Release Notes

Version 6.4.0

Released Date: October 10, 2024

What's New in Version 6.4.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.4.0. 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) 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 6x Upgrade Path Update

The ThreatQ 6x migration process now supports the restore of a ThreatQ v5.29.4 backup file in a ThreatQ v6.4.0 instance. This change allows customers to upgrade from ThreatQ 5.29.4 to ThreatQ 6.4.0.

Trusted Root CA Certificates

We updated ThreatQ to use the operating system's trusted CA bundle for ThreatQ 6x Ubuntu and RHEL instances.

System Configuration | Bypass Proxy Settings

ThreatQ now uses the values you add to the Bypass Proxy Setting for these Hosts and Domains field to bypass the proxy for operations, CDFs, and ThreatQ TDR Orchestrator in addition to custom connectors.

> Integration-level proxy configurations take priority over the ThreatQ system-level proxy configuration.

STIX Export Bundles | Indicator Expiration

The STIX export process now includes indicator expiration timestamps in the valid_until field.

STIX Parser | Relational Data Parsing

To improve performance, we modified the process the STIX parser uses to locate relational data.

NOTABLE BUG FIXES

- When you added more than one Threat Library filter set that included source criteria and changed one of the filter sets from source to object source, your change was applied to the first filter set that included source criteria instead of the filter set you updated.
- When you attempted to install a custom connector in a ThreatQ RHEL instance, you could receive a permission error.
- During some Security Technical Implementation Guide (STIG) installs of ThreatQ 6x, there was a delay in reloading trustdb so that the installation reached the Terraform stage first. This resulted in a failed install. We updated the installer to ensure that the hash of each terraform provider exists in trustdb before continuing the install process.
- We updated the ThreatQ Developer guide so that it no longer displays errors.
- If a ThreatQ instance had more than a thousand sources, the Scoring tab in the Data Controls page did not allow you to view or search all of the sources. We updated this tab to support the display and search of over one thousand sources. In addition, we added pagination that allows you to view sources in increments of 10, 25, 50, or 100 sources per page.
- You could not create two Threat Library source filters that used the same source. For instance, if you created a source filter to exclude objects with SourceAlpha and SourceBeta, you could not create a second source filter to exclude objects with only SourceAlpha. We updated source filter creation to allow you to create two source filters that use the same source.
- When ThreatQ attempted to ingest a STIX 1.2 file that included an SSDEEP indicator, ThreatQ returned a namespace error. This occurred because the object namespace and rules are not loaded into the namespace definitions when an object type was previously found. We resolved this issue by updating STIX parsing to load base object information after a specific object type's information has been loaded.
- When TQAdmin encountered an incorrect or missing $PATH variable, the TQAdmin preflight check for RKE2 failed and stopped the upgrade process. To resolve this issue, we updated the RKE2 preflight check process.
- We made the following updates to the handling of tag data ingested from the MISP Import CDF:
    - Updated the Save Tags As option to apply to indicators as well as events.
    - Added NCSC and TLP tags to the CDF’s mapping.

ThreatQ TDR Orchestrator (TQO)

The following is a bug fix for ThreatQ Orchestrator.

NOTABLE BUG FIXES

- When you ran a manually triggered workflow that did not include a data collection, ThreatQ returned the following error: `Error applying filter`. We resolved this issue so that you can run manually triggered workflows that do not include a data collection.

ThreatQ Data Exchange (TQX)

The following is a new feature for ThreatQ Data Exchange.

NEW/UPDATED FEATURES

STIX Export Bundles | Indicator Expiration

We updated the STIX export processes to include indicator expiration dates in the valid_until field. The valid_until field is included in TAXII collections for indicators that have expiration dates.

Security and System Updates

The following Security and System updates have been made:

- Updated the API container image to Alpine 3.20.
- Changed the policy selected for the AWS Application Load Balancer (ALB) to ELBSecurityPolicy-TLS13-1-2-Res-2021-06 to prevent the use of ciphers that provide weak encryption on hosted systems.
- Falco:

UPDATED TO	CESA/GITHUB REFERENCE
Helm Chart 4.8.3	CVE-2022-48303 CVE-2024-6104 CVE-2022-48174 CVE-2022-28391 CVE-2023-46129 CVE-2023-39325 CVE-2023-42366 CVE-2023-42363 CVE-2023-42364 CVE-2023-42365 CVE-2023-48795 CVE-2023-3978 GHSA-m5vv-6r4h-3vj9 GHSA-45x7-px36-x8w8

- NGINX Ingress:

UPDATED TO	CESA/GITHUB REFERENCE
Controller 1.11.2	CVE-2022-48174 CVE-2024-6197 CVE-2024-25062 CVE-2023-42366 CVE-2023-42363 CVE-2023-42364 CVE-2023-42365 CVE-2024-0853 CVE-2024-6874 CVE-2023-33460 CVE-2020-8561 CVE-2024-7264

- Frontend:

UPDATED TO	CESA/GITHUB REFERENCE
Axios v1.7.7	CVE-2024-39338 CVE-2023-45857 GHSA-8hc4-vh64-cxmj GHSA-wf5p-g6vw-rhxx
body-parser v1.20.3	GHSA-qwcr-r2fm-qrc7
express v4.21.0	GHSA-rv95-896h-c2vc GHSA-qw6h-vgh9-j6wx
follow-redirects v1.15.6/8	CVE-2023-26159 GHSA-jchw-25xp-jwwc GHSA-cxjh-pqwp-8mfp
path-to-regexp v0.1.10	GHSA-9wv6-86v2-598j
pug v3.0.3	GHSA-3965-hpx2-q597
pug-code-gen v3.0.3	GHSA-3965-hpx2-q597
send v0.19.0	GHSA-m6fv-jmcg-4jfg
serve-static v1.16.2	GHSA-cm22-4g7w-348p

ThreatQ v6 Installation

- The installation process for ThreatQ 6.4.0 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