



Release Notes

Version 5.25.0

Released Date: January 31, 2024


What's New in Version 5.25.0


The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.25.0. 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)			



ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform included when you upgrade from ThreatQ v5.24.1, or earlier, to 5.25.0.

NEW/UPDATED FEATURES

Threat Library | Notes System Object

A new system object type, Notes, is now seeded in the Threat Library. Notes objects are STIX 2.1 objects that provide further context and/or additional analysis. ThreatQ v5.25.0 allows you to manually add these objects. You can export a Note object to PDF or CSV. Additional support for importing and exporting these objects will be added in future releases.

Keyword Searches

We revised keyword search logic to return to the keyword tokenizer method used in ThreatQ 4x. As a result, keyword searches for phrases return objects that include all the terms in the phrase. For instance, a search for "united kingdom" returns objects that include "united kingdom" instead of objects that include "united" and "kingdom" or "united" or "kingdom". By default, searches return instances where the search term or phrase is a standalone prefaced by and appended by a space. For instance, a search for "panda" does not return "pandas" or "expandability".

To search for characters in a string, you can use a percent sign (%) or asterisk (*) to specify that characters appear in the position represented by the wildcard. For example, specifying "net%" matches "network" and "netware". Specifying "%net" matches "botnet" and "internet". Specifying "%net%" matches "ninety" and "hornets".

Dashboard | Table Widget Display of Attributes

We updated the query process used to pull attribute information for display in table widgets to exclude unnecessary attribute data from the query response. This change improves performance for queries on objects with a large number of attributes.

Threat Library | Related Object Requests

We updated the handling of Threat Library requests for related object information to improve performance.

We updated the handling of Threat Library requests for related object information to improve performance.

NOTABLE BUG FIXES

- When you ingested a STIX 1.2 file via a CDF that contained an object with a TLP label of White, the object was added to the Threat Library with a TLP status of None instead of a TLP label of Clear.
- In the related Adversaries section of the object details page, the display of the Linked By and Confidence columns overlapped.
- We updated the Overview dashboard to suppress the display of the Watchlist Activity widget for Read-Only users. This widget displays objects the user has added to the watchlist. Since Read-Only users cannot add objects to the watchlist, the widget did not display any data for these users.
- You could not execute a TQO workflow from a Threat Library or Dashboard object preview panel. When you clicked the Start Workflow option from the Action menu, the Select Workflow window was not displayed.
- We streamlined the handling of IP address changes by updating container configuration to use the host-gateway IP. This allows the updating of the host IP without requiring the restart of all services to refresh the host IP.
- When you performed a bulk update to set objects to a status of None, the corresponding Update column in the Job Management page was blank. Now, the Update column displays Status Change: None for this type of bulk update.
- In some instances, the Job Management page used a deprecated style for the display of search criteria.
- In the main navigation menu, the dropdown options lists did not display the connecting arrow at the top of the list window.
- Bulk updates that included a TLP label update did not apply the new TLP label to the selected objects.
- In some instances, the Job Management page did not display job entries after you expanded a job's details.
- When you selected the option to remove attributes, the Bulk Changes screen did not provide a dropdown list for attribute name selection.
- AGDS exports did not include descriptions for objects and their relationships.
- In the object details page, Read Only users could not select the display of additional columns for related objects. Now, Read Only and Primary Contributor users can select additional columns. However, the selections are not saved for these account types.
- In some instances, adding a dash followed by a space (-) or a one followed by a period and a space (1.) to an object description caused your browser to crash.

ThreatQ Data Exchange (TQX)

The following is a list of new features for the ThreatQ Data Exchange included when you upgrade from ThreatQ v5.24.1, or earlier, to 5.25.0.

NEW/UPDATED FEATURES

TAXII Server | Build History Audit Log

The new Build History tab in the Edit TAXII Collection page lists audit log entries for each TAXII collection build process. These log entries provide information useful in troubleshooting issues such as build status, start and completion date/time, data collection, reason code, and error information if applicable.

Security and System Updates

The following Security updates have been made:

- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF
Linux Firmware 39.31.5	CVE-2023-20569 CVE-2023-20593
Linux Kernel 3.10.0	CVE-2022-40982 CVE-2023-3611 CVE-2023-3776 CVE-2023-4206 CVE-2023-4207 CVE-2023-4208
OpenJDK 1.8.0	CVE-2024-20918 CVE-2024-20919 CVE-2024-20921 CVE-2024-20926 CVE-2024-20945 CVE-2024-20952



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