Release Notes

Version 6.5.0

Released Date: October 29, 2024

What's New in Version 6.5.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.5.0. 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

Red Hat Enterprise Linux (RHEL) 8.10 Support

ThreatQuotient now supports the deployment of ThreatQ v6.5.0 in a Red Hat Enterprise Linux (RHEL) 8.10 instance as well as a 9.4 instance.

> While ThreatQuotient supports Security Technical Implementation Guide (STIG) installs for RHEL 9.4 instances. We do not currently support STIG installs for RHEL 8.10 instances.

STIX Parser Error Display

The STIX parser now displays more descriptive error messages. When this parser encounters an error, the corresponding error message is displayed at the bottom of the window below the following message: Some issues were found during parsing.

NOTABLE BUG FIXES

- Manually triggered workflows containing the Zscaler action did not set the last_page attribute to True when there were no more entries in the data collection.
- In some instances, a custom connector run by a cron job returned an error indicating the CSV builder could not parse a unicode character. We resolved this issue by updating the process to include the required environment variables to support encoding.
- The User Management page took longer than expected to load as ThreatQ checked point-of-contact data for each user.
- For CDFs that use fulfillment feeds, the fulfillment manager now passes the since and until values of the parent feed to the fulfillment feed as run_meta.since and run_meta.until.
- When a TAXI collection build or a STIX export contained an object that was protected from auto-expiration, ThreatQ returned an error and did not complete the build or export.

Security and System Updates

The following Security and System updates have been made:

- Tika Container:

UPDATED TO	CESA/GITHUB REFERENCE
OpenJDK 17.0.12	CVE-2024-21131 CVE-2024-21140 CVE-2024-21145 CVE-2024-21147

- Solr-backup-handler:

UPDATED TO	CESA/GITHUB REFERENCE
body-parser 1.20.3	CVE-2024-45590
express 4.21.1	CVE-2024-43796
send 0.19.0	CVE-2024-43799
serve-static 1.16.2	CVE-2024-43800

ThreatQ v6 Installation

- The installation process for ThreatQ 6.5.0 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