THREATQUOTIENT

Release Notes

Version 5.16.0

Released Date: June 06, 2023

What's New in Version 5.16.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.16.0. 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 v5.15.0, or earlier, to 5.16.0.

NEW/UPDATED FEATURES

Threat Library | Customize PDF Report Content

When you select the Generate PDF option from a system object's details page or preview panel, you now have the option to specify the object details included in the PDF report. The new Generate PDF window allows you to select object detail sections such as attributes, sources, tags, description, and comments.

Indicator and Spearphish Parser | Pre-Existing Object Flag Display

We updated the badge displayed next to pre-existing system objects in the Import Indicators and Spearphish Parser review screen to improve ThreatQ usability. The badge is now blue and includes a preview eye icon indicating that you can click it to view the existing object's preview panel.

Integrations | Error Response Handling

We updated a feed's ability to dynamically handle 400+ HTTP status codes when desired. Integration YAML files now support the `pass` and `pass_save` handlers that allow integration authors to specify whether or not error responses are saved and/or passed to the filter chain:

- `pass` - The error response is passed without saving
- `pass_save` - If the integration's debug option is enabled, the response is passed and saved to the downloadable feed files. If not, the response is passed but not saved.

Integrations | Custom Object Value Validation

We updated the ingestion process for custom objects to validate the object value field definition and to return the following error message if the object value is missing: `The value field is required.`

Integrations | Indicator and Signature Ingestion

We updated the `/api/indicator/consume` and `/api/signature/consume` endpoints so that they do not require an object status when ingesting objects via an integration. When an integration ingests an object without a status, a new ThreatQ system object is created and assigned a default status based on the integration configuration. If the integration configuration does not specify a default value, the indicator is assigned a default value of Active.

Table Widgets | Related Object Count Column

You can now add Related Object Count columns to Dashboard Table widgets.

Events Analytics |Events Heatmap

Since the Monthly Heatmap table widget defaults to display events over the last twenty-four hours, we updated its title to Events Heatmap.

Threat Library | Indicator Expiration

We made the following changes to the indicator expiration calculation process:

- Modified the process to skip expiration date calculations for indicators set to never expire.
- Updated the process to correctly handle indicators set to never expire that are marked for expiration processing.
- Added a sixty second default timeout for expiration calculations.

NOTABLE BUG FIXES

- The Table widget configuration window did not list all available Manage Column options for the data collection until you accessed the Threat Library once.
- SAML tokens remained in the session cache for fourteen days after creation. We updated the cache record for SAML tokens to expire after an hour.
- We improved error handling for operations.
- When you created a File object that included a Source, the Source was not displayed in the File's object details page and it was not added to the File.
- When you generated a PDF report of an Asset system object, the Overview section displayed XML tags with the Asset icon.
- The First Published field was not displayed in the header section of the system object details page. This field is now displayed next to the Created field.
- The Search Criteria field in the Job Management page did not display conditional logic indicators such as AND, OR, or NOT. We made the following updates to the display:
  - Filter set criteria are displayed in separate sections that begin with the filter set name such as Filter Set 1.
  - An AND or OR operator is displayed to the right of the filter name.
  - A NOT checkbox is displayed next to the AND or OR operator.
- When you viewed a bulk action job's details, the Update field in the Job Management page only listed the added/removed attribute name and not the associated attribute values. Now, the Update field lists the attribute name and attribute value, separated by a colon.

> Attribute names displayed in the Update field are truncated after fifty characters.

- Debug entries were added to the Laravel log while in production mode.
- Upon upgrading to ThreatQ v5.14.0, logrotate did not rotate Laravel logs.
- The Attribute Management tab in the Object Management page listed the same object counts for attribute values that differed only in capitalization. For instance, the page listed a count of 448 for both the "Long-Range" and "Long-range" attribute values when they had object counts of 448 and 5 respectively. You could not resolve this discrepancy by renaming or merging the attribute values.

ThreatQ Investigations (TQI)

The following is a bug fix for ThreatQ Investigations available when you upgrade from ThreatQ v5.15.0, or earlier, to 5.16.0.

NOTABLE BUG FIXES

- When a Primary Contributor or Read Only user attempted to view an investigation, the evidence board did not display the investigation’s action panel.

ThreatQ TDR Orchestrator (TQO)

The following is a list of bug fixes for ThreatQ TDR Orchestrator available when you upgrade from ThreatQ v5.15.0, or earlier, to 5.16.0.

NOTABLE BUG FIXES

- When a workflow action added context to an indicator, the enriched object's status was changed by default.

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