Release Notes

Version 5.20.0

Released Date: October 17, 2023

What's New in Version 5.20.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.20.0. 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)	✗	✓	✗
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 v5.19.0, or earlier, to 5.20.0.

NEW/UPDATED FEATURES

Threat Library | STIX Export for Indicators

ThreatQ now supports STIX exports for custom system objects and the following seeded system objects:

- Adversaries
- Attack Pattern
- Campaign
- Course of Action
- Identity
- Intrusion Set
- Malware
- Tool
- Vulnerability

> The STIX export does not include related objects.

Each STIX export can contain up to 50,000 system objects. If you attempt to exceed this maximum, a tooltip is displayed indicating that the export option is available for searches under 50,000 objects.

Increased Maximums for HTTPD Workers and Database Connections

We updated the maximum connections for MySQL to 502 and the maximum request workers for Apache to 512.

Increased CursorMark Cache Limit

We increased the CursorMark cache limit from one minute to ten minutes.

ACE Library Integration

The ACE library has been integrated with ThreatQ and no longer requires a separate installation.

Air Gapped Data Sync | Source Filter for Exporting Related Data

The new `--include-all-relationships` parameter for the AGDS export command gives you the option to export all related data for an object if its source matches the `--sources` parameter value. If so, the command exports the primary object’s relationships to any object on the system regardless of the sources of the related objects and/or the source that created the relationships. See the threatq:sync-export section of the Help Center for more information.

NOTABLE BUG FIXES

- When you applied a TLP label filter to your Threat Library results and refreshed the page or returned to it after accessing an object details page, the TLP label filter you selected was still displayed but the results list was no longer filtered based on your selection. We resolved this issue so that your previously selected filter option continues to apply to the results list.
- When you added a file object to the Threat Library, you could not apply an existing tag to the object.
- When you added a related object while creating a new event, the related object was listed twice in the Add Event window.
- We resolved the following issues with select and multiselect fields in Operation configuration pages:
    - You could not change the default value of a selection field.
    - When you selected a value in a multiselect field, ThreatQ displayed a blank page.
- The AGDS export command returned the following error message when you included the `--sources` parameter and specified a source associated with a large number of system objects: `General error: 1390 Prepared statement contains too many placeholders`
- When you attempted to upgrade from ThreatQ v4.58.2 to a 5x version, TQAdmin was not able to apply the SQL password entered and returned a SQL syntax error message.
- When you ran the ACE Parser operation on a system object and selected the Dry Run option, the default IOC status you selected was not applied to the parsed indicators. Instead, these indicators were assigned a status of Review.
- When you attempted to export indicators to a STIX bundle, ThreatQ returned an error message and did not create the STIX bundle. This occurred for indicators whose UUIDs were set in the database and did not pass STIX Export RFC 4122 validation. To resolve this issue, we updated stored UUIDs to comply with RFC 4122 standards.
- You could not install an operation with more than one dependency in an air gapped environment.
- After upgrading to ThreatQ v5.19.0, when a source was re-added to a custom object, threat object, or object attribute with a different creator, ThreatQ returned `500` errors.
- We fixed an error encountered when parsing attachments with empty attributes.
- We updated log storage to reduce memory usage by the pynoceros-messenger container.

ThreatQ TDR Orchestrator (TQO)

The following is a list of bug fixes for ThreatQ TDR Orchestrator available when you upgrade from ThreatQ v5.19.0, or earlier, to 5.20.0.

NOTABLE BUG FIXES

- When you ran a TQO action, the action’s supplemental feeds did not apply the correct timestamp format. We updated the handling of timestamps as follows:
  - Any feed (primary, supplemental, action) with its own timestamp_format/timezone configuration uses that configuration regardless of other configurations.
  - If an action feed does not have a timestamp_format/timezone configuration, it uses the configuration from the primary feed.
  - If a supplemental feed does not have a timestamp_format/timezone configuration, it uses the configuration from the primary feed. If an action calls a supplemental feed, that supplemental feed still inherits from the primary feed and not the action.
  - If a primary feed does not have a timestamp_format configuration, it defaults to YYYY-MM-DD HH:mm:ssZZ where the default timezone is UTC.

Security and System Updates

The following Security updates have been made:

- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF
Linux Firmware	CVE-2020-12321
OpenJDK 1.8.0	CVE-2023-22045 CVE-2023-22049

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