THREATQUOTIENT

Release Notes

Version 5.24.0

Released Date: December 19, 2023

What's New in Version 5.24.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.24.0. Below is a list of enhancements, important bugs that have been addressed, and upgrade instructions.

You can access these release notes, along with other ThreatQ product documentation on the ThreatQ Help Center.

Upgrade Impact

The upgrade is expected to take the standard amount of time for a ThreatQ upgrade. The exact time to complete the upgrade depends on your specific environment and resources.

> ⚠ Upgrades to ThreatQ v5.19.0 or later require a minimum version of 5.13.0.

> ⚠ Customers upgrading to ThreatQ v5.19.0 or later may be prompted to enter the MariaDB root user password to apply Process and Connection Admin grants.

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

Upgrading from...	Full Reindex Required	Data Migration Required	Server Reboot Required
5x (most recent version)	✗	✓	✓

ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform included when you upgrade from ThreatQ v5.23.0, or earlier, to 5.24.0.

NEW/UPDATED FEATURES

Object Details | Comments Pane Enhancements

To make it easier to scan a list of object comments, we made the following changes to the object details Comments pane:

- By default, each comment displays up to four lines of text. For longer comments, you can click the Show More option to view the full details. You can then click the Show Less option to return to the truncated view.
- The Expand All/Collapse All option in the Comments pane header allows you to expand/collapse all of an object's comments. If an object does not have any comments, this option is grayed out.
- The add/edit comment field now includes a toolbar that gives you the option to:
  - Apply styles to comment text.
  - Apply inline formatting such as bold, italics, underline, or strikethrough to comment text.
  - Select a font color and font background color.
  - Insert a link.
  - Add a numbered or bulleted list.
  - Specify text alignment. Undo or redo a comment change.
- The formatting in the comment field is reflected in the PDF export of the system object.

Threat Library | Customize Related Object Columns

In the object details page and object preview panel, you now have the option to choose the columns displayed for each related object type, excluding Files. In addition, ThreatQ retains your column settings and applies them to future sessions. To support these changes, we changed the Linked column name to Reported and the Occurrence column name to Date of Occurrence. Default columns and required columns vary by related object type. See the About Relationship Panes section of the Help Center for more information.

Threat Library | Default Cache Update

We reverted the Threat Library cache change introduced in ThreatQ v5.19.0 by decreasing the default cache for Threat Library searches from ten to two minutes. In addition, we reverted the

CursorMark cache change in ThreatQ v5.20.0 by decreasing the CursorMark cache limit from ten to two minutes.

> This change only affects customers using the default cache setting and does not override any custom cache settings.

Description Deduplication

We added the following description handling to the indicator and signature deduplication processes:

- If there are descriptions with the same source on both objects, the description on the original object is retained and the description on the second object, the merged object, is discarded.
- If there are associated descriptions on the second object, the merged object, that do not exist on the original object, the descriptions are added to the original object and appear first in the object details description list as the more recent descriptions. These descriptions appear in alphanumeric order rather than the time-based order on the merged object.

Job Management | Navigation Tab Location

To ensure consistency with ThreatQ UI standards, we moved the Job Management page tabs from the body area of the page to the header area of the page. In addition, we renamed the All and System Delete tabs to User Changes and System Changes, respectively.

Integrations | Renamed Collection Name Field

We renamed the Collection Name field to Collection Name/Title in the Add New TAXII Feed tab of the Add New Integration window.

NOTABLE BUG FIXES

- When you attempted to generate a PDF of a campaign ingested via a feed, you received a 500 error.
- When you performed a bulk delete or CSV export of selected system objects, the objects remained checked in the Threat Library list until you refreshed the page. We resolved this issue so that the objects submitted for deletion or export do not remain checked in the Threat Library list. And, we updated the delete confirmation message to the following: `Bulk delete job <job number> has been submitted for processing! Results may take time to reflect in the Threat Library`
- We resolved the following display issues encountered in the Bulk Changes page during a bulk update to Event objects:

    - When you selected a value of None in the Status field, the status value overlapped the field name. We resolved this issue and updated the page to pass a null value when you select the None option.
    - We removed the Helper text beneath the Status field as it related only to Indicator object updates.
- We updated the display of the Add Relationship field in Add *<object type>* modals to be consistent with ThreatQ standards. This change involved aligning the field name and search icon as well as updating the field border alignment during input.
- When you run the TLP defaults artisan command, the warning now indicates that it overwrites object description sources:
  ```
  This command will overwrite TLP settings for all objects, object
  attributes, and object descriptions using the configured source defaults.
  ```
- For more lengthy object descriptions, when you clicked the Read More option to expand the description, the text and images within the description overlapped.
- When you accessed the Parse for Intelligence window in dark mode, selected a STIX file, and clicked the Next Step button, the Copy/Paste content here field changed to light mode.
- In dark mode, the Spearphish Details icon in the left navigation pane of the object details page was grayed out.
- When you canceled the merge of attribute values and then selected a new attribute value, ThreatQ allowed you to click the Merge button for a single value and displayed your current selection and your prior selections in the Merge Attribute Values window.
- When you selected the Spearphish Parser option from the create menu, the Type field in the Add Event window did not default to Spearphish. As such, the file import and copy/paste content fields were not displayed.
- CSV exports for file objects did not include the object’s description(s).
- In some instances, searches for table widget and Threat Library columns returned results and a No Results warning.
- Bar chart widgets did not display objects with scores greater than ten. Bar charts now include scores greater than ten as a part of the bar representing objects with a score of ten.
- When you created a bulk change and clicked the Apply Changes button more than once, ThreatQ ran the update multiple times. Now, after you click the Apply Changes button the first time, it converts to a grayed out, inactive state to prevent additional clicks.
- In some instances, after upgrading to ThreatQ v5.22, when you opened an adversary object’s details page, the page data displayed briefly and then was replaced by a blank page. Clearing the cache did not resolve this issue.
- We updated the wording of the Helper text in the Add New Integration window to direct customers to the ThreatQ Help Center for integration documentation.
- We made performance improvements to the AGDS import process.
- When you selected an object type and source in the Object Management screen, searches by value failed to return results.

KNOWN ISSUE

- As a result of object status enhancements in ThreatQ v5.23.0, some object details pages may load as a blank page. Clearing your browser cache will correct this issue.

ThreatQ Investigations (TQI)

The following is a bug fix for ThreatQ Investigations included when you upgrade from ThreatQ v5.23.0, or earlier, to 5.24.0.

NOTABLE BUG FIXES

- When you added a lengthy description to an investigation, the investigation card did not wrap the description text to accommodate the card width. Instead, the text continued past the card borders and was obscured by any adjacent investigation cards.

ThreatQ Data Exchange (TQX)

The following is a list of new features for the ThreatQ Data Exchange included when you upgrade from ThreatQ v5.23.0, or earlier, to 5.24.0.

NEW/UPDATED FEATURES

TAXII Server | View in Threat Library Button

After you select a TAXII collection’s data collection, the new View in Threat Library button in the Edit TAXII Collection page allows you to access the Threat Library view of the data collection in a separate page so that you can review or update the objects specified by the collection.

TAXII Server | Renamed Collection Name Field

In the Create a Collection section of the Set Up Data Exchange with TAXII wizard, we renamed the TAXII Collection Name field to TAXII Collection Name/Title. In addition, we renamed the Collection Name field to Collection Name/Title and removed the field’s Helper text in the following pages:

- Create TAXII Collection
- Edit TAXII Collection

ThreatQ TDR Orchestrator (TQO)

The following is a bug fix for ThreatQ TDR Orchestrator included when you upgrade from ThreatQ v5.23.0, or earlier, to 5.24.0.

NOTABLE BUG FIXES

- Regardless of the data collection selected, workflows ran against indicators and the accepted object types for the action instead of the objects specified in the data collection. Now, workflows only run against the objects specified by the data collection and supported by the workflow’s action(s).

Security and System Updates

The following Security updates have been made:

- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF
Bind 9.11.4	CVE-2023-3341
Java 1.8.0	CVE-2023-22067 CVE-2023-22081
Linux Kernel 3.10.0	CVE-2023-32233 CVE-2023-35001 CVE-2023-3609
Libssh2 1.8.0	CVE-2020-22218
Python 2.7.5	CVE-2023-40217

Install Notes

- To upgrade from a 4x version to versions 5.6 through 5.18, you must be on the most recent 4x release. To upgrade to 5.19 or later, you must first upgrade to release 5.13 or later.
- For the upgrade from the most recent 4x release to versions 5.6 through 5.18, you will need to enter your MariaDB root password during the upgrade process. To upgrade from 5.13 or later to 5.19 or later, you may need to enter your MariaDB 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

Platform Check

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:

```
# sudo /usr/local/bin/tqadmin platform check
```

Run a platform check for a specific version:

```
# sudo /usr/local/bin/tqadmin platform check -v <version number>
```

Upgrade Commands

To upgrade, run the following command:

```
# sudo /usr/local/bin/tqadmin platform upgrade
```

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

```
# sudo /usr/local/bin/tqadmin platform upgrade -v <version number>
```

To discuss planning your upgrade, do not hesitate to get in touch with your Customer Success Engineer.

As always, contact our Customer Support Team if you encounter problems when upgrading or need assistance.

Thank you,

The ThreatQuotient Team

✉ support@threatq.com
🖥 support.threatq.com
☎ 703.574.9893