THREATQUOTIENT

Release Notes

Version 5.29.0

Released Date: April 16, 2024

What's New in Version 5.29.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.29.0. 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)	✗	✓	✗

ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform included when you upgrade from ThreatQ v5.28.0, or earlier, to 5.29.0.

NEW/UPDATED FEATURES

Indicator Parser | Normalization of URL Query Strings

When parsing for indicators, the extraction of URL query strings as attributes during the normalization process can result in large numbers of attributes per indicator. To address this issue, we changed the default handling of these query strings when normalization is enabled.

Upon upgrade to ThreatQ v5.29, when normalization is enabled, URL query strings are not extracted as attributes and are instead discarded.

If you need to change the default normalization process, contact ThreatQuotient Support for assistance.

Threat Library | STIX Export of Notes Objects

ThreatQ now supports STIX exports for Notes objects.

Threat Library | Import of Incident Objects from STIX 2.1

ThreatQ now supports the import of Incident objects in STIX 2.1 format.

Exports | Attribute Sources and Updated At Timestamps

You now have the option to include the following attribute details in system object exports:

- Attribute source
- Attribute Updated At timestamp

These options are available for selection from the Insert Variable dropdown list in the Output Format window.

> Any TLP filters specified for the export apply to the attribute source’s TLP label as well as the system object source’s TLP label.

Threat Library Menu

We redesigned the Threat Library menu to improve usability and prepare for future additions of seeded system object types. As a result, the Data Controls section of the menu is now listed on the right instead of the bottom.

NEW KNOWN ISSUES

After upgrading to this release, if scheduled feeds do not run as expected, execute the following command:

```
docker restart threatq-dynamo
```

After this command completes, contact ThreatQuotient Support to report the issue. We are working toward resolution of this issue in a future release.

NOTABLE BUG FIXES

- In some instances, the ThreatQ Ace operation did not parse all the information expected from a PDF. We updated the `ace-indicators` filter used by the ThreatQ Ace operation and ThreatQ Ace action to parse URLs with longer subdomains and to include .med TLDs from URLs, domains, and emails.
- You were able to create a duplicate signature object by copying an ingested signature's details and using the Add Signatures page to manually create another signature object using the ingested signature's details.
- When you attempted to change an event object's type via the `PUT api/events/{id}?with=attributes,sources` endpoint, you received a 500 error. However, you were able to make the change when you removed the URL parameters.
- Source selection fields displayed a blank source as the first option in the list of sources.
- The right-click options for the Threat Library, Data Exchange, and Integrations menus include the Open Link in New Tab and Open Link in New Window options. However, when you selected these options, the resulting new tab or window displayed the ThreatQ overview page. Now, when you select these options, the following page is displayed in a new tab or window:
  - Threat Library menu - Threat Library page with focus on Adversaries
  - Data Exchange menu:
    - TAXII Server is set up - TAXII Users and Collections page
    - OpenDXL is set up - OpenDXL Connections page
    - TAXII Server and OpenDXL are set up - The Open Link in New Tab and Open Link in New Window options are not available.
    - Neither TAXII Server nor OpenDXL is set up - The Open Link in New Tab and Open Link in New Window options are not available.
  - Integrations menu - My Integrations page
- The ThreatQ login page did not display an error message when your session was logged out due to inactivity.

ThreatQ Data Exchange (TQX)

The following is a new feature for the ThreatQ Data Exchange included when you upgrade from ThreatQ v5.28.0, or earlier, to 5.29.0.

NEW/UPDATED FEATURES

TAXII Data Collections | Notes Objects

STIX files generated from TAXII data collections now include Notes objects.

Security and System Updates

The following Security update has been made:

- Pynoceros

UPDATED TO	CESA REF
MongoDB 7.0.5	CVE-2022-29162 CVE-2023-27561 CVE-2023-28642 CVE-2024-21626 CVE-2023-25809

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.

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