



Release Notes

Version 5.13.0

Released Date: April 06, 2023


What's New in Version 5.13.0


The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.13.0. 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.

 Customers upgrading from a 5x release prior 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 Help Center

NEW/UPDATED FEATURES

Updated Best Practices

We updated the Best Practices guidelines with new recommendations for maximizing your use of our products and services. These updates cover new product options, such as the Data Retention Policy, as well as feedback from customer experiences.


ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform available when you upgrade from ThreatQ v5.12.1, or earlier, to 5.13.0.

NEW/UPDATED FEATURES

Data Controls | Data Retention Policy

The new Data Retention Policy tab in the Data Controls page allows you to configure a daily bulk delete process based on the criteria defined within a Data Collection. For example, you can create a Data Retention Policy based on a Data Collection that captures Indicators that expired within the last 7 days. Once you enable this policy, ThreatQ performs an initial bulk delete of the Indicators that meet this criteria and then performs daily bulk deletes. See the Data Retention Policy section of the Help Center for more information on creating and managing your data retention policy.

 We recommend that you perform a backup of your ThreatQ instance before implementing a Data Retention Policy.

Threat Library | Remove an Object's Source

You can now remove an object's source as well as the source's attributes, comments, and relationship links from the Sources pane in the object details page. You can delete a source by clicking the Edit option to access the Edit Sources window or by clicking the X to the right of the source's name. See the Sources Pane section of the Help Center for more information.

Job Management | Redesign and Enhancements

To improve usability, we made the following changes to the Job Management page:

- Added an option to allow you to expand and view job details. You can click any location on a row to expand/collapse job details.

- Changed the Actions column name to Job Type.
- Updated the default column order to:
 - Job ID
 - Job Type
 - Author
 - Date Created
 - Total Objects
 - Status
 - Percent Completed
- The Percent Completed column now displays three indications of the job's progress:
 - A progress bar with the overall percentage completed.
 - A count of the number of objects that have been processed from the total number of objects (e.g., 300 of 3,400).
 - The estimated time remaining.
- Added color-coded fonts and backgrounds to Status indicators. For example, the status of completed job is displayed as **Completed**.
- Replaced the Refresh Page button with a refresh icon button.
- Added job type tabs that allow you to filter your view by job type such as Delete, Update, Relationship, or Retention Policy. Your view defaults to the All tab which lists all job types.

See the Job Management section of the Help Center for more information on these changes.

Threat Library | Caching

Caching is now enabled by default for Threat Library queries.

Resizing Description Fields

You now have the option to click and drag the right corners of Description fields to resize them while entering data.

Dashboard Performance

We enhanced Dashboard performance by adding sort parameters (when applicable) to Table widget cache keys.

Threat Library | Object Counts

The new `/api/threatlibrary/objects/counts/{hash?}` endpoint retrieves a count of threat objects per definition in a single query. ThreatQ now uses this endpoint to optimize search queries to retrieve object details for the selected/active object type and retrieve only object counts for all other object types.

Threat Library | Data Collection Updates

We modified the handling of changes to Data Collections that use Relationship Criteria filters which include additional Value Contains criteria. Previously, when you added, removed, or updated a custom object, every Data Collection that used this type of filter had to be manually updated to include/remove the custom object type from the `api_query` payload. Now, the Data Collection is updated the next time the system runs it.

NOTABLE BUG FIXES

- When you made changes to a related object in the preview panel, the corresponding related object information displayed in the object details page was not updated until you reloaded the page.
- We improved dashboard performance by updating the handling of Threat Library queries.
- We resolved the following cosmetic issues within the Attribute Management tab:
 - Table rows did not have top and bottom borders.
 - The search icon was located outside of the Search field.
 - The Search field name was displayed in bold.
 - Selected rows were not highlighted with a background color.
- We updated the Light mode display of the following Table widget elements to support ThreatQ standards:

- Table header row background color.
- Gear, delete, and drag icons' standard and hover colors.
- We updated the Dark mode display of the background and text colors for Operation fields to support ThreatQ standards.
- When you loaded a Data Collection that included a date filter, it displayed a date one day prior to your original selection. For instance, when you accessed a Data Collection created with an Expiration Date of February 28th 2023, it listed an expiration date of February 27th 2023.
- When you accessed a Data Collection's information window and hovered over the pencil (edit) icon next to its name, the icon moved slightly to the right.
- The Attribute Management tab in the Object Management page did not list source values for attributes.

ThreatQ Data Exchange (TOX)

The following is a list of new features and bug fixes for ThreatQ Data Exchange available when you upgrade from ThreatQ v5.12.1, or earlier, to 5.13.0.

NOTABLE BUG FIXES

- In Dark mode, node names in the Topology View were displayed in a dark font on a dark background.

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:

- Updated moment-timezone to version 0.5.34.
- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF	
Docker Engine 20.10.21	CVE-2019-14271	CVE-2022-2879
	CVE-2021-21284	CVE-2022-2880
	CVE-2021-21334	CVE-2022-29162
	CVE-2021-30465	CVE-2022-29526
	CVE-2021-36221	CVE-2022-29804
	CVE-2021-39293	CVE-2022-30580
	CVE-2021-41089	CVE-2022-30629
	CVE-2021-41091	CVE-2022-30634
	CVE-2021-41092	CVE-2022-31030
	CVE-2021-41103	CVE-2022-32190
	CVE-2021-41190	CVE-2022-36109
	CVE-2021-44228	CVE-2022-39253
	CVE-2022-24769	CVE-2022-41715
	CVE-2022-27664	
Linux Kernel 3.10.0	CVE-2022-42703	
	CVE-2022-4378	
OpenSSL 1.0.2k	CVE-2023-0286	

NSS 3.79.0

CVE-2023-0767

Zlib 1.2.7

CVE-2022-37434

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 5x release prior 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