Release Notes

Version 6.5.1

Released Date: November 19, 2024

What's New in Version 6.5.1

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.5.1. 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.

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 new feature and a list of bug fixes for the ThreatQ platform.

NEW/UPDATED FEATURES

Red Hat Enterprise Linux (RHEL) 8.10 | STIG Installs

ThreatQuotient now supports Security Technical Implementation Guide (STIG) installs for RHEL 8.10 as well as 9.4 instances.

NEW KNOWN ISSUES

When your search does not return results, the following modals do 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.

NOTABLE BUG FIXES

- When you exported an object's details to PDF, the PDF contained incorrect links for the object and its related objects. We resolved this issue so that the links included in PDF exports are correct.
- When you created a table widget and added an Expiration Date column, the Expiration Date column listed expiration dates only for expired indicators. The Expiration Date column now lists expiration dates for both expired and unexpired indicators.
- Updating the default time in the Date Created window caused unintended changes. When you changed the hour, the minute field automatically changed to 00. When you changed the minutes, the hour field automatically changed to 12. This occurred the first time you changed the time during a login session.
- When you attempted to export CVE indicators to STIX, ThreatQ returned the following error: There was an error compiling the Threat Library objects into STIX objects: *<indicator name>*: {Unsupported: ThreatQ type, 'CVE', cannot be exported to STIX}
  We resolved this issue so that CVE indicators are exported to STIX as vulnerability objects.
- In the Run Frequency section of CDF integration configuration pages, we decreased the Data Collection, Timezone, and run frequency field sizes and changed the time picker used to select the run time.
- When you restarted a ThreatQ v6 install, TQAdmin's preflight check could return an error that incorrectly indicated RKE2 was not installed. We resolved this issue by updating the RKE2 preflight check.
- During the upgrade of a STIG install of ThreatQ v6, the installer blocked execution of executables embedded in the terraform provider directories that were updated/added after

the initial install. Now, the trusted executables database (trustdb) for the file access policy daemon (fapolicyd) is updated with new/changed terraform provider executables during upgrades as well as installs.

ThreatQ Investigations (TQI)

The following is a new feature for ThreatQ Investigations.

NEW/UPDATED FEATURES

Investigations Overview | Investigation Card Order

The Investigations overview page now displays the 100 most recently updated investigation cards in descending order by the date of their last update. As such, the most recently updated investigation is listed first.

NEW KNOWN ISSUES

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

ThreatQ TDR Orchestrator (TQO)

The following is a bug fix for the ThreatQ TDR Orchestrator.

NOTABLE BUG FIXES

- In the right pane of the workflow builder page, the run frequency and run time fields displayed for the Daily and Weekly options were aligned incorrectly. To resolve this issue, we decreased the Data Collection, Timezone, and run frequency field sizes and changed the time picker used to select the run time.

Security and System Updates

The following Security update has been made:

- Added strict transport security including a max age setting to response headers.

ThreatQ v6 Installation

- The installation process for ThreatQ 6.5.1 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.

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