THREATQUOTIENT

Release Notes

Version 5.15.0

Released Date: May 18, 2023

What's New in Version 5.15.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.15.0. 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.

ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform available when you upgrade from ThreatQ v5.14.0, or earlier, to 5.15.0.

NEW/UPDATED FEATURES

Data Retention Policy | Policy Activity & Performance

The Policy Activity & Impact section of the Data Retention Policy page displays a line chart that represents the objects deleted by the data retention policy and the objects added to the system. By default, the Policy Activity & Performance section displays the last 7 days of activity. You can change the date range displayed by clicking the Activity field and selecting Monthly or Yearly. You can click a point on the graph to view object details for a specific day such as the total objects deleted, total objects created, and deletion counts by object type.

The object data displayed in the Policy Activity & Impact chart during the day is cached data reflecting the most recent objects created and policy deletion update processes:

- Objects Created - Updates at 8 AM UTC and reflects the objects created from 12 AM UTC of the prior day until 12 AM UTC of the current day.
- Policy Deletion - Updates after each 12 AM UTC processing of the Data Retention Policy and reflects the policy deletions since the last 12 AM UTC process.

When you update your data retention policy, the line chart does not reflect your updates until the next objects created and policy deletion processes complete.

Data Retention Policy | Save a Data Collection

The Data Retention Policy tab now requires you to select a data collection before enabling the data retention policy. However, you can select and save a data collection without enabling the data retention policy.

In addition, when you disable a data retention policy, the system now returns the following confirmation message: `Your policy has successfully been disabled`

NOTABLE BUG FIXES

- After you clicked the Calculate Impact option in the Data Retention Policy tab, the X in the upper right corner did not allow you to close the display.
- The object details page displayed credentials from an integration's configuration in responses to the `/api/plugins` endpoint. We resolved this issue by removing credential details from the endpoint response.
- When attempting to load a large amount of data, the Event Analytics dashboard locked the browser display.
- The Group By drop down list in the Bar Chart configuration window cropped the bottom of the last list item.
- Operations enrichment search fields in object details pages and preview panels as well as Investigation evidence boards did not include the search icon and the last letter of the field helper text was truncated.
- When you installed a new ThreatQ instance, the Product Analytics page was displayed in Light mode colors. We updated the page to display in Dark mode colors.
- If your system was configured to use the 12 hour time format, the Job Management page Start time and Complete fields did not display the time period, am or pm, associated with the timestamp. If your system was configured to use the 24 hour time format, these fields included unnecessary am/pm time period indicators.
- When you navigated to the Threat Library, ThreatQ generated a duplicate request for object attributes.
- In the integration configuration details page, you could not save Run Frequency setting updates or disable the debug option after enabling it.
- When you attempted to download a file/attachment from within an operation, the system returned an error.
- When you created a data collection with the same name as an existing data collection, the system did not display an error message. Now, when you enter a duplicate data collection name, the Save Data Collection window displays the following error message: `A data collection with this name already exists.`
- The Data Retention Policy screen displayed a field name that referenced a saved search. We changed the field name from "Select a saved search" to "Select a Data Collection".
- When a scheduled run of a configuration driven feed timed out during batching, the API did not send a close or feed timeout error message. To resolve this issue, we updated the API to send close and feed timeout error messages when this occurs.

- When you logged into ThreatQ with Firefox, accessed the Job Management page, and clicked a Retention Policy job to view its details, the data collection name was not displayed. This issue did not occur when you used other browsers such as Chrome and Safari.
- When you viewed the Exports screen in Dark mode, some active checkboxes appeared grayed out. We updated the Dark mode display of checkboxes in this screen to make it clear which checkboxes are active.

ThreatQ Data Exchange (TQX)

The following is a bug fix for ThreatQ Data Exchange available when you upgrade from ThreatQ v5.14.0, or earlier, to 5.15.0.

NOTABLE BUG FIXES

- When you installed or upgraded to ThreatQ 5.14.0, an issue with the iptables script blocked access to a port required by ThreatQ Data Exchange (TQX). As a result, you could not access TQX. We resolved this issue by updating the iptables script to allow traffic on this port.

ThreatQ TDR Orchestrator (TQ0)

The following is a list of new features and bug fixes for ThreatQ TDR Orchestrator available when you upgrade from ThreatQ v5.14.0, or earlier, to 5.15.0.

NEW/UPDATED FEATURES

Expanded System Object Enrichment

TQO now supports the enrichment of all system object types. As we build our portfolio of actions that enrich additional object types, you will be able to use automated or manually triggered workflows to enrich multiple object types. Stay tuned for coming announcements of new actions that enrich multiple system object types.

Orchestrator Page | Display Updates

In the Orchestrator page, we changed the name of the Last Run column to Last Scheduled Run. In addition, if a workflow has not completed a scheduled run, this column displays a value of No Schedule.

NOTABLE BUG FIXES

- The workflow node view truncated the bottom of workflow names that included a letter with a descender, such as p or q.
- When you uploaded a new version of an action that included a change to the action’s name, the name change was reflected in the action configuration panel for existing TQO workflows but not in the node view. Now, action name changes are reflected in the configuration panel and node view.
- In the workflow node view, we updated the Search Criteria display in the data collection details panel to be consistent with ThreatQ styles and formatting.

Security and System Updates

The following System update has been made:

- Updated Apache Batik to version 1.16.

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