Release Notes

Version 5.29.3

Released Date: July 03, 2024

What's New in Version 5.29.3

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.29.3. 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 bug fix for the ThreatQ platform.

NOTABLE BUG FIXES

- When you enabled the Bypass Proxy option for an operation, the operation did not function correctly in some cases. As such, if your operation needed to reach resources in your intranet that required bypassing a configured proxy, the operations could not reach them. Additionally, operations which were not able to access the Internet at startup could not download any additional required dependencies.
  We resolved this by updating ThreatQ to allow operations to bypass proxies and allow for the usage of a dependency archive when the network the operation must execute in is isolated from the internet.

ThreatQ Data Exchange (TQX)

The following is a bug fix for ThreatQ Data Exchange.

NOTABLE BUG FIXES

- When you restored your ThreatQ instance from a backup, ThreatQ returned opendxlbroker SSL errors. This occurred because the prior folder contents of `/opt/threatq/containers/opendxlbroker/` were not backed up or restored.
  We modified the backup process so that:
  - For ThreatQ Data Exchange publishers, the backup process backs up the `opendlxbroker` directory.
  - When a backup file from a ThreatQ Data Exchange publisher is restored on a different instance, the restore process restores the `opendxlbroker` directory including its SSL information.

Security and System Updates

The following Security update has been made:

- Modified the user image upload endpoint to prevent remote code execution (RCE).

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