Release Notes

Version 5.21.0

Released Date: October 12, 2023

What's New in Version 5.21.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.21.0. 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.

⚠ 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)	✗	✓	✗

⚠ 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 included when you upgrade from ThreatQ v5.20.0, or earlier, to 5.21.0.

NEW/UPDATED FEATURES

Multiple Descriptions for System Objects

ThreatQ now supports multiple descriptions for system objects. You can add, edit, or delete these descriptions through the object details page or preview panel. You can also ingest multiple descriptions through integrations.

> Upon upgrade, all existing object descriptions are assigned a default source of ThreatQ System.

To support multiple descriptions, we made the following changes:

- Object Details and Preview Panel Changes:
  - Changed the object details and preview panel Description pane title to Descriptions. Each description consists of a header and a body. The description header lists the description source's TLP label (if TLP view settings are enabled), source name, last modified timestamp, feed update setting, as well as Edit and Delete options. The Protect from feed updates checkbox allows you to specify whether the description is updated when you ingest a description change from an integration. The description body can include text, tables, and images.
  - Updated the Generate PDF option on the object details and preview Action menus to allow you to select all descriptions or select specific descriptions by source and include them in the PDF output.
- Threat Library Changes:
  - Added a Descriptions section to the Manage Columns dropdown. This section allows you to select the descriptions displayed by source. For each description source you select, the corresponding column is displayed with a title of Description (*Source Name*).
  - Updated the Export CSV option to include multiple descriptions in separate columns by source. For example, the export for an adversary with an Adversary Source and an Assets Source description would include description::Adversary Source and description::Assets Source columns that list the corresponding descriptions.
  - Modified the Source filter to also filter objects by description source.
- Export Changes:
  - Added a new description template variable to allow the export of descriptions as a relation. Description output format template fields used for ThreatQ exports remain the same.

  - Expanded export options to include the option to export multiple object descriptions as well as filter descriptions by TLP and source.
- Dashboard Change:
  - Updated the table widget to allow you to select the description(s) displayed by source. The Descriptions section in the Manage Columns dropdown lists allows you to select the descriptions displayed by source. For each description source you select, the corresponding column is displayed with a title of Description (Source Name).
- Object Creation/Import Changes:
  - Modified the process for creating a system object in ThreatQ so that if you create an object with a description but do not select a source, the description is assigned a source of ThreatQ System and the object is assigned a source based on the ThreatQ login of the user adding the object.
  - Updated system object import processes to assign the selected source to the import object's description(s) as well as the object itself.
- Artisan Command Change:
  - Modified the artisan command for applying a source's default TLP to object sources and attributes sources to also update object description sources.

Threat Library | PDF Exports

We modified the Generate PDF window so that it only displays sections that have content. For instance, if an object does not have any comments, the Comments section is not displayed.

NOTABLE BUG FIXES

- When you created an adversary without a description via the `api/adversary/consume` endpoint, ThreatQ created the adversary object without its description and returned a 500 error.
- For customers on ThreatQ v5.14, upon upgrading an integration, it was unable to execute a manual or scheduled run. To resolve this issue, we modified the integration upgrade process to assign a definition type instead of using the existing definition type.
- We removed the Uuid Bin and Uuid options from the Insert Variable dropdown list in the Output Format window.
- A ThreatQ 4x to 5x upgrade failed due to special characters in the instance's root password. These characters caused the MySQL upgrade command to fail. To resolve this, we changed the upgrade process to isolate the root password from the MySQL upgrade command.
- When you imported a custom object through the STIX parser, it had null `uuid` and `uuid_bin` values.
- When you imported indicators through a parser, the indicators were not assigned `uuid` and `uuid_bin` values.
- When you ran an AGDS export, ThreatQ required you to enter the MariaDB root password before the process started. In addition, your password entry was not validated. We updated the AGDS export process so that you are not required to enter the root password.
- When you performed an operation on an indicator, you were unable to ingest the indicators in the response.

- In some instances, you could not install an Action zip file from a Windows environment. We resolved this issue by updating the Integrations uploader to detect alternate, deprecated MIME types for zip files.
- We removed the display of `uuid` and `uuid_bin` fields in the object details page as well as the Threat Library page.

KNOWN ISSUES

- When you export a file object to a CSV file, the object's description(s) are not included in the export.
- When you add a description to an object via the object details page, you must refresh the page in order to view an updated description count in the object type menu on the left side of the page.

ThreatQ Investigations (TQI)

The following is a new feature for ThreatQ Investigations included when you upgrade from ThreatQ v5.20.0, or earlier, to 5.21.0.

NEW/UPDATED FEATURES

Investigation Object Details | Description Field

We changed the Description field name to Description (ThreatQ System). This field displays the ThreatQ System description of the object if available. If the object does not have a ThreatQ System description, the field lists a value of none.

ThreatQ Data Exchange (TQX)

The following is a list of new features and bug fixes for the ThreatQ Data Exchange included when you upgrade from ThreatQ v5.20.0, or earlier, to 5.21.0.

NEW/UPDATED FEATURES

Multiple Descriptions for System Objects

If a system object included in a TQX feed includes multiple descriptions, TQX includes all of the object's descriptions in the feed.

NOTABLE BUG FIXES

- In some instances, a Publisher instance was unable to send feed data to a Subscriber instance. To resolve this issue, we increased the default heartbeat variable value from 60 to 240.

Security and System Updates

The following Security updates have been made:

- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF
LibWebP7 1.0.3	CVE-2023-4863

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