THREATQ
A SECURONIX COMPANY

Release Notes

Version 6.12.0

Released Date: September 09, 2025

What's New in Version 6.12.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.12.0. 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.

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 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

ThreatQ Rebranding

As of version 6.12.0, ThreatQ has been rebranded under Securonix, following the acquisition of ThreatQuotient. This change is cosmetic only, involving updates to the color palette and branding elements across the platform. Core functionality and integrations remain fully intact.

In addition, Split Mode has been retired. User accounts currently set to Split mode will convert to Light mode upon upgrade.

ThreatQ Help Center Login

The ThreatQ Help Center, https://helpcenter.threatq.com, is now open to the public and no longer requires YUM credentials to access its content.

There is no change required for customers. Existing links to the Help Center that utilize the reverse proxy process (ThreatQ versions <=6.12.0) will still work as intended. Those links will be updated in a future release as login credentials are no longer required.

NOTABLE BUG FIXES

- When you attempted to export an object’s details to PDF, the export process failed if the object details contained a non-breaking hyphen (U+2011). To resolve this issue, we updated the export process to convert a non-breaking hyphen into a hyphen-minus (U+002D).
- In an Adversary Analytics dashboard that displayed more than 1,000 adversary objects, the adversary overlap details were not reflected on the Indicator Distribution pie chart.
- Previously, when you updated feed settings during a feed run (for example, increasing the number of objects to ingest), the feed returned an error while continuing to ingest the updated number of objects. We resolved this issue so that feed updates trigger a restart as expected.
- In some instances, scheduled feed runs for hosted customers did not run. We resolved this issue by updating the feed run scheduler.

Security and System Updates

The following Updates have been made:

- For ThreatQ hosted customers, updated to Falco helm chart 6.2.2.
- Updated Tika to version 3.2.1 (CVE-2025-2158, CVE-2025-3069, CVE-2025-3069, CVE-2025-21502).
- Solr-backup-handler container:

UPDATED TO	CESA REFERENCE
brace-expansion 2.0.2	CVE-2025-5889
cross-spawn 7.0.6	CVE-2024-21538
path-to-regexp 0.1.12	CVE-2024-52798

- Frontend container:

UPDATED TO	CESA REFERENCE
brace-expansion 1.1.12	CVE-2025-5889
cross-spawn 7.0.6	CVE-2024-21538
form-data 4.0.4	CVE-2025-7783

- Threatqtaxii and Operations-manager containers:

UPDATED TO	CESA REFERENCE
requests 2.32.4	CVE-2024-47081
urllib3 2.5.0	CVE-2025-50181 CVE-2025-50182

- Pynoceros container:

UPDATED TO	CESA REFERENCE

UPDATED TO	CESA REFERENCE
aiohttp 3.12.14	CVE-2025-53643
requests 2.32.4	CVE-2024-47081
urllib3 2.5.0	CVE-2025-50181 CVE-2025-50182

ThreatQ v6 Installation

- **Migrating to ThreatQ v6:**
    - 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.
    - 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.
- **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 Customer Success Engineer.

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