Release Notes

Version 5.17.0

Released Date: July 20, 2023

What's New in Version 5.17.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.17.0. 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.

> ⚠ Customers upgrading from a 5x release prior to 5.12.1 will be prompted to enter their MySQL root password during the upgrade process to allow an adjustment of the subnet mask of the Solr MySQL user’s host.

> ⚠ 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)	✗	✓	✓
4x (most recent version)	✓	✓	✓

> ⚠ If you are upgrading to this release from 5.6 or earlier, a full reindex is required.

Help Center Updates

ThreatQuotient launched a new version of the Help Center on Wednesday, June 21, 2023. The new Help Center provides optimized search results, context-sensitive mini tables of content, table of contents icons, improved top navigation, and a content refresh of major user guides.

Help Center links embedded in the product will continue to work as before. However, you may need to update bookmarked links to specific Help Center pages.

In addition, we removed the Help Center search option from ThreatQ. You can still perform searches from within the Help Center itself.

ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform available when you upgrade from ThreatQ v5.16.0, or earlier, to 5.17.0.

NEW/UPDATED FEATURES

Threat Library | Select Multiple Options

The Threat Library results list now allows you to select multiple objects of the same type for workflows, exports, or bulk actions. You can select individual objects by checking the checkbox to the left of the object or select all the objects currently displayed by clicking the header checkbox next to the Value column title. In addition, the drop down options for the Start Workflow, Export, and Bulk Actions buttons now give you the option to apply your choice to all objects or just the selected objects.

Threat Library | Optimize Queries

We improved the processing of Threat Library queries that include filters and are launched from the user interface.

TQAdmin | Generate a Troubleshooting Package

TQAdmin now supports a command that allows you to generate a troubleshooting package that ThreatQuotient Support can use to identify issues and determine next steps for resolution. See the Generating a Troubleshooting Package section of the Help Center for more information.

NOTABLE BUG FIXES

- If you used the object details page to remove a source from an object, you could not re-add it to the object nor could it be re-added by a feed.
- Object details and preview pages displayed the Add to Watchlist button for Read Only users even though this option is not available to these users. We updated these pages to suppress the button’s display for Read Only users.
- If you left a value of 0 in a required integration configuration field or left this type of field blank, ThreatQ returned the following error: `Failed to update feed`. We replaced this error message with a more descriptive one: `Failed to update feed settings`. In addition, required fields are emphasized with red text and field borders.
- The object details and preview pages did not display scores for indicators.
- When you performed a bulk update without applying a filter to the Threat Library, the corresponding job details in the Job Management page displayed a blank Search Criteria field.

Now, when you perform a bulk update without applying a filter, the Search Criteria field displays the following message: `No search criteria to display.`

- We removed the deleted_at field from `POST /api/:object/:id/sources` endpoint responses and added the existing field.
- Attribute values deleted via the Attribute Management page continued to appear in Threat Library results.
- When you added an incorrect group name to the list option for the `threatq:oauth2-client` artisan command, the system returned a `not a valid group` error. However, when you pressed Enter, it listed client IDs. Now, the error message prompts you to press Enter to view users in the default group.
- In the Job Management page, we updated the display of filter set details in the Search Criteria field to list the IS ONLY field to the left of the source pill.
- When you used the Add New TAXII Feed tab in the Add New Integration window to create a STIX/TAXII server, ThreatQ did not correctly save the TAXII Server Version you entered. As a result, when you tried to enable the feed, the system returned the following error message: `Cannot enable connector due to missing values for required fields.`
- When a data retention policy did not find any objects that matched its parameters and as a result did not delete any objects, its job details listed a Percent Completed value of 0%. Now, the job details for this type of job display a Percent Completed value of 100% and 0 of 0 objects. However, if a data retention policy did not delete any objects due to an error, its job details display a Percent Completed value of 0% and 0 of *X* objects.
- When increasing the volume of data in a Virustotal Collections 1.0.0 or Cisco Threat Grid 1.0.4 CDFs, they sometimes experienced filter-mapping time-outs. We optimized Virustotal Collections and Cisco Threat Grid feeds to prevent filter-mapping timeouts, improve performance of the feeds, and increase logging ability for better diagnostics.
- We resolved the following display issues for Campaign and Identity objects:
  - Campaign Objects - The preview panel did not include the object's objective information. If you generated a PDF from the preview panel, Objective was not listed as an option in the Generate PDF window. If you generated a PDF from the object details page, Objective was listed as an option in the Generate PDF window but the icon was not displayed to the left of the option.
  - Identity Objects - The preview panel did not include the object's contact information. If you generated a PDF from the preview panel, the Contact Information was not listed as an option in the Generate PDF window. If you generated a PDF from the object details page, Contact Information was listed as an option in the Generate PDF window but the icon was not displayed to the left of the option.
- We resolved the following TAXII issues:
  - Type confusion in HTTP responses.
  - Process loop caused when a paged result from a TAXII 2.0 server did not include a Content-Range header.
- In job details, lengthy text displayed on pills in the Search Criteria field was truncated incorrectly. Now, the system appends an ellipsis (...) to truncated pill text.
- When an expired or soft deleted indicator was re-added to the Threat Library, it was not flagged to calculate an expiration date. Now, these types of system objects are flagged by default to calculate an expiration date based on expiration rules defined for their new or pre-existing source.

- In some instances, the artisan command for deduplicating indicators returned the following error message: `[Error Exception] Trying to get property ‘id’ of non-object`
- When you deleted a source from an object, it was removed from the object details page but continued to display on the Threat Library results page.
- We updated dashboard caching to improve dashboard load times for table widgets.
- In the Job Management page, we changed the object type icons displayed in job details from a square background to a round background.
- The Bulk Changes page did not list the correct number of objects affected in the page header.
- When you created a relationship criteria filter that specified the date created was within a specific range and then changed the date created parameter to dates before or after a specific date, the filter continued to apply the date range parameter instead of the newly selected option.
- In the object details page, we updated the display of operation configuration parameters to display the option name on the first line and associated helper text on the next line.
- In the Generate PDF window, we corrected the size, padding, and alignment of data type options.
- When you created a Threat Library value containing a filter with multiple values and AND/OR operators, the system appended an unnecessary AND/OR operator after the last filter value.
- We modified the ThreatQ v5.17.0 upgrade process to handle invalid TLP IDs of 0 by converting them to null. After you upgrade, the system returns an error if a TLP ID of 0 is added.
- We improved the dynamo logging process.
- When you ran the NVD feed with indicators selected, feed run returned a timeout error.
- We made the following changes to streamline system logs:
    - Removed the logging of warning messages for insecure certificates when talking to the API.
    - Set the default log level to Info or above to suppress heartbeat message logs for RabbitMQ.
    - Added logging of operation uninstalls.
- We improved the operation installation process for air gapped deployments.
- When you added a new root CA certificate, it was not applied to operations-server containers.
- We updated the Threat Library process for retrieving system object relationship data to decrease latency.
- Upon upgrading to 5.13.1, some ThreatQ instances experienced a discrepancy between indicator counts in Solr and the database. We resolved this issue by updating delta import processing to ensure that Solr does not exclude objects updated in the same microsecond.

ThreatQ Investigations (TQI)

The following is a bug fix for ThreatQ Investigations available when you upgrade from ThreatQ v5.16.0, or earlier, to 5.17.0.

NOTABLE BUG FIXES

- When a user added a system object to an Investigation from the object details or preview page, the Select Investigation window did not display the investigation name in the correct format. Now, the investigation name is preceded by the investigation icon and followed by the delete icon.

ThreatQ TDR Orchestrator (TQO)

The following is a list of bug fixes for ThreatQ TDR Orchestrator available when you upgrade from ThreatQ v5.16.0, or earlier, to 5.17.0.

NOTABLE BUG FIXES

- The data collection pane included Filter Set fields in the Search Criteria section even though the data collection did not include a filter set. Now, the data collection pane displays the following message for a data collection that does not include a filter set: `No search criteria to display.`
- ThreatQ allowed you to install TQO actions in instances that did not have the required ThreatQ version or a later version. For instance, you could install an action with a required ThreatQ version of 5.13.0 or later in a ThreatQ v5.12.1 instance.

Security and System Updates

The following Security updates have been made:

- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF
Apache Portable Runtime Utility 1.5.2	CVE-2022-25147
Git 1.8.3.1	CVE-2023-25652 CVE-2023-29007
Httpd 2.4.6	CVE-2023-25690
Linux Kernel 3.10.0	CVE-2022-43750
OpenJDK 1.8.0	CVE-2023-21930 CVE-2023-21939 CVE-2023-21954 CVE-2023-21967 CVE-2023-21937 CVE-2023-21938 CVE-2023-21968

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.
- Customers upgrading from a 5x release prior to 5.12.1 will be prompted to enter their MySQL root password during the upgrade process to allow an adjustment of the subnet mask of the Solr MySQL user's host.
- 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