



Release Notes

Version 5.12.1

Released Date: March 14, 2023


What's New in Version 5.12.1


The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.12.1. 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.

 Customers upgrading from a prior 5x release to 5.12.1 will be prompted to enter their MySQL root password during the upgrade process to allow an adjustment of the subnet mask of the Solr MySQL user's host.

 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			

 If you are upgrading to this release from 5.6 or earlier, a full reindex is required.

ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform available when you upgrade from ThreatQ v5.12.0, or earlier, to 5.12.1.

NOTABLE BUG FIXES

- We improved performance to address an issue which could cause timeouts when ingesting a large amount of attribute updates from Configuration Driven Feeds (CDFs).
- When you created a dashboard with a Table widget, the Sort By option did not work.
- We resolved the following Dark Mode issues by updating these pages to reflect standard Dark Mode colors:
 - When you accessed the Signature Parser, the text next to the Next Step button was displayed in a dark font on a dark background. In addition, when you clicked the Next Step button, the text in the Results window was also displayed in a dark font on a dark background.
 - When you accessed the Proxy tab in the System Configurations page, the text was displayed in a light font on a light background.
 - When you used a Windows machine to access the Add Event window, the drop-down list for the Type field displayed a light font on a light background.
- We resolved the following Dashboard Table widget issues:
 - The table body font size was not consistent with ThreatQ standards.
 - The Related Adversary Names column displayed commas instead of adversary names.
- The integration details page did not display Helper text for Operations.
- We resolved the following Indicator Parser issues:
 - When you unchecked the options to normalize URL indicators, URLs that contained ampersands (&) were highlighted.
 - When you unchecked the options to normalize URL indicators and parse FQDNs, URLs with query parameters that contained a plus sign (+) were not parsed as URLs.
 - The parser did not remove the brackets from [.com] in order to defang it as .com.

- When you clicked the Load Data Collection option in the Threat Library and an existing data collection was associated with a TQO workflow, the Used by section displayed the workflow ID instead of the workflow name.
- The Source Ingest Time filter did not return correct results when you selected the Not option. For instance, if you created a Source Ingest Time filter to return indicators from Source A within the last day and checked the Not option, your results included indicators from Source A that were ingested an hour prior.
- During some ThreatQ OVA installs, the pynoceros-messenger container was created but the tqdx, rabbitmq, websocket, or memcached containers were not restarted.

ThreatQ TDR Orchestrator (TQO)

The following is a list of new features and bug fixes for ThreatQ TDR Orchestrator available when you upgrade from ThreatQ v5.12.0, or earlier, to 5.12.1.

NOTABLE BUG FIXES

- We improved performance to address an issue which could cause timeouts when ingesting a large amount of attribute updates from TQO Advanced Workflows.
- In Dark mode, when you clicked the View in Threat Library button from the data collection details panel, the Threat Library was displayed in Light mode.
- The audit log entry for a system object updated by a workflow listed the author's unique identifier instead of its name.
- The Timeline Entry window displayed 00 in the Author field.


ThreatQ Investigations (TQI)

The following is a list of new features and bug fixes for ThreatQ Investigations available when you upgrade from ThreatQ v5.12.0, or earlier, to 5.12.1.

NOTABLE BUG FIXES

- When you accessed an investigation in Light Mode and clicked a timeline entry, the Timeline Entry window was displayed in Dark Mode.
- When you accessed an investigation in Dark or Split Mode and accessed the Operations window to run an operation on an object, the object name was displayed in a dark font on a dark background. We updated the font color to improve readability and changed the window name from Operations to Run Operations For.
- When you clicked a timeline entry, the details popover displayed above the timeline instead of above the timeline entry.

Security and System Updates

 After upgrading to 5.11.0 or later, you can no longer use root to log in via SSH. You must create an alternate non-root OS/Linux user with sudo privileges (wheel group) to access the platform via SSH. Root access is still available via the hypervisor console.

The following Security updates have been made:

- Modified the ThreatQ user interface to prevent the execution of script tags injected in intercepted API responses for the Disclaimer Acceptance Title and Banner.
- Updated the version of git stored in the ThreatQuotient updates repository to 1.8.3.1.

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.
- Customers upgrading from a prior 5x release to 5.12.1 will be prompted to enter their MySQL root password during the upgrade process to allow an adjustment of the subnet mask of the Solr MySQL user's host.
- 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