Release Notes

Version 5.26.0

Released Date: February 21, 2024

What's New in Version 5.26.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.26.0. 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 may take longer than 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)	*✗	✓	✓

⚠ *Upgrading to ThreatQ v5.26.0 requires a limited reindex, restricted to Adversary system objects.

Rhino Support AI - Beta Release

ThreatQuotient is pleased to announce the Beta launch of Rhino Support AI, a Help Center chat option powered by Artificial Intelligence (AI). This AI chatbot is fully trained on ThreatQ Help Center resources and ready to assist you with product questions.

You can access Rhino Support AI by clicking the chat window in the bottom right corner of any Help Center page. Then, just enter your product-related question to start interacting and exploring using natural language questions and receiving natural language answers.

When you enter a question, Rhino Support AI parses through the Help Center's documentation resources to quickly locate the information related to your question, determine the data's relevance, and deliver an answer in a conversational format. If Rhino Support AI does not have the answer to your question, you can reach out to ThreatQuotient Support via email, web, or chat with a live agent options.

Rhino Support AI is available 24/7 to assist you. It supports chats in twenty-six languages so you can ask questions and receive answers in your language of choice.

Since this is a beta launch, we will be refining the Rhino Support AI based on your questions and feedback. Also, keep in mind that AI chatbots give you answers with a high percentage of accuracy based on the data they have been trained on. See the ThreatQ Help Center for the Rhino Support AI FAQ. However, if you need more assistance you are always welcome to reach out to our ThreatQuotient Support team.

ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform included when you upgrade from ThreatQ v5.25.0, or earlier, to 5.26.0.

NEW/UPDATED FEATURES

Exports | Status and Point of Contact Options

You can now create exports for custom objects and the following system object types that include the object's status and point of contact:

- Assets
- Attack Patterns
- Campaigns
- Courses of Action
- Events
- Exploit Targets
- Identities
- Incidents
- Intrusion Sets
- Malware
- Reports
- Tools
- TTPs
- Vulnerabilities

Data Retention Policy | Data Collection Permissions

Now, when a Maintenance or Administrative user selects a data collection for use by the data retention policy, ThreatQ gives all users view-only access to the data collection.

Threat Library | Bulk Change Event and Custom Object Status

You can now use the Bulk Changes option on the Bulk Actions menu to change or remove the status of Event and custom objects.

Spearphish Parser | Event Status and Point of Contact Option

Now, when you import a spearphish event, the Spearphish Parser gives you the option to assign an event status and/or point of contact.

> The Event Status field is displayed only if an Admin or Maintenance user has configured Event Statuses in the Object Management page.

STIX Parser

You can now apply a status to a custom object during a STIX parser import. This option is available for all custom objects for which an Admin or Maintenance user has configured object statuses.

Keyword Searches

We expanded keyword searches to include object Status and Point of Contact fields.

User Management | Remove Point of Contact and Task for Deleted Users

When you delete a user that is listed as an object’s point of contact or assigned a task, you have the option to replace or remove the user.

Dashboards | Group Events and Custom Objects by Status and Point of Contact

When you configure a bar or pie chart widget for a dashboard, you now have the option to group event and custom objects by status and/or point of contact.

> The group by status option is displayed only if an Admin or Maintenance user has configured Event Statuses in the Object Management page.

User Interface Updates

To improve the user experience, we made the following display changes:

- Updated the Dark Mode hover state of the Load Data Collection menu to display the Owned by Me tab title in white.
- Updated the Dark Mode hover state of the My Integration page tabs to display the tab titles in white.
- Updated the Dark Mode hover state of table column titles to display the column title in white.

In addition, we added new login page images. Each time you load or refresh the login page, ThreatQ selects an image from the library for display.

NOTABLE BUG FIXES

- In some instances, updating the data collection used by your Data Retention Policy (DRP) could cause the DRP to ignore Threat Library filters and result in the unintended deletion of system objects. For instance, if you edited the data collection intended for use with DRP and added an object-specific filter, such as Indicator Type, while viewing another object type category in the Threat Library, that object-specific filter was ignored by the DRP and the entire Threat Library was included in the data collection. We resolved this issue so that DRPs continue to apply the object-specific filters of their data collections.

- Some fields in the Select a status section of the STIX import page displayed overlapping field name text.
- When you ran `GET /api/indicators/search?value=1.1.1.1`, the system returned two null fields, class and status.description. Now, when you run this command, the status.description field does not return a null value.
- You could not add URLs to object descriptions. When you clicked the link button in the Add Description window, the Link URL field did not allow you to enter the link.
- When you applied a Value Contains filter that included a special character to the Threat Library, the search did not return the system objects that matched the filter criteria.
- In the Attribute Management tab of the Object Management page, if you selected an attribute on one results page and selected an attribute on another results page, the original attribute was unselected. As a result, you could not merge two attribute values that were listed on different results pages.
- When you entered a valid MySQL root password that included special characters during an upgrade, the password failed the validation process. We updated the upgrade process to resolve this issue.
- We updated the display of related objects in the object details and object preview pages to center align the manage column icon and dropdown arrow.
- When you accessed the Edit Description window to update a system object’s description, the current description was not displayed. Instead, the Description field was blank.

ThreatQ Data Exchange (TQX)

The following is a list of new features for the ThreatQ Data Exchange included when you upgrade from ThreatQ v5.25.0, or earlier, to 5.26.0.

NEW/UPDATED FEATURES

TAXII Collections | Build History Updates

The TAXII Users & Collections page now includes a Build History option accessible from the settings menu to the right of each collection name. In the Build History tab, the Reason code for builds that ran at the normal, scheduled time is now Scheduled Rebuild instead of Expired.

TAXII Server | Client Access Log

The new Client Access Log tab in the TAXII Collections & Collections page tracks connection attempts and data polling on the TAXII server.

Security and System Updates

The following System and Security updates have been made:

- Upgraded Python to 3.11.8.
- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF
Linux Kernel 3.10.0	CVE-2023-42753

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