



Release Notes

Version 6.18.0

Released Date: May 04, 2026

What's New in Version 6.18.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.18.0. Below is a list of enhancements, important bugs that have been addressed, and upgrade instructions.

ThreatQ Platform

The following is a list of new features and bug fixes for the ThreatQ platform included when you upgrade to 6.18.0.

NEW/UPDATED FEATURES

Threat Research Agent

The Threat Research Agent is an AI-powered capability within the ThreatQ platform that enables analysts to interact with threat intelligence using natural language. It enhances analysis by combining a customer-configured large language model (LLM) with ThreatQ data and operations to deliver contextual insights, automate enrichment, and support investigative workflows.

The agent allows users to query the Threat Library, retrieve object details, and execute enrichment actions through integrated tools, reducing manual effort and accelerating decision-making. It can also perform multi-step workflows and generate structured outputs, including reports, based on user interactions.

Users can access the Threat Research Agent through the agent chat interface within the platform or directly from an object's details page using the Insights option, which launches context-aware queries.

Key features include:

- Natural language querying of ThreatQ data.
- Integration with customer-provided LLMs (OpenAI, Anthropic, Gemini, or Ollama).
- Automated enrichment using ThreatQ operations as tools.
- Context-aware insights from object-level access.
- Support for multi-step, agent-driven workflows.
- Report generation from chat interactions.
- Secure, role-based access with controlled data sharing.

See the Threat Research Agent section on the ThreatQ Help Center for more information.



Installation/Upgrades | Certificate Validation

A pre-deployment validation has been added to ensure that any user-specified certificate and key files are present. This enhancement introduces checks during the Terraform plan phase to detect missing files early and halt execution with a clear error message, preventing partial upgrades and failures during services configuration (such as NGINX) caused by absent or removed certificates.

NOTABLE BUG FIXES

The following list of issues and bugs that have been resolved with ThreatQ v6.18.0.

- Resolved an issue where the backup and restore process did not include files from `/var/www/api/public/assets/branding/default`, resulting in the loss of custom images uploaded via the Report Options screen. This caused report generation to fail in environments relying on these assets; the process now ensures branding assets are properly preserved and restored.
- Resolved an issue where the Assigned To and Reporter dropdowns in the Task Preview Panel were unresponsive.
- Resolved an issue where tasks completed through Bulk Changes were not populating the `completed_at` field, causing them to remain visible as open on the Overview Dashboard despite being marked as Done.
- Resolved an issue where the text editor cursor would intermittently reset to the beginning of the field while typing. This behavior affected multiple areas of the platform utilizing the editor component and has been corrected to ensure consistent and reliable text input across all instances.
- Resolved an issue where the ThreatQ installer could overwrite existing system packages with outdated bundled RPMs, resulting in unintended package downgrades. The installer logic has been updated to ensure that dependencies are installed only when missing or out of date, preventing newer system packages from being replaced and aligning installed versions with the host operating system.

Security and System Updates

The following updates have been made with ThreatQ v6.18.0:


RHEL	PACKAGE	UPDATED TO
8	rsync	3.1.3-19.el8_7.1.x86_64



RHEL	PACKAGE	UPDATED TO
8	zstd	1.4.4-1.el.x86_64
8	tmux	2.7-3.el8.x86_64
8	libsemanage	2.9-9.el8_6.x86_64
8	Python3-libsemanage	2.9-9.el8_6.x86_64
8	libzstd	1.4.4-1.el8.x86_64
9	rsync	3.2.3-19.el9.x86_64
9	libzstd	1.5.1-2.el9.x86_64
9	zstd	1.5.1-2.el9.x86_64
9	tmux	3.2a-5.el9.x86_64

Upgrading

Perform the following steps to upgrade your ThreatQ v6 instance.

 After you start the upgrade, do not cancel the installation. Doing so will leave your system in an unusable state.

1. Perform a platform check to ensure adequate disk space and that your installed integrations are compatible with the new ThreatQ version. You will be unable to proceed with the upgrade until clearing this check. It is important to note that the command does not apply to integrations installed on third-party systems such as the ThreatQ App for QRadar.

Platform Check Against the Most Recent ThreatQ Version

```
# sudo /usr/local/bin/tqadmin platform check
```

Platform Check Against a Specific ThreatQ Version

```
# sudo /usr/local/bin/tqadmin platform check -v <version number>
```

2. Run the upgrade command:

Upgrade to the Latest ThreatQ Version

```
# sudo /usr/local/bin/tqadmin platform upgrade
```

Upgrade to a Specific ThreatQ Version

```
# sudo /usr/local/bin/tqadmin platform upgrade -v <version number>
```

New Installations


If you are installing ThreatQ version 6 for the first time, it is highly recommended that you review the ThreatQ 6x Installation section and guides before proceeding with installation. The guide provides useful information including:

- Required Firewall Ports
- Suggested Partitioning Scheme
- System Requirements (Hardware Specifications, Core CPUs, RAM etc.)
- Steps to pin your RHEL 9 and Ubuntu versions to prevent upgrades to unsupported environments
- Security Hardening Guides

Migrating ThreatQ v5 to v6

It is important that you use the correct ThreatQ version when migrating a ThreatQ v5 instance to ThreatQ v6.

- Migrating to ThreatQ v6.9.1 or greater requires a ThreatQ v5.29.5 backup file.
- Migrating to ThreatQ v6.9.0 and prior requires a ThreatQ v5.29.4 backup file.

 Using a backup other than the ones listed above will result in a restore error.

Contact ThreatQ Support or your Technical Account Manager for additional information and to obtain the ThreatQ Migration Guide. The ThreatQuotient team highly recommends that you review the ThreatQ 6x Installation guide when planning your migration.

Support

Don't hesitate to get in touch with your Technical Account Manager to discuss planning your upgrade.

As always, contact our Customer Support Team if you encounter problems when upgrading or need assistance.

Thank you,

The ThreatQuotient Team

✉ tq-support@securonix.com

🖥 ts.securonix.com

📞 703.574.9893