THREATQUOTIENT

Release Notes

Version 5.29.4

Released Date: August 13, 2024

What's New in Version 5.29.4

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.29.4. 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.

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

ThreatQ Platform (TQ)

The following is a list of bug fixes for the ThreatQ platform.

NOTABLE BUG FIXES

- Exports that included attribute_sources returned an out-of-memory error and did not complete.
- The timezone schema migration failed when a ThreatQ instance included disabled custom objects. To resolve this, we updated the backup process to identify any disabled object definitions and prompt you to delete the objects or contact ThreatQuotient Support for assistance.

Security and System Updates

The following Security updates have been made:

- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF
Apache Tika 2.9.2.1	CVE-2024-20918 CVE-2024-20919 CVE-2024-20921 CVE-2024-20932 CVE-2024-20945 CVE-2024-20952
bind 9.11.4	CVE-2023-50387 CVE-2023-4408 CVE-2023-50868
glibc 2.17	CVE-2024-33599 CVE-2024-2961 CVE-2024-33601 CVE-2024-33600 CVE-2024-33602
grub2 2.02	CVE-2022-2601
less 458-9	CVE-2024-32487
Python 2.7.5	CVE-2023-24329

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

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

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