THREATQ
A SECURONIX COMPANY

Release Notes

Version 6.15.1

Released Date: December 12, 2025

What's New in Version 6.15.1

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.15.1. 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.

Migration Impact

> The migration process for ThreatQ 6.9.1 and later releases requires a ThreatQ 5.29.5 backup file. The migration process for releases prior to ThreatQ 6.9.1 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.

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, 9.4, or 9.6 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 Technical Account Manager 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 bug fixes for the ThreatQ platform.

NEW/UPDATED FEATURES

Dynamo-Worker Enhancements

In ThreatQ v6.15.1, the dynamo-worker service scales up from one service to two. This change allows feeds to use an additional feed processing resource, and benefits environments with heavy data ingress.

Additionally, ThreatQ v6.15.1 enables the Redis Publisher feature within the dynamo-worker service. This allows data feeds to process faster with enhanced concurrency and data deduplication strategies.

These changes may impact customer feeds as follows:

- There will be some instances in which the Feed Activity Log's Ingestion Summary will be empty or show less information than typical.
- Data feeds that repeatedly ingest large numbers of byte-identical objects across runs will now show lower ingress counts in the Feed Ingestion Summary. This is due to Redis Publisher's use of a new deduplication routine that reduces overall load on ThreatQ in these cases.

Backup and Restore Authentication Enhancement

Credentials for the Backup and Restore processes are now handled automatically, simplifying the process and increasing security. Users are no longer prompted for MariaDB credentials, and a separate MariaDB user is now created as part of the install process.

See the Backup and Restore topic in the Help Center for the updated process.

NOTABLE BUG FIXES

The following platform bugs were fixed with ThreatQ version 6.15.1:

- Previously, the Source filter in the Threat Library displayed internal client sources, such as ThreatQ API, ThreatQ Platform, ThreatQ System, and ThreatQ Front End. The Source filter no longer displays these sources.
- We resolved the following time zone display issues:
  - The Time picker field displayed the browser timezone instead of the default UTC timezone or the timezone specified at the system or user level.
  - Threat Library search results displayed timestamps in UTC regardless of the timezone specified at the system or user level.

- When typing quickly or pressing a character and the spacebar simultaneously in the task Description field, the cursor moved to the beginning of the line. We resolved this issue so that the user interface now maintains the correct cursor position during typing.
- When you attempted to share a data collection, dashboard, or investigation, the Sharing modal allowed you to select the **Everybody (Public)** option when you assigned editing permissions or updated ownership. When you applied this change, ThreatQ returned the **Error adding sharing permissions** message since the **Everybody (Public)** option is only available for view-only permissions. We updated the Sharing modal so that the **Everybody (Public)** option appears only when assigning view-only permissions.
- ThreatQ continued to display relationship limit banners even after you took action to reduce the number of object relationships. We resolved this issue by:
    - Updating the soft delete process for relationships.
    - Ensuring that when you import the same object/related object, the object count per source is not incremented an additional time.
- Google fonts added for use by CKEditor in ThreatQ v6.9.1 were loaded from external Google APIs. This caused longer than normal load times upon login for air gapped instances or instances that blocked access. To resolve this issue, these fonts are now bundled with ThreatQ instead of loaded from Google APIs.
- We resolved an issue where line chart widget labels did not include a space between the date and the object name.
- When ThreatQ v6.15.0 instances ingested objects via a CDF or TQO workflow, some object relationships, such as relationships between attack patterns and reports or identities and reports, were not created. For example, when related report and attack pattern objects were ingested, the attack pattern was not listed as a related object for the report object. We resolved this by updating ingestion logic to ensure these relationships are created during the ingestion process.

Security and System Updates

The following updates have been made:

- We revised the generation of session tokens, client IDs, and client secrets to increase entropy and provide additional security against brute forcing or guessing of keys.
- Websocket container:

UPDATED TO	CESA REF
axios 1.12.2	CVE-2025-58754
form-data 4.0.4	CVE-2025-7783

- Redis container

UPDATED TO	CESA REF
Redis 7.4.7	CVE-2025-49844

ThreatQ v6 Installation

- If you are migrating from ThreatQ v5 to ThreatQ v6, see the Migration Impact section.
- **Pinning your RHEL 9 release:**

  The following steps allow you to pin your current RHEL 9 release so that you cannot inadvertently upgrade your RHEL 9 environment to an unsupported release. See the **Red Hat Enterprise Linux 9 Support** section of the Help Center for more information on currently supported RHEL 9 versions.

  > Run the following commands as root or prefix them with sudo.

  1. Set release to minor version:
  2. subscription-manager release --set=**<release number>**
  3. Clean repositories:
  4. yum clean all
  5. Check which release is set locally:
  6. subscription-manager release --show
- **Pinning your Ubuntu release:**
  We recommend you update the release-upgrades file to disable manual Ubuntu upgrades so that you cannot inadvertently upgrade your Ubuntu 22.04 environment to an unsupported release.
  - Use a text editor, such as vi, to access `/etc/update-manager/release-upgrades`.
  - Change the `Prompt=` setting to `Prompt=never`.
  - Save your changes and exit the file.

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

> Air gapped customers should reference the **Upgrading an Air Gapped ThreatQ Instance** section of the Help Center.

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 Technical Account Manager.

As always, contact our Customer Support Team if you encounter problems when upgrading or need assistance.

Thank you,

The ThreatQuotient Team

✉ tq-support@securonix.com
🖥 ts.securonix.com
☎ 703.574.9893