Release Notes

Version 6.13.0

Released Date: October 01, 2025

What's New in Version 6.13.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.13.0. 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, 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 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

Integrations | ACE Parser Updates

In addition to relating and creating system objects, the ACE parser now links existing objects in the Threat Library if the name of the object exists in the content:

- When matching on objects from the Threat Library, the ACE parser only matches exact system object names, regardless of their case. As before, a TQO action's configuration options also influence which objects the ACE parser processes. For example, the ThreatQ Ace Action can be configured to parse for Adversaries and exclude a subset of Adversary names.
- If a system object name consists of more than one word, the ACE parser matches the entire name, the name without spaces, as well as the name with separators such as dashes, colons, or underscores. For example, the ACE parse would return a match for Sad Panda, SadPanda, and Sad-Panda.
- System objects with ACE as their only source are exempt from keyword matching.

Red Hat Enterprise Linux (RHEL) Support

ThreatQ now supports RHEL 9.6 and provides steps to assist customers in setting up a hardened Red Hat Enterprise Linux (RHEL) 9.6 environment according to DISA STIG for Red Hat Enterprise Linux 9 V2R3 hardening standards. See the Security Hardening section of the Help Center for more information.

Help Center Links

Since the Help Center no longer requires YUM credentials, we have updated all Help Center links in ThreatQ v6.13.0 and later to remove reverse proxy references.

NOTABLE BUG FIXES

- When you parsed a file that contained an indicator already in the Threat Library but that did not specify its source, the parsing process removed the TLP label assigned to the indicator source. For example, if Indicator101 had a source of Source202 with a green TLP label, when you parsed a file containing indicator101 without a source value, the parsing process removed the green TLP label from the indicator's source in the Threat Library, Source202. We resolved this issue so that an indicator's TLP label persists even if the source is not provided in the parsed file.

- The `GET api/attributes/{id}/values` endpoint returned a 400 error when the required `type` parameter was missing. We resolved this issue by updating the endpoint to enforce `type=indicator` as a required query parameter.
- When the Feed Run Activity tab listed multiple pages of log entries, you could not access all pages. To resolve this issue, we updated pagination logic so that all pages are now accessible.
- We resolved an issue in the Indicator Details page that prevented the consistent display of sources contributing to an indicator's score in the Score Summary popover.
- We resolved an issue where pie chart dashboard widgets configured to display task object information grouped by Assigned To or Reporter failed to display data.
- STIX exports from the Threat Library and the TQX TAXII server generated STIX 2.1 patterns with improperly escaped backslashes, causing validation failures. For example, the **c:\test\test** file path was not correctly escaped, resulting in an invalid escape sequence of **c:\\test\\test** instead of **c:\\\\test\\\\test**. We updated STIX export creation to ensure that STIX patterns with backslashes are correctly escaped.
- Upon upgrading to ThreatQ v6.11.2, any export that was configured to filter by one or more TLP labels failed. We updated the export logic so that you can now filter by any combination of TLP labels without causing the export to fail.
- We resolved an issue where the Score Summary in an indicator's object details page remained in a Pending Calculation state when an indicator attribute with a scoring policy contained a forward slash.

Security and System Updates

The following Updates have been made:

- Updated RabbitMQ to version 4.1.4.
- Updated Tika to version 3.2.3 (CWE-611). Resolved a privilege escalation vulnerability that allowed users with Primary Contributor access to read files outside the attachments directory, including Kubernetes tokens.
- TQ-OpenDXL-Broker container:

UPDATED TO	CESA REFERENCE
urllib3 2.5.0	CVE-2025-50181 CVE-2025-50182

- Pynoceros-Messenger container:

UPDATED TO	CESA REFERENCE
aiohttp 3.12.15	CVE-2025-53643
requests 2.32.5	CVE-2024-47081
urllib3 2.5.0	CVE-2025-50181 CVE-2025-50182

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 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