Release Notes

Version 6.19.0

Released Date: June 02, 2026

What's New in Version 6.19.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.19.0. 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 6.19.0.

NEW/UPDATED FEATURES

System Banner Display

The System Banner Display feature provides administrators with the ability to configure custom banner and marking displays within the ThreatQ platform. These banners can be used to clearly identify the classification, purpose, or operational role of a ThreatQ instance through configurable header and/or footer messaging.

This functionality is particularly useful for organizations operating multiple ThreatQ environments, such as development, testing, staging, or production systems, by providing users with a clear visual indicator of the environment they are currently accessing. The feature helps reduce user confusion, supports operational awareness, and promotes safer interaction across multiple platform instances.

The banner capability is designed to support a wide range of organizational, operational, and compliance-related use cases through flexible and customizable display settings.

See the System Banner Display Settings section on the ThreatQ Help Center for more information.

Threat Research Agent | Updated Terms and Conditions

The terms and conditions have been updated and added directly to the Threat Research Agent configuration page in ThreatQ. Prior to ThreatQ version 6.19.0, users were required to follow an external link to review Securonix's AI Terms and Conditions hosted on a separate site.

NOTABLE BUG FIXES

The following list of issues and bugs that have been resolved with ThreatQ v6.19.0.

- Hosted Instances - Resolved a platform stability issue where memory-intensive integrations could exhaust resources and impact an entire hosted node. Resource limits now isolate memory exhaustion to the affected Dynamo worker pod, allowing the pod to restart without affecting node availability or unrelated services.
- Hosted Instances - Resolved an issue where login attempts could fail if audit logging to OpenSearch was unavailable. Audit logging to OpenSearch no longer blocks user authentication when the logging destination is unreachable.
- Resolved an issue in the Data Retention Policy (DRP) interface where collections beyond the first 100 entries were not displayed due to a UI pagination limitation, causing affected collections to incorrectly appear as "Not Shared".
- Resolved an issue where users with Orchestration permissions but without Integration permissions encountered a `You do not have permission to view the resource` error when accessing the TQO Orchestrator interface.
- Resolved an issue in the Report Editor where repeatedly performing bulk attribute add and delete actions could trigger a UI reset, causing newly added attributes to disappear.
- Resolved an issue where TQX feeds could fail to ingest on subscriber instances due to an API Consume processing bug triggered by related report objects with custom status configurations.
- Resolved an issue where switching between dashboard tabs could trigger duplicate permissions API requests, resulting in unnecessary backend calls and reduced dashboard navigation performance.
- Resolved a dashboard performance issue where chart-based widgets retrieved unnecessary result data, causing increased API payload sizes, slower dashboard loading, and reduced UI responsiveness.
- Resolved an issue where Attachment (File) objects containing special characters in file paths could cause UUID generation and serialization failures, resulting in ingestion errors, duplicate attachments, or inconsistent object uniqueness behavior.

- Improved `api/search/query` performance by eliminating redundant RBAC permission serialization during response generation, reducing excessive backend processing and improving response times for large result sets.
- Improved dashboard performance by preventing unnecessary resource-permission resolution processing when requests include `sharingPermissions.source` without explicitly requesting `sharingPermissions.source.resource_permissions`.
- Improved Threat Library search performance by optimizing Solr query generation for large same-field equality filters, reducing slow response times and improving UI responsiveness when applying multi-value filters.
- Improved Threat Library and relationship search performance by moving eligible Solr filters from the main query into dedicated filter queries, enabling better filter-cache reuse while preserving existing search results and API behavior.
- Resolved an issue where Solr date-math expressions used in time-based filters could be incorrectly converted during query compilation, resulting in inaccurate relative date searches and inconsistent query results.
- Improved API and dashboard performance by optimizing Solr field-list generation and eliminating unnecessary automatic field expansion, reducing query overhead, response payload sizes, and backend processing time.

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 Manage 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