Release Notes

Version 6.16.0

Released Date: February 23, 2026

What's New in Version 6.16.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.16.0. 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.

Migration Impact

> The migration process for ThreatQ 6.9.1 and later releases requires a ThreatQ 5.29.5 backup file. The migration process for releases prior to ThreatQ 6.9.1 requires a ThreatQ 5.29.4 backup file. If you attempt to use a backup file from a different ThreatQ 5x release, the restore process will return an error.

If you are deploying ThreatQ 6x for the first time, the upgrade requires setting up a new Ubuntu 22.04 LTS or Red Hat Enterprise Linux (RHEL) 8.10, 9.4, or 9.6 instance, installing ThreatQ 6x in this new instance, and then restoring the data from your ThreatQ 5x instance. The exact time to complete the upgrade depends on your specific environment and resources.

Access the ThreatQ Help Center to view or download the **ThreatQ Version 6 Installation** guides. Contact our Customer Support Team or your Technical Account Manager to request the **ThreatQ Version 6 Migration** guide for detailed information on migrating to ThreatQ 6x.

Upgrade Impact

If you are upgrading from one ThreatQ 6x version to another, see the How to Upgrade section for more information on executing a platform check and upgrade.

ThreatQ Platform (TQ)

The following is a list of new features and bug fixes for the ThreatQ platform.

NEW/UPDATED FEATURES

User Management | Data Access Permissions

The new Data Access Permissions section in the Create Role and Edit Role pages allows you to set permissions by system object type (for example, Indicator, Adversary, Event, Campaign). For each object type you can assign Create, Edit, Delete, No Access, or View Access Only permission. These permissions override the Objects permission assigned to a role. For example, you can create a role with Create, Edit, Delete permissions for Objects but specify a View Only data access permission for Event objects.

User Management | LDAP/SAML Group Mapping Support

ThreatQ v6.16.0 also supports the mapping of LDAP and SAML User Groups to custom user roles. LDAP and SAML configuration pages now include permission mapping fields for all custom user roles.

Upon upgrade, ThreatQ sends a system notification to all Admin users based on the enabled authentication method:

- LDAP Authentication can now map Custom Roles to LDAP User Groups to enable authentication for users in these roles. Your existing group mappings have been migrated. Custom Roles can now be mapped using LDAP User Management.
- SAML Authentication can now map Custom Roles to SAML User Groups to enable authentication for users in these roles. Your existing group mappings have been migrated. Custom Roles can now be mapped using SAML User Management.

Role Based Access Control (RBAC) | API Updates

To ensure RBAC permissions are enforced for API requests, the following API endpoint categories are now governed by RBAC controls:

- Alerts and Notifications
- Spearphish
- Authentication and Licensing
- Reporting (Dashboards)
- Images and Files
- Object context such as the object watchlist as well as object attributes, relationships, and comments

These changes expand your ability to control the access granted to logins used for API requests.

In addition, a number of endpoints related to user groups have been removed in favor of new ones supporting RBAC functionality. See the ThreatQ REST API documentation for more details.

User Profile | Session Timeout Updates

The Edit User Management permission now controls the ability to update Session Timeout settings from your user profile. If your user role does not include the Edit User Management permission, the Session Timeout Minutes field displayed on your user profile is view-only and cannot be updated. In addition, the Disable Timeout checkbox is not displayed.

User Management | Role Assignment Error Message

We updated error messaging for the Role Assignment field in the Add User modal so that if you leave the field blank, ThreatQ returns the following error message: **The User Role field is required.**

Operations-Manager Container Change

We updated the operations-manager container to eliminate the use of the pkg_resources package. This change prevents the display of the associated deprecation warning when the operations-manager container starts.

Conditional Audit Logging Enablement

Audit logging is now automatically disabled when the audit log host is not configured. This prevents ThreatQ from attempting to send audit log records and eliminates unnecessary error messages.

NOTABLE BUG FIXES

The following platform bugs were fixed with ThreatQ version 6.16.0:

- Upon upgrading to ThreatQ v6.8, the Adversary Analytics dashboard no longer displayed the Adversary Overlap widget. We resolved this issue so that the Adversary Overlap widget is now displayed in the Adversary Analytics dashboard.
- In some instances, when you deployed a large ThreatQ instance, the redis-persisted pod ran out of disk space and returned the following error: **Errors writing to the AOF file.** To resolve this issue, we increased the redis-persisted PVC size for large deployments to ensure sufficient space for AOF persistence. .

Security and System Updates

The following update has been made:

- For hosted customers, we replaced the Falco security deployment with a Sophos connector to improve runtime threat detection and alerting coverage.

ThreatQ v6 Installation

- If you are migrating from ThreatQ v5 to ThreatQ v6, see the Migration Impact section.
- **Pinning your RHEL 9 release:**

  The following steps allow you to pin your current RHEL 9 release so that you cannot inadvertently upgrade your RHEL 9 environment to an unsupported release. See the **Red Hat Enterprise Linux 9 Support** section of the Help Center for more information on currently supported RHEL 9 versions.

  > Run the following commands as root or prefix them with sudo.

  1. Set release to minor version:
  2. subscription-manager release --set=**<release number>**
  3. Clean repositories:
  4. yum clean all
  5. Check which release is set locally:
  6. subscription-manager release --show
- **Pinning your Ubuntu release:**
  We recommend you update the release-upgrades file to disable manual Ubuntu upgrades so that you cannot inadvertently upgrade your Ubuntu 22.04 environment to an unsupported release.
  - Use a text editor, such as vi, to access `/etc/update-manager/release-upgrades`.
  - Change the `Prompt=` setting to `Prompt=never`.
  - Save your changes and exit the file.

How to Upgrade

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

Platform Check

ThreatQ 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

> Air gapped customers should reference the **Upgrading an Air Gapped ThreatQ Instance** section of the Help Center.

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, don't hesitate to get in touch with your Technical Account Manager.

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