



Release Notes

Version 5.7.0


Released Date: November 01, 2022







What's New in Version 5.7.0

The ThreatQuotient team is pleased to announce the general availability of ThreatQ version 5.7.0. Below is a list of enhancements, important bugs that have been addressed, and upgrade instructions.

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.

 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			
4x			

ThreatQ Platform (TQ)

The following is a list of new features, bug fixes, and new identified issues for the ThreatQ platform.

NEW/UPDATED FEATURES

Threat Library | Author Filter Options and Column

The Author context filter allows you to filter the system objects displayed based on the object's source author. It now allows you to filter by Configuration Driven Feed (CDF), Operation, and/or ThreatQ TDR Orchestrator (TQO) Workflow/CDW author in addition to the existing options that allow you to filter by user and/or ThreatQ Data Exchange (TOX) feed.

When you apply the Author filter, the Author column is automatically added to the results listing. The Author column displays the source author(s) listed alphabetically in pill format.

Threat Library | Relationship Criteria Filter Option

The Relationship Criteria filter has a new Additional Criteria option, With Attribute. The With Attribute option allows you to filter results based on one or more specific attribute keys or attribute key and value combinations. In addition, you can specify that an object must meet all or at least one of your With Attribute criteria.

NOTABLE BUG FIXES

- In the Threat Library object details page, the Edit Sources window displayed a TLP selection field when TLP was disabled at the system level.
- While parsing a file for system objects, if you selected a system object that was not present in the Add Relationship field, the `No results found` error message was not displayed correctly.

- The ThreatQ build process did not clean up or archive json.log docker logs under `/var/lib/docker/containers/$CONTAINER_ID`.
- When you added multiple yara rules from the signature parser and added the same rules again, it caused rules duplication. As a result, each rule had two signature IDs.
- When you clicked quickly between two attribute keys in the Attribute Management page, the system did not cancel your first request to display attribute values. As a result, the second attribute key you clicked displayed the attribute values associated with the first one you clicked.
- When TLP functionality was enabled, you were not able to add a system object until you selected a TLP label other than the default value of None.
- An AGDS import required more time than expected due to the handling of adversary descriptions. To resolve this, we updated the `threatq: sync-import` process handling of indicators attributes and adversary descriptions.
- When you attempted to import Indicator objects from a source with an indicator expiration rule, the system returned the following error message:
`Failed to complete the import.`

ThreatQ TDR Orchestrator (TQO)

NEW/UPDATED FEATURES

Actions | Confirm Install

When you click the Uninstall button on an Action's configuration details page, the Are You Sure? window warns you that the uninstall cannot be undone and prompts you to confirm the uninstall. You must click the Uninstall Action button to complete the process.

NOTABLE BUG FIXES

- When you clicked the Save button after updating a workflow description, your changes were not saved. To save your description changes, you had to click the Save Changes button at the bottom of the panel. To resolve this issue, we removed the Save button.
- TQO did not automatically disable a workflow when you deleted all of its actions. In addition, you could not manually disable a workflow after deleting all of its actions.

Security and System Updates

The following Security Updates have been made:

- Removed the following from `/etc/ssh/sshd_config`:
 - `3des-cbc`
 - `diffie-hellman-group-exchange-sha1`
- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF
Bind 9.11.4	CVE-2022-38177 CVE-2022-38178
Expat 2.1.0	CVE-2022-40674
Open VM Tools 11.0.5	CVE-2022-31676
OpenJDK 1.8.0	CVE-2022-21619 CVE-2022-21624 CVE-2022-21626

Install Notes

- To upgrade from a 4x version to 5x, you must be on the most recent 4x release.
- For the upgrade from the most recent 4x release to 5x, you will need to enter your MySQL 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



TQAdmin requires elevated privileges and must be run as root.

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:

```
# tqadmin platform check
```

Run a platform check for a specific version:

```
# tqadmin platform check -v <version number>
```

Upgrade Commands:

To upgrade, run the following command:

```
# tqadmin platform upgrade
```

To upgrade to a specific version, run the following command:

```
# tqadmin platform upgrade -v <version number>
```

To discuss planning your upgrade, don't 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