THREATQUOTIENT

Release Notes

Version 5.24.1

Released Date: January 09, 2024

What's New in Version 5.24.1

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 5.24.1. 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.

> ⚠ Upgrades to ThreatQ v5.19.0 or later require a minimum version of 5.13.0.

> ⚠ Customers upgrading to ThreatQ v5.19.0 or later may be prompted to enter the MariaDB root user password to apply Process and Connection Admin grants.

> ⚠ 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 (most recent version)	✖	✖	✖

ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform included when you upgrade from ThreatQ v5.24.0, or earlier, to 5.24.1.

NEW/UPDATED FEATURES

Object Preview | Display of Multiple Descriptions

The object preview pane now displays an object’s descriptions in card format. You can use the arrows above the top right corner of a card to scroll through the object’s descriptions and click the Show More/Show Less option to expand or collapse the description view. When a description is expanded, you can click the Edit option in the Descriptions pane header to update it.

Integrations | Status Updates

We updated the ingestion process to apply different status update processes for CDFs and Workflows. Workflows do not override default statuses. CDFs override indicator statuses to the default status defined in the CDF and override signature statuses to a default value of Active.

HMAC Authentication Output Type Parameter

ThreatQ’s HMAC authentication now includes an optional parameter, `output_type`. This parameter defaults to `hexadecimal`, which will return a `hexdigest` (hexadecimal string). You can change this value to `base64` in order to get a base64 representation of the output digest.

Threat Library | Comment Options Display

We made the following changes to the display of the Show More/Show Less options for comments in the object details and object preview pages:

- Moved the Show More/Show Less options to display above the Edit and Delete options
- Increased the vertical space between the Show More/Show Less options and the Edit and Delete options to 6px.
- Removed the underlining from the Show More/Show Less options.

Integrations | Display of Accepted Data Types for Actions

If a TQO action’s YAML file does not specify accepted data types, the integration details page for the action does not display the Accepted Data Types field.

NOTABLE BUG FIXES

- In the Threat Library, when you created a relationship criteria filter that applied to any object, specified a creation date, and then added a Source filter, the Threat Library did not return any results even though it contained objects that met the filter criteria.
- When you viewed a spearphish event in dark mode, the Email Content field in the Spearphish Details section was displayed in light mode.
- If the ThreatQ users table contained user records that were not soft-deleted and did not have a related sources table row, you could not not share dashboard access because the Search by name field in the Sharing window disabled text input after two characters.
- When you used the Indicator Parser option, URLs with query parameters were parsed as FQDNs.
- In dark mode, the Indicator Expiration panel in the Data Controls page was displayed with a gray background.
- Customers were unable to generate STIX exports that included identity or intrusion objects that had multiple attributes with the same name.
- When you set a new status for a CDF, your change did not apply until the one-day cache elapsed. We changed the CDF update process to clear the CDF cache after you save a change to the CDF’s status field.

ThreatQ Investigations (TQI)

The following is a bug fix for ThreatQ Investigations included when you upgrade from ThreatQ v5.24.0, or earlier, to 5.24.1.

NEW/UPDATED FEATURES

Comment Options Display

We made the following changes to the display of the Show More/Show Less options for comments in investigations:

- Moved the Show More/Show Less options to display above the Edit and Delete options
- Increased the vertical space between the Show More/Show Less options and the Edit and Delete options to 6px.
- Removed the underlining from the Show More/Show Less options.

ThreatQ Data Exchange (TQX)

The following is a list of new features for the ThreatQ Data Exchange included when you upgrade from ThreatQ v5.24.0, or earlier, to 5.24.1.

NEW/UPDATED FEATURES

User Access Display

We updated the TAXII Users & Collections page to only display the username table when at least one user exists. In addition, the Edit TAXII Collection page only displays the username table when at least one user has been given access to the TAXII collection. We also updated these pages to return the following message when you enter a user search that does not return a match:

```
No results for “name”. Click Create User below to add a new TAXII User.
```

Security and System Updates

The following Security updates have been made:

- To prevent privilege escalation through API SAML configuration by a user with Primary Contributor permissions, we modified the SAML configuration endpoints to deny access to all but Maintenance and Admin users.
- To increase the security of API client secret information, we removed `client_secret` information from the data returned by GET requests to the following endpoints:
  `/gate/clients{?limit,offset,sort,with}`
  `/gate/clients/{client_id}{?with}`
- Remote CentOS Linux 7 host:

UPDATED TO	CESA REF			
Apache Tika 2.9.1.0	CVE-2022-3715	CVE-2016-20013	CVE-2017-11164	CVE-2023-21954
	CVE-2016-2781	CVE-2023-4806	CVE-2022-3857	CVE-2023-21967
	CVE-2022-27943	CVE-2023-4813	CVE-2023-4016	CVE-2023-21968
	CVE-2022-3219	CVE-2023-2603	CVE-2023-7104	CVE-2023-22006
	CVE-2023-1981	CVE-2023-2602	CVE-2022-46908	CVE-2023-22025
	CVE-2023-38469	CVE-2023-32324	CVE-2023-2650	CVE-2023-22036
	CVE-2023-38470	CVE-2023-32360	CVE-2023-5363	CVE-2023-22041
	CVE-2023-38471	CVE-2023-34241	CVE-2022-3996	CVE-2023-22044
	CVE-2023-38472	CVE-2023-4504	CVE-2023-0464	CVE-2023-22045
	CVE-2023-38473	CVE-2023-34969	CVE-2023-0465	CVE-2023-22049
	CVE-2023-1981	CVE-2022-27943	CVE-2023-0466	CVE-2023-22081
	CVE-2023-38469	CVE-2023-29499	CVE-2023-1255	CVE-2023-25193
	CVE-2023-38470	CVE-2023-32611	CVE-2023-2975	CVE-2023-2650
	CVE-2023-38471	CVE-2023-32636	CVE-2023-3446	CVE-2023-5363
	CVE-2023-38472	CVE-2023-32643	CVE-2023-3817	CVE-2023-1255
	CVE-2023-38473	CVE-2023-32665	CVE-2022-27943	CVE-2023-2975
	CVE-2023-1981	CVE-2023-5981	CVE-2023-29491	CVE-2023-3446
	CVE-2023-38469	CVE-2023-36054	CVE-2022-29458	CVE-2023-3817
	CVE-2023-38470	CVE-2023-25193	CVE-2022-4899	CVE-2023-29383
	CVE-2023-38471	CVE-2023-36054	CVE-2023-29383	CVE-2023-31484
	CVE-2023-38472	CVE-2023-36054	CVE-2023-29491	CVE-2023-47038
	CVE-2023-38473	CVE-2023-36054	CVE-2022-29458	CVE-2022-48522
	CVE-2023-4911	CVE-2020-22916	CVE-2023-29491	CVE-2023-4016
	CVE-2023-5156	CVE-2023-29491	CVE-2022-29458	CVE-2023-39804
	CVE-2016-20013	CVE-2022-29458	CVE-2023-21930	CVE-2023-2976
	CVE-2023-4806	CVE-2023-29491	CVE-2023-21937	CVE-2020-8908
	CVE-2023-4813	CVE-2022-29458	CVE-2023-21938	CVE-2023-42503
		CVE-2023-5388	CVE-2023-21939	CVE-2023-40167

UPDATED TO	CESA REF			
	CVE-2023-4911			
	CVE-2023-5156			
Apache Zookeeper 3.9.1	CVE-2022-3715	CVE-2016-20013	CVE-2023-4016	CVE-2022-29458
	CVE-2016-2781	CVE-2023-4806	CVE-2023-7104	CVE-2023-29491
	CVE-2023-38545	CVE-2023-4813	CVE-2022-46908	CVE-2022-29458
	CVE-2023-46218	CVE-2023-2603	CVE-2023-1667	CVE-2023-5363
	CVE-2023-28321	CVE-2023-2602	CVE-2023-2283	CVE-2023-2975
	CVE-2023-28322	CVE-2023-38545	CVE-2023-48795	CVE-2023-3446
	CVE-2023-38546	CVE-2023-46218	CVE-2023-6004	CVE-2023-3817
	CVE-2022-3219	CVE-2023-28321	CVE-2023-6918	CVE-2023-29383
	CVE-2022-27943	CVE-2023-28322	CVE-2023-2650	CVE-2023-31484
	CVE-2022-3219	CVE-2023-38546	CVE-2023-5363	CVE-2023-47038
	CVE-2022-3219	CVE-2022-27943	CVE-2023-1255	CVE-2022-48522
	CVE-2022-3219	CVE-2023-5981	CVE-2023-2975	CVE-2023-4016
	CVE-2022-3219	CVE-2023-36054	CVE-2023-3446	CVE-2023-39804
	CVE-2022-3219	CVE-2023-36054	CVE-2023-3817	CVE-2021-31879
	CVE-2022-3219	CVE-2023-36054	CVE-2022-27943	CVE-2023-6378
	CVE-2022-3219	CVE-2023-36054	CVE-2023-29491	CVE-2023-6378
	CVE-2022-3219	CVE-2023-2953	CVE-2022-29458	CVE-2023-34462
	CVE-2022-3219	CVE-2020-22916	CVE-2022-4899	CVE-2023-44981
	CVE-2022-3219	CVE-2023-29491	CVE-2023-4911	CVE-2023-40167
	CVE-2023-4911	CVE-2022-29458	CVE-2023-5156	CVE-2023-26048
	CVE-2023-5156	CVE-2023-29491	CVE-2016-20013	CVE-2023-26049
	CVE-2016-20013	CVE-2022-29458	CVE-2023-4806	CVE-2023-34455
	CVE-2023-4806	CVE-2023-44487	CVE-2023-4813	CVE-2023-43642
	CVE-2023-4813	CVE-2017-11164	CVE-2023-29383	CVE-2023-34453
	CVE-2023-4911	CVE-2022-3857	CVE-2023-29491	CVE-2023-34454
	CVE-2023-5156			
Curl 7.29.0	CVE-2022-43552			

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

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