Release Notes

Version 6.6.0

Released Date: December 10, 2024

What's New in Version 6.6.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.6.0. 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.

ThreatQ 4x End of Life

ThreatQuotient provides support for the most current major version of ThreatQ and the immediately previous major version of ThreatQ only. With the general availability of ThreatQ 6x, support for ThreatQ 4x is drawing to a close as ThreatQ 6x becomes the current major version and ThreatQ 5x is its immediate predecessor.

As such, we recommend that any customer still on a ThreatQ 4x version upgrade as soon as possible. Contact ThreatQuotient Support if you have questions or need assistance with upgrading to a supported version.

Migration Impact

If you are deploying ThreatQ 6x for the first time, the upgrade requires setting up a new Ubuntu 22.04 LTS or Red Hat Enterprise Linux (RHEL) 8.10 or 9.4 instance, installing ThreatQ 6x in this new instance, and then restoring the data from your ThreatQ 5x instance. The exact time to complete the upgrade depends on your specific environment and resources.

Access the ThreatQ Help Center to view or download the ThreatQ Version 6 Installation guides. Contact our Customer Support Team or your Customer Success Engineer to request the ThreatQ Version 6 Migration guide for detailed information on migrating to ThreatQ 6x.

Upgrade Impact

If you are upgrading from one ThreatQ 6x version to another, see the How to Upgrade section for more information on executing a platform check and upgrade.

ThreatQ Platform (TQ)

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

NEW/UPDATED FEATURES

Threat Library | Infrastructure Objects

Infrastructure objects are now a seeded object type in ThreatQ. For these objects, ThreatQ stores infrastructure type and kill chain phase information as attributes. In addition, ThreatQ supports STIX exports/imports of infrastructure objects via the Threat Library, object details and preview pages, and the ThreatQ Data Exchange (TQX) TAXII server.

When you import an infrastructure object that includes Kill Chain Phase information from a STIX file, this information is imported as attributes with the attribute name prefaced with the "Kill Chain:". For example, if you import the InfraOne infrastructure item, it has an attribute of Kill Chain: mitre-attack.

When you export an infrastructure object that includes Kill Chain: attributes to a STIX file, these attributes are exported as Kill Chain Phase information.

Threat Library | STIX Export and Import of Location Objects

When you export system objects with the following location keys as attributes to a STIX file, the export process converts these attributes to STIX location objects: latitude, region, city, longitude, country, street address, precision, administrative area, postal code. STIX imports of location objects convert these objects to attributes.

Object Details | STIX Exports

You can now export ThreatQ-supported STIX objects to STIX files from the object details and object preview pages as well as Threat Library search results. Exports from the object details and object preview pages include up to 1,000 relationships per object. Exports from the Threat Library do not include related objects.

> Objects with more than 1,000 relationships return them in an indeterminate order. As a result, there is no sort method available to determine which of the relationships are included in the STIX export.

Note and Report objects can only be exported to STIX from the object details and object preview pages, not from Threat Library search results.

ThreatQ now supports STIX exports of Incident objects from the Threat Library.

Integrations | Feed Run Activity Tab

The My Integrations page has been renamed as the Integrations page. This page contains the My Integrations and Feed Run Activity tabs. The My Integrations tab contains all the information and options previously displayed in the My Integrations page. It displays integration cards and allows you to add, remove, and configure ThreatQ integrations that you have downloaded from the ThreatQ Marketplace or are seeded in ThreatQ.

The new Feed Run Activity tab in the Integrations page lists feed run activity for all installed feeds on the ThreatQ instance within the last ninety days. By default, this tab lists the last seven days of activity but can be updated to display the last twenty four hours, thirty days, or ninety days of activity. You can also filter the display by feed name or view all feeds. You can click a feed run to view more information on it or to run the feed again.

NOTABLE BUG FIXES

- When your search did not return results, the following modals did not give you the option to create an object:
  - Search - accessible from the main menu by clicking the magnifying glass icon next to the Create button.
  - Add Relationships - accessible from the Actions button in the object details page or preview panel.
- When you exported object details to PDF, the links to related investigations were incorrect. These links now point to the investigation's workbench page.
- The STIX parser now ingests STIX Cyber-Observable Objects (SCOs) included in STIX 2.1 files using the same logic as for the ingestion of SCOs in STIX 2.0 files.
- When you used the NOT option in conjunction with the Is protected from auto-expiration filter, the Threat Library did not exclude objects protected from auto-expiration from your search results.

ThreatQ Investigations (TQI)

The following is a bug fix for ThreatQ Investigations.

NOTABLE BUG FIXES

- When you used the Add to Investigation option on the object details page or preview panel Actions menu, the search field in the Select Investigation modal searched system objects as well as investigation names.

ThreatQ Data Exchange (TQX)

The following is a list of new features for ThreatQ Data Exchange.

NEW/UPDATED FEATURES

TAXII Server | Export of Incident, Infrastructure, and Report Objects

The TQX TAXII Server now supports the export of Incident, Infrastructure and Report Objects.

TAXII Server | Relational Data

TAXII Server exports now include up to 1,000 relationships per object.

> Objects with more than 1,000 relationships return them in an indeterminate order. As a result, there is no sort method available to determine which of the relationships are included in the TAXII Server export.

TAXII Server | New TAXII Collection Options

The Create and Edit TAXII Collection pages contain a new Output section. The Relational Data subsection within it allows you to select the relational data included in exports created using the TAXII collection. The Relational Data section allows you to check/uncheck the following STIX 2.1 object types: Adversaries, Attack Pattern, Campaign, Course of Action, Identity, Incident, Indicators, Infrastructure, Intrusion Set, Malware, Notes, Report, Tool, and Vulnerability.

TAXII Server | TAXII Collection Updates

TQX now updates the objects included in a TAXII collection by searching the Threat Library for objects that match the collection criteria and have a modified_at date later than the last Threat Library search.

Security and System Updates

The following Security updates have been made:

- Added output sanitization measures to the ThreatQ frontend to prevent cross-site scripting (XSS) attacks.
- Pynoceros Container:

UPDATED TO	CESA/GITHUB REFERENCE
idna 3.10	CVE-2024-3651
cryptography 43.0.3	GHSA-h4gh-qq45-vh27
aiohttp 3.11.5	CVE-2024-27306 CVE-2024-30251
requests 2.32.3	CVE-2024-35195
zipp 3.2.10	CVE-2024-5569
PyMySQL 1.1.1	CVE-2024-36039

ThreatQ v6 Installation

- The installation process for ThreatQ 6.6.0 requires a ThreatQ 5.29.4 backup file. If you attempt to use a backup file from a different ThreatQ 5x release, the restore process will return an error.
- Access the ThreatQ Help Center to view or download the ThreatQ Version 6 Installation guides. Contact our Customer Support Team or your Customer Success Engineer to request the ThreatQ Version 6 Migration guide for detailed information on migrating to ThreatQ 6x.

How to Upgrade

> After you start the upgrade, do not cancel the installation. Doing so will leave your system in an unusable state.

Platform Check

ThreatQ 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, 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