Release Notes

Version 5.27.0

Released Date: March 12, 2024

What's New in Version 5.27.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.26.0. 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.

Upgrade Impact

The upgrade is expected to take the standard amount of time for a ThreatQ upgrade. The exact time to complete the upgrade depends on your specific environment and resources.

> ⚠ Upgrades to ThreatQ v5.19.0 or later require a minimum version of 5.13.0.

> ⚠ Customers upgrading to ThreatQ v5.19.0 or later may be prompted to enter the MariaDB root user password to apply Process and Connection Admin grants.

> ⚠ After you start the upgrade, do not cancel the installation. Doing so will leave your system in an unusable state.

Upgrading from...	Full Reindex Required	Data Migration Required	Server Reboot Required
5x (most recent version)	✗	✓	✗

New Help Center Videos

The following product videos are available in the Videos section of the ThreatQ Help Center:

- ThreatQ Data Exchange, OpenDXL - Getting Started
- ThreatQ TDR Orchestrator - Building Workflows
- ThreatQ TDR Orchestrator - Adding Actions

These videos provide step-by-step simulations of ThreatQ Data Exchange (TQX) and ThreatQ TDR Orchestrator (TQO) processes.

ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform included when you upgrade from ThreatQ v5.26.0, or earlier, to 5.27.0.

NEW/UPDATED FEATURES

Threat Library | STIX Import of Notes Objects

You can now import Notes objects from STIX 2.1 files via a TAXII feed or the STIX parser. We have also updated the Notes system object so that the Note Author field is no longer a required value and is no longer limited to a maximum of thirty-two characters.

Threat Library | STIX Import of Confidence Values

Confidence is an optional value that specifies the confidence of object creators in their data on a scale from zero to one hundred. ThreatQ now allows you to import system object Confidence values from STIX 2.1 files via a TAXII feed or the STIX parser. These values are imported as object attributes.

User Management | Deletion of Points of Contact

When you delete a user listed as a point of contact on a system object, the Are you sure? window provides links by object type to the corresponding objects. For instance, if a user is a point of contact on three event objects, a Point of Contact on Event Objects link allows you to access a list of these events in the Threat Library.

Threat Library | Files List

We made the following changes to the Threat Library display of Files objects:

- Updated the list format to be more consistent with the standard Threat Library format including rows that alternate lighter and darker backgrounds.
- For dark mode, added a lighter outline to the preview file icon for improved visibility.
- Added the Manage Columns button which allows you to select the columns displayed in the file list.

> These changes also change the default columns included in CSV exports of file objects. If you rely on certain default columns in your file export, you may need to update the process ingesting the CSV files.

Job Management | Job Archiving Updates

To reduce disk space usage associated with some bulk updates, we made the following changes to the handling of job data:

- Removed system versioning from the jobs table.
- Created the new `jobs_archive` table to store archived jobs.
- Resolved an issue where payload column data was also stored in the stats column.
- Introduced a new artisan command to manage database table optimizations.

NOTABLE BUG FIXES

- When you executed the `/api/reports/events/adversary-spearphish-monthly` GET request, the system returned an empty array even if the environment had existing spearphish events.
- When a URL was normalized through the consume API endpoint, the returned data specified the type as URL and type_id as 11 (FQDN).
- In the relationship panes within the object details page, source column titles for lengthy source names overlapped the Linked By column title. Now, source name column titles are truncated based on the current width of the column.
- When you performed a bulk update of system objects filtered by TLP and clicked the corresponding job entry in the Job Management page, ThreatQ displayed a blank page instead of the job details. We resolved this issue by expanding the job details view for Delete, Update, and Relationship jobs to include a Global filters section in the Search Criteria column if the job includes system objects filtered by TLP.
- The help text for the artisan command used to export custom objects indicated that the object definitions were exported to the console or a JSON file. We updated the help text to explain that the object definitions are exported to the console or the tq_object_configuration.tgz archive file.
- When you performed a bulk update of system objects filtered by a tag that included a quotation mark ("), the bulk job completed but did not update any of the objects included in the Threat Library search results.
- When a ThreatQ instance's system timezone was set to a value other than UTC, some Threat Library timestamps reflected the system timezone and others reflected UTC. We made the following changes to resolve this issue:
  - ThreatQ displays times in the system timezone.
  - ThreatQ displays the timezone abbreviation associated with a timestamp. The full timezone is displayed in a hover tooltip in the following format: Country/Major City, Timezone Abbreviation, (UTC+/-hh:mm)
- When you updated indicator scoring, ThreatQ did not update the corresponding object scores. In addition, ThreatQ did not apply the default scores for ingested indicators.
- In some instances, when you clicked the link for a Report, Intrusion Set, Compromised Account, Assets, Malware, or TTP in the Watchlist widget, the object's Threat Library object details page was not displayed.
- An upgrade from ThreatQ v5.24.1 to v5.26.0 failed during the API migration due to an issue with a previous update to the query used pull attributes for display in table widgets. To resolve

this issue, we updated the process for migrating attributes displayed in table, pie, and bar widgets.

ThreatQ TDR Orchestrator (TQO)

The following is a bug fix for the ThreatQ TDR Orchestrator included when you upgrade from ThreatQ v5.26.0, or earlier, to 5.27.0.

NOTABLE BUG FIXES

- TQO workflows did not apply the indicator type filter included in a workflow's data collection.

Security and System Updates

The following System and Security updates have been made:

- Removed the Memcache health check.

  Python Package:

-

UPDATED TO	CESA REF
Aiohttp 3.9.1	CVE-2024-23829 CVE-2024-23334
Cryptography 41.07	CVE-2024-26130 CVE-2024-0727 CVE-2024-50782
Jinja2 3.1.2	CVE-2024-22195

- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF
LibRaw 0.19.4	CVE-2021-32142

Install Notes

- To upgrade from a 4x version to versions 5.6 through 5.18, you must be on the most recent 4x release. To upgrade to 5.19 or later, you must first upgrade to release 5.13 or later.
- For the upgrade from the most recent 4x release to versions 5.6 through 5.18, you will need to enter your MariaDB root password during the upgrade process. To upgrade from 5.13 or later to 5.19 or later, you may need to enter your MariaDB root password during the upgrade process.
- The following warning will be displayed during the upgrade process:

  ```
  Warning: RPMD altered outside of yum.
  **Found 5 pre-existing rpmdb problem(s), ‘yum’ check output follows
  ```

  This warning does not require any action on your part and will be resolved during the upgrade.
- Do not restart your instance during the upgrade process.

> We highly recommend that you perform a backup of your ThreatQ instance before upgrading.

How to Upgrade

Platform Check

ThreatQ version 5x 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, do not 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