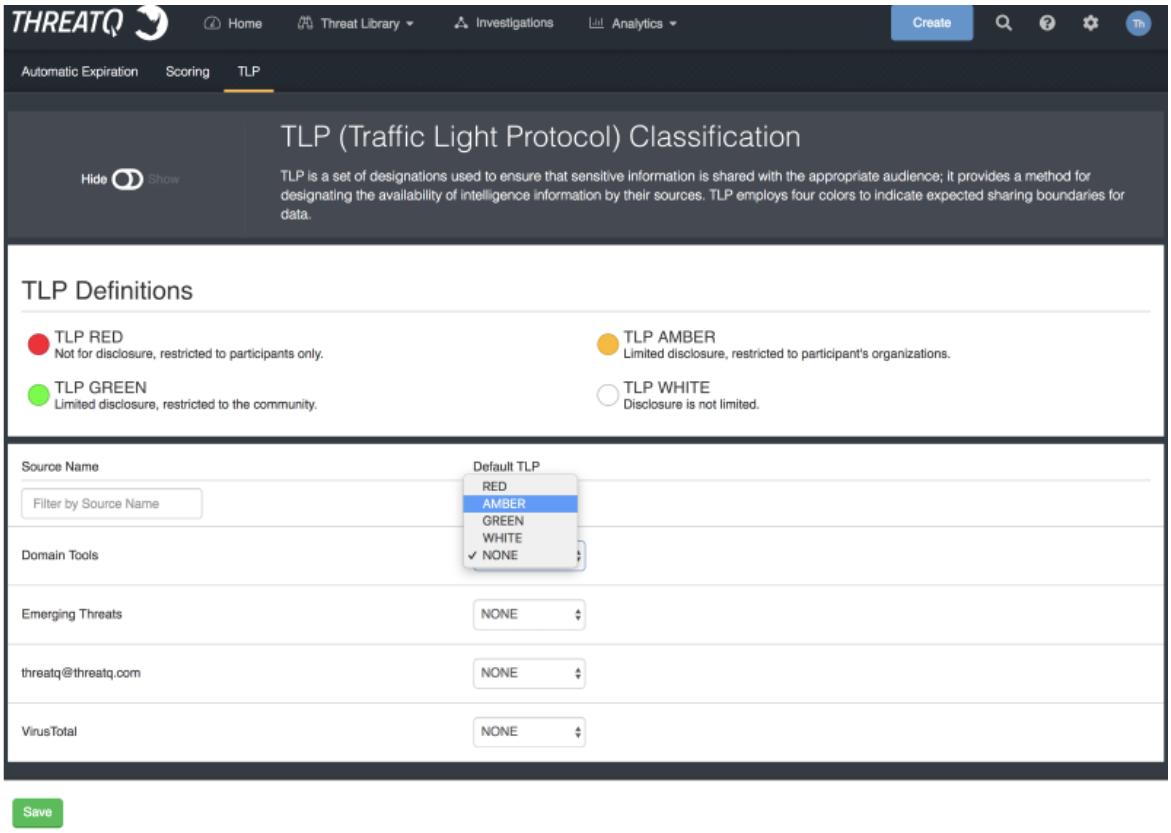
From the TLP Settings Page (see the Access TLP Settings topic):

1. Locate the source to update from the list provided.

You can use the Filter by Source Name field to locate the desired source.



2. Click on the TLP dropdown to the right of the source and select the appropriate TLP classification.



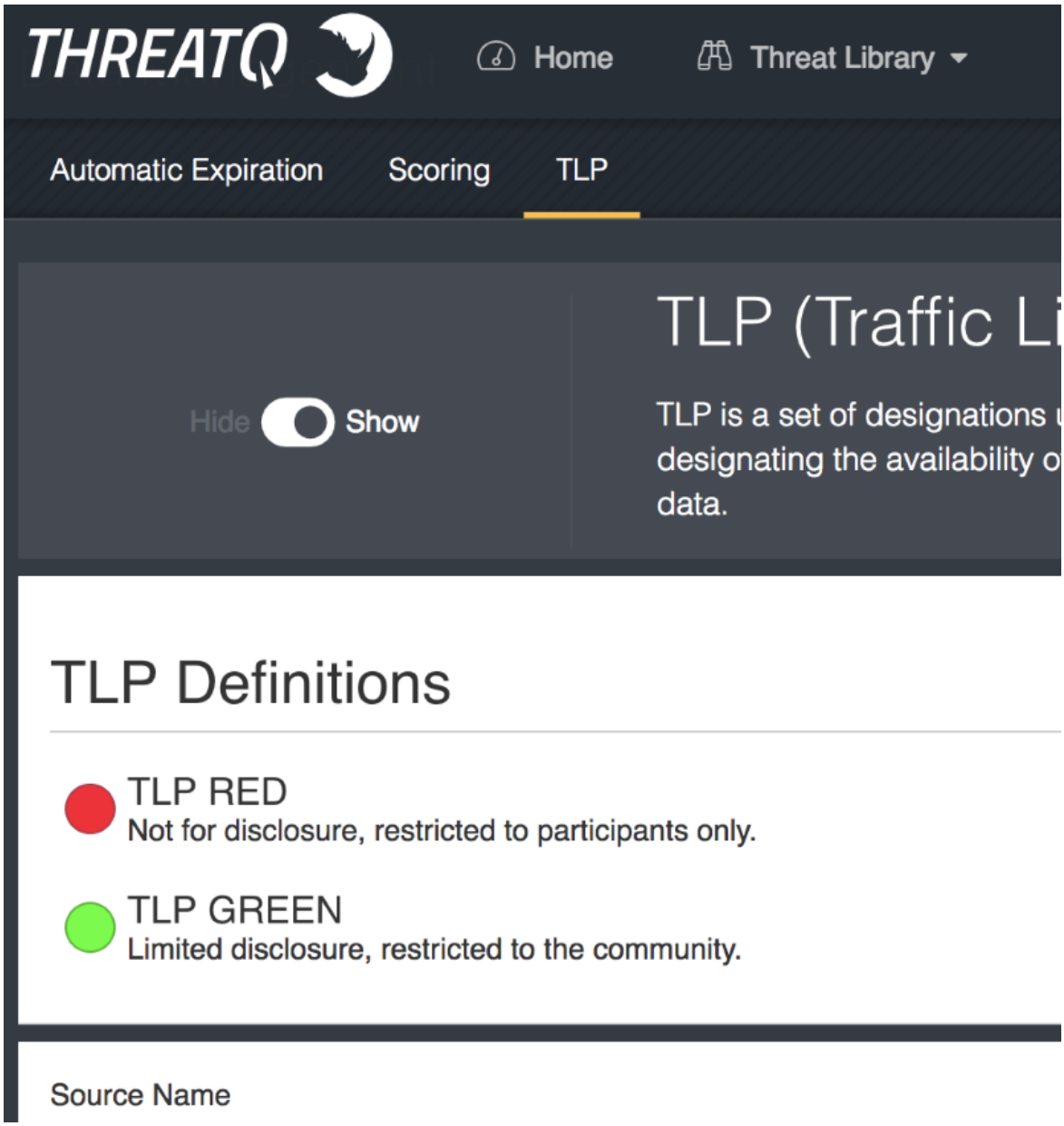
3. Click on **Save**.

Configure TLP Visibility

System administrators can set visibility settings to either hide or show indicator classification lights to users.

From the TLP Settings Page (see the Access TLP Settings topic):

1. Click on the Show/Hide toggle switch located to the left of the TLP Classification definition.



Administrators will not need to click on the Save button, changes will be made upon clicking on the switch.

Update TLP Classification using TLP Default - Command

Use the following command to update the TLP classification for an Object Source or Object Attribute Source with the source's default TLP classification.

See Apply TLP Classification to Source topic for more details on setting a default TLP classification for a source.

You should use this command to update your system to match default TLP configurations, specifically attributes and sources that were added to the Threat Library prior to the release of the TLP feature introduced with ThreatQ 4.11. This command will override previous TLP classification settings for a source including ones set by users. You will be prompted to confirm the action after entering the command. All updates will be recorded in the audit log.

The command will update using the default TLP classification. If a default classification is set to None, all references to the source will be updated to None.

All Sources

```
sudo /var/www/api/artisan threatq:apply-tlp-
defaults
```

Update a Specific Source

```
sudo /var/www/api/artisan threatq:apply-tlp-
defaults --sources="your source"
```

Example

```
sudo /var/www/api/artisan threatq:apply-tlp-
defaults --sources="CrowdStrike"
```

You can apply the command to multiple sources by listing the sources in a comma-delimited format.

Example

```
sudo /var/www/api/artisan threatq:apply-tlp-
defaults --sources="CrowdStrike,DigitalShadows"
```

Convert TLP Command

Use the following command to update all object sources and object attribute sources that have TLP stored as an object attribute. This command will not affect TLP attributes that have already been converted. Users should use this command for new incoming data, such as migrating data into the system, which has TLP attributes but no TLP set.

```
sudo /var/www/api/artisan threatq:convert-tlp-
attributes
```

Use Scenarios:

Object has one or more TLP Attributes with an invalid TLP (not currently in the TLP options)

- If the Object has just one TLP Attribute - none of its Sources or Attribute Sources will be updated.
- If the Object has more than one TLP Attribute - any Sources or Attribute Sources that match the Attribute Source of the TLP Attribute will not be updated.

Object has a single valid TLP Attribute

- All of the Object Sources and Object Attribute Sources will be updated to match the value of the TLP Attribute.

Object has multiple TLP Attributes

- Each TLP Attribute will be evaluated separately.
- Any Object Sources or Object Attribute Sources whose source matches that of the TLP Attribute will be updated with the value of the TLP Attribute.
- Any Object Sources or Object Attribute Sources whose sources do not match will not be updated.
- If there are no matches at all between the source of the TLP Attribute and any of the Object Sources or Object Attribute Sources, a new Object Source will be added using the Attribute's TLP value. Each of the Object Attributes will receive a new Object Attribute Source with the TLP value as well.

Threat Library

The Threat Library is the central repository within ThreatQ that organizes and combines external and internal threat data.

The Threat Library can be broken down into three segments:

System Objects
Threat data, both ingested and manually added, is referred to as System Objects and is sorted and categorized by object type.

Advanced Search
The Advanced Search page is the primary interface for the Threat Library that allows you to search, filter, and sort through System Objects.

Object Details
The Object Details page allows you view detailed information about a specific object.

Advanced Search

The Advanced Search page is the primary interface for the Threat Library. You can search for any system object within the application, filter returned system objects, and apply bulk changes to search results. You can click on an individual object to navigate to its details page.

Depending on how you have navigate to the Threat Library will determine which object types appear on the page.

Threat Library Navigation Menu

You can click on **Threat Library > Object Type** to open the advanced search for a particular object type or select **Browse All**. You can change or add additional object types using the Global Filters.

Search Link

You can click on **Search > Advanced Search** to open the advanced search for all object types within the Threat Library.

Refining Search Results

You can use the Global and List filters to narrow down your search for a specific object or object type.

Related Topics:

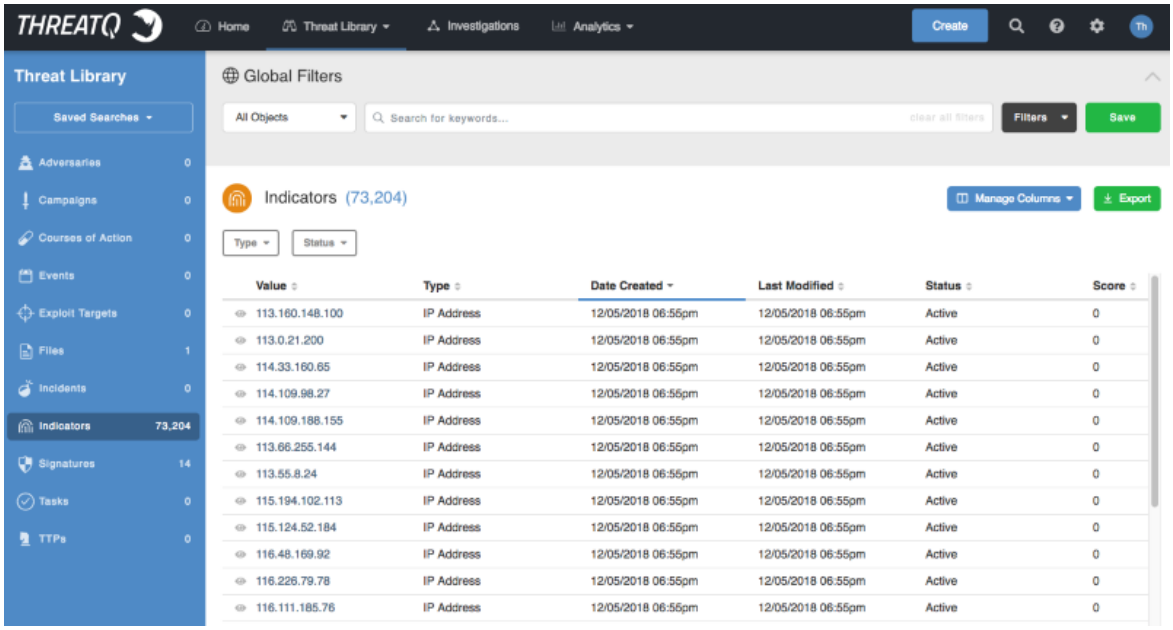
- Performing an Advanced Search
- Managing Search Columns
- Exporting Search Results to CSV
- Managing Searches
- Global Filters
- List Filters

Performing an Advanced Search

You can also click on **Threat Library** > **Browse All** to navigate to the advanced search page or click **Threat Library** >**Object Type** to navigate to the advanced search page for a specific object type.

To perform an advanced search:

1. Choose the Search icon.
2. In the Search dialog box, choose **Advanced Search**.



   The Advanced Search page opens.

3. Choose your object search category by selecting an object type from the Global Filter dropdown list or selecting an object type from the left-hand list.

   > See the Global Filters and List Filters topics for more information on narrowing down your search.

4. Press Enter or Return.
5. Optionally, repeat steps 3 and 4 to further narrow your search.

Managing Search Columns

You can choose which columns to display in your search results.

To select columns:

1. Navigate to the Advanced Search page.
2. Choose **Manage Columns**.

3. Select the columns you wish to display. Clear the columns you wish to hide.

Global Filters

Global filters allow you to filter advanced search results by specific details associated with an object.

Additional Topics:

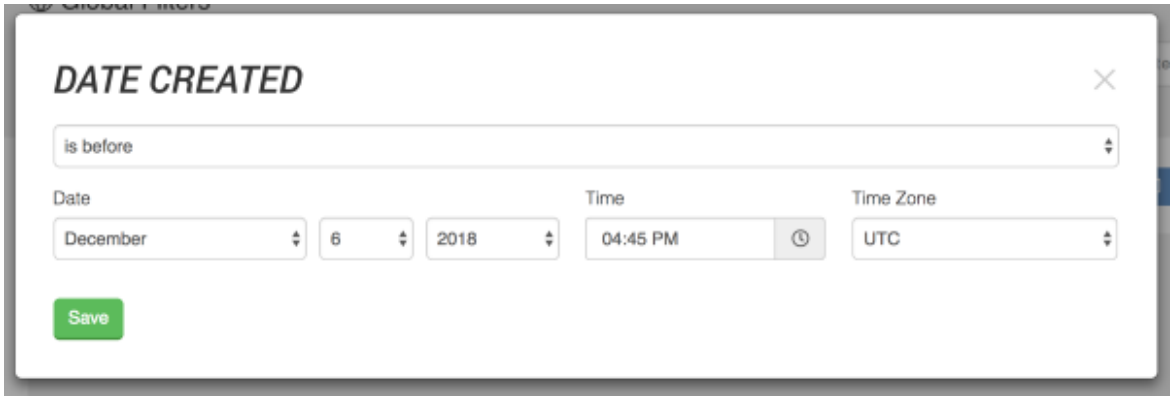
- Filtering by Attribute
- Filtering by Date Created
- Filtering by Keyword
- Filtering by Last Modified
- Filtering by Object Type
- Filtering by Relationship

Filtering by Date Created

Complete the following procedure to filter Advanced Search results by the date the objects were created.

To filter by Date Created:

1. Click on the **Filters** option and select **Date Created**.



The Date Created dialog box opens.

2. Select one of the following options to determine how the filter is applied:

Option	Result
is before	Search results include items before a selected date
is after	Search results include items after a selected date
is in the range of	Search results include items in a selected range of dates
is within the last	Search results include items within the selected number of days.

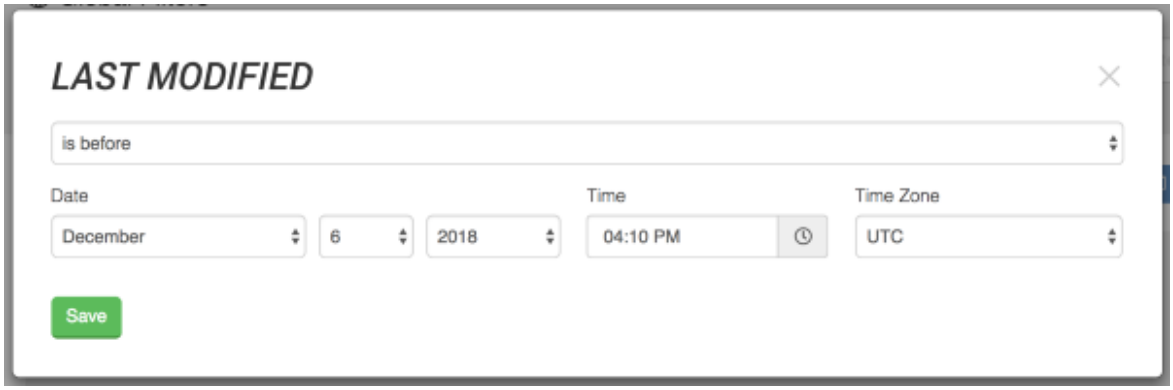
3. Use the controls to select date options based upon the selection in step 2.
4. Click **Save**.

Filtering by Last Modified

Complete the following procedure to display Advanced Search results by the date objects were last modified.

To filter by Last Modified:

1. Click on the **Filters** option and select either **Last Modified**.



The Last Modified dialog box opens.

2. Select one of the following options to determine how the filter is applied:

Option	Result
is before	Search results include items before a selected date
is after	Search results include items after a selected date
is in the range of	Search results include items in a selected range of dates
is within the last	Search results include items within the selected number of days.

3. Use the controls to select date options based upon the selection in step 2.
4. Click **Save**.

Filtering by Attribute

You can filter the Threat Library list to include or exclude objects with a specific attribute.

From the search results:

1. Click on the **Filters** option and select either **With Attribute** or **Without Attribute**.

The Attribute Filter dialog box opens.

2. Select an **Attribute Type**.
3. Enter an **Attribute Value** associated with the **Attribute Type**.

> Users can leave the **Attribute Value** field blank to filter for *any value* associated with the selected **Attribute Type**.

4. Click on the **Plus** icon to the right of the dialog box to add another attribute and repeat steps 2-3. This step is optional.
5. Click on the **Add** button.

The filters will be applied to the search results.

The following section applies to using multiple attribute filters.

> The **Match Any/All** toggle option will allow users to configure the filter to include objects that either fit one attribute filter or all. The **Any** option will be selected by default. This means the filter will display results that fit any of the attribute filters. The **All** option means the filter will display results that fit all attribute filters.

Example:

ANY - Match Toggle Selection

Setting	Field	Value
Filter A	Attribute Type	Attack Phase
	Attribute Value	C2
Filter B	Attribute Type	Severity
	Attribute Value	High
Filter Options	Any/All Toggle	Any
Result	Search Results are filtered to include/exclude objects with Attack Phase: C2 **OR** Severity: High attributes.	

ALL - Match Toggle Selection		
Setting	**Field**	**Value**
Filter A	Attribute Type	Attack Phase
	Attribute Value	C2
Filter B	Attribute Type	Severity
	Attribute Value	High
Filter Options	Any/All Toggle	All
Result	Search Results are filtered to include/exclude objects with Attack Phase: C2 **AND** Severity: High attributes.	

Common Scenarios

The following scenarios demonstrate the Attribute Filter option in use with search results.

Applying a "With Attribute" filter (All items with an Attribute Type and Value)

1. User clicks on the **Threat Library** tab and selects on the **Indicators** tab.
2. User clicks on the **Filters** button and select **With Attribute**.

The Attribute Filter dialog box opens.

3. User selects **Attack Pattern** as the **Attribute Type** and **C2** as the **Attribute Value**.
4. User clicks on **Add**.

*The User will now see a search parameter **With Attribute** with **Attack Pattern: C2** listed. The search results update to show all Indicators with an attribute of **Attack Pattern: C2**.*

Applying a "Without Attribute" filter (All items without an Attribute Type and Value)

1. User clicks on the **Threat Library** tab and selects on the **Indicators** tab.
2. User clicks on the **Filter** button and select **Without Attribute**.

The Attribute Filter dialog box opens.

3. User selects **Attack Pattern** as the **Attribute Type** and **C2** as the **Attribute Value**.
4. User clicks on **Add**.

*The User will now see a search parameter **With Attribute** with **Attack Pattern: C2 listed**. The search results update to show all Indicators without an attribute of **Attack Pattern: C2**.*

Applying a "Without Attribute" filter (All items Without a specific Attribute Type with any Value)

1. User clicks on the **Threat Library** tab and selects on the **Indicators** tab.
2. User clicks on the **Filters** button and select **Without Attribute**.

The Attribute Filter dialog box opens.

3. User selects **Attack Pattern** as the **Attribute Type** and leave the **Attribute Value** blank.
4. User clicks on **Add**.

*The User will now see a search parameter **Without Attribute** with **Attack Pattern** listed. The search results update to show all Indicators that do not have an **Attribute Type** of **Attack Pattern** assigned to them.*

Applying keyword filters then applying a "With Attribute" filter

1. User clicks on the **Threat Library** tab and selects on the **Indicators** tab.
2. User searches for keyword: **demo**.

The User will see a search parameter listed Keyword: "demo" and the results update to show only indicators that mention demo.

3. User clicks on the **Filters** button and select **With Attribute**.

The Attribute Filter dialog box opens.

4. User selects **Attack Pattern** as the **Attribute Type** and **C2** as the **Attribute Value**.
5. User clicks on **Add**.

The User will now see a search parameter **With Attribute** with **Attack Pattern: C2** listed. The search results will update to show all Indicators that mention the keyword **demo AND** have an attribute of **Attack Pattern: C2**.

Editing multiple attributes that were applied as part of the search parameters

1. User clicks on the **Threat Library** tab and navigates to the **Indicators** tab.
2. User clicks on the **Filter** button and select **With Attribute**.

   The Attribute Filter dialog box opens.

3. The User specifies two attributes:
   - Attack Pattern:C2
   - Severity: High
4. User clicks on **Add**.

   *The User will now see two search parameters under the **With Attribute** section - **Attack Pattern: C2** and **Severity: High**. The search results updates to show all Indicators with an attribute of **Attack Pattern: C2** and **Severity: High**. The search parameter for attributes is defaulted to Any. This indicates that objects with an attribute of **Attack Pattern: C2** or **Severity: High** are displayed.*

5. User clicks on the **Filters** option and selects **With Attribute**.

   A form will load with all applied filter attributes.

6. The User clears the **Attack Pattern's Attribute Value** field and clicks **Add**.

   The User will now see two search parameters under the **With Attribute** section: **Attack Pattern: Any** and **Severity: High**. The search results updates to show all Indicators with an attribute type of **Attack Pattern OR Severity: High**.

Add multiple attributes and toggle Match from Any to All

1. User applies two attribute filters to the indicators results: **Attack Phase: C2** and

Severity:High.

The filtered results will display any indicators that has either of those attributes.

2. User clicks on the **Any/All** Match toggle button and select **All**.

The filtered results will display any indicator that has both of those attributes

Filtering by Relationship

The Relationship Filter option allows you to filter the Threat Library by related objects. Using the Relationship filter, you can:

- Filter search results to include objects related to a specific object.
- Filter search results to include objects using multiple related object filters. You will also have the option to set the filter to include objects that fit one of the multiple filters or all.

To Filter by Related Object:

From the search results:

1. Click on the **Filters** option and select **Relationship**.

The Filter by Relationship dialog box opens.

2. Use the textbox provided to select an object.

Repeat step 2 to add multiple object filters.

3. Click on **Add** to apply the filter.

The **Match Any/All** toggle option will allows you to configure the filter to include objects that either fit one related object filter or all. The **Any** option will be selected by default. This means the filter will display results that fit any of the related object filters. The **All** option means the filter will display results that fit all related object filters.

Examples:

ANY - Match Toggle Selection	
Setting	**Related Object**
Filter A	ABC Indicator
Filter B	DEF Event
Filter Option	Any
Result	Search Results are filtered to include objects related to the ABC Indicator **OR** the DEF Event.

ALL - Match Toggle Selection	
Setting	**Related Object**
Filter A	ABC Indicator
Filter B	DEF Event
Filter Option	All
Result	Search Results are filtered to include objects related to the ABC

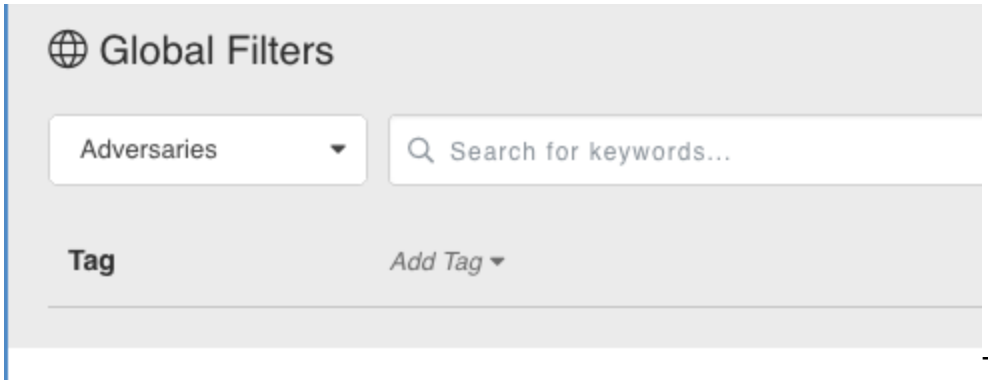
	Indicator **AND** the DEF Event.

Filtering using Tags

Using the **Tags** filter allows you to filter search results based on tags applied to an object.

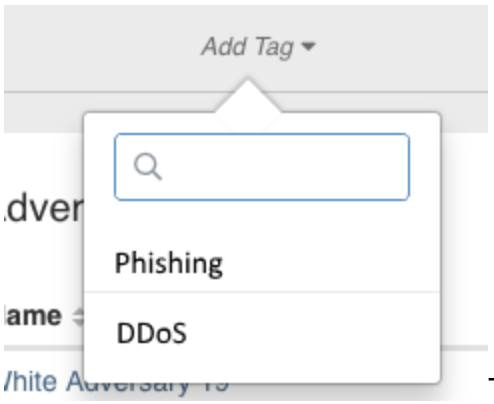
From the search results:

1. Click on the **Filters** option and select **Tags**.



The Filter by Tag row opens.

2. Select **Add Tag**.



The Add Tag dialog box opens.

3. Use the supplied text field to select a tag.
4. Repeats steps 2-3 to apply multiple tag filters.

The **Match Any/All** toggle option will allows you to configure the filter to

include objects that either fit one tag filter or all. The **Any** option will be selected by default. This means the filter will display results that fit any of the tag filters. The **All** option means the filter will display results that fit all-tag filters.

Examples:

ANY - Match Toggle Selection	
Setting	**Tag**
Filter A	Phishing
Filter B	DDoS
Filter Option	Any
Result	Search Results are filtered to include items with either Phishing **OR** the DDoS tags.

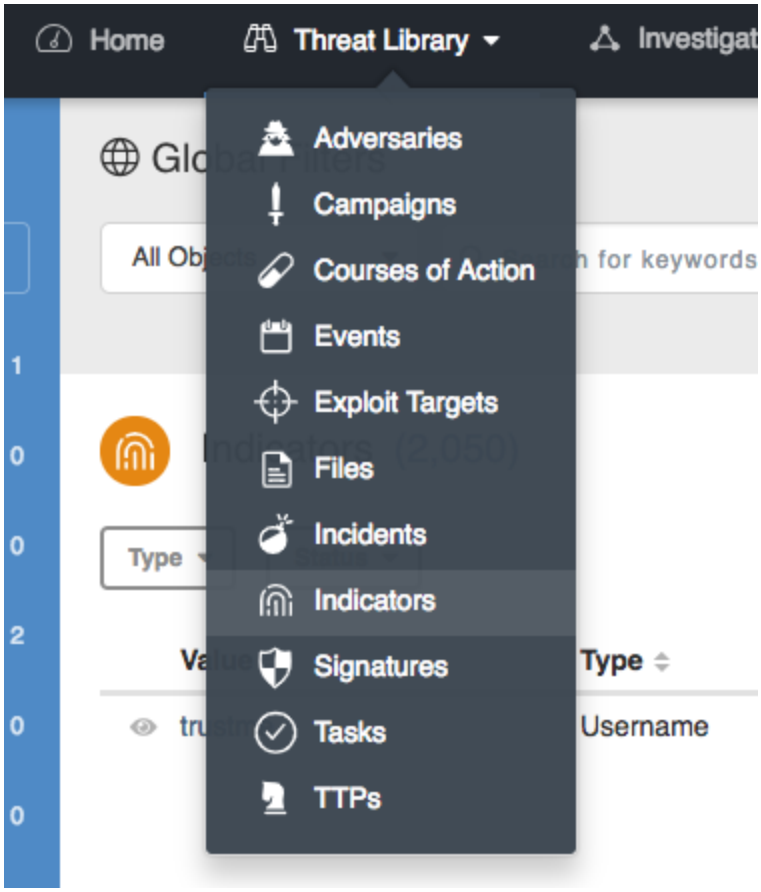
ALL - Match Toggle Selection	
Setting	**Tags**
Filter A	Phishing
Filter B	DDoS
Filter Option	All
Result	Search Results are filtered to include items with both Phishing **AND** DDoS tags.

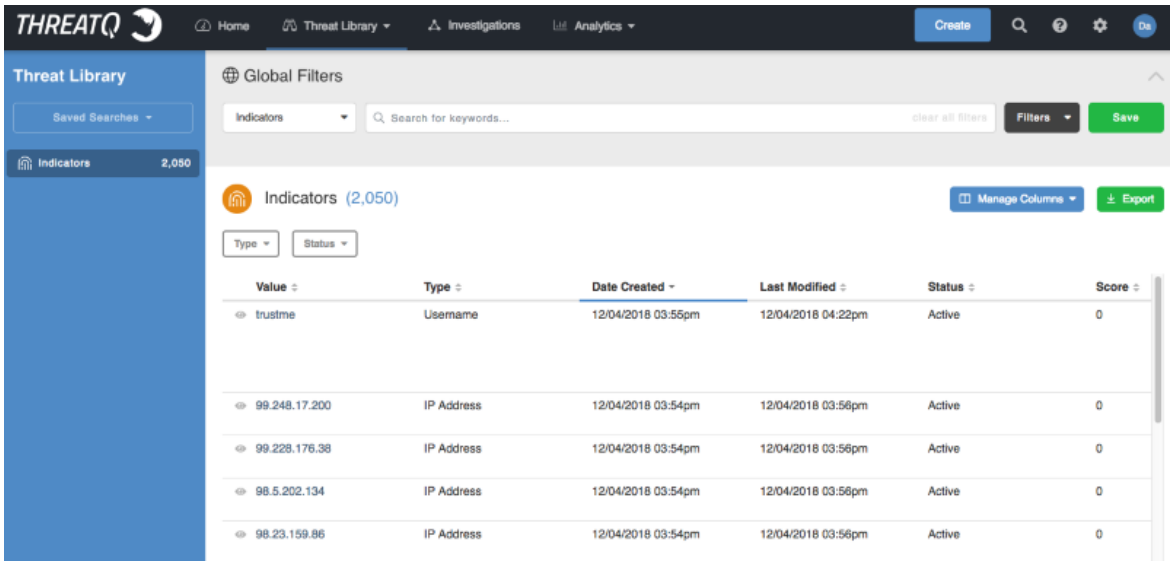
Filtering by Object Type

You can filter the Threat Library by object type using the following methods:

Threat Library Navigation Menu:

1. Click on the **Threat Library** navigation dropdown and select an **Object Type**.



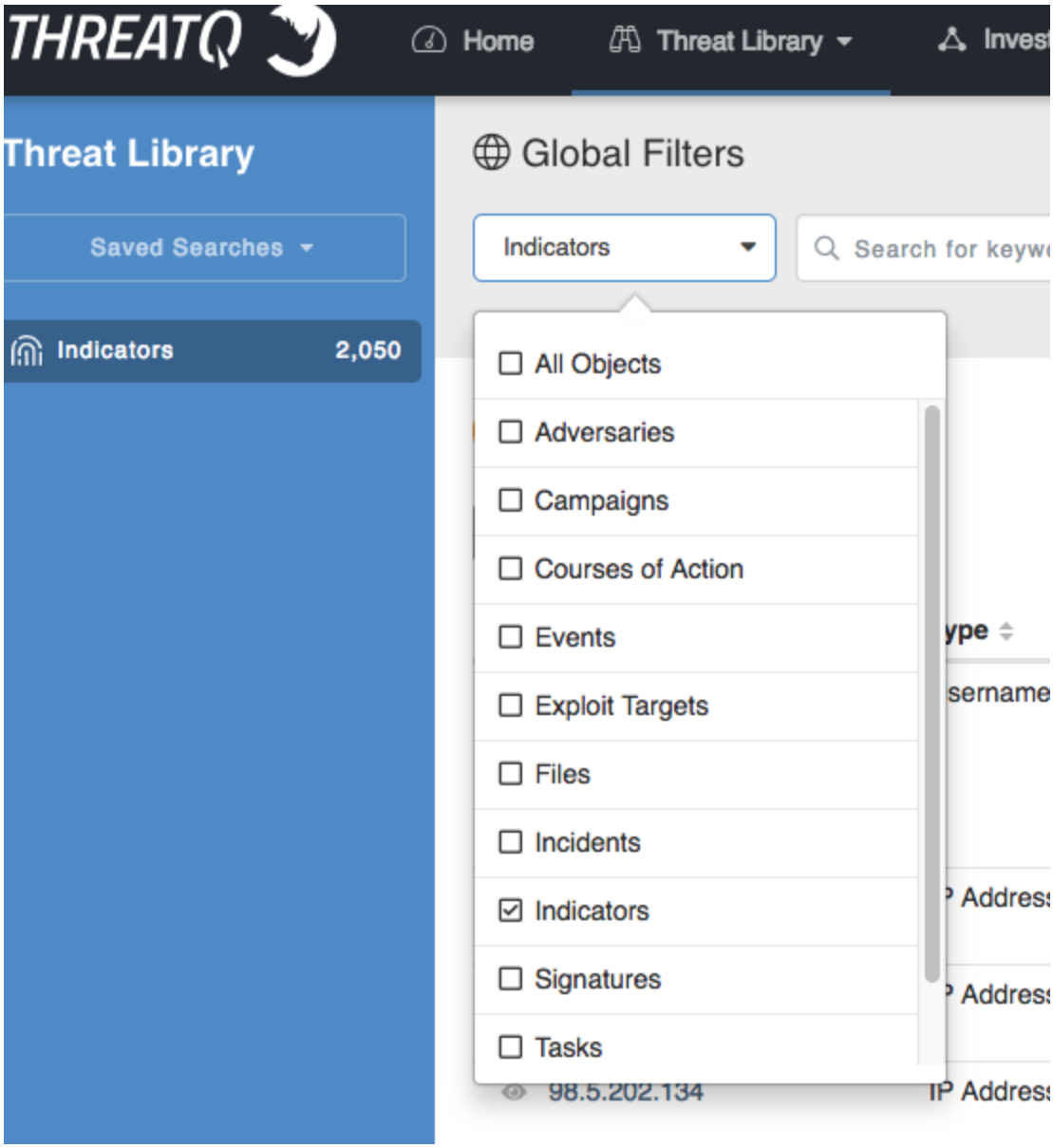


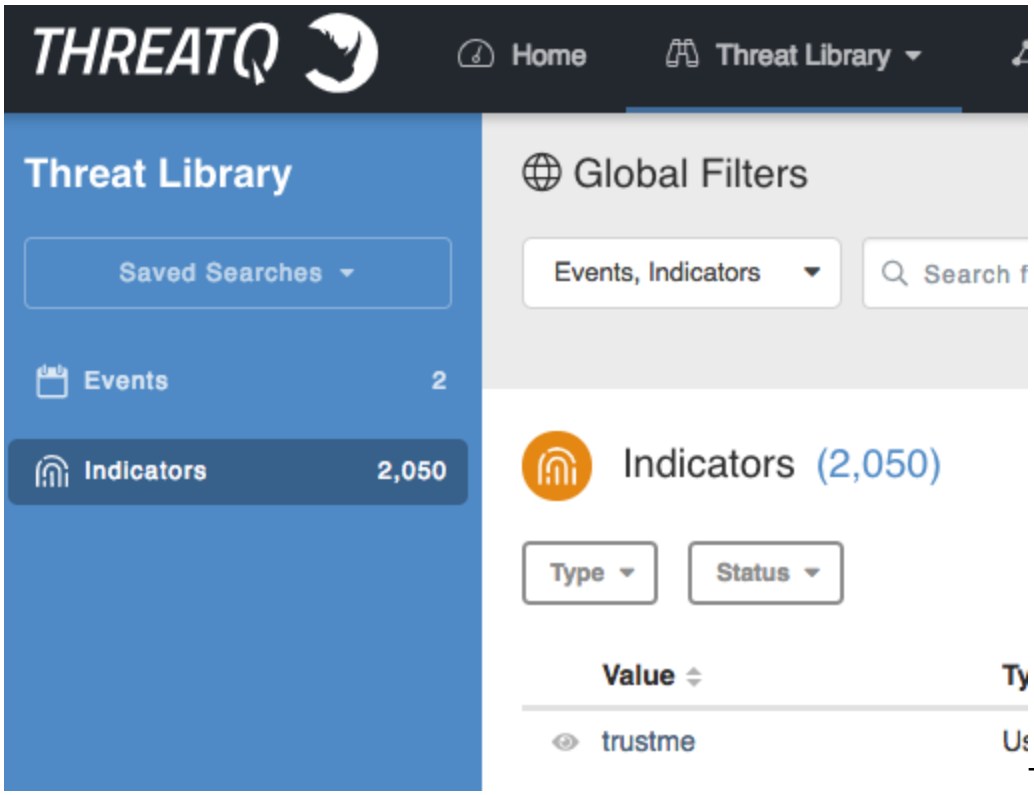
The Advanced Results page opens with the applied object type filter.

Object Global Filter Dropdown List

You can use the Global Filter dropdown list to select more than one object type.

1. Click on the **Object Type** dropdown list and select one or more object types.





The Advanced Search Results page updates the list with the selected object type(s).

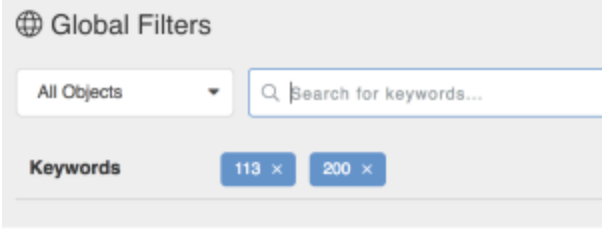
Filtering by Keyword

You can filter the Threat Library items on the Advanced Search by keyword.

To filter by keyword:

1. Navigate to the Advanced Search page.
2. Enter a keyword in the Keyword text field and press **<Enter>** or **<Return>**.

> Repeat Step 2 to apply multiple keyword filters



Each keyword filter appears in a box below the keyword text field.

3. Click on the **X** for each filter to remove it or select **Clear All Filters** to remove all filters

List Filters

List filters allow you to apply object type-specific filters to the advanced search results.

> List filter options vary based the object type currently being viewed.
> Example: the score filter can only be applied to indicators.

- Filtering by Type
- Filtering by Status
- Filtering by Score

Filtering by Type

You can filter Indicators, Signatures and Files by specific types of each.

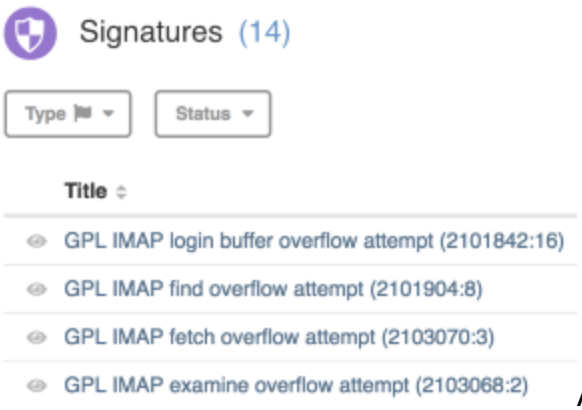
Example: Filter the Signature list to include YARA types only.

To filter by status:

1. Click on the **Type** button and select a type from the dropdown menu.

   > You can select multiple types using the check boxes.

   The search results will update with the applied filter.



A flag icon at the top of the results list will indicate that a filter is in use.

Filtering by Status

You can filter Indicators, Signatures and Tasks by Status.

To filter by status:

1. Click on the **Status** button and select a status from the dropdown menu.

   You can select multiple statuses using the check boxes.

   The search results will update with the applied filter.

A flag icon at the top of the results list will indicate that a filter is in use.

Filtering by Score

You can filter indicators in the advanced search results by score.

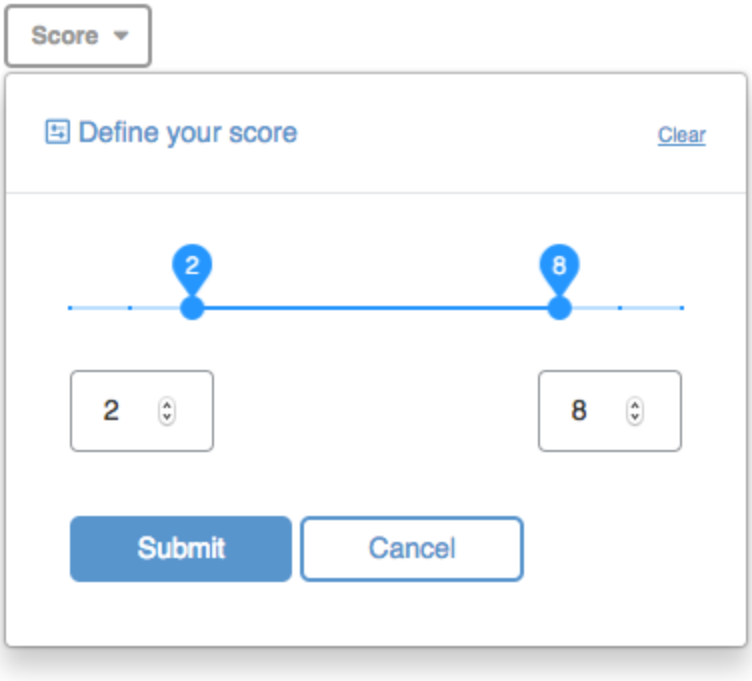
This option is only available for indicators.

To filter by score:

1. Navigate to the Advanced Search results page by selecting **Search > Advanced Search** then selecting **Indicators** from the left-hand object type menu.

   You can also select **Threat Library > Indicators** from the main menu.

2. Enter a keyword in the **Keyword** field and press **<Enter>** or **<Return>**. This step is optional.
3. Select the **Score** filter option.



The Scoring Filter dialog dropdown opens.

The scale offers a range of 1-10.

4. Adjust the score scale to filter the results.

   Filtering by Scoring Range

   You can move the two scale markers to select a scoring range.

   Example: Move the left marker to 6 and the right marker to 8 to filter the search results to include indicators with a score between 6 and 8.

   Filtering by Specific Score

   You can move the scale makers to the same scoring number to filter by a specific score.

   Example: Move the left and right markers to 8 to filter the search results to only include indicators with a score of 8.

5. Select **Submit** to apply the filter.

Select the **Score** filter again and select **Clear** to remove the filter.

Managing Searches

If you are following a particular area of interest, you can create a Saved Search. Saved Searches can then be run at any time.

Related Topics:

- Saving Searches
- Running Saved Searches
- Deleting Saved Search

Saving Searches

To save a search:

1. Choose the **Search** icon.
2. In the Search dialog box, choose **Advanced Search**.

   > You can also select **Threat Library** > **Object Type** to navigate to the advanced search page for a specific object type.

3. Perform an Advanced Search.
4. Choose **Save**.

   The Save Search dialog box opens.

5. Enter a name for the search in the Save Search dialog box.
6. Choose **Save Search**.

Running Saved Searches

To run a saved search:

1. Navigate to the Advanced Search page.
2. Choose Saved Searches dropdown list and then select the desired saved search from the list.

Deleting Saved Search

To delete a saved search:

1. Navigate to the Advanced Search page.
2. Choose **Saved Searches** and then select the desired saved search from the list.
3. Click on the **Delete** icon.

Exporting Search Results to CSV

You can export your search results as a CSV file, which allows you to use the data in another application, such as external spreadsheet software.

If you export a file with too many search results, the file may be too large to open in desktop applications. If you encounter this issue, you should separate your exports into smaller chunks of data.

When exporting search results to a CSV file, if you include additional columns beyond the default, this modification will impact the performance of the export process.

To export search results to a CSV file:

1. Navigate to the Advanced Search page.
2. Perform your search.
3. Choose **Export**.
   The CSV file downloads to your desktop.

System Objects

Threat data, both ingested and manually added, is referred to as System Objects and is sorted and categorized by object type.

See the topics below to learn more about each object type and how to manage them.

System Objects:

- Adversaries
- Events
- Files
- Indicators
- Signatures
- STIX Overview

Adversaries

Adversaries are the suspected groups that are attempting to do malicious activity.

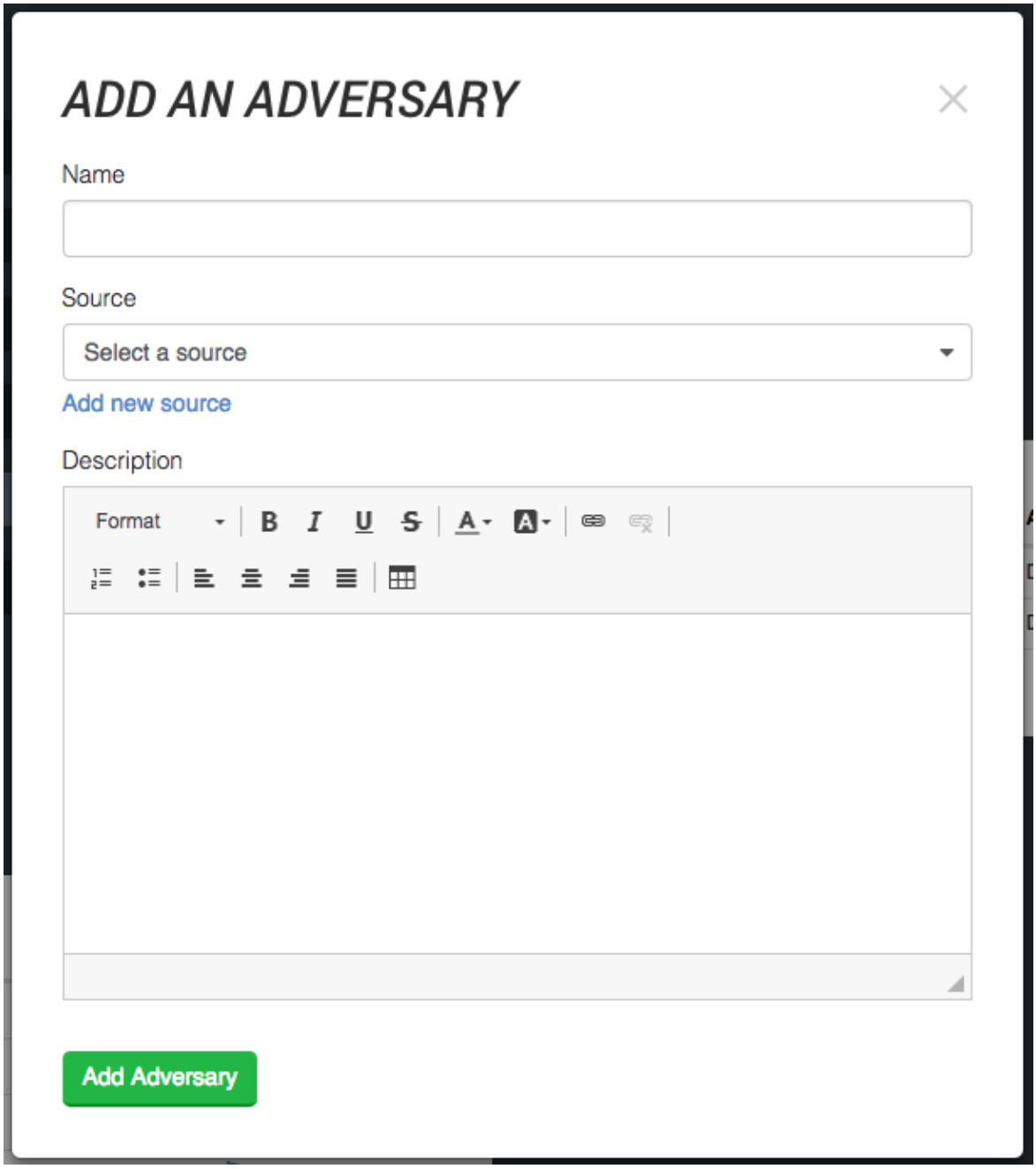
Related Topics

- Adding Adversaries
- Editing Adversaries
- Deleting Adversaries

Adding Adversaries

To create an Adversary:

1. Go to **Create > Adversary**.

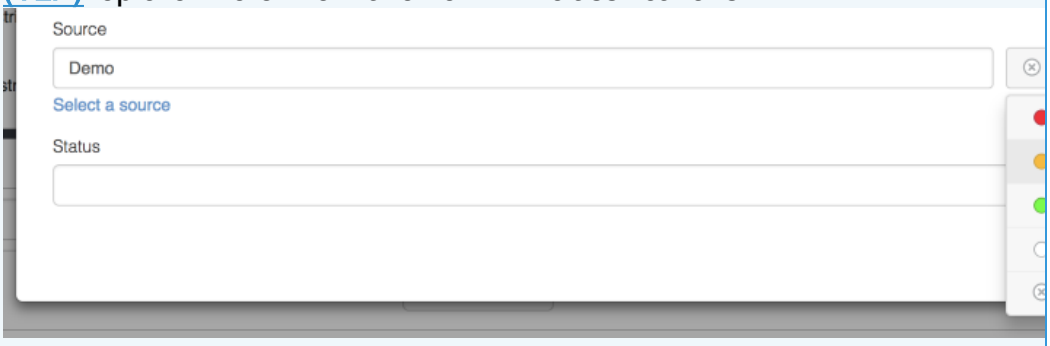


The Add an Adversary dialog box opens.

2. Enter a name.

3. Select a **Source** from the dropdown provided.

You can also click on **Add a New Source** if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, users can select a TLP classification light for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP classifications.

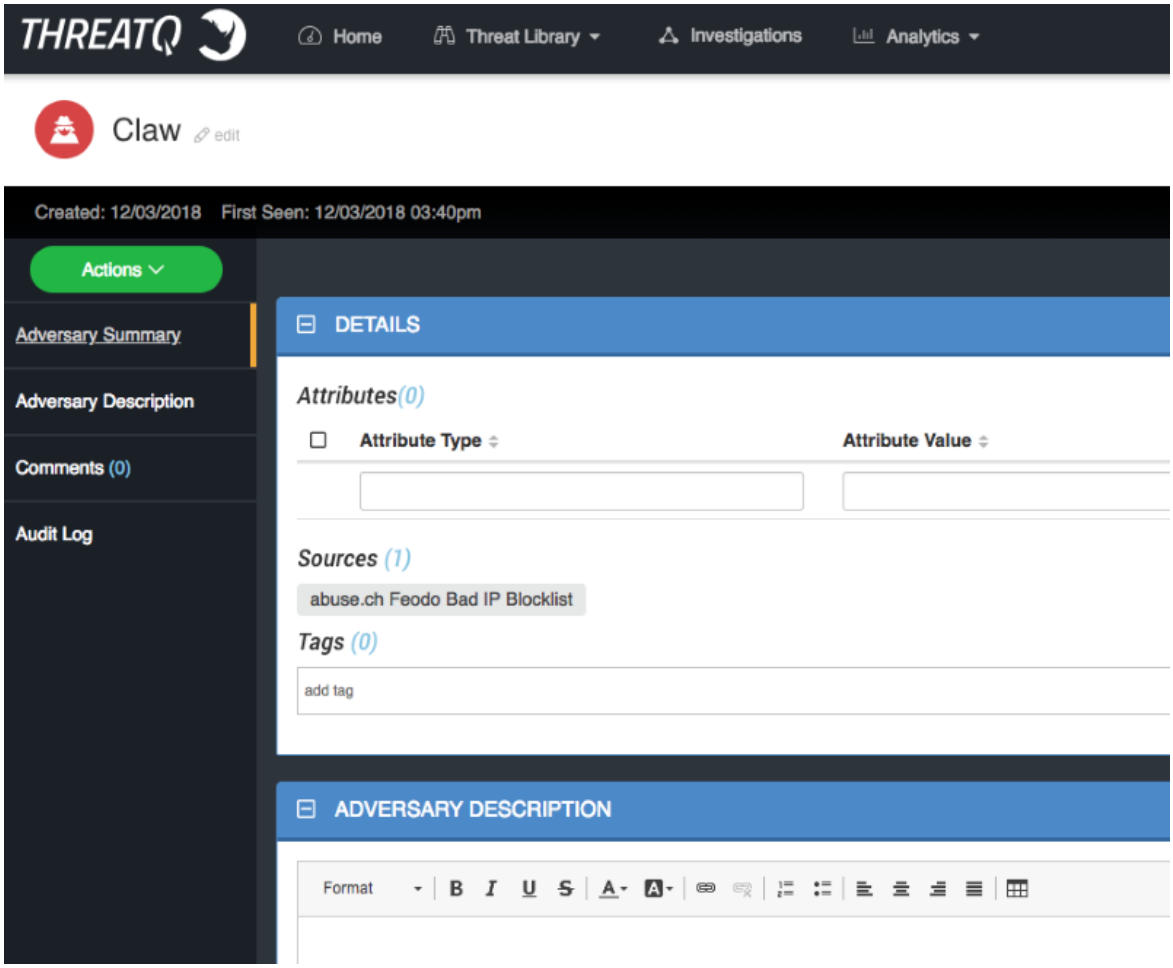


4. Enter a description.
5. Click **Add Adversary**.

Editing Adversaries

To edit the name of an Adversary:

1. Locate and click the adversary.



The Adversary Details page opens.

2. Click on **Edit** next to the Adversary name.

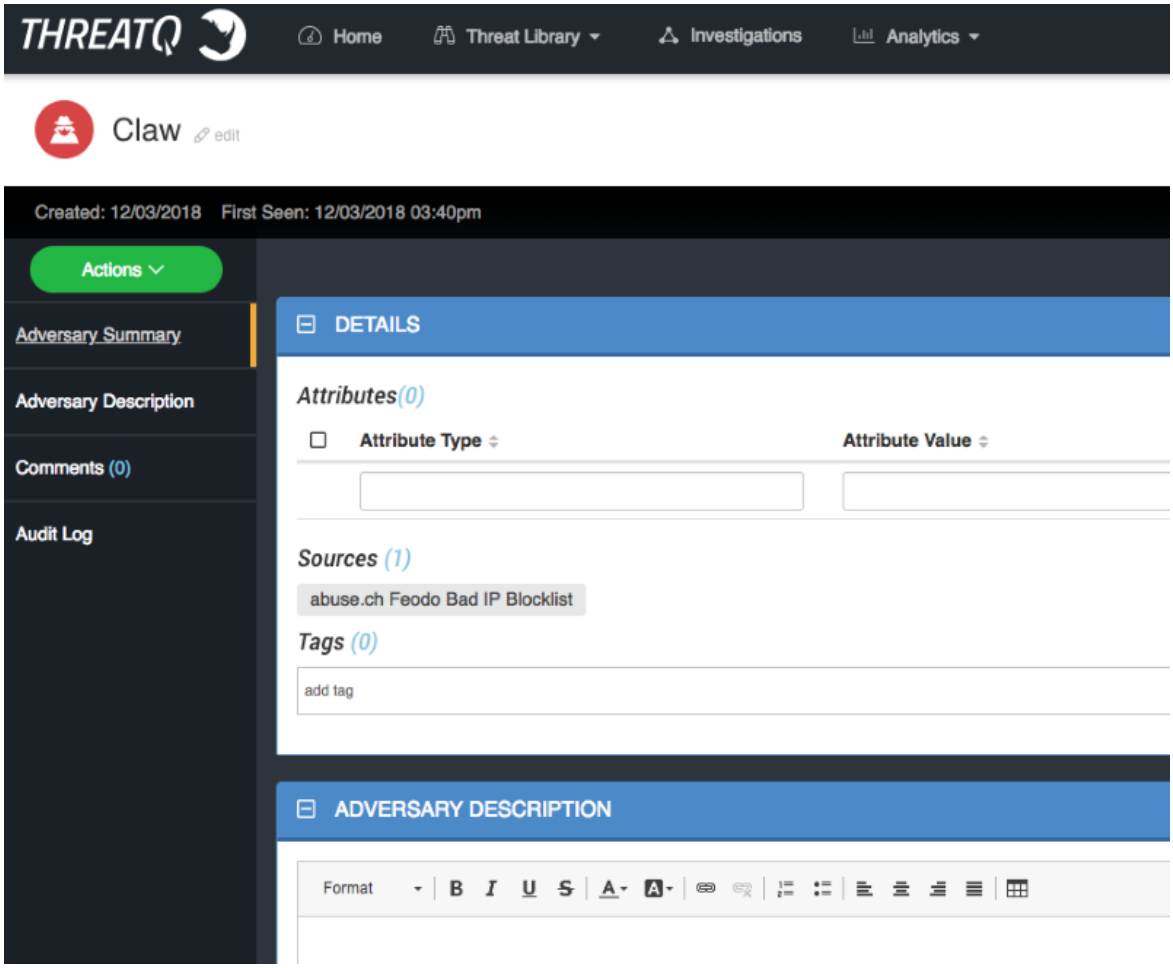
   The Edit Adversary dialog box opens.

3. Make the desired change to the Adversary name.
4. Click on **Save Adversary**.

Deleting Adversaries

To delete an Adversary:

1. Locate and click the adversary.



The Adversary Details page opens.

2. Click on **Delete this Adversary** located to the top right of the page.

A confirmation dialog box appears.

3. Click on **Delete Adversary**.

Events

Events are observations made by the threat intelligence community of adversaries' malicious attempts.

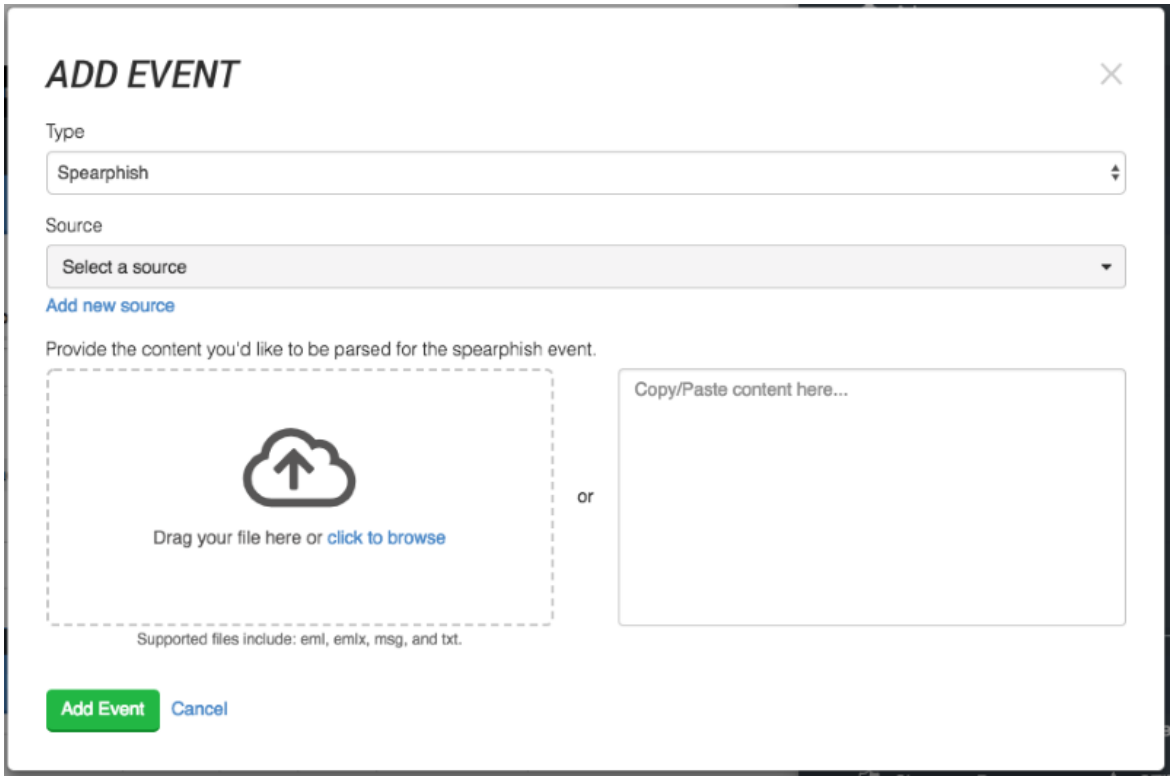
Related Topics:

- Adding Events
- Editing Events
- Deleting Events

Adding Events

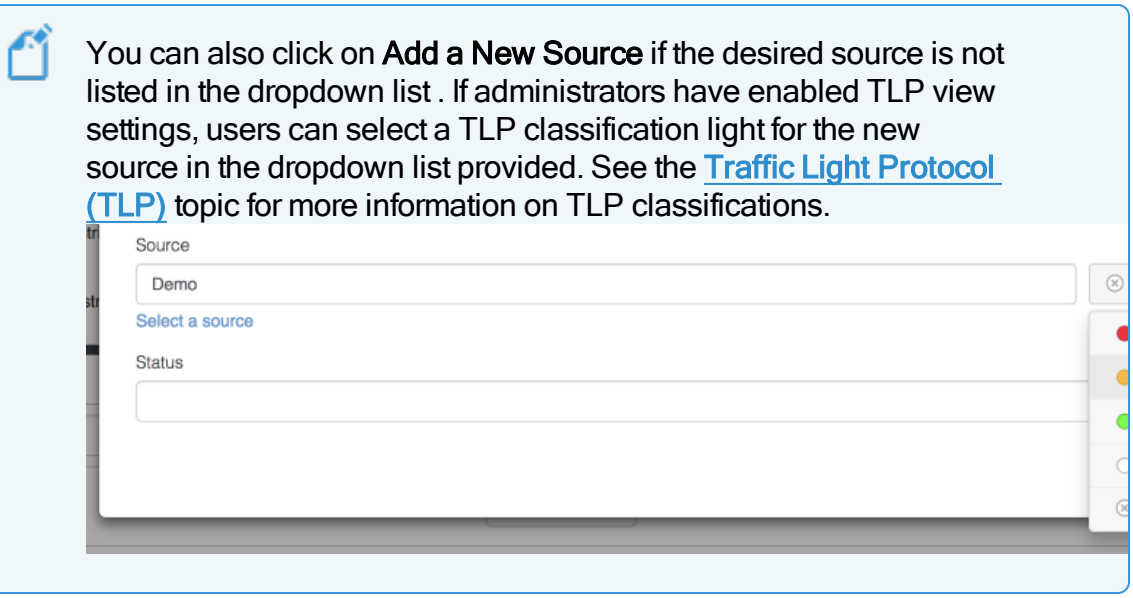
To add an Event:

1. Go to **Create > Event**.



The Add Event dialog box opens.

2. Select the **Event Type**.
3. Select a **Source** from the dropdown list provided.

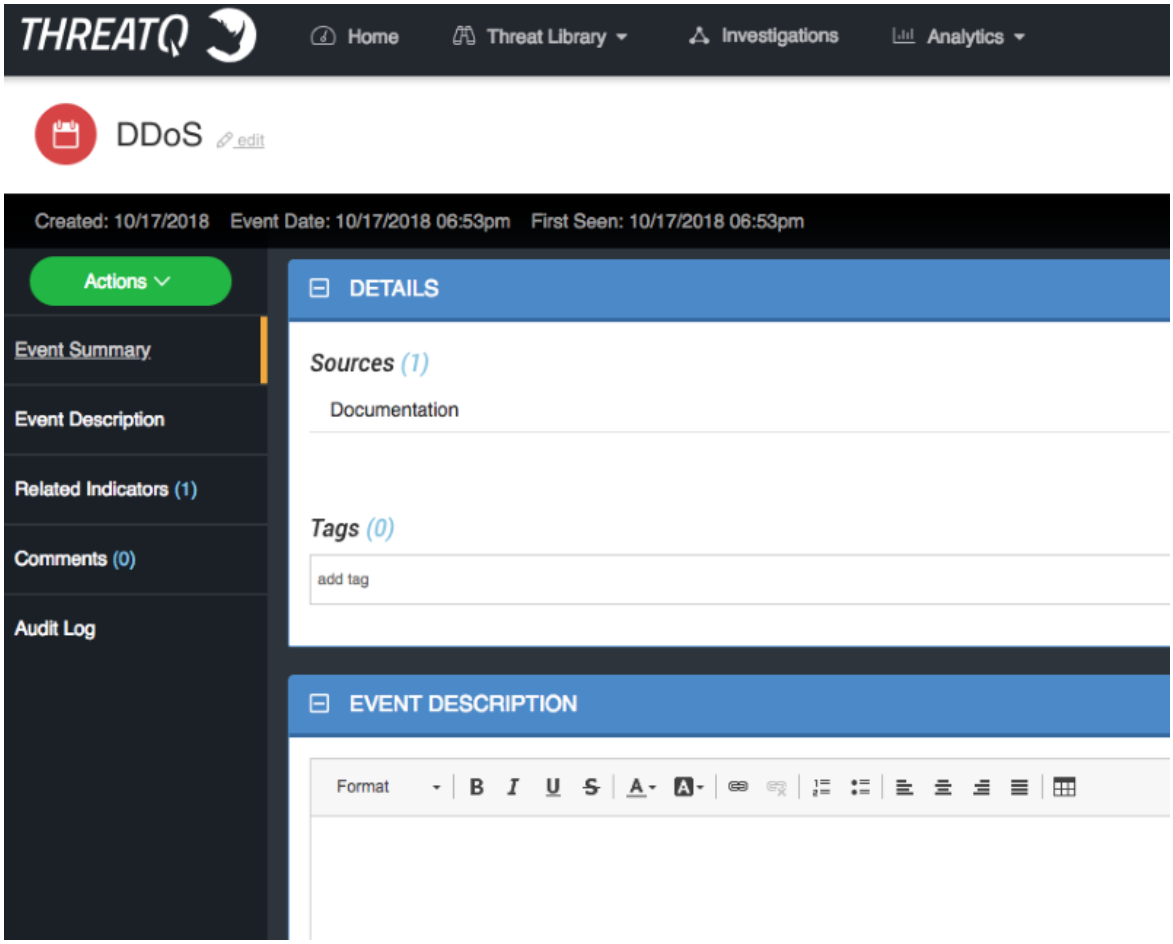


4. Add the date and time the event occurred in the **Date of Occurrence** fields.
5. Add an **Event Title**.
6. Click **Add Event**.

Editing Events

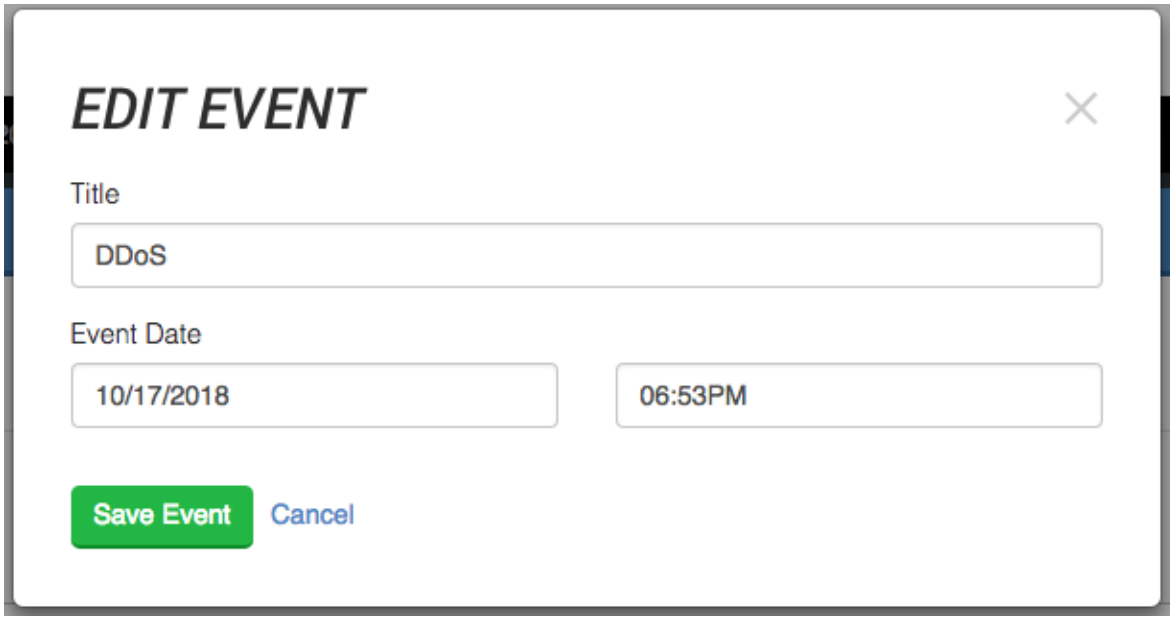
To edit an Event:

1. Locate and click on the event.



The Event Details page opens.

2. Click on **Edit** next to the Event name.



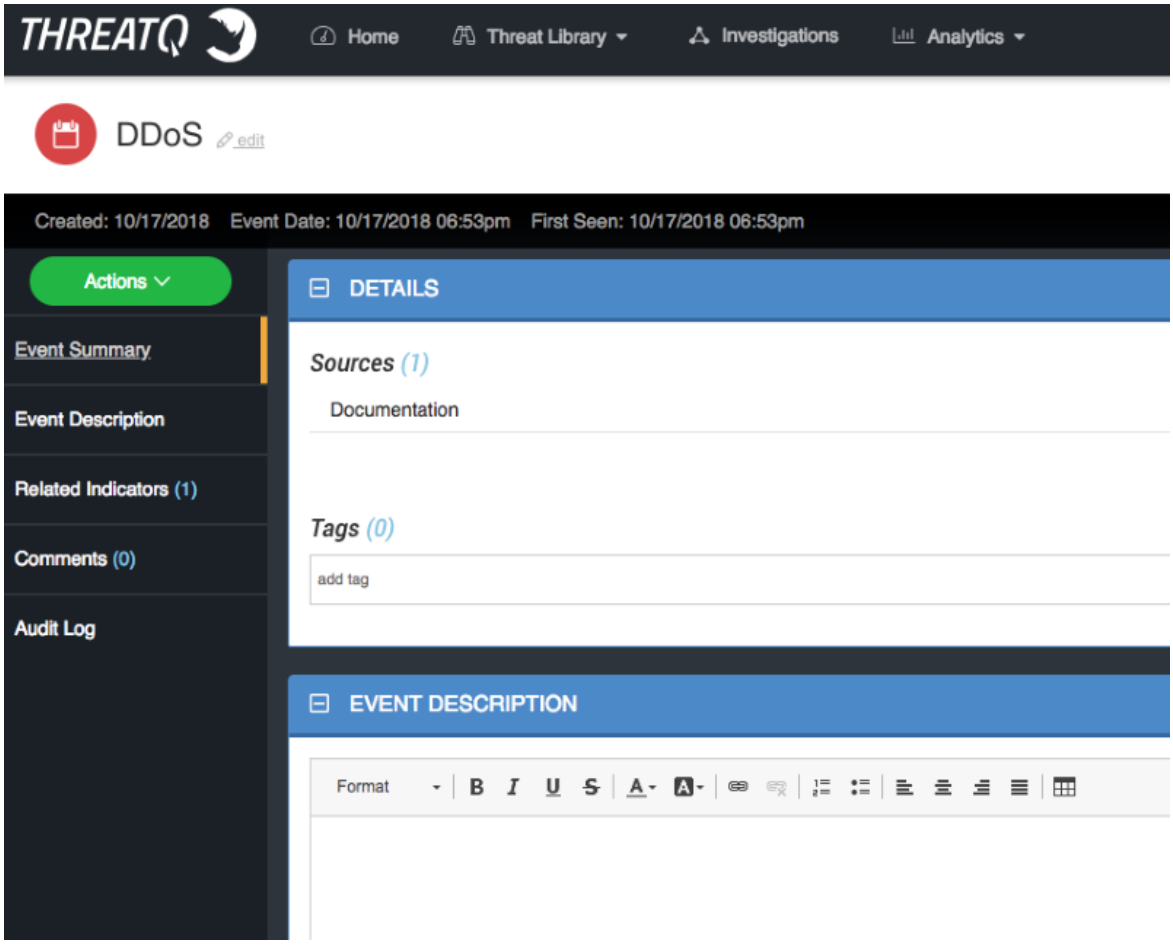
The Edit Event dialog box opens.

3. Make the desired change to the Event Name and Event Date.
4. Click on **Save Event**.

Deleting Events

To delete an Event:

1. Locate and click the event.



The Events Details page opens.

2. Click on **Delete this Event** located to the top right of the page.

A confirmation dialog box appears.

3. Click on **Delete Event**.

Files

Files are received from various intelligence providers and contain information on indicators, adversaries, and events within ThreatQ.

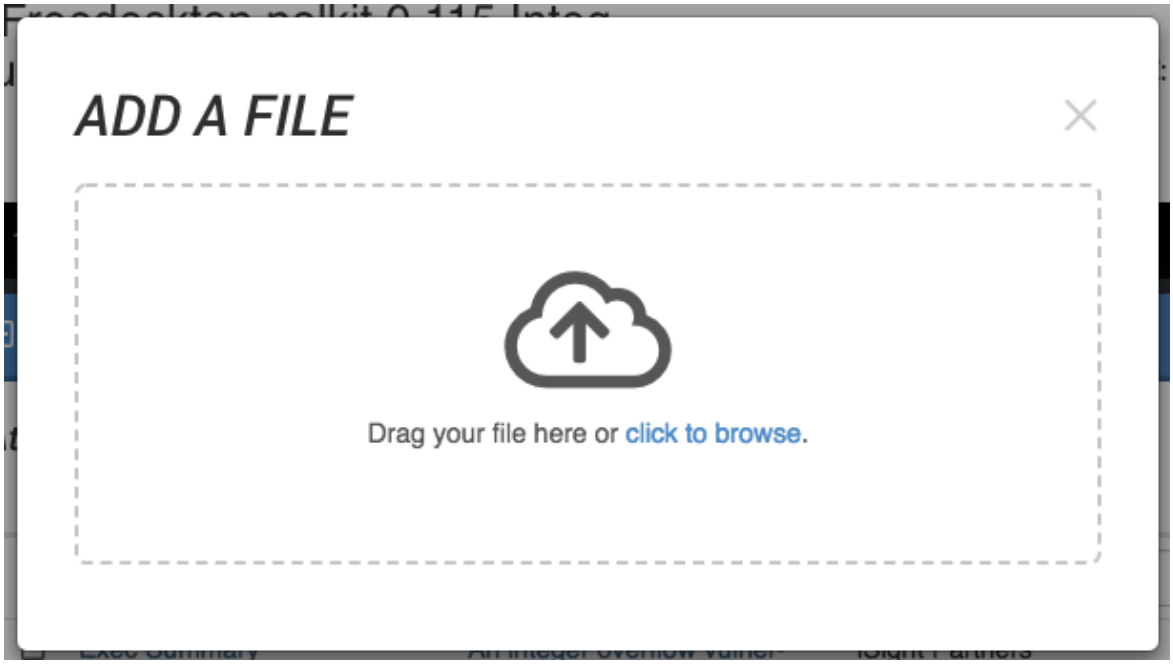
Related Topics:

- Adding Files
- Editing Files
- Deleting Files

Adding Files

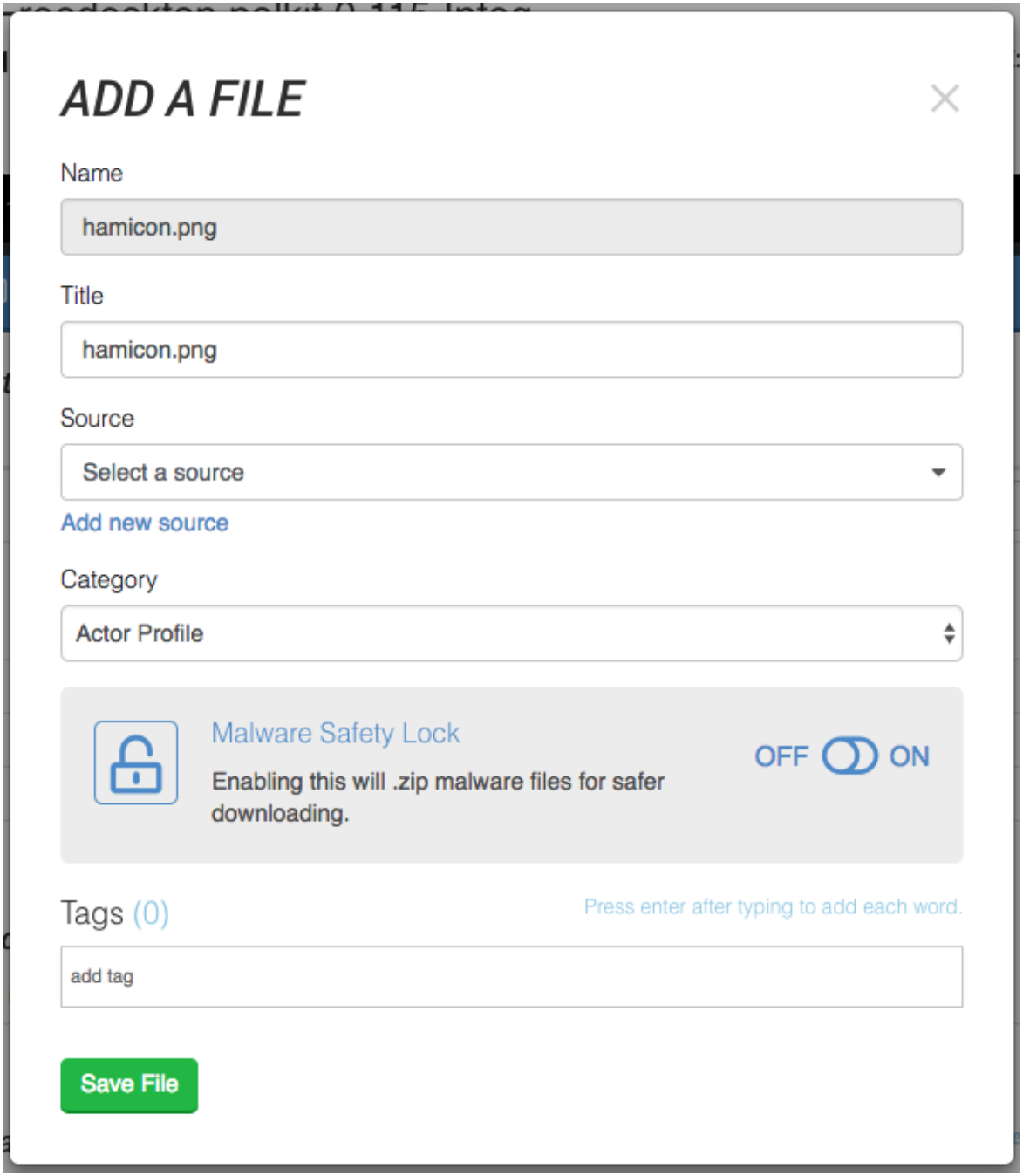
To add a File:

1. Click **Create New > File**.



The Add a File dialog box opens.

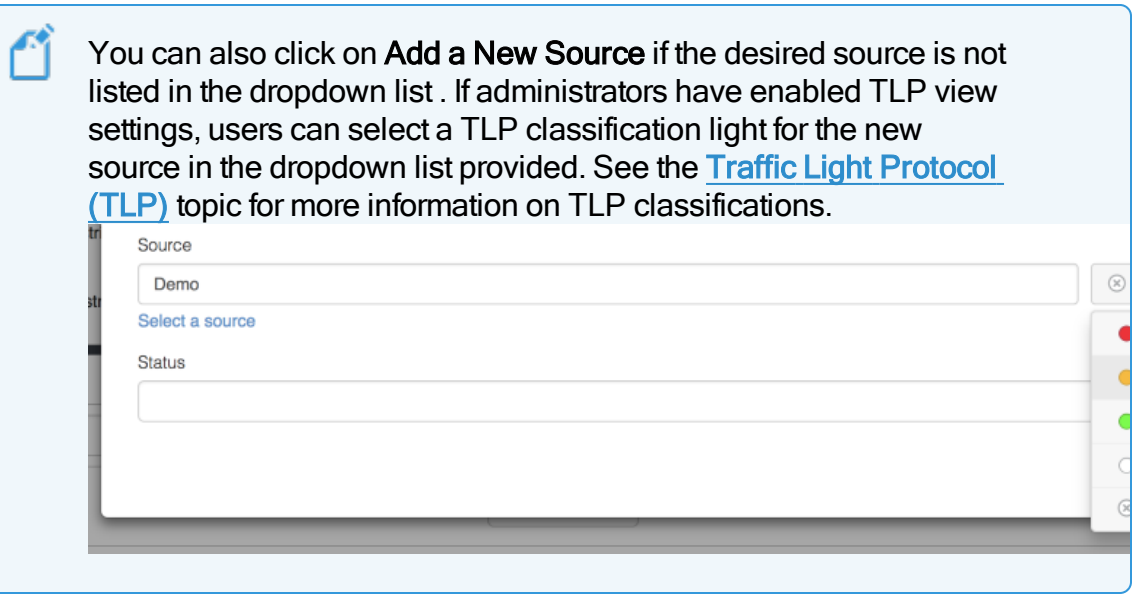
2. Drag the file into the dialog box or browse and locate the file.



The Add a File Dialog box will update.

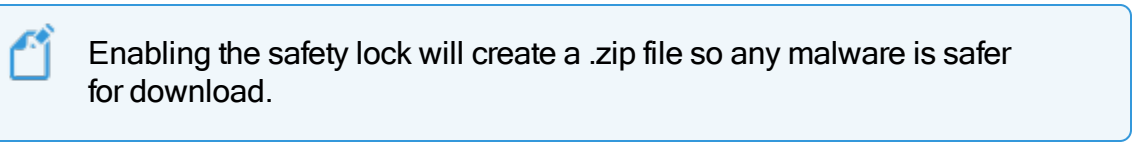
3. Update the **Title** if desired.

4. Select a **Source** from the dropdown list provided.



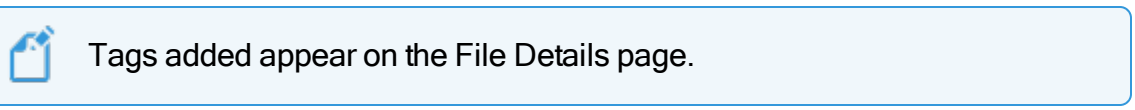
You can also click on **Add a New Source** if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, users can select a TLP classification light for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP classifications.

5. Select a **Category**.
6. Select whether to have the **Malware Safety Lock** on or off.



Enabling the safety lock will create a .zip file so any malware is safer for download.

7. Add any desired tags.



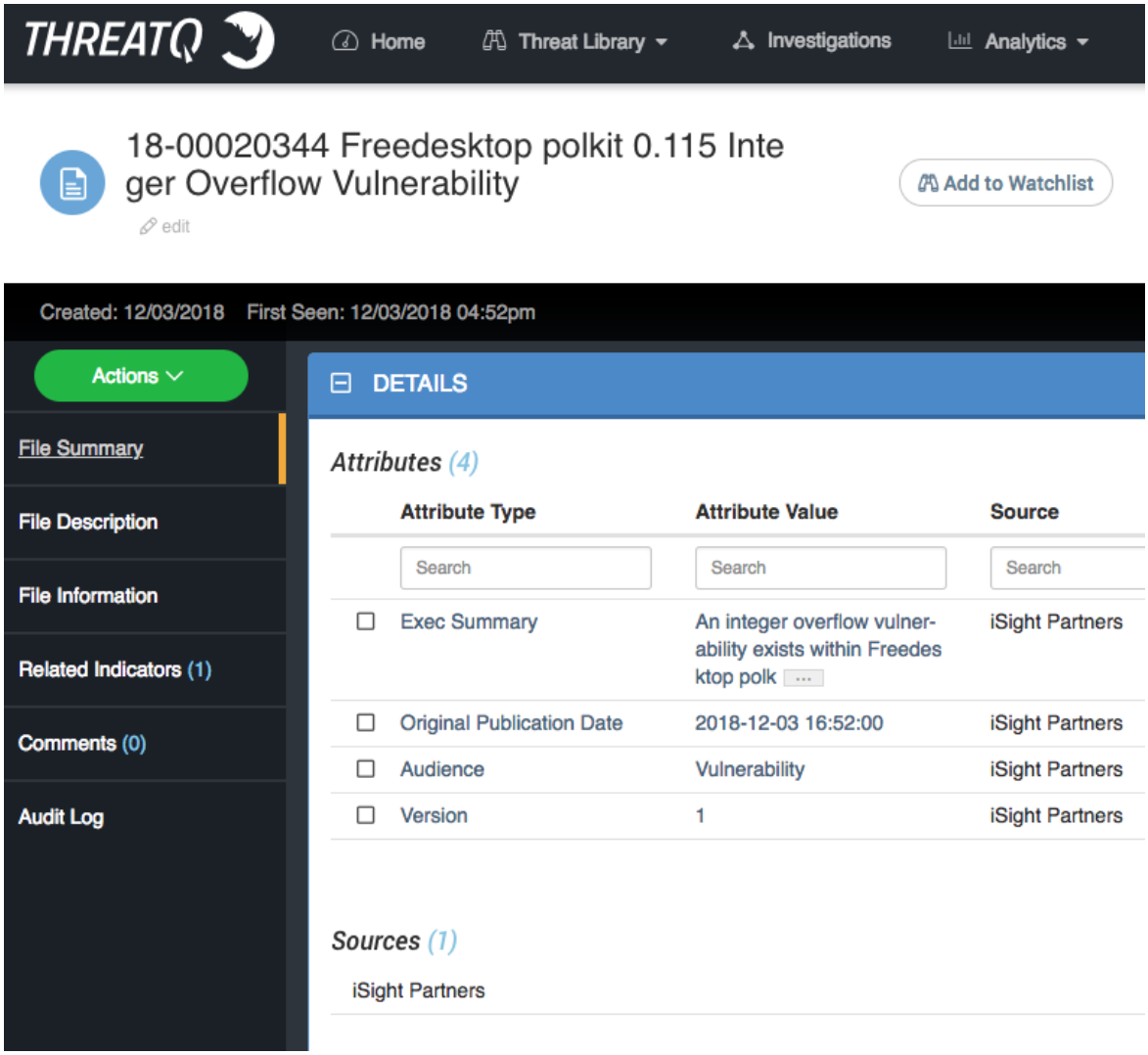
Tags added appear on the File Details page.

8. Click **Save File**.

Editing Files

To edit a File Name:

1. Locate and click on the file.



The File Details page opens.

2. Click on **Edit** next to the File name.

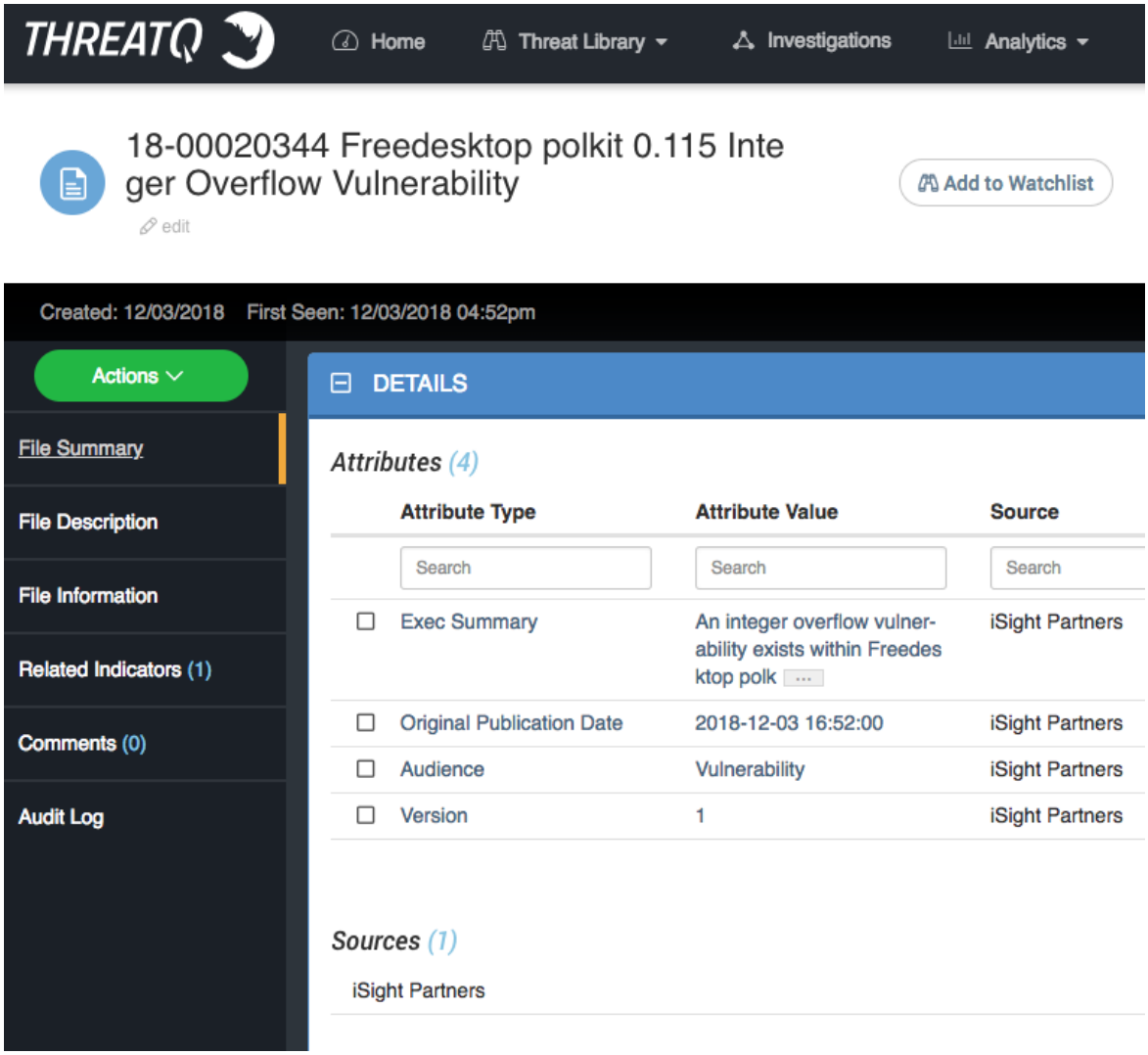
The Edit File dialog box opens.

3. Make the desired change to the File Name.
4. Click on **Save File**.

Deleting Files

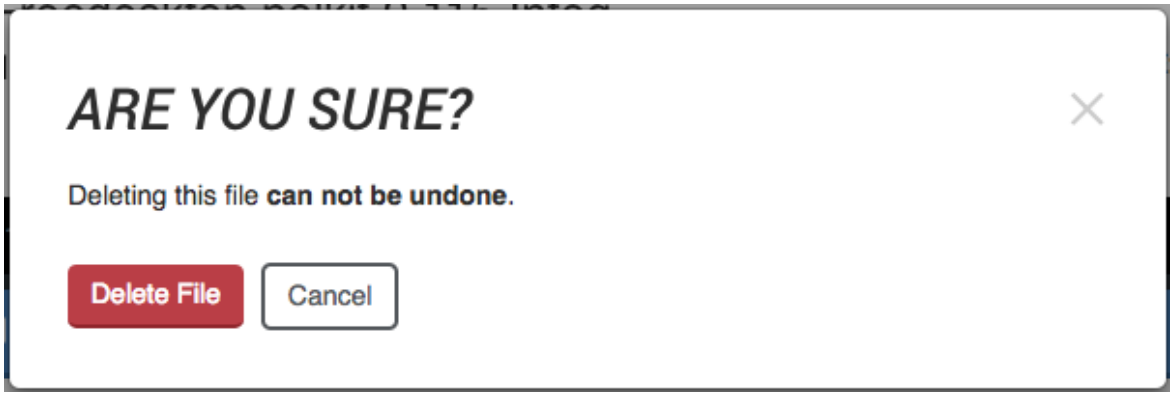
To delete a File:

1. Locate and click the file.



The File Details page opens.

2. Click on **Delete this File** located to the top right of the page.



   A confirmation dialog box appears.

3. Click on **Delete File**.

Indicators

Indicators are the so called "finger prints" associated with a malicious attempt or adversary group.

Indicators can be scored to allow you to apply weighting using contextual information, such as sources, attributes, and indicator types, as they are added to ThreatQ. You can also set a manual score per indicator.

You can also apply expiration dates to an indicator to when it is determined to pose less of a threat to your infrastructure than other indicators.

Related Topics:

- Adding an Indicator
- Parsing for an Indicator
- Indicator Search
- Indicator Expiration
- Automatic Expiration and Policies
- Indicator Scoring

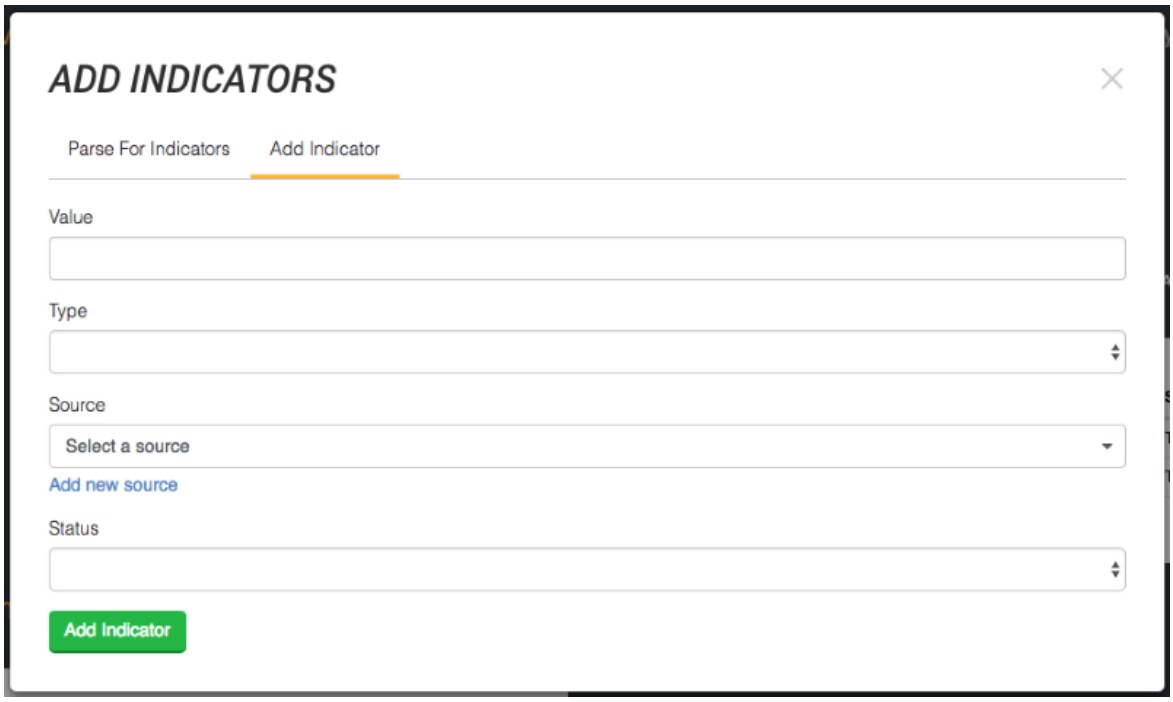
- Whitelisted Indicators
- Indicator URL Normalization

Adding an Indicator

To add an Indicator:

1. Click on **Create > Indicator**.

   You can also select **Indicator Parser** from the Create menu if importing a file. The option is located under the Import section of the Create menu. See the Parsing for an Indicator topic.

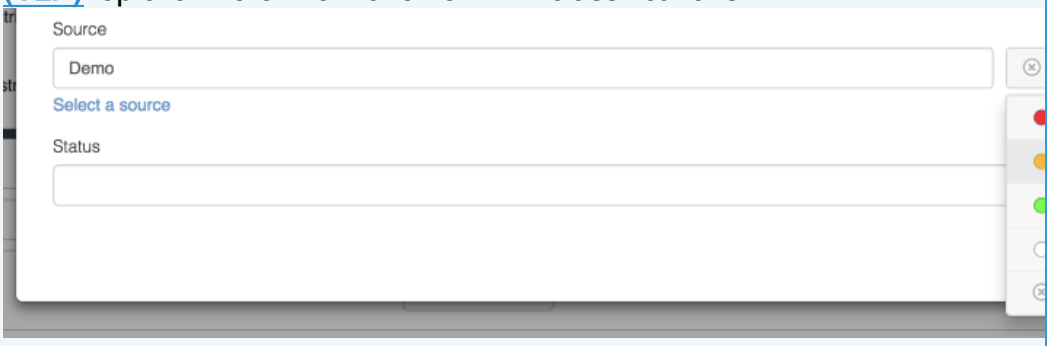


   The Add Indicators dialog box opens.

2. Enter a value in the **Value** field.
3. Select the **Type** of Indicator.

4. Select a **Source** from the provided dropdown list.

You can also click on **Add a New Source** if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, users can select a TLP classification light for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP classifications.

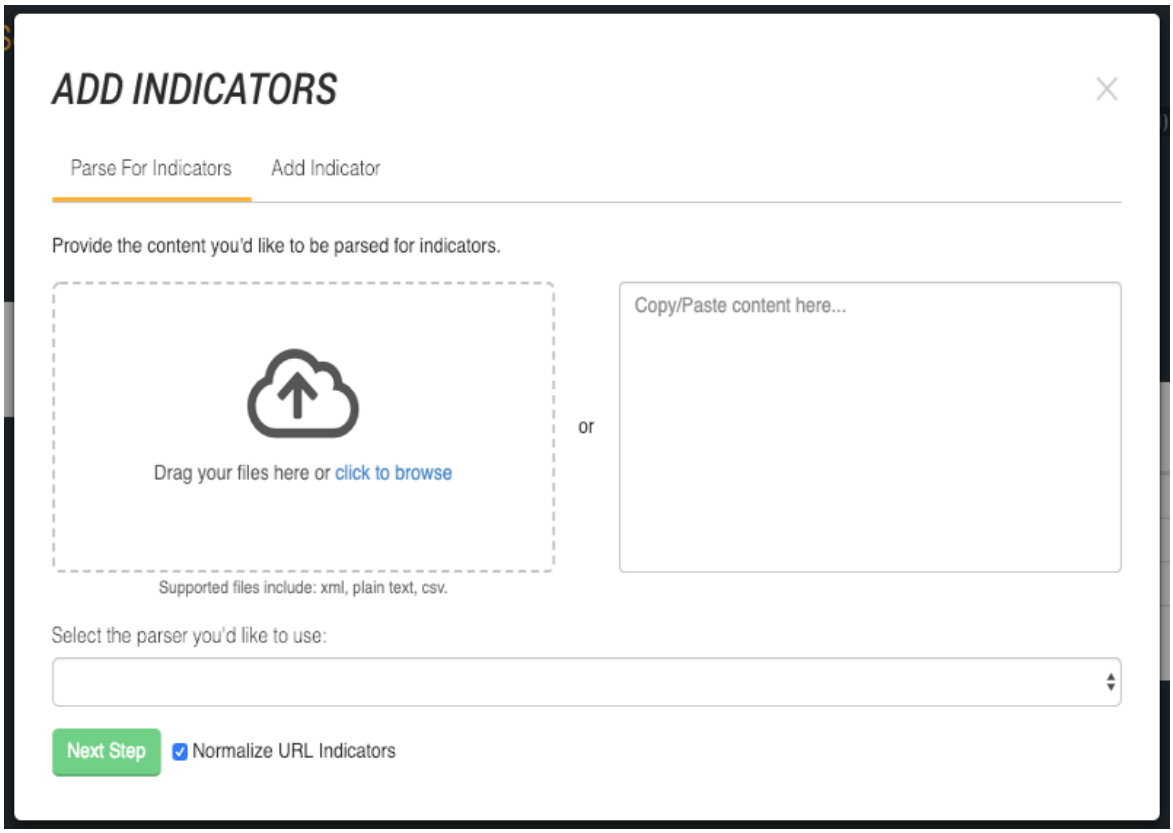


5. Select a **Status** for the indicator.
6. Click **Add Indicator**.

Parsing for an Indicator

1. Click on the **Create** button, located at the top of the dashboard and select **Indicator Parser** under the *Import* heading.

You can also click on **Create** > **Indicator** and then select the **Parse for Indicators** option at the top of the **Add Indicators** modal.



The Add Indicators dialog box will load.

2. Do one of the following:

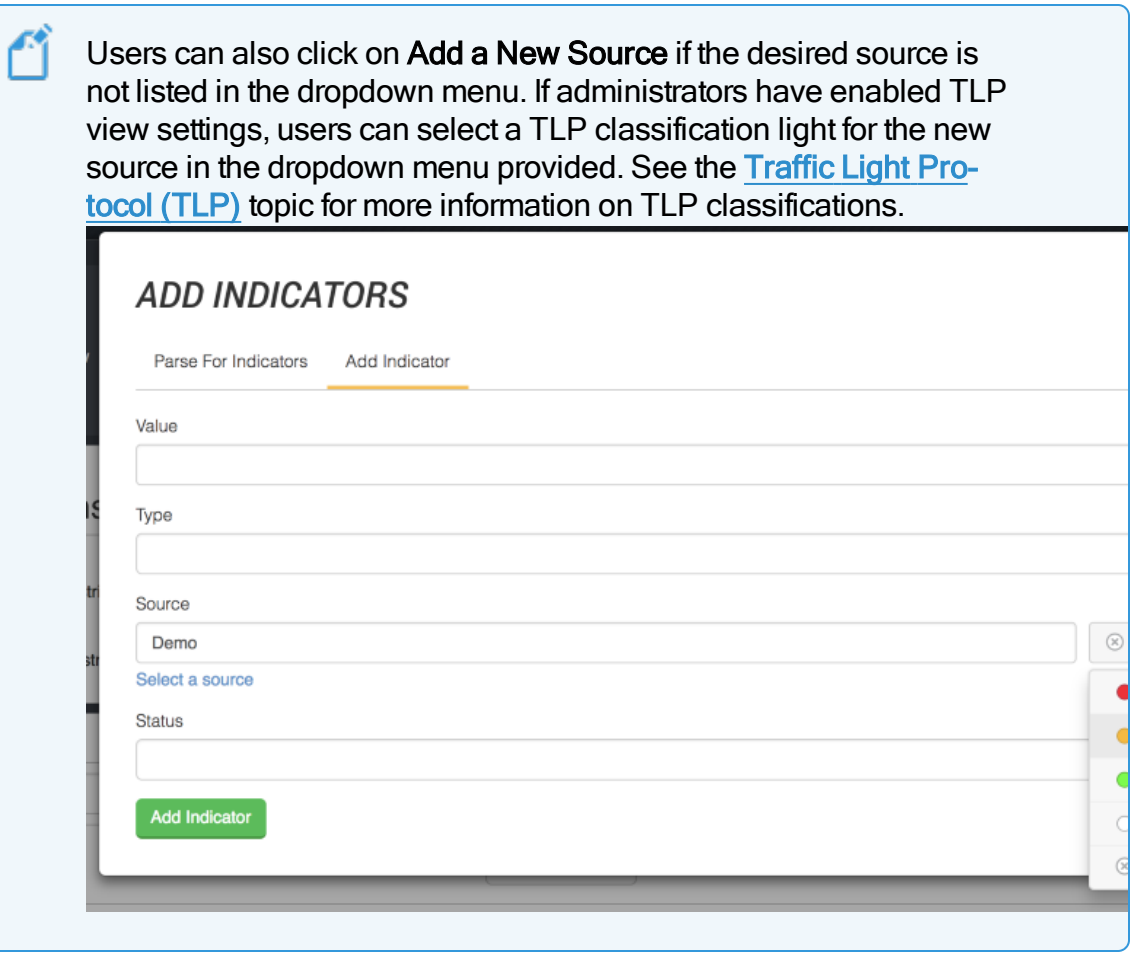
   - Drag your file(s) into the left pane.
   - Click on **Click to Browse**, and locate the file you wish to upload.
   - Copy/paste the content in the right pane.

3. Select the **Parser** to use and click on **Next Step**.
4. Select whether to save or delete the file after the import.

   Steps 5-7 pertain to saving the file. Skip to step 8 if you are not saving the file after import.

5. Update the **File Title** if needed.

6. Enter an optional **File Description**.
7. Confirm or update the **File Category**.
8. Select a **Source** from the dropdown menu provided.



Users can also click on **Add a New Source** if the desired source is not listed in the dropdown menu. If administrators have enabled TLP view settings, users can select a TLP classification light for the new source in the dropdown menu provided. See the Traffic Light Protocol (TLP) topic for more information on TLP classifications.

9. Select a **Status** to be applied to the extracted indicators.
10. Select any optional **Attributes** to be applied.
11. Click on **Next Step**.

If the file contains events that are detected, the Step 2: Review Events page opens. Indicators may be new or pre-existing. Pre-existing indicators are identified by a badge within the table. You can isol-

ate new and pre-existing indicators by using the tabs at the top of the right hand panel.

12. Locate and select one or more indicators using one of the following options:
    - From within the contents (on the left)
    - From the table (on the right)
    - By using the Select dropdown menu
13. Once you have selected one or more indicators, you can perform these functions:
    1. **Add Info** – Click the Add Info button to open the Add Info dialog box where you can perform the following functions:
        - Add Attributes to the indicator: add one or more attributes to the selected indicator(s). Once completed, click Add Attributes.
        - Link to Another Object: Link the selected indicator(s) to another object (indicator, event, adversary, file) and click Link Object.
        - Set Status: Select a status and click Set Status.
    2. **Edit** the type or status of an indicator by clicking its type or status in the table and selecting an option from the dropdown menu.
    3. **Add Indicator** - If you notice an indicator on the left that was not extracted, you can add it by clicking Add Indicator and completing the process.
    4. If you want to search within the table, use the fields at the top of the columns.

If at any point, you wish to abandon the import, click **x ABANDON THIS IMPORT**.

15. Click on **Finish Import**.

CSV File Format - Parsing

When importing a .csv file to parse for indicators using the ThreatQ CSV File Parser, the .csv file **must** meet the following criteria:

- The file must be comma-delimited.
- The file must include **at least** the following columns:
  - Indicator
  - Type: This column cannot contain types that are not already established in ThreatQ. You cannot add custom indicator types and indicator types are case sensitive. Choose from the following:
    - CIDR Block
    - CVE
    - Email Address
    - Email Attachment
    - Email Subject
    - File Path
    - Filename
    - FQDN
    - Fuzzy Hash
    - GOST Hash
    - IP Address
    - MD5
    - Mutex
    - Password
    - Registry Key
    - SHA-1
    - SHA-256

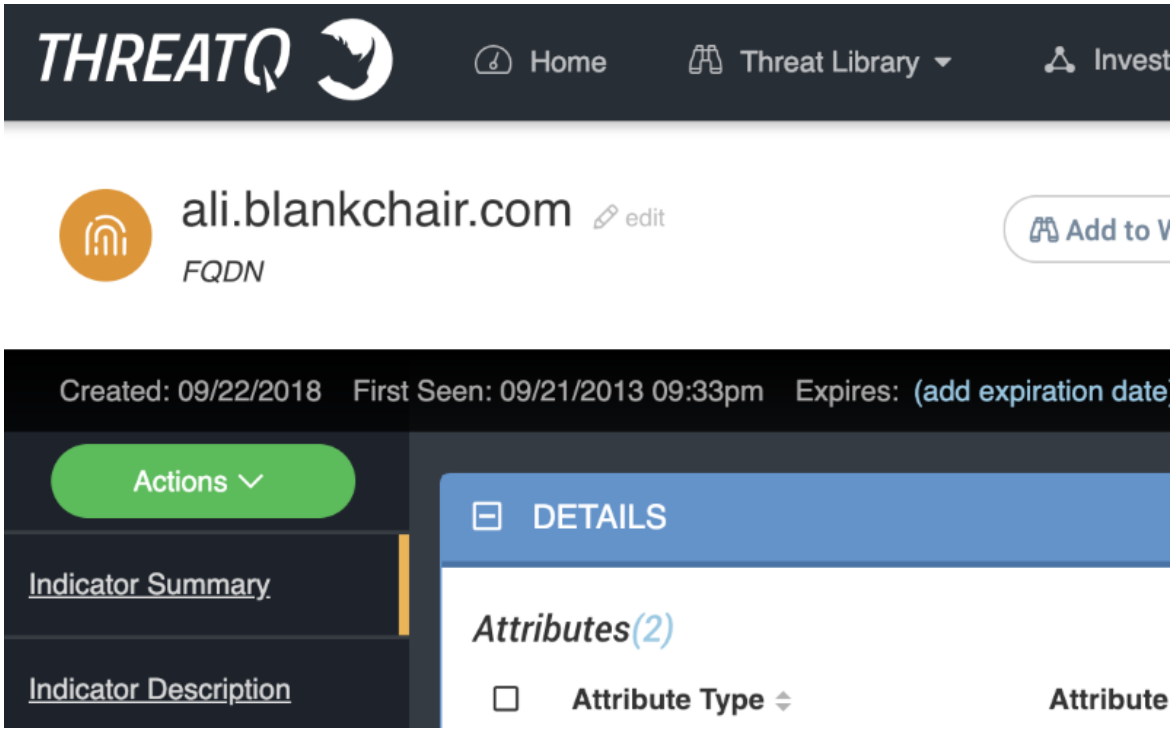
        - SHA-384
        - SHA-512
        - String
        - URL
        - URL Path
        - User-agent
        - Username
        - X-Mailer
    - Status

If the file is not properly delimited, missing a required column, or containing a valid type, it will fail upon upload.

Editing Indicators

To edit an Indicator:

1. Locate and click on the indicator.



The Indicator Details page opens.

2. Click on **Edit** next to the Indicator name.

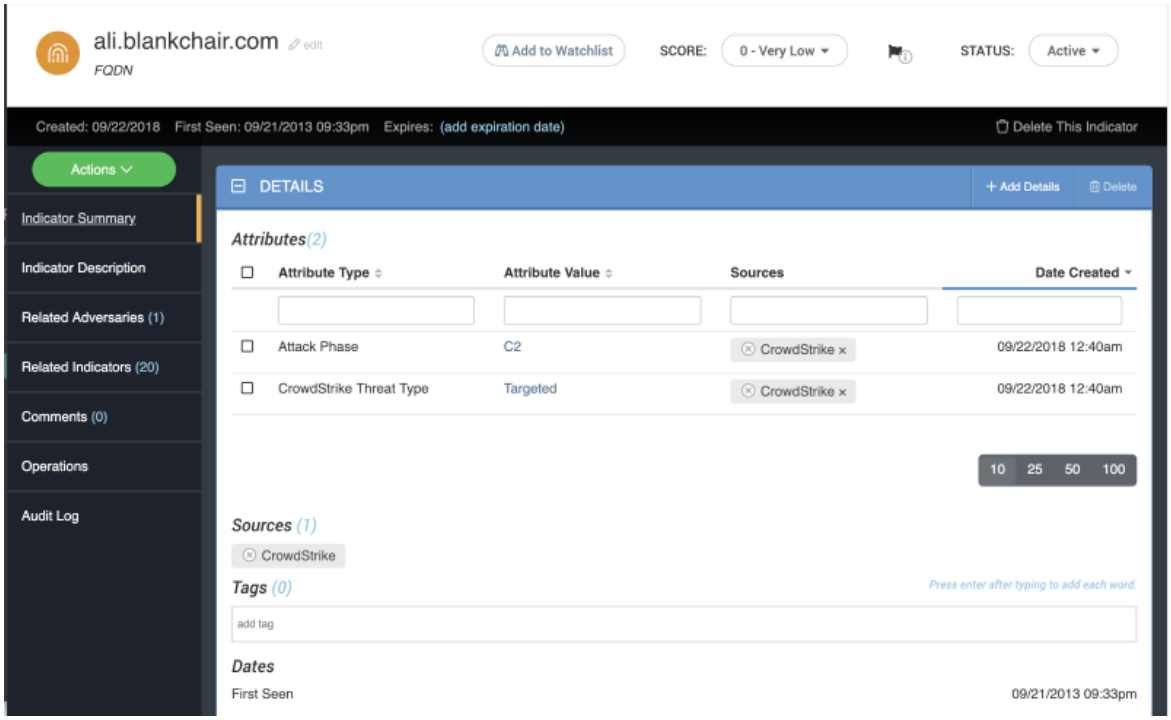
The Edit Indicator dialog box opens.

3. Make the desired change to the indicator Value and Type.
4. Click on **Save Indicator**.

Deleting Indicators

To delete an Indicator:

1. Locate and click the Indicator.



The Indicator Details page opens.

2. Click on **Delete this Indicator** located to the top right of the page.

   A confirmation dialog box appears.

3. Click on **Delete Indicator**.

Indicator Search

Indicator Search allows you to search indicators based on a wide range of modifiers and search criteria. For example, when searching for an event, the results will include all indicators related to that event.

> Using indicator search will provide the total number of indicators matching the criteria of your search, however, the page will only load 1,000 indicators within the results table.

With respect to searching for IP Address or CIDR Block indicators, your results will be as follows:

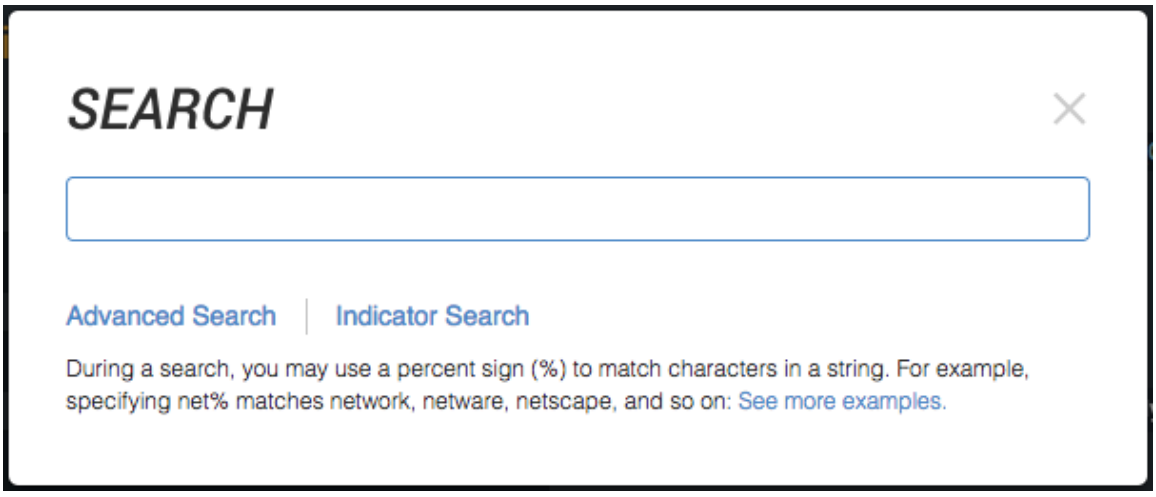
- If searching for an IP Address, CIDR blocks will be returned if they fall within the range.
- If searching for CIDR blocks, IP addresses will be returned if they fall within the range.

> This will search indicator values as well as Attribute of type “IP Address” (for instance, if an IP address is associated to another IP address through a passive DNS relationship).

Performing an Indicator Search

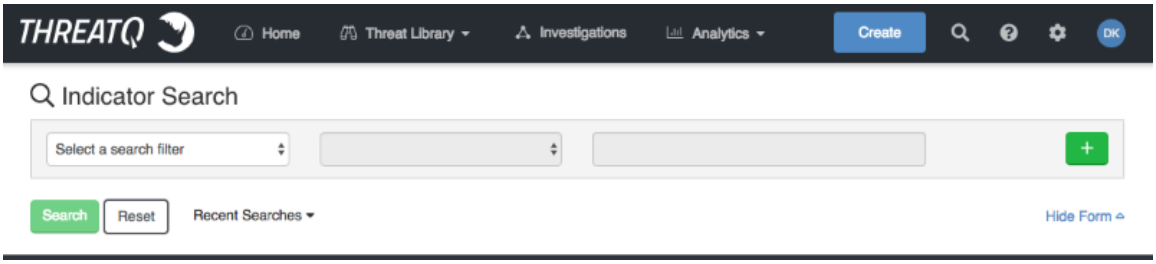
To perform an Indicator Search:

1. From the main menu, click the **Search** icon.



   The Search dialog box appears.

2. Click **Indicator Search.**



   The Indicator Search page appears.

3. Select the desired search parameters and operators using the dropdowns, and enter the values.

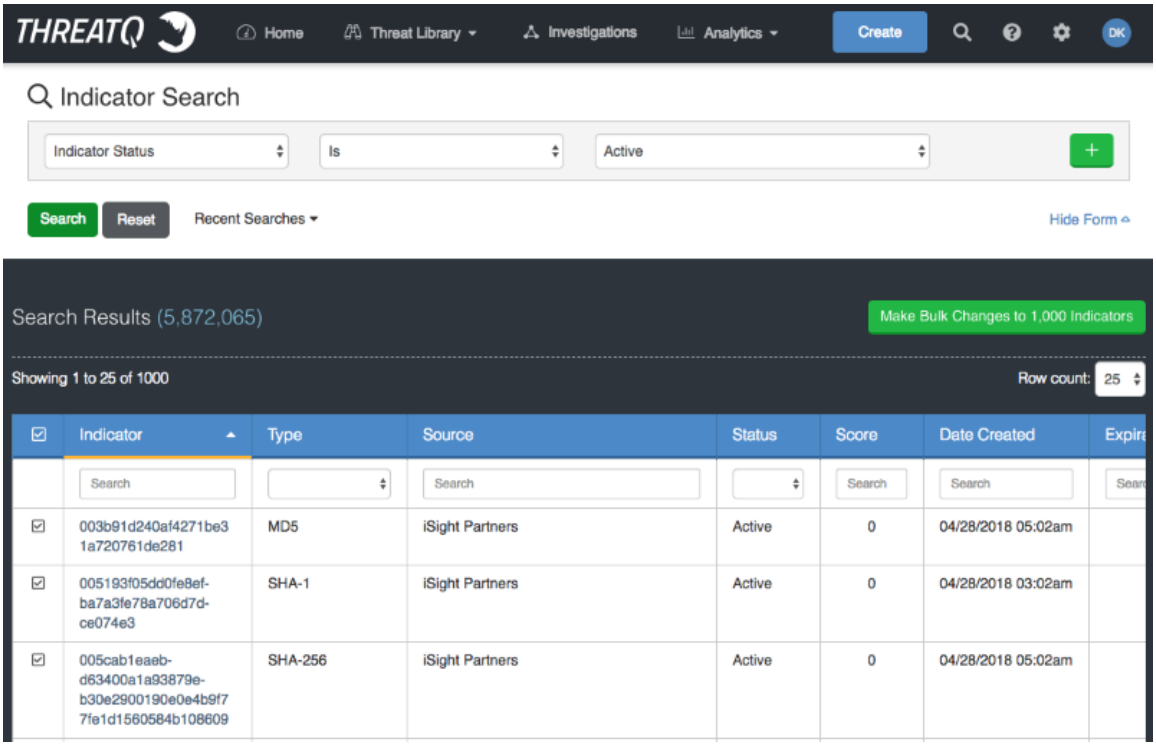
Parameter	Operator
Indicator Class	Is Is not Is Blank Is Not Blank

Parameter	Operator
Indicator Value	Contains Does Not Contain Is Is not Is Blank Is Not Blank
List of Indicators	Contains Does Not Contain Is Is not Is Blank Is Not Blank
Indicator Status	Is Is not Is Blank Is Not Blank
Indicator Type	Is Is not Is Blank Is Not Blank
Date Created	Is Is not Is after Is before Is in the range of Is Blank Is Not Blank
Date Last Modified	Is Is not Is after Is before Is in the range of Is Blank Is Not Blank

Parameter	Operator
Attachment Title	Contains Does Not Contain Is Is not Is Blank Is Not Blank
Adversary	Contains Does Not Contain Is Is not Is Blank Is Not Blank
Event Title	Contains Does Not Contain Is Is not Is Blank Is Not Blank
Event Type	Is Is not Is Blank Is Not Blank
Attribute	Contains Does Not Contain Is Is not Is Blank Is Not Blank

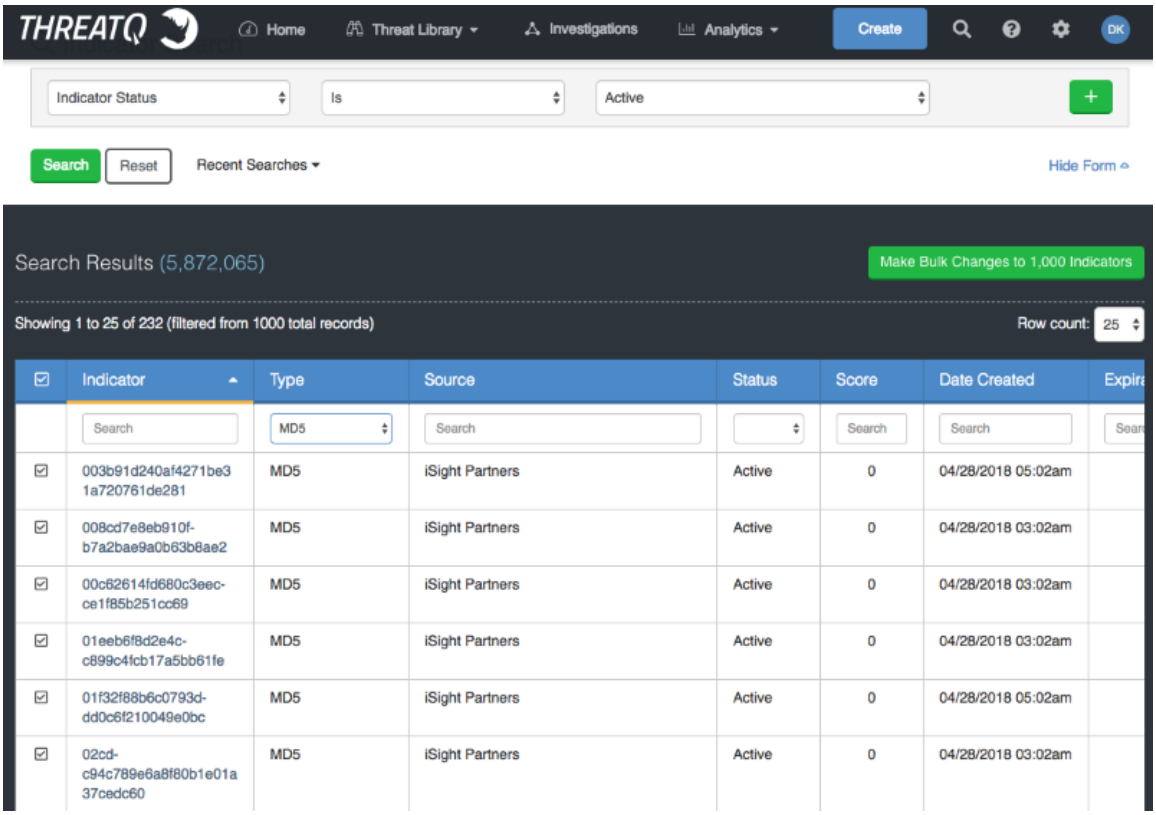
Click **+** to add more parameters. When your search consists of more than one parameter, you can select **and** or **or** using the dropdown between the search parameters.

4. Click **Search**.



Search results are displayed in a search results table.

5. (Optional) Change the number of entries shown in the search results table by clicking the dropdown menu at the top right and selecting the desired option.
6. (Optional) Click a column header to sort the data by column, and click again to reverse sort order.
7. (Optional) Search within a column by clicking within the search field at the top of the column, entering a search keyword, and pressing Enter.



Results will be shown below the search query.

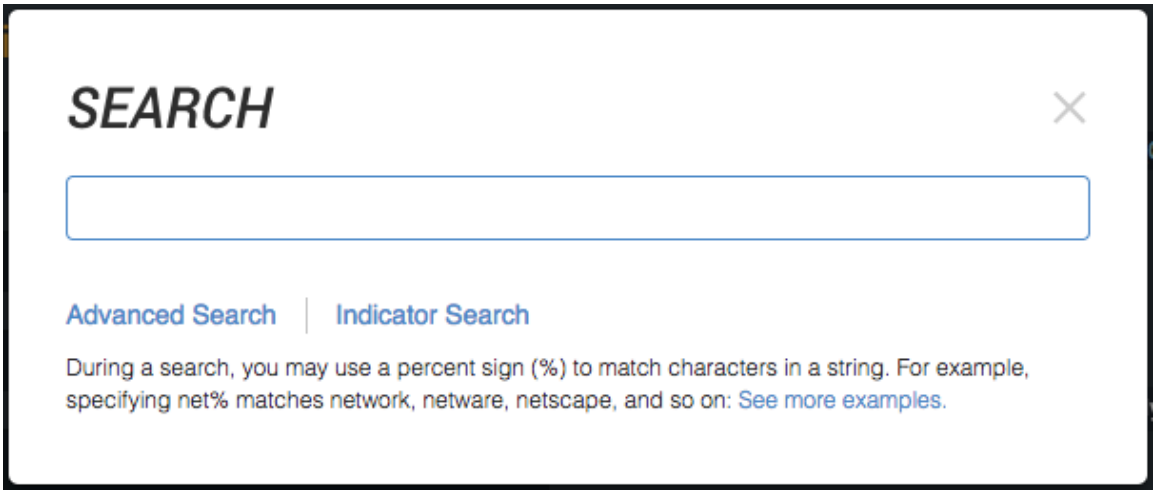
You can hide the query to view more of the search results.

Making Bulk Updates to Search Results

The bulk update tool allows you to make batch changes to the objects in your Search results. The tool is limited to 1000 objects per update.

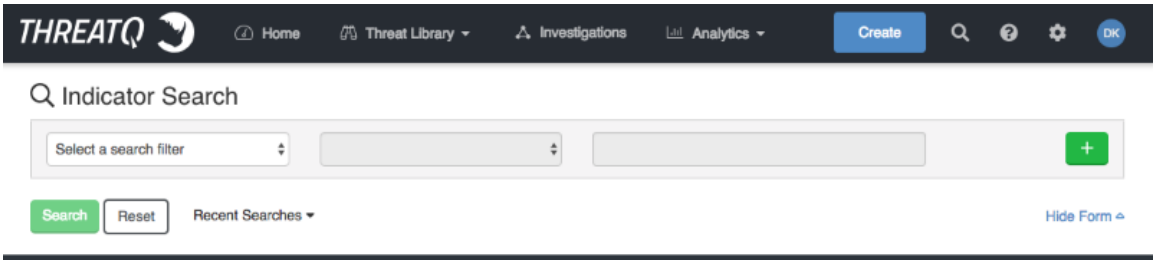
To make bulk updates to search results:

1. From the main menu, click the Search icon.



The Search dialog box appears.

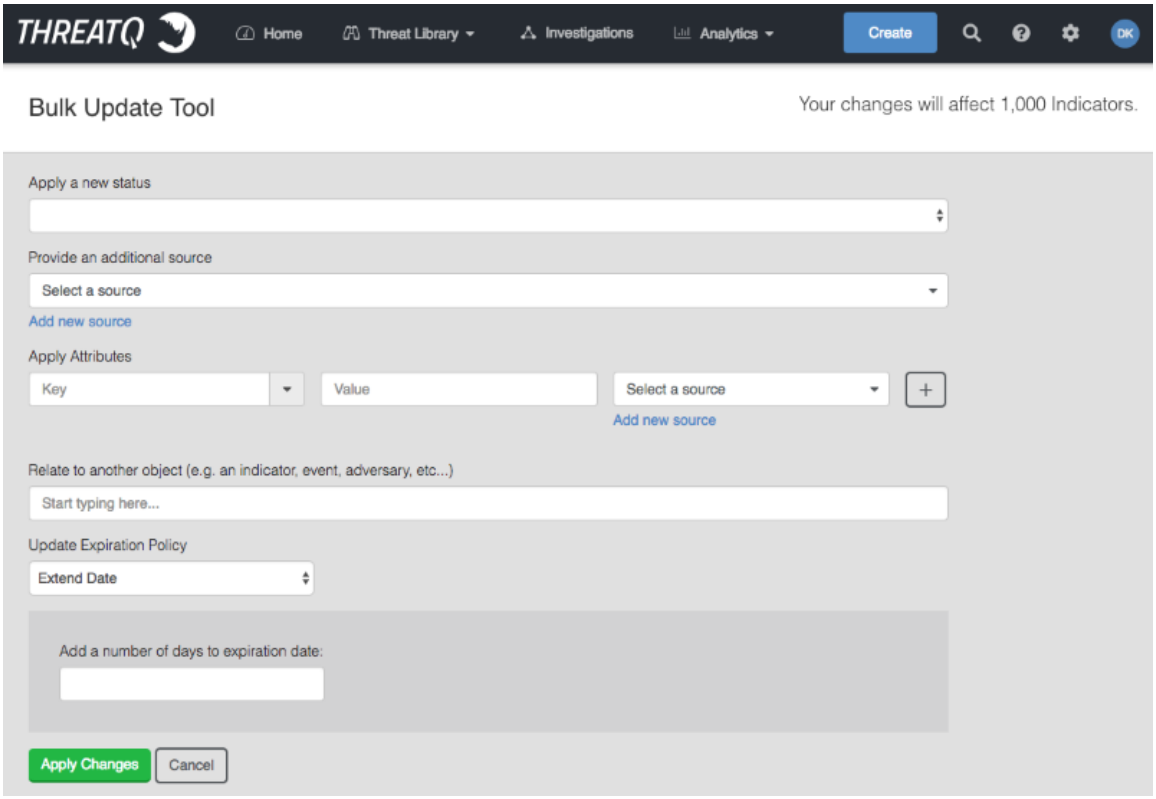
2. Click **Indicator Search.**



The Indicator Search page appears.

3. Perform your Indicator Search.

4. At the top of the Search Results, choose **Make Bulk Changes to 1,000 Indicators**.



The Bulk Update Tool appears.

5. Optionally, apply a new object status by choosing from the dropdown.
6. Optionally, enter an additional source.
7. Optionally, apply one or more attributes:
    a. Choose an Attribute Type from the dropdown.
    b. Enter an Attribute Value.
    c. Enter an Attribute Source.
    d. Optionally, choose the add icon to apply additional attributes.
8. Optionally, relate your search results to another object in the platform. As you enter the related object, ThreatQ offers type-ahead suggestions.

9. Optionally, update the object's expiration policy, by choosing an option from the Update Expiration Policy dropdown.
10. Click **Apply Changes**.

Indicator Status

Every indicator in the system will have a status applied to it.

The default statuses that ship with a standard installation of ThreatQ are as follows:

Status	Description
Active	Poses a threat and is being exported to detection tools.
Indirect	Associated to an active indicator or event (i.e. pDNS).
Review	Requires further analysis.
Whitelisted	Poses NO risk and should never be deployed.
Expired	Indicator has reached its expiration and has been is deemed by an analyst to pose less of a threat to their infrastructure than other indicators.

You cannot delete a default status but you can add new custom statuses to be used. See Adding an Indicator Status and the Related Topics section below for more details.

Most exports in ThreatQ are configured to use the Active status to signal deployment to external devices. However this can be modified and each status can be used however your organization sees fit.

Related Topics:

- Changing the Status of an Indicator
- System Configuration: Indicator Statuses

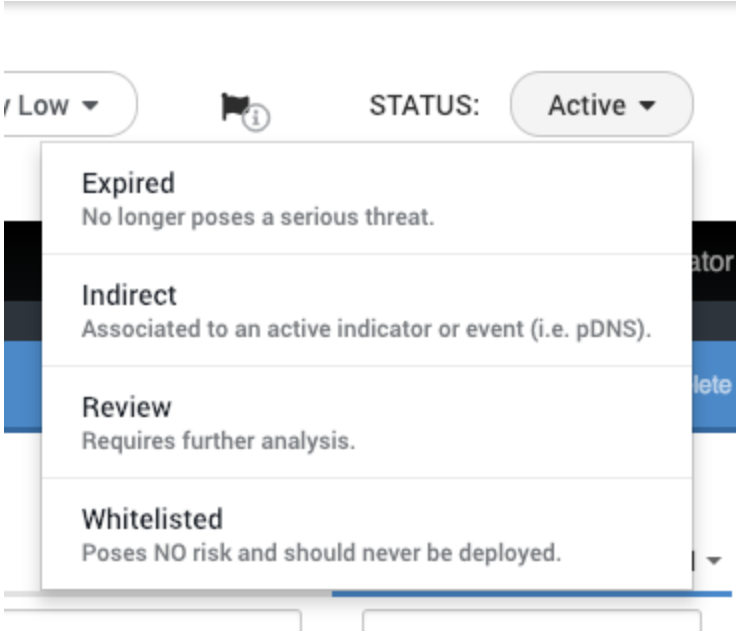
- Indicator Expiration
- Automatic Expiration and Policies

Changing the Status of an Indicator

Changing an indicator's status is straightforward, except in the case of whitelisting CIDR Block indicators. When whitelisting a CIDR Block indicator, this process generates a whitelisting rule. See Whitelisted Indicators for more information.

Changing the status of an indicator:

1. Locate and click the indicator to open its details page.
2. Click the status dropdown menu, and select the desired status.



The status will be updated.

If an Administrator or the Primary Contributor are whitelisting a CIDR BLOCK indicator, there is a different process, as this actually generates a whitelisting rule. For more information, see the Creating a Whitelist Rule topic.

Indicator Expiration

Expiration ("Expired") is a status that can be assigned to an indicator. The expired status should be used when an indicator is deemed by an analyst to pose less of a threat to their infrastructure than other indicators.

Related Topics:

- Ways an Indicator can Expire
- Expiration Date Displays
- Changing an Individual Indicator's Date
- Automatic Expiration and Policies

Ways an Indicator can Expire

- **An analyst manually changes an indicator(s) status to "Expired"**

  This can be achieved by visiting an individual indicator's details page, then using the Status dropdown in the top right hand corner of the page to change the status.

  If the analyst wishes to change the status of multiple indicators at the same time, they can use the advanced search tool to find the indicators they'd like to update, then click the Bulk Update button found directly to the right above the search results.

- **An analyst manually sets an expiration date for a specific indicator**

  Each indicator has the option to have an expiration date set, which once past, will toggle the status of that indicator from it's current status to "Expired".

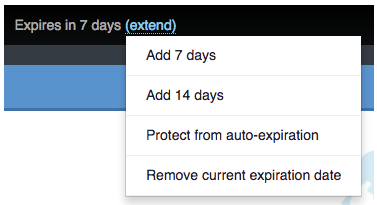
- **An expiration policy has been applied to the source reporting an indicator and therefore an expiration date is automatically set for that indicator during ingestion**

Using the “Expiration” tab on the Indicator Management page, a ThreatQ admin has the ability to apply expiration policies to all ingested information, both new and existing, coming from a specific intelligence source.

If an indicator is reported by multiple sources that have expiration policies, the date will be set using the greater expiration date. For example, if both Feed A (with a 5 day policy) and Feed B (with a 3 day policy) report the same indicator on the same day, that indicator will automatically expire 5 days from now.

Changing an Individual Indicator's Date

When viewing a specific indicator, its expiration date can be changed by clicking on the link next to the expiration information.

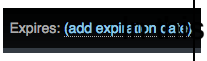
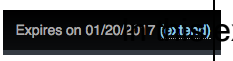


Options include:

Option	Description
Add 7 Days	This will extend the current expiration date by 7 days.
Add 14 Days	This will extend the current expiration date by 14 days.
Protect from Auto-Expiration	This will set the indicator to "Never Expire". Once set, this indicator will be exempt from all automated expiration processes regardless of circumstances. The only way for this indicator to expire moving forward is by analyst choice.
Remove Current Expiration Date	This will remove the currently set expiration date. If this indicator is reported by an intelligence feed (with an expiration policy) in

Option	Description
	the future, a new expiration date will be added at that point in time.

Expiration Date Displays

Option	Image	Description
No expiration date has been set		example, the indicator will not automatically expire because an expiration date has not been specified. This status will be changed if an analyst sets an expiration date or a new source (with an expiration policy applied to it) reports this indicator in the future.
An expiration date is set		example, the indicator has an expiration date set of 1/20/2017. This means that this indicator will expire when the calendar day changes from the 19th to the 20th of January (based on ThreatQ's server time, not the user's local time).
		an expiration date is less than 7 days away, ThreatQ will switch to show a relative version of the date.
Protected from automatic expiration (Never Expire)		times an analyst will want an indicator to stay "Active" regardless of any automated circumstances. In this case you can set an indicator to be protected from auto-expiration, which will display the words "Never Expire". This can only be "overwritten" by an analyst.

Automatic Expiration and Policies

Automatic expiration allows you to deprecate stale intelligence based on a set of defined criteria. As the data becomes less relevant, ThreatQ sets the status to Expired, which relieves the data burden on your team or infrastructure.

You can configure automatic expiration from the Data Management page.

1. From the navigation menu, click on settings icon and select **Data Management**.

   The Data Management page will open with the Automatic Expiration tab selected by default.

Related Topics:

- How ThreatQ Calculates Expiration Dates
- Selecting an Expiration Policy per Feed
- Applying Expiration Policy Changes to Data
- Adding Exceptions
- Common Expiration Policy Scenarios

How ThreatQ Calculates Expiration Dates

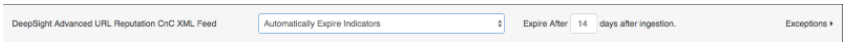
Scenario	Description
Indicator Reported by Source with an Expiration Policy	If an indicator has an expiration date and it's reported by a new source that has an expiration policy, ThreatQ will set the expiration date using the policy with the greater expiration date.
Indicator Report by a Source with an Expiration Policy of Never Expire	If an indicator has an expiration date and it's reported by a new source that has an expiration policy of Never Expire, ThreatQ sets that indicator to Never Expire.
Indicator Reported by a	If an indicator is reported by a source that has an exception for the indicator, the exception expiration date will be used regardless of

Source with an Exception for that Indicator	the greater expiration date. An exception takes precedence over the source's expire policy.
Indicator Reported by Two Different Sources	If an indicator is reported by a source with an Expiration Policy and then reported by a second source with another Expiration Policy, the greatest expiration date is selected to set the expiration date. The expiration date will be set based on the date the second source reported the indicator.
Indicator Reported by Two Different Sources, one with an Exception	If an indicator is reported by a source that has an exception for the indicator and then reported by a second source, the greatest expiration date is selected despite the exception. The expiration date will be set based on the date the second source reported the indicator.

Selecting an Expiration Policy per Feed

You can choose from three options when configuring an expiration policy for a source of intelligence:

Option	Description
Don't automatically expire (No policy set)	ThreatQ sets all feeds to **Don't Automatically Expire** until an analyst decides otherwise. When set, indicators reported from this specific feed do not have an expiration date automatically applied to them. If an indicator is reported by Source A (an intelligence feed without an expiration policy), and is later reported by Source B (an intelligence feed that expires data in 7 days), ThreatQ sets

Option	Description
	the indicators to automatically expire in 7 days.
Automatically Expire Indicators	When setting a specific intelligence feed to **Automatically Expire Indicators**, ThreatQ requires you to provide a specific number of days. After you configure this setting, it applies to all intelligence currently in the system, as well as new intelligence as it is ingested. ThreatQ calculates the appropriate expiration date based on the number of days from ingestion. Once an indicator's expiration date is met, its status changes to **Expired**. 
Never Expire	Using this setting ensures that all intelligence reported by a specific feed is protected from automatic expiration, regardless of scenario.

Applying Expiration Policy Changes to Data

When updating an expiration policy, the system now applies the update to all selected existing data in the platform to honor the new policy. This process can take a while based on system resources and the number of indicators in the system.

Refer to the following table for estimates on the total time required for the system to apply the selected policy to existing data, based on the following criteria:

- Dataset: 6 Million Indicators
- System Specifications: 32GB VM 4 vCPU

Indicators to reset expiration out of 6m total indicators	Reset and Recalculate Expiration	Expire Indicators	Total Time for Reset
50,000	3 hours and 30 minutes	53 seconds	3 hours 31 minutes
100,000	4 hours and 51 minutes	1.8 minutes	4 hours 53 minutes
200,000	10 hours 20 minutes	3.5 minutes	10 hours 24 minutes
1.2 million	2 days 7 hours 4 minutes	35 minutes	2 days 7 hours 40 minutes
3.1 million	3 days 16 hours 42 minutes	3.5 hours	3 days 20 hours
5.3 million	4 days 7 hours 17 minutes	4.7 hours	4 days 12 hours

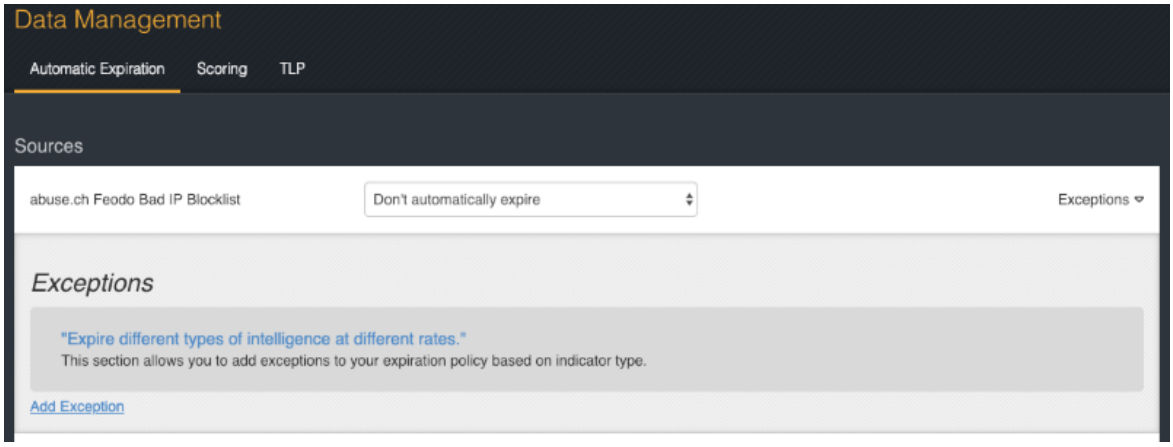
Adding Exceptions

ThreatQ allows you to add exceptions based on specific indicator types within in a feed in addition to setting an expiration policy at a global level for all intelligence ingested by a specific feed.

To Add an Exception:

1. Navigate to the **Automatic Expiration** tab under **Data Management**.
2. Locate the source.
3. Click **Exceptions** to expand the option.

The Exceptions option menu opens.



4. Click **Add Exception**.
5. Select the **Indicator Type** from the dropdown.
6. Enter the number of days after the item has been ingested before expiring.

> Repeat steps 4-6 to add multiple

7. Click on **Delete** next to the row to delete an exception.
8. Click on **Save**.

Common Expiration Policy Scenarios

Scenario	Description
An indicator is reported by a single source (with an expiration policy)	1. On 10/1, Source A reports the indicator and the expiration date is set to 10/8. 2. When the date switches from 10/7 to 10/8, this indicator is queued to have its status changed to **Expired**.
An indicator is reported by Source A (with an expiration policy of 7 days)	1. On 10/1, Source A reports the indicator and the expiration date is set to 10/8.

Scenario	Description
and 3 days later is reported by Source B (with an expiration policy of 10 days).	2. Source B reports the same indicator 3 days later (10/4). The indicator's expiration date is set using the greatest expiration date between the two sources. In this example, the new expiration date will be 10/14 (10 days from when it was reported by Source B). 3. When the date switches from 10/14 to 10/15, this indicator is queued to have its status changed to **Expired**.
An indicator is reported by Source A (with an expiration policy of 7 days) and is later reported by Source B (with an expiration policy of Never Expire).	1. On 10/1, Source A reports the indicator and the expiration date is set to 7 days. 2. Source B reports the same indicator 3 days later with a policy of **Never Expire**. The indicator's expiration date is removed and the indicator is now set to **Protect from auto-expiration**.
An indicator is currently set to Expired and is reported by Source A (with an expiration policy of 7 days).	1. On 10/1, an indicator is in ThreatQ with a status of **Expired**. 2. On 10/1, Source A reports the indicator. The status of the indicator changes to whatever the default status is for Source A and the expiration date is set to 10/8. 3. When the date switches from 10/7 to 10/8, this indicator is queued to have its status changed to **Expired**.

Scenario	Description
An indicator is currently set to Expired and is reported by Source A (with an expiration policy of 7 days).	1. An indicator is in ThreatQ with a status of Expired. 2. Source A (with an expiration policy of Never Expire reports the indicator. The expiration of that indicator changes to Protect from auto-expiration.
A FQDN indicator is reported by Source A (with an expiration policy of 10 days with an exception for 5 days for FQDN indicators) and is later reported by Source B (with an expiration policy of 15 days).	1. On 10/1, Source A reports the FQDN indicator and the expiration date is set to 10/6.  An exception takes precedence over the source's expire policy. 2. Source B reports the same indicator 1 day later (10/2). The indicator's expiration date is set using the greatest expiration date between the two sources. In this example, the new expiration date will be 10/17 (15 days from when it was reported by Source B). 3. When the date switches from 10/17 to 10/18, this indicator is queued to have its status changed to **Expired**.

Indicator Scoring

Indicator scoring allows you to apply weighting to indicators and their contextual information, such as sources, attributes, and indicator types, as they are added to ThreatQ. Indicator scoring allows you to set manual scores or you can rely on ThreatQ's scoring algorithm to

calculate scores. After scores are calculated, you can change the score as desired to your custom value or accept the calculated value.

Related Topics:

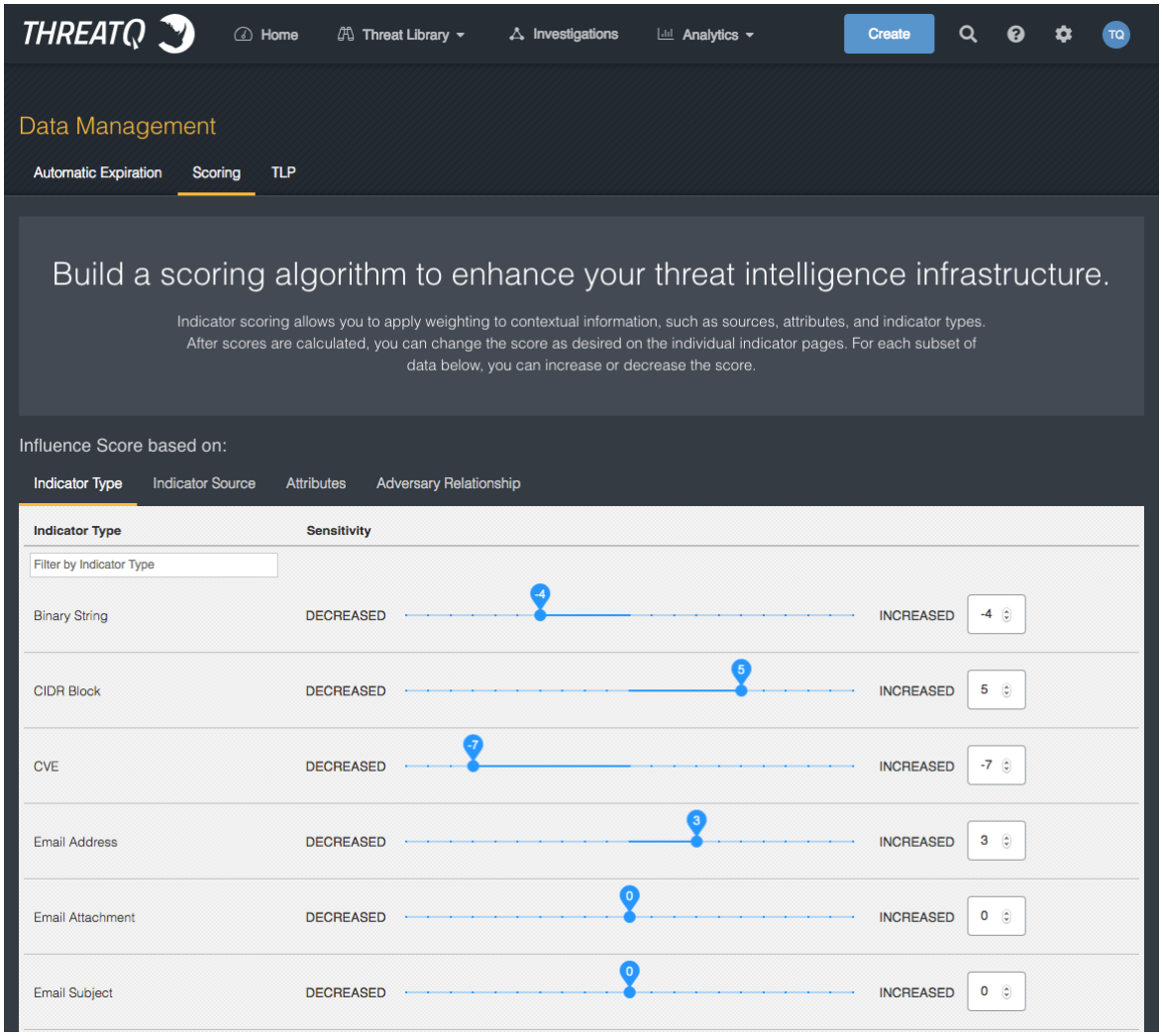
- Configure Indicator Scoring
- Building a Scoring Algorithm
- Overriding the Scoring Algorithm with a Manual Score

Configure Indicator Scoring

1. From the navigation menu, click on settings icon and select **Data Management**.

   The Data Management page will open with the Automatic Expiration tab selected by default.

2. Click on the **Scoring** tab.

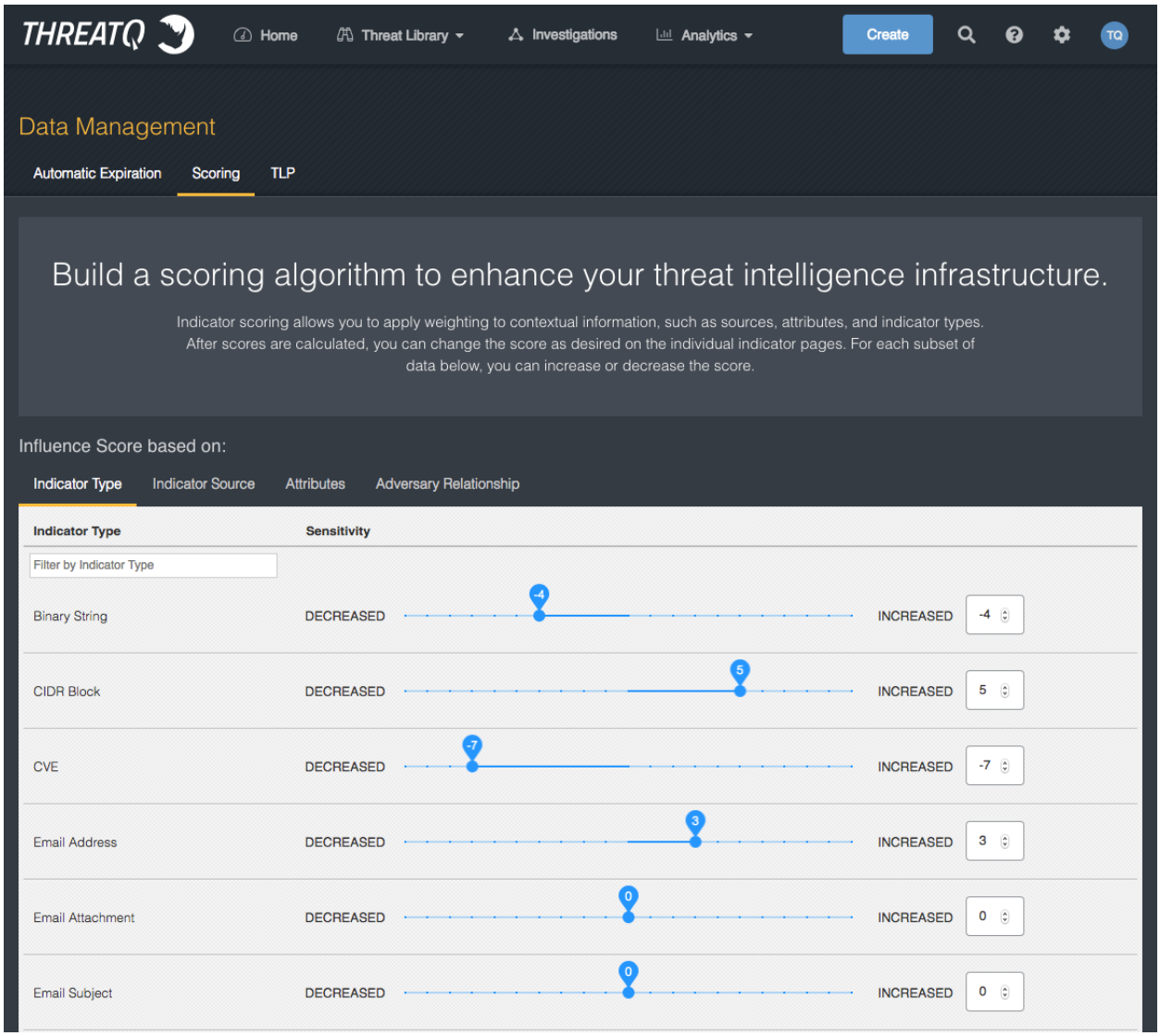


Building a Scoring Algorithm

As you build a scoring algorithm, you influence indicator scores based on the following criteria:

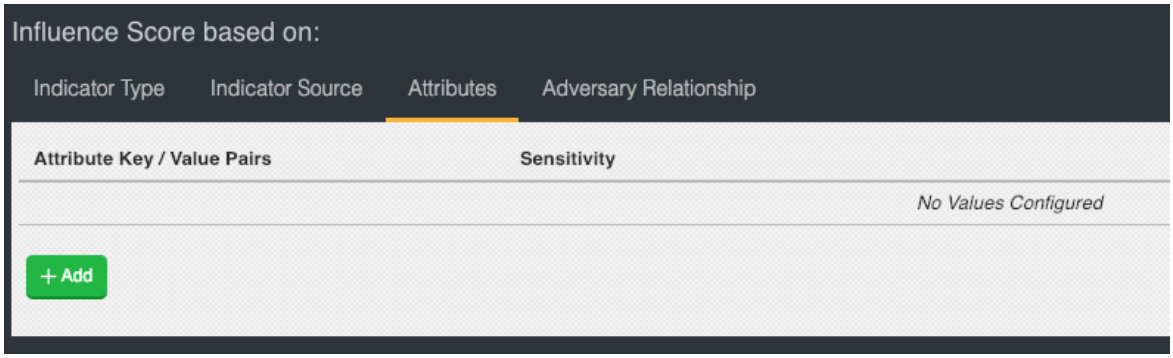
- Indicator Type
- Indicator Source
- Attributes
- Adversary Relationship

Use the slider to determine the sensitivity of the criterion you select. By default, the slider is positioned in neutral position, which in isolation produces an indicator score of zero. You may increase the score up to 10, which creates a score of **Very High**. You may also decrease the score, which creates a score of **Very Low**.



Influencing Score Based on Attributes

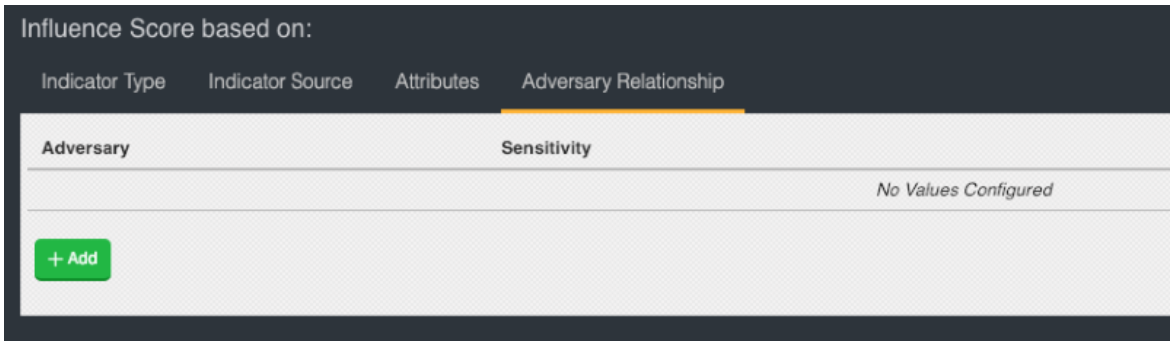
1. Navigate to the Attributes category under Scoring.



2. Click **Add**
3. Designate an **Attribute Key** / **Value Pair**
4. Adjust the sensitivity using the slider.
5. Click **Save**.

Influencing Score based on Adversary Relationship

1. Navigate to the Adversary category under Scoring.

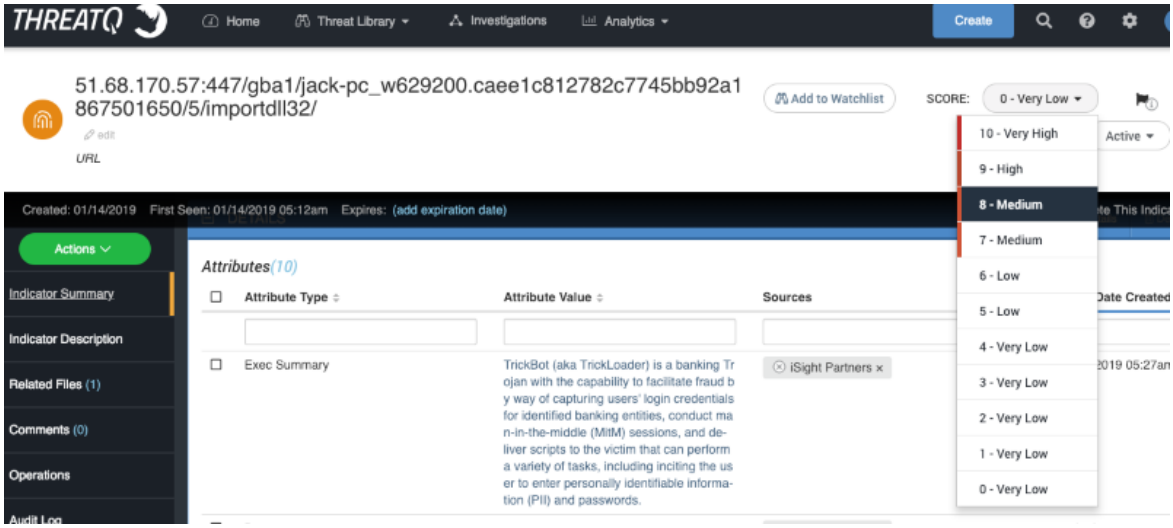


2. Click **Add**
3. Select an **Adversary**.
4. Adjust the sensitivity using the slider.
5. Click **Save**.

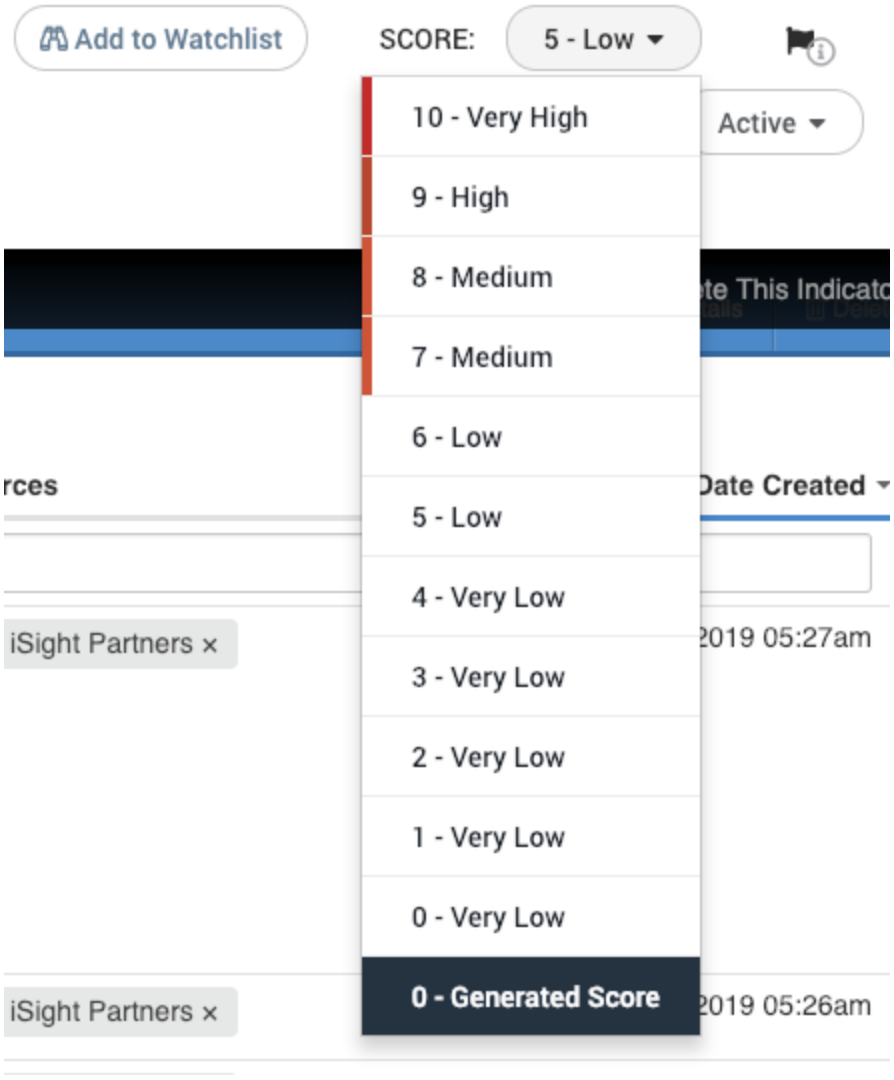
Overriding the Scoring Algorithm with a Manual Score

Setting a manual Indicator Score:

1. Navigate to an Indicator's Details page.
2. Click the **Score** dropdown and select a score.



Optionally, you may revert to the calculated score by clicking on the Score dropdown and selecting **Generated Score**.



Whitelisted Indicators

There are some indicators that should be considered to be whitelisted, or non-malicious, and we do not want those indicators going out to other systems. For example, a company's own domain name would never need to be blocked.

The whitelisting process creates rules that apply to particular indicators, so that when those indicators come in in the future, they will be automatically whitelisted.

Within this section, the following options are available:

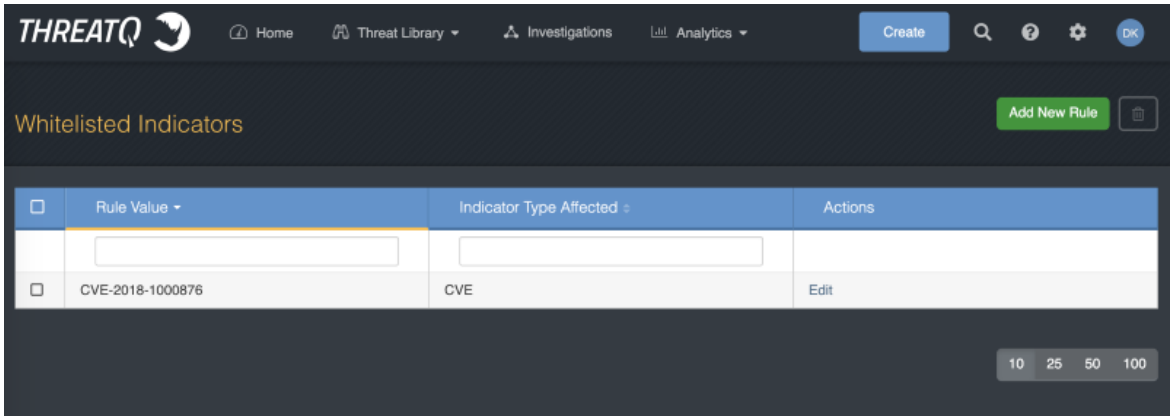
- Viewing Existing Whitelist Rules
- Creating a Whitelist Rule
- Editing a Whitelist Rule
- Removing a Whitelist Rule

Viewing Existing Whitelist Rules

To view existing whitelist rules:

1. Click on the settings icon and select **Whitelisted Indicators**

   The Whitelist Rules page opens. Existing whitelist rules are listed in the Whitelist Rules table.



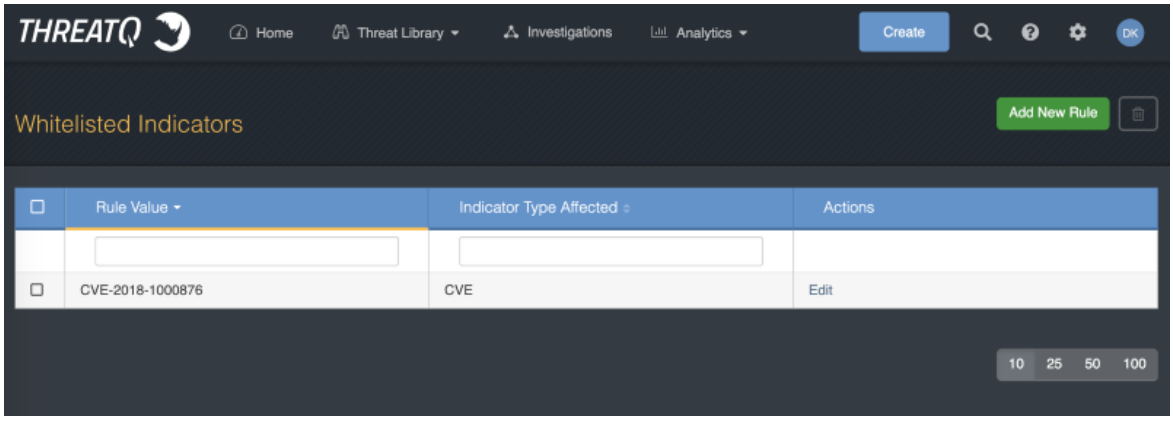
Creating a Whitelist Rule

The process of creating a whitelist rule is almost exclusively available via the Tools menu. However, it is important to note that whitelisting a CIDR Block indicator also creates a whitelist rule.

To create a whitelist rule:

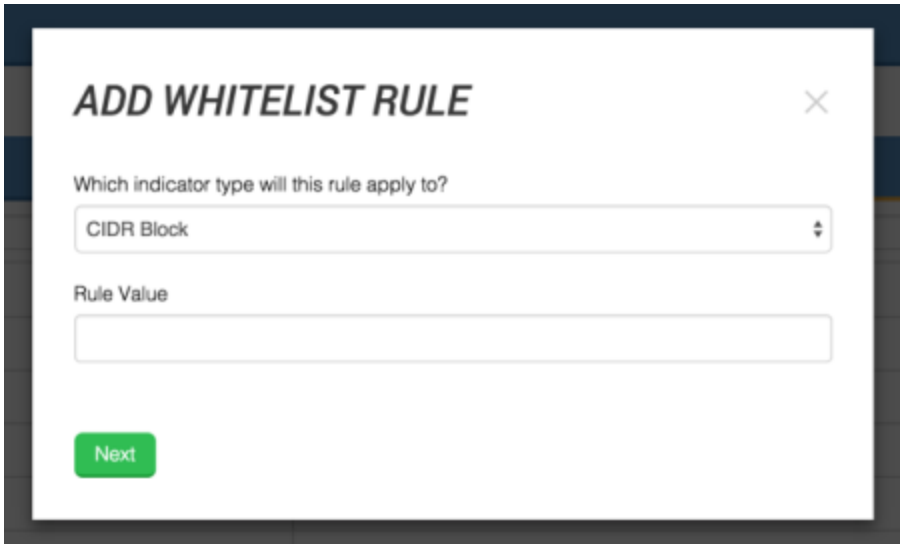
1. Click on the settings icon and select **Whitelisted Indicators**.

   The Whitelist Rules page opens.



2. Click **Add Rule**.

   The Add Whitelist Rules page opens.



3. Select the Indicator type the rule will apply to.
4. Add a Rule Value.
5. Click **Next**.

Affected indicators are listed in the dialog box.

6. Review the affected indicators to determine if you are satisfied with the rule.

> The rule has not been applied yet, so you still have time to edit it based on whether you are satisfied with how it affects the indicators.

7. Click **Continue Editing this Rule**.
8. If you are satisfied with the rule, click **Add Rule**.

The rule is applied to existing indicators, and it is entered into the Whitelist Rules table.

Any new indicators will also have the rule applied to them as they enter the system.

Editing a Whitelist Rule

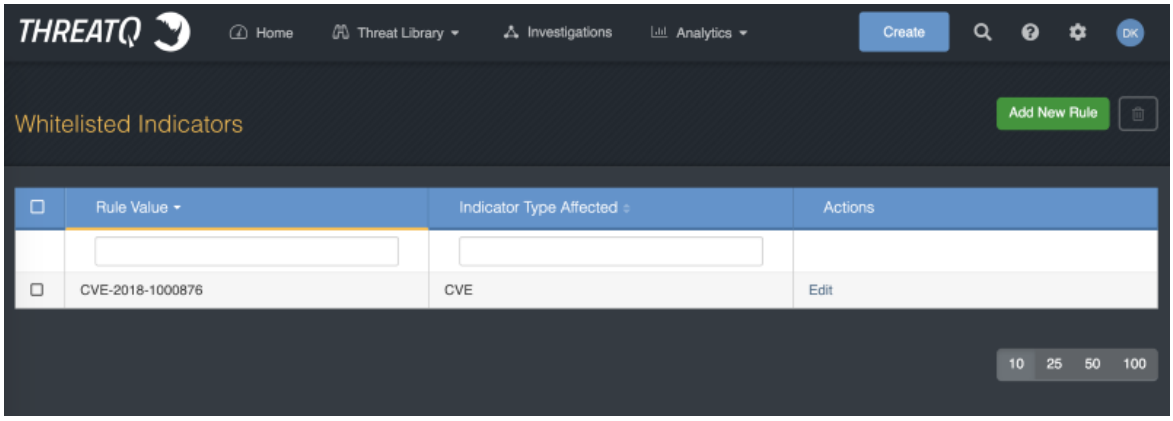
> **Important:** Editing a whitelist rule will not undo any changes the rule had made prior to being edited.

To edit a whitelist rule:

1. Click on the settings icon

and select **Whitelisted Indicators**.

The Whitelist Rules page opens.



2. In the Whitelist Rules table, locate the rule you wish to edit.
3. Click **Edit**.

The Edit Whitelist Rule dialog box opens.

4. Make the desired edits and click **Next**.

   Affected indicators are listed in the dialog box.

5. Review the affected indicators to determine if you are satisfied with the rule.

   The rule has not been applied yet, so you still have time to edit it based on whether you are satisfied with how it affects the indicators.

6. If you are satisfied, click **Edit Rule**.

   The rule is applied to existing indicators, and it is updated in the Whitelist Rules table.

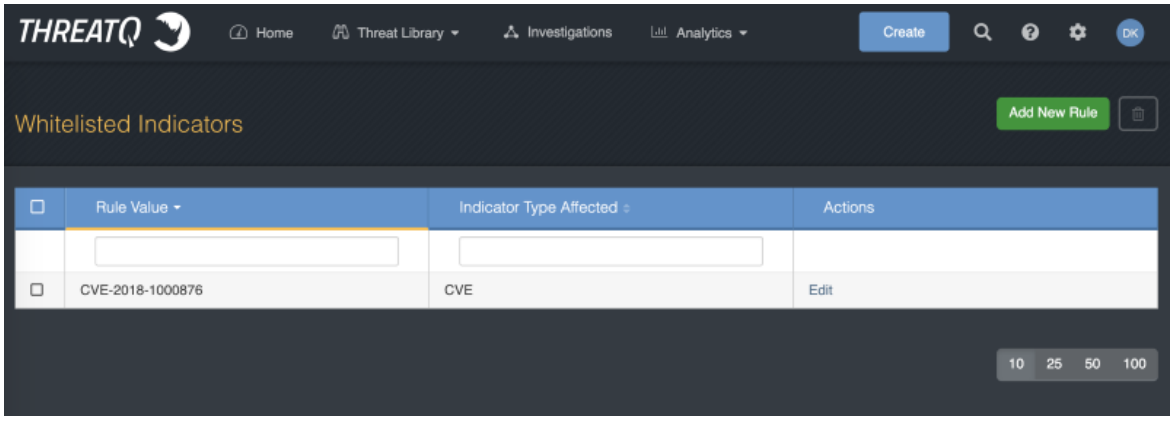
   Any new indicators will also have the rule applied to them as they enter the system.

Removing a Whitelist Rule

To remove a whitelist rule:

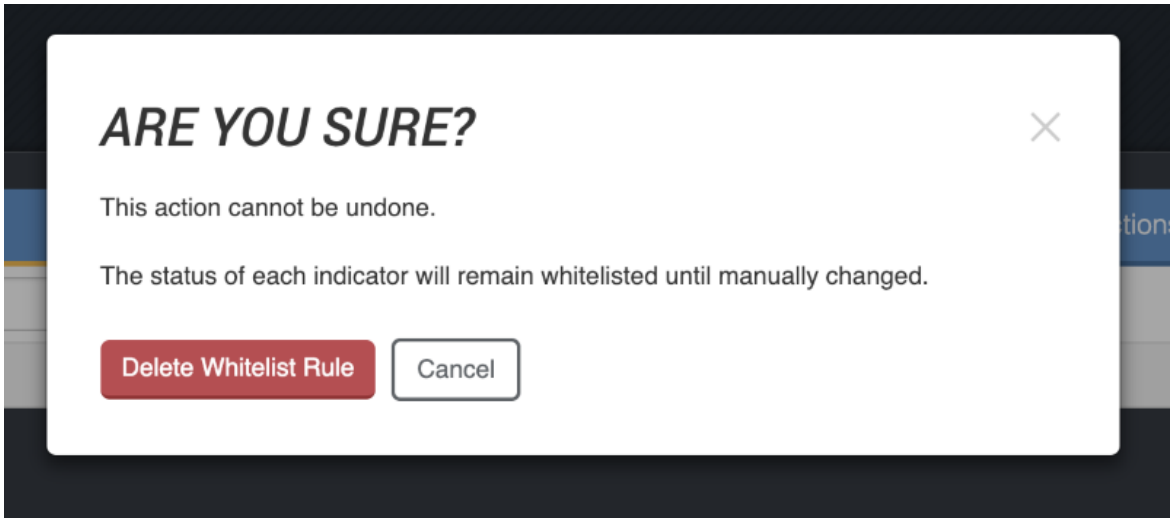
1. Click on the settings icon and select **Whitelisted Indicators**.

   The Whitelist Rules page opens.



2. Locate and select the rule(s) from the table that you wish to remove.
3. Click on the delete Icon .

   A confirmation dialog box opens, asking if you are sure.



4. Click **Delete Whitelist Rule**.

   The rule is deleted and a confirmation alert appears in an alert bar at the top of the page.

Indicator URL Normalization

Remove Quotes from the Beginning and/or End of an Indicator

Single and double quote characters are removed if they are the first or last character of an indicator.

Remove Unneeded Spaces found within an Indicator

All spaces irrelevant of their position in the Indicator value are removed (when applicable).

Adjust leading protocol from indicators

Indicators with a leading protocol [http://, https://, ftp://, or ftps://] are extracted and included as an attribute. When applicable, this indicator adjustment could change the indicator type from URL to FQDN.

Example: Original URL indicator of http://evilsubdomain.no-ip.biz/ would convert to a FQDN = evildomain.no-ip.biz.

Adjust the Port from an IP Address

An IP address with a port [ex. 199.7.136.88:8143] will be truncated to the IP address and the port assignment will be added as an attribute.

Using the previous example the following indicator/attribute will be created:

Field	Value
URL	199.7.136.88
Attribute > Port	8143

Adjust Defanged/Neutered Indicators

Indicators that have been defanged/neutered in order to “safely” share them (i.e. www [dot] 3322 [dot] org or badguy [at] gmail.com) need to be adjusted during import in order to ensure the indicators are properly deployed.

Create an IP Address from a URL (when applicable)

Using the previous example the following indicators will be created:

Field	Value
URL	51.255.131.66/civis/viewforum.php
IP Address	51.255.131.66

Create a FQDN from a URL (when applicable)

When a URL contains a domain [ex. bat99-11611.co/gate777.php] a second indicator will be created for the domain [bat99-11611.co].

Using the previous example, the following indicators will be created:

Field	Value
URL	bat99-11611.co/g-ate777.php
FQDN	bat99-11611.co

Extract HTTP Parameters from a URL Indicator

HTTP parameters [chained.j3oil-gasinc.net/civis/viewforum.php?keywords=9obo&fid0=c27] are important but can significantly limit pattern-matching detection capabilities due to the likelihood of parameter deviations, as well as, hamper the volume of URL indicators being deployed. To increase the probability of detection the http parameters are extracted and created as attributes.

In this example:

Field	Value
URL IOC	chained.j3oilgasinc.net/civis/viewforum.php
Attribute = HTTP Parameter = keywords	9obo&fid0=c27

Maintain "WWW" on FQDN Indicators

When parsing or importing a FQDN the "www" will be maintained.

Replace and/or Remove Special Characters

Character	Replacement
ASCII Values < 32 ASCII Values > 127	<space>
Ascii 96	-
Ascii145	'
Ascii146	'
Ascii147	"
Ascii148	"
Ascii151	-
carriage return and line feed	<space>
Control Characters	Remove
Convert to UTF8	
Remove leading and trailing space, tab, newline, carriage return, vertical tabs and null characters.	

Supported Defanging Techniques

The table below lists all supported indicator defanging techniques.

[.]	=>	.

[dot]	=>	.
(dot)	=>	.
[d]	=>	.
-dot-	=>	.
dot	=>	.
hxxp://	=>	http://
hxxx://	=>	http://
hxxps://	=>	https://
hxxxs://	=>	https://
[hxxp]	=>	http
hxtp://	=>	http://
htxp://	=>	http://
hxtps://	=>	https://
htxps://	=>	https://
[http]	=>	http
[http://]	=>	http://

[https]	=>	https
[https://]	=>	https://
[at]	=>	@
-at-	=>	@
_at_	=>	@
-@-	=>	@
_@_	=>	@
[@]	=>	@
[www]	=>	www

Signatures

ThreatQ allows you to ingest and manage Signatures, such as Snort and OpenIOC. While importing, ThreatQ parses the signature file for Indicators to add. Once signatures are included in your deployment, you can add contextual information and correlate them with Indicators, Events, Adversaries, and Files.

Related Topics:

- Signatures Management Page
- Adding a Signature
- Adding a Yara Signature

Signatures Management Page

The Signatures Overview page displays all signatures in the platform. For each signature, the table displays the Date Created, Signature Type, and Signature Title.

You can filter the table based on criteria to view specific signatures. For each signature, you can click to view expanded details.

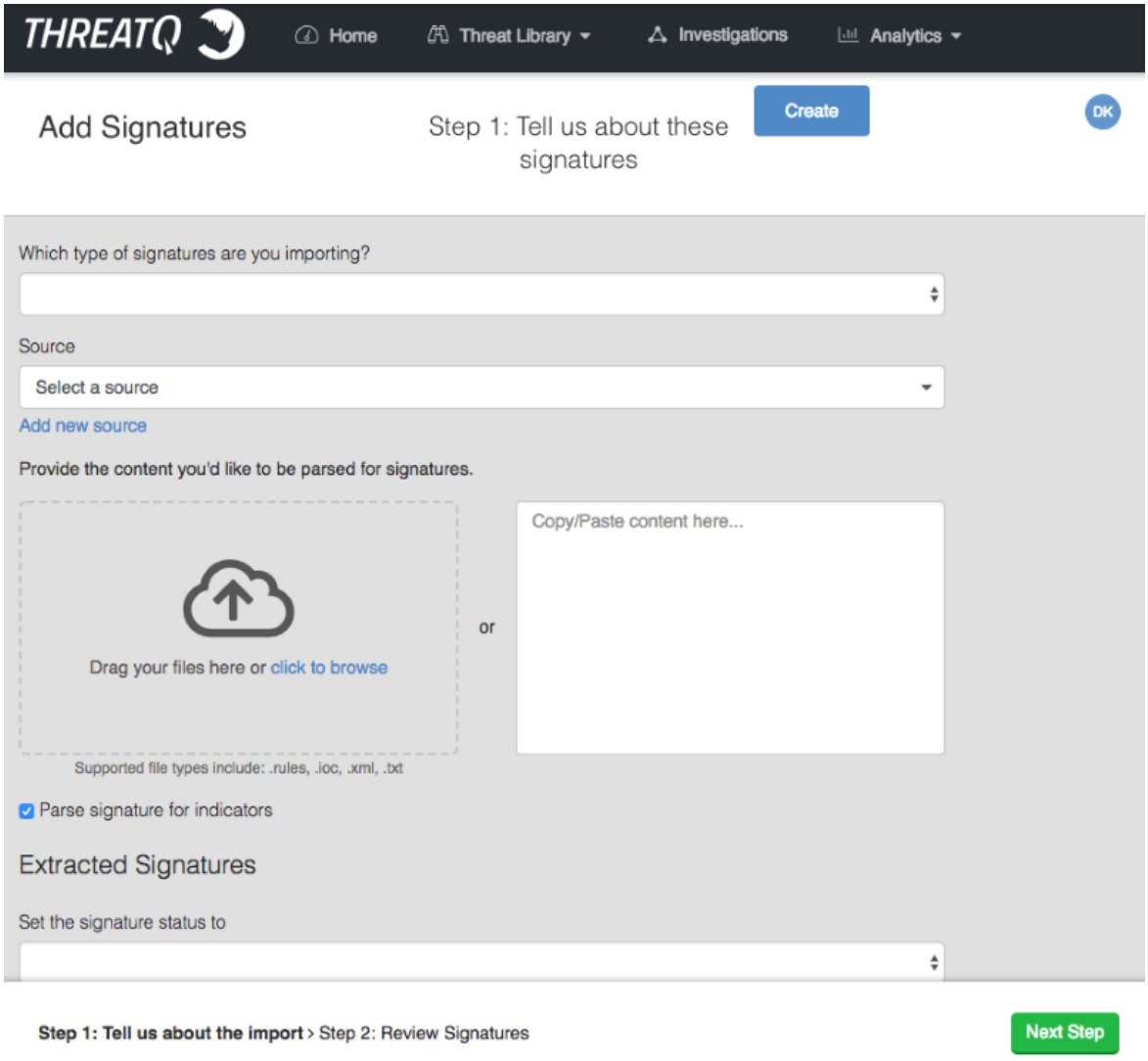
From the Signatures Overview page, you can do the following:

- View all signatures in the platform and details for each signature
- Filter signatures by Date Created, Signature Type, and Signature Title
- Add new signatures

Adding a Signature

To add a Signature:

1. From the main menu, choose **Create > Signature**.



The Add Signatures dialog box opens.

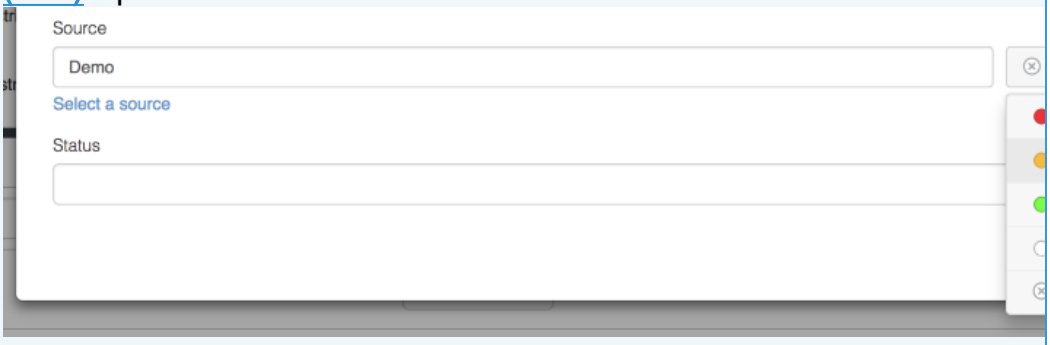
2. Choose the type of signature from the drop-down .

> For Yara, see Adding a Yara Signature.

3. Select a **Source** from the dropdown provided.

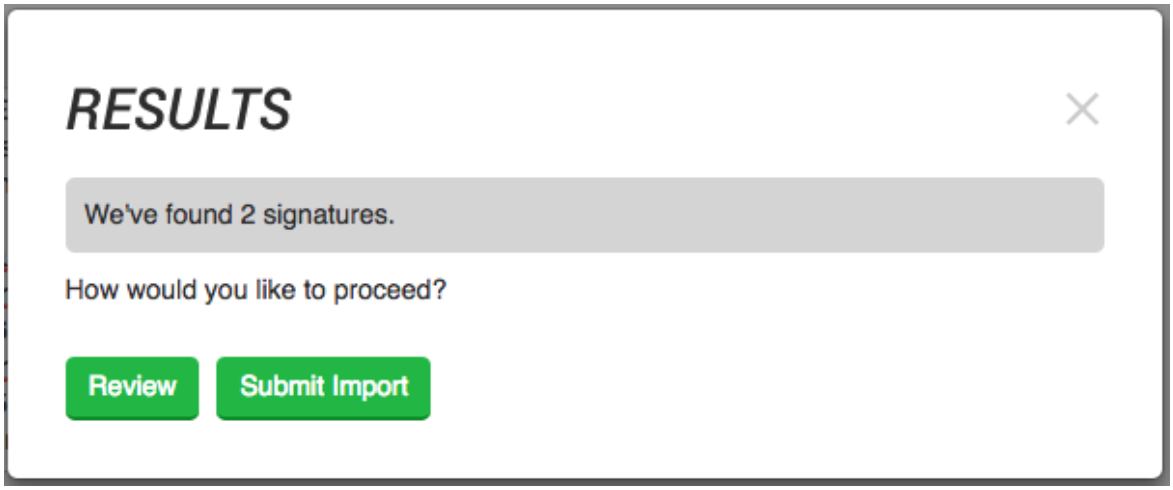
> You can also click on **Add a New Source** if the desired source is not

listed in the dropdown list . If administrators have enabled TLP view settings, users can select a TLP classification light for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP classifications.



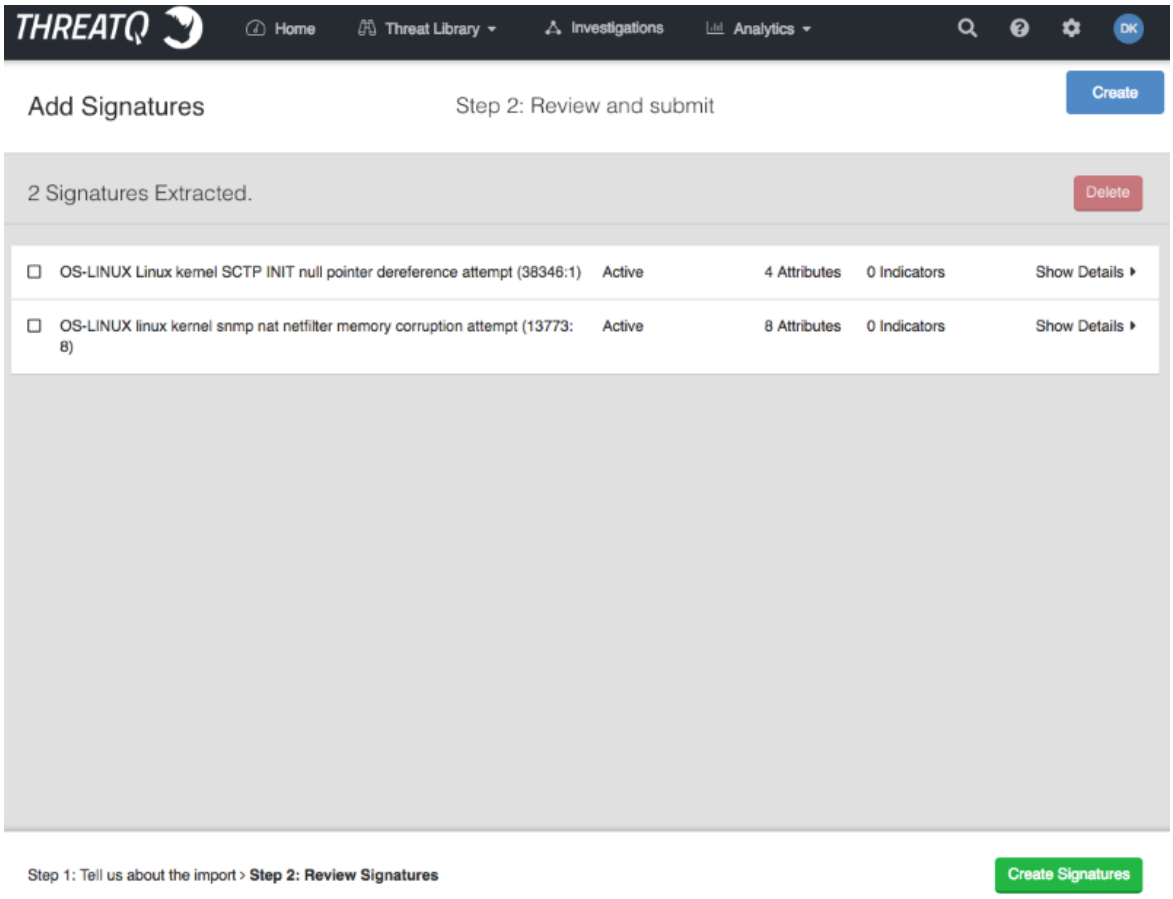
5. Do one of the following:
   - Drag your file(s) into the left pane.
   - Click **click to browse**, and locate the file you wish to upload.
   - Copy/paste content into the right pane.
6. Optionally, select to parse the signature for indicators.
7. Choose a **Signature Status** from the drop-down menu.
8. Optionally, **Apply attributes to all extracted signatures**:
   - Select an **Attribute Type**.
   - Enter an **Attribute Value**.
   - Enter an **Attribute Source**.
   - Optionally, click the Add icon for additional attributes.
9. Optionally, relate the signature to another object by entering the object in the **Relate signatures to another object** field.

10. Click **Next Step**.



If signatures are discovered, the Results dialog box appears.

11. You can either select **Submit Import** to finish adding the signatures or **Review** to customize what data is imported.



If you selected to review signatures, the Add Signatures Step 2: Review page

loads.

12. Select one or more signatures and click **Delete**.
13. Click on **Show Details** for a signature to review individual items in a signature. Use the checkboxes to select unwanted signature items and click **Delete**.

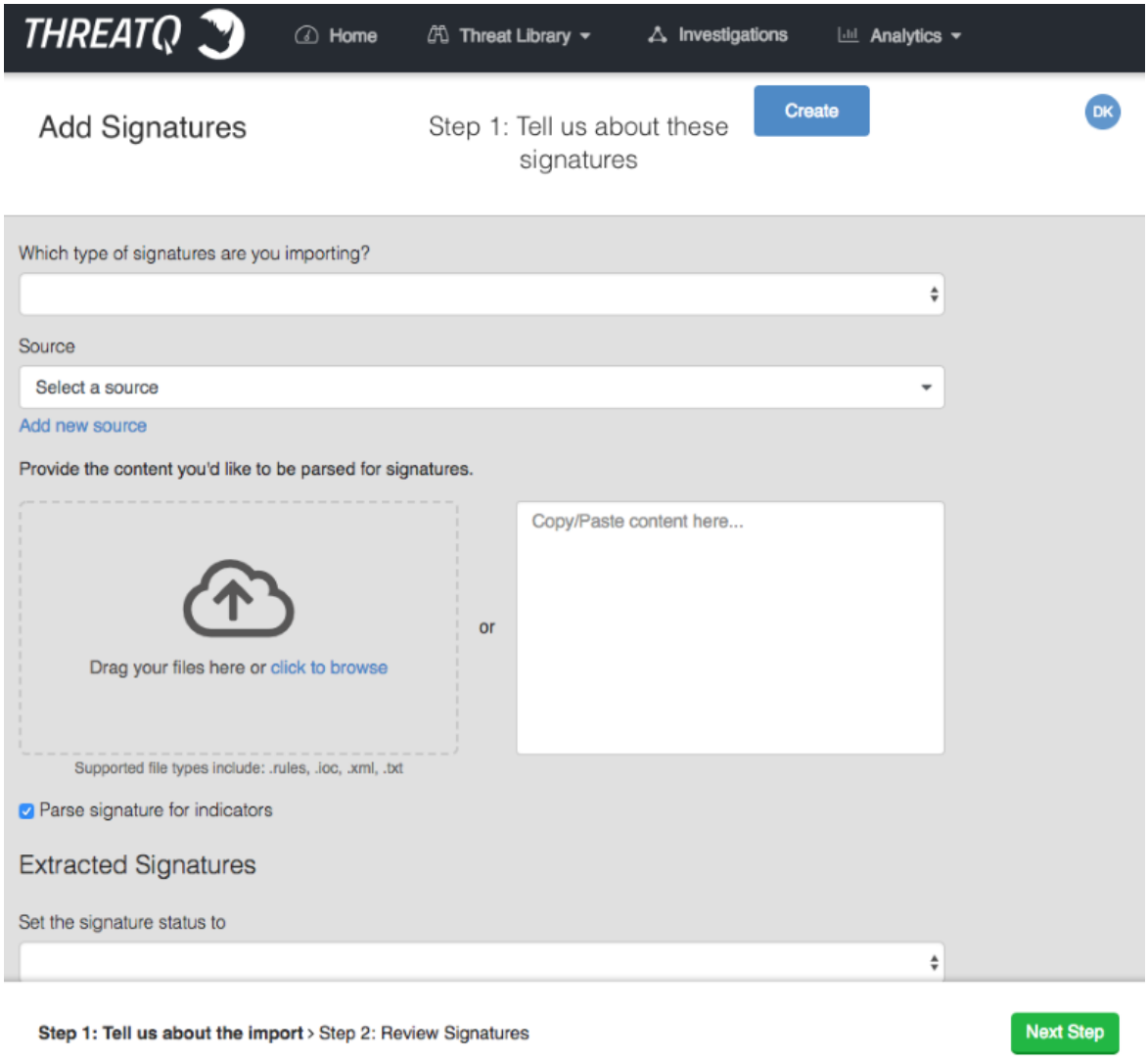
A warning dialog box appears.

14. Click **Delete** to remove the unwanted items.
15. Click **Create Signatures** when finished.

Adding a Yara Signature

To add a Signature:

1. From the main menu, choose **Create > Signature**.

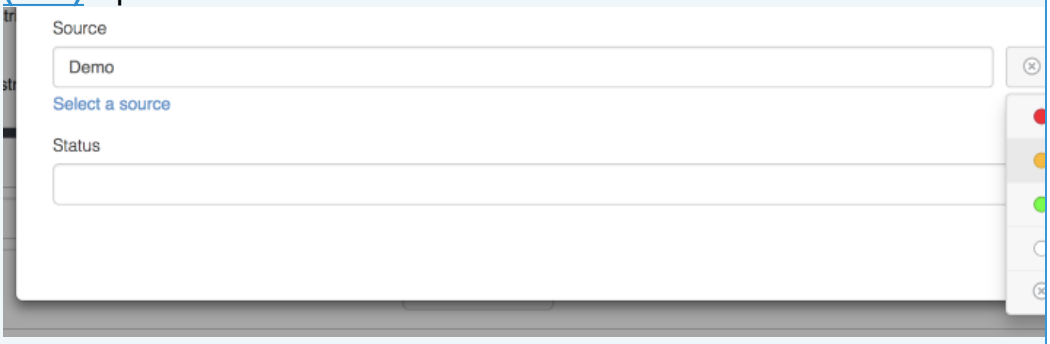


The Add Signatures dialog box opens.

2. Select **Yara** as the type of signature from the drop-down .
3. Select a **Source** from the dropdown provided.

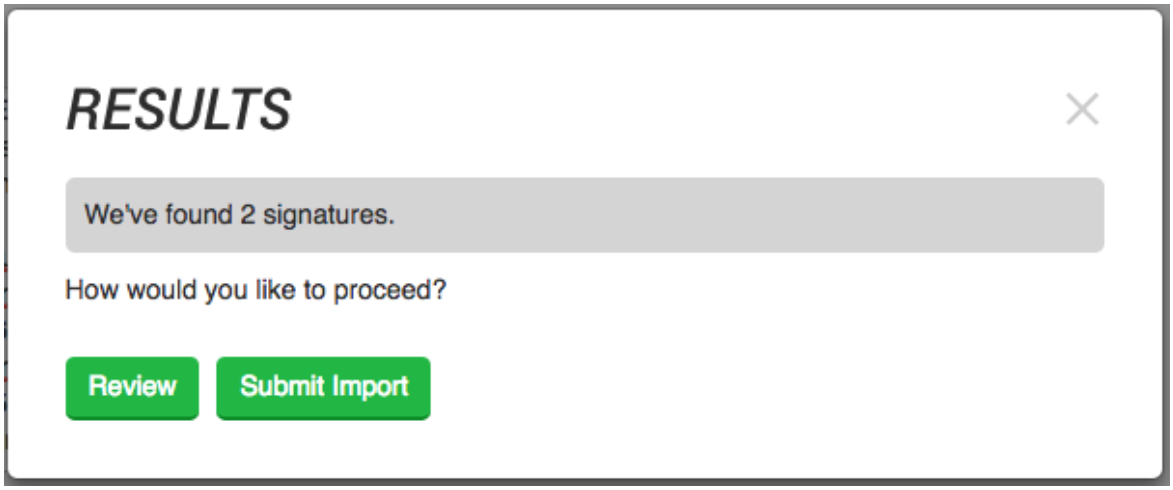
> You can also click on **Add a New Source** if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, users can select a TLP classification light for the new

source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP classifications.



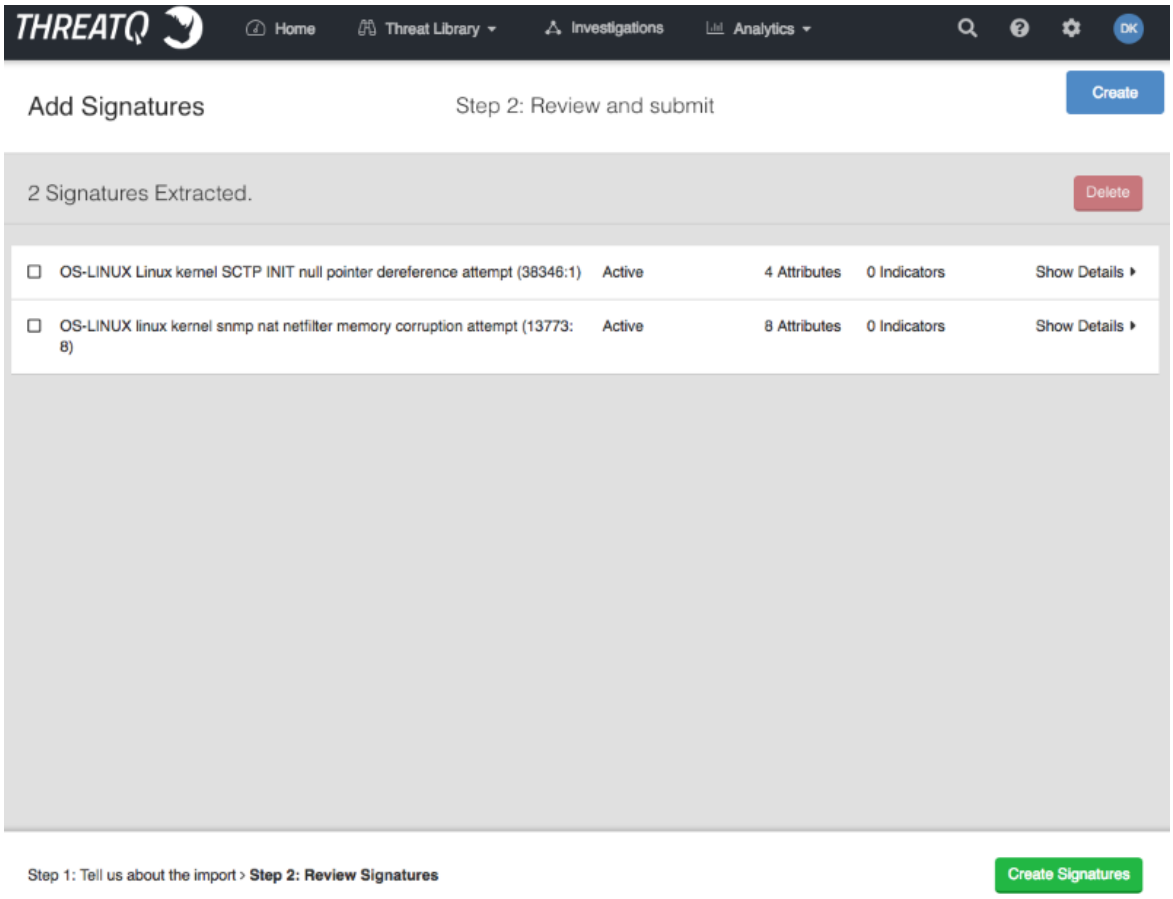
5. Do one of the following:
   - Drag your file(s) into the left pane.
   - Click **click to browse**, and locate the file you wish to upload.
   - Copy/paste content into the right pane.
6. Optionally, select to parse the signature for indicators.
7. Determine the method to use if multiple signatures are discovered:
   - Save independently as unique signatures
   - Save as a single signature
8. Choose a **Signature Status** from the drop-down menu.
9. Optionally, **Apply attributes to all extracted signatures**:
   - Select an **Attribute Type**.
   - Enter an **Attribute Value**.
   - Enter an **Attribute Source**.
   - Optionally, click the Add icon for additional attributes.
10. Optionally, relate the signature to another object by entering the object in the **Relate signatures to another object** field.

11. Click **Next Step**.



If signatures are discovered, the Results dialog box appears.

12. You can either select **Submit Import** to finish adding the signatures or **Review** to customize what data is imported.



If you selected to review signatures, the Add Signatures Step 2: Review page

loads.

13. Select one or more signatures and click **Delete**.
14. Click on **Show Details** for a signature to review individual items in a signature. Use the checkboxes to select unwanted signature items and click **Delete**.

A warning dialog box appears.

15. Click **Delete** to remove the unwanted items.
16. Click **Create Signatures** when finished..

STIX

The following describes how to use STIX in ThreatQ:

- STIX Overview
- ThreatQ STIX Object Types
- STIX Data Mapping
- Parsing a STIX File for Indicators

STIX Overview

ThreatQ allows you to ingest and manage STIX files. You can ingest STIX data in two ways:

- You can set up a STIX/TAXII Feed, as described in STIX/Taxii Feeds.
- You can upload a STIX file or insert STIX data to parse for indicators, as described in Parsing a STIX File for Indicators.

ThreatQ supports STIX 1.1.1 and STIX 1.2.

Related Topics

- STIX Data Mapping
- ThreatQ STIX Object Types

ThreatQ STIX Object Types

STIX integration provides ThreatQ with the following additional object types.

- Campaigns
- Courses of Action
- Exploit Targets
- Incidents
- TTP objects

These objects enable better understanding and communication of STIX data. STIX data will be mapped to these objects and existing objects in the system.

STIX Data Mapping

The following sections display how STIX data becomes mapped to indicator objects and attributes in ThreatQ.

- STIX Threat Actors Mapping
- STIX Indicators Mapping
- STIX Exploit Targets Mapping
- STIX Observables Mapping
- STIX Campaigns Mapping
- STIX Courses of Action Mapping
- STIX Incidents Mapping
- STIX TTP Mapping
- STIX CIQ Identity Mapping

STIX Threat Actors Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Identity	Adversary.value	
ID	Adversary.attribute	STIX Reference ID
Title	Adversary.value	
Type	Adversary.attribute	Type
Timestamp	Adversary.published_at	
Description	Adversary.attribute	Description
Motivation	Adversary.attribute	Motivation
Sophistication	Adversary.attribute	Sophistication
Intended_Effect	Adversary.attribute	Intended Effect
Role	Adversary.attribute	Role
Confidence	Adversary.attribute	Confidence
Handling	Adversary.tlp	
Observed_TTPs	TTP	
Associated_Actors	Adversary	
Associated_Campaigns	Campaign	

Related Topics

- STIX Data Mapping
- STIX Threat Actors Mapping
- STIX Indicators Mapping

- STIX Exploit Targets Mapping
- STIX Observables Mapping
- STIX Courses of Action Mapping
- STIX Incidents Mapping
- STIX TTP Mapping
- STIX CIQ Identity Mapping

STIX Indicators Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Title	Indicator.attribute	Indicator Title
ID	Indicator.attribute	STIX Reference ID
Timestamp	Indicator.published_at	
Type	Indicator.attribute	Indicator Type
Description	Indicator.attribute	Description
Short Description	Indicator.attribute	Short Description
Producer	Indicator.source	
Observable	Indicator	
Indicated_TTP	TTP	
Kill_Chain_Phases	Indicator.attribute	Kill Chain Phase
Likely_Impact	Indicator.attribute	Likely Impact
Suggested_COAs	Course of Action	
Handling	Indicator.tlp	
Confidence	Indicator.attribute	Confidence

STIX Field	ThreatQ Field Mapping	ThreatQ Name
	Indicator.attribute.source	
Related_Observables		
Related_Indicators	Indicator	
Related_Campaigns	Campaign	
	Signature	
	Signature.type = "Snort"	
	Signature.value	
	Indicator.source	
	Course of Action	
	Indicator.attribute	Start Time
	Indicator.attribute	End Time
	Indicator.published_at	

Related Topics

- STIX Data Mapping
- STIX Indicators Mapping
- STIX Threat Actors Mapping
- STIX Exploit Targets Mapping
- STIX Observables Mapping
- STIX Courses of Action Mapping
- STIX Incidents Mapping

- STIX TTP Mapping
- STIX CIQ Identity Mapping

STIX Exploit Targets Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Title	Exploit Target.value	
ID	Exploit Target.attribute	STIX Reference ID
Description	Exploit Target.attribute	Description
Short Description	Exploit Target.attribute	Short Description
Weakness	Exploit Target.attribute	CWE ID
Weakness	Exploit Target.attribute	Weakness Description
Configuration	Exploit Target.attribute	CCE ID
Configuration	Exploit Target.attribute	Configuration Description
Configuration	Exploit Target.attribute	Configuration Short Description
Vulnerability	Exploit Target.attribute	CVE ID
Potential_COAs	Course of Action	
Related_Exploit_Targets	Exploit Target	

Related Topics

- STIX Data Mapping
- STIX Exploit Targets Mapping
- STIX Threat Actors Mapping
- STIX Indicators Mapping
- STIX Observables Mapping

- STIX Courses of Action Mapping
- STIX Incidents Mapping
- STIX TTP Mapping
- STIX CIQ Identity Mapping

STIX Observables Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
ID	Indicator.attribute	STIX Reference ID
	Indicator.attribute	Description
	Indicator.type	IP Address
	Indicator.value	
	Indicator.type	Filename
	Indicator.value	
	Indicator.type	File Path
	Indicator.value	
	Indicator.attribute	File Size
	Indicator.attribute	File Format
	Indicator.attribute	Packer
	Indicator.type	MD5
	Indicator.type	SHA-256
	Indicator.type	SHA-1
	Indicator.type	SHA-512

STIX Field	ThreatQ Field Mapping	ThreatQ Name
	Indicator.value	
	Indicator.type	SSDEEP
	Indicator.value	
	Indicator.type	FQDN
	Indicator.value	
	Indicator.type	URL
	Indicator.value	
	Indicator.type	Email Subject
	Indicator.value	
	Indicator.type	Email Address
	Indicator.value	
	Indicator.type	IP Address
	Indicator.value	
	Indicator.type	User-agent
	Indicator.value	
	Indicator.type	Filename
	Indicator.value	
	Indicator.type	Mutex
	Indicator.value	
	Indicator.attribute	Port

STIX Field	ThreatQ Field Mapping	ThreatQ Name
	Indicator.attribute	Protocol
	Object.Description	
	Spearphish.value	
	Indicator.type	Registry Key
	Indicator.value	
	Indicator.attribute	Hive

Related Topics

- STIX Data Mapping
- STIX Observables Mapping
- STIX Threat Actors Mapping
- STIX Indicators Mapping
- STIX Exploit Targets Mapping
- STIX Courses of Action Mapping
- STIX Incidents Mapping
- STIX TTP Mapping
- STIX CIQ Identity Mapping

STIX Campaigns Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Title	Campaign.value	
ID	Campaign.attribute	STIX Reference ID
Description	Campaign.attribute	Description

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Short Description	Campaign.attribute	Short Description
Timestamp	Campaign.started_at	
Names	Campaign.attribute	Alias
Status	Campaign.attribute	Status
Intended_Effect	Campaign.attribute	Intended Effect
Confidence	Campaign.attribute	Confidence
Activity	Campaign.attribute	Activity
Related TTPs	TTP	
Related Incidents	Incident	
Attribution	Adversary	
Associated_Campaigns	Campaign	

Related Topics

- STIX Data Mapping
- STIX Threat Actors Mapping
- STIX Indicators Mapping
- STIX Exploit Targets Mapping
- STIX Observables Mapping
- STIX Courses of Action Mapping
- STIX Incidents Mapping
- STIX TTP Mapping
- STIX CIQ Identity Mapping

STIX Courses of Action Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Title	Course of Action.value	
ID	Course of Action.attribute	STIX Reference ID
Description	Course of Action.attribute	Description
Stage	Course of Action.attribute	Stage
Objective	Course of Action.attribute	Objective
Objective Confidence	Course of Action.attribute	Objective Confidence
Type	Course of Action.attribute	Type
Short Description	Course of Action.attribute	Short Description
Parameter_Observables	Indicator	
Impact	Course of Action.attribute	Impact
Cost	Course of Action.attribute	Cost
Efficacy	Course of Action.attribute	Efficacy
Related_COAs	Course of Action	

Related Topics

- STIX Data Mapping
- STIX Courses of Action Mapping
- STIX Threat Actors Mapping
- STIX Indicators Mapping
- STIX Exploit Targets Mapping
- STIX Observables Mapping

- STIX Incidents Mapping
- STIX TTP Mapping
- STIX CIQ Identity Mapping

STIX Incidents Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Title	Incident.value	
ID	Incident.attribute	STIX Reference ID
Timestamp	Incident.published_at	
Description	Incident.attribute	Description
Categories	Incident.attribute	Category
First Malicious Action	Incident.attribute	First Malicious Action
Initial_Compromise	Incident.attribute	Initial Compromise
First_Data_Exfiltration	Incident.attribute	First Data Exfiltration
Incident_Discovery	Incident.attribute	Incident Discovery
Incident_Opened	Incident.attribute	Incident Opened
Incident_Opened	Incident.started_at	
Containment_Achieved	Incident.attribute	Containment Achieved
Restoration_Achieved	Incident.attribute	Restoration Achieved
Incident_Reported	Incident.attribute	Incident Reported
Incident_Closed	Incident.attribute	Incident Closed
Incident_Closed		

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Coordinator	Incident.attribute	Coordinator
	Incident.attribute	Coordinator
Reporter	Incident.attribute	Reporter
	Incident.attribute	Reporter
Responder	Incident.attribute	Responder
	Incident.attribute	Responder
Victim	Incident.attribute	Victim
	Incident.attribute	Victim
Related Indicators	Indicator	
Related Observables	Indicator	
Leveraged_TTPs	TTP	
Intended_Effect	Incident.attribute	Intended Effect
COA_Requested	Course of Action	
COA_Taken	Course of Action	
Confidence	Incident.attribute	Confidence
Attributed_Threat_Actors	Adversary	
Discovery_Method	Incident.attribute	Discovery Method
Related_Incidents	Incident	

Related Topics

- STIX Data Mapping
- STIX Incidents Mapping
- STIX Threat Actors Mapping
- STIX Indicators Mapping
- STIX Exploit Targets Mapping
- STIX Observables Mapping
- STIX Courses of Action Mapping
- STIX TTP Mapping
- STIX CIQ Identity Mapping

STIX TTP Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Title	TTP.value	
ID	TTP.attribute	STIX Reference ID
Description	TTP.attribute	Description
Handling	TTP.tlp	
Kill_Chain_Phases	TTP.attribute	Kill Chain Phase
Intended_Effect	TTP.attribute	Intended Effect
	TTP.attribute	CAPEC ID
Behavior	TTP.attribute	Attack Pattern
	TTP.attribute	Attack Pattern Description
	TTP.attribute	Attack Pattern Short Description

STIX Field	ThreatQ Field Mapping	ThreatQ Name
	TTP.attribute	Malware Type
	TTP.attribute	Malware Name
	TTP.attribute	Malware Description
	TTP.attribute	Malware Short Description
	TTP.attribute	Malware Detection Vendor
	TTP.attribute	Malware Family
	TTP.attribute	Exploit
	TTP.attribute	Exploit Description
	TTP.attribute	Exploit Short Description
Exploit_Targets	Exploit Target	
Related_TTPs	TTP	
Resources	TTP.attribute	Tool
	TTP.attribute	Tool
	TTP.attribute	Tool Type
	TTP.attribute	Tool Description
	TTP.attribute	Tool Short Description
	TTP.attribute	Infrastructure Type
	TTP.attribute	Infrastructure
	TTP.attribute	Infrastructure Short Description
	TTP.attribute	Infrastructure Description

STIX Field	ThreatQ Field Mapping	ThreatQ Name
	Indicator	
	TTP.attribute	Persona
Victim Targeting	TTP.attribute	Victim Name
	TTP.attribute	Victim <CIQ Identity Name>
	TTP.attribute	Targeted Systems
	TTP.attribute	Targeted Information
	Indicator	

Related Topics

- STIX Data Mapping
- STIX TTP Mapping
- STIX Threat Actors Mapping
- STIX Indicators Mapping
- STIX Exploit Targets Mapping
- STIX Observables Mapping
- STIX Courses of Action Mapping
- STIX Incidents Mapping
- STIX CIQ Identity Mapping

STIX CIQ Identity Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Party Name	Object.attribute	Name
Organization Name	Object.attribute	Organization

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Industry Sector	Object.attribute	Industry
Nationality	Object.attribute	Nationality
Languages	Object.attribute	Language
Address	Object.attribute	Country
Email Address	Object.attribute	E-Mail Address
Chat Handle	Object.attribute	Chat Handle
Phone	Object.attribute	Phone

Related Topics

- STIX Data Mapping
- STIX CIQ Identity Mapping
- STIX Threat Actors Mapping
- STIX Indicators Mapping
- STIX Exploit Targets Mapping
- STIX Observables Mapping
- STIX Courses of Action Mapping
- STIX Incidents Mapping
- STIX TTP Mapping

Parsing a STIX File for Indicators

ThreatQ allows you to upload a STIX file or insert STIX data to parse. for indicators.

To parse a STIX file for indicators:

1. Click on the **Create** button, located at the top of the dashboard and select **STIX Parser** under the *Import* heading.

   The Parse For Intelligence dialog box will load.

2. Do one of the following:

   - Drag your file(s) into the left pane.
   - Click on **Click to Browse**, and locate the file you wish to upload.
   - Copy/paste the content in the right pane.

3. Select or clear the **Normalize URL Indicators** check box. See Indicator URL Normalization for more information.
4. Click **Next Step**.
5. Enter an optional **Name**.
6. Select a **Source** from the dropdown menu provided.

   You can also click on **Add a New Source** if the desired source is not listed in the dropdown menu

7. Select any optional **Attributes** to be applied.
8. Optionally, enter a comment.
9. Optionally, use the **Add relationships** search field to add object relationships.
10. Optionally, add any desired **Tags**.

If at any point, you wish to abandon the import, click **Cancel**.

11. Click **Apply**.

    New objects will become available in the Threat Library.

Object Details Page

You can click on an object within the ThreatQ application to access its details page. The Object Details page provides you with an in-depth look at an individual object. You can enter comments for others to view, link related objects, and view an audit log of all activity associated with the object.

Specific objects, such as Indicators, will display additional information such as the indicator's status, score, and expiration data.

Items marked with an * in the Object Details Legend indicate an option only available to specific object types.

Object Details Page Legend			
Header Section			
Number	**Field**	**Description**	**Reference**
1	Edit Object Link	The Edit link allows you to edit specific details about an object. Edit fields will differ based on the	• Editing Adversaries • Editing Events • Editing Files

Object Details Page Legend			
		type of object.	• Editing Indicators
2	Add to Watchlist	The Watchlist toggle button allows you to add and remove the object from the Watchlist widget.	• Configuring the Watchlist
3	Score Selection* *Applies to Indicator Object Types Only*	The Score Selection dropdown allows you to override an indicator's score set by the scoring algorithm.	• Overriding the Scoring Algorithm with a Manual Score
4	Scoring Influence* *Applies to Indicator Object Types Only*	You can click on the Flag icon to review the criteria utilized by the application's scoring algorithm to generate the Indicator's score.	• Configure Indicator Scoring • Building a Scoring Algorithm
5	Status* *Applies to Indicator Object Types Only*	The Status dropdown menu allows you to manually set the status of an indicator. Default statuses include: Active, Expired, Indirect, Review, and Whitelisted.	• Indicator Status
6	Expiration* *Applies to Indicator Object Types Only*	The Expire link allows you to set an expiration date for the indicator, protect from auto-expiration policies, and remove an existing set expiration date.	• Indicator Expiration • Automatic Expiration and Policies
7	Delete Object	The Delete icon allows you to delete the object.	• Deleting Adversaries • Deleting Events • Deleting Files • Deleting Indicators
Details Section			
Number	**Pane**	**Description**	**Reference**

Object Details Page Legend			
8	Details	The Details pane displays Attributes, Sources, and Tags associated with the object. You can Add, Edit, and Delete items found in this section.	• Details Panes
9	Description	The Description pane allows you to add general information about the Indicator.	• Description Pane
10	Related Objects	There are several different related panes depending on the types of objects linked to the object. You can use these panes to view and add/remove linked indicators, files, signatures, events, adversaries, tasks, and investigations.	• Related Panes
11	Comments	The Comments pane allows you to record comments about the object for other users to read and reference.	• Comments Pane
12	Operations	The Operations pane allows you to associate third-party attributes and related indicators to the indicator. **Note:** This options requires the installation of Operations. See the Operations Overview topic for more details.	• Operations Overview • ThreatQ Operations Development Guide
13	Audit Log	The Audit Log panel displays all actions and changes made to an Object.	• Common Enrichment and Audit Log Questions
Left-Hand Navigation			

Object Details Page Legend			
Number	**Field**	**Description**	**Reference**
14	Action Menu	The Actions menu allows you to execute the following actions for an object: • Add a New Attribute • Add a New Comment • Create a Task • Generate a Report • Add a Relationship • Add a Source	• Actions Menu
15	Details Navigation Tabs	This allows you to jump to a particular pane on the Object Details page.	N/A

Details Panes

The Details Pane section of the object details page displays attributes, sources, and tags associated with the system object.

Related Topics:

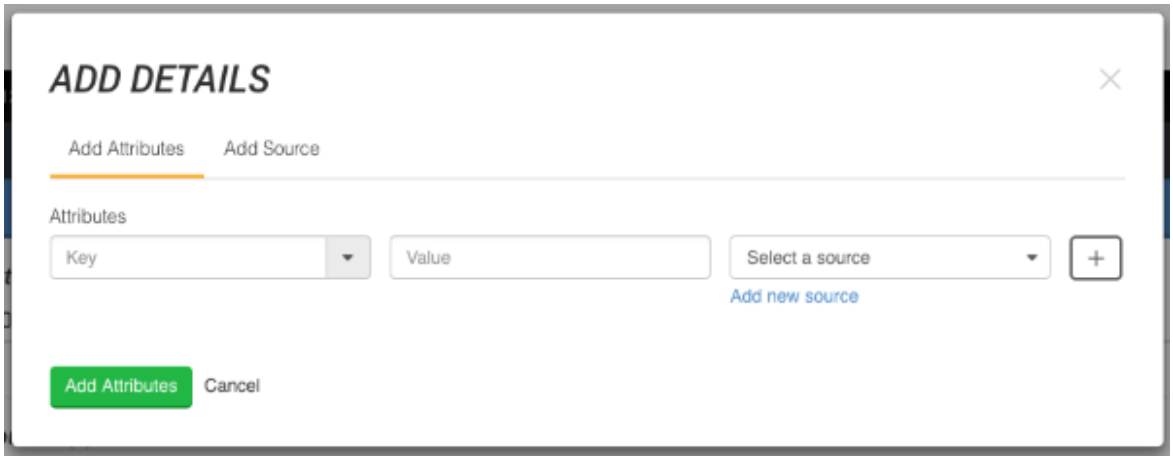
- Adding an Attribute to an Object
- Deleting an Attribute
- Deleting an Attribute Source
- Adding a Source to an Object
- Managing Tags

Adding an Attribute to an Object

You can link adversaries to a system object.

To add an attribute:

1. Locate the Details pane on the object details page.
2. Click on the **+ Add Details** link located to the top-right.



   The Add Details dialog box opens with the Add Attributes tab selected by default.
3. Select an **Attribute Type** from the Attributes dropdown and enter an **Attribute Value** and **Source**.

   You can select the **+** icon to add additional attributes.
4. Select **Add Attributes**.

Deleting an Attribute

You can delete an attribute from the object details page.

To delete an attribute:

1. Locate the Details pane on the object details page.
2. Select the checkbox next to the attribute to delete.

   You can select more than one attribute to delete

3. Select **Delete**.

The confirmation dialog box opens.

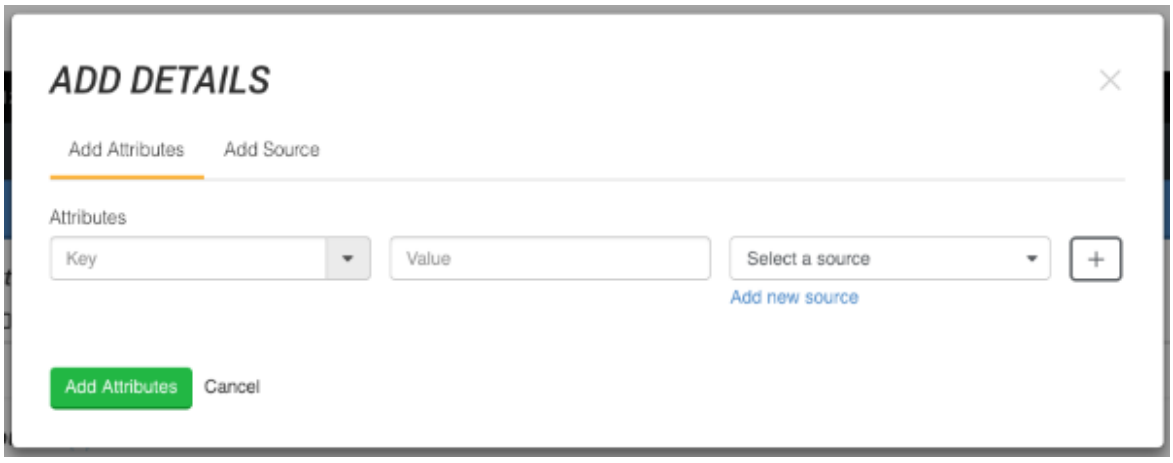
4. Select **Delete Attributes**.

Adding a Source to an Object

You can add sources to a system object in its details pane.

To add a source:

1. Locate the Details pane on the object details page.
2. Click on the **+ Add Details** link located to the top-right.

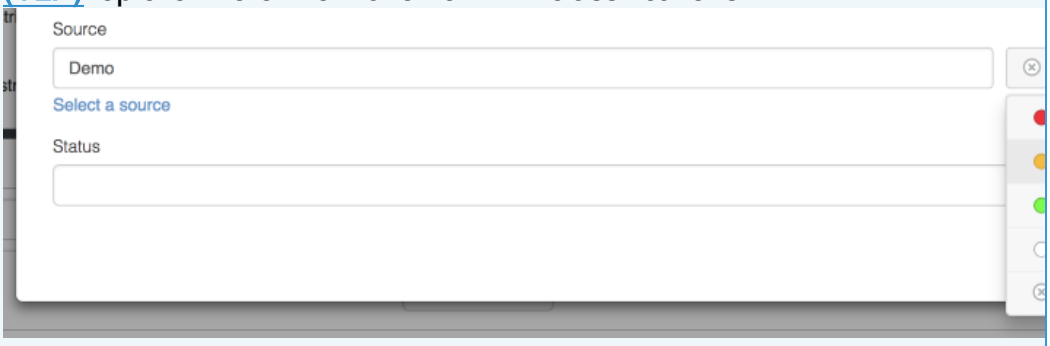


The Add Details dialog box opens with the Add Attributes tab selected by default.

3. Select the **Source** tab.

4. Select a **Source** from the dropdown provided.

You can also click on **Add a New Source** if the desired source is not listed in the dropdown list . If administrators have enabled TLP view settings, users can select a TLP classification light for the new source in the dropdown list provided. See the Traffic Light Protocol (TLP) topic for more information on TLP classifications.



5. Select **Add Source**.

Deleting an Attribute Source

You can delete an attribute's source from the object details page.

To delete an attribute source:

1. Locate the Details pane on the object details page.
2. Select the **X** next to the attribute's source.

The confirmation dialog box opens.

3. Select **Delete Attribute Source**.

Managing Tags

You can add and remove tags in the Details pane on the object details page.

To add a tag:

1. Locate the Details pane on the object details page.
2. Select the Tags text field and enter the tag.
3. Press **[Enter]** or **[Return]**.

Repeat steps 2-3 to add additional tags.

To delete a tag:

1. Locate the Details pane on the object details page.
2. Select the **X** next to the tag to delete.

Description Pane

The Description Pane section of the object details page allows you to add a description for the system object.

To update the Description pane:

1. Locate the Description pane on the object details page.
2. Select **Edit**.
3. Make the required changes and select **Save**.

Comments Pane

The Comments pane allows users to record comments about the system object for other users to see.

The following functions can be performed:

- Adding Comments
- Editing Comments
- Deleting Comments

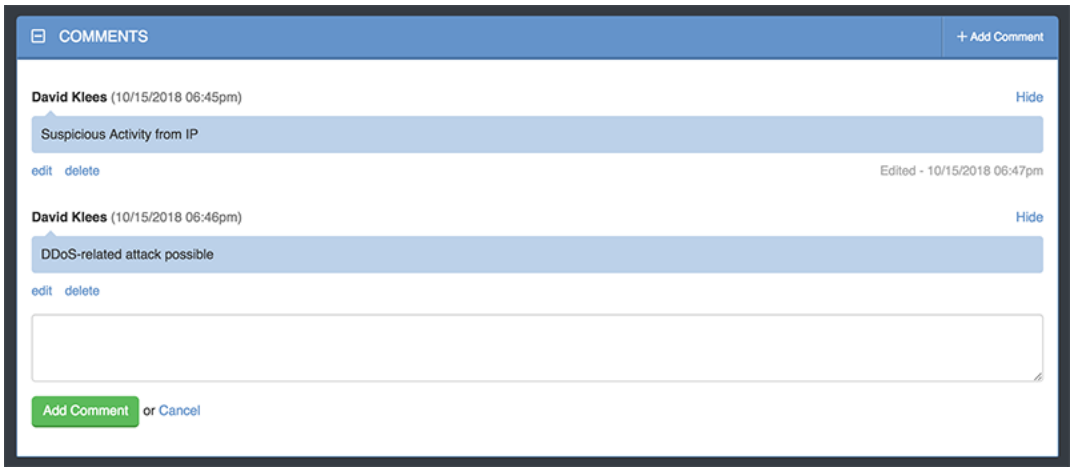
Adding Comments

Users can also click on the **Actions** menu and select the **Comment** option.

From the Object Details page:

1. Click on the expand icon to expand the Comments pane.
2. Click on the **Add Comment** link located at the top-right and lower-left of the pane.

   The new comment text box opens.



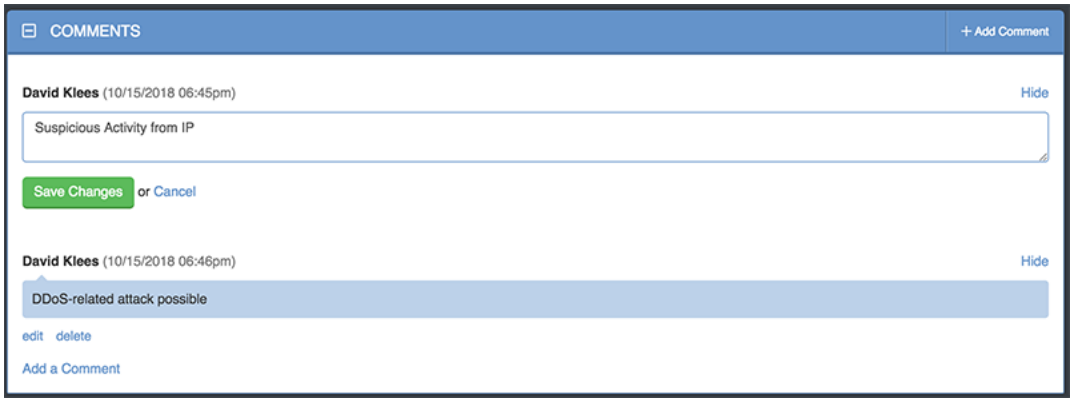
3. Enter a comment.
4. Click on the **Add Comment** button.

Editing Comments

From the Object Details page:

1. Click on the expand icon to expand the Comments pane.
2. Click on the **Edit** link located beneath the comment to update.

   The edit comment text box opens.



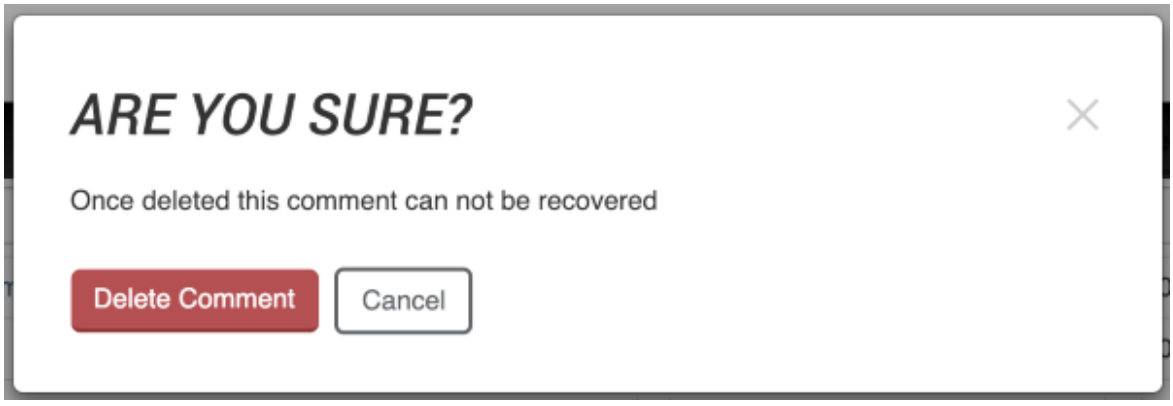
3. Edit the comment.
4. Click on the **Save Changes** button.

Deleting Comments

From the Object Details page:

1. Click on the expand icon to expand the Comments pane.
2. Click on the **Edit** link located beneath the comment to update..

   The delete confirmation dialog text box opens.



3. Click on the **Delete Comment** button.

Related Panes

The Related Panes section of the object details page displays other system objects that have been related to the current object.

You can link/unlink system objects from related panes and perform bulk updates (related indicators pane only). You can click on a related object to navigate to its object details page.

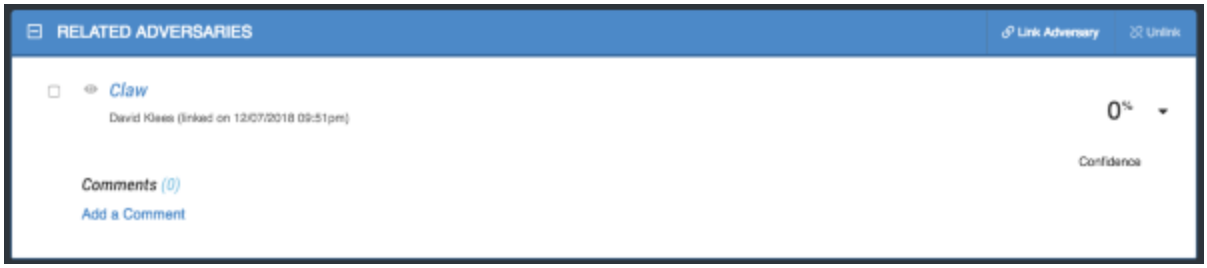
Related panes will only appear if a system object is already related to the object. Use the **Actions** button to create the initial object: **Actions > Relationship**.

Related Topics:

- Related Indicators Pane
- Related Adversaries Pane
- Related Files Pane
- Related Investigations Pane
- Related Signatures Pane
- Related Events Pane

Related Adversaries Pane

The Related Adversaries Pane allows you to link and unlink adversary to an object. You can also add comments and adjust the adversary's confidence level.



Related Topics:

- Linking Adversaries
- Configuring Confidence Level
- Commenting on Related Adversaries
- Unlinking Related Adversaries

Linking Adversaries

You can link adversaries to a system object.

To link an adversary:

1. Locate the Related Adversaries pane on the object details page.
2. Select **Link Adversary**.
   The Add Relationships dialog box opens.

3. Use the supplied text field to select a file.

   Repeat Step 3 to select multiple adversaries.

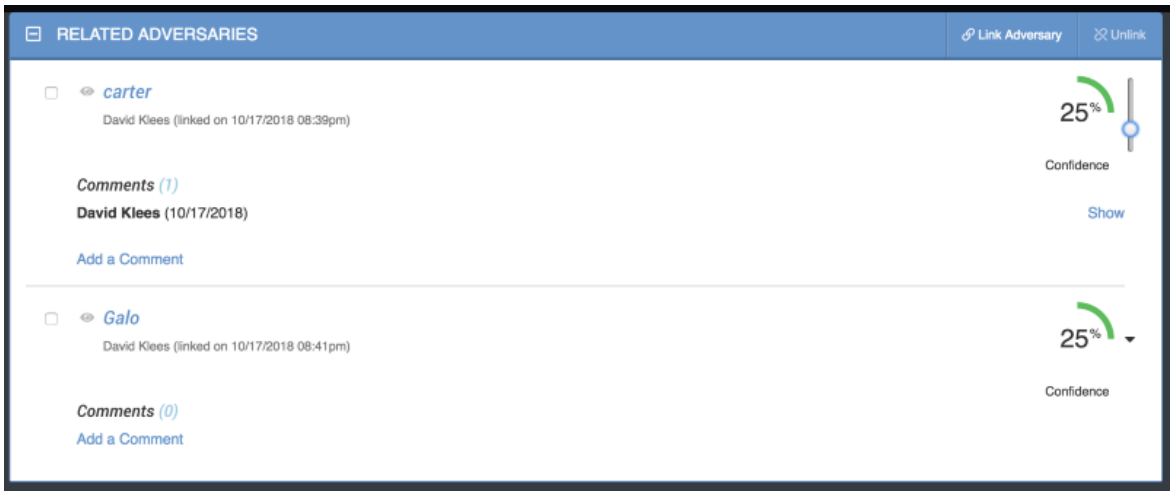
4. Click **Add**.

Configuring Confidence Level

You can configure a related adversary's confidence level from the Related Adversaries pane.

To configure the confidence level of a related adversary:

1. Locate the Related Adversaries pane on the object details page.
2. Click the dropdown arrow to the right of the adversary, and slide the scale to the desired confidence level.



The confidence level can be set to 0, 25, 50, 75, and 100.

The displayed confidence level will be modified to reflect your selection.

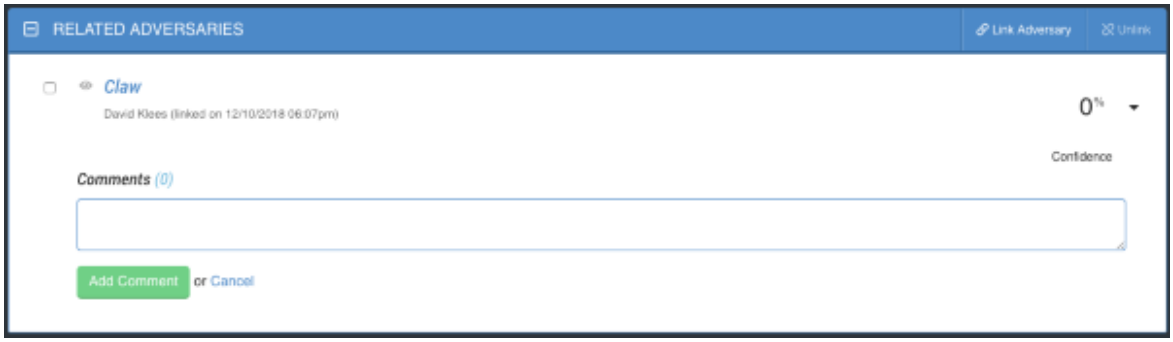
Commenting on Related Adversaries

You can add, edit, and remove comments to related adversaries.

To add a comment to a related adversary:

1. Locate the Related Adversaries pane on the object details page.
2. Select **Add a Comment**.

   The Comments text field opens.



3. Enter a comment.
4. Click **Add Comment**.

To edit a related adversary comment:

1. Locate the Related Adversaries pane on the object details page.
2. Select **Edit** under the comment to update.
3. Update the comment.
4. Click **Save Changes**.

To delete a related adversary comment:

1. Locate the Related Adversaries pane on the object details page.
2. Select **Delete** under the comment to update.

   A confirmation dialog box opens.
3. Select **Delete Comment**.

Unlinking Related Adversaries

You can unlink related adversaries for an object.

To unlink related adversaries:

1. Locate the Related Adversaries pane on the object details page.
2. Select the checkbox(es) next to the adversary(ies) to unlink.

3. Select **Unlink**.

Related Indicators Pane

The Related Indicators Pane allows users to link and unlink indicators to an object as well as perform a bulk update to selected linked indicators.

Related Topics:

- Linking Indicators
- Performing Bulk Updates to Related Indicators
- Unlinking Related Indicators

Linking Indicators

You can link indicators to a system object.

To link an indicator:

1. Locate the Related Indicators pane on the object details page.
2. Select **Link Indicator**.
   The Add Relationships dialog box opens.

3. Use the supplied text field to select an indicator.

   Repeat Step 3 to select multiple indicators.

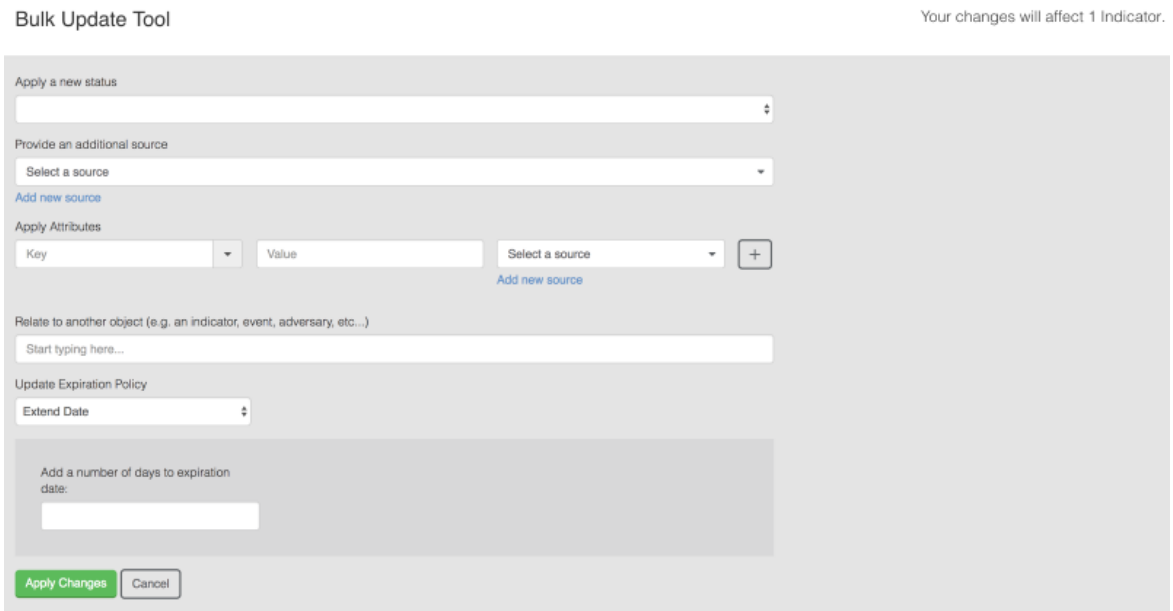
4. Click **Add**.

Performing Bulk Updates to Related Indicators

You can perform bulk updates to linked indicators listed in the Related Indicators pane of an object.

To perform a bulk update:

1. Locate the Related Indicators pane on the object details page.
2. Select the checkbox(es) next to the indicator(s) to update.
3. Select Bulk Update.



   The Bulk Update form loads.

4. Select the desired changes and click **Apply Changes**.

Unlinking Related Indicators

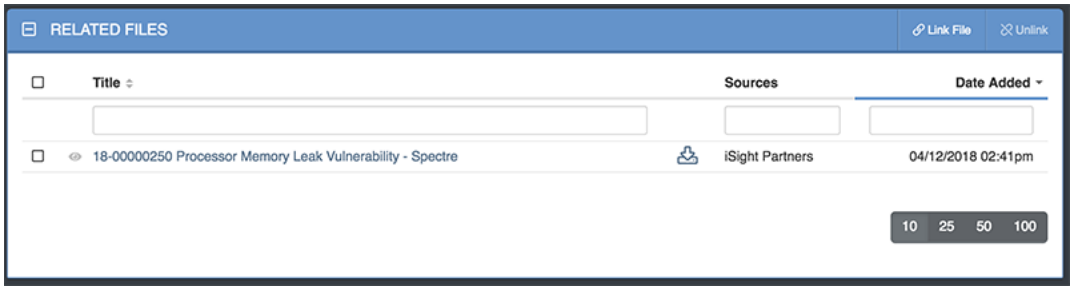
You can unlink related indicators for an object.

To unlink related indicators:

1. Locate the Related Indicators pane on the object details page.
2. Select the checkbox(es) next to the indicators to unlink.
3. Select **Unlink**.

Related Files Pane

The Related Files Pane allows you to link and unlink files to an object.



You can view a quick summary of the file by clicking the on the eye icon to the left of the file name or, click on the name itself to navigate to its Files Details page. You can also download a copy of the file by clicking on the download icon .

Related Topics:

- Linking Files
- Unlinking Related Files

Linking Files

You can link Files to a system object.

To link a file:

1. Locate the Related Files pane on the object details page.

2. Select **Link File**.

   The Add Relationships dialog box opens.

3. Use the supplied text field to select a file.

   Repeat Step 3 to select multiple files.

4. Click **Add**.

Unlinking Related Files

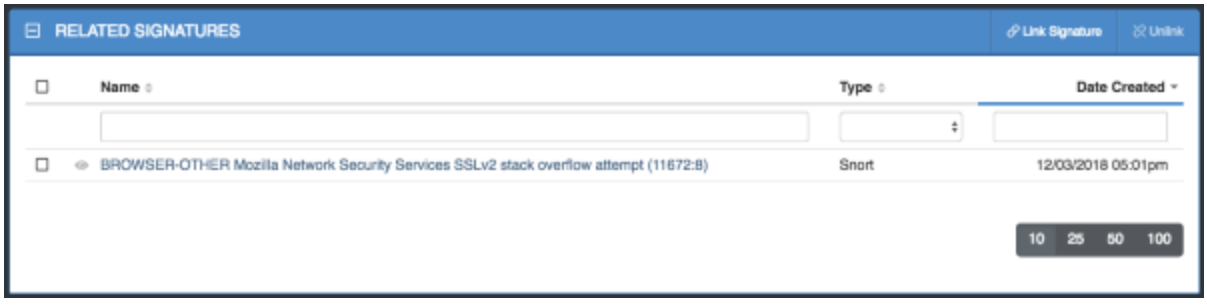
You can unlink related files for an object.

To unlink related files:

1. Locate the Related Files pane on the object details page.
2. Select the checkbox(es) next to the files to unlink.
3. Select **Unlink**.

Related Signatures Pane

The Related Signatures Pane allows you to link and unlink signature to an object.



Related Topics:

- Linking Signatures
- Unlinking Related Signatures

Linking Signatures

You can link Signatures to a system object.

To link a file:

1. Locate the Related Signatures pane on the object details page.
2. Select **Link Signature**.

   The Add Relationships dialog box opens.

3. Use the supplied text field to select a file.

   Repeat Step 3 to select multiple files.

4. Click **Add**.

Unlinking Related Signatures

You can unlink related signatures for an object.

To unlink related indicators:

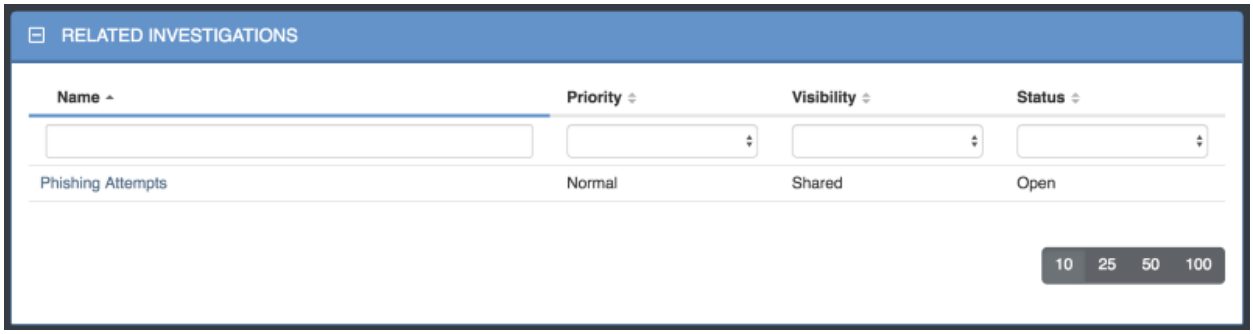
1. Locate the Related Signatures pane on the object details page.
2. Select the checkbox(es) next to the signatures to unlink.

3. Select **Unlink**.

Related Investigations Pane

> ThreatQ Investigations requires a separate license.

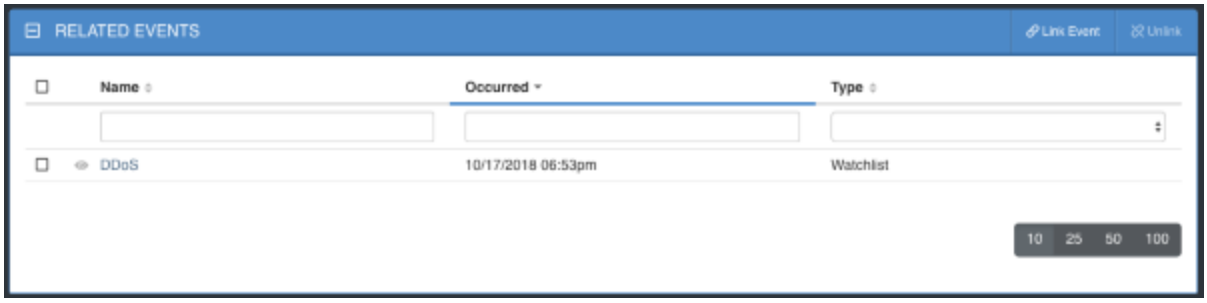
The Related Investigations pane displays any ThreatQ Investigation related to the object. Adding and removing an object to an investigation is controlled through the Investigations interface.



You can click on the investigation to open ThreatQ Investigations.

Related Events Pane

The Related Events Pane allows you to link and unlink events to a system object.



Related Topics:

- Linking Events
- Unlinking Related Events

Linking Events

You can link events to a system object.

To link an event:

1. Locate the Related Events pane on the object details page.
2. Select **Link Event**.

   The Add Relationships dialog box opens.

3. Use the supplied text field to select a file.

   Repeat Step 3 to select multiple events.

4. Click **Add**.

Unlinking Related Events

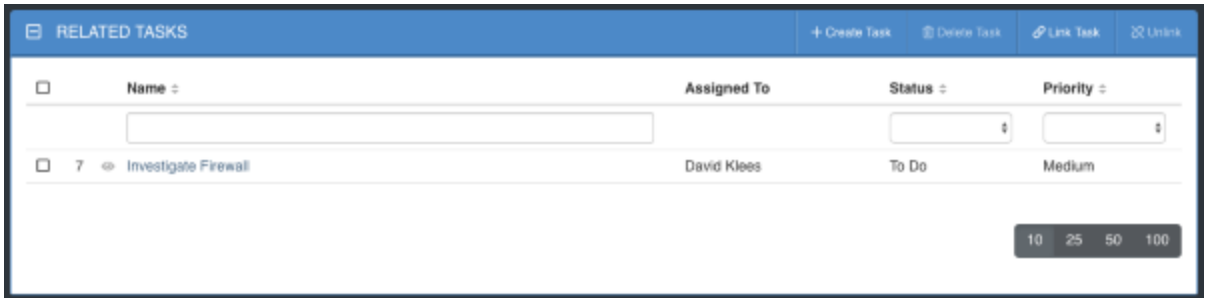
You can unlink related events for an object.

To unlink related events:

1. Locate the Related Events pane on the object details page.
2. Select the checkbox(es) next to the event(s) to unlink.
3. Select **Unlink**.

Related Tasks Pane

The Related Tasks Pane allows you to link, unlink, and delete tasks associated with an object.



You can view a quick summary of the file by clicking the on the eye icon to the left of the task name or, click on the name itself to navigate to its Task Details page.

Related Topics:

- Linking Tasks
- Unlinking Related Tasks
- Deleting Related Tasks

Linking Tasks

You can link Tasks to a system object from its object details page.

> You can also related a task to a system object while creating a task.

To link a task:

1. Locate the Related Tasks pane on the object details page.

2. Select **Link Task**.

   The Add Relationships dialog box opens.

3. Use the supplied text field to select a file.

   Repeat Step 3 to select multiple files.

4. Click **Add**.

Unlinking Related Tasks

You can unlink related tasks for an object.

To unlink related tasks:

1. Locate the Related Tasks pane on the object details page.
2. Select the checkbox(es) next to the files to unlink.
3. Select **Unlink**.

Deleting Related Tasks

You can delete Tasks related to a system object from its object details page.

To delete a task:

1. Locate the Related Tasks pane on the object details page.
2. Select the checkbox next to the task to delete.

3. Select **Delete Task**.

   A confirmation dialog box opens.

4. Select **Delete Task**.

Actions Menu

The Action Menu, located on the left-hand of the Object Details page, allows users to quickly execute system object processes.

Actions Include:

Action	Function	Reference
Attribute	Brings up the Add Details dialog box to add an attribute to the object.	• Adding an Attribute to an Object
Comment	Creates a new text box entry in the comment pane.	• Adding Comments
Create Task	Opens up the Add Task dialog box.	• Assigning a Task
Generate Report	Generates a PDF report of the object.	• Generating Reports
Relationship	Brings up the Add Relationships dialog box to link	• Linking

Action	Function	Reference
	other system objects to the object.	Adversaries • Linking Events • Linking Files • Linking Indicators • Linking Signatures • Linking Tasks
Source	Brings up the Add Details dialog box to add a source to the object.	• Adding a Source to an Object

Analytics

The Analytics tab provides a summary view of Adversary, Event, File, Indicator, and Signature Object Types.

Global and List filters are not available for these views nor can you modify the types of columns used. Use the Advanced Search to utilize these options.

Analytics pages include:

- Adversaries Overview
- Events Overview
- Files Overview
- Indicators Overview
- Signatures Overview

Adversaries Overview

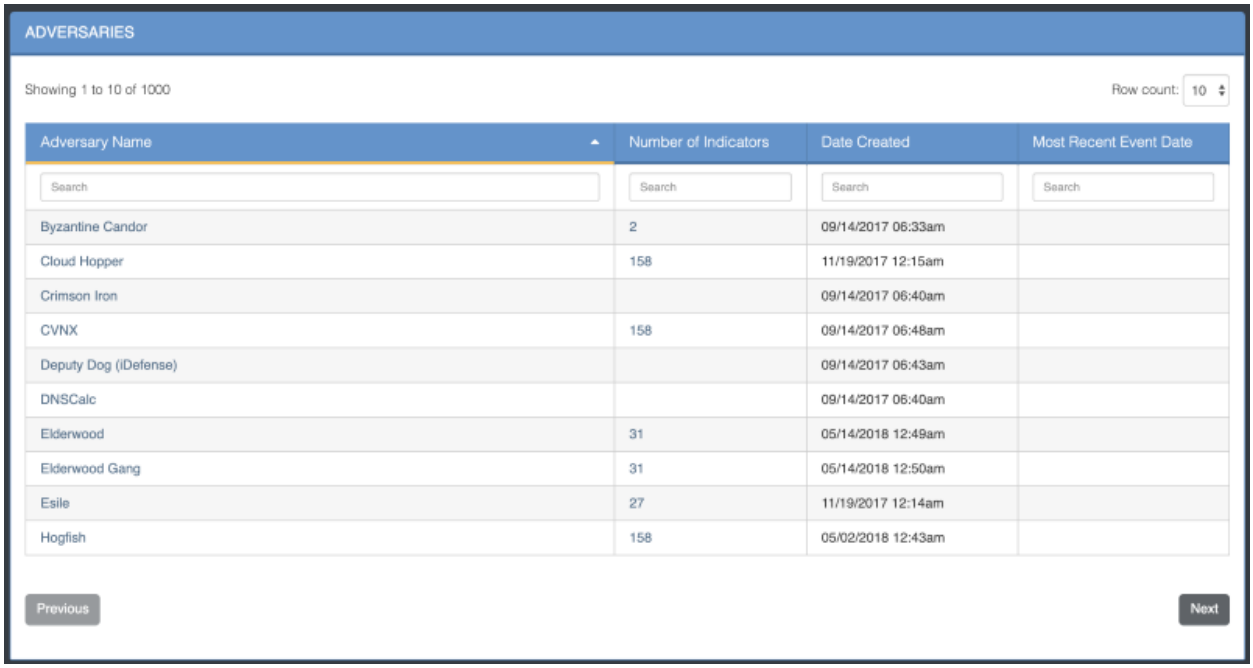
The Adversaries page provides an overview of all the adversaries within ThreatQ as well as overlapping use of specific indicators.

There are three sections:

- Adversaries Summary Table
- Adversaries Overlap Table.
- Indicator Distribution Pie Chart

Adversaries Summary Table

The Adversaries Summary table lists adversaries by name, number of indicators, date created, and the most recent event date associated with the adversary.



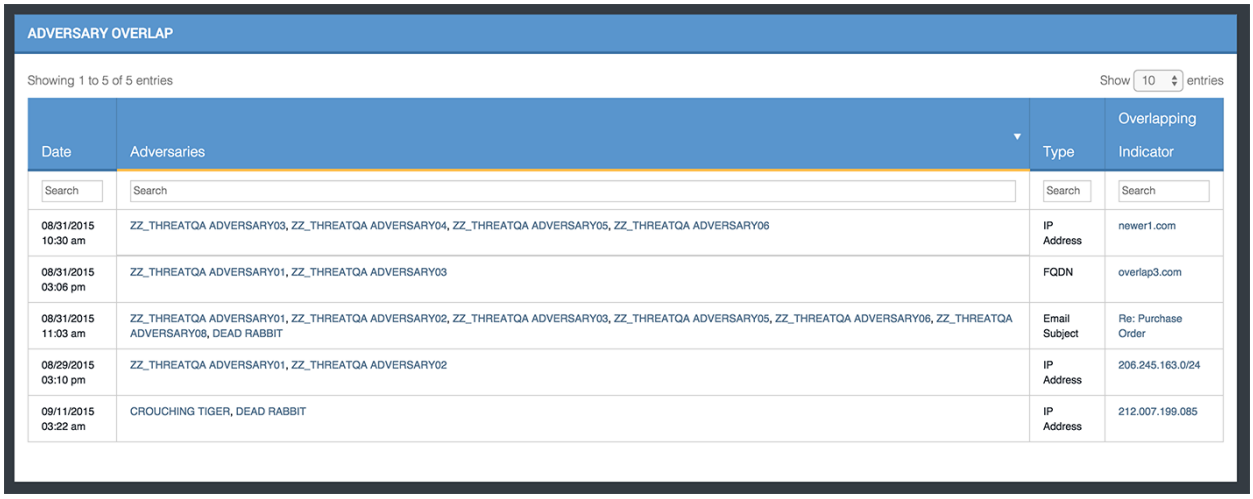
The following functions are available:

Function	Details
Opening the Adversary Details page for an adversary	1. Click the name in the Adversary Name column.
Performing a search for related indicators	1. Click the number in the Number of Indicators column to set the adversary name as a search criterion and open the Advanced Search page.
Opening the Event Details page for an adversary event	1. Click the date in the Most Recent Event Date to open the Event Details page.

Function	Details
Changing the number of entries displayed in the table	1. Click the paging batch option located to the bottom-right of the table.
Sorting the table by a column	1. Click the column header. To reverse the column sorting order, click the header a second time.
Searching within the Adversary Name column	1. Click within the search box at the top of the column, and enter your search criteria.

Adversaries Overlap Table

The Adversary Overlap table lists adversaries, the date and time they were created, their type, and any overlapping indicators.



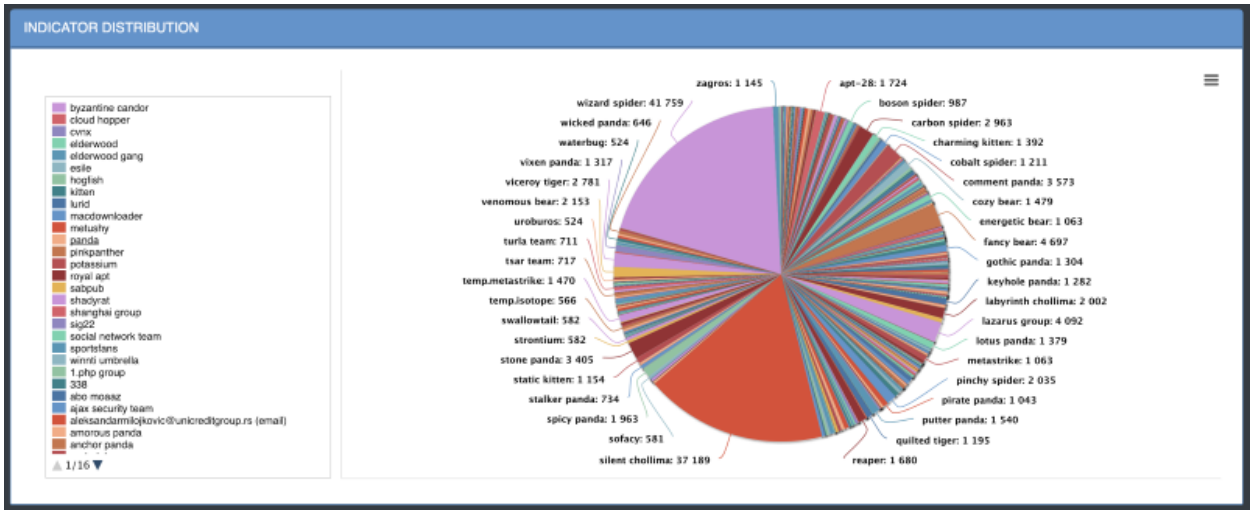
The following functions are available:

Function	Details
Opening the Adversary Details page for an adversary	1. Click the name in the Adversary Name column.

Function	Details
Opening the Indicator Details page for an overlapping indicator	1. Click the identity in the Overlapping Indicator column.
Changing the number of entries displayed in the table	1. Click the paging batch option located to the bottom-right of the table.
Sorting the table by a column	1. Click the column header. To reverse the column sorting order, click the header a second time.
Searching within a column	1. Click within the search box at the top of the column, and enter your search criteria.

Indicator Distribution Pie Chart

The Adversary Overlap table lists adversaries, the date and time they were created, their type, and any overlapping indicators.



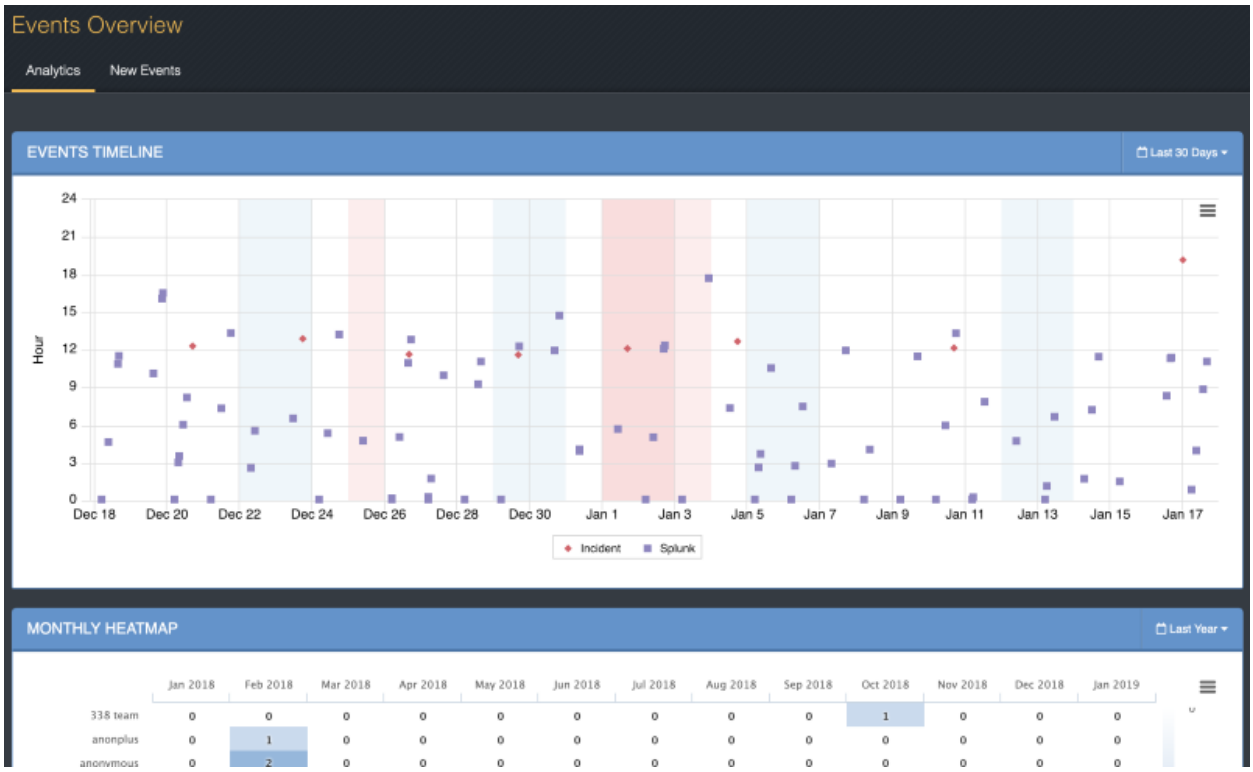
The following functions are available:

Function	Details
Viewing more information	1. Hover over a colored section of the pie chart to open

Function	Details
about a selected value	a popup identifying the indicator. The number of times the indicator was found within the specified time frame, and what percentage of the total number of indicators it represents.
Hiding or unhiding one of the values from the pie chart	1. Click the indicator on the left of the pie chart to remove it; click a second time to reinstate it.
Adjusting the time frame of the information displayed	1. Click the dropdown menu at the top right and select the desired timeframe. You can select from: • Last 24 Hours • Last 7 Days • Last 30 Days • Last Year • User-set custom range
Printing the graph or saving it as a PNG, JPEG, PDF, or SVG	1. Click the hamburger menu ☰ and select the desired option.

Events Overview

The Events page provides a high-level view of what types of events have occurred and how frequently they are occurring.



To Access the Events Overview page:

1. In the navigation menu, choose **Analytics** > **Events**.

   The Events Overview page opens.

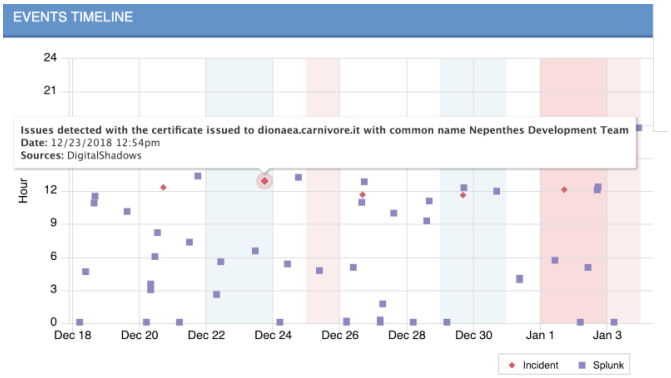
The tab options include:

- Events History Scatter Plot
- Monthly Heatmap
- New Events Summary

Events History Scatter Plot

The scatter plot points are plotted by date (x-axis) and hour (y-axis). The legend under the scatter plot identifies the different kinds of events shown.

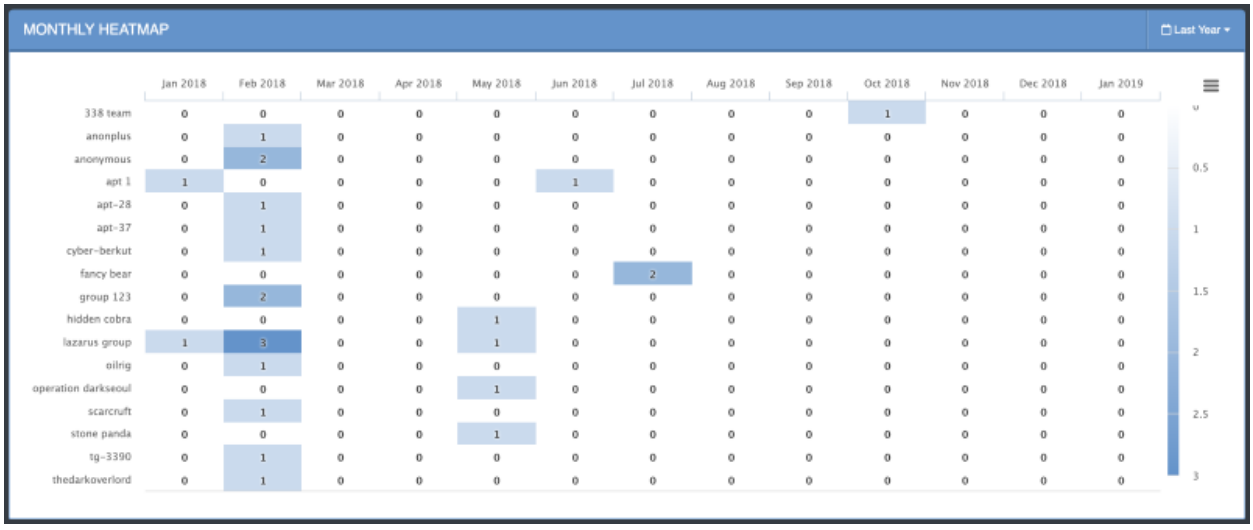
The following functions are available:

Function	Details
Viewing an event's name, date and time, and source	1. Hover your mouse over an event on the scatter plot to see its name, date and time, and source. 
Opening the Event Details page for one of the events	1. Click the event in the scatter plot. For more information, see Object Details Page.
Hiding or unhiding one or more of the event types	1. Click the event type in the legend immediately below the scatter plot to remove it from the graph; click it again to reinstate it.
Adjusting the time frame of the information displayed	1. Click the dropdown menu at the top right and select the desired time frame.

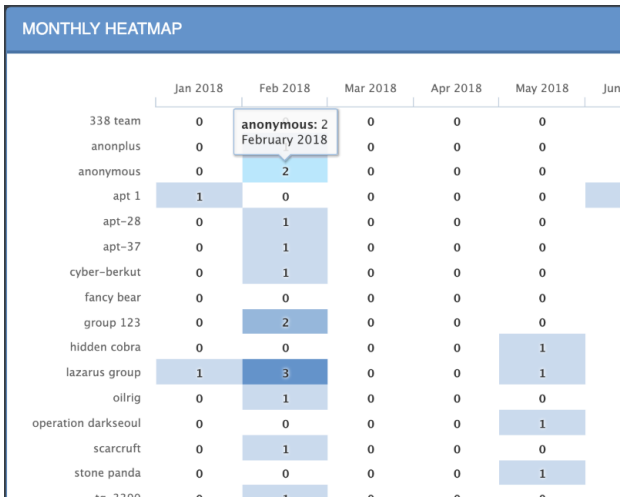
Function	Details
	You can select from: • Last 24 Hours • Last 7 Days • Last 30 Days • Last Year • User-set custom range
Printing or downloading the scatter plot as a PNG, JPEG, PDF, or SVG file	1. Click the hamburger menu and select the desired option.

Monthly Heatmap

The Monthly Heatmap table lists events that happened per adversary each month. Shading of the monthly totals is used to allow you to quickly scan for patterns in the events and to quickly detect events with higher monthly counts.

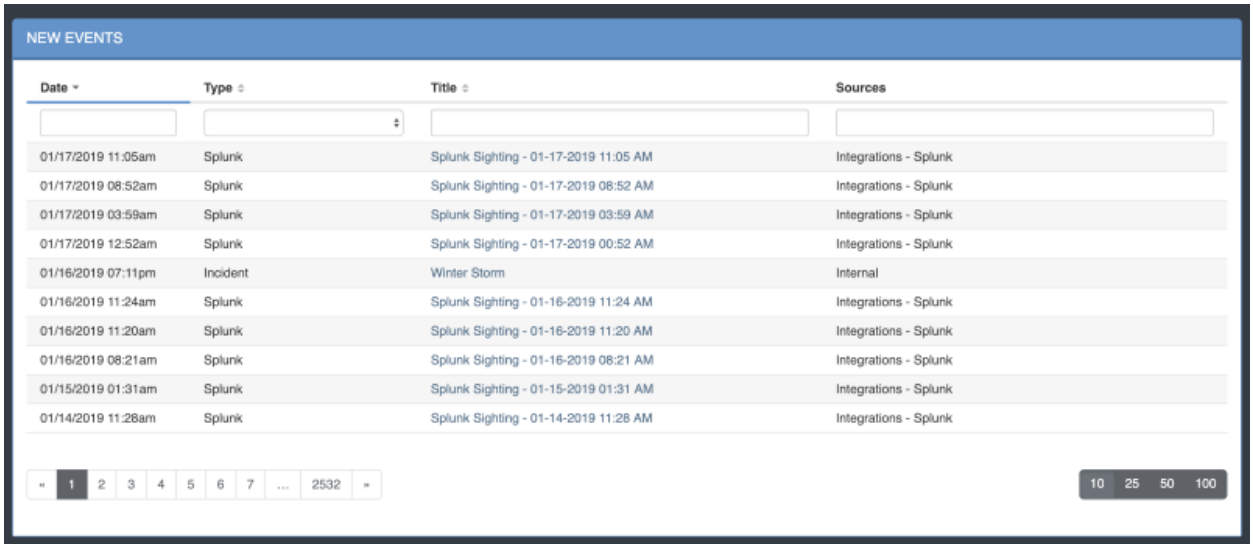


The following functions are available:

Function	Details
Viewing an event's name and monthly count	1. Hover your mouse over an event on the heatmap to see its name and monthly count. 
Adjusting the time frame of the information displayed	1. Click the dropdown menu at the top right and select the desired time frame. You can select from: • Last 24 Hours • Last 7 Days • Last 30 Days • Last Year • User-set custom range
Printing the graph or saving it as a PNG, JPEG, PDF, or SVG	1. Click the hamburger menu ☰ and select the desired option.

New Events Summary

The New Events Summary table provides a breakdown of events by date, type, title, and sources.

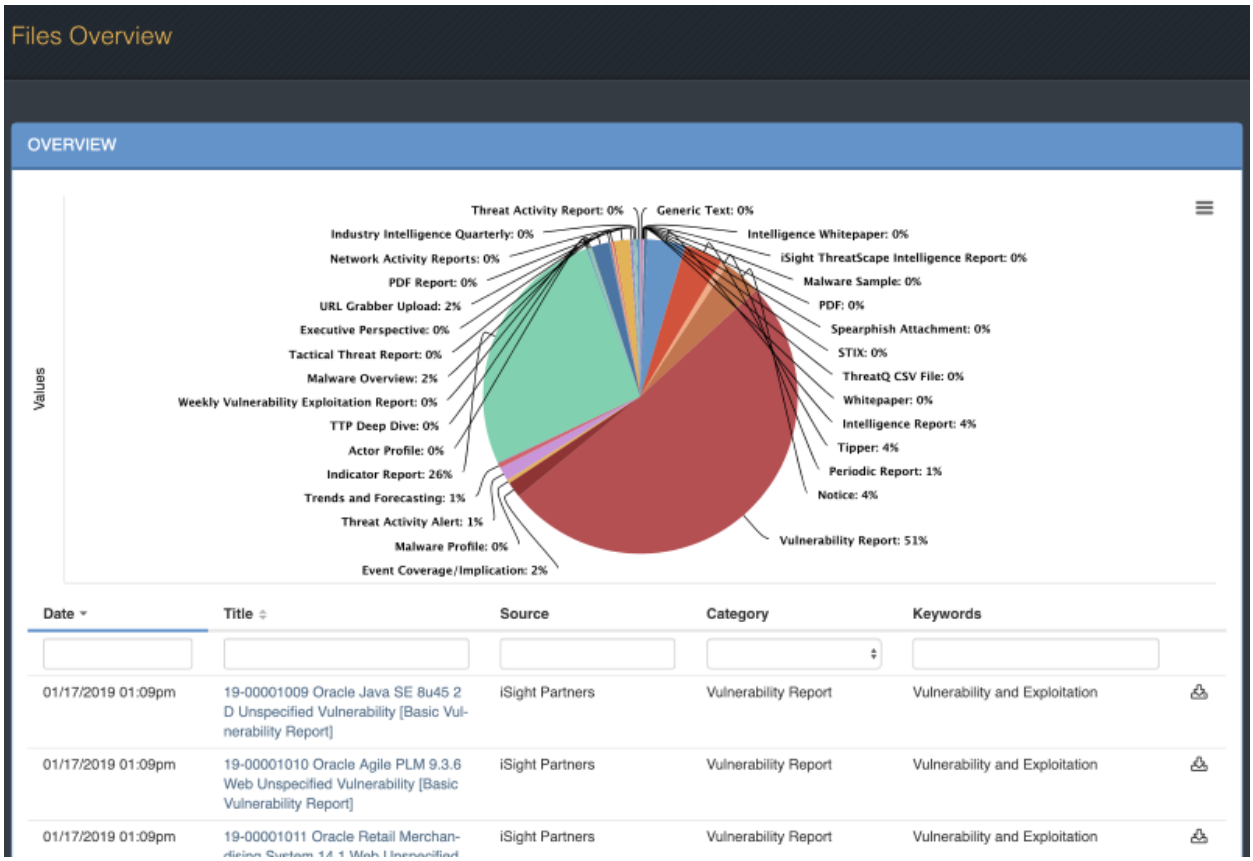


The following functions are available:

Function	Details
Opening the Event Details page for one of the events	1. Click the event title. For more information, see Object Details Page.
Changing the number of entries displayed in the table	1. Click the dropdown menu at the top right of the table, and select the desired option.
Sorting the table by a column	1. Click the column header. 2. Click the header a second time to reverse sort order.
Searching within a column	1. Click within the search box at the top of the column, and enter your search criteria.

Files Overview

The Files Overview page provides you with a pie chart displays the percentage of different types of files within the system and a table that lists the files, the date and time they were created, their title, their source, their category, and associated keywords.

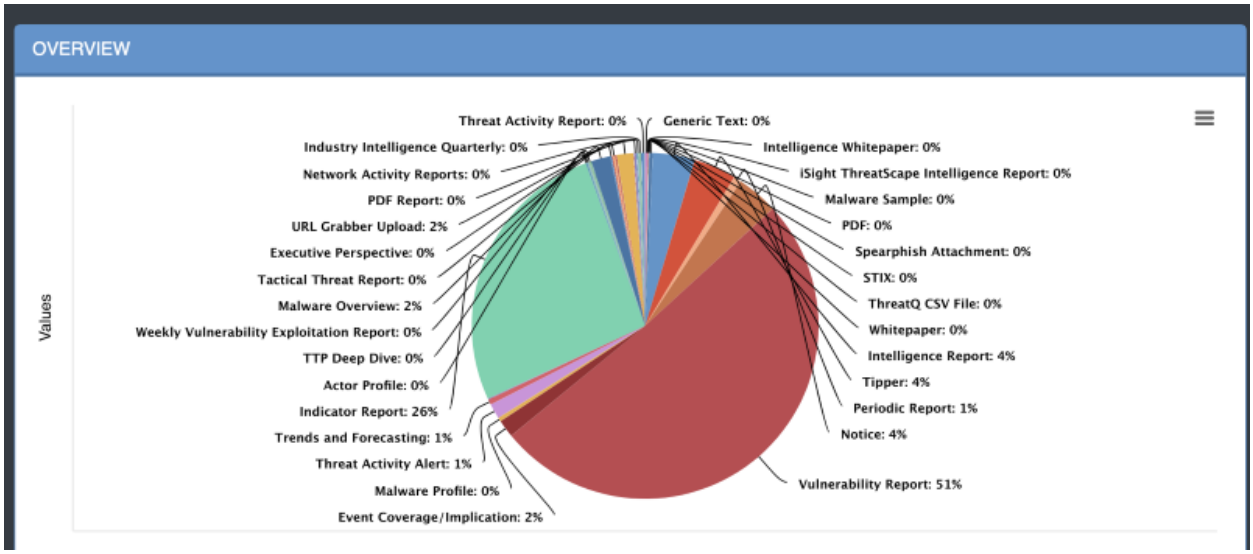


Available views include:

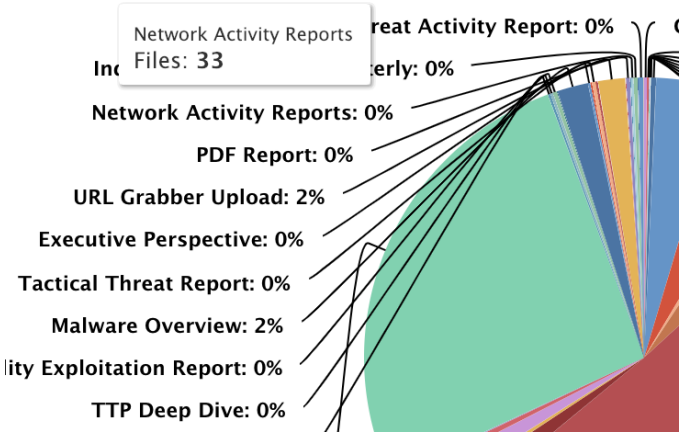
- Files Pie Chart
- Files Table

Files Pie Chart

The File Types pie chart displays the percentage of different types of files within the system.



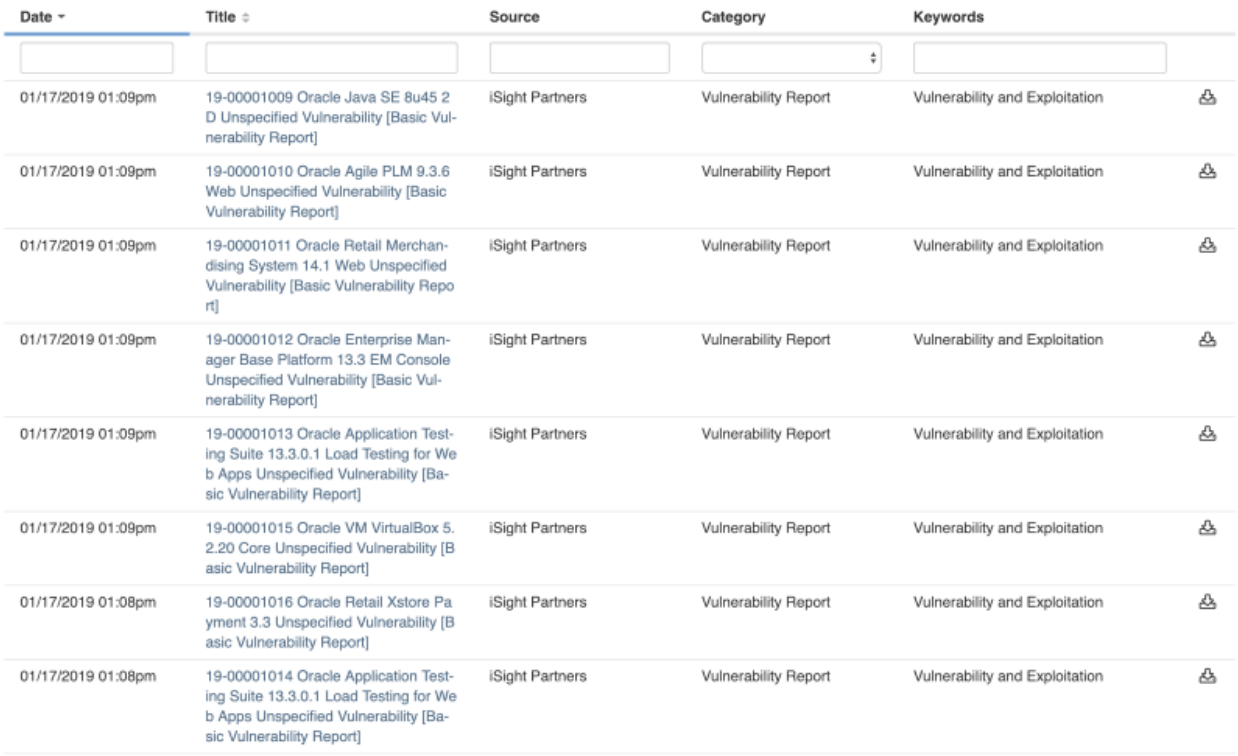
The following function is available:

Function	Details
Viewing more information about a selected file	1. Hover over a colored section of the pie chart to open a popup that gives the number of attachment types. 
Printing the graph or saving it	1. Click the hamburger menu ☰ and select the

Function	Details
as a PNG, JPEG, PDF, or SVG	desired option.

Files Table

Immediately below the Browse pie chart is a table that lists the files, the date and time they were created, their title, their source, their category, and associated keywords.



Date	Title	Source	Category	Keywords
01/17/2019 01:09pm	19-00001009 Oracle Java SE 8u45 2D Unspecified Vulnerability [Basic Vulnerability Report]	iSight Partners	Vulnerability Report	Vulnerability and Exploitation
01/17/2019 01:09pm	19-00001010 Oracle Agile PLM 9.3.6 Web Unspecified Vulnerability [Basic Vulnerability Report]	iSight Partners	Vulnerability Report	Vulnerability and Exploitation
01/17/2019 01:09pm	19-00001011 Oracle Retail Merchandising System 14.1 Web Unspecified Vulnerability [Basic Vulnerability Report]	iSight Partners	Vulnerability Report	Vulnerability and Exploitation
01/17/2019 01:09pm	19-00001012 Oracle Enterprise Manager Base Platform 13.3 EM Console Unspecified Vulnerability [Basic Vulnerability Report]	iSight Partners	Vulnerability Report	Vulnerability and Exploitation
01/17/2019 01:09pm	19-00001013 Oracle Application Testing Suite 13.3.0.1 Load Testing for Web Apps Unspecified Vulnerability [Basic Vulnerability Report]	iSight Partners	Vulnerability Report	Vulnerability and Exploitation
01/17/2019 01:09pm	19-00001015 Oracle VM VirtualBox 5.2.20 Core Unspecified Vulnerability [Basic Vulnerability Report]	iSight Partners	Vulnerability Report	Vulnerability and Exploitation
01/17/2019 01:08pm	19-00001016 Oracle Retail Xstore Payment 3.3 Unspecified Vulnerability [Basic Vulnerability Report]	iSight Partners	Vulnerability Report	Vulnerability and Exploitation
01/17/2019 01:08pm	19-00001014 Oracle Application Testing Suite 13.3.0.1 Load Testing for Web Apps Unspecified Vulnerability [Basic Vulnerability Report]	iSight Partners	Vulnerability Report	Vulnerability and Exploitation

The following function is available:

Function	Details
Opening the File Details page for a file	1. Click the name in the Title column.
Changing the number of entries displayed in the table per page	1. Click the paging batch option located to the bottom-right of the table.

Function	Details
Sorting the table by a column	1. Click the column header. 2. To reverse the column sorting order, click the header a second time.
Searching within a column	1. Click within the search box at the top of a column, and enter your search criteria.
Downloading a file	1. Click the download icon .

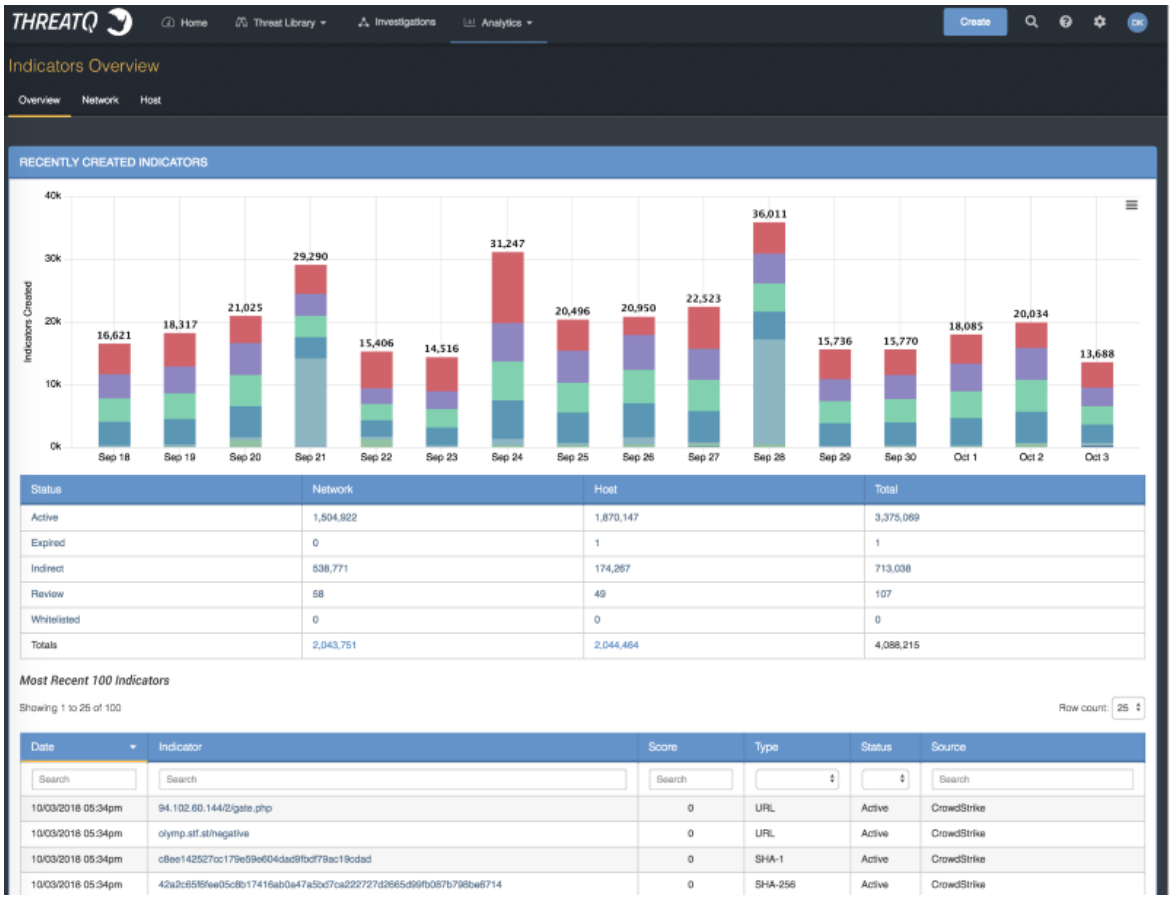
Indicators Overview

The Indicators Overview page provides an insight into what indicators have been added to the system within the last 15 days, as well as an overview of how many indicators fall under each indicator type.

To Access the Indicators Overview Page:

1. From the navigation menu, click on **Analytics** and choose **Indicators**.

The Indicators Overview page will open with three view tab options at the to of the page.



The page is broken down into different Indicator class views that are accessible via the tabbed navigation located at the top of the page.

The tab options include:

- Overview
- Network (Indicator Class = Network)
- Host (Indicator Class = Host)

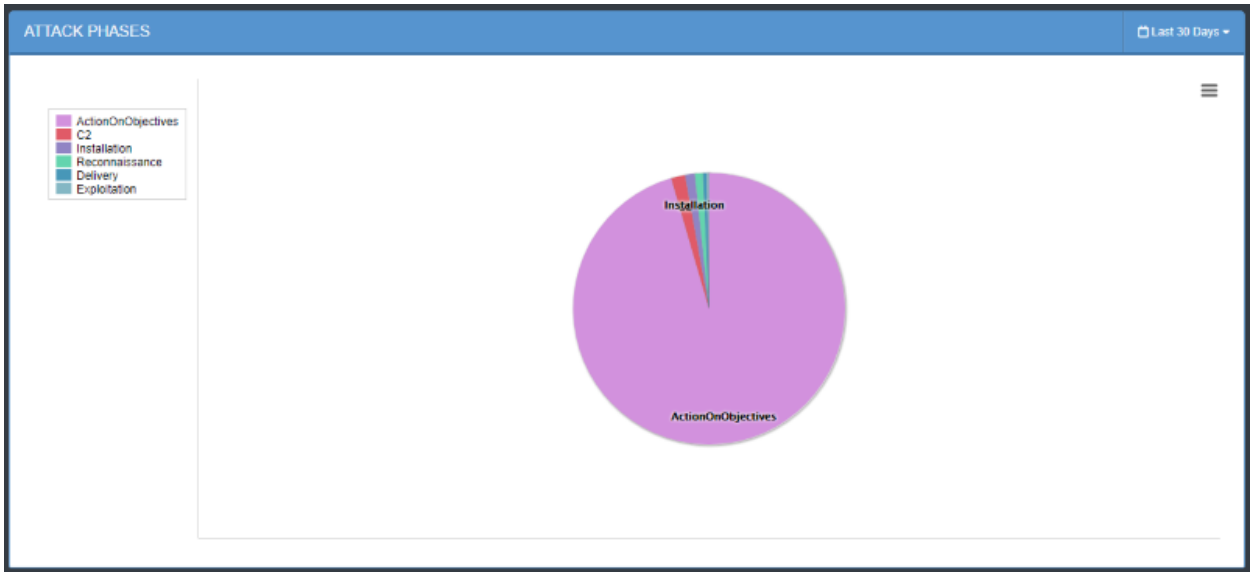
Summaries included on the Indicator Overview Page Include:

- Recently Created Indicators Histogram
- Summary Status (Overview view only)

- Most Recent 100 Indicators
- Attributes Table (Network and Host views only)
- Recent Sources (Network and Host views only)
- Attack Phases (Network and Host views only)

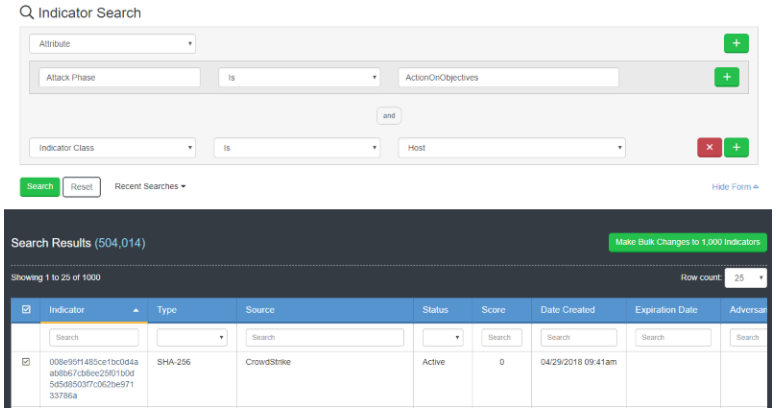
Attack Phases

Attack Phases are the ways an indicator might be used and are listed as indicator attributes. The Attack Phases pie chart displays the number of indicators that fall under each attack phase.



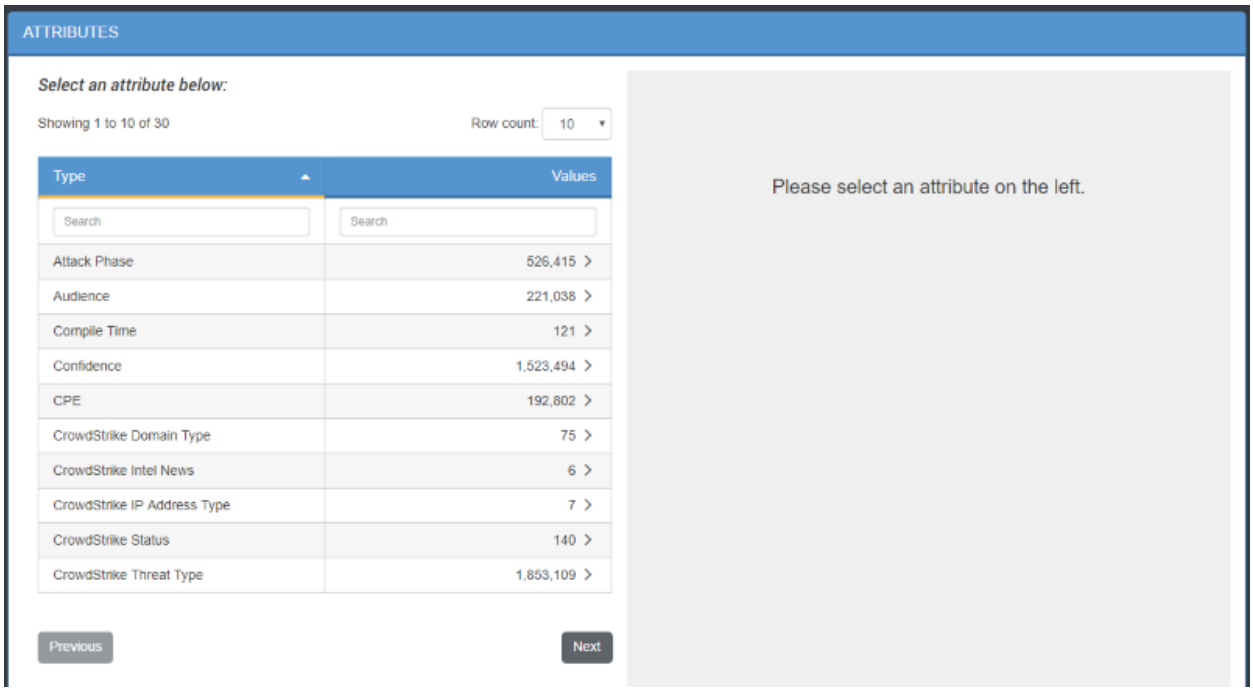
The following functions are available:

Function	Details
View the Number of Indicators for an Attack Phase	1. Hover the mouse over a portion of the pie chart to view a popup the Attack Phase and number of indicators associated with it. 2. Clicking on a pie chart section will open the Indicator Search page with the specific filter settings used for

Function	Details
	that selection. 
Adjust the Date Range for the Information Displayed	The default Date Range is 30 days. 1. Click the date range icon located to the top-right of the chart and use the dropdown menu select the desired range. Users can select from: • Last 24 Hours • Last 7 Days • Last 30 Days • Last Year • User-set custom range
Hide a Values from the Pie Chart	1. Click on a Attack Phase in the legend to the left of the pie chart to hide it. The Attack Phase will be removed from the pie chart and the source in the legend appear greyed out. 2. Click on the Attack Phase again to add it back to the pie chart.

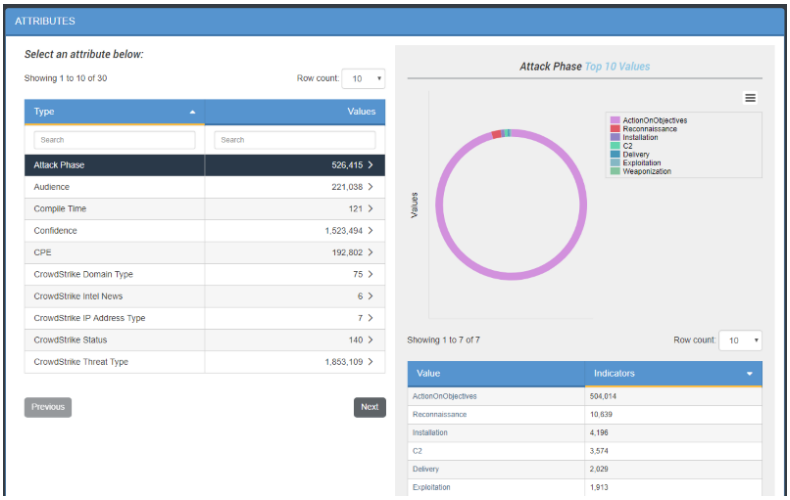
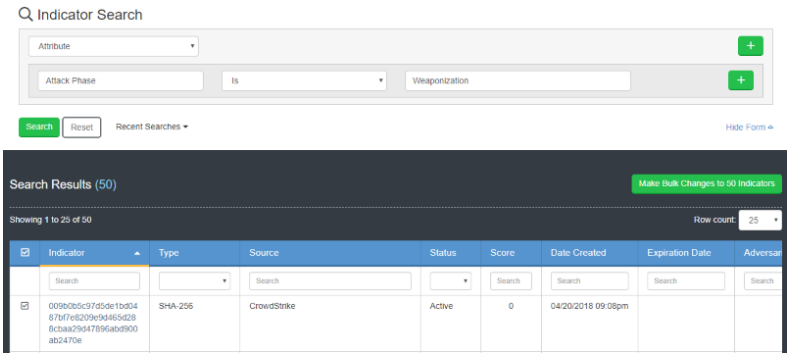
Attributes Table

The attributes list on the left side displays attributes related to indicators in your system.



The following functions are available:

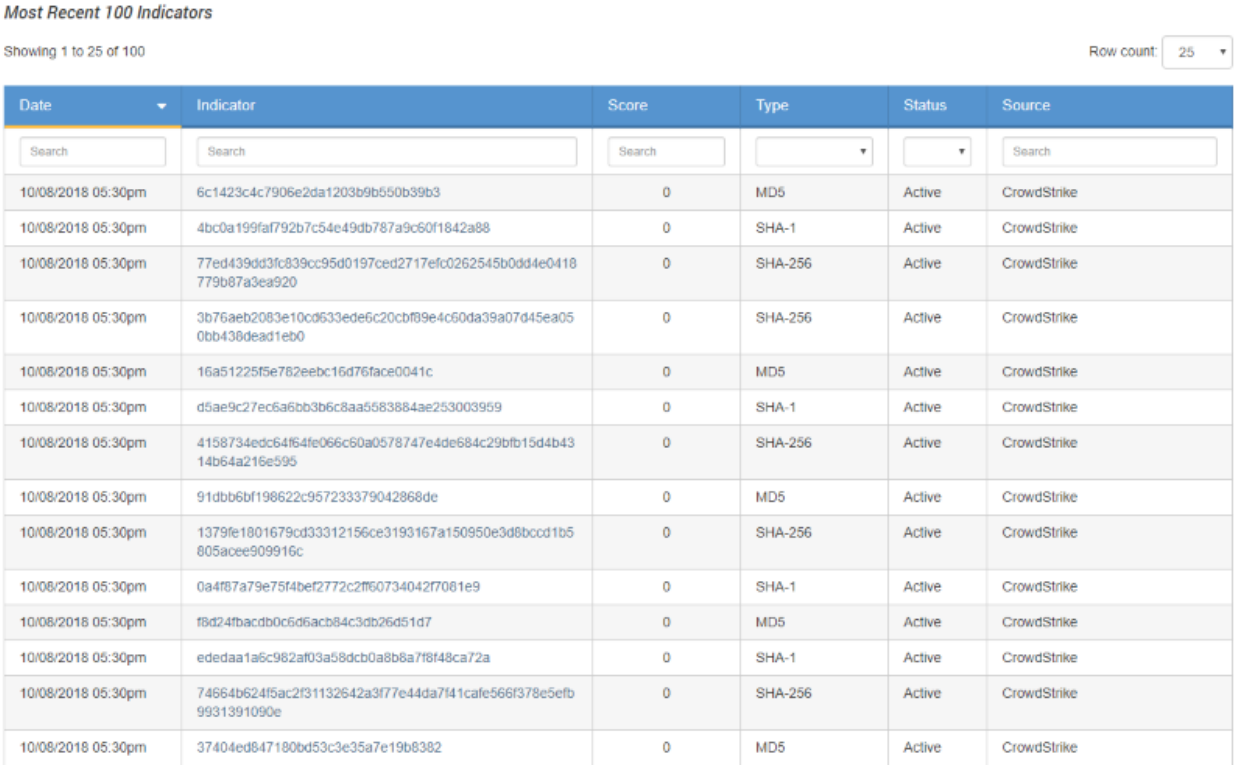
Function	Details
Change the Number of Entries Displayed in the Table	1. Click the **Row Count** icon located to the top-right of the chart and select a new display count from the drop-down.
Search/Filter Attributes and Values	1. Click within the search box at the top of the column, and enter your search criteria.
View More Information About a Selected Attribute	1. Click on an attribute row in the table to view additional information in the right pane.

Function	Details
	 2. Hover the mouse over different portions of the pie chart to reveal the segment's value. 3. Click on an **Attribute Value** in the summary table below the pie chart to open the Indicator Search page with those attribute values applied. 

.

Most Recent 100 Indicators

The Most Recent 100 Indicators list displays the 100 most recently reported indicators.



Most Recent 100 Indicators

Showing 1 to 25 of 100 — Row count: 25

Date	Indicator	Score	Type	Status	Source
10/08/2018 05:30pm	6c1423c4c7906e2da1203b9b550b39b3	0	MD5	Active	CrowdStrike
10/08/2018 05:30pm	4bc0a199faf792b7c54e49db787a9c60f1842a88	0	SHA-1	Active	CrowdStrike
10/08/2018 05:30pm	77ed439dd3fc839cc95d0197ced2717efc0262545b0dd4e0418779b87a3ea920	0	SHA-256	Active	CrowdStrike
10/08/2018 05:30pm	3b76aeb2083e10cd633ede6c20cbf89e4c60da39a07d45ea050bb438dead1eb0	0	SHA-256	Active	CrowdStrike
10/08/2018 05:30pm	16a51225f5e782eebc16d76face0041c	0	MD5	Active	CrowdStrike
10/08/2018 05:30pm	d5ae9c27ec6a6bb3b6c8aa5583884ae253003959	0	SHA-1	Active	CrowdStrike
10/08/2018 05:30pm	4158734edc64f64fe066c60a0578747e4de684c29bfb15d4b4314b64a216e595	0	SHA-256	Active	CrowdStrike
10/08/2018 05:30pm	91dbb6bf198622c957233379042868de	0	MD5	Active	CrowdStrike
10/08/2018 05:30pm	1379fe1801679cd33312156ce3193167a150950e3d8bccd1b5805acee909916c	0	SHA-256	Active	CrowdStrike
10/08/2018 05:30pm	0a4f87a79e75f4bef2772c2ff60734042f7081e9	0	SHA-1	Active	CrowdStrike
10/08/2018 05:30pm	f8d24fbacdb0c6d6acb84c3db26d51d7	0	MD5	Active	CrowdStrike
10/08/2018 05:30pm	ededaa1a6c982af03a58dcb0a8b8a7f8f48ca72a	0	SHA-1	Active	CrowdStrike
10/08/2018 05:30pm	74664b624f5ac2f31132642a3f77e44da7f41cafe566f378e5efb9931391090e	0	SHA-256	Active	CrowdStrike
10/08/2018 05:30pm	37404ed847180bd53c3e35a7e19b8382	0	MD5	Active	CrowdStrike

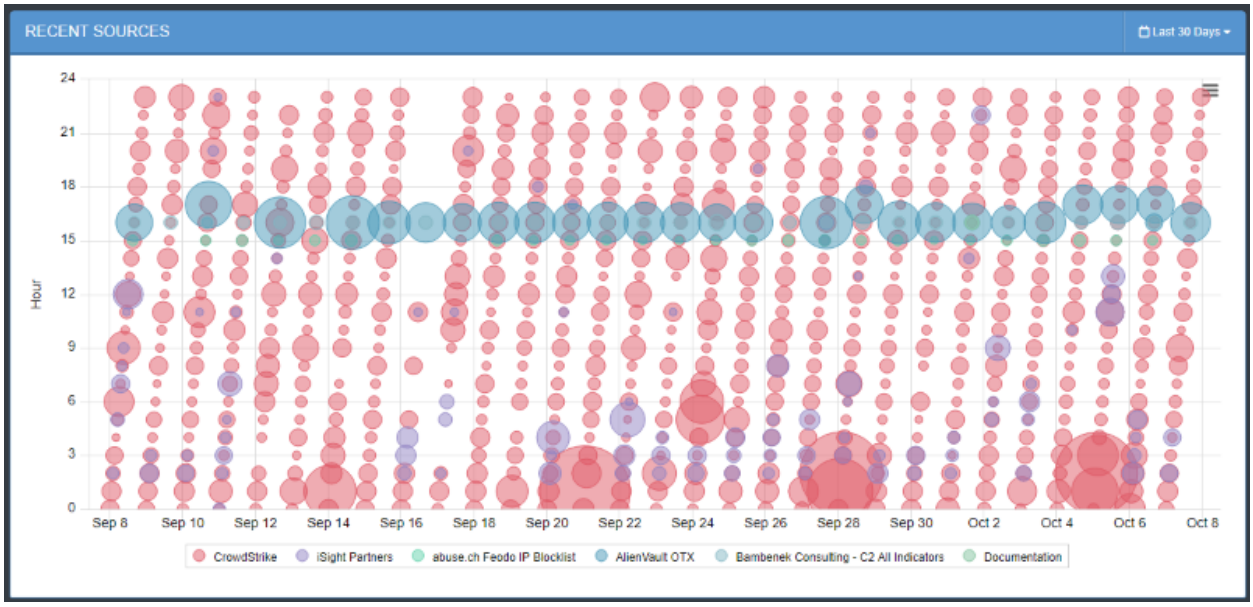
The following functions are available:

Function	Details
Resort the Table	1. Click on the different table headings to resort that table by that column.
Search and Filter Table Results	1. Click on one of the search boxes at the top of the columns and enter a keyword to filter the results. You can use the supplied dropdown selections for the Status and Type columns to filter by system-available values.
Modify the Number of	1. Click on the **Row Count** icon located to the top-

Function	Details
Rows Displayed	right of the chart and select a new display count from the dropdown.
Access the Indicator Details Page for a Specific Indicator	1. Click on the specific Indicator to review to open the Indicator Details page.

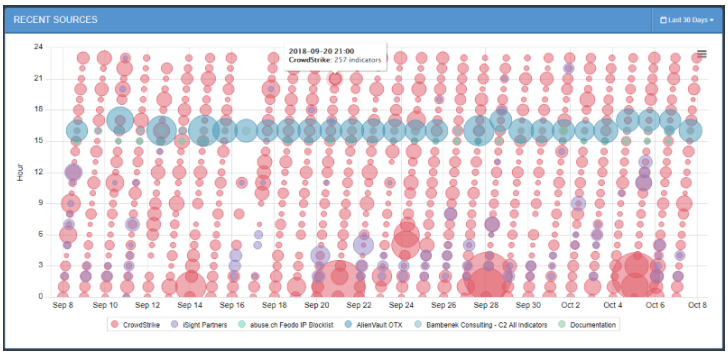
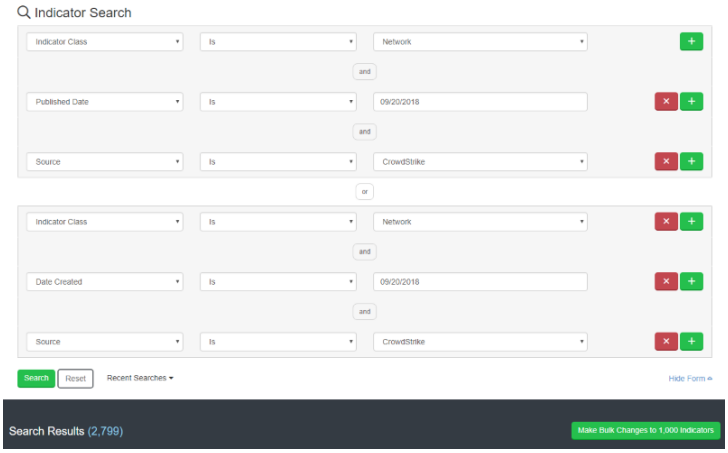
Recent Sources

The Recent Sources Scatter plot displays how many indicators were provided by a given source each day within a specified time frame.



The following functions are available:

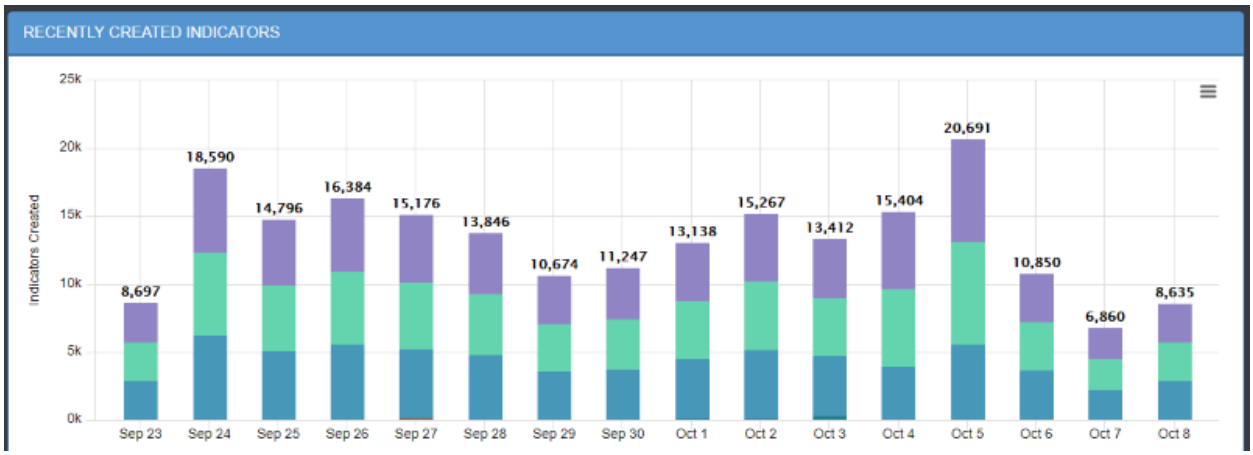
Function	Details
View the Date and Number of Indicators from a Given	1. Hover the mouse over one of the scatter plot circles to view a popup with the Source, Date, Time and

Function	Details
Source	Number of Indicators.  2. Click on the one of the scatter plot circles to open a filtered Indicator Search page with those values. 
Adjust the Date Range of the Information Displayed	The default date range is 30 days. 1. Click the date range icon located to the top-right of the chart and use the dropdown menu select the desired range. You can select from: • Last 24 Hours • Last 7 Days

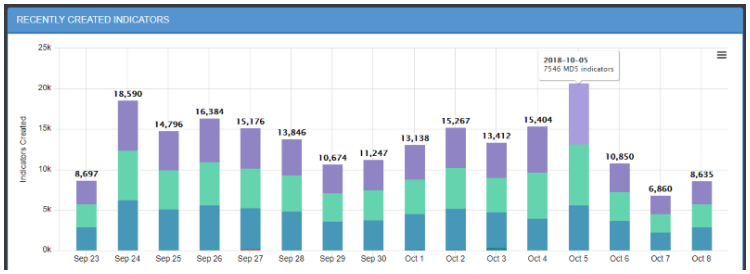
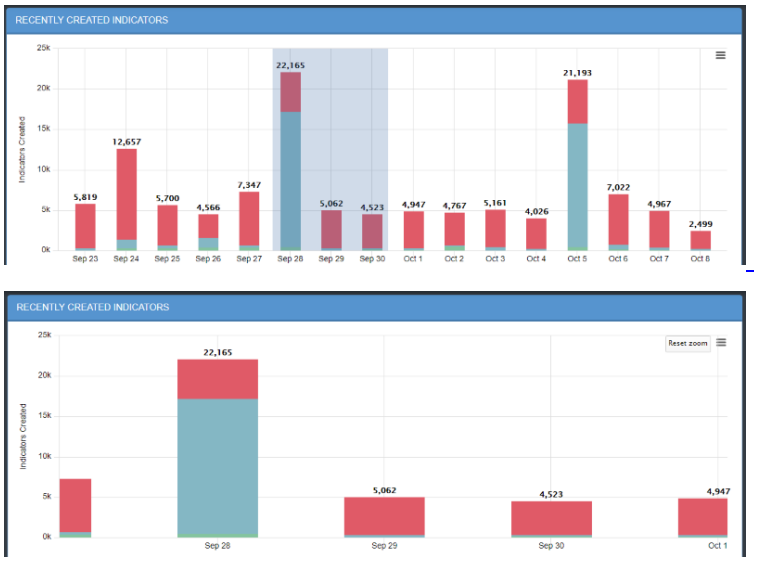
Function	Details
	• Last 30 Days • Last Year • User-set custom range
Hide Values from the Scatterplot	1. Click on a source in the legend under the scatter plot to hide it. The Source will be removed from the scatter plot and the source in the legend appear grayed out. 2. Click on the source again to add it back to the scatter plot.

Recently Created Indicators Histogram

The histogram is organized by date. Daily indicator totals are at the top of each column. Each bar is broken down into colors, one for each indicator type.



The following functions are available:

Function	Details
Viewing the number of indicators created each day by type	1. Hover over a colored section to view a popup showing how many attempts of a particular type (for example, MD5, SHA-1, SHA-256) were made on that date. 
Zooming in for a closer view	1. Drag your mouse over a section of the histogram, and your view will be magnified.  2. Click **Reset Zoom** to return to the full histogram.
Printing the histogram or downloading it as a PNG, JPEG, PDF, or SVG file	1. Click the hamburger menu ☰, and select the desired option.

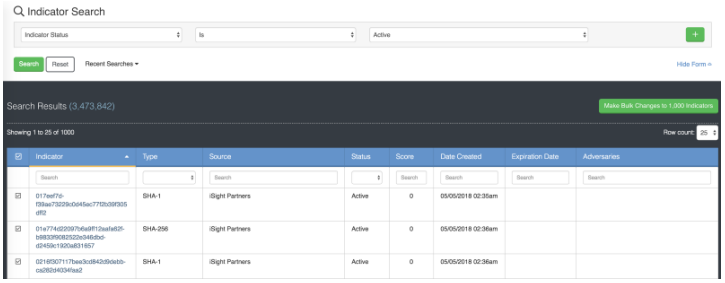
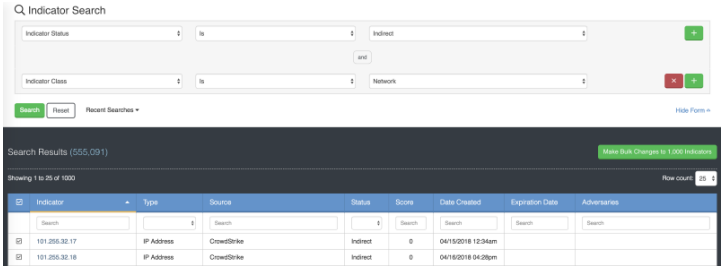
Summary Status

The Status Summary table is located under the Overview tab.

The Status Summary table provides a breakdown of Indicators, categorized by Status, for the Network and Host Indicator Classes.

Status	Network	Host	Total
Active	1,531,333	1,942,423	3,473,756
Expired	0	1	1
Indirect	555,091	176,729	731,820
Review	58	49	107
Whitelisted	0	0	0
Totals	2,086,482	2,119,202	4,205,684

The following functions are available:

Function	Details
Search By Indicator Status	1. Click on a Status to load the Indicator Search page with that status applied to the search. 
Search by Indicator Class or Indicator Class with a Specific Status	1. Click on an indicator value to load the Indicator Search page with the selected indicator class and status applied to the search. 

Signatures Overview

The Signatures page provides an overview of all the signatures within ThreatQ.

You can perform the following functions:

Function	Details
Filtering table by Date	1. Click within the search box at the top of the column, and enter your search criteria.
Opening the Signature Details page for an signature	1. Click the name in the Signature Title column.
Filtering table by Signature Type	1. Click the on dropdown at the top of the Signature Type column and select a type.
Changing the number of entries displayed in the table	1. Click the paging dropdown option located to the top-right of the table and select a value.
Sorting the table by a column	1. Click the column header. To reverse the column sorting order, click the header a second time.
Searching within the Signature Title column	1. Click within the search box at the top of the column, and enter your search criteria.

Incoming Feeds

The following describes how to use incoming feeds to ingest threat intelligence data.

Incoming Feeds Overview

You can enable and manage incoming feeds in ThreatQ to ingest threat intelligence data. Incoming feeds are organized into the following categories:

- Commercial
- OSINT or Open Source
- STIX/TAXII Feeds
- Labs

Commercial Feeds

Commercial feeds are provided by paid feed providers as a service. To enable these feeds in ThreatQ, you will need an API ID or API Key from the provider. Commercial feeds typically provide highly contextual threat intelligence data. You can learn more about these feeds on their vendor's websites.

OSINT Feeds

OSINT feeds are open source threat intelligence feeds. Open source feeds are free to use, but some may require you to register with the feed provider to attain an API Key.

STIX/Taxii Feeds

STIX stands for Standard Threat Information Expression, it is an emerging standard for the sharing of machine readable intelligence and incident data. A STIX package is an XML document that can contain many indicators and related context information. For the automated sharing of STIX packages, a protocol called TAXII (Trusted Automated eXchange of Indicator Information) is used to provide a feed to consumers.

ThreatQ provides a feature for consuming STIX/Taxii feeds.

Related Topic

Adding a New STIX/Taxii Feed

Labs Feeds

Labs (formerly known as ThreatQ Labs) are driven by ThreatQuotient's Threat Intelligence Services Team. Labs feeds provide a solution for data ingestion that is not provided by the feeds pre-configured with the ThreatQ platform. You should inquire with a Threat Intelligence Engineer to see what Labs are available.

Managing Incoming Feeds

Manage threat intelligence feeds on the Incoming Feeds page.

The following table describes the actions you can take to manage Incoming Feeds.

To	Do this..
Turn a feed on or off	Toggle the switch next to the feed name.
Editing a feed's display name or URL	Click **Feed Settings** for the feed you wish to edit, and make desired edits.

To	Do this..
Install/Upgrade Configuration Driven Feed (CDF)	See the Installing or Upgrading a CDF from the ThreatQ Interface topic.
Uninstall Configuration Driven Feed (CDF)	See the Uninstalling a CDF from the ThreatQ Interface topic.

Install/Upgrade CDF Command

The command below will allow you to install or upgrade a Configuration Driven Feed in your application. The command creates connectors for each feed defined in the feed definition file.

```
sudo /var/www/api/artisan threatq:feed-install
<Feed Definition File>
```

Upgrading Feed

The application will notify you if a feed in the feed definition file already exists in the system and will cancel the installation. You can add an **upgrade flag** to the command to allow the application to upgrade an existing feed.

```
threatq:feed-install 6266 Started > 2019-02-21 18:47:24
threatq:feed-install 6266 Command failed:
The provided definition file contains the following installed feeds:
Testing at 5 AM. Proceed with the update by using the --upgrade flag.
```

```
sudo /var/www/api/artisan threatq:feed-install
<Feed Definition File> --upgrade
```

This command can be used to update a feed's Category and Namespace. If the category exists on the appliance, the command will update both fields and link the feed to the designated category. ThreatQ will confirm that the defined category exists before completing the update command. If the category does not exist, ThreatQ will not update the feed.

Changes in User Configurations

When upgrading an existing feed using the **--upgrade flag**, the application will compare the existing version of the feed with the new version for differences in the user configuration. If a difference is detected, the application will inform you that the current user configuration for that feed will be overwritten. The application will require user input to continue with the feed upgrade.

```
threatq:feed-install 6674 Started > 2019-02-21 18:48:28
threatq:feed-install 6674 Warning: The provided definition file
contains updated user configurations. It is highly recommended to
create a copy of the configuration values for the following feeds
before proceeding with the update: Testing at 5 AM.
Do you want to continue? (Y/N) Y
threatq:feed-install 6674 Number of connectors in the definition file:
1
threatq:feed-install 6674 Number of existing connectors updated: 1
threatq:feed-install 6674 Finished > 2019-02-21 18:48:34 > 6.19s
```

It is recommended that you create a copy of the existing configuration values before proceeding with the upgrade.

Command Flag Help

You can also see a full list of command flags using the following command:

```
$ /var/www/api/artisan threatq:feed-install --help
```

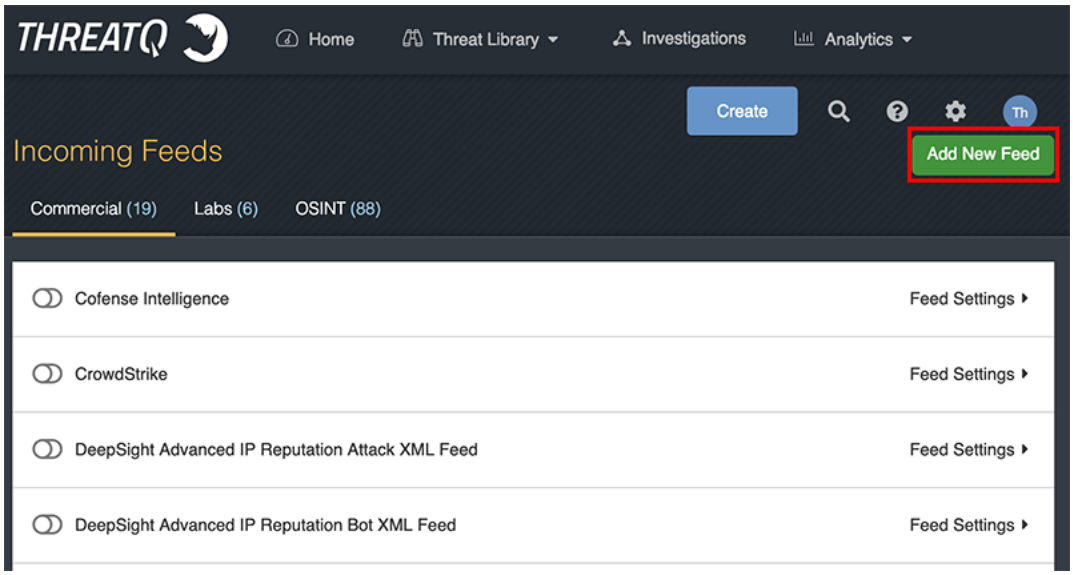
Installing or Upgrading a CDF from the ThreatQ Interface

You can install or upgrade a CDF from the **Incoming Feeds** page of the ThreatQ interface.

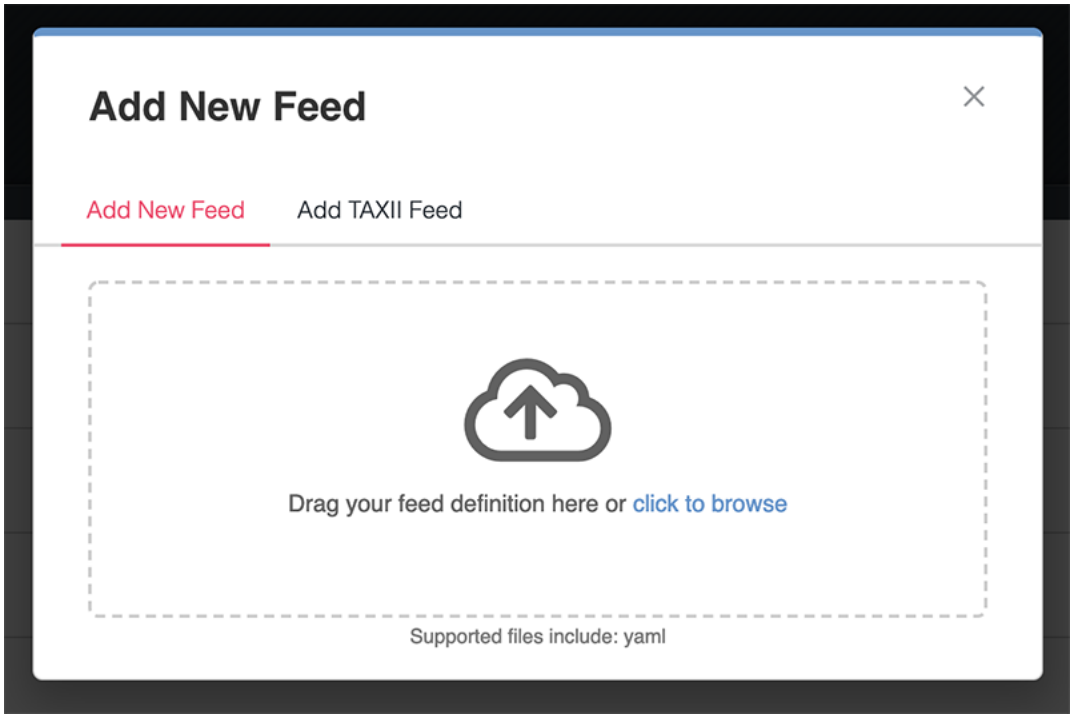
The process to upgrade a CDF is the same as installing a new CDF.

To install a CDF from the ThreatQ Interface:

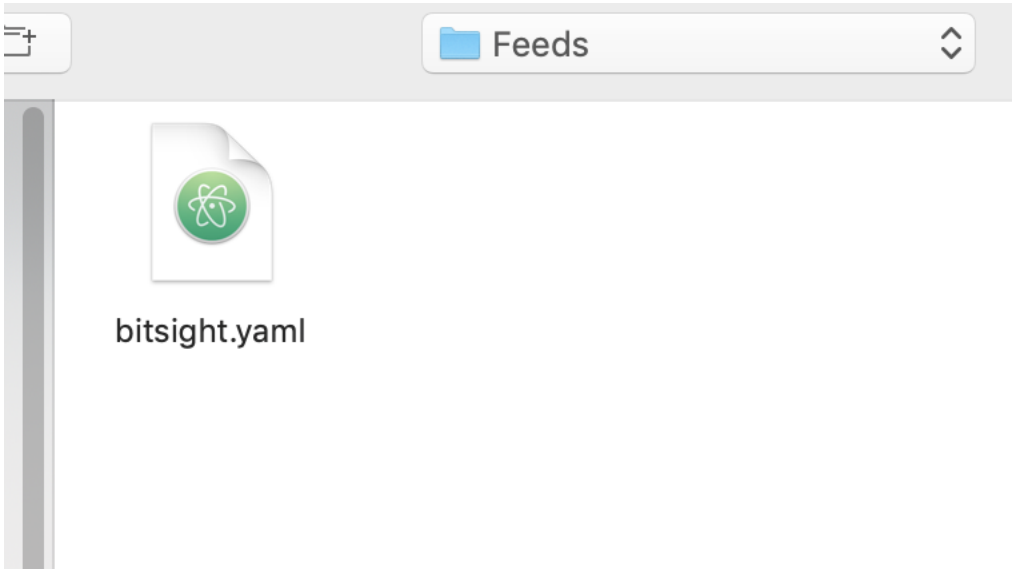
1. Go to **System Settings** > **Incoming Feeds**.
2. Click on the **Add New Feed** button.



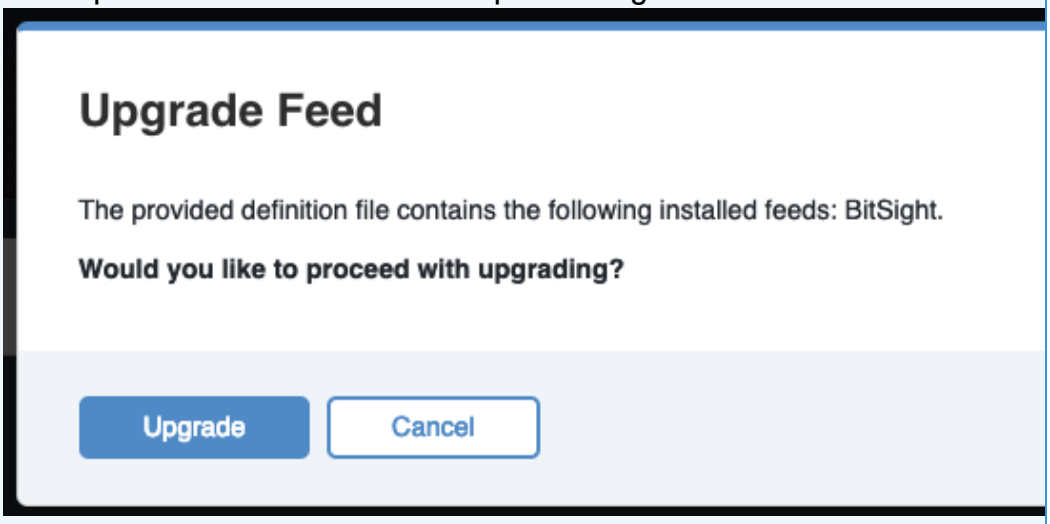
The Add New Feed dialog box opens.



3. Select the file to upload by either clicking and dragging the file onto the dialog box or using the link supplied to browse for the file on your local machine.

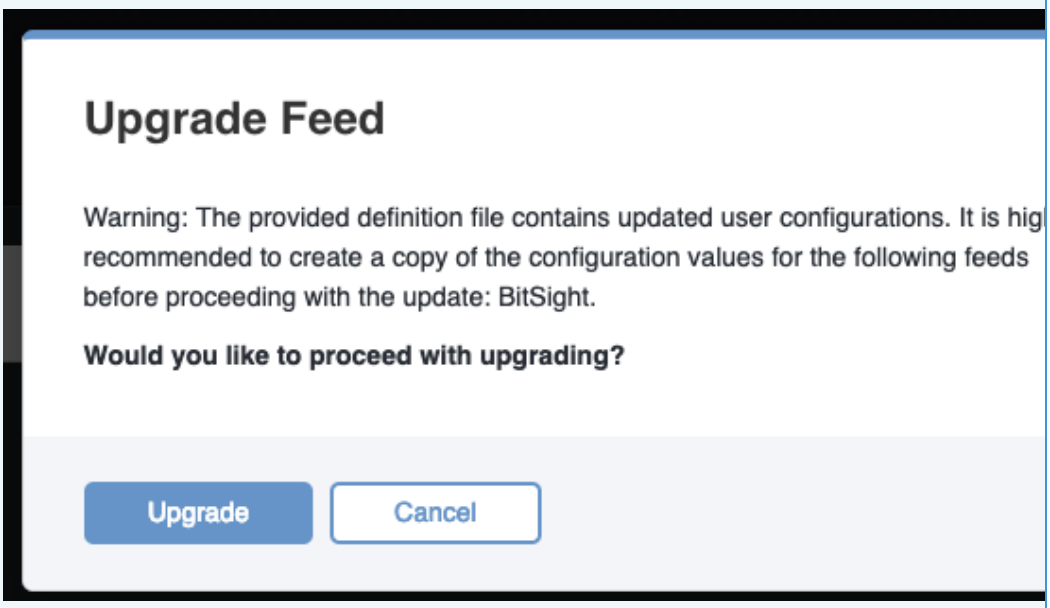


Existing Feeds
ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding.

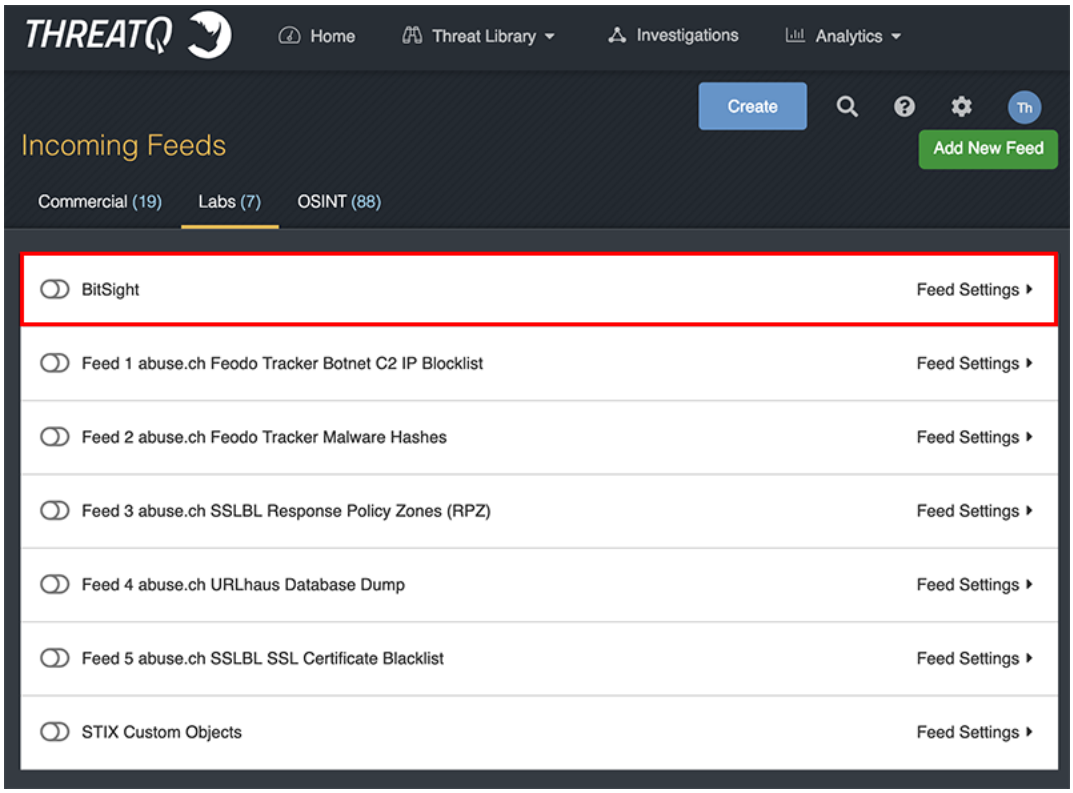


User Configurations
ThreatQ will also inform you if the new version of the CDF contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed. The platform will require

user confirmation before proceeding.



4. The new feed(s) will be installed.



You will need to configure and enable the feed after install.

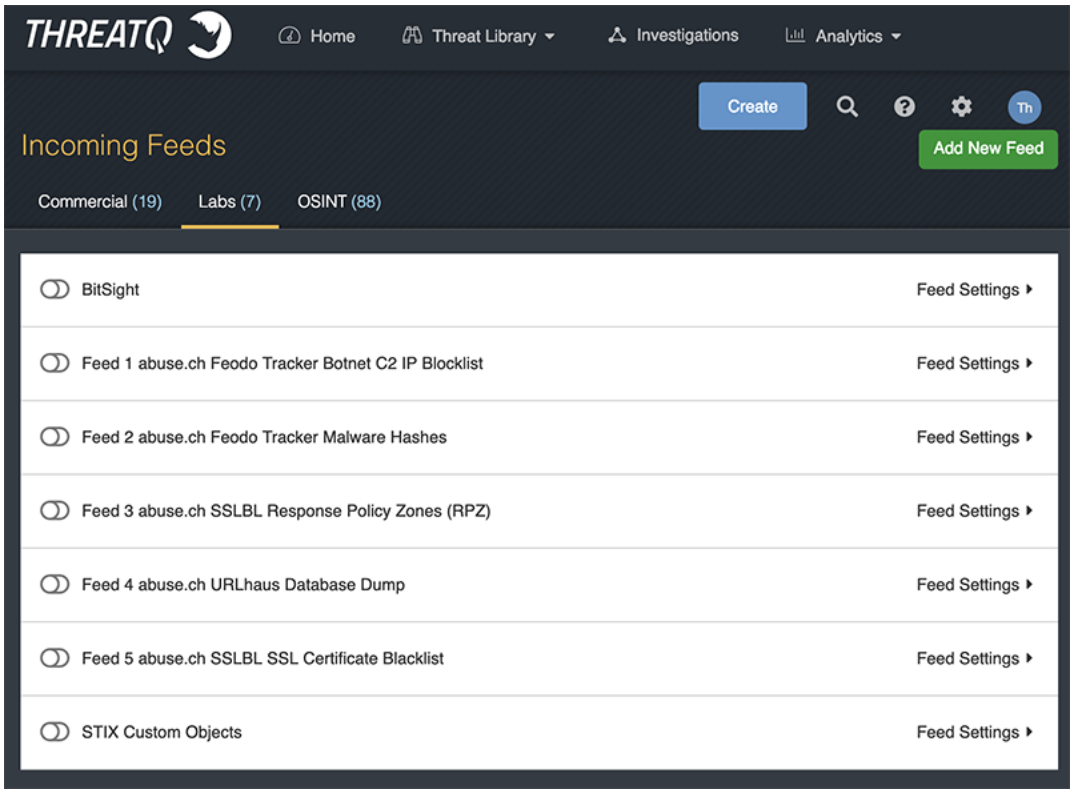
Uninstalling a CDF from the ThreatQ Interface

You can uninstall CDFs from the **Incoming Feeds** page of the ThreatQ interface.

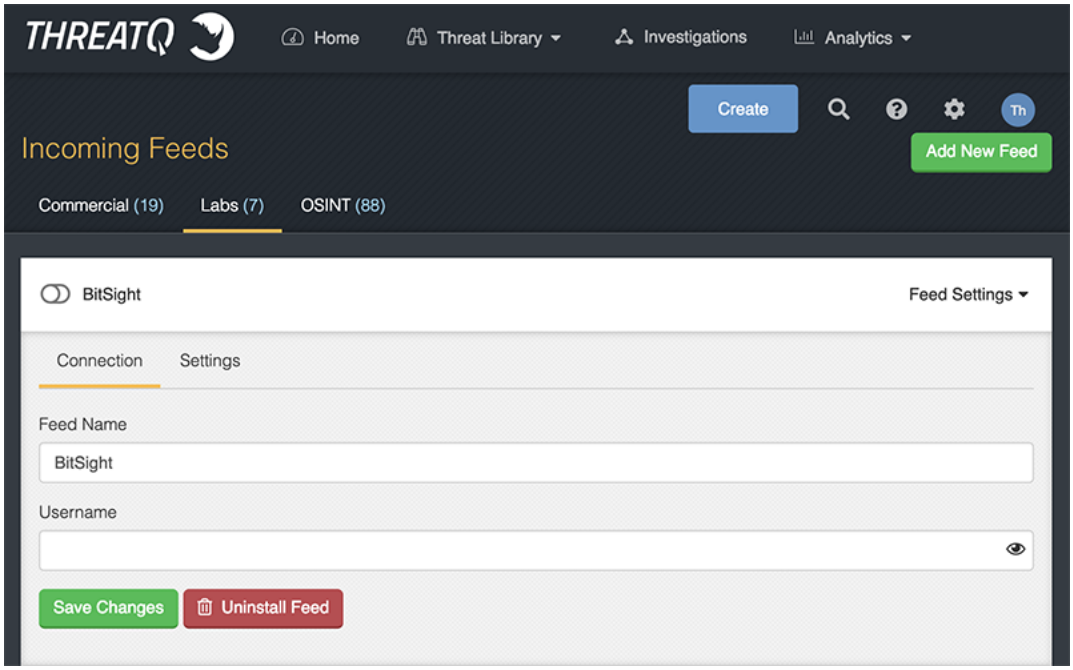
This feature only applies to CDFs.

To uninstall a CDF from the ThreatQ Interface:

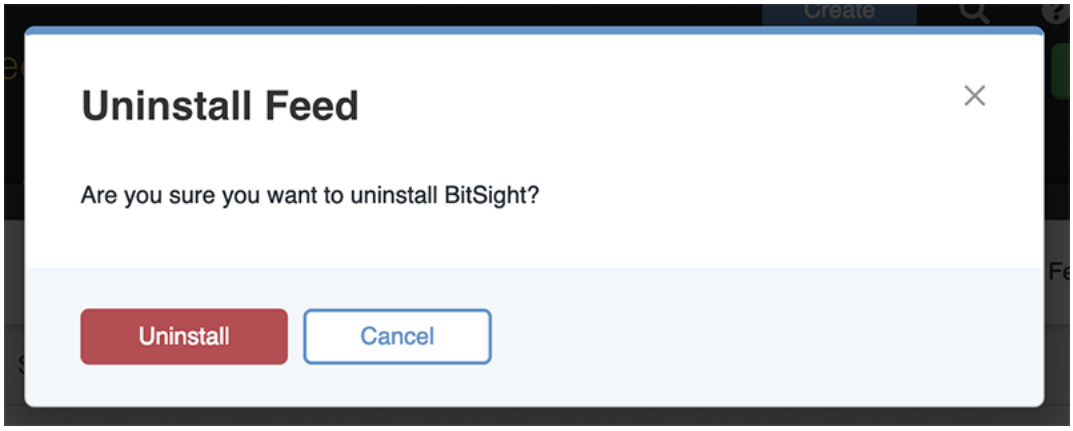
1. Go to **System Settings** > **Incoming Feeds**.
2. Click on the **Feed Settings** link for the feed.



3. Click on the **Uninstall Feed** button.

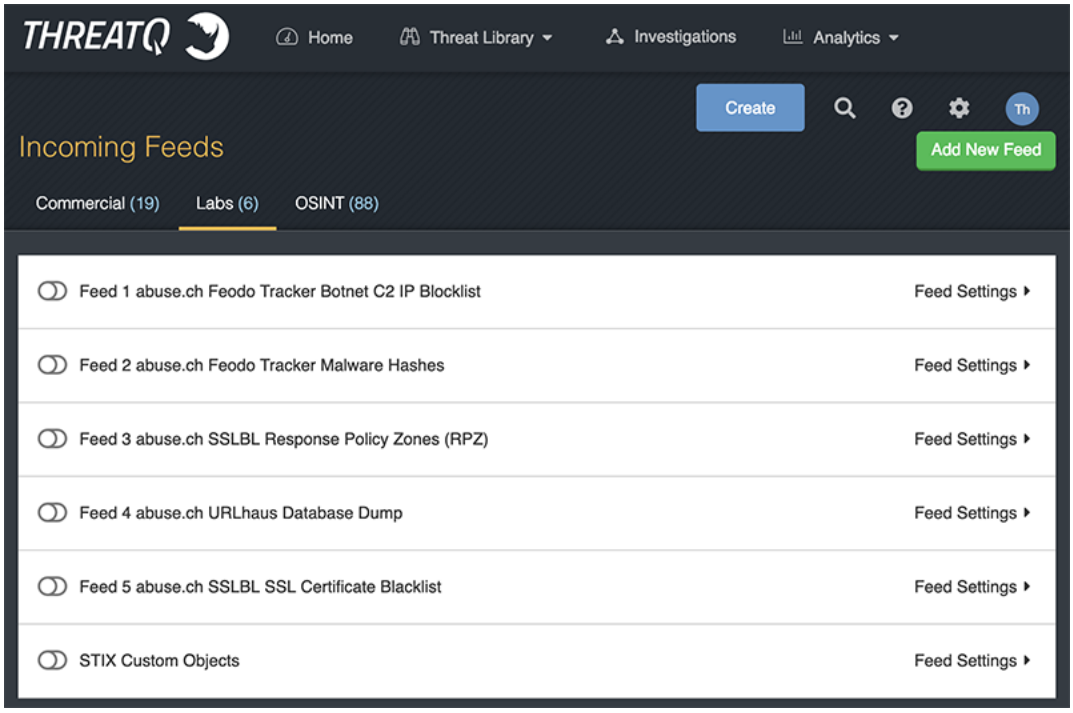


The Uninstall Feed dialog box opens.



4. Click on **Uninstall**.

5. The feed will be uninstalled.



Enabling a Commercial Feed

To enable a commercial feed, you will need an API ID and API Key provided by the feed provider.

Procedure:

1. Choose the **Settings icon > Incoming Feeds**.
2. Click the toggle switch next to the feed you want to enable.

   Green indicates enabled.

3. Expand **Feed Settings**.
4. On the Connection tab, enter:
   - Feed Name - the name displayed in ThreatQ
   - API ID - provided by the feed vendor for authorization

- API Key - provided the feed vendor for authorization
- Feed URL - this field is autofilled

5. On the Settings tab, select:
   - the status that incoming indicators from this feed will receive.
   - the frequency that ThreatQ pulls information from the feed.
6. Click **Save Changes**.

Enabling an OSINT Feed

OSINT feeds do not require API IDs, but some may require an API key from the feed provider.

Procedure:

1. Choose the **Settings icon > Incoming Feeds**.
2. Click the toggle switch next to the feed you want to enable.

   Green indicates enabled.

3. Expand **Feed Settings**.
4. On the Connection tab, enter:
   - Feed Name - the name displayed in ThreatQ
   - API Key (if required) - provided the feed vendor for authorization
   - Feed URL - this field is autofilled
5. On the Settings tab, select:
   - the status that incoming indicators from this feed will receive.
   - the frequency that ThreatQ pulls information from the feed.
6. Click **Save Changes**.

Viewing Feed Queues

When upgrading a feed, it is recommended to allow the previous implementation the feed to complete processing of the data it has already downloaded, prior to upgrade, to avoid any data loss.

Perform the following steps to confirm that the queues have been cleared.

1. Run the following command:

```
/var/www/api/artisan threatq:list-queues -p
feeds
```

2. Locate and confirm that the feed's Indicators and Reports rows display a value of "0" for the Messages Ready and Messages Unacknowledged columns.

The queues should be cleared, reporting 0 values, before proceeding with the update.

Adding a New STIX/Taxii Feed

Complete the following steps to add a new STIX/TAXII indicator feed.

Procedure:

1. Choose the **Settings icon > Incoming Feeds**.
2. Choose **Add New Taxii Feed**.
3. **What would you like to name this feed?** Enter the feed name that will be displayed throughout ThreatQ. It does not need to match the Collection Name.
4. **How often would you like to pull new data from this feed?** Choose **Every Hour** or **Every Day**.
5. Enter the **Discovery URL** where the TAXII server can be reached.

6. Optionally, enter a **Poll URL**.
7. Enter the **Collection Name**, which is the name of the collection of data on the feed you would like to access.
8. If required for the feed, under Login Credentials, enter a **Username** and **Password**.
9. If required for the feed, under Certificates/Keys, enter a **Certificate** and **Private key**.
10. Choose **Add TAXII Feed**.

CrowdStrike CDF

Starting with ThreatQ version 4.2, the CrowdStrike feed will be updated to use the configuration driven method. This update will allow users to review an Activity Log that will provide a summary of the feed and including important details such as:

- how the feed was triggered,
- start and completion time,
- raw response received from the vendor,
- how many objects were processed by ThreatQ.

Query Range

Query Range is a new feature with this update that uses the exact date/time that ThreatQ queried CrowdStrike's API for information.

This feature, unique to the updated CrowdStrike feed, ensures that there isn't a gap in feed coverage in the event of a feed run failure or server downtime. ThreatQ will use the last completed run time when performing a new run.

Example: *Customer has CrowdStrike configured to perform scheduled runs every hour. The customer powers down the server for three hours for maintenance. The next time the feed runs, it will automatically use the last successful run time in its range which will cover the three-hour gap when the server was down.*

PlaceHolder Files

The Placeholder file concept is currently used by the updated CrowdStrike feed with expanded support to other feeds to be added in future releases. Placeholder files prevent linking information delays between the vendor and ThreatQ by creating a placeholder file immediately after receiving a file or report from the vendor. ThreatQ will fulfill the placeholder and update the object information accordingly. ThreatQ will mark placeholder files on the details and file overview pages.

Related Information

- CrowdStrike Update Instructions
- Performing Manual Feed Runs

CrowdStrike Update Instructions

CrowdStrike users must update their proxy server settings to use http: for their https: traffic before upgrading CrowdStrike.

Prior to upgrade, and to avoid any data loss, it is recommended to allow the previous implementation of CrowdStrike to complete processing of the data it has already downloaded.

Perform the following steps to confirm that the queues have been cleared.

1. Run the following command:

```
/var/www/api/artisan threatq:list-queues -p
feeds
```

2. Locate and confirm that the **CrowdStrike Indicators** and **Reports** rows display a value of "**0**" for the **Messages Ready** and **Messages Unacknowledged** columns.

The queues must be cleared, reporting 0 values, before proceeding with the update.

3. Proceed with the standard feed update procedures.

The update process is quick. A confirmation message will confirm that the update process is complete. The **Activity Log** feature will load once CrowdStrike is enabled and a feed run instance has been created or completed.

Source Consolidation Command

Use the command below to consolidate/deduplicate similarly named sources and to remove unused sources from the ThreatQ application. A source that have been removed or merged will have its data mapped to a new source.

The command does not require recalculation of scoring.

```
sudo /var/www/api/artisan threatq:consolidate-
sources
```

Example Scenario:

1. User manually adds ABC as a source.
2. User enables ABC.

   There are now two ABC sources in the system.

3. User runs consolidation command.
4. The application merges the sources and remaps any items linked to the correct source.

Source Merge Command

Use the command below to merge a user-created source (source origin) with another source (source destination). After merging, the source origin will be deleted and source changes will be reflected in the Audit log (Example: Source A become Source B).

The platform must be placed into **Maintenance Mode** before running the Source Merge Command.

The command does not affect date stamps nor does it require a recalculation of scoring.

```
sudo php artisan threatq:merge-sources --origin-source="<source a>" --destination-source="<source b>"
```

Example Scenarios:

Scenario	Details
Merge user-created source (origin source) with a system source (destination source).	1. User places the platform into Maintenance Mode. 2. User runs Source Merge command. 3. User is presented with merge confirmation dialog. 4. User consents to the merge. 5. The platform will merge the origin source into the destination source and then delete the origin source after completion. 6. The platform will record the source merge in the audit log for affected data. 7. The user receives a command success message.

Scenario	Details
	8. The user brings the platform out of Maintenance Mode.
Merge system source (origin source) with a user-created source (destination source).	1. User places the platform into Maintenance Mode. 2. User runs Source Merge command. 3. The platform will inform the user that a system source cannot be merged into another source. 4. The user brings the platform out of Maintenance Mode.
Merge user-created source (origin source) with a system source (destination source) with duplicate records.	1. User places the platform into Maintenance Mode. 2. User runs Source Merge command. 3. The platform will inform the user that there are duplicate records between the two sources and prompt the user to run the Source Consolidation Command before proceeding with the merge. 4. User runs the Source Consolidation command. 5. User runs Source Merge command. 6. User is presented with merge confirmation dialog. 7. User consents to the merge. 8. The platform will merge the origin source into the destination source and then delete the origin source after completion. 9. The platform will record the source merge in the audit log for affected data. 10. The user receives a command success message. 11. The user brings the platform out of Maintenance Mode.
Merge user-created	1. User places the platform into Maintenance Mode.

Scenario	Details
source (origin source) with a system source (destination source) with an assigned TLP.	2. User runs Source Merge command. 3. User is presented with merge confirmation dialog. 4. User consents to the merge. 5. The platform will merge the origin source into the destination source, and then delete the origin source after completion. 6. The platform will then apply the destination source's default TLP settings to the merged data and record the source merge in the audit log for affected data. 7. The user receives a command success message. 8. The user brings the platform out of Maintenance Mode.

Feed Activity Log

The feed activity log summarizes each feed run, including information such as how the feed was triggered, its start time, completion time, the raw response received from the feed vendor, and how many objects were processed.

The Activity log is currently available for the following Configuration-Driven Feeds (CDF):

Commercial Feeds

- CrowdStrike
- Cofense Intelligence (formerly known as Phishme Intelligence)

OSINT Feeds

- AlienVault OTX
- All abuse.ch feeds, except for abuse.ch SSBL (Extended)
- Bambenek
- BitSight
- CI Army List IPs
- Cybercrime Tracker
- Emerging Threats Compromised IPs
- malc0de Domain
- malc0de IP
- Malware Domain List (IP)
- Malware Patrol
- Phishtank

Viewing a Feed's Activity Log

To view a feed's activity log, that feed must be enabled.

Procedure

1. From the main menu, choose the **Settings icon > Incoming Feeds**.
2. Choose a feed and expand **Feed Settings**.
3. Choose the **Activity Log** tab.

Historic Feed Pulls

Historic pulls provide a method for you to ingest threat intelligence data from a particular vendor prior to the date you enabled the incoming feed. The procedure for running historic feeds varies based on the type of feed.

See the following topics for more information:

Feeds that do not Support Historic Pulls

The following feeds do not support historic pulls:

- All OSINT feeds
- The following Commercial Feed:
  - DeepSight

Performing Manual Feed Runs

For some feeds, you can perform a manual feed run for a selected date range. This allows you to generate a historic feed pull from the user interface.

You can perform a manual feed run for the following feeds:

- CrowdStrike

Procedure:

1. From the main menu, choose the **Settings icon > Incoming Feeds**.
2. Select a feed and expand **Feed Settings**.
3. Click **+Manual Run**.
4. Select a **Start Date**, **Start Time**, and **Time Zone** for your run.
5. Select an **End Date**, **End Time**, and **Time Zone** for your run.
6. Click **Queue Run**.

iSight Historic Pull Command

To run an iSight historic pull, run the following command from the command line, substituting your desired start and end date:

```
sudo isight_connector -s MM-DD-YYYY -e MM-DD-YYYY
```

General Historic Pull Commands

If not called out specifically in Historic Feed Pulls, use the following commands at the command line to run historic pulls for most other connectors, including most TAXII feeds.

1. Run the following command to determine the feed name ($FEEDNAME):

   ```
   tqconnector -h
   ```

   Take note of the desired feed name.

2. Run the following command to run the historic pull, substituting your desired start and end date:

   ```
   sudo -u threatq tqconnector -f $FEEDNAME -s MM-DD-YYYY -e MM-DD-YYYY
   ```

Threat Intelligence Services Custom Feeds Historic Pull Commands

Custom feeds provided by Threat Intelligence Services provide a mechanism for you to generate a historic pull during the initial feed run. After the initial feed run, feeds typically perform an hourly pull, but can be adjusted within cron.

Refer to the documentation for your custom feed or integration for more information.

Dashboard

The following describes how to use the dashboard to view various threat intelligence metrics.

Dashboard Overview

Dashboard Overview

The Dashboard displays metrics and visualizations to provide at-a-glance views of your threat intelligence data, including:

- Overview of intelligence by score
- Watchlist activity
- Incoming intelligence
- Open assigned tasks

The dashboard serves as your landing page when you log in to ThreatQ.

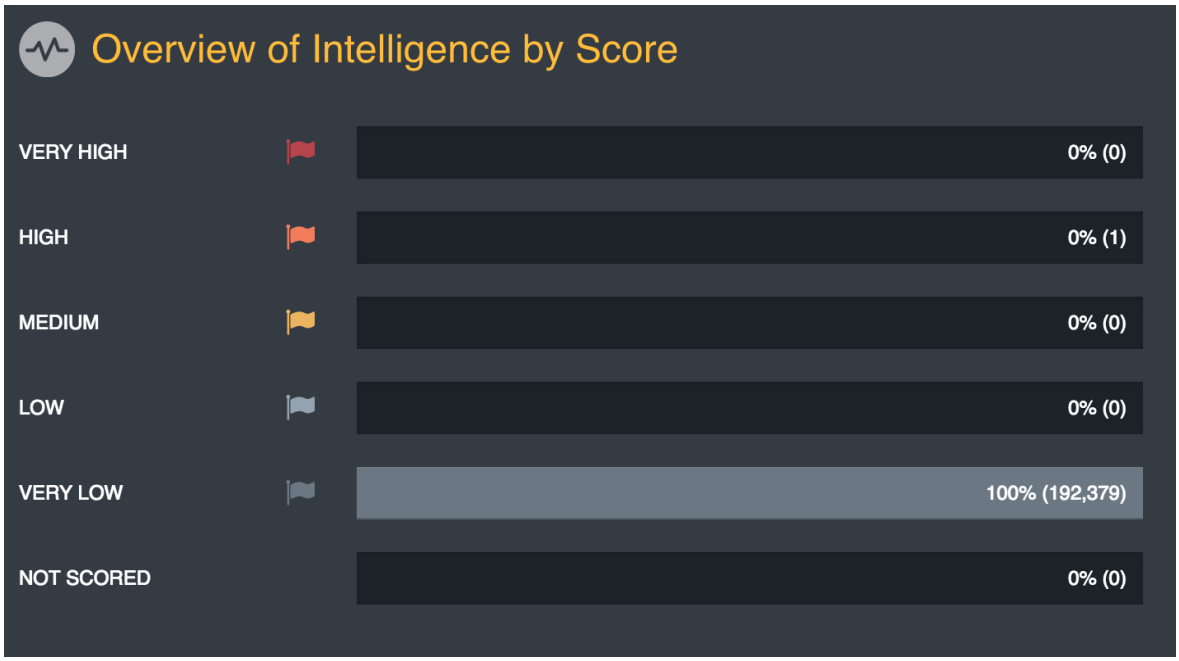
Overview of Intelligence By Score

This dashboard graph provides a summary of indicator scoring in the system. It lists total indicators by score in the following order:

- Very High
- High
- Medium
- Low

- Very Low
- Not Scored

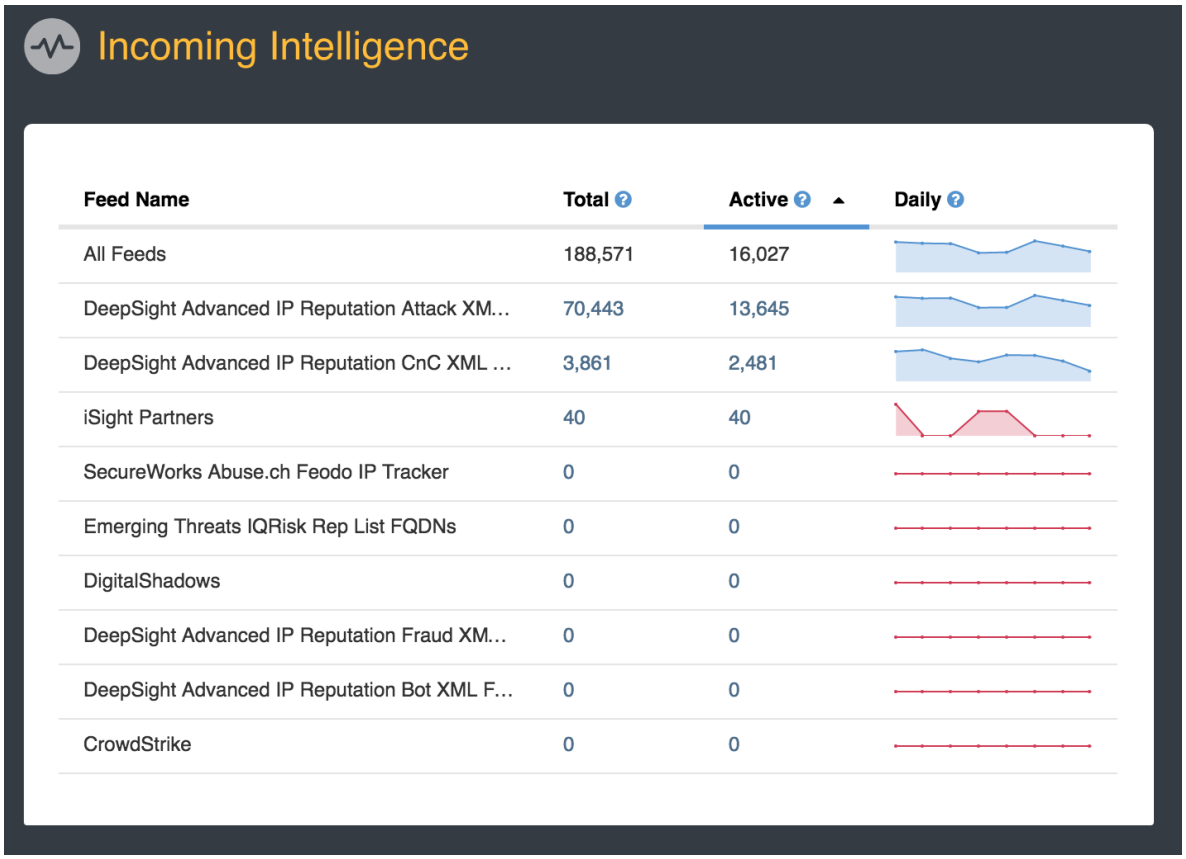
You may click on the percentage/number of indicators to launch an indicator search based on that criteria.



Incoming Intelligence

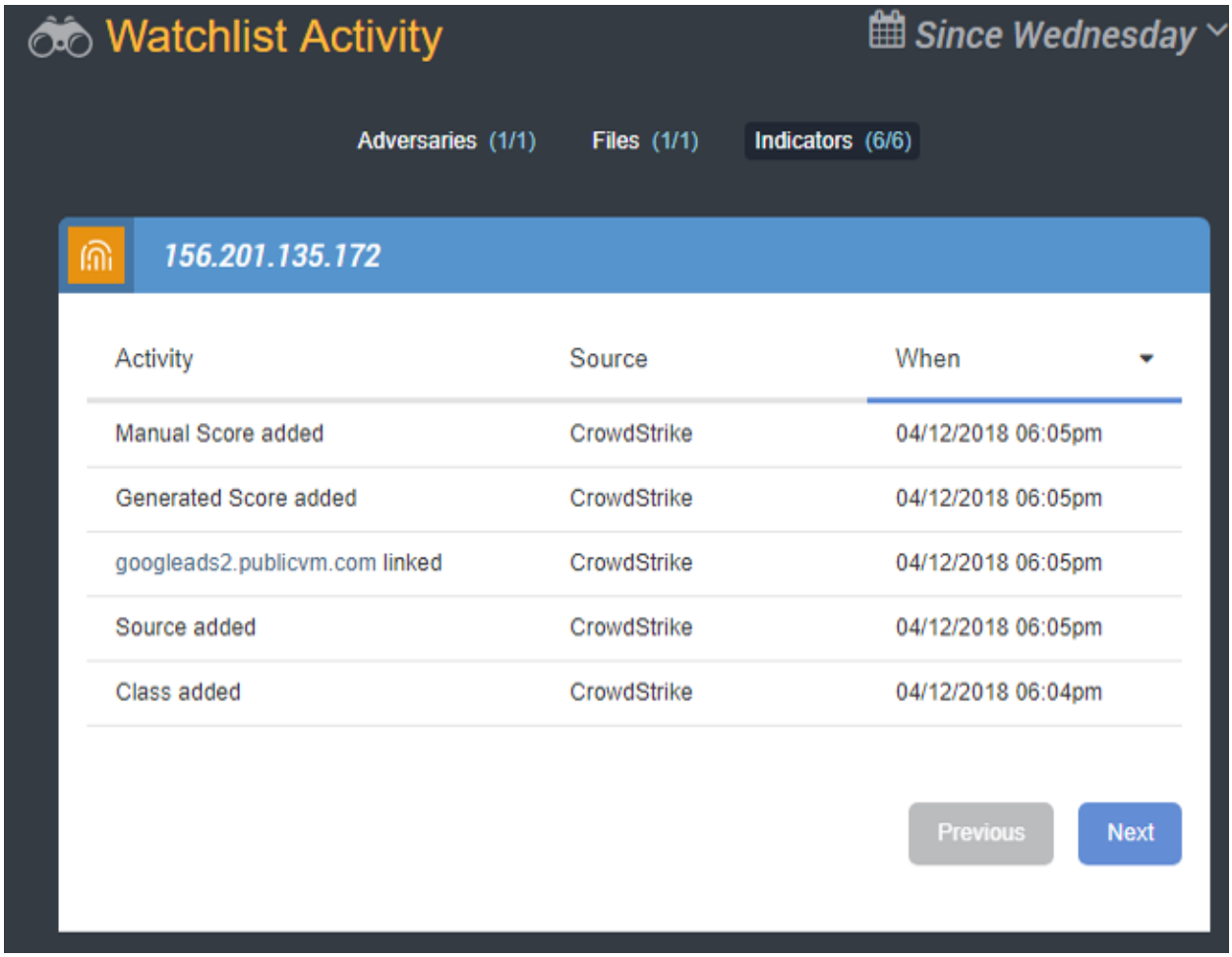
This dashboard graph provides a view of threat intelligence from all incoming feeds. The system categorizes threat intelligence by:

- Feed Name
- Total number of indicators reported by a source
- Indicators reported by a source with a status of active
- All indicators reported by a source per day (includes existing indicators)



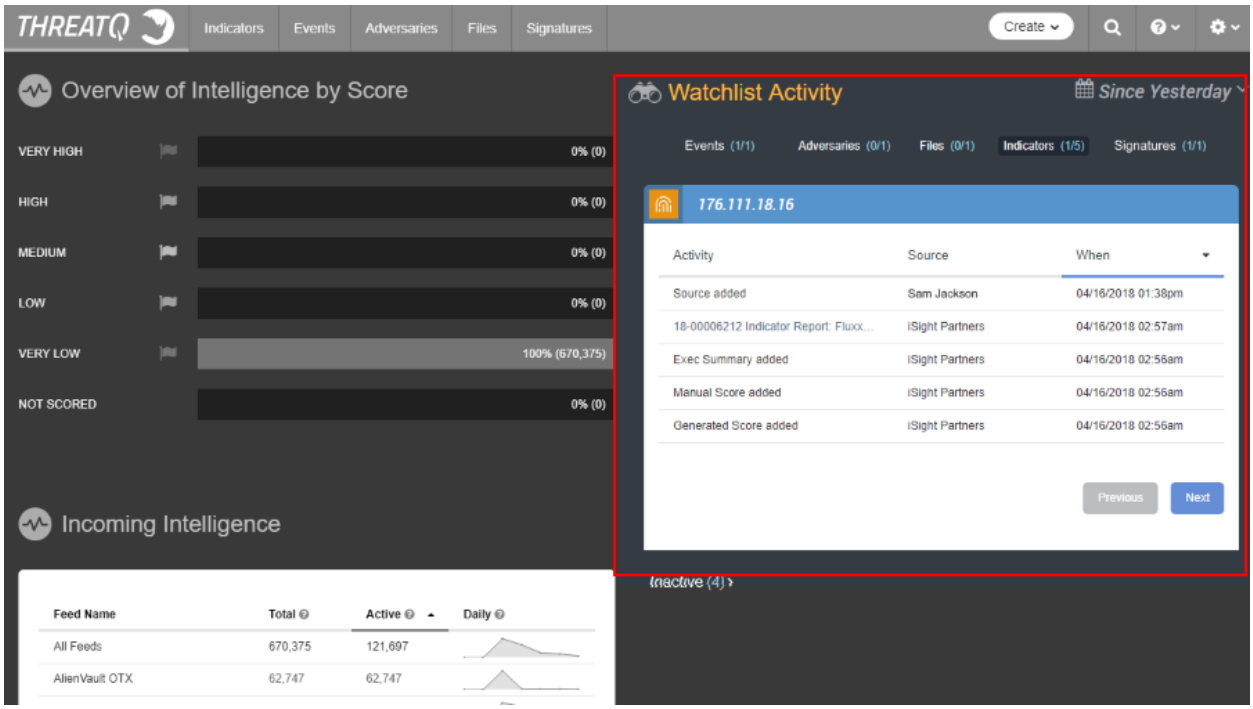
Watchlist Activity

This dashboard section provides a view of the intelligence data that you selected to watch. You may click on any accompanying link to view the details page of the item being watched.



Watchlist

The Watchlist allows you to track threat intelligence data and user activity of interest from a view on the dashboard.

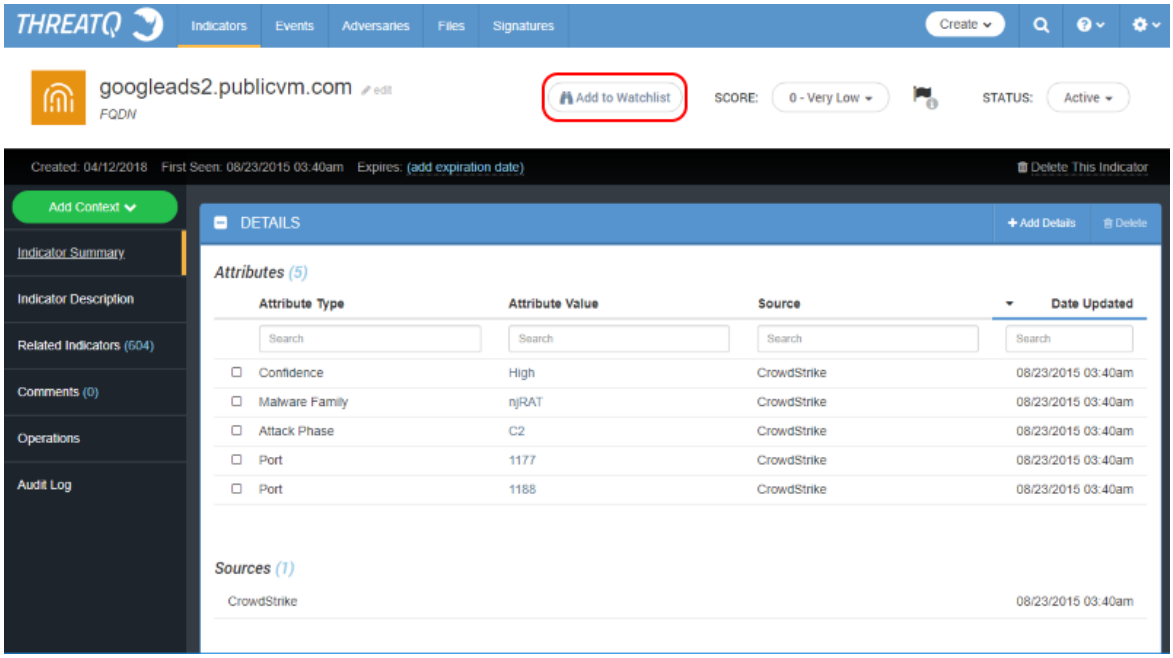


Configuring the Watchlist

To create a watchlist that displays on the dashboard, complete the following steps:

1. From the ThreatQ user interface, navigate to the Details page of the indicator, event, adversary, file, or signature you want to track.

2. Click **Add to Watchlist** to track that item.



3. Return to the dashboard to view your watchlist.

Viewing Tasks on the Dashboard

This dashboard widget provides a view of all open tasks in the platform. You can view your open tasks or view all open tasks. Tasks on the dashboard are categorized by:

- Task ID
- Task Name
- User the Task is Assigned To
- Due Date
- Status.

Search

The following describes how to search for indicators and other objects using ThreatQ's search features.

- Search Overview
- Wildcards and Symbols in Searches

Search Overview

Search allows you to find objects you are looking for quickly, without having to browse through a large number of objects. There are three search features in ThreatQ:

- Basic Search, which offers a quick method to search if you know exactly what you are looking for.
- Advanced Search, which gives you more options for limiting your search.

  The advanced search also serves as the primary interface for the Threat Library.

- Indicator Search, which served as the legacy advanced search prior to ThreatQ version 4.0.

Using these varieties of search, you can create as broad or as granular a view of your data as desired.

For more information, see:

- Basic Search
- Advanced Search

- Indicator Search

Basic Search

Basic Search allows you to search for all objects in the system: indicators, events, adversaries, files, signatures, and so on. The search capability looks at high level aspects of each object, including:

- Indicators (network or host)
- Attachment titles, hashes, keywords
- Attributes
- Adversary name
- Event title

  If searching for *google.com*, the following indicators will also be returned:

  - www.google.com (FQDN)
  - analytic.google.com (FQDN)
  - www.google.com/analytic (URL)
  - analytic@google.com (email address)

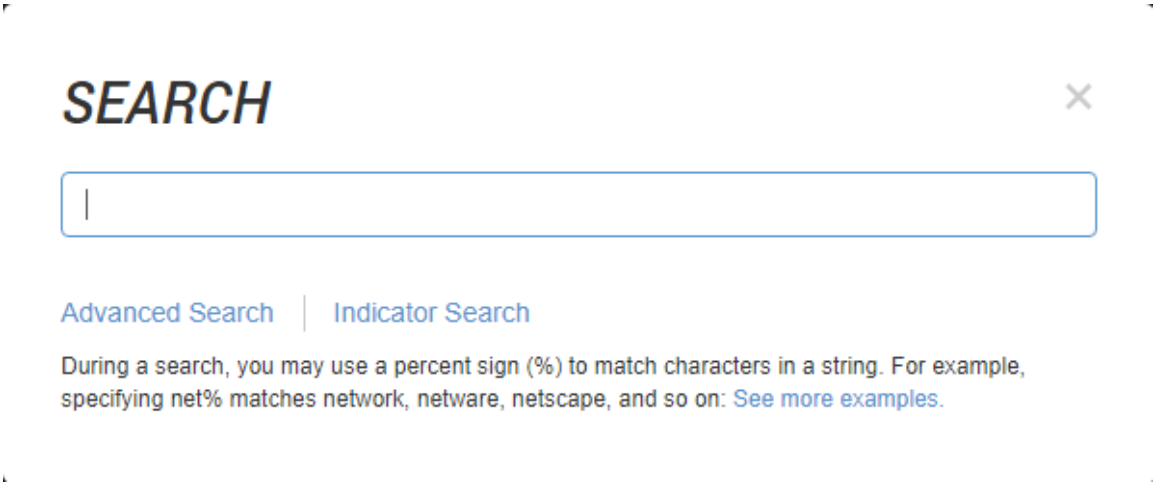
Related Topics:

- Performing a Basic Search
- Wildcards and Symbols in Searches

Performing a Basic Search

Procedure:

1. Choose the Search icon.



   The Search dialog box appears.
2. Enter the search criteria.
   The Search field provides type ahead suggestions, if any, based on what you have typed.
3. Select the desired result.
   - If you do not retrieve any search results, we recommend trying the EnhancedAdvanced Search.
   - If there is only one result, the object details page appears.

Wildcards and Symbols in Searches

During a search, you may use a percent sign (%) to match characters in a string. The percent wildcard specifies that any characters can appear in multiple positions represented by the wildcard. For example, specifying net% matches network, netware, netscape, and so on.

Here are a number of examples showing search terms with percent wildcards:

Search Query	Description
% panda	Finds any adversaries and indicators with <name> panda
%ear	Finds any character string that ends with "ear," such as bear
%panda%	Finds any character string that has panda in any position
panda%	Finds any character string that begins with panda
pan%a	Finds any character string that has pan in the first three positions and ends with an "a"

Reports

The following describes how to generate reports in ThreatQ.

Reports Overview

You can export a PDF Summary of an object from an object's details page.

The generated PDF may contain active links to internal and external locations. Related objects in the PDF link to an internal ThreatQ instance that may require authentication. Please be aware of potential impacts before distribution of the generated report.

Google Chrome's pop-up blocker prevents object PDF summary reports from downloading. We recommend changing your browser settings to allow pop-ups from your ThreatQ instance.

Report Options

You can navigate to **Settings > Report Options** to customize the PDF reports that are generated. Report options apply to all reports generated platform-wide. You can make the following customizations:

- Customizing Report Text Colors
- Adding a Custom Disclaimer to a Report

Previewing Report Customization

You can preview report customization to view a representation of a report's output.

Procedure:

1. Select the **Settings** icon > **Report Options**.
2. Under Customized PDF Reports, click **Preview**.

   The sample report downloads to your computer.

Customizing the Report Header

Complete the following steps to add a custom header to your PDF.

Procedure:

1. Select the **Settings** icon > **Report Options**.
2. Under **Header Banner**, complete one of the following steps:
   - Drag and drop the image you want to use as the header.
   - Click **Browse** and navigate to the image you want to use as the header.
3. Optionally, click **Restore header banner to defaults**.
4. Click **Save**.

Customizing Report Text Colors

Complete the following steps to customize the colors in your PDF.

Procedure:

1. Select the **Settings** icon > **Report Options**.
2. Under **Colors**, use the drop down menus to select:
   - Header Text
   - Heading Text
   - Body Text
3. Click **Save**.

Adding a Custom Disclaimer to a Report

You can add a custom disclaimer to include with your report to communicate any liabilities or limitations to the end users of the report.

Procedure:

1. Select the **Settings** icon > **Report Options**.
2. Under **Disclaimer**,enter your disclaimer text and then use the formatting tools to customize your message.
3. Click **Save**.

Generating Reports

Complete the following steps to export a PDF Summary of an object from an object's details page.

Procedure:

1. Access the object's detail's page for which you want to generate a report summary.
2. Select **Actions > Generate PDF**.

   The PDF summary downloads and opens in a new browser tab.

Google Chrome Users: Google Chrome's pop-up blocker prevents object PDF summary reports from downloading. We recommend changing your browser settings to allow pop-ups from your ThreatQ instance. See Turning Off the Pop-up Blocker in Chrome for more information.

The generated PDF may contain active links to internal and external locations. Related objects in the PDF link to an internal ThreatQ instance that may require authentication. Please be aware of potential impacts before distribution of the generated report.

Turning Off the Pop-up Blocker in Chrome

This topic applies to ThreatQ version 4.7

By default, Google Chrome blocks pop-ups from automatically showing up on your screen. When a pop-up is blocked, the address bar will display a pop-up blocked alert. This pop-up blocker will prevent your PDF from being downloaded. Complete the following steps to allow pop-ups from ThreatQ.

Procedure:

1. Go to ThreatQ where pop-ups are blocked.
2. In the address bar, click the **Pop-up blocked** alert icon.
3. Click the link for the pop-up you want to see.
4. To always see pop-ups for the site, select Always allow pop-ups from [your ThreatQ instance].
5. Click **Done**.

Tasks

The following describes how to manage tasks in ThreatQ.

Tasks Overview

ThreatQ allows you to create and assign tasks to yourself or other users in the platform.

Once tasks are included in your deployment, you can add contextual information and correlate them with Indicators, Events, Adversaries, Signatures, and Files. You can also add comments, change the task priority, change the task status, and delete the task.

Assigning a Task

Complete the following steps to assign a task in ThreatQ.

1. From the main menu, choose **Create > Task**.

   The Add Task dialog box opens.

2. Enter a task **Name**.
3. Enter the assignee's email address in the **Assigned To** field.
4. Optionally, use the date picker to select a **Due Date**.
5. Select one of the following statuses:
   - To Do
   - In Progress

- Review
- Done

6. Select one of the following task priorities:
    - Low
    - Medium
    - High
7. Optionally, enter any **Associated Objects**.
8. Enter a **Description** for the task.
9. Click **Save**.

Managing Tasks

After a task is created, you can manage it on the task's Details page.

The following table describes the actions you can take to manage your tasks on a Task Details page.

To	You can...
Change task priority	Choose the **Priority** drop-down and select a new priority.

To	You can...
Change task status	Choose the **Status** drop-down and select a new status.
Add Attributes, Comments, Relationships, and Sources	Choose the **Add Context** drop-down and select an item.
View and Add Comments	Choose **Comments**.
View the Audit Log	Choose **Audit Log**.

Operations

The following explains how to configure and manage operations.

Operations Overview

Operations enhance your threat intelligence data by allowing you to add attributes, as well as related indicators, from third party security services, both commercial and open source. You accomplish this by creating objects to connect to a desired service, receive threat intelligence, and display that threat intelligence in ThreatQ.

To develop custom operations, you should possess a basic functional knowledge of Python version 3 development. In ThreatQ version 3.0 and later, you can create operations for:

- Indicators
- Events
- Adversaries
- Files
- Signatures

ThreatQ operations are written in Python v3.5.2. We recommend allocating a non-production ThreatQ appliance for Operations development. You may use this development appliance to troubleshoot your operations before deploying them to production. You may also set up a local Python environment, write your script, and then copy it onto your ThreatQ appliance.

Installing Operations

You can install Operations from the user interface, instead of the command line.

1. From the navigation menu, choose the gear icon > **Operations Management**.
2. Click **Install Operation**.
3. Choose one of the following:
   - Drag and drop your operation package onto the **Add Operation** dialog box.
   - Browse to your operation package, select it, and then click **Open**.

   If successful, the operation appears in your list of operations where you can enable or disable it.

Deleting Operations

Complete the following steps to delete an operation from ThreatQ:

1. From the navigation menu, choose the gear icon > **Operations Management**.
2. For the operation you want to delete, click **Delete Operation**.
3. Click **Uninstall**.

Exports

The following explains how to configure and manage exports of threat intelligence data from ThreatQ.

Exports Overview

Exporting is one of the most important ThreatQ features, as it allows you to output non-whitelisted indicators to an external threat detection system.

ThreatQ provides a number of standard system exports that have previously been identified as useful. You have the option to use those and create your own.

Managing Exports

Manage Exports on the Exports page, accessible by navigating to the **Settings icon > Exports**.

The following describes the actions you can take to manage Exports.

- Accessing/Editing an Export's Connection Settings
- Accessing/Editing an Export's Output Format
- Deleting an Export

Viewing the Exports List

The Exports page provides a list of all standard and user-defined exports in the platform.

To view the exports list:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

Enabling/Disabling an Export

To enable/disable an export:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Locate the export you wish to enable/disable.
3. Toggle the switch in the On/Off column to enable/disable the export.
   A confirmation of your action appears in an alert bar at the top of the page.

Viewing an Export

To view an export:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Click the desired URL.

   A new tab opens in your browser, and you are taken to the data returned from that export.

   The load time may be lengthy depending on the amount of data being returned.

Duplicating an Export

Duplicating an export allows you to have a version that you can edit.

To duplicate an export:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Locate the Export you wish to duplicate.
3. Click **duplicate** in the Actions column.
4. The duplicate appears at the bottom of the Exports table. A confirmation of the duplication appears in an alert bar at the top of the page.

   By default, the copy you just created is toggled Off.

Adding an Export

To add an export

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Click **+ Add Export**.

   The Connection Settings dialog box opens.

3. Enter the Export name.

4. Verify or edit the token.
5. Click **Next Step**.

   The Output Format dialog box opens.

   For detailed information on formatting the Output Format dialog box, see Accessing/Editing an Export's Output FormatAccessing/Editing an Export's Output Format

6. Select which type of information you would like to export from the first dropdown menu.
7. Select the Output type from the second dropdown menu.
8. Un-select any of the checkboxes under the **Filter by TLP** section to exclude data by its source TLP classification. All classifications will be selected (included in the export) by default.

   The **Filter by TLP** option will only appear if administrators have enabled TLP viewing. See the Traffic Light Protocol (TLP) topic for more information.

9. (Optional) Enter special parameters.
10. Customize the **Output Format Template** by putting your cursor where you want the variable to go and selecting the variable you'd like to use from the **Insert Variable** select box.
11. Verify the information entered.
12. Click **Save Settings**.

    The export you just created appears at the bottom of the Exports table, and a confirmation alert appears in an alert bar at the top of the page.

    By default, the new export is toggled Off.

Accessing/Editing an Export's Connection Settings

Connection settings are available for each of the exports. The Connection Settings dialog box contains the name of the export as well as the token you'll need to use when connecting a device to ThreatQ.

While you cannot edit or delete any of the exports originally supplied by ThreatQ, you can edit exports you have added to ThreatQ or copies of the original exports.

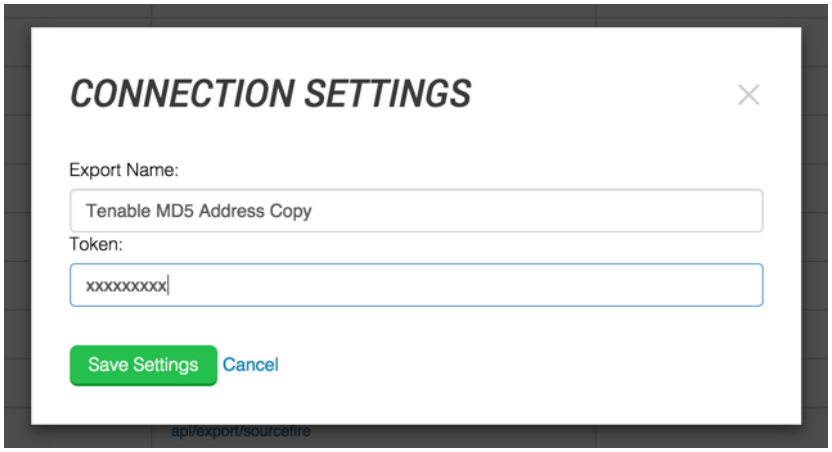
To edit an export's connection settings:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Locate the export you wish to edit.
3. Click **connection settings** in the Connection column.

   The Connection Settings dialog box opens.



4. Make the desired edits.
5. Click **Save Settings**.

   The settings are saved, and a confirmation alert appears in an alert bar at the top of the page.

Accessing/Editing an Export's Output Format

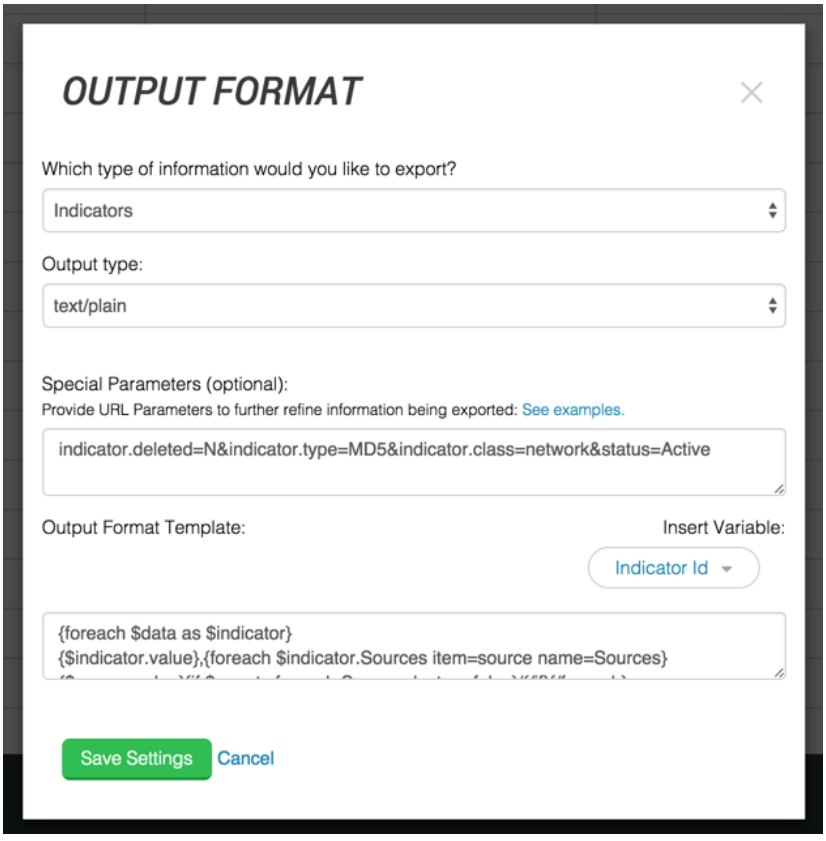
While you cannot edit or delete any of the exports originally supplied by ThreatQ, you can edit exports you have added to ThreatQ or copies of the original exports.

To edit an export's output format:

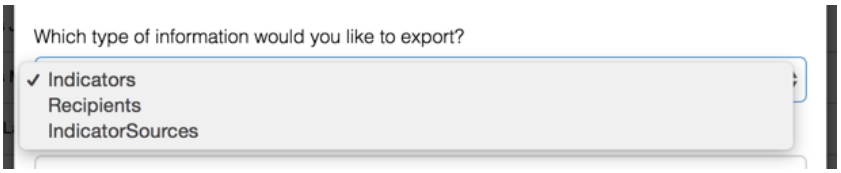
1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Locate the export you wish to edit.
3. Click **output format** in the Output Format column.
   The Output Format dialog box opens.



4. Select which type of information you would like to export from the first dropdown menu.



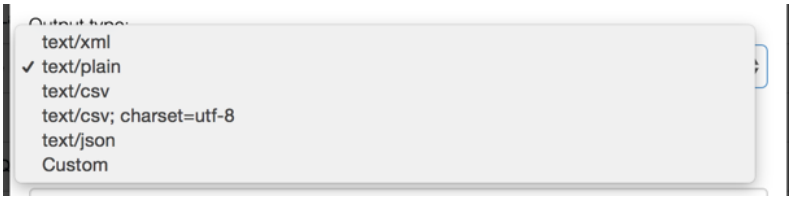
An admin has the ability to choose between the following options:

- Indicators – Outputs only indicators
- Recipients – Outputs only recipients
- IndicatorSources – Outputs indicators with the source as supporting information

5. Select the Output Type from the second dropdown menu.

   This sets the content type of the export response to a specific value (e.g. text/csv, text/plain, text/xml). Output Type does not have an impact on how the data is formatted but it does affect the content type within the header of the exported document. For example, if you select Output Type = text/csv, when viewing the source of the export, the header will contain a Content Type = text/csv attribute.

   Please see http://www.w3.org/Protocols/rfc1341/4_Content-Type.html for more information.



6. (Optional) Enter special parameters. There are two ways to do this:
   - Adding Special Parameters within ThreatQ. One advantage of using this option is that the URL for the export remains non-specific and therefore you can change what is being exported without having to manage each external device individually.

- Customizing the Output Format Template. Choosing this option means you lose the ability to have one place to manage what is being exported.

Adding Special Parameters within ThreatQ

This is where an admin can provide additional parameters to further specify which data will be output via this export. Here are some examples.

To export all indicators with an active status	*Indicator.Status=Active*
To export all CIDR Block indicators that have an active status	*Indicator.Status=Active&Indicator.Type=cidr block*
To export all CIDR Block indicators and IP Addresses that have an active status	*Indicator.Status=Active&Indicator.Type=cidr block&Indicator.Type=ip address*

A wide range of filtering parameters are available:

Parameters for Indicators	Parameters for Recipients	Parameters for Indicator Sources
indicator.id	recipient.id	
indicator.type	recipient.value	indicator.id
indicator.status	recipient.count	indicator.type
indicator.value	recipient.to_count	indicator.status
indicator.class	recipient.cc_count	indicator.value
indicator.hash	recipient.updated_at	indicator.class
indicator.updated_at	recipient.deleted	indicator.hash
indicator.last_detected_at	recipient.deleted_at	indicator.updated_at
indicator.deleted	recipient.spearphish_count	indicator.last_detected_at
indicator.deleted_at	recipient.Adversaries	indicator.deleted
indicator.Attributes	recipient.Attributes	indicator.deleted_at
indicator.Adversary	recipient.Sources	indicator.source

Parameters for Indicators	Parameters for Recipients	Parameters for Indicator Sources
indicator.Sources indicator.sources_count		

Adding Parameters to the end of the URL

You can append the same parameters listed above to the end of any export URL to achieve the same results. By pursuing this option, you will lose the option of having one place to manage what is being exported via that export.

Using Logical Operators in Export Filters

You can configure exports to output objects matching filter conditions that use logical AND and OR operators. Exports allow the following filters:

1. Searching using greater than, less than, or equal to
    - Examples in special parameters string section:

```
indicator.score>=5
```

```
indicator.score<=5
```

    - Examples in request URI:

```
&indicator.score=>=5
```

```
&indicator.score=<=8
```

2. Adding multiple criteria for a single field using an OR comparison

- Example in special parameters string section:

```
indicator.score=5&indicator.score=8
```

- Example in request URI:

```
&indicator.score[]=5&indicator.score[]=8
```

3. Adding multiple criteria for a single field using an AND comparison

- Example in special parameters string section:

```
indicator.score>=5&indicator.score<=8
```

- Example in request URI:

```
&indicator.score[]=>=5&indicator.score
[]=<=8
```

Customizing the Output Format Template

1. Customize the **Output Format Template** by putting your cursor where you want the variable to go and selecting the variable you'd like to use from the **Insert Variable** select box.

   This template provides you with the ability to format exactly how your data is printed out within an export.

   Important: When formatting your output template, you must wrap all of your declarations within a loop. Please refer to the following as an example:

```
{foreach $data as $indicator}

Your variables go here

{/foreach}
```

The Output Format Template is populated based on your selection.

2. Verify the information entered.
3. Click **Save Settings**.

Export Output Format Templates

The following topics contain template files that you can use to customize an export's output format.

The Output Format Template field for an export is found under its Output Format modal. You can access this by clicking on the **Output Format** link for an export from the main exports page.

- Export Adversaries Output Format Template
- Export Events Output Format Template
- Export Indicators Output Format Template
- Export Signatures Output Format Template

Export Adversaries Output Format Template

Use the template below to format exactly how your data is printed out within an export.

Important: When formatting your output template, you must wrap all of your declarations within a loop.

Template

```
{foreach $data as $adversary}
ID: {$adversary.id}
Name: {$adversary.name}
Description: {$adversary.description}
Created At: {$adversary.created}
Updated At: {$adversary.updated_at}
Touched At: {$adversary.touched_at}
Deleted At: {$adversary.deleted_at}
Deleted: {$adversary.deleted}

Your variables go here

{/foreach}
```

The following items are variables that can added to the template.

Sources

```
{foreach $adversary.Sources item=source name-
e=Sources}{$source.value} {if !empty($source.tlp)}
({$source.tlp}){/if}
{/foreach}
```

Attributes

```
{foreach $adversary.Attributes item=attribute name-
e=Attributes}
Name: {$attribute.name}
```

```
Value: {$attribute.value}
{/foreach}
```

Adversaries

```
    {foreach $adversary.Adversaries item=adversary name-
    e=Adversaries}
    Name: {$adversary.name}
    Value: {$adversary.value}
    {/foreach}
```

Attachments

```
    {foreach $adversary.Attachments item=attachment
    name=Attachments}
    Name: {$attachment.name}
    Value: {$attachment.value}
    {/foreach}
```

Events

```
    {foreach $adversary.Events item=event name=Events}
    Name: {$event.name}
    Value: {$event.value}
    {/foreach}
```

Indicators

```
{foreach $adversary.Indicators item=indicator name-
e=Indicators}
Name: {$indicator.name}
Value: {$indicator.value}
{/foreach}
```

Investigations

```
{foreach $adversary.Investigations item-
m=investigation name=Investigations}
Name: {$investigation.name}
Value: {$investigation.value}
{/foreach}
```

Signatures

```
{foreach $adversary.Signatures item=signature name-
e=Signatures}
Name: {$signature.name}
Value: {$signature.value}
{/foreach}
```

Tasks

```
{foreach $adversary.Tasks item=task name=Tasks}
Name: {$task.name}
Value: {$task.value}
{/foreach}
```

Export Events Output Format Template

Use the template below to format exactly how your data is printed out within an export.

Important: When formatting your output template, you must wrap all of your declarations within a loop.

Template

```
{foreach $data as $event}

{$event.title} ID: {$event.id}
Title: {$event.title}
Type: {$event.type}
Happened: {$event.happened_at}
Description: {$event.description}
Created At: {$event.created}
Updated At: {$event.updated_at}
Touched At: {$event.touched_at}
Deleted At: {$event.deleted_at}
Deleted: {$event.deleted}

Your variables go here

{/foreach}
```

The following items are variables that can added to the template.

Sources

```
{foreach $event.Sources item=source name=Sources}
{$source.value} {if !empty($source.tlp)}{/if}
{/foreach}
```

Attributes

```
{foreach $event.Attributes item=attribute name-
e=Attributes}
Name: {$attribute.name}
Value: {$attribute.value}
{/foreach}
```

Adversaries

```
{foreach $event.Adversaries item=adversary name-
e=Adversaries}
Name: {$adversary.name}
Value: {$adversary.value}
{/foreach}
```

Attachments

```
{foreach $event.Attachments item=attachment name-
e=Attachments}
Name: {$attachment.name}
Value: {$attachment.value}
{/foreach}
```

Events

```
{foreach $event.Events item=event name=Events}
Name: {$event.name}
Value: {$event.value}
{/foreach}
```

Indicators

```
{foreach $event.Indicators item=indicator name-
e=Indicators}
Name: {$indicator.name}
Value: {$indicator.value}
{/foreach}
```

Investigations

```
{foreach $event.Investigations item=investigation
name=Investigations}
Name: {$investigation.name}
Value: {$investigation.value}
{/foreach}
```

Signatures

```
{foreach $event.Signatures item=signature name-
e=Signatures}
Name: {$signature.name}
Value: {$signature.value}
{/foreach}
```

Tasks

```
{foreach $event.Tasks item=task name=Tasks}
Name: {$task.name}
Value: {$task.value}
{/foreach}
```

Export Indicators Output Format Template

Use the template below to format exactly how your data is printed out within an export.

Important: When formatting your output template, you must wrap all of your declarations within a loop.

Template

```
{foreach $data as $indicator}

{$indicator.value}
ID: {$indicator.id}
Value: {$indicator.value}
Type: {$indicator.type}
Status: {$indicator.status}
Class: {$indicator.class}
Description: {$indicator.description}
Score: {$indicator.score}
Hash: {$indicator.hash}
Source Count: {$indicator.sources_count}
Whitelisted: {$indicator.whitelisted}
Last Detected At: {$indicator.last_detected_at}
Created At: {$indicator.created}
```

```
Updated At: {$indicator.updated_at}
Touched At: {$indicator.touched_at}
Since Deleted: {$indicator.sincedeleted}
Deleted At: {$indicator.deleted_at}
Deleted: {$indicator.deleted}

Your variables go here

{/foreach}
```

The following items are variables that can added to the template.

Sources

```
{foreach $indicator.Sources item=source name-
e=Sources}{$source.value} {if !empty($source.tlp)}
({$source.tlp})
{/foreach}
```

Attributes

```
{foreach $indicator.Attributes item=attribute name-
e=Attributes}
Name: {$attribute.name}
Value: {$attribute.value}
{/foreach}
```

Adversaries

```
{foreach $indicator.Adversaries item=adversary name-
e=Adversaries}
Name: {$adversary.name}
Value: {$adversary.value}
{/foreach}
```

Attachments

```
{foreach $indicator.Attachments item=attachment
name=Attachments}
Name: {$attachment.name}
Value: {$attachment.value}
{/foreach}
```

Events

```
{foreach $indicator.Events item=event name=Events}
Name: {$event.name}
Value: {$event.value}
{/foreach}
```

Indicators

```
{foreach $event.Indicators item=indicator name-
e=Indicators}
Name: {$indicator.name}
Value: {$indicator.value}
{/foreach}
```

Investigations

```
{foreach $indicator.Investigations item-
m=investigation name=Investigations}
Name: {$investigation.name}
Value: {$investigation.value}
{/foreach}
```

Signatures

```
{foreach $indicator.Signatures item=signature name-
e=Signatures}
Name: {$signature.name}
Value: {$signature.value}
{/foreach}
```

Tasks

```
foreach $indicator.Tasks item=task name=Tasks}
Name: {$task.name}
Value: {$task.value}
{/foreach}
```

Export Signatures Output Format Template

Use the template below to format exactly how your data is printed out within an export.

Important: When formatting your output template, you must wrap all of your declarations within a loop.

Template

```
{foreach $data as $signature}

{$signature.name}
ID: {$signature.id}
Name: {$signature.name}
Value: {$signature.value}
Type: {$signature.type}
Status: {$signature.status}
Description: {$signature.description}
Hash: {$signature.hash}
Detected At: {$signature.last_detected_at}
Touched At: {$signature.touched_at}
Created At: {$signature.created}
Updated At: {$signature.updated_at}
Deleted At: {$signature.deleted_at}
Deleted: {$signature.deleted}

Your variables go here

{/foreach}
```

The following items are variables that can added to the template.

Sources

```
{foreach $signature.Sources item=source name-
e=Sources}{$source.value} {if !empty($source.tlp)}
({$source.tlp}){/if}
{/foreach}
```

Attributes

```
{foreach $signature.Attributes item=attribute name-
e=Attributes}
Name: {$attribute.name}
Value: {$attribute.value}
{/foreach}
```

Adversaries

```
{foreach $signature.Adversaries item=adversary name-
e=Adversaries}
Name: {$adversary.name}
Value: {$adversary.value}
{/foreach}
```

Attachments

```
{foreach $signature.Attachments item=attachment
name=Attachments}
Name: {$attachment.name}
Value: {$attachment.value}
{/foreach}
```

Events

```
{foreach $signature.Events item=event name=Events}
Name: {$signature.name}
```

```
Value: {$signature.value}
{/foreach}
```

Indicators

```
    {foreach $signature.Indicators item=indicator name-
    e=Indicators}
    Name: {$indicator.name}
    Value: {$indicator.value}
    {/foreach}
```

Investigations

```
    {foreach $signature.Investigations item-
    m=investigation name=Investigations}
    Name: {$investigation.name}
    Value: {$investigation.value}
    {/foreach}
```

Signatures

```
    {foreach $signature.Signatures item=signature name-
    e=Signatures}
    Name: {$signature.name}
    Value: {$signature.value}
    {/foreach}
```

Tasks

```
{foreach $signature.Tasks item=task name=Tasks}
Name: {$task.name}
Value: {$task.value}
{/foreach}
```

Deleting an Export

While you cannot delete any of the exports originally supplied by ThreatQ, you can delete any exports you have added to ThreatQ or copies of the original exports.

To delete an export:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Locate the export(s) you wish to delete.
3. Click the export(s).
4. Click the delete icon at the top right of the Exports table.

Specific Indicator Export Configuration Instructions

The following topics provide instructions on how to export specific indicators for use with an external threat detection system.

- Configuring Bro Exports
- Configuring Fidelis Exports
- Configuring Lancope Exports
- Configuring Netwitness Exports
- Configuring OpenIOC Signature Exports
- Configuring Palo Alto Exports
- Configuring Reservoir Labs Exports

- Configuring Splunk Exports
- Configuring Tenable Exports

Configuring Bro Exports

This topic explains how to export Bro indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the instructions below to export your data.

To export to Bro:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**, choose **text/plain**.
   - Under **Special Parameters**, enter **indicator.status=Active&indicator.deleted=N**
   - Under **Output Format Template**, enter:

     #fields{$tab}indicator{$tab}indicator_type{$tab}meta.source{$tab}meta.url

     {foreach $data as $indicator}

```
{$indicator_type=""}

{$source_found=0}

{if $indicator.type eq "CIDR Block"}{$indicator_type="Intel::SUBNET"}{/if}

{if $indicator.type eq "IP Address"}{$indicator_type="Intel::ADDR"}{/if}

{if $indicator.type eq "URL"}{$indicator_type="Intel::URL"}{/if}

{if $indicator.type eq "Email Address"}{$indicator_type="Intel::EMAIL"}{/if}

{if $indicator.type eq "FQDN"}{$indicator_type="Intel::DOMAIN"}{/if}

{if $indicator.type eq "MD5"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator.type eq "SHA-1"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator.type eq "SHA-256"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator.type eq "SHA-256"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator.type eq "SHA-384"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator.type eq "SHA-512"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator.type eq "Filename"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator_type ne ""}

{$indicator.value}{$tab}{$indicator_type}{$tab}{foreach $indicator.Sources
item=source name=Sources}{if $smarty.foreach.Sources.first == true}

{$source.value}{$source_found=1}{/if}{/foreach}{if $source_found == 0}-{/if}

{$tab}https://{$http_host}/indicators/{$indicator.id}/details

{/if}
```

{/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

Configuring Fidelis Exports

This topic explains how to export Fidelis indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the instructions below to export your data for:

- Fidelis FQDN
- Fidelis FQDN Text
- Fidelis IP Address
- Fidelis IP Address Text
- Fildeis MD5
- Fidelis MD5 Text
- Fidelis URL
- Fidelis URL Text

To export to Fidelis FQDN:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.

4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:

   - For **Which type of information would you like to export?** Choose: **Indicators**
   - For **Output type**, choose **text/xml**.
   - Under **Special Parameters**, enter **indicator.status-s=Active&indicator.deleted=N&indicator.type=FQDN&indicator.class=host**
   - Under **Output Format Template**, enter:

     <MyMD5feed/>

     <description>FQDN feed provided by ThreatQuotient. Possible request parameters are listed as attributes on the result node. The dateBegin parameter defaults to one hour prior. Stay secure my friends!</description>

     <entries>

     <limit>{$row_count}</limit>

     <page>{$row_count}</page>

     <start>{$row_count}</start>

     <end>{$row_count}</end>

     <status>{$row_count}</status>

     <rows_returned>{$row_count}</rows_returned>

     <entry>

     {foreach $data as $indicator}

```
<hostname>{$indicator.value|escape:"url"}</hostname>

<extra_info>https://{$http_host}/indicators/{$indicator.id}/details</extra_info>

{/foreach}

</entry>

</entries>
```

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Fidelis FQDN Text:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**, choose **text/plain**
   - Under **Special Parameters**, enter **indicator.status=Active&indicator.deleted=N&indicator.type=FQDN&indicator.class=host**

- Under **Output Format Template**, enter:

  {foreach $data as $indicator}

  {$indicator.value}

  {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Fidelis IP Address:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**, choose **text/xml**.
   - Under **Special Parameters**, enter **indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.class=network**.
   - Under **Output Format Template**, enter:

     <MyMD5feed/>

<description>IP feed provided by ThreatQuotient. Possible request parameters are listed as attributes on the result node. The dateBegin parameter defaults to one hour prior. Stay secure my friends!</description>

<entries>

<limit>{$row_count}</limit>

<page>{$row_count}</page>

<start>{$row_count}</start>

<end>{$row_count}</end>

<status>{$row_count}</status>

<rows_returned>{$row_count}</rows_returned>

<entry>

{foreach $data as $indicator}

<ip>{$indicator.value|escape:"url"}</ip>

<extra_info>https://{$http_host}/indicators/{$indicator.id}/details</extra_info>

{/foreach}

</entry>

</entries>

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Fidelis IP Address Text:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**, choose **text/plain**.
   - Under **Special Parameters**, enter **indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.class=network**.
   - Under **Output Format Template**, enter:

     {foreach $data as $indicator}

     {$indicator.value}

     {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Fidelis MD5:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**, choose **text/xml**.
   - Under **Special Parameters**, enter **indicator.status=Active&indicator.deleted=N&indicator.type=MD5&indicator.class=host.**
   - Under **Output Format Template**, enter:

     <MyMD5feed/>

     <description>MD5 feed provided by ThreatQuotient. Possible request parameters are listed as attributes on the result node. The dateBegin parameter defaults to one hour prior. Stay secure my friends!</description>

     <entries>

     <limit>{$row_count}</limit>

     <page>{$row_count}</page>

     <start>{$row_count}</start>

     <end>{$row_count}</end>

     <status>{$row_count}</status>

```
<rows_returned>{$row_count}</rows_returned>

<entry>

{foreach $data as $indicator}

<md5>{$indicator.value|escape:"url"}}</md5>

<extra_info>https://{$http_host}/indicators/{$indicator.id}/details</extra_info>

{/foreach}

</entry>

</entries>
```

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Fidelis MD5 Text:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**, choose: **text/plain**.

- Under **Special Parameters**, enter **indicator.status=Active&indicator.deleted=N&indicator.type=MD5&indicator.class=host**
- Under **Output Format Template**, enter:

  {foreach $data as $indicator}

  {$indicator.value}

  {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Fidelis URL:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**, choose **text/plain**.
   - Under **Special Parameters**, enter: **indicator.status=Active&indicator.deleted=N**

- Under **Output Format Template**, enter:

  <MyMD5feed/>

  <description>URL feed provided by ThreatQuotient. Possible request parameters are listed as attributes on the result node. The dateBegin parameter defaults to one hour prior. Stay secure my friends!</description>

  <entries>

  <limit>{$row_count}</limit>

  <page>{$row_count}</page>

  <start>{$row_count}</start>

  <end>{$row_count}</end>

  <status>{$row_count}</status>

  <rows_returned>{$row_count}</rows_returned>

  <entry>

  {foreach $data as $indicator}

  <url>{$indicator.value|escape:"url"}}</url>

  <extra_info>https://{$http_host}/indicators/{$indicator.id}/details</extra_info>

  {/foreach}

  </entry>

  </entries>

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Fidelis URL Text:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose: **Indicators**.
   - For **Output type**: choose **text/plain**.
   - Under **Special Parameters**, enter **indicator.status=Active&indicator.deleted=N&indicator.type=URL&indicator.class=host**
   - Under **Output Format Template**, enter:

     {foreach $data as $indicator}

     {$indicator.value}

     {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

Configuring Lancope Exports

This topic explains how to export Lancope indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the instructions below configure an export for your data.

To export to Lancope:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose **Indicators**.
   - For **Output type**, choose **text/csv; charset=utf-8**
   - Under **Special Parameters**, enter:

     indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.type=CIDR Block&indicator.class=network

   - Under **Output Format Template**, enter:

     RECORD_NUMBER,GROUP_NAME,GROUP_ID,NETWORK_DEFINITION,PARENT_NAMESPACE

     0,ThreatQ,-1,,/

```
{foreach $data as $indicator}

0,"{foreach $indicator.Sources item=source name=Sources}{$source.value}
{if $smarty.foreach.Sources.last != true},{/if}{/foreach}",-1,

{$indicator.value|regex_replace:"/[\r\t\n]/":""|replace:"\"":""},"/ThreatQ/"

{/foreach}
```

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

Configuring Netwitness Exports

This topic explains how to export Netwitness indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the instructions below to export your data for:

- Netwitness FQDN
- Netwitness IP

To export to Netwitness FQDN:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose **Indicators**.
   - For **Output type**, choose **text/csv; charset=utf-8**.
   - Under **Special Parameters**, enter:

     indic-
     ator.status-
     =Ac-
     ctive&indicator.deleted=N&indicator.type=FQDN&indicator.class=network

   - Under **Output Format Template**, enter:

     {foreach $data as $indicator}

     "{$indicator.value}","{foreach $indicator.Sources as $source}{$source.value},

     {foreachelse}{/foreach}","https://{$http_host}/indicators/{$indicator.id}/details"

     {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Netwitness IP:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.

4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose Indicators.
   - For **Output type**, choose **text/csv; charset=utf-8**.
   - Under **Special Parameters**, enter:

     indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.class=network

   - Under **Output Format Template**, enter:

     {foreach $data as $indicator}

     "{$indicator.value}","{foreach $indicator.Sources as $source}{$source.value}, {foreachelse}{/foreach}","https://{$http_host}/indicators/{$indicator.id}/details"

     {/foreach}

6. Click **Save Settings**.
7. Under **On/Off,** toggle the switch to enable the export.

Configuring OpenIOC Signature Exports

This topic explains how to export OpenIOC signatures for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the instructions below to export your data.

To export to OpenIOC CSV:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose **Signatures**.
   - For **Output type**, choose **text/csv**.
   - Under **Special Parameters**, enter:

     signature.status=Active&signature.deleted=N&signature.type=OpenIOC

   - Under **Output Format Template**, enter:

     {foreach $data as $signature}

     "{$signature.name|replace:"":'\"'}","{$signature.value|replace:"":'\"'}"

     {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

Configuring Palo Alto Exports

This topic explains how to export Palo Alto indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the

instructions below to export your data.

To export to Palo Alto FQDN:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose **Indicators**.
   - For **Output type**, choose **text/plain**.
   - Under **Special Parameters**, enter:

     indic-
     ator.status-
     =Ac-
     ctive&indicator.deleted=N&indicator.type=FQDN&indicator.class=network

   - Under **Output Format Template**, enter:

     {foreach $data as $indicator}

     {$indicator.value}

     ***.{$indicator.value}**

     {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

Configuring Reservoir Labs Exports

This topic explains how to export Reservoir Labs indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the instructions below to export your data.

To export to Reservoir Labs:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose **Indicators**.
   - For **Output type**, choose **text/plain**.
   - Under **Special Parameters**, enter:

     indicator.status=Active&indicator.deleted=N

   - Under **Output Format Template**, enter:

     #fields{$tab}indicator{$tab}indicator_type{$tab}meta.source{$tab}meta.url

```
{foreach $data as $indicator}

{if $indicator.type eq "CIDR Block"}{continue}{/if}

{if $indicator.type eq "SHA-1"}{continue}{/if}

{if $indicator.type eq "SHA-256"}{continue}{/if}

{if $indicator.type eq "SHA-384"}{continue}{/if}

{if $indicator.type eq "SHA-512"}{continue}{/if}

{$indicator_type=""}

{$source_found=0}

{if $indicator.type eq "IP Address"}{$indicator_type="Intel::ADDR"}{/if}

{if $indicator.type eq "URL"}{$indicator_type="Intel::URL"}{/if}

{if $indicator.type eq "Email Address"}{$indicator_type="Intel::EMAIL"}{/if}

{if $indicator.type eq "FQDN"}{$indicator_type="Intel::DOMAIN"}{/if}

{if $indicator.type eq "MD5"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator.type eq "Filename"}{$indicator_type="Intel::FILE_HASH"}{/if}

{if $indicator_type ne ""}

{$indicator.value}{$tab}{$indicator_type}{$tab}{foreach $indicator.Sources
item=source name=Sources}{if $smarty.foreach.Sources.first == true}

{$source.value}{$source_found=1}{/if}{/foreach}{if $source_found == 0}-{/if}

{$tab}https://{$http_host}/indicators/{$indicator.id}/details

{/if}
```

{/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

Configuring Splunk Exports

This topic explains how to export indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the instructions below to export your data.

To export to Splunk:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

   - Provide the following information:
   - For **Which type of information would you like to export?** Choose **Indicators**.
   - For **Output type**, choose **text/plain**.
   - Under **Special Parameters**, enter:

     indicator.sincedeleted=Y

- Under **Output Format Template**, enter:

  #indicator{$tab}indicator_type{$tab}last_modified{$tab}reference_url{$tab}-source{$tab}campaign{$tab}status

  {foreach $data as $indicator}

  {$indicator.value}{$tab}{$indicator.type}{$indicator.updated_at}

  {$tab}https://{$http_host}/indicators/{$indicator.id}/details{$tab}{foreach $indicator.Sources item=source name=Sources}{$source.value}{if $smarty.-foreach.Sources.last == false}, {/if}{/foreach}{$tab}{foreach $indicator.Adversaries item=adversary name=Adversaries}{$adversary.value}{if $smarty.foreach.Adversaries.last == false}, {/if}{/foreach} {$tab}{$indicator.status}

  {/foreach}

5. Click **Save Settings**.
6. Under **On/Off**, toggle the switch to enable the export.

Configuring Tenable Exports

This topic explains how to export Tenable indicators for use with an external threat detection system. See Exports Overview for more details about configuring exports. Follow the instructions below to export your data for:

- Tenable FQDN
- Tenable IP Address
- Tenable MD5 Address

To export to Tenable FQDN:

1. Select the **Settings icon >Exports**.

   The Exports page appears with a table listing all exports.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.

   The Output Format dialog box appears.

5. Provide the following information:
   - For **Which type of information would you like to export?** Choose **Indicators**.
   - For **Output type**, choose text/plain.
   - Under **Special Parameters**, enter:

     indic-
     ator.status-
     =Ac-
     ctive&indicator.deleted=N&indicator.type=FQDN&indicator.class=network

   - Under **Output Format Template**, enter:

     {foreach $data as $indicator}

     {$indicator.value},{foreach $indicator.Sources item=source name=Sources}

     {$source.value}{if $smarty.foreach.Sources.last == false}/{/if}{/foreach}

     {/foreach}

6. Click **Save Settings**.
7. Under **On/Off**, toggle the switch to enable the export.

To export to Tenable IP Address:

1. From the navigation menu, choose the **gear icon > Exports**.
2. The Exports page appears.
3. Click **Add New Export**.
4. The Connection Settings dialog box appears.
5. Enter an **Export Name**.
6. Click **Next Step**.
7. The Output Format dialog box appears.
8. Provide the following information:
   - For **Which type of information would you like to export?** Choose **Indicators**.
   - For **Output type**, choose **text/plain**.
   - Under **Special Parameters**, enter:

     indicator.status=Active&indicator.deleted=N&indicator.type=IP Address&indicator.class=network

   - Under **Output Format Template**, enter:

     {foreach $data as $indicator}

     {$indicator.value},{foreach $indicator.Sources item=source name=Sources}

     {$source.value}{if $smarty.foreach.Sources.last == false}/{/if}{/foreach}

     {/foreach}
9. Click **Save Settings**.
10. Under **On/Off**, toggle the switch to enable the export.

To export to Tenable MD5 Address:

1. From the navigation menu, choose the **gear icon > Exports**.

   The Exports page appears.

2. Click **Add New Export**.

   The Connection Settings dialog box appears.

3. Enter an **Export Name**.
4. Click **Next Step**.
5. The Output Format dialog box appears.
6. Provide the following information:
   - For **Which type of information would you like to export?** Choose **Indicators**.
   - For **Output type**, choose **text/plain**.
   - Under **Special Parameters**, enter:

     indic-
     ator.status-
     s=Active&indicator.deleted=N&indicator.type=MD5&indicator.class=network

   - Under **Output Format Template**, enter:
   - **{foreach $data as $indicator}**
   - **{$indicator.value},{foreach $indicator.Sources item=source name-e=Sources}**
   - **{$source.value}{if $smarty.foreach.Sources.last == false}/{/if}{/foreach}**
   - **{/foreach}**
7. Click **Save Settings**.
8. Under **On/Off**, toggle the switch to enable the export.

Common Enrichment and Audit Log Questions

The ThreatQ Audit Log tracks every change made to every object in the system. If there is a change to an object, that change is displayed in the audit log. The audit log is only updated if the data itself changes, not just the **updated_at** value.

The following questions below address further details about the audit logging process.

In the case where an activity is triggered (with nothing updated), where will the activity be logged?

The activity will not show in the audit log, as there were no changes to report. While ThreatQ does not track duplicate objects that enter the application, there is a **touched_at** date field on primary objects (Adversaries, Files, Events, Indicators, and Signatures) that indicates when a relation of the object has been changed.

Is there another raw audit log within the system where events are logged?

No, there are no other raw audit logs where events are logged.

Is there an option in the User Interface to enable all activities to be shown in the Audit Log?

There is no option in the User Interface to limit or expand the audit log. All entries are pulled for an object when the Audit Log panel is opened. The audit log displays changes to the individual fields of an object; object comments, sources, attributes, and tags; as well as to object links, object link comments, and object link attributes. Additionally, any changes to the score of an Indicator are included.

Air Gapped Data Sync

The following explains how to configure and complete an Air Gapped Data Sync from a source ThreatQ instance to a target air-gapped ThreatQ instance.

Air Gapped Data Sync Overview

Air Gapped Data Sync allows you to transfer data from a source ThreatQ installation to a target air-gapped ThreatQ installation. ThreatQ defines an air-gapped system as one that is not connected to a public network. This means that **external** feed ingestion will not occur on the air-gapped installation.

You should consult with ThreatQ Support or a Threat Intelligence Engineer prior to performing an Air Gapped Data Sync.

Air Gapped Data Sync consists of two synchronization commands:

- **threatq:sync-export**: the read command that copies data from the source ThreatQ installation
- **threatq:sync-import**: the write command that copies data to the target ThreatQ installation

This section includes deployment details and configurations that should not be deviated from or changed without first consulting with

ThreatQuotient. Any deviation of the ThreatQuotient recommended settings could result in system and platform instability, may render the system non-operational, and are not supported.

Air Gapped Data Sync System Requirements

To use Air Gapped Data Sync, ThreatQ installations must meet the following requirements:

- ThreatQ v4.15 or later must be installed.
- All ThreatQ installations must run the same software version.
- All ThreatQ installations must be set to the correct time, time zone, and date, and using a clock source available to all. UTC is recommended.

Understanding threatq:sync-export

The purpose of this command is to pull all objects, object context, tags, and object links from the source ThreatQ installation and then store them in CSV data dump files. You can specify which objects are pulled, based on a date or via configuration. All data pulled into the CSV data dump files can then be transferred to a target air-gapped ThreatQ installation for validation and import. Each run of this command also generates a sync report with output logs for the run.

threatq:sync-export Parameters

The following table outlines the parameters for the command. All parameters for the threatq:sync-export command are optional. If you do not set any parameters, the system runs a default configuration as explained in threatq:sync-export Configuration.

Parameter	Explanation
--target	Target directory where the output file should be placed. This value is required. Default: /tmp example: --target=/my/directory
--start-date	The start date for data selection. This value is required. ex: --start-date="2018-01-01 00:00:00"
--end-date	The end date for data selection. This value is required. Applies only to objects themselves, not object context or object links.

Parameter	Explanation
	example: --end-date="2018-01-02 00:00:00"
--include-deleted	Determines whether objects that have been soft-deleted are included in the result set. Options are Y(es) or N(o). Default: N example: --include-deleted=Y
--include-investigations	Determines whether Investigations and Tasks are included in the result set. This value is required. Options are Y(es) or N(o). Default: N example: --include-investigations=N
--meta-only	If present, tells the command to only include meta data (no object data) in the result set. No value necessary.
--memory-limit	Sets the PHP memory limit in Megabytes or Gigabytes. This value is required. Default: 2G example: --memory-limit=4G

Parameter	Explanation
--object-limit	Sets the limit on the number of objects selected at a time. Recommended use is to set the limit to a number smaller than the default (50,000) on boxes with very large data sets. Default: 50,000 example: --memory-limit=10000

threatq sync-export Examples

This command should be run from inside the `/var/www/api directory`. The following examples provide use cases for air gapped data sync.

No Time Limit, Default Configuration

```
sudo ./artisan threatq:sync-export
```

This example will pull all objects in the system (with the exception of Investigations, Tasks, and soft-deleted Objects). The output will appear in /tmp.

Meta Data Only

```
sudo ./artisan threatq:sync-export --meta-only
```

This example will pull only meta data objects from the system (Attributes, Sources, Object Statuses and Types, and so on).

Time Limit

```
sudo ./artisan threatq:sync-export --start-date
="2018-10-01 00:00:00" --end-date="2018-11-01
00:00:00"
```

This example will pull objects whose `updated_at` or `touched_at` occurs between the start and end date.

Cron Configuration

```
sudo ./artisan threatq:sync-export
--target=/my/directory --include-deleted=Y
--include-investigations=N
```

This example will do a search for a previous synchronization record with the same hash (comprised of the three options provided). If any hash matches are found, the run will use the `started_at` date of the most recent previous record as the start date for the current run.

If you do not require soft-deleted Objects, Investigations, or Tasks to be transferred to the target ThreatQ installation, then only the `--target option` is necessary (as the defaults for the other two options are both (N)o).

threatq sync-export Initial Cron Setup for First Time Use

Basic Instructions

Determine what the cron configuration options should be:

- target directory
- whether investigations/tasks should be included

- whether deleted objects should be included

The cron configuration options must be the same for every run, but they only need to be specified if different from the defaults.

Run the command with the cron configuration options:

```
php artisan threatq:sync-export
--target=/my/directory --include-investigations=Y
--include-deleted=N
```

Instructions for Larger Data Sets (Starting from the Beginning of Time)

For larger data sets, it is undesirable to do a full run from the beginning of time (performance will suffer).

ThreatQuotient recommends that you use the `--end-date` option to specify an upper limit on the date range pulled. Multiple runs will be necessary to process all data up to the current date.

Determine what the cron configuration options should be:

- target directory
- whether investigations/tasks should be included
- whether deleted objects should be included

The cron configuration options will need to be the same for every run, but they only need to be specified if different from the defaults.

For each of the runs, provide the configuration options along with the `--end-date` option:

```
php artisan threatq:sync-export
--target=/my/directory --include-investigations=Y
--end-date="2017-01-01 00:00:00"
```

Once the current date has been reached, the `--end-date` option will no longer be necessary.

Instructions for Larger Data Sets (Starting from a Specified Date)

For larger data sets, it is undesirable to do a full run from the beginning of time (performance will suffer).

ThreatQuotient recommends that you use the `--end-date` option to specify an upper limit on the date range pulled. Multiple runs will be necessary to process all data up to the current date.

If only a subset of data needs to be processed up to the current date, then you should use the `--initial-start-date` option.

Determine what the cron configuration options should be:

- target directory
- whether investigations/tasks should be included
- whether deleted objects should be included

The cron configuration options will need to be the same for every run, but they only need to be specified if different from the defaults.

For the first run, provide the configuration options along with the `--initial-start-date` option.

```
php artisan threatq:sync-export
--initial-start-date="2017-01-01 00:00:00" --
```

```
target=/my/directory
--include-investiagtions=Y --end-date="2017-02-01
00:00:00"
```

For each of the runs, provide the configuration options along with the `--end-date` option:

```
php artisan threatq:sync-export
--target=/my/directory --include-investigations=Y
--end-date="2017-01-01 00:00:00"
```

Once the current date has been reached, the `--end-date` option will no longer be necessary.

threatq sync-export Run Scenarios

Success

When a run of this command completes successfully, a tarball of data will appear in the target directory you specified (or /tmp by default). A report file describing the run will be available in the data tarball, under the /sync directory. There will also be a record in the database synchronizations table for the run.

Errors

If a run of this command fails before completion, the tarball will not be created. There will be a data directory in the target directory (where the data is stored before it is compressed) that contains all the data that was processed before the failure. The report file will appear in this directory under /sync. Error messages will not appear in the report file - though they will appear in the laravel log and in the console.

Regardless of whether the run was part of a cron configuration, it can simply be restarted. The cron configuration will look for the last completed run to find the next start date.

threatq:sync-export Dates

Start Date

A start date is applied to objects according to the column available - `touched_at or updated_at`.

`touched_at Objects`

Adversaries, Attachments, Events, Indicators, Signatures, Custom Objects

`updated_at Objects`

Investigations, Tasks, Object Links, Tagged Objects

End Date

An end date is applied only if you provide one at run time. It is applied everywhere a start date is used.

threatq:sync-export Configuration

The configuration used for each run of this command consists of the `--target`, `--include_deleted`, and `--include_investigations` command line options and is stored in the `config_json` column of the Synchronization record. The hash column of each Synchronization record is a md5 hash of the `config_json` column.

Default

The default configuration is used if the command is run with no options provided:

- target_directory = /tmp
- include_deleted = false
- include_investigations = false

In this configuration, the initial run start date will default to 1970-01-01 00:00:00.

Cron

If the command is run with the `--target`, `--include_deleted`, and `--include_investigations` parameters, the hash of these values will be compared against the hash column of previous runs. Using these three options on every run allows for the command to be incorporated into a scheduled task.

If any hash matches are found, the start date for the run will be set to the `started_at` date in the Synchronization record of the previous run with the same hash.

If no hash matches are found, the start date will be set to 1970-01-01 00:00:00.

Start Date Provided

If a start date is included in the command run using the `--start-date` option, any other options also provided will be honored. However, if the `--target`, `--include_deleted` and `--include_investigations` options are also included, a Cron check against the hash of these three options will **not** occur. The start date provided will be included in `config_json` as the **manual_start_date** so that the run does not collide with any Cron-related runs.

If a "beginning of time" run is necessary, use the option as `--start-date="1970-01-01 00:00:00"`.

threatq:sync-export Output and Sync Report

The following sections detail the data you may find in the export output and sync report.

threatq:sync-export Meta Data

Meta data is transferred with every run of this command by default. You can specify that only meta data (no object data) should be pulled in a run by using the `--meta-only` option.

Meta data includes information about Sources, Attributes, Tags, as well as Object Statuses and Types (both seeded and user-provided).

While meta data like Connectors and Operations are included in this list, they are not installed on the target ThreatQ installation as part of the air gapped data sync process. They are only placed in the requisite tables for use as Sources of Objects that are transferred. The same is true of any Users that are copied - these will not be enabled Users on the target installation; they will be transferred as disabled.

Meta Data Objects:

- Attributes
- Clients
- Connectors
- Connector Categories
- Connector Definitions
- Content Types
- Groups
- Investigation Priorities
- <Object Type> Statuses
- <Object Type> Types
- Other Sources
- Operations
- Sources
- Tags

- TLP
- Users

threatq:sync-export Objects

This command covers any objects installed on the system by default, and any custom objects that have been installed by the user. The only objects that can be excluded are Investigations and Tasks (using the `--include-investigations` command line option).

> Custom Objects that are installed on a source ThreatQ installation that have NOT been installed on a target ThreatQ installation will NOT be installed by the air gapped data sync process. If an object is included in the export data, but is not found on the target, it will be ignored.

Default Objects:

- Adversaries
- Attachments (Files)
- Events
- Indicators
- Signatures
- Campaigns
- Courses of Action
- Exploit Targets
- Incidents
- TTPs

Storage:

The data for each object is copied as a dump file in CSV format using "SELECT * INTO OUTFILE..." MariaDB syntax. The full query for the data is built up using the options you

provided (start date, end date, etc).

Dump files contain a maximum object limit of 50,000 (set in the Synchronization base class). Dump files are created (with a counter appended to the file name) until the entire object result has been covered.

To ensure that any Objects present in Object Links, Tagged Objects, or Investigation Timeline Objects are also included in the base Object data, CSV dump files for each Object type are also created from queries against each of these tables. This is necessary because of the differing date columns used in each query (an object may appear in an Object Link in the specified date range according to the Object Link's `updated_at` date, even though the Objects themselves saw no change to their `touched_at` date in that date range). When the data from all of these object files is transferred to the target ThreatQ installation, any duplicates across dump files will be consolidated.

Sample Object File List (all of these files will contain Adversary records):

- adversaries/adversaries_0.csv
- adversaries/adversaries_investigation_timelines_0.csv
- adversaries/adversaries_object_links_dest_0.csv
- adversaries/adversaries_object_links_src_0.csv
- adversaries/adversaries_tags_0.csv

threatq:sync-export Object Context

The date range for queries on Object Context tables uses the `updated_at` date column, with the exception of Adversary Descriptions, which uses the `created_at` date column.

Adversary Descriptions are handled as part of the Object Context gathering process. The `adversary_descriptions` table is queried using the created_at date column, and the

entirety of the `adversary_description_values` table is pulled, as it doesn't have a date column.

Not all Objects have all Object Contexts (Attributes, Attribute Sources, Comments, and Sources). Tables are only polled if they exist.

Tables Covered for each Object Type:

- <object type>_attributes
- <object type>_attribute_sources
- <object type>_comments
- <object type>_sources

Sample Object Context File List (Indicator Object Type):

- indicators/indicator_attribute_sources_0.csv
- indicators/indicator_attributes_0.csv
- indicators/indicator_comments_0.csv
- indicators/indicator_sources_0.csv

threatq:sync-export Other Data

Attachment Files

Physical files for all attachments included in the date range are copied into the attachments/files directory of the data tarball.

Object Links

The date range for queries on Object Links uses the `updated_at` date column.

Tables Covered (Object Links and Object Link Context):

- object_links
- object_link_attributes
- object_link_attribute_sources
- object_link_comments
- object_link_sources

Sample Object Link File List:

- object_links/object_links_0.csv
- object_links/object_link_attributes_0.csv
- object_links/object_link_attribute_sources_0.csv
- object_links/object_link_comments_0.csv
- object_links/object_link_sources_0.csv

Tags

The date range for queries on Tagged Objects uses the `updated_at` date column.

Tables Covered (Tags themselves are covered in the Meta Data):

tagged_objects

Sample Tagged Objects File List:

tagged_objects/tagged_objects_0.csv

Spearphish

The date range for queries on Spearphish uses the `updated_at` date column.

Tables Covered:

spearphish

Sample Spearphish File List (Spearphish files are stored with Event data):

events/spearphish_0.csv

Investigations

The date range for queries on additional Investigation context tables uses the `updated_at` column.

Tables Covered:

- investigation_nodes
- investigation_node_properties
- investigation_timelines
- investigation_timeline_objects
- investigation_viewpoints

Sample Investigation additional context File List:

- investigations/investigation_node_properties_0.csv
- investigations/investigation_nodes_0.csv
- investigations/investigation_timeline_objects_0.csv
- investigations/investigation_timelines_0.csv
- investigations/investigation_viewpoints_0.csv

threatq:sync-export File Output

threatq:sync-export Data Tarball

Once all data has been processed, a tarball is created containing all output files. This tarball will be dropped in the directory specified in the `--target option`, or the /tmp directory by default.

Tarball Naming Convention: `tqSync_<run date>.tar.gz`

Example: tqSync-19-01-16-1547649934-0849.tar.gz

threatq:sync-export Sync Report

The output for each run is stored in a Sync Report output file, which is located in the sync directory of the data tarball. The file is always named sync-export.txt.

threatq:sync-export Command Line Output

Command line output displays command progress, object totals, and files written.

threatq:sync-export Synchronizations

Table

synchronizations

- `id` - The auto-incremented id for the Synchronization record
- `type` - The Synchronization direction (options are "export" or "import")
- `started_at` - The date and time the command run was started
- `finished_at` - The date and time the command run completed
- `config_json` - A JSON representation of the command run configuration
- `report_json` - A JSON representation of the command run parameters (command line options, object counts, files created, etc)
- `pid` - The process id of the command run
- `hash` - Unique identifier for a command run (md5 hash of the config_json column)
- `created_at` - The date and time the Synchronization record was created

- `updated_at` - The date and time the Synchronization record was updated

Record Handling

Hash

The Synchronization record hash column is automatically calculated as an md5 of the `config_json` column on record creation.

Initial Creation

A Synchronization record is created at the beginning of a command run, right after all command line options have been processed. Initial creation only covers the `type`, `started_at`, `pid`, and `config_json` columns. For this command (`threatq:sync-export`), the type will be "export". The command line option portion of the `report_json` is added as well, but this column will not be complete until the record is finalized. The `finished_at` column remains NULL.

Finalization

A Synchronization record is finalized when the command run has completed. At this time, the `finished_at` column is filled with the completion datetime, and the `report_json` column is updated to include information about the run (object counts, files created, etc).

Understanding threatq:sync-import

The purpose of this command is to process the tarball of object data created by the threatq:-sync-export command. Temporary sync tables are created on the target to house this object data, and integrity checks are run against existing data to verify IDs and check for duplicate objects. Duplicate objects from the source ThreatQ installation are updated, and new objects are inserted. The temporary sync tables are dropped when data processing is complete. Each run of this command also generates a sync report without output logs for the run.

threatq:sync-import Parameters

The following table outlines the parameters for the command. With the exception of `--file`, which is required, all parameters for the threatq: sync-import command are optional.

Parameter	Explanation
--file	File path to the tarball created by the `threatq:sync-export` command. This command is required to run the `threatq:sync-import` command. example: --file=/tmp/tqSync-19-01-16-1547660837-8345.tar.gz

Parameter	Explanation
--keep-created-at	Determines whether the oldest `created_at` date between the source and target ThreatQ installations should be maintained, or a new `created_at` is set on the target system. The default if this option is not provided by the user is for the oldest `created_at` date to be maintained. This value is required. Options are Y(es) or N(o). Default: Y example: --keep-created-at=N
--object-limit	Integer value used as the limit for the number of objects updated or inserted at a time. This value is required. When using this option, the size of the data sets on both source and target ThreatQ installations should be taken into account. Setting the limit too high may hinder performance. Default: 1000 example: --object-limit=50000
--memory-limit	Sets the PHP memory limit in Megabytes or Gigabytes. This value is required. Default: 2G example: --memory-limit=4G

threatq:sync-import Examples

This command should be run from inside the `/var/www/api` directory.

Basic Run

```
sudo ./artisan threatq:sync-import
--file=/tmp/tqSync-19-01-16-1547660837-8345.tar.gz
```

This example will process all the data in the tarball provided in the `--file` option, using an object limit of 1000 for all inserts and updates. The `created_at` date of all transferred objects will be updated on the target ThreatQ installation if it is older than the current `created_at` date (if the object is already present on the source ThreatQ installation). Newly inserted objects will keep the `created_at` date of the source ThreatQ installation.

Set New created_at Dates on the Write System

```
sudo ./artisan threatq:sync-import
--file=/tmp/tqSync-19-01-16-1547660837-8345.tar.gz
--keep-created-at=N
```

This example will process all the data in the tarball provided in the `--file` option using an object limit of 1000 for all inserts and updates. The `created_at` date of all transferred will be left alone in the case of object updates, and to the current time in the case of new object inserts.

Increase the Object Limit

```
sudo ./artisan threatq:sync-import
--file=/tmp/tqSync-19-01-16-1547660837-8345.tar.gz
--object-limit=50000
```

This example will process all the data in the tarball provided in the `--file` option using an object limit of 50000 for all inserts and updates. The `--keep-created-at` option has

been left out, so it will use the default setting of Y(es) and `created_at` dates will be maintained from the read system.

threatq sync-import Run Scenarios

Success

When a run of this command completes successfully, a report will appear in the directory the command was run in (/var/www/api). There will also be a record in the database synchronizations table for the run. Both of these will contain data describing performance metrics and object counts.

Errors

If a run of this command fails before completion, error messages will not appear in the report file - though they will appear in the laravel log and in the console. There is not currently a means of restarting the command from where it left off. The command will need to be restarted and will run through all the data again. Any data from the tarball that was written during the previous failed run will simply be updated (rather than inserted again), meaning the end result will be the same - all data will be transferred from the tarball to the target system.

threatq:sync-import Data Processing

Data found in CSV dump files for a table from the tarball provided in the `--file option` is inserted into a corresponding sync table. A sync table is just a copy of a base table, with column structure maintained but indexes excluded. Indexes are added to unique columns on sync tables (which will later be used in table joins and where clauses) once data insertion from dump files is complete, since indexes slow the insertion process down.

The naming convention for a sync table is sync_import_<base table name>_<process id>.

Example:

Base table: adversaries

Sync table: sync_import_adversaries_12345

All sync tables are removed from the target ThreatQ installation's database once data processing is complete.

threatq:sync-import Basic Table

A basic table has no foreign keys pointing to other tables in the database. It has a single identifier (id) column for each record. Once all the data stored in the tarball for a basic table has been transferred to a sync table, the sync table has an `existing_id` column added with a default value of NULL for each record. This column is used to determine whether the record already exists on the target ThreatQ installation. The id for the record on the target system may be different from that of the record from the source ThreatQ installation, so this `existing_id` column ensures that data integrity is maintained between the two.

Sample Basic Table:

`attachment_type`s - (id, name, is_parsable, parser_class, created_at, updated_at, deleted_at)

Sample Sync Table created from Basic Table:

`sync_import_attachment_types_12345` - (existing_id, id, name, is_parsable, parser_class, created_at, updated_at, deleted_at)

threatq:sync-import Tables with Pivots

A pivot table has one or more foreign keys pointing to other tables in the database. Once all the data stored in the tarball for a table with pivots has been transferred to a sync table, the sync table has an `existing_<pivot>_id` column added for each foreign key column, as well as an `existing_id` column for the record itself (all set to a default value of NULL).

threatq:sync-import File Output

threatq sync-import File Output and Sync Report

Once all data has been processed, a Sync Report will be generated in the `/var/www/api` directory (where the command is run). This file will be named after the tarball used in the run, with the extension "-sync-import.txt"

Example:

> Tarball used: tqSync-19-01-16-1547660837-8345.tar.gz
>
> Sync Report name: tqSync-19-01-16-1547660837-8345-sync-import.txt

threatq:sync-import Command Line Output

Command line output displays command progress and object totals. It will be similar to the output in the Sync Report.

threatq:sync-import Synchronizations

Table

synchronizations

- `id` - The auto-incremented id for the Synchronization record
- `type` - The Synchronization direction (options are "export" or "import")
- `started_at` - The date and time the command run was started
- `finished_at` - The date and time the command run completed
- `config_json` - A JSON representation of the command run configuration
- `report_json` - A JSON representation of the command run parameters (command line options, object counts, tables created, etc)

- `pid` - The process id of the command run
- `hash` - Unique identifier for a command run (md5 hash of the config_json column)
- `created_at` - The date and time the Synchronization record was created
- `updated_at` - The date and time the Synchronization record was updated

Record Handling

Hash

The Synchronization record hash column is automatically calculated as an md5 of the `config_json` column on record creation.

Initial Creation

A Synchronization record is created at the beginning of a command run, right after all command line options have been processed. Initial creation only covers the type, `started_at`, `pid`, and `config_json` columns. For this command (`threatq:sync-import`), the type will be "import". The command line option portion of the `report_json` is added as well, but this column will not be complete until the record is finalized. The `finished_at` column remains NULL.

Finalization

A Synchronization record is finalized when the command run has completed. At this time, the `finished_at` column is filled with the completion date and time, and the `report_json` column is updated to include information about the run (object counts, tables created, etc).

Executing Air Gapped Data Sync

Using artisan commands at the command line of the ThreatQ installation, you execute air gapped data sync in two steps:

1. You run the **threatq:sync-export** command on the source ThreatQ installation; see Understanding threatq:sync-export.
2. You run the **threatq:sync-import** command on the target ThreatQ installation, see Understanding threatq:sync-import.

Running the threatq:sync-export Command

To run the threatq:sync-export command, complete the following steps:

1. Access the command line on the source ThreatQ installation.
2. Change directories to `/var/www/api`.
3. Run the following command: `sudo ./artisan threatq:sync-export`, appended by the necessary parameters, as described in threatq:sync-export Parameters.
4. Review the Output and Sync report; see threatq:sync-export Output and Sync Report.

Running the threatq:sync-import Command

To run the threatq:sync-import command, complete the following steps:

1. Access the command line on the target ThreatQ installation.
2. Change directories to `/var/www/api`.
3. Run the following command: `sudo ./artisan threatq:sync-import`, appended by the necessary parameters, as described in Running the threatq:-sync-import Command.

4. Review the Output and Sync report; see threatq sync-import File Output and Sync Report.

Backup and Restore

The following describes how to back up and restore a ThreatQ instance.

ThreatQ Backup

Before performing a backup of a ThreatQ instance, note the following:

- The backup process stops and starts all ThreatQ services automatically in order to prevent modifications to the file system and database. Requests made during this time are queued and resumed once the backup process completes.
- The time it takes to back up ThreatQ depends primarily on the size of the database. For this reason, we recommend performing a backup when system availability is not critical, such as during a scheduled maintenance window.
- The resulting backup file can be large. We recommend that you write it to a mounted drive or file location rather than the local file system. For instructions on how to mount a network-available drive, contact ThreatQ Support. If the backup file must be stored locally, you should move it off the local file system at the earliest opportunity.
- By default, the system creates a backup of the threat intelligence data index required for improved search performance and includes it in the backup file. This operation may take hours. You can omit this portion of the backup by running the backup command with the --exclude-solr option. However, this means that your threat intelligence data must be re-indexed during or after the restore process.

Backing Up a ThreatQ Instance

By default, the system creates a backup of the threat intelligence data index required for improved search performance and includes it in the backup file. This operation may take hours. You can omit this portion of the backup by running the backup command with the --exclude-solr option. However, this means that your threat intelligence data must be re-indexed during or after the restore process.

Before you begin, refer to ThreatQ Backup.

To perform a ThreatQ backup:

1. SSH to the ThreatQ command line and elevate your user privilege to root or sudo.
2. Change the directory to **/var/www/api**.
3. Choose one of the following options:
   - To create a backup that includes a Threat Library re-index, run the following command: `sudo php artisan threatq:backup`
   - To create a backup that excludes a Threat Library re-index, run the following command: `sudo php artisan threatq:backup --exclude-solr`
4. When prompted, provide the **root mysql** password you configured during first boot.
5. Provide the path to the file location where you want to create the backup.

The script generates a backup file in the specified file location. The name of the file will be **threatq_backup_x.x.x_yyyy-mm-dd.tgz**, where **x.x.x** is the TQ version and **yyyy-mm-dd** is the date when the backup was performed.

ThreatQ Restore

To restore from a ThreatQ backup, note the following:

- The target machine must be an existing ThreatQ instance running the same version of the instance captured in the backup.
- The restore process completely overwrites the current installation.
- The backup file needs to be accessible by the target ThreatQ instance, either locally or on a mounted drive.
- The backup file will be unzipped in the same directory where it resides. Ensure that the available disk has sufficient space to hold both the backup archive and the extracted directory. The extracted directory can be removed after the restore is complete.
- Depending on the size of the instance being restored, the process can take a while.
- The machine running the target ThreatQ instance automatically restarts once the restore process is complete.

How to Restore from a ThreatQ Backup

Before you begin, refer to ThreatQ Restore.

To restore from a ThreatQ backup, perform the following procedure on the target ThreatQ instance.

1. Complete the first boot process on the new host by navigating to its IP address in a web browser and entering your credentials. If this step is not completed, the remaining steps are not successful.
2. SSH to the command line and elevate your user privileges to root or sudo.
3. Verify that you have the necessary utilities in place by running: **yum install policycoreutils-python-2.2.5-20.el7.x86_64**.
4. Change directory to **/var/www/api**.

5. Issue the following commands:
   - **php artisan threatq:restore </path/to/backup_file>**
   - **php artisan threatq:update-events**
6. When prompted, provide the root mysql password you configured during first boot.
7. If the backup file does not include the intelligence data index required for improved search performance, the system prompts you to either allow an automatic re-index or manually perform it later.

   This operation may take hours.

8. After the restore completes, you should reboot the target ThreatQ system to ensure that the system processes start up correctly.

OAuth Management

The OAuth Management section is where you can find your credentials, a unique Client ID, which will allow you to connect with ThreatQ's API.

ThreatQ Purge Command

Read this topic carefully before running the ThreatQ Purge Command. After running this command, your threat intelligence data cannot be recovered.

The ThreatQ Purge command will **permanently** delete all object-related threat intelligence data from your ThreatQ installation, including audit logs. It will maintain any configuration-related settings, such as expiration, scoring, and so on.

Running the ThreatQ Purge Command

1. SSH to your ThreatQ Installation.
2. Run the following artisan command:

```
/var/www/api/artisan threatq:purge-threat-intel-
ligence
```

3. You will be presented the following prompt:

```
You are about to erase all of your data, are
you sure?
```

4. Enter **Yes** or **No**.