Release Notes

Version 5.8.0

Released Date: December 01, 2022

What's New in Version 5.8.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.8.0. 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.

> ⚠ 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	✗	✓	✗
4x	✓	✓	✓

ThreatQ Platform (TQ)

The following is a list of new features, bug fixes, and new identified issues for the ThreatQ platform.

NEW/UPDATED FEATURES

Indicator Parsing | New Defanging Technique

The Indicator Parser now supports the `http[://]` defanging technique. This technique allows you to import URLs with this prefix, such as `http[://]example.com`.

Threat Library | Relationship Criteria Filter Options

The Relationship Criteria filter has the following new Additional Criteria options:

- Source - Allows you to filter your results based on one or more sources. In addition, you can specify that an object must meet all or at least one of your Source criteria.
- Date Created - Allows you to narrow your results based on the date a related object was created. This filter allows you to specify creation before or after a date, within a date range, or within a specific number of preceding days.

NOTABLE BUG FIXES

- We updated SAML authentication to ensure that the user email address is populated during ThreatQ user account creation.
- The Indicator Parser did not recognize defanged indicators that used the `hxxp[:]//` defanging technique.
- When you use TQAdmin to upgrade to or install a 5x release, you are prompted to confirm the action. When you entered “no” at the Do you wish to continue prompt, the system returned an upgrade/install completed message even though you had exited the process.
- After you manually updated an indicator, the Splunk differential export returned an empty data response instead of listing the updated indicator.

- When an integration YAML file used the `multiple: False` configuration to specify a dropdown field, the integration's configuration screen displayed checkboxes instead of the dropdown field.
- When you created a dashboard with a Line Graph widget and selected Expiration Date as the date type option, the dashboard display was blank and a console error was generated.
- When you ran an operation on an indicator from the object preview window and clicked the Add Selected Attributes button, the attributes were not added to the indicator.
- The Edit Sources window displayed TLP fields even when TLP functionality was disabled.
- Images in an object's description were not displayed in the PDF report for the object.
- When you attempted to update scoring algorithms, the system returned stack trace errors in dynamo logs.
- Events ingested via the Cofense CDF included brackets in event names.
- When you changed a radio button selection in a custom connector's configuration page, the newly selected button was not updated to reflect your selection.
- The object details page did not display a score summary when you clicked the info button next to the system object's score.
- When you set a system object's expiration to Protect from auto expiration, the object's Expiration Date field was not updated to display Never Expire.

ThreatQ Orchestrator (TQO)

The following is a list of new features, bug fixes, and new identified issues for ThreatQ Orchestrator.

NEW/UPDATED FEATURES

Actions | Display of Accepted Data Types

The new Accepted Data Types section in the workflow-level Action configuration panel and default Action configuration page displays the indicators supported by an action.

Install Notes

- To upgrade from a 4x version to 5x, you must be on the most recent 4x release.
- For the upgrade from the most recent 4x release to 5x, you will need to enter your MySQL 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

The TQAdmin tool used for platform checks and upgrades requires elevated privileges and must be run as root.

To elevate to root, run the following command:

```
# sudo su -
```

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:

```
# tqadmin platform check
```

Run a platform check for a specific version:

```
# tqadmin platform check -v <version number>
```

Upgrade Commands

To upgrade, run the following command:

```
# tqadmin platform upgrade
```

To upgrade to a specific version, run the following command:

```
# 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