Release Notes

Version 5.23.0

Released Date: November 30, 2023

What's New in Version 5.23.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.23.0. 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 v5.22.0, or earlier, to 5.23.0.

NEW/UPDATED FEATURES

Threat Library | Status and Point of Contact

You now have the option to add status information to custom objects and all seeded system objects except for Adversaries, Files, Signatures, and Tasks objects. In addition, you can add point of contact information to custom objects and all seeded system objects except for Adversaries, Files, Indicators, Signatures, and Tasks. To support these new fields, we made changes to the following areas:

- Object Management:
  - Replaced the Event Statuses tab with the new Object Statuses tab that allows Admin users to configure and manage statuses as well as control the order in which they are displayed in drop-down lists.
- Object Details Page and Preview Panel:
  - Added the Point of Contact and Status fields to the object details and preview panels.
  - Updated the Generate PDF option on the object details and preview panel Action menus to include Status and Point of Contact in the Overview section of PDF reports.
- Threat Library:
  - Added optional Point of Contact and Status columns.
  - Added Point of Contact and Event Status filters.

> Future releases of ThreatQ will include support for bulk updates of object statuses.

NOTABLE BUG FIXES

- We updated the date format used in PDF exports of custom object details to match the format specified in your System Configurations settings.
- When you filtered Threat Library search results by TLP label, the results list displayed only items that matched your filter criteria. However, if an object had additional object and attribute sources that did not match your filter criteria, the Sources and attribute columns listed those as well. Now, when you apply a TLP filter, the Sources, attribute, and description columns only display data that match the TLP filter.
- To reflect vendor branding, we updated the parser selection field in the Add Indicators window to list a Trellix Analysis option instead of a FireEye Analysis option.
- When an integration install failed, the system did not return an error message and the display of the Add New Integration window was locked. We updated the install process to close the Add New Integration window and return the following error message upon installation failure: `There was an error analyzing feed definition file`

- When you created a bulk update to add a source to file objects, the system returned a SQLstate error and did not apply the update.
- We updated the formatting of the Threat Library Search field to be consistent with ThreatQ standards.
- The last modified timestamp for an object was updated even though the object was not updated. This occurred when a feed ran and the objects ingested had relationships.
- When ThreatQ ingested URLs with a scheme but no file path from a CDF, ThreatQ converted the URL to an FQDN but did not normalize it. We modified the feed ingestion process to normalized URLs and FQDNs.
- When you installed a CDF and configured it with invalid credentials, ThreatQ did not generate an error.json or record.log file in the results folder for the event.
- Threat Library Manage Columns and table widget column selection options did not include the ThreatQ System or other custom description sources. This issue affected customers who upgraded from a ThreatQ 4x release to 5.13 and then to 5.22 and customers who upgraded from ThreatQ 5.13 to 5.20 and then to 5.22. To resolve this we increased the default number of sources displayed for these options from 100 to 1,000.
- We resolved the following issues within the Add Attributes window:
  - When you clicked the Add new name option, the Name field remained grayed out instead of converting into the Type new name entry field. Once you began to type the new attribute name, the field became active.
  - When you searched for an attribute name that did not exist, the Add <attribute name> option was not displayed.
- In ThreatQ 5.18 and 5.21, AGDS imports returned a Failed query error. This occurred while importing tagged objects with different sources or destination type IDs.
- We improved STIX parser performance to address slower parse time for collections with large numbers of objects.
- The Policy Activity & Performance section of the Data Retention Policy page did not display Total Deleted/Policy Deleted values.
- We updated the upgrade process to ensure that ownership and permissions on config.yaml files remain consistent and to correct file permissions as needed.

ThreatQ Investigations (TQI)

The following is a bug fix for ThreatQ Investigations included when you upgrade from ThreatQ v5.22.0, or earlier, to 5.23.0.

NEW/UPDATED FEATURES

Investigation Workbench | Display Multiple Descriptions

The Description (ThreatQ System) section name has been changed to Description. This section displays an object's descriptions in card format and includes description formatting such as tables. You can use the arrow above the top right corner of a card to scroll through the object's descriptions and click the Read More option to view a description in a separate window. From the description window, click the edit icon to update the description.

> When you change a description in TQI, your change is also reflected in the object's Threat Library object details page.

NOTABLE BUG FIXES

- When you hovered on a user icon in the Investigation board, the top left corner of the username field was obscured.

ThreatQ Data Exchange (TQX)

The following is a list of bug fixes for the ThreatQ Data Exchange included when you upgrade from ThreatQ v5.22.0, or earlier, to 5.23.0.

NEW/UPDATED FEATURES

TAXII Server

ThreatQ Data Exchange (TQX) now allows you to configure a TAXII server, create a TAXII collection to specify the STIX object information you want to share, and manage TAXII user credentials to control access to TAXII collection files. To support this change, we have updated TQX to distinguish between the new TAXII server option and the existing OpenDXL data transport options:

- New menu options: The Data Exchange menu is now divided into two sections, TAXII and OpenDXL, with the associated setup and maintenance options listed in each section.
- Page updates:
  - Removed the Transport field from the Edit Feed and the Create Feed pages.
  - Updated the name of the Connections page to OpenDXL Connections.
  - Updated the name of the Data Feeds page to OpenDXL Data Feeds.
  - Updated the data collection info menu to list any TAXII collections associated with the data collection.
  - Updated the data collection deletion process to warn you if you attempt to delete a data collection associated with a TAXII collection.

See the updated ThreatQ Data Exchange section of the Help Center for more information on configuring and using the TAXII server.

NOTABLE BUG FIXES

- We removed the Uuid and Uuid Bin options from the Supporting Context sections of the Create Feed and Edit Feed pages.
- TQX returned an error message when a subscriber attempted to ingest a package containing custom objects.

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