



Release Notes

Version 5.22.0

Released Date: November 01, 2023

What's New in Version 5.22.0


The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.22.0. 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




Due to the performance improvements included in ThreatQ 5.22.0, this upgrade may require more time than a standard ThreatQ upgrade. The exact time to complete the upgrade depends on your specific environment and resources. Refer to the following guidelines to estimate the time required for your upgrade:

INDICATORS	OBJECT RELATIONS RECORDS	ESTIMATED UPGRADE TIME
6M	3M	less than 1 hour
40M	40M	4 to 6 hours
120M	215M	18 to 20 hours

 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)			



ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform included when you upgrade from ThreatQ v5.21.0, or earlier, to 5.22.0.

NEW/UPDATED FEATURES

Threat Library | Event Status and Point of Contact

You now have the option to add status and point of contact information to Event objects. To support these new fields, we made changes to the following areas:

- Object Management:
 - Added an Event Statuses tab that allows admins to configure and manage event statuses as well as control the order in which these statuses are displayed in drop-down lists.
- Object Details Page and Preview Panel:
 - Added the Point of Contact and Status fields to the object details and preview panels of event objects.
 - Updated the Generate PDF option on the object details and preview panel Action menus to include Event Status and Point of Contact in the Overview section of PDF reports for event objects.
- Threat Library:
 - Added optional Point of Contact and Status columns for Event objects.
 - Added Point of Contact and Event Status filters for Event objects.

Threat Library | STIX Exports

We updated STIX export creation to include the object description with the earliest Created At date. For each object in the export, whether it has a single description or multiple descriptions, the export now includes the description with the earliest Created At date.

Backup/Restore | Include Dynamo Credentials

The backup process now includes the configuration file that stores the Dynamo user password (`/etc/threatq/dynamo/config.yaml`). This allows the restore process to restore Dynamo credentials.

NOTABLE BUG FIXES

- When you selected the Generate PDF option from an object's preview panel, the object's file information was not listed in the Generate PDF window.

- For objects with multiple sources, you could not delete a source from the object preview panel or object details page by clicking the X next to the source name. Nor could you delete a source from the preview panel by using the Edit Sources window.

KNOWN ISSUES

- The following integrations require an upgrade to the versions listed below in order to be compatible with ThreatQ v5.22:
 - Hybrid Analysis CDF v1.2.1
 - RSS Feed Reader CDF v1.0.5

In addition, any feeds that access files outside of the `/var/files` directory will require an update in order to be compatible with ThreatQ v5.22.

ThreatQ Investigations (TQI)

The following is a bug fix for ThreatQ Investigations included when you upgrade from ThreatQ v5.21.0, or earlier, to 5.22.0.

NOTABLE BUG FIXES

- To improve the load time of investigations, we made the following changes:
 - Limited the requests to refresh graph data to prevent a backlog of refresh requests during a long running request.
 - Increased the amount of time between data refreshes from thirty seconds to five minutes to allow more time for one request to complete before another begins.

ThreatQ Data Exchange (TOX)

The following is a list of bug fixes for the ThreatQ Data Exchange included when you upgrade from ThreatQ v5.21.0, or earlier, to 5.22.0.

NOTABLE BUG FIXES

- When a Subscriber ingested an object description, the description retained the Last Modified timestamp sent by the Publisher instead of being updated to reflect the date/time of ingestion. We modified the description ingestion process to update the description's Last Modified timestamp.
- Upon upgrading to 5.21, you could not create events or view object details on a ThreatQ instance with an incoming TOX feed.



ThreatQ TDR Orchestrator (TQO)

The following is a bug fix for the ThreatQ TDR Orchestrator included when you upgrade from ThreatQ v5.21.0, or earlier, to 5.22.0.

NOTABLE BUG FIXES

- The ThreatQ ACE Action was unable to defang and parse a fanged email address that contained [.]. We updated the ACE library to defang [.].



Security and System Updates

The following Security update has been made:

- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF
Linux Kernel 3.10.0	CVE-2023-20593 CVE-2023-35788



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