Release Notes

Version 5.6.0

Released Date: October 19, 2022

What's New in Version 5.6.0

The ThreatQuotient team is pleased to announce the general availability of ThreatQ version 5.6.0. Below is a list of enhancements, important bugs that have been addressed, and upgrade instructions.

Upgrade Impact

5.6.0 is the first generally available (GA) release of ThreatQ 5x. Due to the scope of this release as well as changes to the upgrade process, we urge customers with a large number (>15M) of Threat Library objects to reach out to ThreatQ Support for an estimate of upgrade time and to review the upgrade process. Once started, the upgrade can't be stopped and the system remains unavailable until the upgrade is complete.

All ThreatQ Data Exchange (TQX) and Air Gapped Data Sync (AGDS) customers must contact ThreatQuotient Support for assistance with the upgrade from 4x to 5x.

After you start the upgrade, do not cancel the installation. Doing so will leave your system in an unusable state.

Full Reindex Required	Data Migration Required	Server Reboot Required
✓	✓	✓

Help Center Updates

We have made the following updates to the Help Center:

- Version 5 Icon - We have added a version 5 icon and note to each page of the Help Center that describes new or updated 5x functionality. As always, information on previous versions is available in PDF user guides.
- Integration Web Guides - Integration docs are now available in web-format on the Help Center. These web guides will reflect the most recent version of the integration. PDF versions of the integration guides will still be available for download.
- Video Updates - The following videos are now available:
  - Attribute Management Overview
  - Feedly CDF Demo

  Additionally, all videos now include closed captions, accessible via the video player's toolbar, as well as downloadable text transcripts.

- Best Practices - The new Best Practices topic in the ThreatQ Support section provides recommendations for maximizing your use of ThreatQuotient products and services.

ThreatQ TDR Orchestrator (TQO)

NEW/UPDATED FEATURES

The ThreatQuotient team is pleased to announce the release of ThreatQ TDR Orchestrator (TQO). ThreatQ TDR Orchestrator includes enhanced automation, analysis, and reporting capabilities that accelerate threat detection and response across disparate systems.

TQO gives you the ability to use Data Collections as data-driven triggers to target specific threat information on the ThreatQ platform.

These Data Collections can then be selected to run through data-driven playbooks, referred to as Configuration Driven Workflows (CDWs), using third-party tools such as Shodan, to curate further detailed threat information. This additional information is then ingested back into the ThreatQ platform for further analysis and refinement.

TQO gives you the option to import advanced workflows from predefined YAML files or create your own workflows in the TQO node view.

See the ThreatQ Help Center for documentation and/or contact our Sales team for more information.

ThreatQ Platform (TQ)

The following is a list of new features, bug fixes, and new identified issues for the ThreatQ platform.

NEW/UPDATED FEATURES

Single Solr Core/SolrCloud

As an investment in the stability and performance of ThreatQ, we are pleased to announce the implementation of Single Solr Core/SolrCloud. This infrastructure enhancement does not impact your user interface experience but does support the continued growth of the ThreatQ Platform and products.

Last Modified Date/Time Stamp

The Last Modified field has been updated to better align with customer needs. The field now accounts for additional object-specific data updates such as changes to the object's attributes and relationships. In response to this enhancement, the Touched At field has been removed from the ThreatQ UI, as this is now reflected in the Last Modified field.

Attribute Management

The new Attribute Management tab within the Object Management page provides you with an overview of attribute data across the Threat Library and allows you to filter this data by Source. In addition, this page allows you to refine and consolidate your Threat Library data by editing, merging, and deleting attribute keys and values associated with system objects.

> When you edit, merge, or delete an attribute key or value, it may take up to one minute for your changes to be reflected in the Attribute Management page and/or Threat Library.

The Add Dashboard window now displays an All and an Owned By Me tab. The All tab lists all of the dashboards you have access to including default, shared, and owned dashboards. The Owned By Me tab lists only the dashboards for which you are designated as the owner. This change makes it easier to locate and select the dashboards you created and/or were assigned ownership of.

> If you are a read-only user or do not own any dashboards, the Owned By Me tab is grayed out and inactive.

Integration Logs

We made the following improvements to integration logging:

- Response Body Text for Errors - To assist with debugging, we added the response body text for HTTP requests that receive an error response to the Dynamo log.
- Configuration Error Messages - To improve troubleshooting, we added more descriptive error messages to logs for the following CDF configuration errors:
  - Too many elements error
  - Too many arguments error
  - Invalid keywords error

  These error messages are displayed in the log when you enable a feed with a configuration error but are not displayed in the ThreatQ user interface.

- New Log File Location - We changed the directory used to store `threatq-dynamo-cli.log` from `/var/files/feed_data/` to `/var/files/log/`.

Task Notifications

The ThreatQ Notification Center now alerts you when you are assigned a task. These task notifications will appear in the Notifications Center dropdown in the platform and will include a link to the assigned task.

Threat Library | Related Object Count Columns

You can now update your Threat Library results list to display related object counts for:

- Adversaries
- Attack Patterns
- Campaign
- Course of Action
- Events
- Exploit Target
- Files
- Identity
- Incident
- Indicators
- Intrusion Set
- Investigations
- Malware
- Report
- Signatures
- TTP
- Tasks
- Tool
- Vulnerability

Click the Manage Columns button to select the columns you want to display. You can click the values in these columns to view the corresponding list of system objects.

In addition, we updated the name of the Threat Library column that displays a comma-separated list of related adversary names to Related Adversary Names. This change differentiates it from the Related Adversaries column that lists the number of related adversaries associated with a system object.

Add Images to Object Descriptions and Description Widgets

The edit fields for object descriptions and Description dashboard widgets now give you the option to insert images. The new icon is located between the text alignment and table options. When you insert an image, you also have the option to:

- Change from the default center image alignment to right or left alignment.
- Add an image caption.
- Add an image text alternative.
- Resize the image.
- Insert a line above and/or below the image.

Threat Library | Edit a Source's TLP Label

You can now update the TLP label assigned to a source from the system object's details page. To do this, click a source in the Sources pane to access the Edit Sources window. Then, select the new TLP label from the dropdown list and click the Save button.

> The option to edit a source's TLP label is only available if TLP visibility is enabled via the Data Controls page.

Object Details | File Preview

You can now preview an unlocked file in the ThreatQ platform as opposed to downloading it to your local device. Clicking the Preview button for the file opens the preview in a new tab. The Preview button has been added to the following locations:

- Object Details
- Files Analytics dashboard
- Table widgets that reference files in your dashboards

> File preview may not be available for some file types or browsers. In these cases, the file is downloaded.

API | User Activity Endpoint Access

We updated the following endpoints to prevent Primary Contributor or Read-Only user access to other users' data:

- `GET api/users/:user_id/activity`
- `GET api/mfa/generate/:user_id`
- `DELETE api/mfa/disable/:user_id`

If these users attempt to provide another user's ID to that endpoint, the system returns a `403 Forbidden` error. In addition, we updated the `POST api/mfa/confirm` endpoint to ensure that

Primary Contributors and Read-only users cannot update the 2-Step Verification settings of other users and instead receive a `403 Forbidden` error.

Data Controls | Scoring Sensitivity Configuration

We updated the Select Adversary field in the Scoring Sensitivity tab to allow you to begin typing the adversary name to narrow down the list of drop-down options.

Integrations | CDF Scheduling Options

ThreatQuotient enhanced its support of Configuration Driven Feeds (CDFs) to provide additional scheduling options. The new Run Frequency section in the Configuration tab for CDFs provides the following new Scheduled options:

- Daily at a specific time
- Weekly on a specific day and at a specific time

As before, you also have Periodic scheduling options.

Integrations | Configuration Page Format

We increased the checkbox spacing and corrected helper text alignment in the Integration configuration page to be consistent with ThreatQ standards.

Integrations | Operations Category Tag

Operations cards in the My Integrations page no longer display a Category tag since this tag is not relevant to operations.

Integrations | TAXII 2.x Feeds

You now have the option to use certificates, instead of HTTP Basic Authentication, to authenticate TAXII 2.x feeds.

Integrations Update | Unseeded Integrations

The following Configuration Driven Feeds (CDFs) have been unseeded from the ThreatQ platform:

- CI Army List IPs
- www.dan.me.uk Tor Node List
- malc0de Domain
- malc0de IP
- MITRE Enterprise ATT&CK
- MITRE PRE-ATT&CK
- MITRE Mobile ATT&CK
- MultiProxy Anonymous Proxy List
- PhishTank
- VXVault URL

These integrations will not be included if you are installing a new ThreatQ instance using ThreatQ version 5.6.0 or later.

This change does not affect customers upgrading from a previous ThreatQ version where the integrations were seeded with the platform (example: upgrading from v4.58 to v5.6.0). The integrations will remain installed and their data unaffected after upgrading to v5.6.0 or later.

Customers can download and install the latest versions of ThreatQ integrations from the ThreatQ Marketplace.

Threat Library | Author Filter and Column

The new Threat Library Author filter is a context filter that allows you to filter the system objects displayed by the user or ThreatQ Data Exchange (TQX) feed that added them. You can also add an Author column to your Threat Library view. This column lists the user or TQX feed associated with the system object.

Threat Library | Bulk Delete Actions

ThreatQuotient made performance improvements to bulk delete actions.

Threat Library | Edit Attributes

You can now edit an attribute's value and source as well as the source's TLP label from the Threat Library object details page. To do this, click the checkbox next to the attribute and then click the Edit option in the Attributes pane to access the Edit Details window. After you make your changes, click the Save button.

> You can only edit one attribute at a time. If you check the box next to more than one attribute, the Edit option is disabled.

> The option to edit a source's TLP label is only available if TLP visibility is enabled via the Data Controls page.

Threat Library | Expiration Date Filter Option

We added a new Expiration Date filter option, is greater than, which allows you to filter your Threat Library view to system objects that have exceeded their expiration date by a specific number of days. For instance, if you create a filter on 7/16/22 for expiration dates greater than 15 days, your Threat Library results list system objects with an expiration date of 7/1/22 or prior.

Threat Library | Keyword Filters

Keyword filters now treat whitespace and punctuation as keyword delimiters. As such, if you search for a phrase such as "Operation Molerats" or "Operation-Molerats", your search returns any object that includes "Operation" or "Molerats" as well as "Operation" and "Molerats". For example, a search for Operation Molerats returns "Operation Molerats" and "Molerats".

Threat Library | Source Is Only Filter Option

The new Source filter option, Is Only, allows you to specify that a filter includes system objects or object attributes that do not have any sources other than the ones specified in your filter. In addition, you can further customize your search to only evaluate the sources assigned to the object, sources assigned to object attributes, or sources assigned to objects and attributes. For instance, you can create a filter to view only the campaigns that have an object or attribute source of Domain Tools. This filter only displays campaigns that have a single object source , Domain Tools, assigned at either the object or attribute level and omits campaigns that have additional object attribute sources such as Domain Tools and This Platform.

Threat Library | Spearphish Event Preview

When you click the eye icon next to a spearphish event, the preview pane now includes a Spearphish Details section that mirrors the section displayed in the object details page for the spearphish event.

Object Details | Adding Tags

We updated the process for adding existing or new tags to an object. To add an existing tag, click the Select an existing tag field and select the tag from a dropdown list of all tags or narrow the list by entering all or part of the tag name. As you type, the dropdown list displays matches for your entry. To add a new tag, click the Create a new tag link. Then, add the new tag name to the Tag name field and press Enter.

Object Details | Description Character Length

The maximum character length for an object's description has been increased from 65,535 characters to 4,294,967,295. This change was made to support intelligence feeds that provide reports with long descriptions.

Object Details | Format Updates

We updated the colors used in the Object Details page to ensure consistency with the ThreatQ color palette.

Object Details | Operations Selection

We updated the Select An Operation field in the object details page to display an operation's logo after you select it from the dropdown list. We also modified the dropdown list so that the operation you select is highlighted but not underlined.

NOTABLE BUG FIXES

- Account Activity logs displayed the same IP address for all user logins. We resolved this by updating activity logging to use Forwarded and X-Forwarded-For headers when logging user IPs to ensure accurate IP logging when ThreatQ resides behind a proxy and the proxy IP is used to connect to ThreatQ.

  > If your ThreatQ instance passes Forwarded and X-Forwarded-For headers with different IP values, ThreatQ returns an error message.

- Under the following conditions, the Comments section of the Object Details page for an adversary record displayed two Add links, one to the left of the Comments section title and one centered within the Comments section:
  - When you clicked the Cancel button before adding a comment.
  - When you expanded an empty Comments section.
- When you specified a chunk-size greater than the API limit of 1000, the threat-collection source failed due to the check that determines if the system has reached the end of the data from the endpoint. We resolved this issue by modifying this process to reference the chunk-size limit specified by the API regardless of what is requested by Dynamo.
- When TLP was disabled in your ThreatQ instance and you duplicated an export that included TLP filters, the copy did not include the TLP configuration. We resolved this issue by updating the duplication process to include TLP configuration whether or not

TLP is enabled. In addition, the Output Format window for an export now displays TLP filters whether or not TLP is enabled.

- When you clicked the trashcan icon next to a related object in the Add An Adversary form, the system deleted the first adversary listed in the Related Objects section instead of the item you selected for deletion.
- When you tried to authenticate via the API using a username instead of an email address, the system returned an error. To address this, we modified the authentication process to accept either a username or email address.
- The Add Indicators window returned the following error when you attempted to add a indicator with a Type of URL and a Value containing a plus sign (+):
  `The indicator value and type do not match`
- The Threat Library filter search was case sensitive. For example, a search for an indicator type of “binary” yielded different results from a search for an indicator type of “Binary”.
- When you used the object details page to update the case of a letter in an attribute value, the system did not retain your change. For instance, if you changed an attribute value from “true” to “True”, the change was not saved and the attribute value remained “true”.
- When you navigated to the Files/Attachments details page or opened the object details preview panel via the Threat Library, API requests made for indicator scoring caused `404` errors.
- When you replaced your current license with a license that included fewer applications, the license was updated correctly. However, the Version window displayed the following error:
  `Error loading license file`
- RSS Feed Reader reports displayed in the Description pane of the object details page for a system object in Threat Library displayed HTML tags instead of applying HTML formatting to the report content.
- In some instances, clicking data collection links in system notifications did not display the corresponding data collection in the Threat Library. For instance, if you had a system notification for the Adversaries data collection and another for the Malware data collection, the first data collection link you clicked displayed the correct data collection and the second link you clicked did not display the correct data collection until you refreshed the Threat Library page.
- When an indicator was set to never expire, you could not edit and save the description.

- When you attempted to import a YARA rule as a signature and it contained an `xor(0x0b)` modifier, the import failed and ThreatQ returned the following error message: `There was a problem uploading your file.`
  We modified the signature import process to parse this type of file.
- Maintenance and Admin users could view shared data collections that had not been shared with them.
- When you added a YARA rule via the signature parser, the `import "math"` line was ignored.

ThreatQ Data Exchange (TQX)

The following is a list of new features, bug fixes, and new identified issues for ThreatQ Data Exchange.

NEW/UPDATED FEATURES

Relational Data

We added the following options to the Relational Data section in the Create and Edit Feed pages:

- Attack Pattern
- Campaign
- Course of Action
- Events
- Exploit Target
- Identity
- Incident
- Indicators
- Intrusion Set
- Malware
- Report
- Signatures
- Tool
- TTP
- Vulnerability

When you check these options, the data feed includes the following name/value, ID, and context fields for each object:

- Description
- Attributes
- Tags
- Comments
- Sources

NOTABLE BUG FIXES

- In the Connections page, when you clicked the Unsubscribe/Subscribe button for an incoming feed, TQX applied your change but did not update the display of the toggle to reflect the new feed status.

- The display of the Last Run, Next Run, and Last Modified fields in the Feed Status page was inconsistent. For Publisher instances, the run time fields reflected the time format specified in your browser, such as Eastern Standard Time (EST), and the Last Modified time reflected the UTC format. For Subscriber instances, the run time fields reflected the UTC format and the Last Modified time was based on the time format specified in your browser.

ThreatQ Investigations (TQI)

The following is a list of new features, bug fixes, and new identified issues for ThreatQ Investigations.

NOTABLE BUG FIXES

- When you selected the Create Object and Link right-click menu option from an evidence board, TQI created the new object but did not link it to the selected node(s).
- When you right-clicked a node not currently assigned to an investigation, the right-click menu displayed the Create Object option. Now, the Create Object option is only displayed when you right-click a node committed to the investigation.
- When you attempted to enter - or = in the TQI search field, the character was not included in your search string. Instead, if you entered a -, the evidence board was zoomed out. If you entered an =, the evidence board was zoomed in. To resolve this, we updated the search field to allow entry of - or =.
- When you added two objects that had attributes with matching names and similar, lengthy attribute values to an investigation, TQI combined the two attributes into one and linked the combined attribute to both objects.

Security and System Updates

The following System updates have been made:

- Upgraded MariaDB to 10.5.
- Modified the firstboot process to use `sudo` instead of `su`.

The following Security Updates have been made:

- Updated ThreatQ to ensure that all session cookies are marked with the `SameSite` attribute. This change prevents the use of cookies in cross-origin requests.
- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF
Apache Log4j 2.17.1	CVE-2021-44832
Apache Zookeeper 3.7.1	CVE-2021-21295 CVE-2021-28165 CVE-2021-21409 CVE-2021-34429 CVE-2020-36518 CVE-2020-9493 CVE-2022-23307
Linux Kernel 3.10.0	CVE-2022-1729 CVE-2022-1966 CVE-2022-21123 CVE-2022-21125 CVE-2022-21166
Moment.js 2.29.4	CVE-2022-24785 CVE-2022-31129

UPDATED TO	CESA REF
OpenJDK 1.8.0	CVE-2022-21540 CVE-2022-21541 CVE-2022-34169
Python 2.7.5	CVE-2020-26116 CVE-2020-26137 CVE-2021-3177

Install Notes

- To upgrade from a 4x version to 5x, you must be on the most recent 4x release.
- For the upgrade from the most recent 4x release to 5x, you will need to enter your MySQL root password during the upgrade process.
- The following warning will be displayed during the upgrade process:

  ```
  Warning: RPMD altered outside of yum.
  **Found 5 pre-existing rpmdb problem(s), 'yum' check output follows
  ```

  This warning does not require any action on your part and will be resolved during the upgrade.
- Do not restart your instance during the upgrade process.

We highly recommend that you perform a backup of your ThreatQ instance before upgrading.

How to Upgrade

> TQAdmin requires elevated privileges and must be run as root.

ThreatQ version 5x provides you with the ability to run an independent preflight check, prior to upgrading, to ensure adequate disk space. The system will also scan your installed integrations for any incompatible versions. You will be unable to perform the upgrade if an incompatible integration version is detected.

> This scan does not apply to integrations installed on third-party systems such as the ThreatQ App for QRadar.

Run a platform check for the most recent ThreatQ version:

```
# tqadmin platform check
```

Run a platform check for a specific version:

```
# tqadmin platform check -v <version number>
```

Upgrade Commands:

To upgrade, run the following command:

```
# tqadmin platform upgrade
```

To upgrade to a specific version, run the following command:

```
# tqadmin platform upgrade -v <version number>
```

As always, contact our Customer Support team if you encounter problems when updating, have any questions, or need assistance.

Thank you,

The ThreatQuotient Team

support@threatq.com
support.threatq.com
703.574.9893