THREATQUOTIENT

Release Notes

Version 5.12.0

Released Date: February 23, 2023

What's New in Version 5.12.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.12.0. 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.

> ⚠ 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	✗	✓	✓
4x	✓	✓	✓

> ⚠ 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 v5.11.0, or earlier, to 5.12.0.

NEW/UPDATED FEATURES

User Management | Display Theme

We increased customers' display options by moving display theme control from the system to the user level. Now, you can use the Edit User screen to specify each user's ThreatQ display theme as Light, Dark, or Split.

Each user's display theme defaults to Split mode which reflects a mix of light and dark pages. However, if you used the system-level display theme configuration available in v5.11, the user-level setting reflects this change. For instance, if you set all users to Dark mode in 5.11, when you upgrade to 5.12 each user record reflects Dark mode.

If you change your display theme, you will see the update immediately. If you change another user's display theme, the new mode displays the next time they log in.

NOTABLE BUG FIXES

- When you used the Attribute Management tab in the Object Management page to filter attributes by source, the attribute key list was filtered correctly but the attribute value list was not.
- ThreatQ did not rotate or archive Solr logs. We modified Solr log handling to implement:
  - Daily Solr log file handling - When a Solr log file reaches 1 gb, it is archived and the system creates a new log file. The system supports a daily limit of thirty archived Solr log files before deleting the oldest archived log file to make room for a new one. At the beginning of each day, the current log file is archived and a new one is created.
  - Archived Solr file naming convention - Each archived log file name ends with a sequence number. As archived files are deleted, ThreatQ updates the sequence numbers of the remaining archived log files. For instance, when ThreatQ deletes

`solr-2023-02-15-30.log.gz`, `solr-2023-02-15-29.log.gz` is renamed to `solr-2023-02-15-30.log.gz`.

  - Monthly (30 day) Solr log file handling - The system retains thirty days of archived log files, deleting log files for the oldest day as they age out of the thirty day window.

- The With Attribute option for Relationship Criteria filters allowed you to enter an attribute value without an attribute key. We updated the Relationship Criteria window to return the following error message if you attempt to enter an attribute value without an attribute key:
  `Please enter attribute key`
- In the integration details page for each operation, the Required ThreatQ Version defaulted to 2.1. We updated the integration details page to display this field only if the operation file specifies a minimum ThreatQ version. If it does not, the field is suppressed.
- After upgrading from 4.58.1 to 5.9, a customer's MITRE ATT&CK feeds returned connection timeout errors. To resolve this issue, we modified ThreatQ to time out TAXII feeds and return a proxy error if it encounters an invalid proxy.
- In the Threat Library, attributes with long Attribute Values were not truncated and did not include a more/less option to expand/collapse the full display.
- When you updated the system Display mode and opened the System Configuration page in a different browser, the page did not reflect the new Display mode.
- In some instances, upgrades from one 5x version to another took longer than expected due to a lengthy Solr import running during the upgrade. To resolve this issue, we updated the upgrade process, to abort Solr imports after the application is taken into maintenance mode. This change ensures that any running imports are stopped. And, because the system is in maintenance mode, no additional delta imports start outside of the upgrade process.
- Threat Library keyword phrase searches returned more results than expected due to a change in how the search process handles keyword terms. We made the following changes to the search process:
  - Updated keyword searches to specify that the results contain all terms in the phrase. For example, a search for "wicked grommet" returns results that include "wicked" and "grommet".
  - Updated the NOT option to exclude terms from search results. For example, a search for "wicked" and NOT "wicked grommet" includes results that include "wicked" but not both "wicked" and "grommet".

- The Add New Integration window did not allow you to upgrade a previously installed Operation to a new version.
- We resolved the following display mode issues:
  - The Dark mode version of the Threat Library Attribute pane's Date Created date picker calendar was displayed in Light mode colors.
  - The Light mode version of the Watchlist Activity and Tasks widgets in the Overview dashboard used incorrect font colors.
  - In Split mode, some icons on the object details left menu, such as the Investigations icon, had dark outlines on a dark background. This made it difficult to view the icon's outlines.
- Bar, line, and pie chart widgets did not auto-refresh.

ThreatQ TDR Orchestrator (TQO)

The following is a list of new features and bug fixes for ThreatQ TDR Orchestrator available when you upgrade from ThreatQ v5.11.0, or earlier, to 5.12.0.

NEW/UPDATED FEATURES

TQO Actions | Action Icons

TQO actions can now be installed with custom icons. To streamline the install process, these actions are available as ZIP files which include the action's YAML file and icon image file. In addition, the Add New Integration window lists ZIP as a supported file format in addition to YAML and WHL. Note: ZIP install files are only available for TQO actions. They are not available for other integration types such as Apps, CDFs, Connectors or Operations.

Workflows | Workflow Name Updates

You now have the option to change the name of a workflow created in TQO in the workflow's Node view. See the Managing Workflows section of the Help Center for more information on this process.

NOTABLE BUG FIXES

- The Light mode version of the workflow Node View did not display the Virus Total action's logo. In addition, the display of the action node connector lines was not consistent with ThreatQ standards.
- We resolved the following issues with the display of workflow names:
  - When you viewed a workflow created in TQO, the browser page title displayed the unique workflow ID (stored in the name field).
  - When you upgraded to ThreatQ 5.9, the system populated the new `display_name` field with the unique workflow ID instead of populating that value in the `name` field. As a result, the display names for your existing workflows were changed to the corresponding unique workflow IDs.

> This issue only affected workflows created in TQO. It did not affect advanced workflows.

ThreatQ Data Exchange (TQX)

The following is a list of new features and bug fixes for ThreatQ Data Exchange available when you upgrade from ThreatQ v5.11.0, or earlier, to 5.12.0.

NOTABLE BUG FIXES

- When an existing customer with a license that included TQX applied a new license to their ThreatQ server, ThreatQ created a duplicate local DXL broker.
- When you deleted a data feed, the deleted feed continued to display on the Data Feeds page until you refreshed the page.

ThreatQ Investigations (TQI)

The following is a list of new features and bug fixes for ThreatQ Investigations available when you upgrade from ThreatQ v5.11.0, or earlier, to 5.12.0.

NOTABLE BUG FIXES

- We updated the Light mode display of investigation comments and timelines to improve usability and be more consistent with ThreatQ standards.

Security and System Updates

⚠ After upgrading to 5.11.0 or later, you will no longer be able to use root to log into the console. You will need to create an alternate non-root OS/Linux user with sudo privileges to access the console.

The following Security updates have been made:

- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF
Bind 9.11.4	CVE-2021-25220 CVE-2022-2795
Kernel 3.10.0	CVE-2021-26401 CVE-2022-2964
LibXpm 3.5.12	CVE-2022-4883
Mariadb 10.5.19	CVE-2022-47015
OpenJDK 1.8.0	CVE-2023-21830 CVE-2023-21843
Sudo 1.8.23	CVE-2023-22809

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.
- 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, don't 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