ThreatQuotient

ThreatQ User Guide

Version 4.13

December 18, 2018

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: Wednesday, December 19, 2018

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

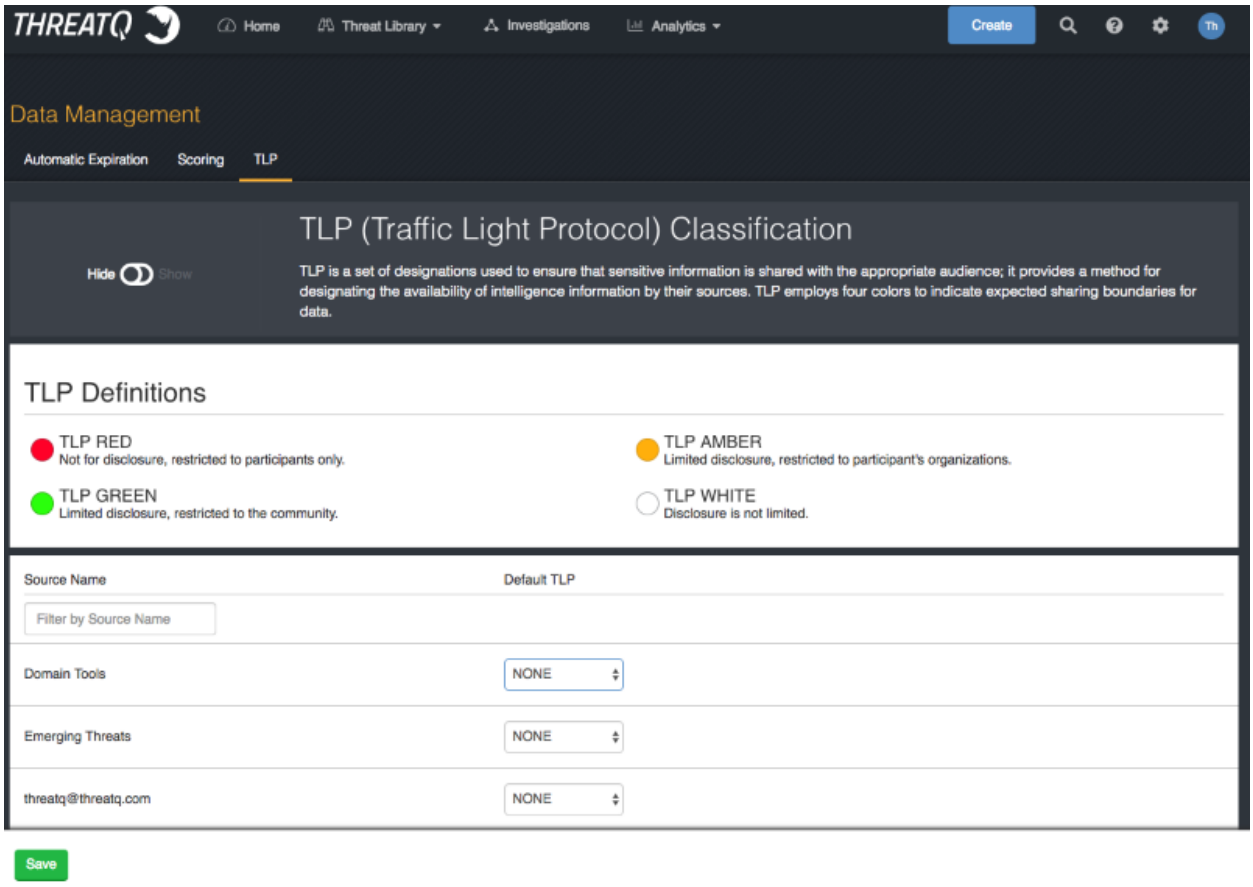
Configuring Date and Time Format

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.

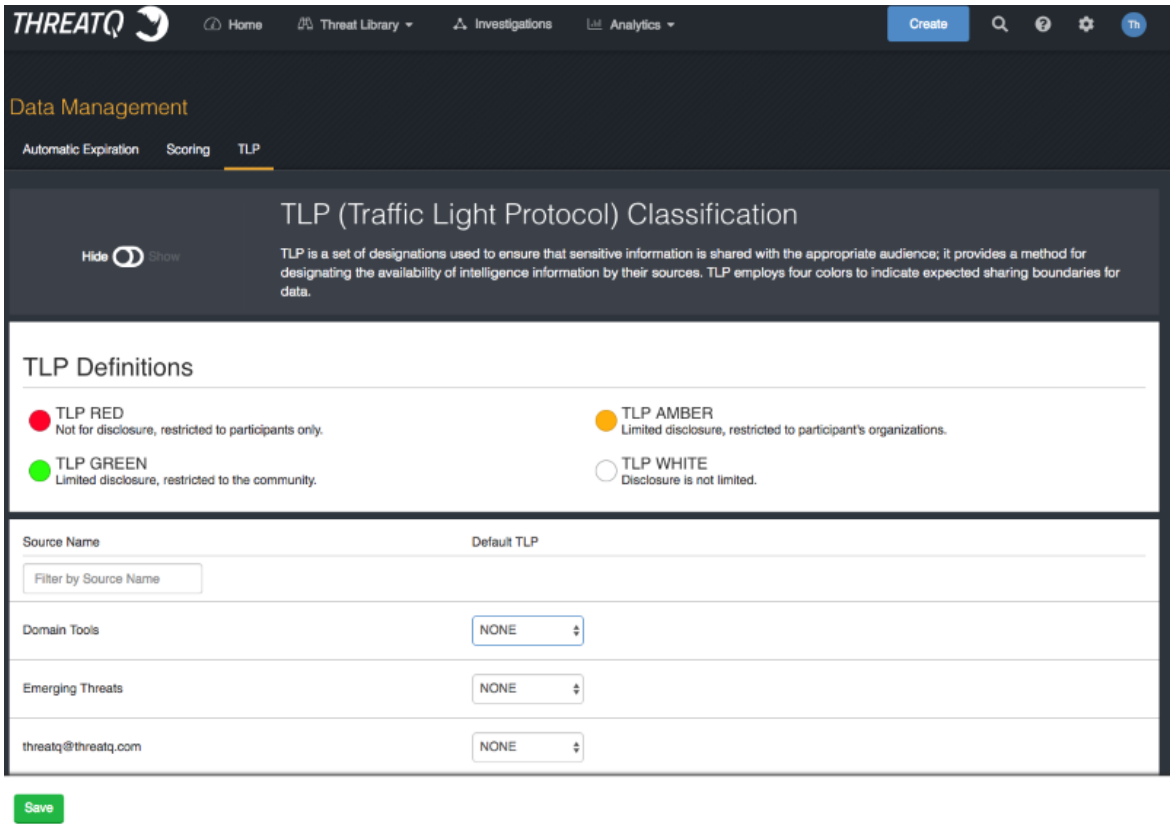
The Indicator Management option is now Data Management.

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.

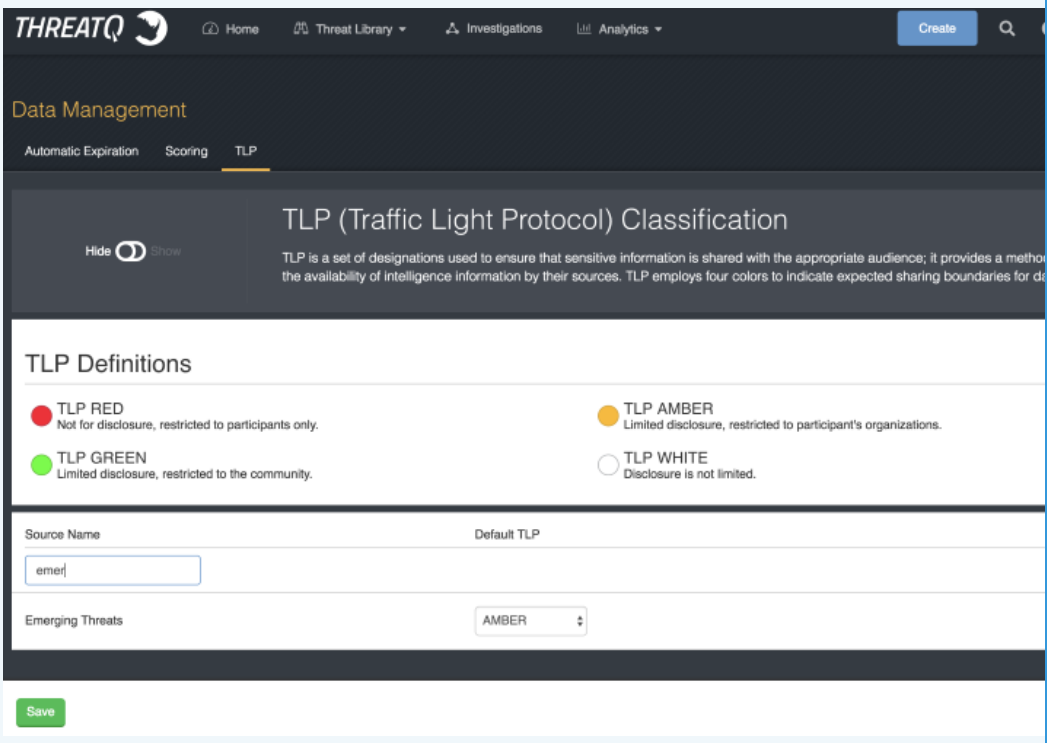


Apply TLP Classification to Source

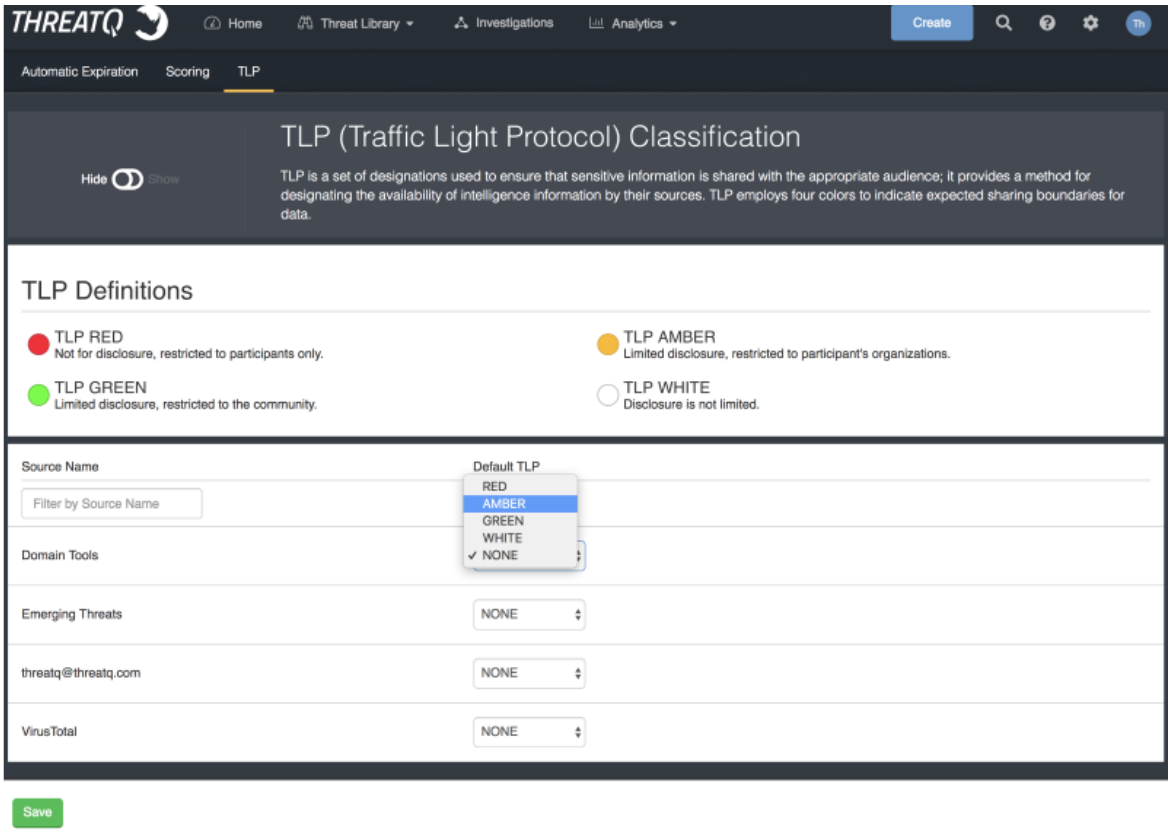
From the TLP Settings Page (see the Access TLP Settings topic):

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.



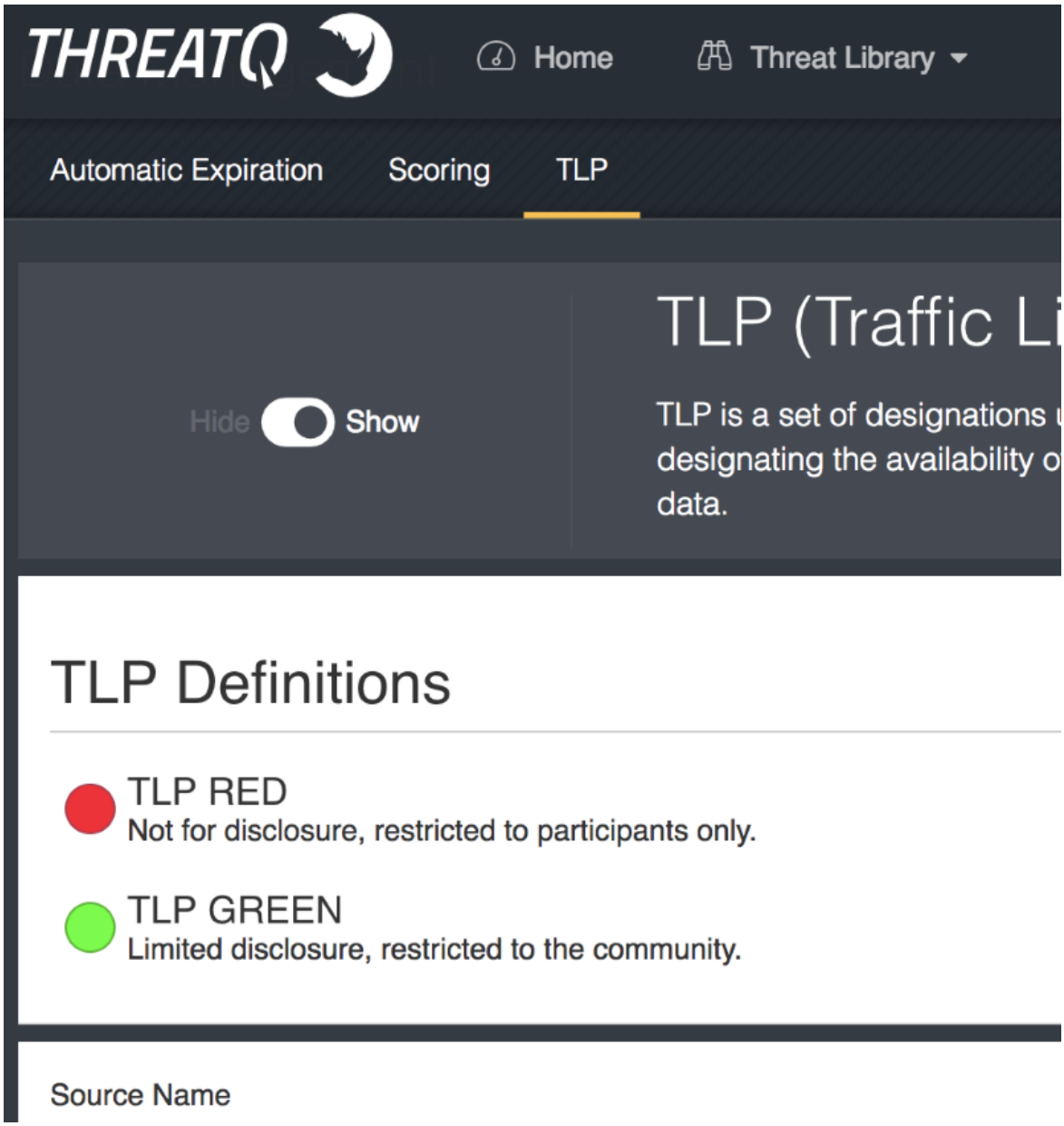
3. Click on **Save**.

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.

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

STIX Field	ThreatQ Field Mapping	ThreatQ Name
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 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 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

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Likely_Impact	Indicator.attribute	Likely Impact
Suggested_COAs	Course of Action	
Handling	Indicator.tlp	
Confidence	Indicator.attribute	Confidence
	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

STIX Field	ThreatQ Field Mapping	ThreatQ Name
	Indicator.published_at	

Related Topics

- STIX Data Mapping
- STIX Threat Actors 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 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

STIX Field	ThreatQ Field Mapping	ThreatQ Name
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 Threat Actors Mapping
- STIX Indicators Mapping
- STIX Observables Mapping

- STIX Campaigns 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

STIX Field	ThreatQ Field Mapping	ThreatQ Name
	Indicator.type	MD5
	Indicator.type	SHA-256
	Indicator.type	SHA-1
	Indicator.type	SHA-512
	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	

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

Related Topics

- STIX Data Mapping
- 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 Campaigns Mapping

STIX Field	ThreatQ Field Mapping	ThreatQ Name
Title	Campaign.value	
ID	Campaign.attribute	STIX Reference ID
Description	Campaign.attribute	Description
Short Description	Campaign.attribute	Short Description
Timestamp	Campaign.started_at	
Names	Campaign.attribute	Alias
Status	Campaign.attribute	Status
Intended_Effect	Campaign.attribute	Intended Effect

STIX Field	ThreatQ Field Mapping	ThreatQ Name
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 Threat Actors Mapping
- STIX Indicators Mapping
- STIX Exploit Targets Mapping
- STIX Observables Mapping
- STIX Campaigns 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

STIX Field	ThreatQ Field Mapping	ThreatQ Name
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		
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

STIX Field	ThreatQ Field Mapping	ThreatQ Name
	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 Threat Actors Mapping
- STIX Indicators Mapping
- STIX Exploit Targets Mapping
- STIX Observables Mapping

- STIX Campaigns 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
	TTP.attribute	Malware Type

STIX Field	ThreatQ Field Mapping	ThreatQ Name
	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

STIX Field	ThreatQ Field Mapping	ThreatQ Name
	TTP.attribute	Infrastructure Type
	TTP.attribute	Infrastructure
	TTP.attribute	Infrastructure Short Description
	TTP.attribute	Infrastructure Description
	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 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 CIQ Identity Mapping

STIX CIQ Identity Mapping

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

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.

Install CDF Command

The command below will allow you to install 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>
```

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

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

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

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

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.

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.

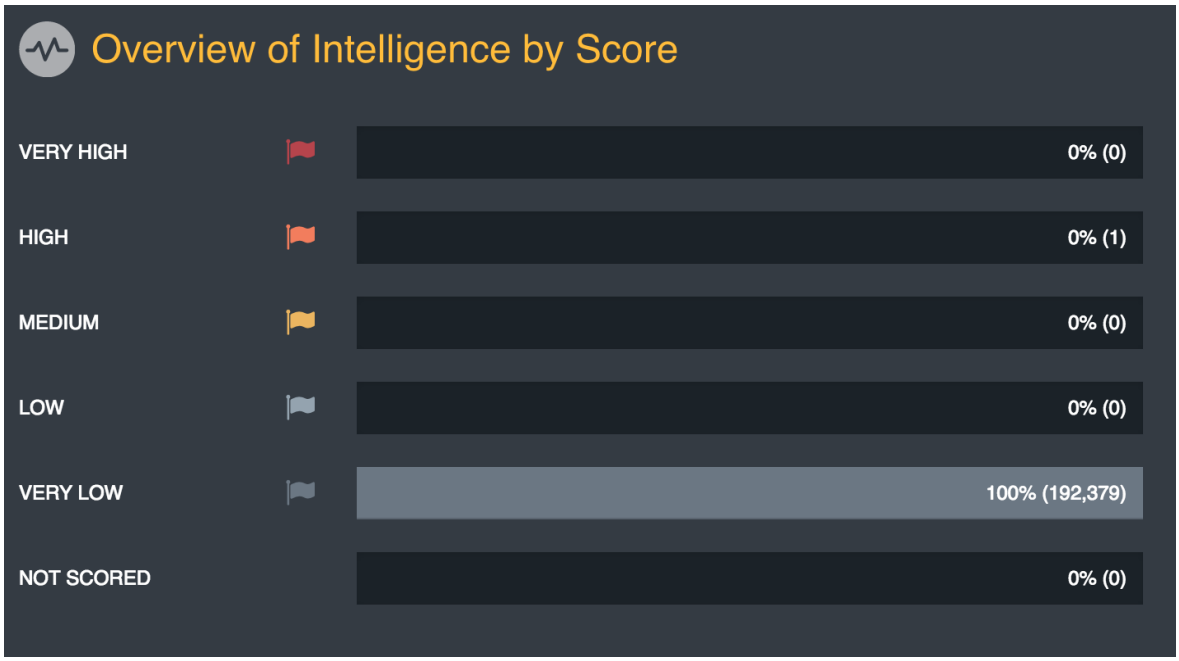
Overview of Intelligence By Score

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

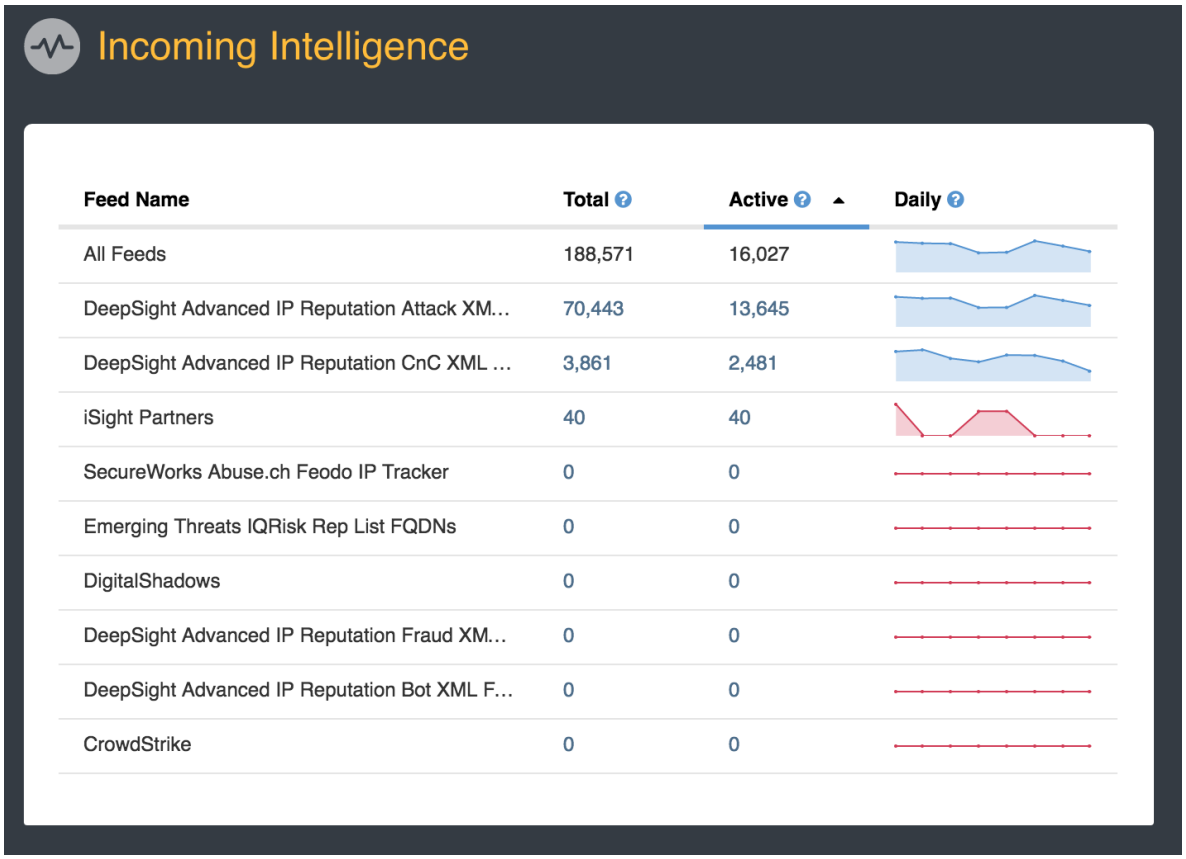
You may click on the percentage/number of indicators to launch an indicator search based on that criteria.



Incoming Intelligence

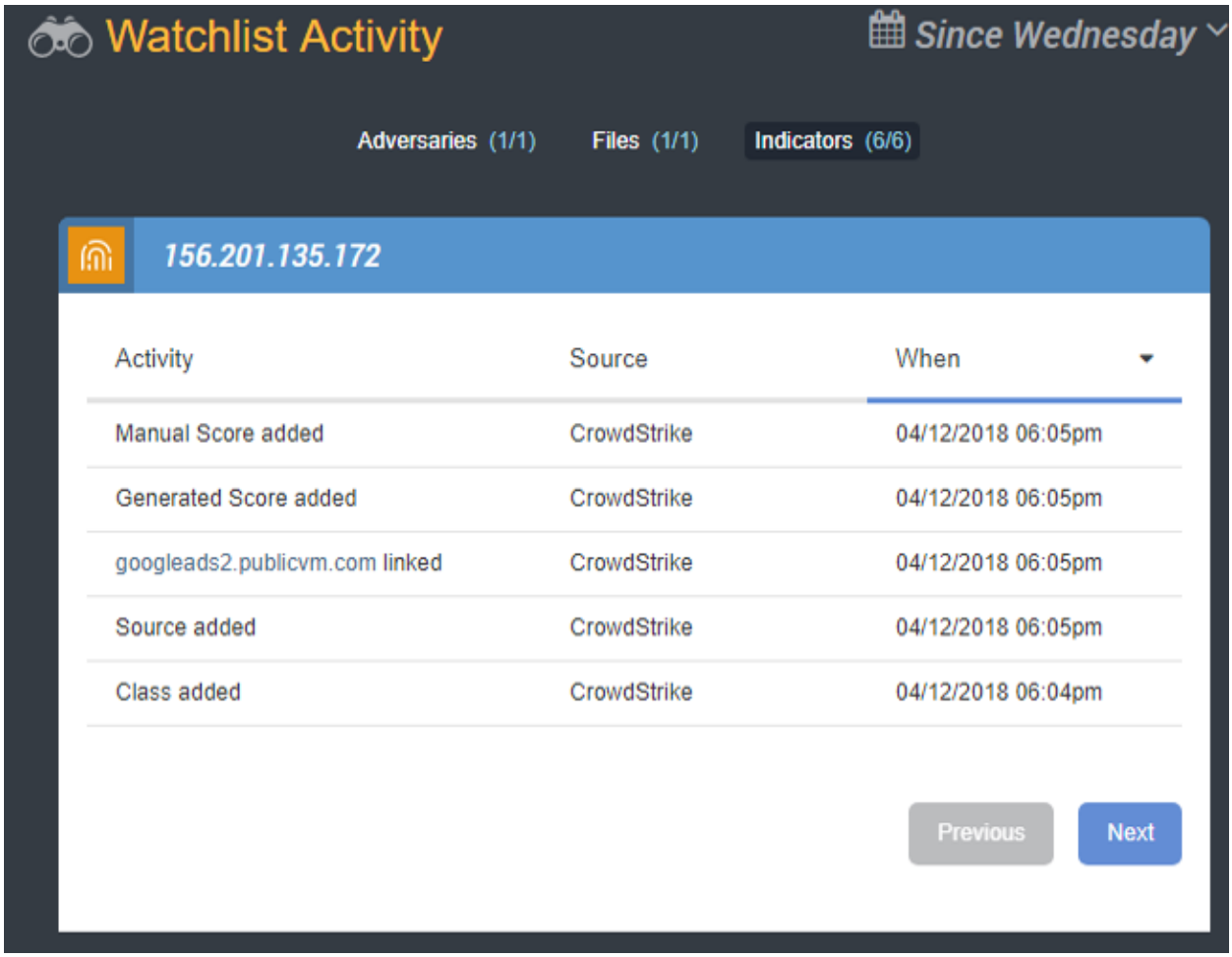
This dashboard graph provides a view of threat intelligence from all incoming feeds. The system categorizes threat intelligence by:

- 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)



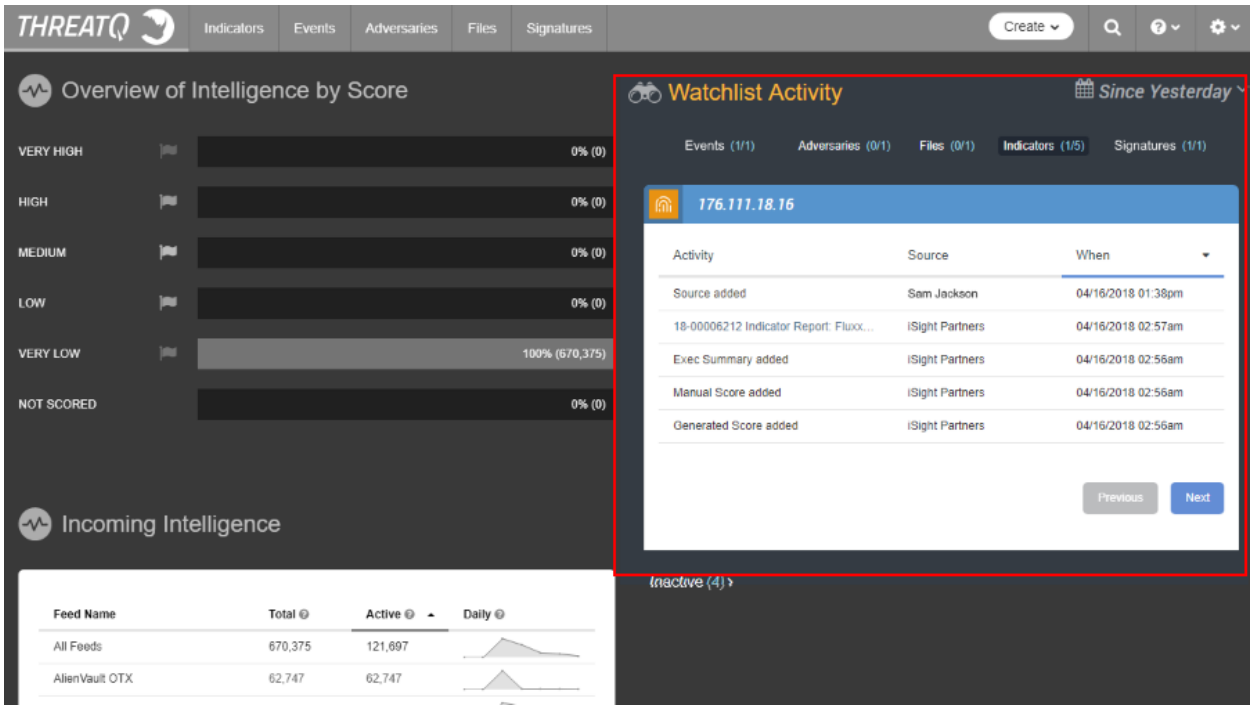
Watchlist Activity

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.

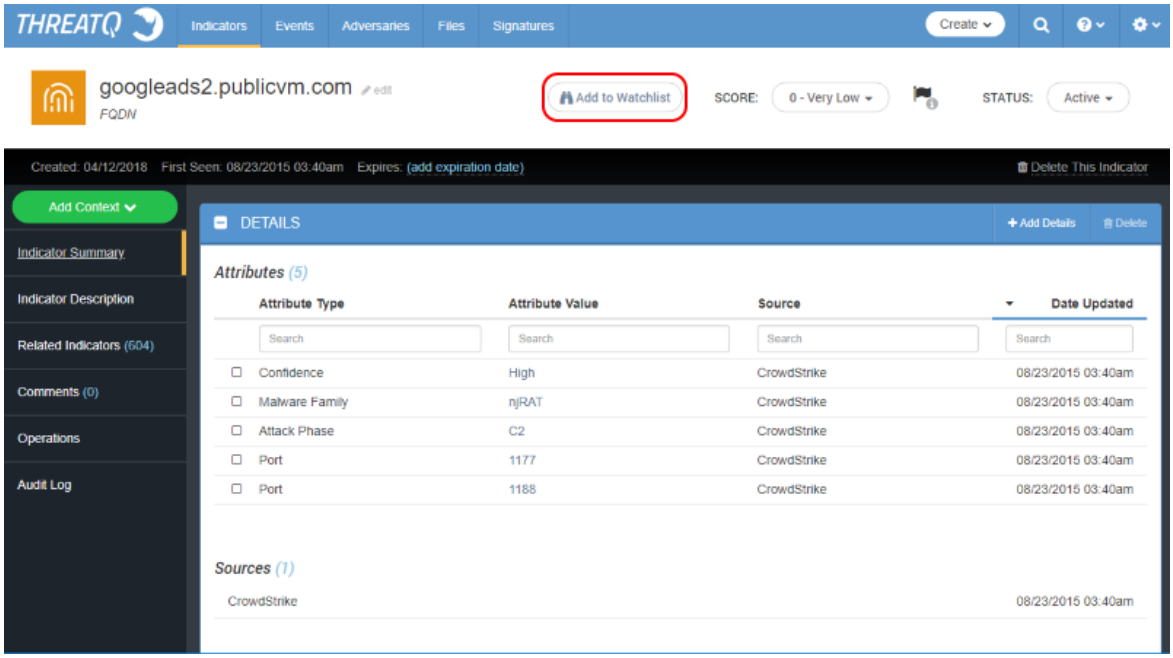


Configuring the Watchlist

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
- Finding Items By Object Type
- 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.
- 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:

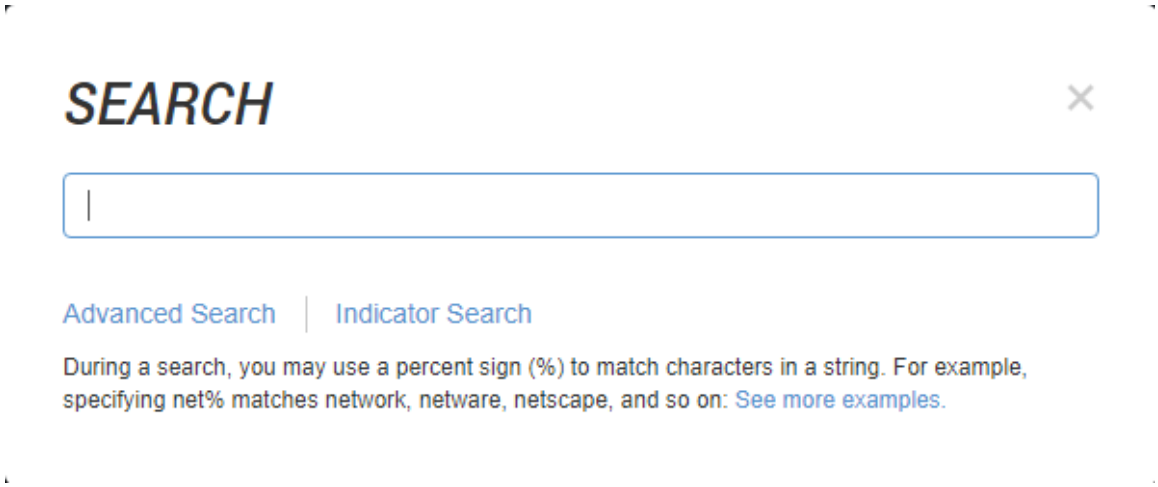
  - www.google.com (FQDN)
  - analytic.google.com (FQDN)
  - www.google.com/analytic (URL)
  - analytic@google.com (email address)

- Performing a Basic Search

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 Advanced Search.
   - If there is only one result, the object details page appears.

Advanced Search

Advanced Search allows you to search Indicators, Events, Adversaries, Files, Signatures, and so on for mentions of one or more search keywords that can exist in the object or any of its attributes. You can easily add and remove keywords to try out many search combinations. After fine-tuning your search results, you can save your search queries for later use.

Advanced search serves as the landing page when you select an object type from the Threat Library menu.

- Performing an Advanced Search
- Refining Your Advanced Search
- Saving Searches

- Choosing Attributes to Display in Search Results
- Exporting Search Results to a CSV file

Performing an Advanced Search

Build your object search by category, optionally including one or more keywords.

1. Choose the Search icon.
2. In the Search dialog box, choose **Advanced Search**.
3. Under **Threat Library**, choose your object search category.
4. Optionally, under Global Filters, enter a keyword to narrow your search.
5. Press **Enter** or **Return**.
6. Optionally, repeat steps 4 and 5 to further narrow your search.

Refining Your Advanced Search

After performing an advanced search, you can refine your search results by applying filters.

- Filtering a Search by Last Modified

Filtering a Search by Last Modified

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

Procedure:

1. Choose the Search icon.
2. In the Search dialog box, choose **Advanced Search**.
3. Perform an Advanced Search, as described in Performing an Advanced Search.
4. Choose **Filters > Last Modified**.

5. Select one of the following options to determine how the filter is applied:
    - 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.
6. Use the controls to select date options based upon the selection in step 5.
7. Click **Save**.

Filtering a Search by Dated Created

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

Procedure:

1. Choose the Search icon.
2. In the Search dialog box, choose **Advanced Search**.
3. Perform an Advanced Search, as described in Performing an Advanced Search.
4. Choose **Filters > Date Created**.
5. Select one of the following options to determine how the filter is applied:
    - is before - search results include items before a selected date
    - is after - search results include items after a selected date
    - is between - search results include items in a selected range of dates
    - is within the last - search results include items within the selected number of days.
6. Use the controls to select date options based upon the selection in step 5.
7. Click **Save**.

Saving 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.

1. Choose the Search icon.
2. In the Search dialog box, choose **Advanced Search**.
3. Perform an Advanced Search.
4. Choose **Save**.
5. In the Save Search dialog box, enter a name for the search.
6. Choose **Save Search**.

Running Saved Searches

Complete the following steps to run a Saved Search.

1. Choose the **Search icon** .
2. In the Search dialog box, choose **Advanced Search**.
3. Choose **Saved Searches** and then select the desired saved search from the list.

Deleting Saved Searches

Complete the following steps to delete a Saved Search.

1. Choose the **Search icon** .
2. In the Search dialog box, choose **Advanced Search**.
3. Choose **Saved Search** and then choose the desired saved search from the list.
4. Click the Delete icon.

Choosing Attributes to Display in Search Results

You can choose which attributes to display in your search results by completing the following steps:

1. Choose the **Search icon** .
2. In the Search dialog box, choose **Advanced Search**.
3. Perform your search.
4. Choose **Manage Columns**.
5. Select the attributes you wish to display. Clear the attributes you wish to hide.

Exporting Search Results to a CSV file

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.

1. Choose the **Search icon** .
2. In the Search dialog box, choose **Advanced Search**.
3. Perform your search.
4. Choose **Export**.

   The CSV file downloads to your desktop.

Clearing Your Search

Complete the following steps to clear your search, so that you may begin a new search.

1. Choose the Search icon.
2. In the Search dialog box, choose **Advanced Search**.
3. Perform and refine your search.

4. In the Search field, choose **clear all filters**.
5. In the dialog box, choose **Reset Search**.

Filtering by Relationship

The Relationship Filter option allows you to filter search results 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.

Filtering using Related Objects

Using the **Relationship** filter allows you to filter search results based on related objects.

From the search results:

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

   The Filter by Relationship modal will open.

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 both. 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.

Filter by Attributes

The Filter by Attribute feature is available with ThreatQ version 4.6 and later.

The Filter by Attribute option allows users to filter search results by Attribute Types and Values.

Using the Attributes filter, users can:

- Filter search results to include/exclude objects using a specific Attribute Type and Attribute Value.
- Filter search results to include/exclude objects using a specific Attribute Type and any Attribute Value.
- Filter search results to include/exclude objects using multiple Attribute filters. Users will also have the option to set the filter to include objects that fit one of the multiple filters or all.

See the following topics for more details:

- Filter Using WITH Attribute Option
- Filter Using WITHOUT Attribute Option
- Edit Existing Attribute Filter
- Apply Multiple Filters
- Common Scenarios

Filter Using WITH Attribute Option

The Filter by Attribute feature is available with ThreatQ version 4.6 and later.

Using the **With Attribute** filter allows users to include objects with a specific attribute.

From the search results:

1. Click on the **Filters** option and select **With Attribute**.

   The Attribute modal will open.

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 **Add** to apply the filter.

Filter Using WITHOUT Attribute Option

The Filter by Attribute feature is available with ThreatQ version 4.6 and later.

Using the **Without Attribute** filter allows users to exclude objects with a specific attribute.

From the search results:

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

   The Attribute modal will open.

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 **Add** to apply the filter.

Edit Existing Attribute Filter

Users can edit existing Attribute filters applied to the search results.

From the search results:

1. Click on the **Filters** option and select they type of filter option to edit.

   ***Example**: If you are editing a W**ithout Attribute**, select **Without Attribute** option from the **Filter** dropdown.*
   The Attribute modal will open.

2. Make all the required updates and click on **Add** to apply the updated filter.

Apply Multiple Filters

Users have the ability to apply multiple Attribute filters to the search results. Users also have the ability to configure **Any/All** options for the filters to include objects that fit one of the filters or all.

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

   The Attribute modal will open.

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 modal to add another attribute and repeat steps 2-3.
5. Click on the **Add** button.

The filters will be applied to the search results.

The **Match Any/All** toggle option will allow users to configure the filter to include objects that either fit one attribute filter or both. 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 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 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 modal pops up with an attribute form.

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 modal pops up with an attribute form.

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 modal pops up with an attribute form.

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 modal pops up with an attribute form.

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 modal pops up with an attribute form.

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

Filter by Status

The Filter by Status feature is available with ThreatQ version 4.6 and later. Users can filter search results by the object's status.

Users can filter **Indicators**, **Signatures** and **Tasks** by Status.

From the search results page:

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

   Users 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.

Common Scenarios

Apply Status Filter

1. User clicks on the **Threat Library** tab and selects on the **Indicators** tab.
2. User clicks on the **Status** filter button and selects **Active**.

   *The results page will automatically update to show only indicators with a status of **Active**.*

Apply Status Filter and Type Filter

1. User clicks on the **Threat Library** tab and selects on the **Indicators** tab.
2. User clicks on the **Status** filter button and selects **Active**.

   *The results page will automatically update to show only indicators with a status of **Active**.*

3. The User clicks on the **Type** filter and selects **IP Addresses**.

   *The results page will automatically update to show all **IP Addresses** with a status of **Active***

Apply Multiple Status Filters

1. User clicks on the **Threat Library** tab and selects on the **Indicators** tab.
2. User clicks on the **Status** filter button and selects **Active**.

   *The results page will automatically update to show only indicators with a status of **Active**.*

3. User clicks on the **Status** filter button and selects **Expired**.

*The results page will automatically update to show all indicators with a status of **Expired** OR **Active**.*

Filter by Source

The Filter by Source feature is available with ThreatQ version 4.6 and later. Users can filter search results by the object's source.

From the search results page:

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

   A source header will load above the results.

2. Click on the **Add Source** link and select the source to used in the filter.
3. Repeat step 2 to add multiple **Source** filters to the results.

Users applying multiple **Source** filters to the results can use the **Must Match** toggle option to determine whether the objects match **Any** or **All** of the sources identified in the filter.

Filtering by Object Type

The Filter by Object Type global filter allows you to filter search results by object type such as indicators or events.

You can also select an object type from the Threat Library navigation menu to automatically filter the Threat Library to that specific object type.

From the Advanced Search page:

1. Click on the **Object Type** dropdown in the *Global Filters* section of the page.

The filter will display as **All Objects** by default.

2. Select the checkboxes next to the object type(s) to apply to the search results.

   The search results will filter automatically.

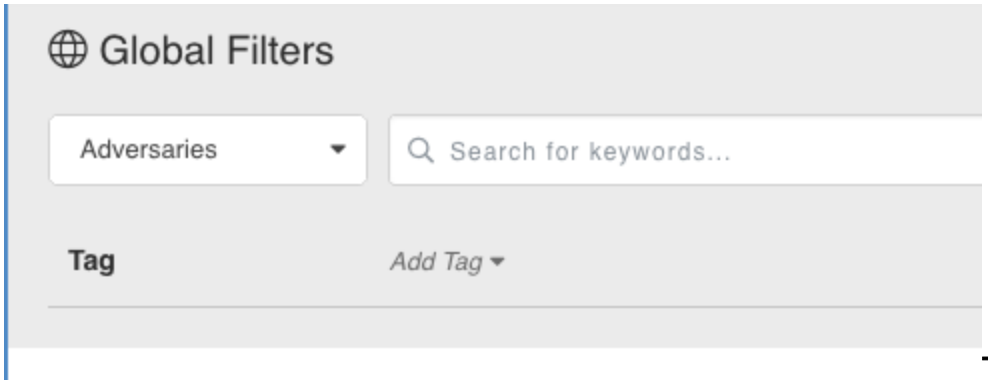
3. Click on the **Object Type** dropdown to select new object types and clear existing ones.

Filtering using Tags

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

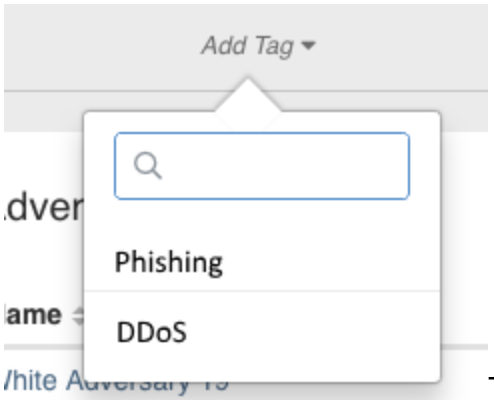
From the search results:

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. Repeat 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.

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

Procedure

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 dropdown menus, and enter the values.

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

Parameter	Operator
	Is before Is in the range of Is Blank Is Not Blank
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 menu 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.

Procedure:

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 drop down menu.
6. Optionally, enter an additional source.
7. Optionally, apply one or more attributes:
    - Choose an Attribute Type from the drop down menu.
    - Enter an Attribute Value.
    - Enter an Attribute Source.
    - 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 drop down menu.
10. Click **Apply Changes**.

Finding Items By Object Type

To find items by object type, you can use the Advanced Search feature from the main menu or select an object from the **Threat Library** menu. From here, add keywords or filters to fine-tune the search results.

Procedure

From the main menu, select **Threat Library > [Your Desired Object Type]**.

The Advanced Search results 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"

Indicators

Within this section, the following options are available:

- Viewing Indicators
- Indicators Overview Page
- Network Indicators Page
- Host Indicators Page

Adding an Indicator

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

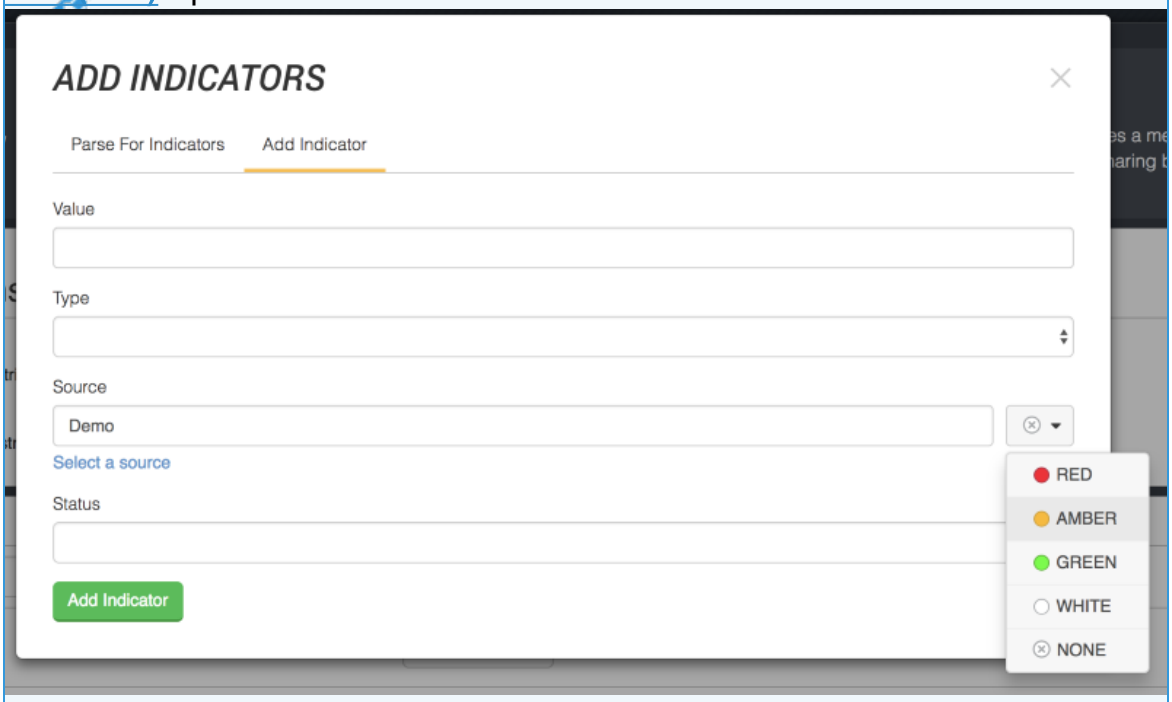
You can also select Indicator Parser from the Create menu if importing a file. The option is located under the Import section of the Create menu. See the Parse for an Indicator topic.

The **Add Indicators** dialog box will open.

2. Enter a value in the **Value** field.
3. Select the **Type of Indicator**.
4. Select a **Source** from the provided dropdown menu.

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 theTraffic Light Pro-

tocol (TLP) topic for more information on TLP classifications.



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

Parse 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 modal 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.

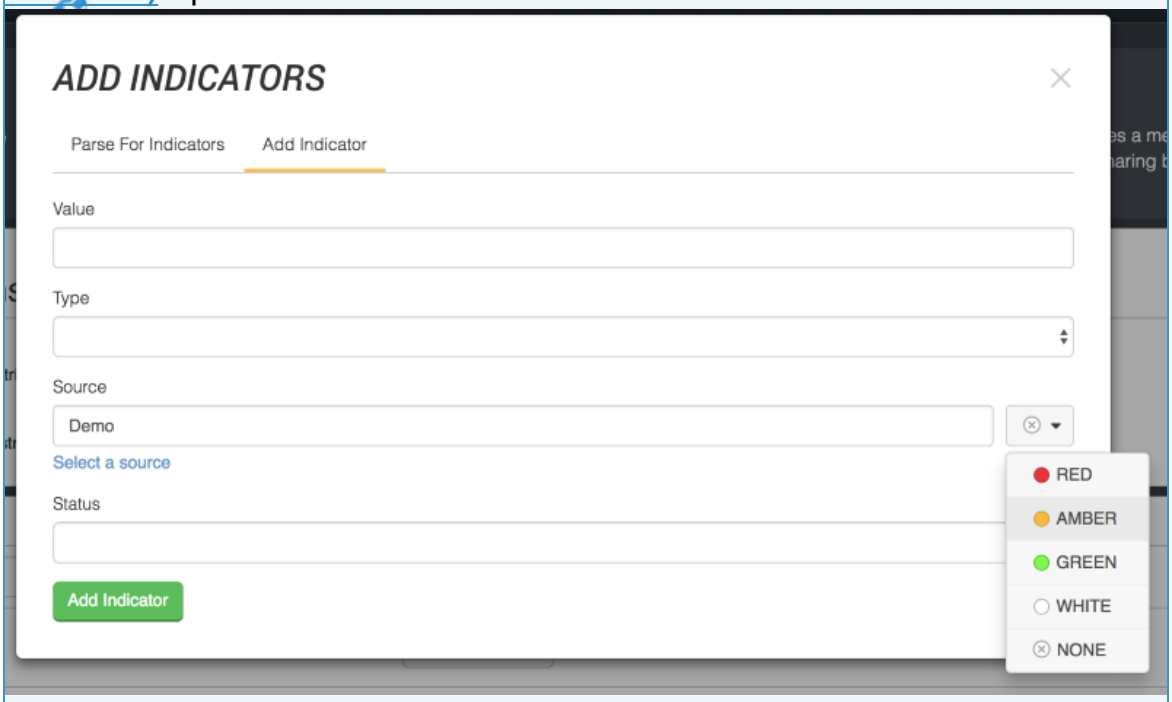
3. Select the **Parser** to use and click on **Next Step**.
4. Select whether to save or delete the file after the import.

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 Pro-

tocol (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 isolate 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**.

The Indicators Overview page auto-refreshes with the new indicators added to the data, and a confirmation alert appears in an alert bar at the top of the page.

.CSV File Format for Proper 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.

Viewing Indicators

There are three ways to access a list of indicators:

- Indicators Overview Page
- Network Indicators Page
- Host Indicators Page

Indicators Overview Page

This 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.

Within this section, the following options are available:

- Accessing the Indicators Overview Page
- Indicators Overview Page: Information and Functions

Accessing the Indicators Overview Page

1. In the navigation menu, choose **Analytics > Indicators**.
2. The Indicators Overview page opens.

Indicators Overview Page: Information and Functions

The Indicators Overview page consists of three sections:

- Recently Created Indicators histogram
- Recently Created Indicators Summary table
- Most Recent 100 Indicators table

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:

- ***Viewing the number of indicators created each day by type***

  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***

  Drag your mouse over a section of the histogram, and your view will be magnified.

  Click **Reset Zoom** to return to the full histogram.

- ***Printing the histogram or downloading it as a PNG, JPEG, PDF, or SVG file***

  Click the hamburger menu (see graphic below), and select the desired option.

Recently Created Indicators Summary table

Immediately below the histogram is a summary table, showing you indicator totals by status, network, and host. The following functions are available:

- *Sorting the table by a column*

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

- *Conducting a search based on one of the criteria in the table*

  Click the desired criterion (a status, network, or host).

Most Recent 100 Indicators table

This table shows the 100 most recent indicators, the date and time they were created, and their name, type, status, and sources. The following functions are available:

- *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.

- *Searching within a column*

  Click within the search box at the top of the column, and enter your search criteria.

- *Accessing the Indicator Details page for one of the indicators*

  Click an indicator to access the Indicator Details page.

Network Indicators Page

This page provides an overview of how many and which types of indicators were added to the system within the last 15 days, as well as supporting information related to them. Within this section, the following options are available:

- Accessing the Network Indicators Page
- Network Indicators Page Information & Functions

Accessing the Network Indicators Page

- In the navigation menu, choose **Analytics > Network Indicators** and then choose the **Network** tab.
  The Network Indicators page opens.

Network Indicators Page Information & Functions

The Network Indicators page consists of the following sections:

- Recently Created Indicators histogram
- Recently Created Indicators Summary table
- Attributes pane
- Recent Sources scatterplot
- Attack Phases pie chart
- Indicators By Type pie chart

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:

- *Viewing the number of indicators created each day by type*

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*

  Drag your mouse over a section of the histogram, and your view will be magnified.

  Click **Reset Zoom** to return to the full histogram.

- *Printing the histogram or downloading it as a PNG, JPEG, PDF, or SVG file*

  Click the hamburger menu (see graphic below), and select the desired option.

Summary Table

Immediately below the histogram is a summary table, showing you a breakdown of indicators by date, name, type (network/host), status, and sources. The following functions are available:

- *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.

- *Searching within a column*

  Click within the search box at the top of the column, and enter your search criteria.

- *Accessing the Indicator details page for one of the listed indicators*

  Click the indicator to open the Indicator Details page.

Attributes pane

The attributes pane helps provide insight into trends of attribute values and keys. Analysts are able to see which attribute keys they have the most information for, and use that information to look for trends. The attributes pane is made up of a number of areas:

- Recently Created Indicators Attributes List
- Accessed Time Top 10 Values Circle Graph
- Indicator Values List

Recently Created Indicators Attributes List

The attributes list on the left side lists attributes related to indicators in your system and gives you ways to access more information about them. The following functions are available:

- *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.

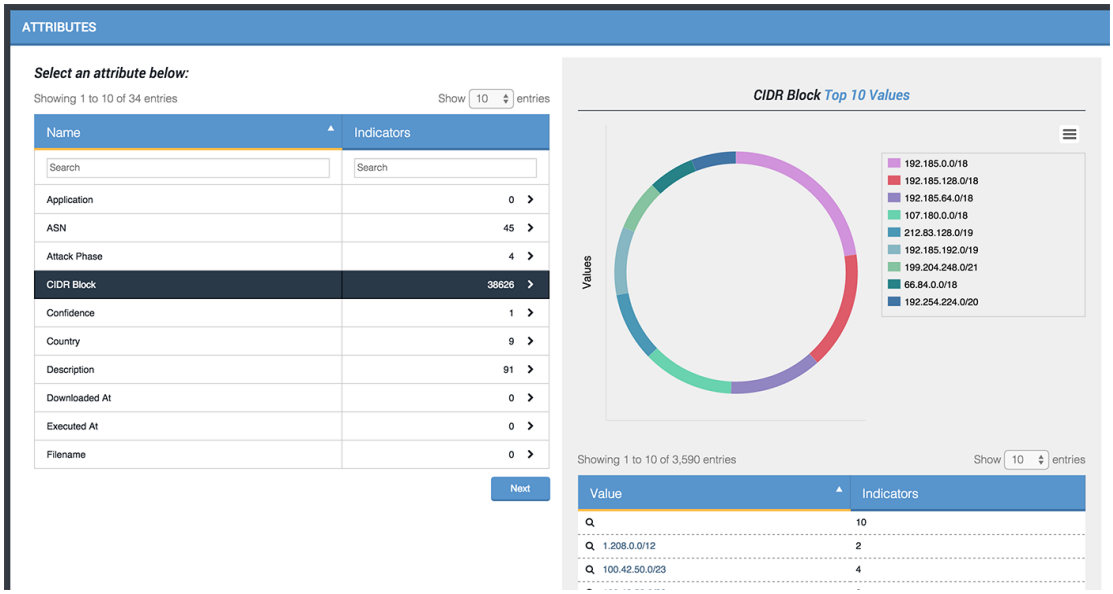
- *Searching within a column*

  Click within the search box at the top of the column, and enter your search criteria.

- *Viewing more information about a selected attribute*

  Select the row/attribute in the table, and additional information will populate the right side.

Accessed Time Top 10 Values Circle Graph



Once an attribute has been selected, and the right side is populated, this circle graph is accessible. The following functions are available:

- ***Viewing more information about a selected value***

  Hover over a colored section of the circle graph to open a popup identifying the attribute name and how different indicators contain the exact attribute.

- ***Hiding or unhiding one of the values from the circle graph***

  Click the value on the right of the circle graph to remove it from the graph; click a second time to reinstate it.

- ***Printing the circle graph or downloading it as a PNG, JPEG, PDF, or SVG file***

  Click the hamburger menu (see graphic below), and select the desired option.

Indicator Values List

This table lists each value and the number of related indicators. The following functions are available:

- Changing the number of entries displayed in the table

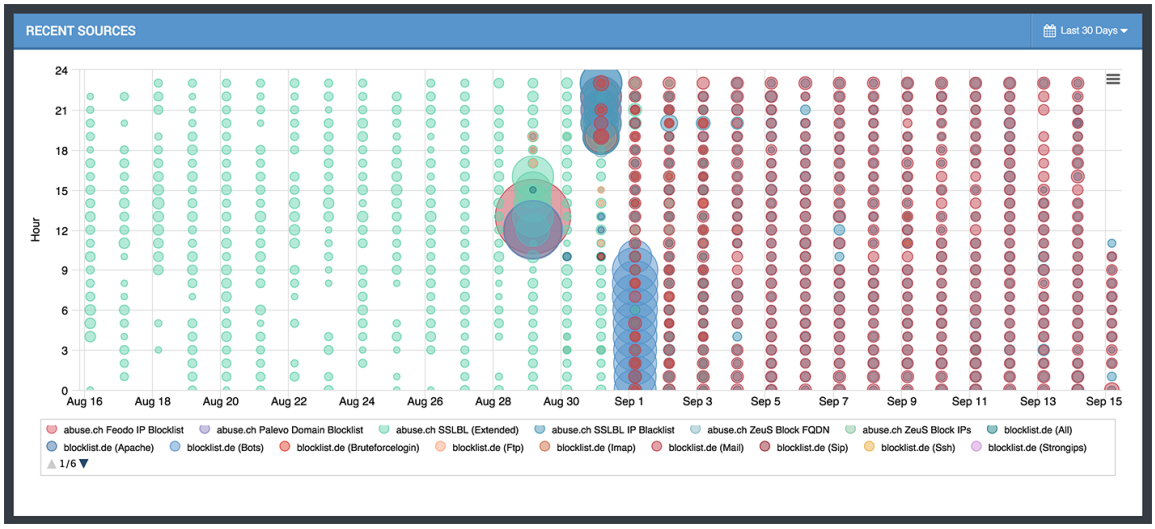
  Click the dropdown menu at the top right of the table and select the desired option.

- Conducting an indicator search based on one of the values

  Click the value to open the Indicator Search tool.

  For more information on using the advanced search tool, see Performing an Indicator Search.

Recent Sources scatterplot



This scatterplot shows how many indicators were provided by a given source each day within a specified timeframe. The following functions are available:

- *Viewing the date and number of indicators from a given source*

  Hover over one of the circles to open a popup with this information.

- *Adjusting the timeframe of the information displayed*

  Click the dropdown menu at the top right and select the desired timeframe.

- *Hiding or unhiding one of the values from the scatterplot*

  Click the source in the legend under the scatterplot to hide it. Click again to unhide it.

Attack Phases pie chart

Attack phases are the ways an indicator might be used. They are listed as indicator attributes. This pie chart shows the number of indicators that fall under each attack phase. The following functions are available:

- *Viewing the number of indicators with a given attack phase*

  Hover over one of the sections of the pie chart to open a popup with this information.

- *Adjusting the timeframe of the information displayed*

  Click the dropdown menu at the top right and select the desired timeframe.

- *Hiding or unhiding one of the values from the pie chart*

  Click the source in the legend to hide it. Click again to unhide it.

Indicators By Type pie chart

This pie chart shows you the number of indicators by type. The outer ring displays indicators in review, and the inner ring shows totals. The following functions are available:

- **Viewing the number of indicators of a given type**

  Hover over one of the sections of the pie chart to open a popup with this information.

- **Adjusting the timeframe of the information displayed**

  Click the dropdown menu at the top right and select the desired timeframe.

- **Hiding or unhiding one of the values from the pie chart**

  Click the type in the legend to hide it. Click again to unhide it.

Host Indicators Page

The Host Indicators page provides an overview of how many and which types of indicators were added to the system within the last 15 days, as well as supporting information related to them. Within this section, the following options are available:

- Accessing the Host Indicators Page
- Host Indicators Page: Information & Functions

Accessing the Host Indicators Page

- In the navigation menu, choose **Analytics > Indicators** and then choose **Host**. The Host Indicators page opens.

Host Indicators Page: Information & Functions

The Host Indicators page consists of the following sections:

- Recently Created Indicators histogram
- Host Indicators Summary table
- Host Indicators Attributes pane
- Host Indicators Recent Sources scatterplot
- Host Indicators Attack Phases pie chart
- Host Indicators Summary table

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:

- *Viewing the number of indicators created each day by type*

  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*

  Drag your mouse over a section of the histogram, and your view will be magnified.

  Click **Reset Zoom** to return to the full histogram.

- *Printing the histogram or downloading it as a PNG, JPEG, PDF, or SVG file*

  Click the hamburger menu (see graphic below), and select the desired option.

Host Indicators Summary table

Immediately below the histogram is a summary table, showing you a breakdown of indicators by date, name, type (network/host), status, and sources. The following functions are available:

- *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.

- *Searching within a column*

  Click within the search box at the top of the column, and enter your search criteria.

Host Indicators Attributes pane

The attributes pane helps provide insight into trends of attribute values and keys. Analysts are able to see which attribute keys they have the most information for, and use that information to look for trends. The attributes pane is made up of a number of areas:

- Host Indicators Attributes List
- Host Indicators Accessed Time Top 10 Values Circle Graph
- Host Indicators Values List

Host Indicators Attributes List

The attributes list on the left side lists attributes related to indicators in your system and gives you ways to access more information about them. The following functions are available:

- *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.

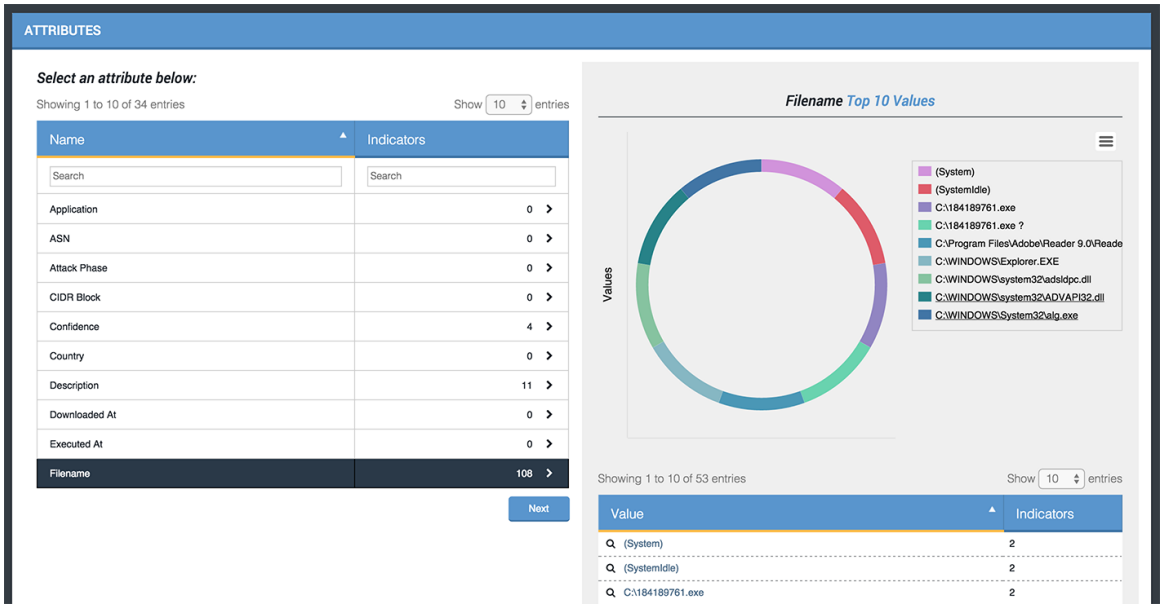
- *Searching within a column*

  Click within the search box at the top of the column, and enter your search criteria.

- *Viewing more information about a selected attribute*

  Select the row/attribute in the table, and additional information will populate the right side.

Host Indicators Accessed Time Top 10 Values Circle Graph



Once an attribute has been selected, and the right side is populated, this circle graph is accessible. The following functions are available:

- ***Viewing more information about a selected value***

  Hover over a colored section of the circle graph to open a popup identifying the attribute name and how different indicators contain that exact attribute.

- ***Hiding or unhiding one of the values from the circle graph***

  Click the value on the right of the circle graph to remove it from the graph; click a second time to reinstate it.

- ***Printing the circle graph or downloading it as a PNG, JPEG, PDF, or SVG file***

  Click the hamburger menu (see graphic below), and select the desired option.

Host Indicators Values List

This table lists each value and the number of related indicators. The following functions are available:

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

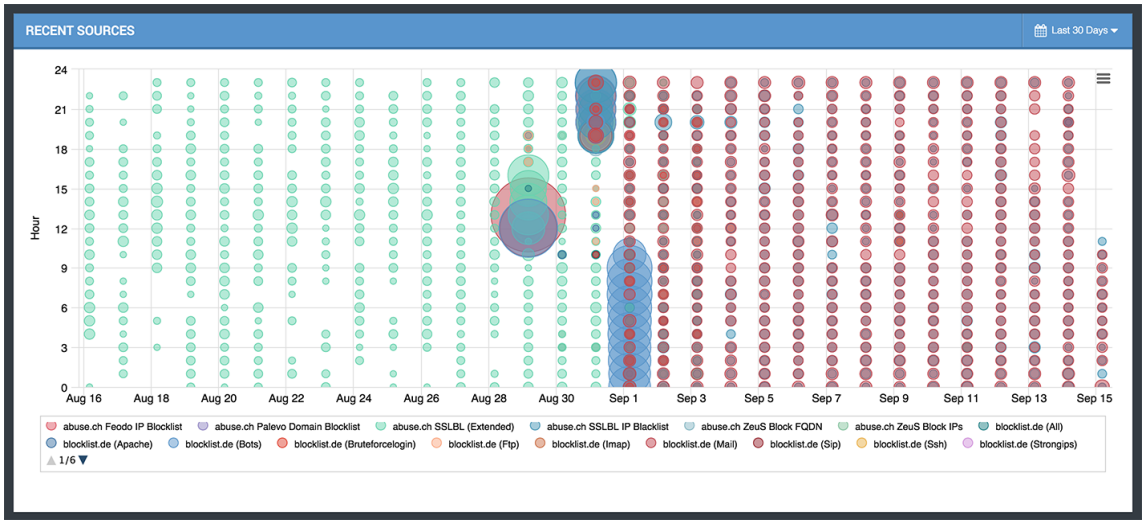
  Click the dropdown menu at the top right of the table and select the desired option.

- *Conducting an indicator search based on one of the values*

  Click the value to open the Indicator Search tool.

  For more information on using the advanced search tool, see Performing an Indicator Search.

Host Indicators Recent Sources scatterplot



This scatterplot shows how many indicators were provided by a given source each day within a specified timeframe. The following functions are available:

- *Viewing the date and number of indicators from a given source*

  Hover over one of the circles to open a popup with this information.

- *Adjusting the timeframe of the information displayed*

  Click the dropdown menu at the top right and select the desired timeframe.

- *Hiding or unhiding one of the values from the scatterplot*

  Click the source in the legend under the scatterplot to hide it. Click again to unhide it.

Host Indicators Attack Phases pie chart

Attack phases are the ways an indicator might be used. They are listed as indicator attributes. This pie chart shows the number of indicators that fall under each attack phase. The following functions are available:

- *Viewing the number of indicators with a given attack phase*

  Hover over one of the sections of the pie chart to open a popup with this information.

- *Adjusting the timeframe of the information displayed*

  Click the dropdown menu at the top right and select the desired timeframe

- *Hiding or unhiding one of the values from the pie chart*

  Click the source in the legend to hide it. Click again to unhide it.

Host Indicators By Type pie chart

This pie chart shows you the number of indicators by type. The outer ring displays indicators in review, and the inner ring shows totals. The following functions are available:

- *Viewing the number of indicators of a given type*

  Hover over one of the sections of the pie chart to open a popup with this information.

- *Adjusting the timeframe of the information displayed*

  Click the dropdown menu at the top right and select the desired timeframe.

- *Hiding or unhiding one of the values from the pie chart*

  Click the type in the legend to hide it.

Indicator Details Page

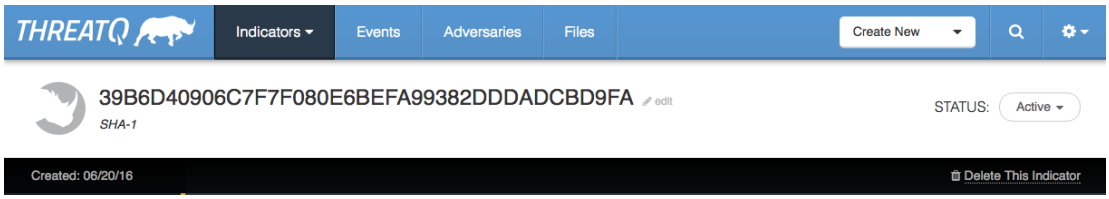
Within this section, the following options are available:

- Accessing the Indicator Details Page for a Particular Indicator
- Indicator Details Page: Information & Functions

Accessing the Indicator Details Page for a Particular Indicator

- Locate and click the indicator.
  The Indicator Details page opens.

Indicator Details header



At the top of the Indicator Details page is a header with the indicator value, date created, type, and status.

The following functions are available:

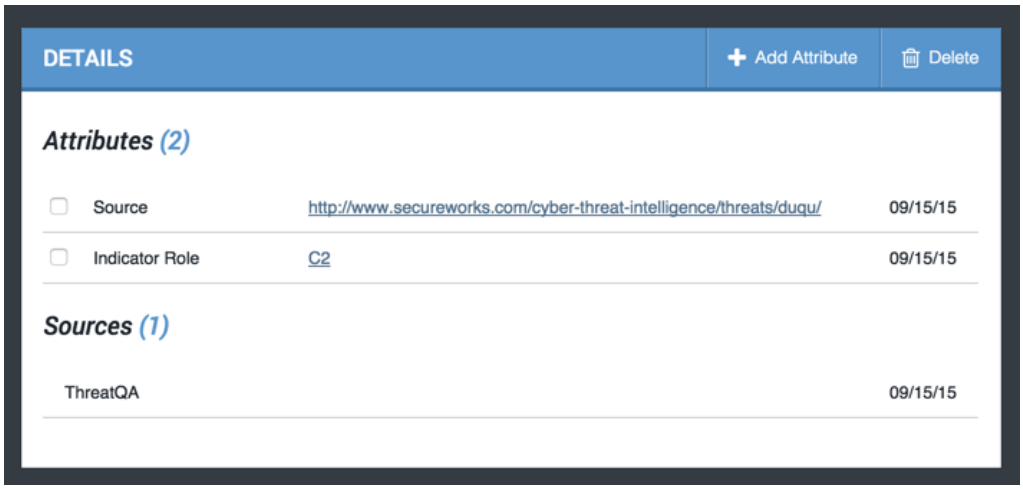
- Editing the Value of an Indicator
- Changing the Type Associated with an Indicator
- Changing the Status of an Indicator
- Deleting an Indicator

Indicator Details Summary Page: Information & Functions

The Indicator Details Summary page consists of five sections:

- Details pane
- Related Adversaries pane
- Related Events pane
- Related Files pane
- Related Indicators pane

Details pane



This pane provides information about the attributes and sources of the Indicator, including the name and date created. The following functions can be performed:

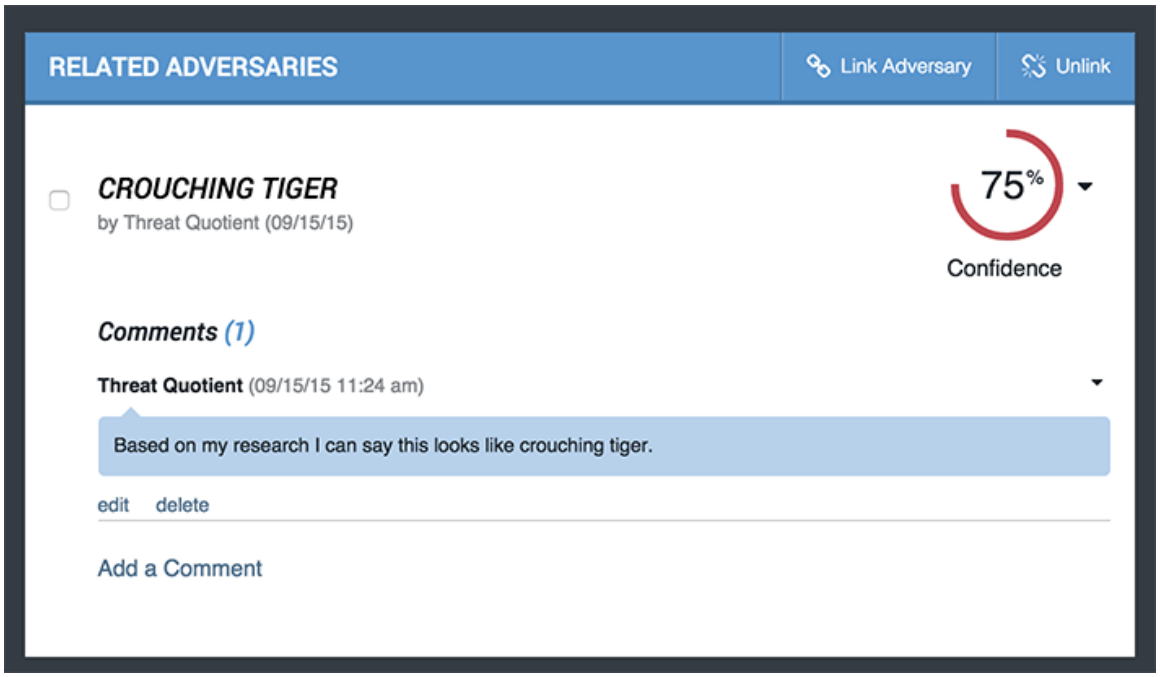
- Adding an Attribute to an Indicator
- Deleting an Attribute from an Indicator

Performing a search for a listed attribute

Click the attribute to set it as a search criterion and open the Advanced Search page.

For more information on using the advanced search tool, see Performing an Indicator Search.

Related Adversaries pane



This pane provides information about adversaries related to the indicator, including the name and date created, and the confidence level. The following functions are available:

- Linking an Adversary to an Indicator
- Unlinking an Adversary from an Indicator
- Editing the Confidence Level of an Adversary Related to an Indicator
- Adding a Comment to an Adversary Related to an Indicator
- Viewing a Comment for an Adversary Related to an Indicator
- Editing a Comment for an Adversary Related to an Indicator
- Deleting a Comment for an Adversary Related to an Indicator

For more information on one of the functions, click the function.

Related Events pane

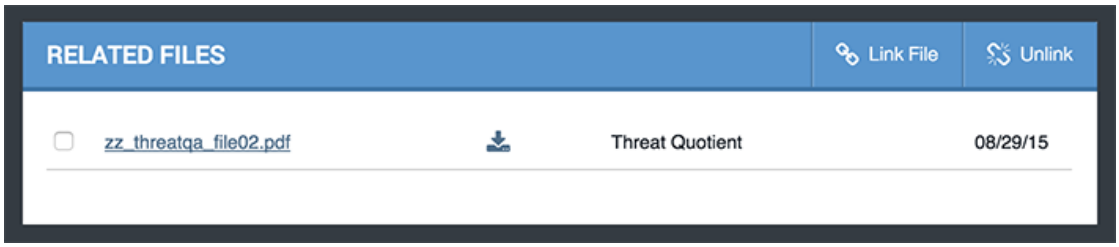
This pane provides information about events related to the indicator, including the date and type of the event. The following functions are available:

- Sorting the list by date or type

  Use the dropdown menu.

- Linking an Event to an Indicator
- Unlinking an Event from an Indicator

Related Files pane



This pane provides information about files related to the indicator, including the name and the date the file was created. The following functions are available:

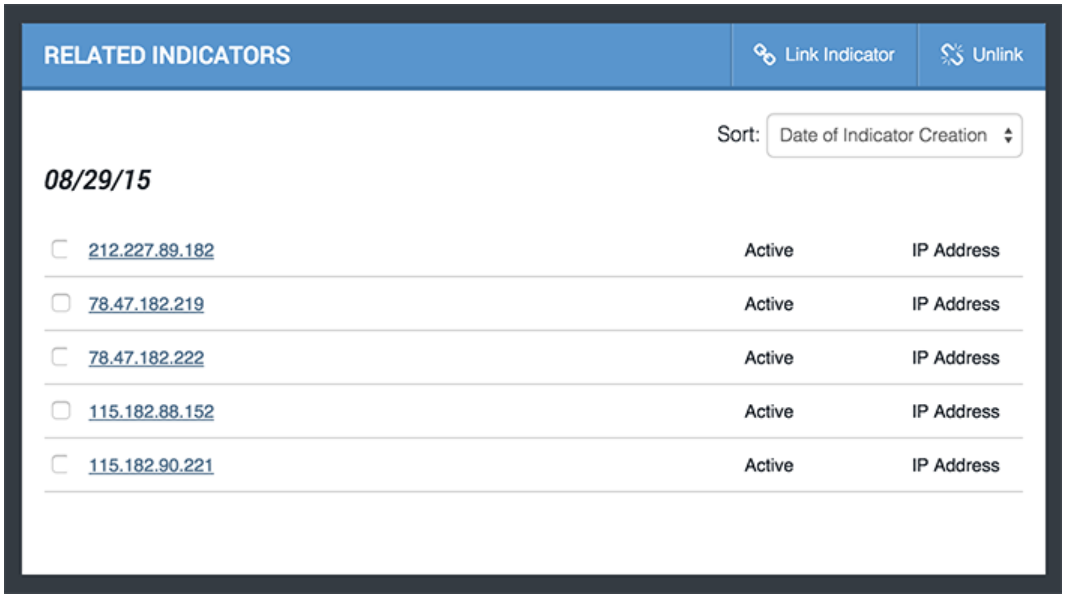
- Linking a File to an Indicator
- Unlinking a File from an Indicator
- ***Accessing the File Details page of a related file***

  Click the File name.

- ***Downloading a related file***

  Click the download icon.

Related Indicators pane



This pane provides information about indicators related to the indicator, including the name of the related indicator, its date created, its type, and its status. The following functions are available.

- Linking a File to an Indicator
- Unlinking a File from an Indicator
- ***Sorting the list by date of creation or type***

  Use the dropdown menu

- ***Accessing the Indicator details page for one of the related indicators***

  Click the indicator name.

  For more information, Accessing the Indicator Details Page for a Particular Indicator and Indicator Details Page: Information & Functions.

Indicator Details History Page: Information & Functions

The Indicator Details History page consists of one section:

- History pane

History pane

This pane provides a history of the indicator. The following function is available:

- ***Show or hide details***

  Click the appropriate link

Indicator Details Data Enrichment Page: Information & Functions

The sidebar lists the different tools available within ThreatQ. Click a tool on the left to send the indicator to that tool in order to see if it has any information about the indicator. Results will be displayed in a table on the right. The following functions are available:

- ***Sending the indicator out to one of the listed tools***

  Click the tool on the left. Any results will populate a table on the right.

  Any returned indicators can be added to ThreatQ and automatically linked to the indicator submitted.

Indicator Details Page: Procedures

Within this section is a comprehensive set of procedures found on the Indicator Details page. The following options are available:

- Editing the Value of an Indicator
- Changing the Type Associated with an Indicator
- Changing the Status of an Indicator

- Whitelisting a CIDR Block Indicator
- Deleting an Indicator
- Adding an Attribute to an Indicator
- Deleting an Attribute from an Indicator
- Searching by Attribute
- Linking an Adversary to an Indicator
- Unlinking an Adversary from an Indicator
- Editing the Confidence Level of an Adversary Related to an Indicator
- Adding a Comment to an Adversary Related to an Indicator
- Viewing a Comment for an Adversary Related to an Indicator
- Editing a Comment for an Adversary Related to an Indicator
- Deleting a Comment for an Adversary Related to an Indicator
- Linking an Event to an Indicator
- Unlinking an Event from an Indicator
- Linking a File to an Indicator
- Unlinking a File from an Indicator
- Linking an Indicator to another Indicator
- Unlinking an Indicator from another Indicator

Editing the Value of an Indicator

To edit the value of an indicator

1. Locate and click the indicator.
   The Indicator Details page opens.
2. Click the edit icon (edit).

3. An Edit Indicator window will pop up. Change the indicator value and/or indicator type and click the “Save Indicator” button.
   An indicator updated confirmation alert appears in an alert bar at the top of the page.

Changing the Type Associated with an Indicator

There are a number of types of indicators, such as CIDR Block, Email Address, Filename, FQDN.

To change the type associated with an indicator:

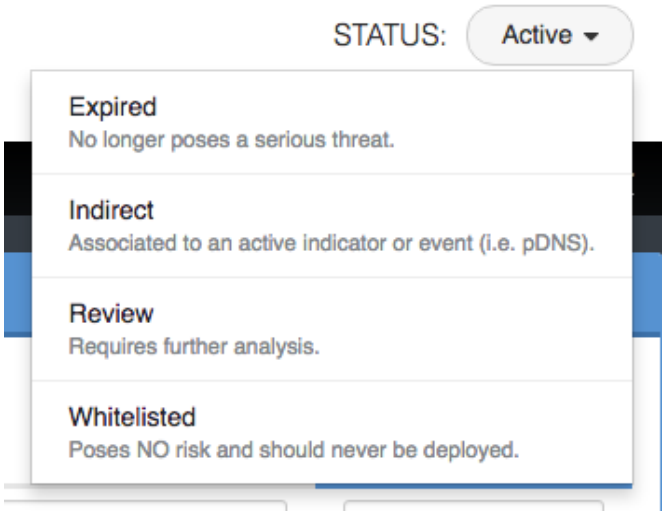
1. Locate and click the indicator.
   The Indicator Details page opens.
2. Click the indicator type dropdown menu, and select the desired type.
   An Indicator updated confirmation alert appears in an alert bar at the top of the page.

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:

- 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.



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.

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. For more information, Changing the Status of an Indicator.

To change the status of an indicator:

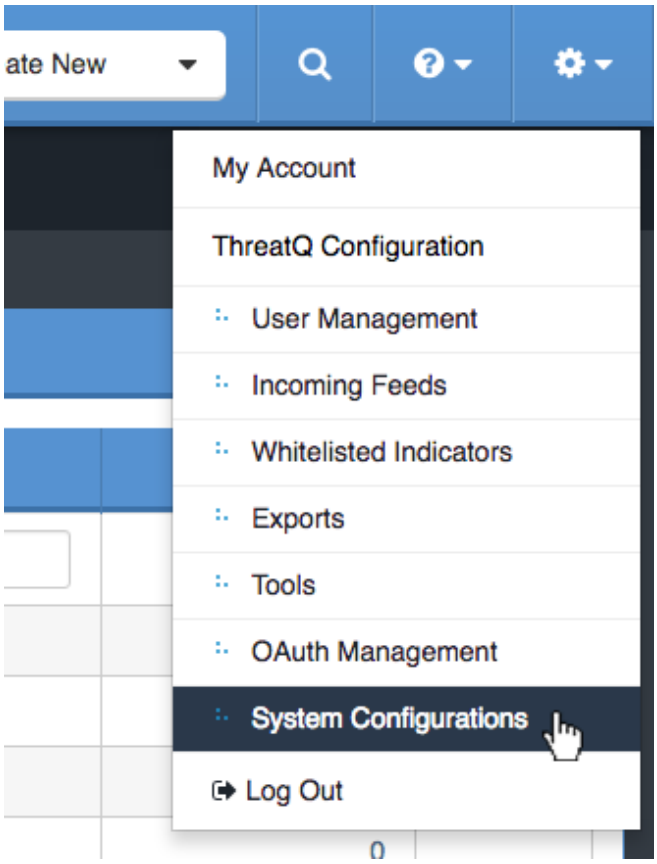
1. Locate and click the indicator.
   The Indicator Details page opens.
2. Click the status dropdown menu, and select the desired status.
   The status will be updated, and a confirmation alert appears in an alert bar at the top of the page.

   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 Whitelisting a CIDR Block Indicator below.

Adding Custom Statuses

There are use cases where an organization would like to use their own statuses within ThreatQ and we've set it up so that it's easily achievable.

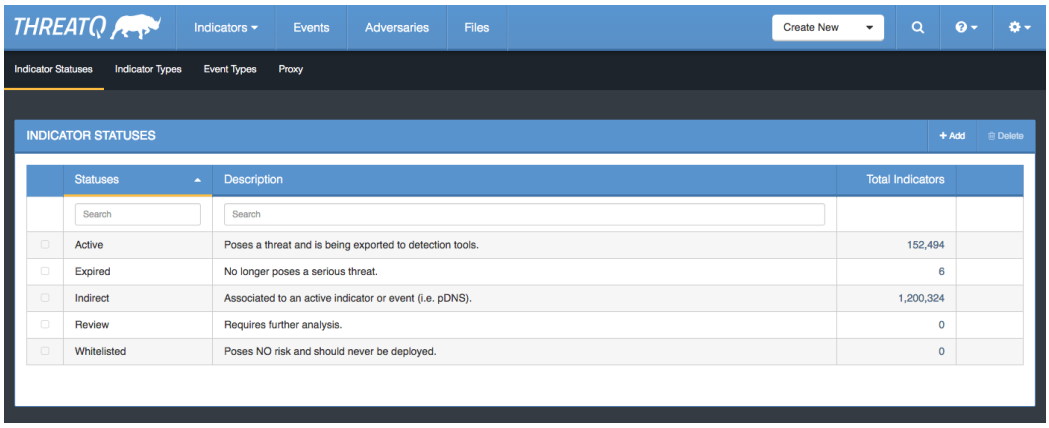
First, as a ThreatQ admin, you'll need to go to the **User dropdown (gear icon)** in the top right hand corner of the site and click on the **System Configurations** section.



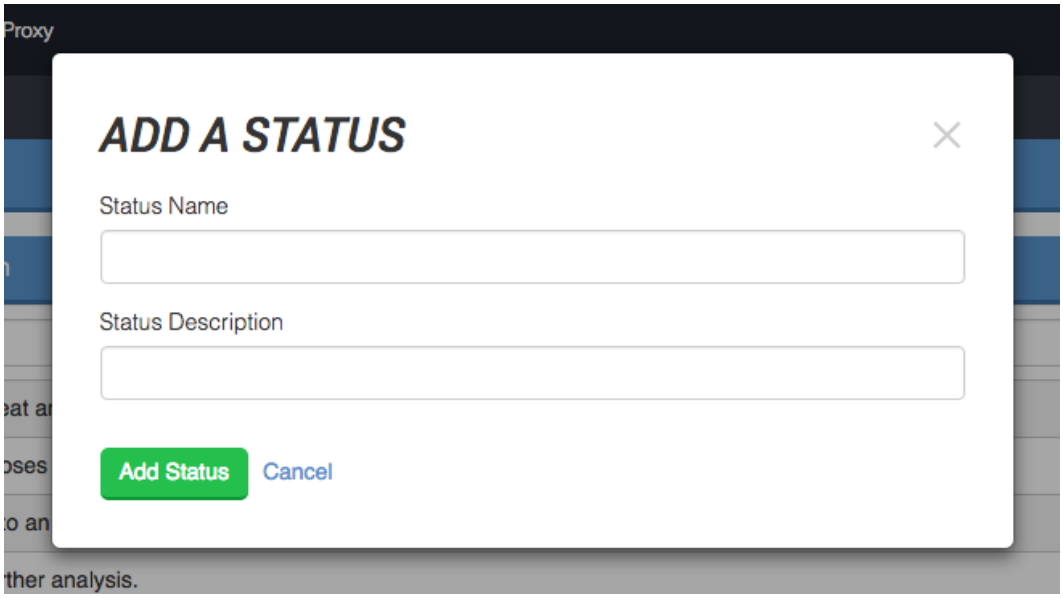
Next you'll arrive on the **Indicator Statuses** page.

Here you'll see a list of Indicator Statuses with the following information:

- Status Name
- Description
- Total count of indicators associated with that status



To add a new status **click the "+ Add" button** on the right side of the Indicator Statuses panel header.



You'll be asked to add the Status Name and Status Description. Only the Status Name is required.

Whitelisting a CIDR Block Indicator

Whitelisting a CIDR Block indicator creates a whitelisting rule. This rule will be applied to other indicators in the system, and any indicators added to ThreatQ henceforth.

The process below explains how to whitelist a CIDR Block indicator from the Indicator Details page for the indicator. A CIDR Block indicator can also be whitelisted via the tools menu. For more information on this process, see Creating a Whitelist Rule.

To whitelist a CIDR Block indicator:

1. Locate the CIDR Block indicator you wish to create a whitelist rule for.
2. Access the Indicator Details page for the indicator.
3. Click the status dropdown, and select **Whitelisted**.
   A confirmation dialog box opens asking if you are sure.
4. Click **Whitelist Indicator**.
   The Add Whitelist Rule dialog box opens with type and value according to the CIDR BLOCK indicator you chose to whitelist.
5. If you are satisfied with the type and value, 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. 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.

Deleting an Indicator

To delete an indicator:

1. Locate and click the indicator.

   The Indicator Details page opens.

2. Click the **Delete This Indicator** button.

   A warning dialog appears.

   Once an indicator has been deleted, this cannot be undone.

3. To proceed, click **Delete Indicator**.

   The Indicators Overview page refreshes, and a confirmation alert appears in an alert bar at the top of the page.

Adding an Attribute to an Indicator

To add an attribute to an indicator

1. Locate and click the indicator.

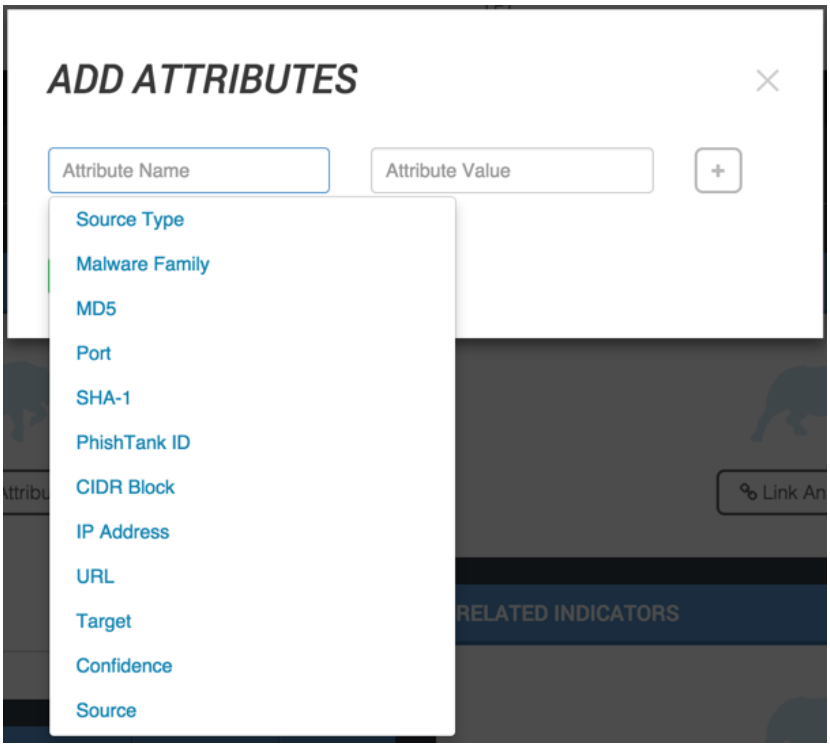
   The Indicator Details page opens.

2. In the Details pane, click **+ Add Attribute**.

   The Add Attributes dialog box opens.

3. In the Add Attributes dialog box, specify the Attribute Name and Attribute Value.

   When you click within the Attribute Name field, a dropdown menu opens.



4. Click **+**.
5. Once you have added all desired attributes, click **Add Attributes**.
   The attribute(s) are added, and a confirmation alert appears in an alert bar at the top of the page.

Deleting an Attribute from an Indicator

To delete an attribute from an indicator:

1. Locate and click the indicator.

   The Indicator Details page opens.

2. In the Details pane, select the attribute(s) you wish to delete.

   Click **Delete**.

   A confirmation dialog box will open asking if you are sure.

3. Click **Delete Attribute**.

   The attribute(s) are deleted, and a confirmation alert appears in an alert bar at the top of the page.

Searching by Attribute

To search by attribute

1. Locate and click the indicator.

   The Indicator Details page opens.

2. In the Details pane, click the Attribute you wish to search for.

   The Indicator Search window opens.

3. Review search formatting and add any other search criteria.

4. Click **Search**.
   A results table appears below the search pane.

Linking an Adversary to an Indicator

To link an adversary to an indicator

1. Locate and click the indicator.

   The Indicator Details page opens.

2. In the Related Adversaries pane, click **Link Adversary.**

   The Link an Adversary dialog box opens.

3. Type the name of the adversary into the search tool.

   Search results appear immediately below.

4. Select one or more adversary names from the results.

5. (Optional) Add a comment.

6. Click **Link Adversary**.
   The adversary is linked, and a confirmation alert appears in an alert bar at the top of the page.

Unlinking an Adversary from an Indicator

To unlink an adversary from an indicator

1. Locate and click the indicator.

   The Indicator Details page opens.

2. In the Related Adversaries pane, select one or more adversaries you wish to unlink.

3. Click **Unlink**.
   A confirmation dialog box will open asking if you are sure.

4. Click **Unlink Adversary**.

   The adversary is unlinked, and a confirmation alert appears in an alert bar at the top of the page.

Editing the Confidence Level of an Adversary Related to an Indicator

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

To edit the confidence level of an adversary related to an indicator

1. Locate and click the indicator to which the adversary is related.

   The Indicator Details page opens.

2. In the Related Adversaries pane, click the dropdown arrow to the right of the adversary, and slide the scale to the desired confidence level.

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

Adding a Comment to an Adversary Related to an Indicator

When you add a comment to a related adversary, the comment is attached to the indicator, as it pertains to the indicator-adversary relationship, and not the adversary itself.

To add a comment to an adversary related to an indicator.

1. Locate and click the indicator the adversary is related to.

   The Indicator Details page opens.

2. In the Related Adversaries pane, click within the **Comments** field, and type your comment.

3. Click **Add Comment**.
   The comment is added, and a confirmation alert appears in an alert bar at the top of the page.

Viewing a Comment for an Adversary Related to an Indicator

To view a comment for an adversary related to an indicator:

1. Locate and click the indicator the adversary is related to.

   The Indicator Details page opens.

2. In the Related Adversaries pane, locate the comment you wish to view.

3. Click the arrow to the right of the comment row.
   The comment field appears.

Editing a Comment for an Adversary Related to an Indicator

To edit a comment for an adversary related to an indicator

1. Locate and click the indicator the adversary is related to.

   The Indicator Details page opens.

2. In the Related Adversaries pane, locate the comment you wish to edit.

   You can only edit comments you made.

3. Click the arrow at the right of the comment row to expand it.

4. Click **Edit**.
   The comment field appears.

5. Make the desired edits.

6. Click **Update Comment**.
   The comment is updated, and a confirmation alert appears in an alert bar at the top of the page.

Deleting a Comment for an Adversary Related to an Indicator

To delete a comment for an adversary related to an indicator:

1. Locate and click the indicator the adversary is related to.

   The Indicator Details page opens.

2. In the Related Adversaries pane, locate the comment you wish to delete.

   You can only delete comments you made.

3. Click the arrow at the right of the comment row to expand it.

4. Click **Delete**.
   A warning dialog box opens asking if you are sure.

5. Click Delete Comment.

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

Linking an Event to an Indicator

To link an event to an indicator:

1. Locate and click the indicator.

   The Indicator Details page opens.

2. In the Related Events pane, click **Link Event**.

   The Link an Event dialog box opens.

3. Type the name of the event you wish to link.

   The system will provide typeahead suggestions, if any, based on what you have typed.

4. Select the event from the list.

5. Click **Link Event**.

The event is linked, and a confirmation alert appears in an alert bar at the top of the page.

Unlinking an Event from an Indicator

To unlink an event from an indicator:

1. Locate and click the indicator.

   The Indicator Details page opens.

2. In the Related Events pane, select the event(s) you wish to unlink.

3. Click **Unlink**.
   A warning dialog box opens asking if you are sure.

4. Click **Unlink Event**.

   The event(s) are unlinked, and a confirmation alert appears in an alert bar at the top of the page.

Linking a File to an Indicator

To link a file to an indicator:

1. Locate and click the indicator.

   The Indicator Details page opens.

2. In the Related Files pane, click **Link File**.

   The Link Files dialog box opens.

3. Type the filename in the search field.

   The system will provide typeahead suggestions, if any, based on what you have typed.

4. Select the desired file from the options.
5. Click **Link File**.
   The file will now be linked to the indicator in two places: on the Indicator Details page under Related Files; and on the File Details page for the file, under Related Indicators.

Unlinking a File from an Indicator

To unlink a file from an indicator:

1. Locate and click the indicator.

   The Indicator Details page opens.

2. In the Related Files pane, select the file(s) you wish to unlink.
3. Click **Unlink**.
   A warning dialog box opens asking if you are sure.
4. Click **Unlink File**.

   The file(s) will be unlinked, and a confirmation alert appears in an alert bar at the top of the page.

Linking an Indicator to another Indicator

To link an indicator to another indicator:

1. Locate and click the indicator you wish to link another indicator to.

   The Indicator Details page opens.

2. In the Related Indicators pane, click **Link Indicator**.

   The Link an Indicator dialog box opens.

3. Type the name of the indicator you wish to link.

   The system will provide typeahead suggestions, if any, based on what you have typed.

4. Select the indicator(s) you wish to link.

5. Click **Link Indicator**.
   The selected indicator(s) are linked, and a confirmation alert appears in an alert bar at the top of the page.

Unlinking an Indicator from another Indicator

To unlink an indicator from another indicator:

1. Locate and click the indicator you wish to unlink another indicator from.

   The Indicator Details page opens.

2. In the Related Indicators pane, select one or more indicators you wish to unlink.

3. Click **Unlink**.
   A warning dialog box opens asking if you are sure.

4. Click **Unlink Indicator**.

5. The indicator is unlinked, and a confirmation alert appears in an alert bar at the top of the page.

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. Go to **ThreatQ Configuration** > **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.

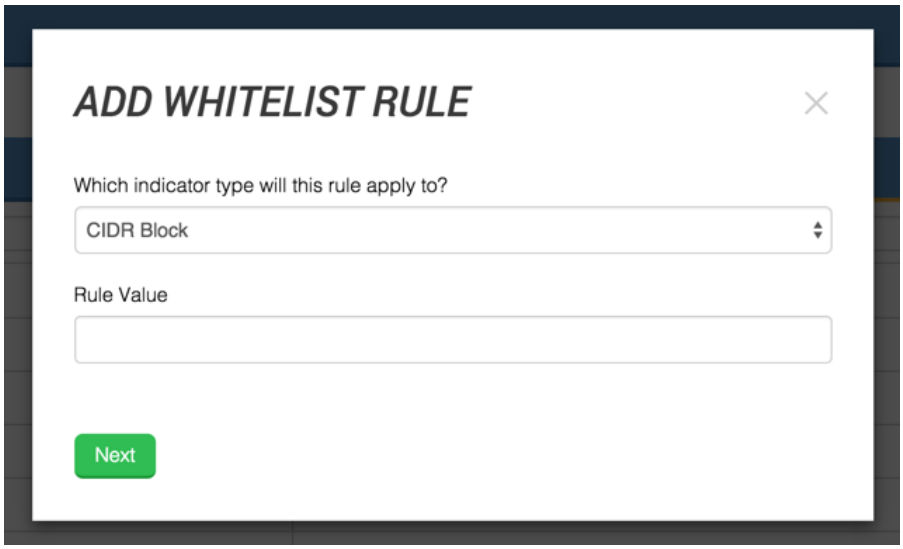
To create a whitelist rule:

1. Go to **ThreatQ Configuration** > **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. To continue editing, click **Continue Editing this Rule**.
7. 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

When you edit a whitelist rule, the changes you make will affect indicators currently in the system, and any new indicators added to the system.

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

To edit a whitelist rule:

1. Go to **ThreatQ Configuration** > **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. Go to **ThreatQ Configuration** > **Whitelisted Indicators**.

   The Whitelist Rules page opens.

2. In the Whitelist Rules table, locate and select the rule(s) you wish to remove.

3. Click **Remove**.
   A confirmation dialog box opens, asking if you are sure.
4. If you are sure, click **Delete Whitelist Rule**.

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

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.

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".

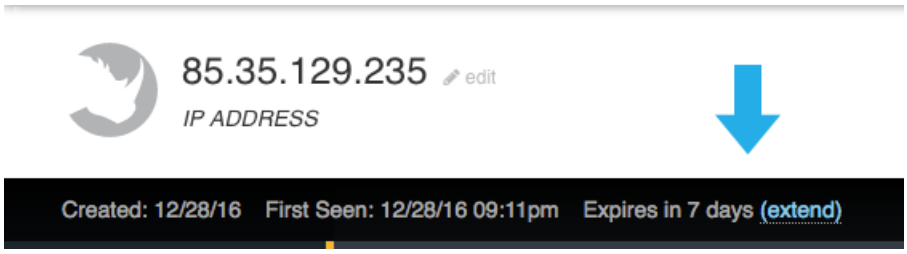
- **An expiration policy has been applied to the source reporting an indicator and therefore an expiration date is automatically set for that indicator during ingestion**

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.

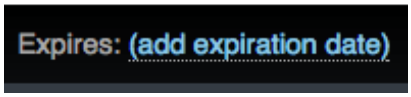
Changing an individual indicator's expiration date

An indicator's expiration information can be found on the black bar directly below the indicator's value on the indicator details page.



Expiration Date Displays

- **No expiration date has been set**

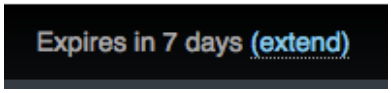


In the example above, this particular indicator will not automatically expire because an expiration date has not been specified.

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.

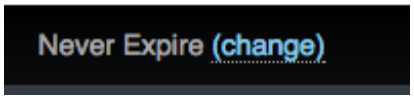
- **An expiration date is set**

In the example above, this particular 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).



When an expiration date is less than 7 days away, ThreatQ will switch to show a relative version of the date.

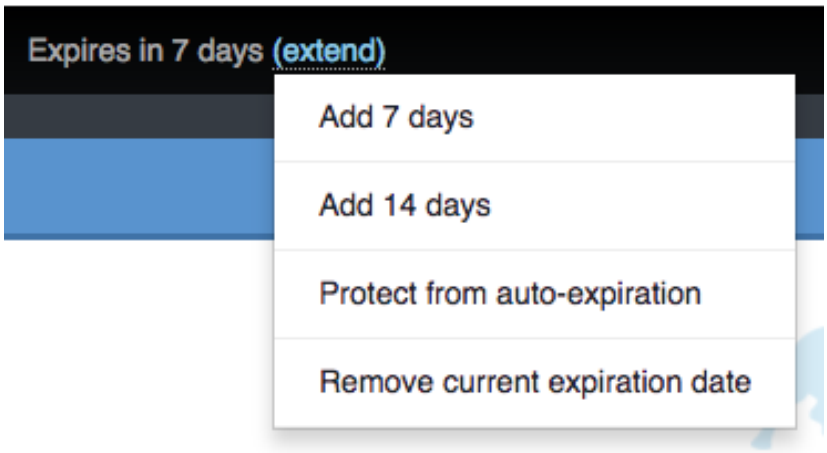
- **Protected from automatic expiration (Never Expire)**



Sometimes 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.

Changing an indicator's expiration date

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



Options include:

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

Automatic Expiration and Expiration Policies

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

Where can I configure Automatic Expiration?

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.

Selecting an Expiration Policy per Feed

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

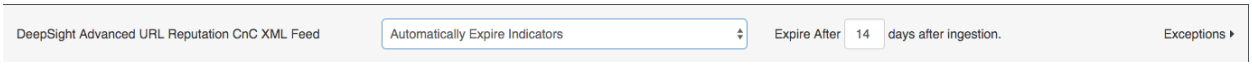
Don't automatically expire (No policy set)

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 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

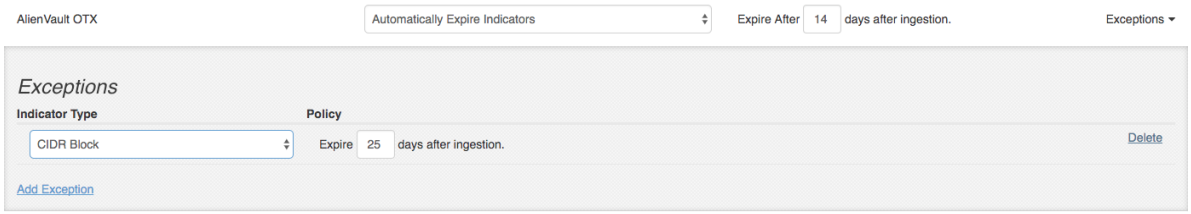
Using this setting ensures that all intelligence reported by a specific feed is protected from automatic expiration, regardless of scenario.

Adding Exceptions

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

To add an exception, while viewing the **Automatic Expiration** tab, choose a source and click **Exceptions** to expand the option.

From here, you can add or remove exceptions to the policy listed above for that specific feed.



How ThreatQ Calculates Expiration Dates

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 Source with an Exception for that Indicator

If an indicator is reported by a source that has an exception for the indicator, the exception expiration date will be used regardless of 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 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.

Common Expiration Policy scenarios

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) and 3 days later is reported by Source B (with an expiration policy of 10 days).

1. On 10/1, Source A reports the indicator and the expiration date is set to 10/8.
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**.

An indicator is currently set to Expired and is reported by Source A (with an expiration policy of Never Expire).

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**.

Applying Expiration Policy Changes to Existing 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

Indicators to reset expiration out of 6m total indicators	Reset and Recalculate Expiration	Expire Indicators	Total Time for Reset
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

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.

Where can I 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**.

- To influence scores based on attributes, you click **Add** and designate an Attribute Key / Value Pair, before adjusting the sensitivity.
- To influence scores based on adversary relationship, you click **Add** and select an adversary, before adjusting the sensitivity.

Overriding the scoring algorithm with a manual score

To set a manual Indicator Score, complete the following steps:

1. Navigate to an Indicator's Details page.
2. Choose the Indicator Score.
3. Optionally, you may revert to the calculated score by choosing **Generated Score**.

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

Events

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

Within this section, the following options are available:

- Accessing the Events Overview page
- Events Page: Information & Functions

Adding an Event

To add an event:

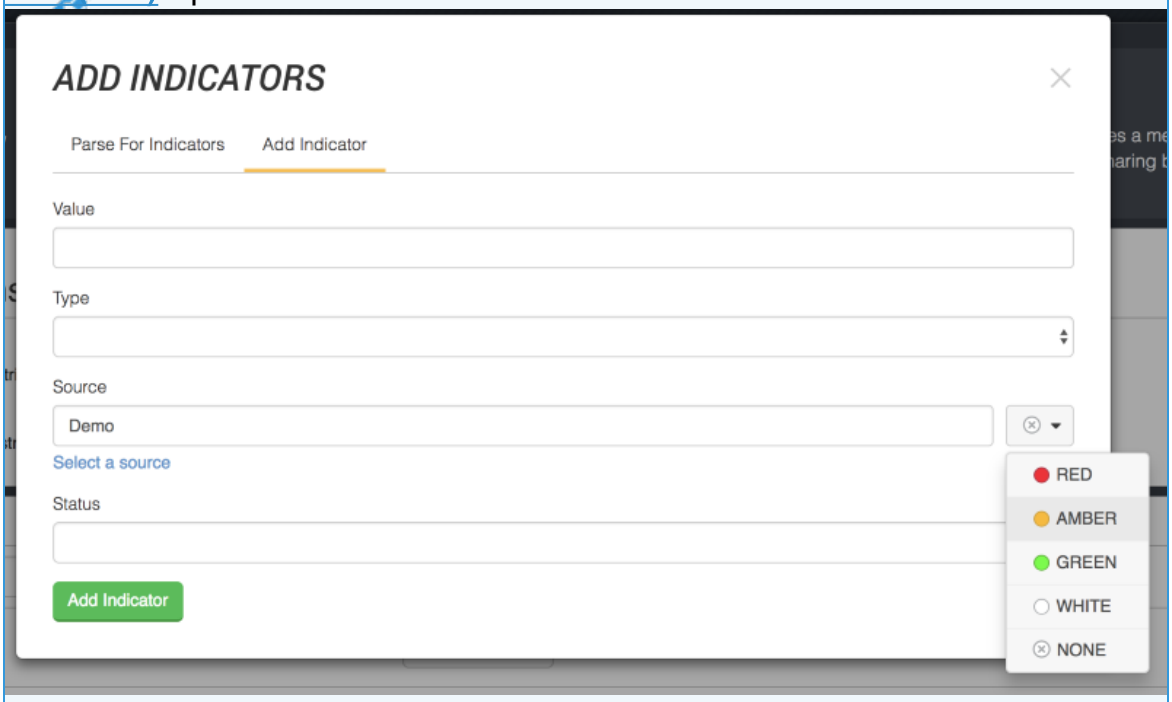
1. Go to **Create** > **Event**.

   The Add Event dialog box opens.

2. Select the **Event Type**.
3. Select a **Source** from the dropdown 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 Pro-

tocol (TLP) topic for more information on TLP classifications.



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

   The Event Details page opens for the event, and a confirmation alert appears in an alert bar at the top of the page.

Accessing the Events Overview page

- In the navigation menu, choose **Analytics > Events**.
  The Events Overview page opens.

Events Page: Information & Functions

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

- Events History scatter plot
- Event Details Summary Page
- Monthly Heatmap table
- Top Recipients of Spearphish table

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:

- ***Viewing an event's name, date and time, and source***

  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***

  Click the event in the scatter plot.

  For more information, see Event Details Page.

- ***Hiding or unhiding one or more of the event types***

  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 timeframe of the information displayed***

  Click the dropdown menu at the top right and select the desired timeframe.

- ***Printing or downloading the scatter plot as a PNG, JPEG, PDF, or SVG file***

  Click the hamburger menu (see graphic below), and select the desired option.

Summary table

Immediately below the scatter plot is a summary table of that provides a breakdown of events by date, type, title, and sources. The following functions are available:

- ***Opening the Event Details page for one of the events***

  Click the event title.

  For more information, see Event Details Page.

- ***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. Click the header a second time to reverse sort order.

- ***Searching within a column***

  Click within the search box at the top of the column, and enter your search criteria.

Monthly Heatmap table

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:

- ***Viewing an event's name and monthly count***

  Hover your mouse over an event on the heatmap to see its name and monthly count.

- *Adjusting the timeframe of the information displayed*

  Click the dropdown menu at the top right and select the desired timeframe.

- *Printing the graph or saving it as a PNG, JPEG, PDF, or SVG*

  Click the hamburger menu (see graphic below), and select the desired option.

Top Recipients of Spearphish table

As Spearphish attempts come into the system, they have recipients and possibly adversaries. Certain recipients may have more spearphish attempts. The following functions are available:

- *Opening the Adversary Details page for one of the adversaries*

  Click the adversary name.

  For more information, see Adversary Details Page.

- *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. Click the header a second time to reverse sort order.

- *Searching within a column*

  Click within the search box at the top of the column, and enter your search criteria.

Event Details Page

Within this section, the following options are available:

- Accessing the Event Details page for a Particular Event
- Event Details Page: Information & Functions

Accessing the Event Details page for a Particular Event

- Locate and click the event.

  The Event Details page opens.

Event Details Page: Information & Functions

The Event Details page is made up of the following:

- Event Details Header
- Two sub-tabs
  - Event Details Summary Page
  - Event Details History Page

Event Details Header

At the top of the Event Details Summary page is a header with the event name, date and time of the event, date and time created, and event type. The following functions are available:

- Editing the Event Value
- Changing the Type Assigned to an Event
- Deleting an Event

Event Details Summary Page

The Event Details Summary page provides a wide range of information and functions related to an event and consists of five sections:

- Event Details pane
- Events Related Adversaries pane
- Events Related Files pane
- Events Related Indicators pane
- Events Spearphish Details pane

- The Spearphish Details pane only appears for Spearphish events.

Event Details pane

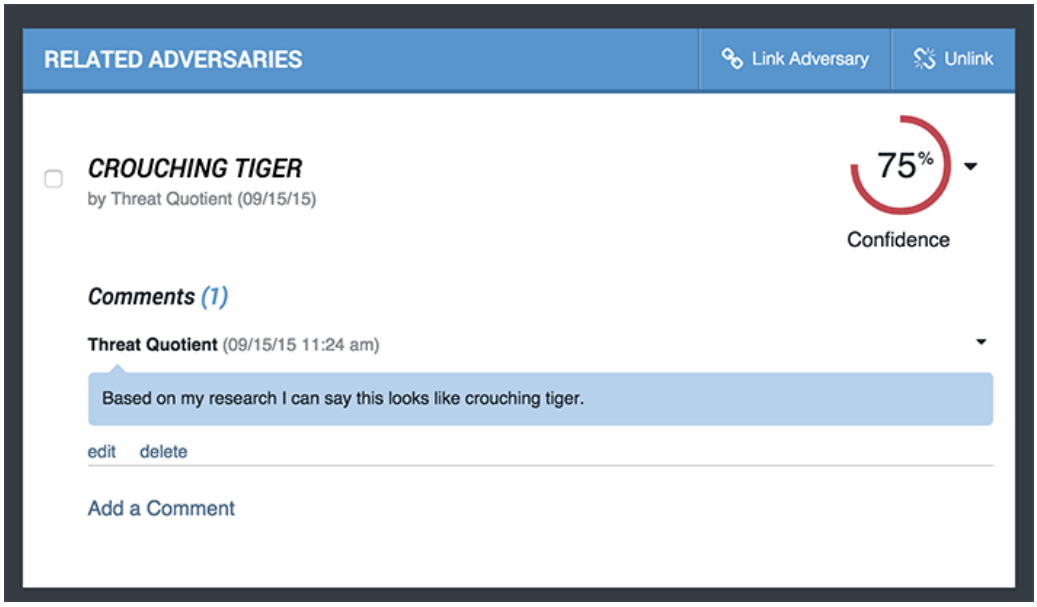
This pane provides information about the attributes and sources of the event, including the name and date. The following functions can be performed:

- Adding an Attribute to an Event
- Deleting an Attribute from an Event
- **Performing a search for a listed attribute**

  Click the attribute to set it as a search criterion and open the Advanced Search page.

  For more information on using the advanced search tool, see Performing an Indicator Search.

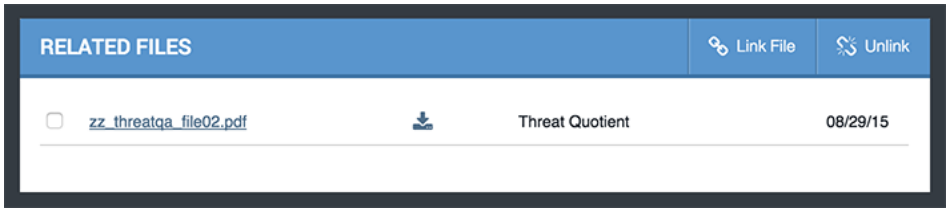
Events Related Adversaries pane



This pane provides information about adversaries related to the event, including the name and date created, and the confidence level. The following functions are available:

- Linking an Adversary to an Event
- Unlinking an Adversary from an Event
- Editing the Confidence Level Associated with a Related Adversary
- Adding a Comment to a Related Adversary
- Viewing a Comment for a Related Adversary
- Editing a Comment for a Related Adversary
- Deleting a Comment from a Related Adversary

Events Related Files pane



This pane provides information about files related to the indicator, including the name and the date the file was created. The following functions are available:

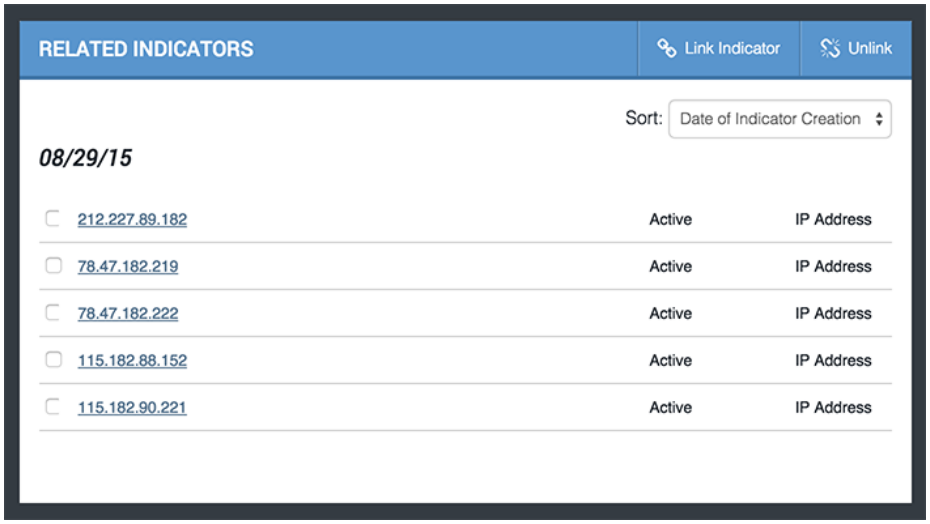
- Linking a File to an Event
- *Unlinking a File from an Event*
- ***Accessing the File Details page of a related file***

  Click the File name.

- ***Downloading a related file***

  Click the download icon

Events Related Indicators pane



This pane provides information about indicators related to the indicator, including the name of the related indicator, its date created, its type, and its status. The following functions are available.

- Linking an Indicator to an Event
- Unlinking an Indicator from an event

- *Sorting the list by date of creation or type*

  Use the dropdown menu.

- *Accessing the indicator details page for one onf the related indicators*

  Click the indicator name.

Events Spearphish Details pane

This pane shows the raw Spearphish email content.

Event Details History Page

The Event Details History page provides a history of the event. The following function is available:

- *Show or hide details*

  Click the appropriate link.

Event Details Page: Procedures

Within this section is a comprehensive set of procedures found on the Event Details page. The following options are available:

- Editing the Event Value
- Changing the Type Assigned to an Event
- Deleting an Event
- Adding an Attribute to an Event
- Deleting an Attribute from an Event
- Searching by Attribute
- Linking an Adversary to an Event
- Unlinking an Adversary from an Event

- Editing the Confidence Level Associated with a Related Adversary
- Adding a Comment to a Related Adversary
- Editing a Comment for a Related Adversary
- Deleting a Comment from a Related Adversary
- Linking a File to an Event
- Unlinking a File from an Event
- Linking an Indicator to an Event
- Unlinking an Indicator from an event

Editing the Event Value

To edit the name of an event

1. Locate and click the event.

   The Event Details page opens.

2. Click within the name field, and make the desired edits.

3. Click outside of the name field.
   An Event updated confirmation alert appears in an alert bar at the top of the page.

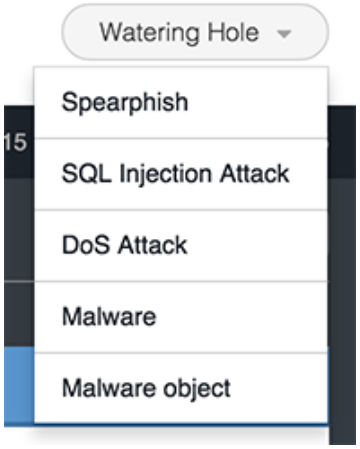
Changing the Type Assigned to an Event

To change the type assigned to an event

1. Locate and click the event.

   The Event Details page opens.

2. Click the event type dropdown menu, and select the desired type.



An Event updated confirmation alert appears in an alert bar at the top of the page.

Deleting an Event

To delete an event

1. Locate and click the event.

   The Event Details page opens.

2. Click the **Delete This Event** button.

   A warning dialog box appears.

3. To proceed, click **Delete Event**.

   The Event Details page refreshes, and a confirmation alert appears in an alert bar at the top of the page.

Adding an Attribute to an Event

To add an attribute

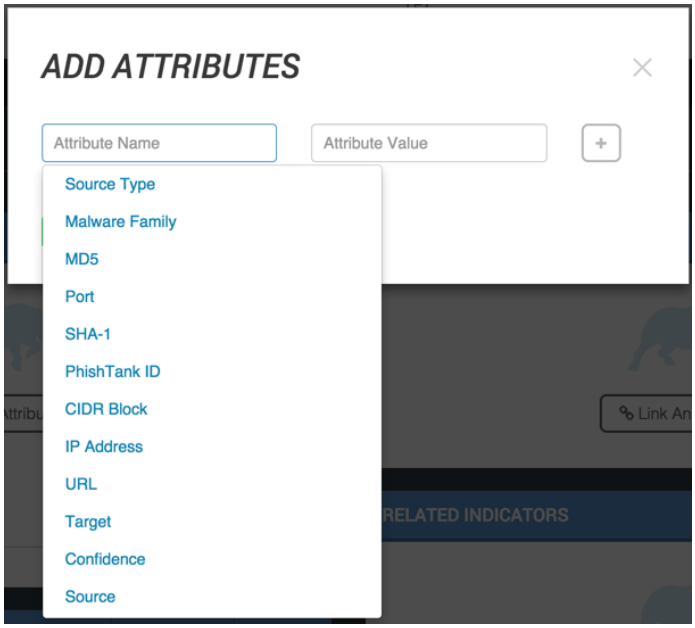
1. Locate and click the event.

   The Event Details page opens.

2. In the Details pane, click **+ Add Attribute**.

   The Add Attributes dialog box opens.

3. In the Add Attributes dialog box, specify the Attribute Name and Attribute Value.



4. Click **+**.
5. Once you have added all desired attributes, click **Add Attributes**.

   A confirmation alert appears in an alert bar at the top of the page.

Deleting an Attribute from an Event

To delete an attribute

1. Locate and click the event.

   The Event Details page opens.

2. In the Details pane, select the attribute(s) you wish to delete.
3. Click **Delete**.
   A confirmation dialog box opens asking if you are sure.
4. Click **Delete Attribute**.

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

Searching by Attribute

To search by attribute:

1. Locate and click the event.

   The Event Details page opens.
2. In the Details pane, click the Attribute you wish to search for.

   The Indicator Search window opens.
3. Review search formatting, and add any other search criteria.
4. Click **Search**.
   A results table appears below the search pane.

Linking an Adversary to an Event

To link an adversary to an event:

1. Locate and click the event.

   The Event Details page opens.
2. In the Related Adversaries pane, click **Link Adversary**.

   The Link an Adversary dialog box opens.

3. Type the name of the adversary into the search field.

   The system will provide typeahead suggestions, if any, based on what you have typed.

4. Select one or more adversaries.
5. (Optional) Add a comment.
6. Click **Link Adversary**.

   The adversary will be linked, and a confirmation alert appears in an alert bar at the top of the page.

Unlinking an Adversary from an Event

To unlink an adversary from an event:

1. Locate and click the event.

   The Event Details page opens.

2. In the Related Adversaries pane, select one or more adversaries you wish to unlink.
3. Click **Unlink**.
   A confirmation dialog box opens asking if you are sure.
4. Click **Unlink Adversary**.

   The adversary will be unlinked, and a confirmation alert appears in an alert bar at the top of the page.

Editing the Confidence Level Associated with a Related Adversary

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

To edit the confidence level:

1. Locate and click the event the adversary is related to.

   The Event Details page opens.

2. In the Related Adversaries pane, click the dropdown arrow to the right of the adversary, and slide the scale to the desired confidence level.

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

Adding a Comment to a Related Adversary

To add a comment:

1. Locate and click the event the adversary is related to.

   The Event Details page opens.

2. In the Related Adversaries pane, click within the **Comments** field, and type your comment.
3. Click **Add Comment**.
   The comment is added, and a confirmation alert appears in an alert bar at the top of the page.

Viewing a Comment for a Related Adversary

To view a comment:

1. Locate and click the event the adversary is related to.

   The Event Details page opens.

2. In the Related Adversaries pane, locate the comment you wish to view.
3. Click the arrow to the right of the comment identity.
   The comment field appears.

Editing a Comment for a Related Adversary

To edit a comment:

1. Locate and click the event the adversary is related to.

   The Event Details page opens.

2. In the Related Adversaries pane, locate the comment you wish to edit.

   You can only edit comments you made.

3. Click **Edit**.

   The comment field appears.

4. Make the desired edits.
5. Click Update Comment.
   The comment is updated.

Deleting a Comment from a Related Adversary

To delete a comment:

1. Locate and click the event the adversary is related to.

   The Event Details page opens.

2. In the Related Adversaries pane, locate the comment you wish to delete.

   You can only delete comments you made.

3. Click **Delete**.

   The warning dialog box opens asking if you are sure.

4. Click Delete Comment.

   The comment is deleted.

Linking a File to an Event

To link a file to an event:

1. Locate and click the event.

   The Event Details page opens.

2. In the Related Files pane, click **Link File**.

   The Link Files dialog box opens.

3. Type the name of the file you wish to link.

   The system will provide typeahead suggestions, if any, based on what you have typed.

4. Select the desired file(s).
5. Click **Link File**.
   The file is added to the Related Files pane, and a confirmation appears in the alert bar at the top of the page.

Unlinking a File from an Event

To unlink an indicator from an event:

1. Locate and click the event.

   The Event Details page opens.

2. In the Related Files pane, select the file(s) you wish to unlink.

3. Click **Unlink**.
   The selected file is unlinked, and a confirmation alert appears in an alert bar at the top of the page.

Linking an Indicator to an Event

To link an indicator to an event:

1. Locate and click the event you wish to link an indicator to.

   The Event Details page opens.

2. In the Related Indicators pane, click **Link Indicator**.

   The Link an Indicator dialog box opens.

3. Type the name of the indicator you wish to link.

   The system will provide typeahead suggestions, if any, based on what you have typed.

4. Select the indicator(s) you wish to link.

5. Click **Link Indicator**.

   The selected indicator(s) are linked; the related indicators pane is updated, and a confirmation alert appears in an alert bar at the top of the page.

Unlinking an Indicator from an event

To unlink an indicator from an event:

1. Locate and click the event.

   The Event Details page opens.

2. In the Related Indicators pane, select the indicator(s) you wish to unlink.

3. Click **Unlink**.
   The selected indicator is unlinked, and a confirmation alert appears in an alert bar at the top of the page.

Adversaries

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

Within this section, the following options are available:

- Accessing the Adversaries Overview Page
- Adversaries Page: Information & Functions

Adding an Adversary

To add an adversary:

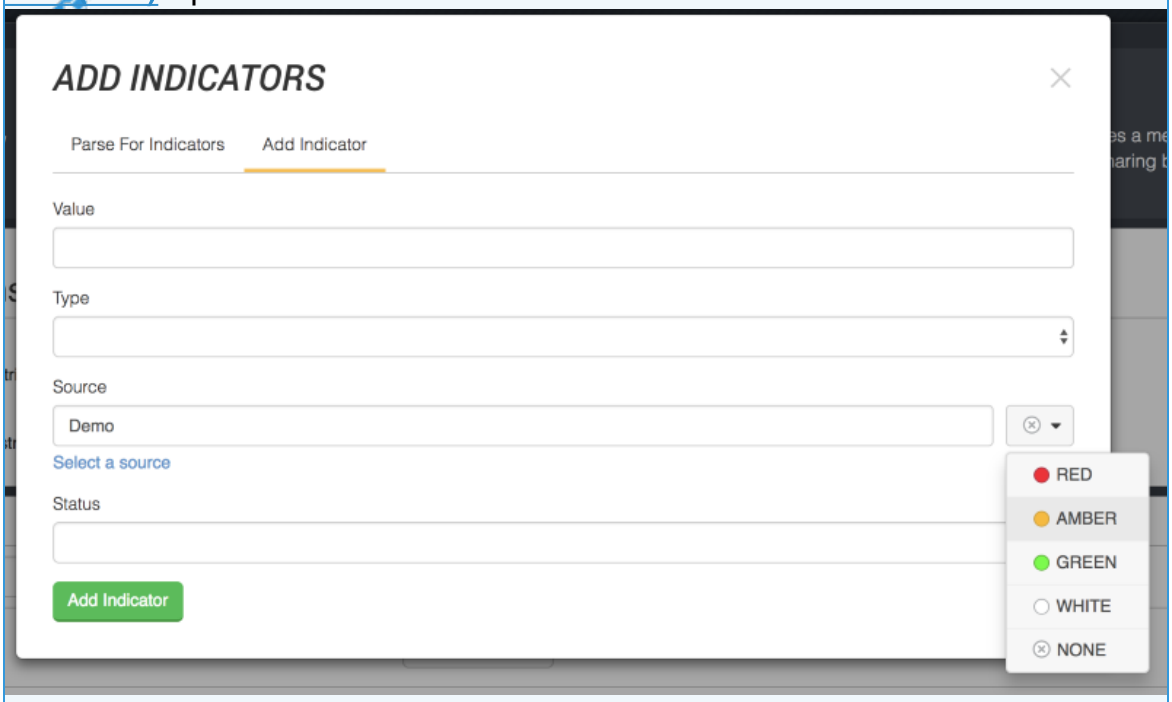
1. Go to **Create** > **Adversary**.

   The Add an Adversary dialog box opens.

2. Enter a name.
3. Select a **Source** from the dropdown 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 Pro-

tocol (TLP) topic for more information on TLP classifications.



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

   The Adversary Details page opens for the adversary, and a confirmation alert appears in an alert bar at the top of the page.

Accessing the Adversaries Overview Page

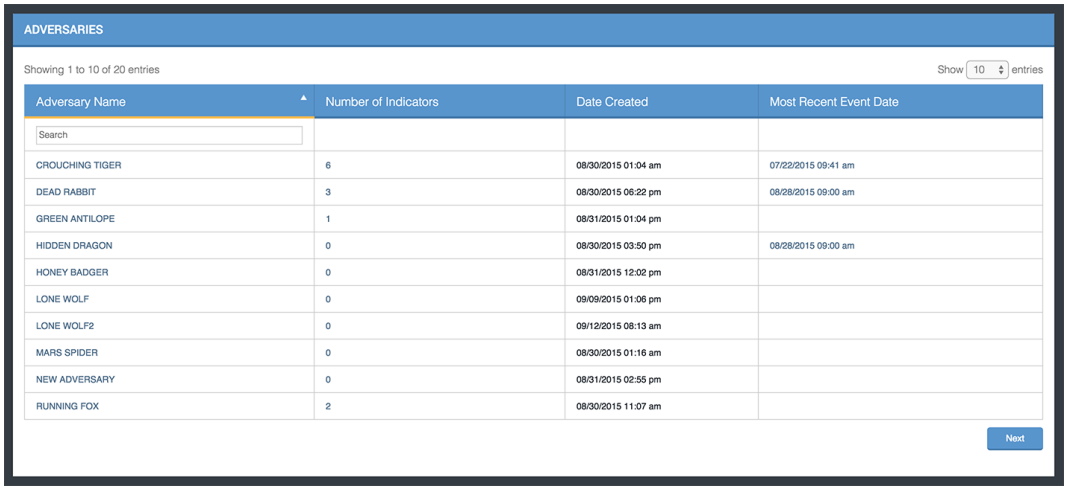
- In the navigation menu, choose **Analytics > Adversaries**.
  The Adversaries Overview page opens.

Adversaries Page: Information & Functions

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
- Adversary Overlap table
- Indicator Distribution pie chart

Adversaries summary table



This 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:

- ***Opening the Adversary Details page for an adversary***

  Click the name in the Adversary Name column.

- ***Performing a search for related indicators***

  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***

  Click the date in the Most Recent Event Date to open the Event Details page.

- ***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.

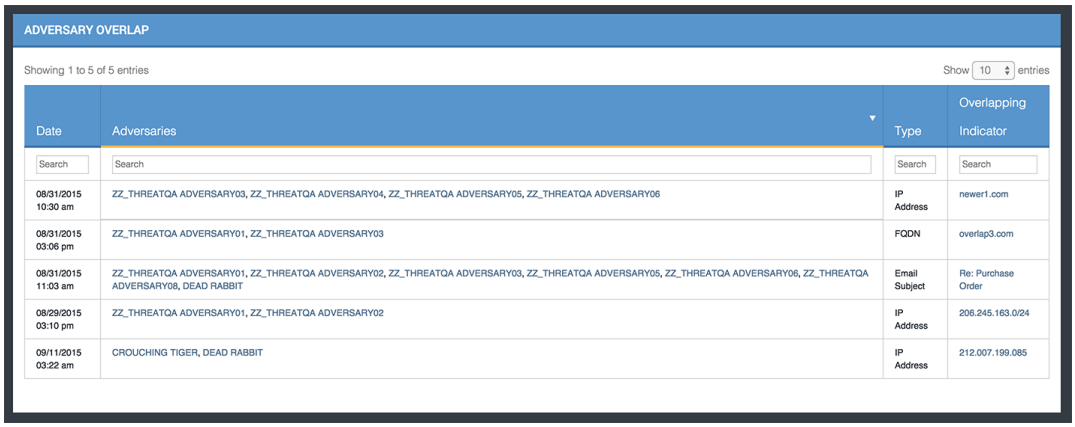
- ***Sorting the table by a column***

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

- ***Searching within the Adversary Name column***

  Click within the search box at the top of the column, and enter your search criteria.

Adversary 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:

- ***Opening the Adversary Details page for an adversary***

  Click the name in the Adversary Name column.

- ***Opening the Indicator Details page for an overlapping indicator***

  Click the identity in the Overlapping Indicator column.

- ***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.

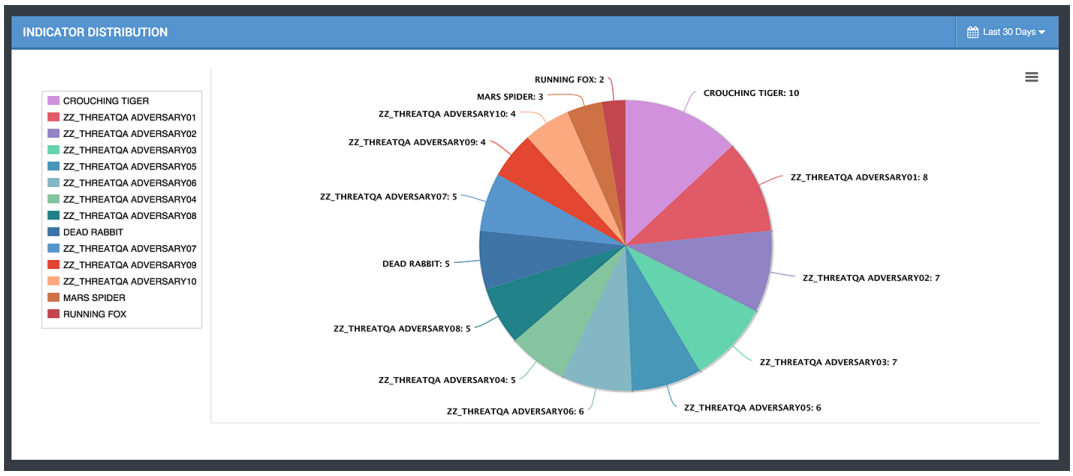
- *Sorting the table by a column*

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

- *Searching within a column*

  Click within the search box at the top of the column, and enter your search criteria.

Indicator Distribution pie chart



The Indicator Distribution pie chart shows you how many indicators were associated with all adversaries, within a specified timeframe. The following functions are available:

- *Viewing more information about a selected value*

  Hover over a colored section of the pie chart to open a popup identifying the indicator, the number of times the indicator was found within the specified timeframe, and what percentage of the total number of indicators it represents.

- *Hiding or unhiding one of the values from the pie chart*

  Click the indicator on the left of the pie chart to remove it; click a second time to reinstate it.

- ***Adjusting the timeframe of the information displayed***

  Click the dropdown menu at the top right and select the desired timeframe.

- ***Printing the graph or saving it as a PNG, JPEG, PDF, or SVG***

  Click the hamburger menu (see graphic below), and select the desired option.

Adversary Details Page

The Adversary Details page provides a wide range of information and actions related to a particular adversary.

Within this section, the following options are available:

- Accessing the Adversary Details Page for a Particular Adversary
- Adversary Details Page

Accessing the Adversary Details Page for a Particular Adversary

To access the Adversary Details page:

- Locate and click the adversary.

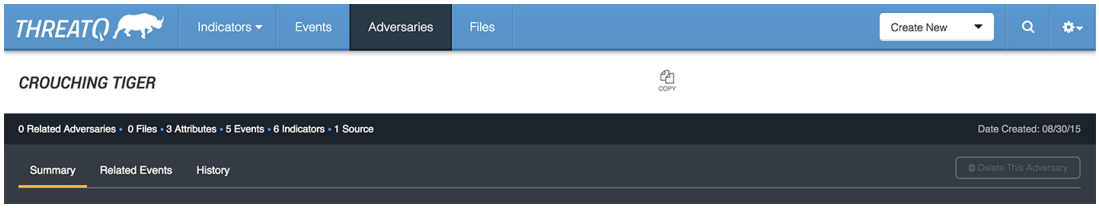
  The Adversary Details page opens.

Adversary Details Page

The Adversary Details page is made up of the following:

- Adversary Details header
- Three sub-tabs:
  - Adversary Details: Summary page
  - Adversary Details: Related Events page
  - Adversary Details: History page

Adversary Details header



At the top of the Adversary Details Summary page is a header with the adversary name, date created, and a quick view list of the number of attributes, related events, related indicators, and sources. The following functions are available:

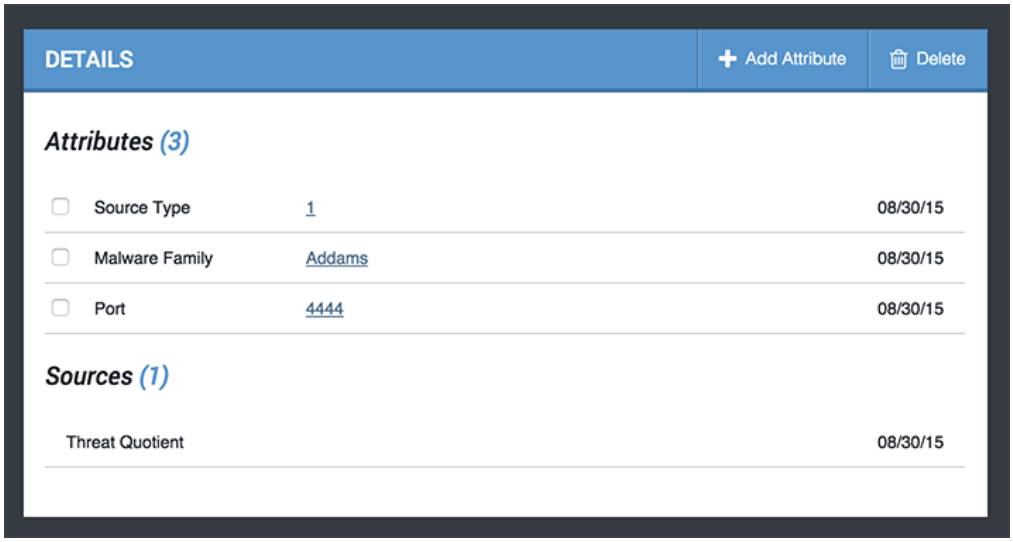
- Editing the Name of an Adversary
- Deleting an Adversary

Adversary Details: Summary page

The Adversary Details: Summary page consists of three sections:

- Details pane
- Related Indicators table
- Adversary Description pane

Details pane



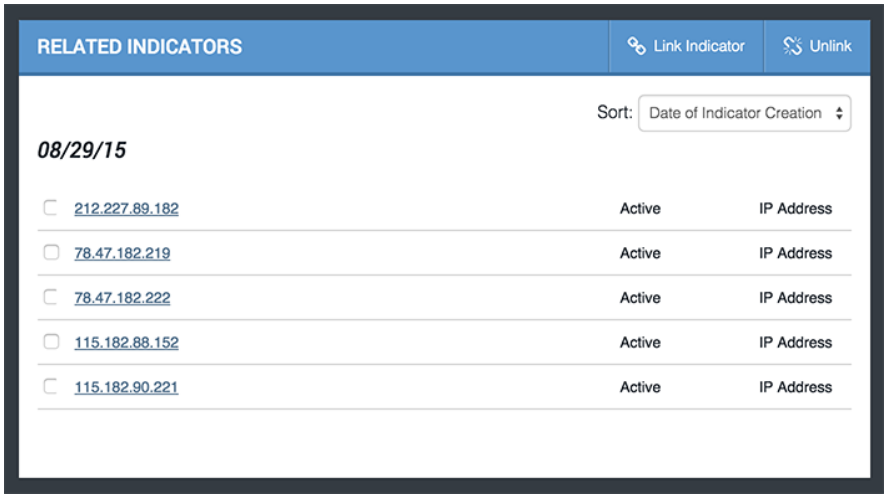
This pane provides information about the attributes and sources of the adversary, including the name and date. The following functions are available:

- Adding an Attribute to an Adversary
- Deleting an Attribute from an Adversary
- ***Performing a search for a listed attribute***

  Click the attribute to set it as a search criterion and open the Indicator Search page.

  For more information on using the indicator search tool, see Performing an Indicator Search.

Related Indicators table



This table provides a list of related indicators. The following functions are available:

- ***Sorting the list by Date of Indicator Creation or Indicator Type***

  Use the dropdown menu to select the desired option.

- ***Accessing the Indicator Details page for a related indicator***

  Click the indicator.

- Linking an Indicator to an Adversary
- Unlinking an Indicator from an Adversary

Adversary Description pane

This pane permits you to fill out information about an adversary. It is a text editor that you can use to paste in information from different files. You can put all supporting information related to the adversary here, for future reference. The following functions are available:

- Adding an Adversary Description
- Editing an Adversary Description

Adversary Details: Related Events page

This page provides information about events related to the adversary. The following function is available:

- Linking an Event to an Adversary

Adversary Details: History page

This page provides a history of the adversary. The following function is available:

- ***Show or hide details***

  Click the appropriate link.

Adversary Details Page: Procedures

Within this section is a comprehensive set of procedures found on the Event Details page. The following options are available:

- Editing the Name of an Adversary
- Deleting an Adversary
- Adding an Attribute to an Adversary
- Deleting an Attribute from an Adversary
- Searching by Attribute
- Adding an Adversary Description
- Editing an Adversary Description
- Linking an Event to an Adversary
- Unlinking an Event from an Adversary

- Linking an Indicator to an Adversary
- Unlinking an Indicator from an Adversary

Editing the Name of an Adversary

To edit the name of an adversary:

1. Locate and click the adversary.

   The Adversary Details page opens.

2. Click within the name field, and make the desired edits.

3. Click outside of the name field.
   The name is updated, and a confirmation alert appears in an alert bar at the top of the page.

Deleting an Adversary

To delete an adversary:

1. Locate and click the adversary.

   The Adversary Details page opens.

2. Click the **Delete This Adversary** button.

   A confirmation dialog box appears.

3. To proceed, click **Delete Adversary**.

   The Adversary Details page will refresh, and the alert bar will confirm the change.

Adding an Attribute to an Adversary

To add an attribute to an adversary:

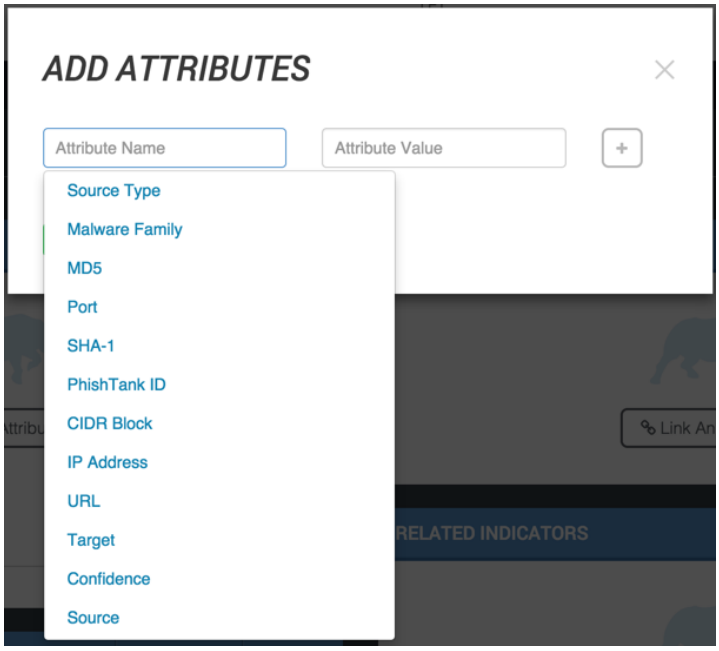
1. Locate and click the adversary.

   The Event Details page opens.

2. In the Details pane, click **+ Add Attribute**.

   The Add Attributes dialog box opens.

3. In the Add Attributes dialog box, specify the Attribute Name and Attribute Value.



4. Click **+**.
5. Once you have added all desired attributes, click **Add Attributes**.

   A confirmation alert appears in an alert bar at the top of the page.

Deleting an Attribute from an Adversary

To delete an attribute from an adversary:

1. Locate and click the adversary.

   The Adversary Details page opens.

2. In the Details pane, select the attribute(s) you wish to delete.
3. Click **Delete**.
   A confirmation dialog box appears, asking if you wish to proceed.
4. Click **Delete Attribute**.

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

Searching by Attribute

To search by attribute:

1. Locate and click the adversary.

   The Adversary Details page opens.
2. In the Details pane, click the Attribute you wish to search for.

   The Search window opens.
3. Review search formatting and add any other search criteria.
4. Click **Search**.
   A results table appears below the search pane.

Adding an Adversary Description

To add an adversary description:

1. Locate and click the adversary.

   The Adversary Details page opens.
2. Click within the edit box in the Adversary Description pane.
3. Add the description.

4. Click **Save**.

   The description is saved, and a confirmation alert appears in the alert bar at the top of the page.

Editing the Name of an Adversary

To edit the name of an adversary:

1. Locate and click the adversary.

   The Adversary Details page opens.

2. Click within the name field, and make the desired edits.

3. Click outside of the name field.
   The name is updated, and a confirmation alert appears in an alert bar at the top of the page.

Linking an Event to an Adversary

To link an event to an adversary:

1. Locate and click the adversary.

   The Adversary Details page opens.

2. Click the **Related Events** sub-tab.
3. Click **Add an Event**.
   The Link an Event dialog box opens.

4. Type the name of the event you wish to link.

   The system will provide typeahead suggestions, if any, based on what you have typed.

5. Select the event from the list.

6. Click **Link Event**.
   The event is linked, and a confirmation alert appears in an alert bar at the top of the page.

Unlinking an Event from an Adversary

To unlink an event from an adversary:

1. Locate and click the adversary.

   The Adversary Details page opens.

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

3. Locate the event you wish to unlink, and click **Unlink**.
   A warning dialog box opens asking if you are sure.

4. Click **Unlink Event**.

   The event is unlinked, and a confirmation alert appears in an alert bar at the top of the page.

Linking an Indicator to an Adversary

To link an indicator to an adversary:

1. Locate and click the adversary.

   The Adversary Details page opens.

2. In the Related Indicators pane, click **Link Indicator**.

   The Link an Indicator dialog box opens.

3. Type the name of the indicator you wish to link.

   The system will provide typeahead suggestions, if any, based on what you have typed.

4. Select each indicator you wish to link.

5. Click **Link Indicator**.
   The selected indicator(s) are linked, and a confirmation alert appears in an alert bar at the top of the page.

Unlinking an Indicator from an Adversary

To unlink an indicator from an adversary:

1. Locate and click the file.

   The Adversary Details page opens.

2. In the Related Indicators pane, select the indicator(s) you wish to unlink.

3. Click **Unlink**.
   The selected indicator(s) are unlinked, and a confirmation alert appears in an alert bar at the top of the page.

Files

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

Within this section, the following options are available:

- Accessing the Files Overview Page
- Files Overview Page: Information & Functions

Adding a File

To add a file:

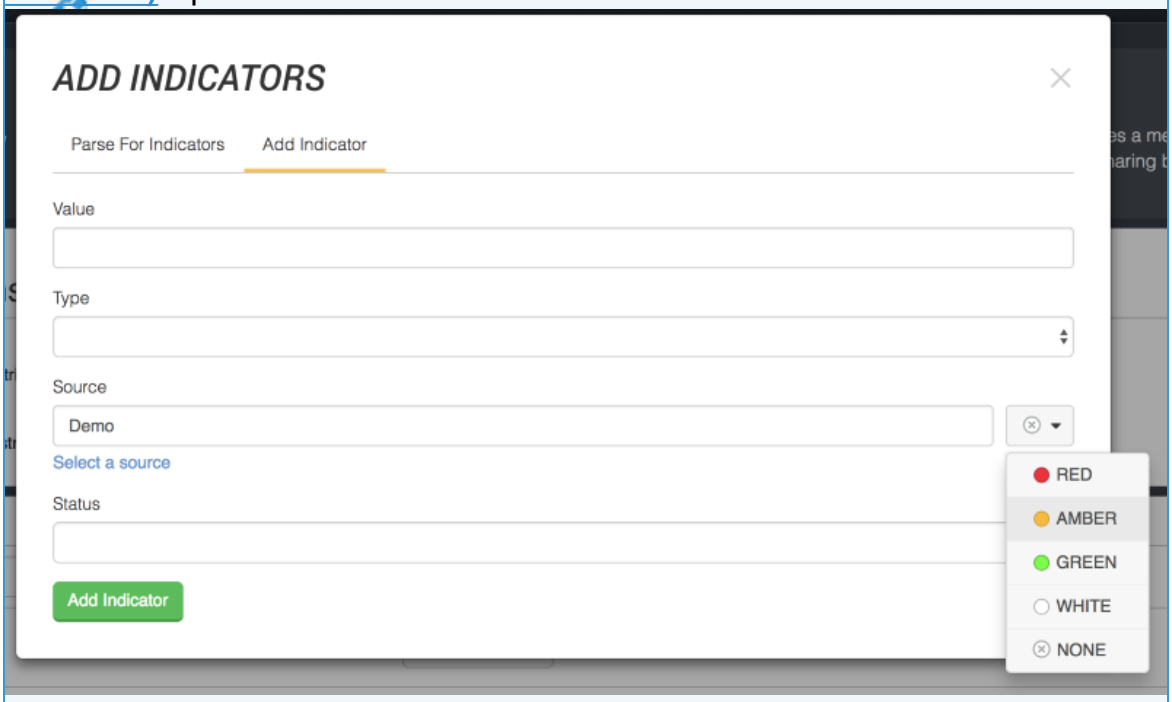
1. Click **Create New** > **File**.

   The Add a File dialog box opens.

2. Drag the file into the dialog box or browse and locate the file.
3. Click **Next Step**.
4. The file will be imported.
5. Select a **Source** from the dropdown 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 Pro-

tocol (TLP) topic for more information on TLP classifications.



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. Identify the File Type.
8. Add any desired tags.

   Tags added appears on the File Details page.

9. Click **Save File**.

   The File Details page opens for the file, and a confirmation alert appears in an alert bar at the top of the page.

Accessing the Files Overview Page

- In the navigation menu,choose **Analytics > Files**.

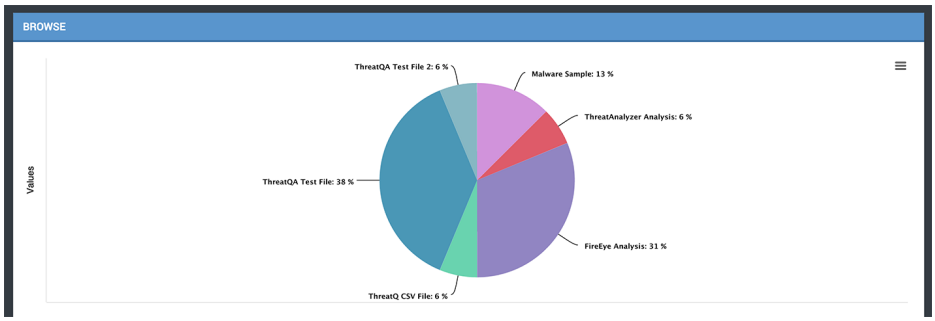
  The Files Overview page opens.

Files Overview Page: Information & Functions

The Files page consists of two sections:

- Files Overview Page: Information & Functions
- Files table

File Types pie chart



The File Types pie chart displays the percentage of different types of files within the system. The following function is available:

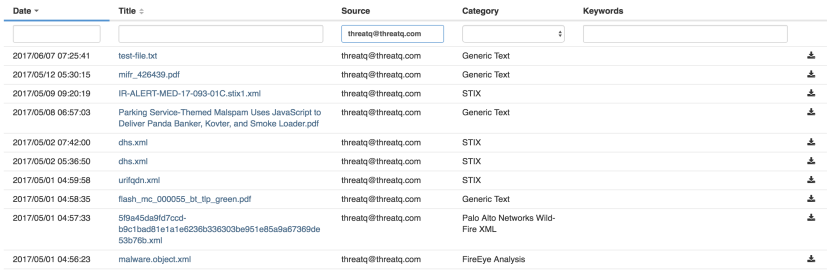
- Viewing more information about a selected file

  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 as a PNG, JPEG, PDF, or SVG

  Click the hamburger menu (see graphic below), and select the desired option.

Files table



Date	Title	Source	Category	Keywords
		threatq@threatq.com		
2017/06/07 07:25:41	test-file.txt	threatq@threatq.com	Generic Text	
2017/05/12 05:30:15	mifr_426439.pdf	threatq@threatq.com	Generic Text	
2017/05/09 09:20:19	IR-ALERT-MED-17-093-01C.stix1.xml	threatq@threatq.com	STIX	
2017/05/08 06:57:03	Parking Service-Themed Malspam Uses JavaScript to Deliver Panda Banker, Kovter, and Smoke Loader.pdf	threatq@threatq.com	Generic Text	
2017/05/02 07:42:00	dhs.xml	threatq@threatq.com	STIX	
2017/05/02 05:36:50	dhs.xml	threatq@threatq.com	STIX	
2017/05/01 04:59:58	urlfqdn.xml	threatq@threatq.com	STIX	
2017/05/01 04:58:35	flash_mc_000055_bt_tlp_green.pdf	threatq@threatq.com	Generic Text	
2017/05/01 04:57:33	5f9a45da9fd7ccd-b9c1bad81e1a1e6236b336303be951e85a9a67369de53b76b.xml	threatq@threatq.com	Palo Alto Networks Wild-Fire XML	
2017/05/01 04:56:23	malware.object.xml	threatq@threatq.com	FireEye Analysis	

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. The following functions are available:

- ***Opening the File Details page for a file***

  Click the name in the Filename column.

- ***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.

- ***Searching within a column***

  Click within the search box at the top of the column, and enter your search criteria.

- ***Downloading a file***

  Click the download icon.

File Details Page

The File Details page provides more information about a particular file.

Within this section, the following options are available:

- Accessing the File Details Page for a Particular File
- File Details Page: Information & Functions

Accessing the File Details Page for a Particular File

1. In the navigation menu, choose **Analytics > Files**.
   The Files Overview page opens.
2. Locate and click the file for which you want to view details.
   The File Details page opens.

File Details Page: Information & Functions

The File Details page consists of the following:

- File Details header
- File Details pane
- Related Indicators pane

File Details header

At the top of the File Details page is a header with the filename, and the date added and last modified. The following function can be performed:

- Deleting a File

File Details pane

This table provides a list of file attributes (type, date and time created and last modified, file name, file size, MIME type, and MD5). The following functions are available.

- Activating the Malware Safety Lock for a File
- Deactivating the Malware Safety Lock for a File
- Adding a New Tag to a File
- Downloading a File

Related Indicators pane

This table provides a list of related indicators. The following functions are available:

- ***Sorting the list by Date of Indicator Creation or Indicator Type***

  Use the dropdown menu to select the desired option.

- ***Accessing the Indicator Details page for a related indicator***

  Click the indicator.

- Linking an Indicator to a File
- Unlinking an Indicator from a File

File Details Page: Procedures

Within this section is a comprehensive set of procedures found on the File Details page. The following options are available:

- Deleting a File
- Activating the Malware Safety Lock for a File
- Deactivating the Malware Safety Lock for a File

- Adding a New Tag to a File
- Downloading a File
- Linking an Indicator to a File
- Unlinking an Indicator from a File

Deleting a File

To delete a file:

1. Locate and click the file.

   The File Details page opens.

2. Click **Delete This File**.

   A confirmation dialog box opens asking if you wish to proceed.

3. Click **Delete File**.

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

Activating the Malware Safety Lock for a File

Activating the Malware Safety Lock will .zip malware files, allowing users to download them without accidentally opening them.

To activate the malware safety lock for file:

1. Locate and click the file.

   The File Details page opens.

2. In the File Details pane, slide the Malware Safety Lock to **ON**.

Deactivating the Malware Safety Lock for a File

To deactivate the malware safety lock for a file:

1. Locate and click the file.
2. The File Details page opens.
3. In the File Details pane, slide the Malware Safety Lock to **OFF**.

Adding a New Tag to a File

To add a new tag to a file:

1. Locate and click the file.

   The File Details page opens.

2. In the File Details pane, under Tags, type the new tag into the **New Tag** field.
3. Press [enter].

Downloading a File

To download a file:

1. Locate and click the file.

   The File Details page opens.

2. In the File Details pane, click **Download File**.

Linking an Indicator to a File

To link an indicator to a file:

1. Locate and click the file.

   The File Details page opens.

2. In the Related Indicators pane, click **Link Indicator**.

   The Link an Indicator dialog box opens.

3. Type the name of the indicator you wish to link.

   The system will provide typeahead suggestions, if any, based on what you have typed.

4. Select each indicator you wish to link.
5. Click **Link Indicator**.
   The selected indicator(s) are linked, and a confirmation alert appears in an alert bar at the top of the page.

Unlinking an Indicator from a File

To unlink an indicator from a file:

1. Locate and click the file.

   The File Details page opens.

2. In the Related Indicators pane, select the indicator(s) you wish to unlink.
3. Click **Unlink**.

   The selected indicator(s) are unlinked, and a confirmation alert appears in an alert bar at the top of the page.

Signatures

The following describes how to manage signatures in ThreatQ.

Signatures Overview

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.

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

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

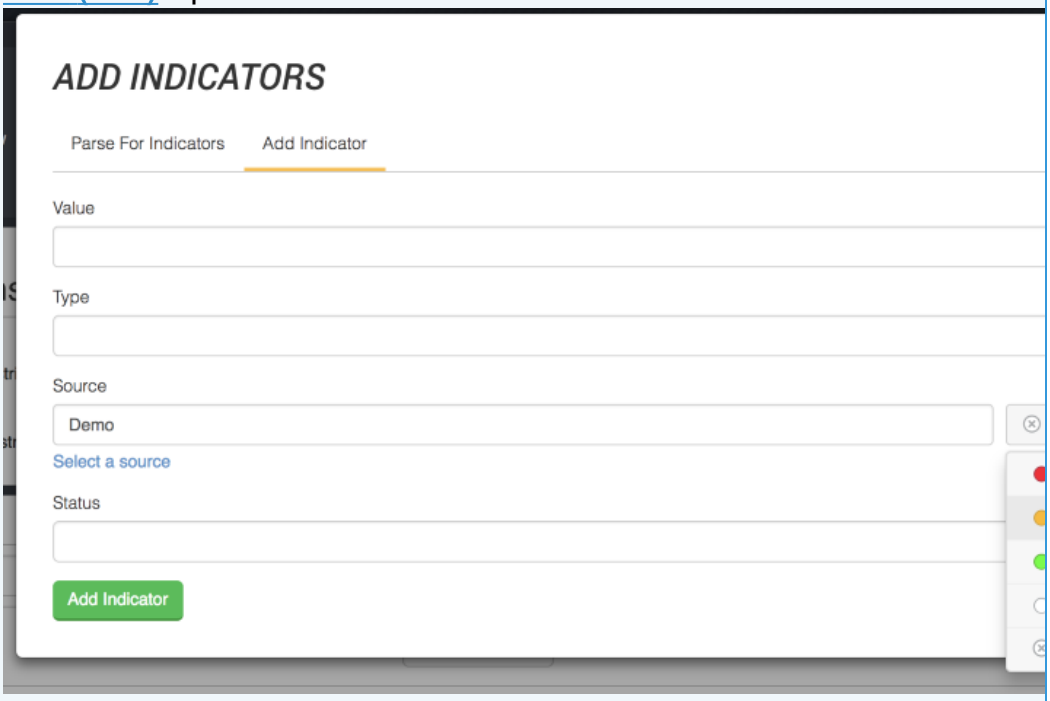
   The Add Signatures dialog box opens.

2. Choose **Which type of signatures are you importing?** from the drop-down menu.

   For Yara, see Adding a Yara Signature.

3. 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.



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 in 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.

    - Click **Review** to accept or reject signatures before completing the import.

      The Add Signatures Step 2: Review and submit page appears.

    - Click **Submit Import** to skip review and finish adding the signatures.

      The Signatures Overview page appears.

11. If you selected to review signatures, choose from the following options:
    - Select one or more signatures and click **Delete**.
    - Click **Create Signatures** to add the signatures displayed on the page.

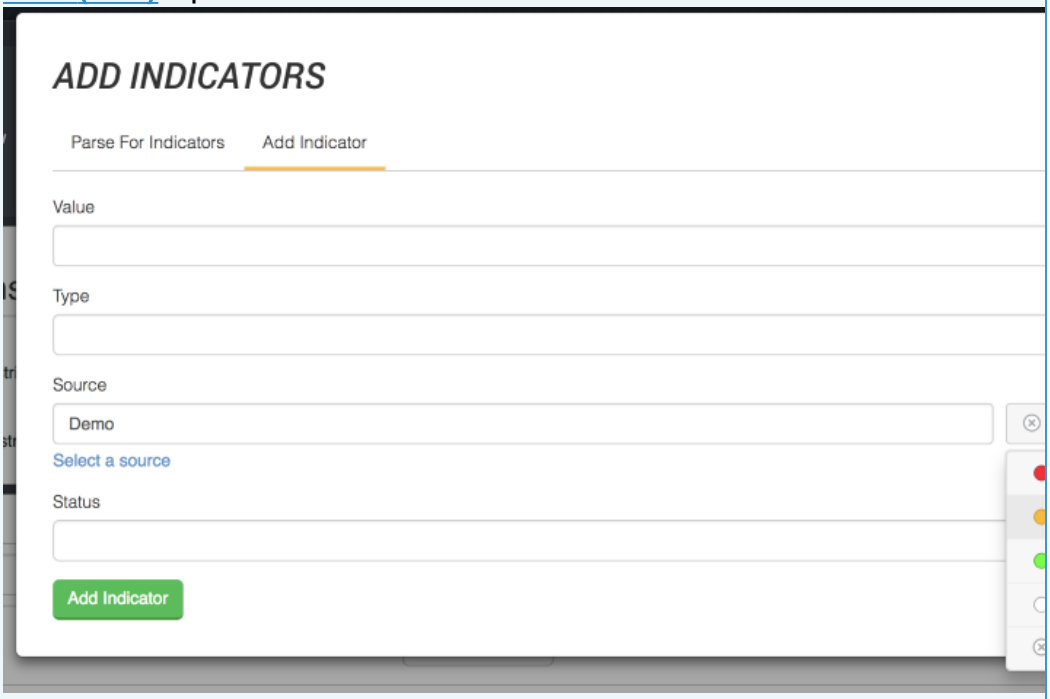
Adding a Yara Signature

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

   The Add Signatures dialog box opens.

2. Choose **Yara** from the**Which type of signatures are you importing?** from the drop-down menu.
3. 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.



4. 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 in the right pane.
5. Optionally, select to parse the signature for indicators.
6. If multiple signatures are found in the yara file, select how you would like to proceed:
   - Save each signature independently as a unique signature.
   - Save as a single signature.
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.

    - Click **Review** to accept or reject signatures before completing the import.

      The Add Signatures Step 2: Review and submit page appears.

    - Click **Submit Import** to skip review and finish adding the signatures.

      The Signatures Overview page appears.
11. If you selected to review signatures, choose from the following options:
    - Select one or more signatures and click **Delete**.
    - Click **Create Signatures** to add the signatures displayed on the page.

Signatures Management

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.

Reports

The following describes how to generate reports in ThreatQ.

- Reports Overview
- Report Options
- Generating Reports

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:

- Previewing Report Customization
- Customizing the Report Header

- 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.

- Exports Overview
- Specific Indicator Export Instructions

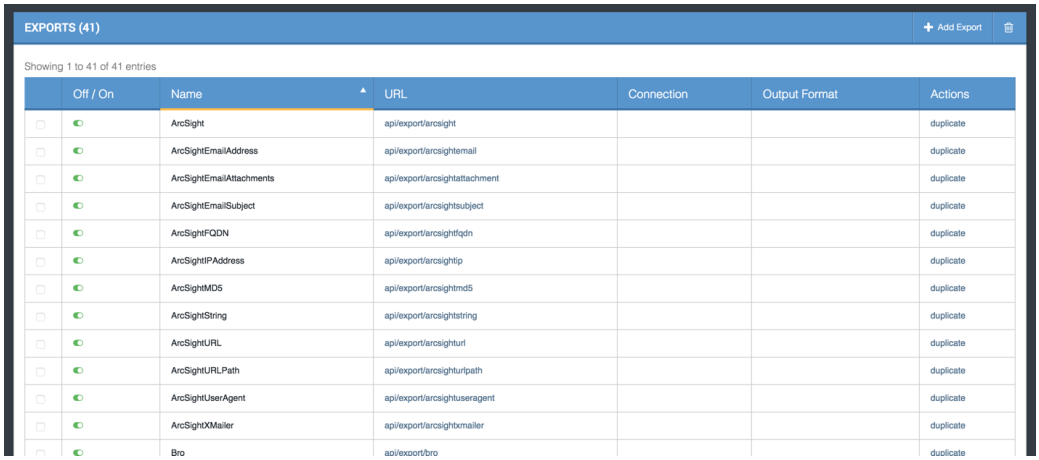
Exports Overview

Exporting is one of the most important parts of ThreatQ as it allows you to output non-whitelisted indicators to an external threat detection system.

ThreatQ comes with a number of standard system exports that have previously been identified as useful. You have the option to use those and/or create your own. Within this section, the following options are available:

- Viewing the Exports List
- Enabling/Disabling an Export
- Viewing an Export
- Duplicating an Export
- Adding an Export
- Accessing/Editing an Export's Connection Settings
- Accessing/Editing an Export's Output Format
- Deleting an Export
- Specific Indicator Export Instructions

Viewing the Exports List



To view the exports list:

- Go to **ThreatQ Configuration** > **Exports**

  The Exports page opens with a table that lists all exports.

Enabling/Disabling an Export

To enable/disable an export:

1. Go to **ThreatQ Configuration** > **Exports**.
2. The Exports page opens with a list of exports.
3. Locate the export you wish to enable/disable.
4. 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. Go to **ThreatQ Configuration** > **Exports**.

   The Exports page opens with a list of 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. Go to **ThreatQ Configuration** > **Exports**.

   The Exports page opens.

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. Go to **ThreatQ Configuration** > **Exports**.

   The Exports page opens.

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

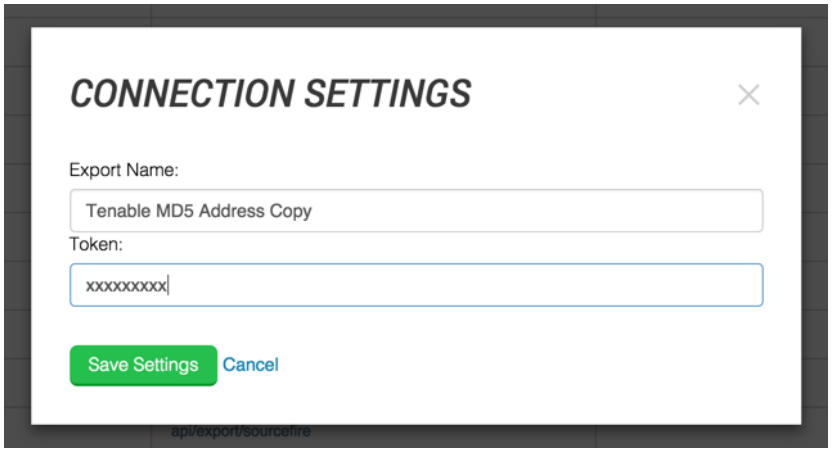
Connection settings are available for each of the exports. The Connection Settings dialog box contains the name of the export as well as the token you'll need to use when connecting a device to ThreatQ.

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. Go to **ThreatQ Configuration** > **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**.

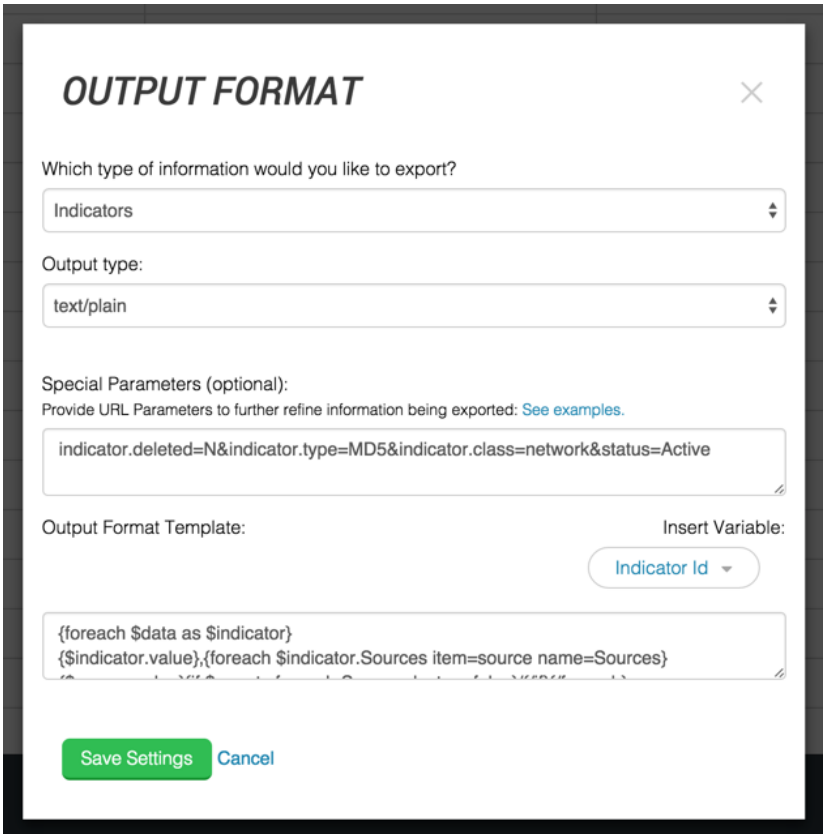
   The settings are saved, and a confirmation alert appears in an alert bar at the top of the page.

Accessing/Editing an Export's Output Format

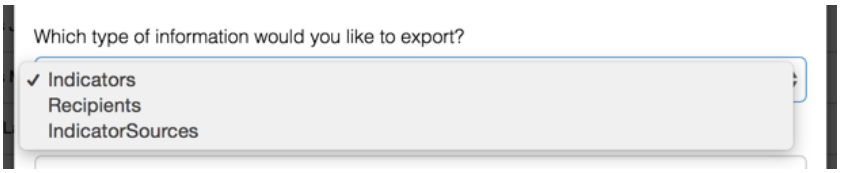
While you cannot edit or delete any of the exports originally supplied by ThreatQ, you can edit exports you have added to ThreatQ or copies of the original exports.

To edit an export's output format:

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



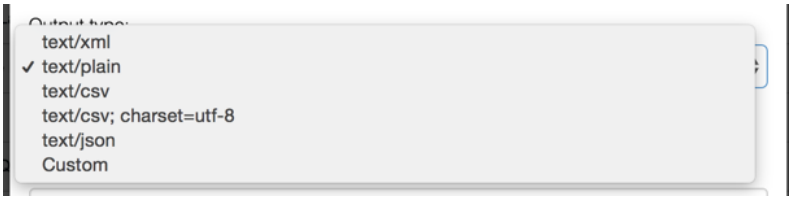
An admin has the ability to choose between the following options:

- 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.

- Customize 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.

Customize 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. Go to **ThreatQ Configuration** > **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 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. 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:

     #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. 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=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. 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.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. 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:

     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. 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 **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. 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:

     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. 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:

     #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. 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.

   - 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 $in-dicator.Sources item=source name=Sources}{$source.value}{if $smarty.-foreach.Sources.last == false}, {/if}{/foreach}{$tab}{foreach $indicator.Adversaries item=adversary name=Adversaries}{$ad-

versary.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. 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:

     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.

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.