Release Notes

Version 6.20.0

Released Date: July 21, 2026

What's New in Version 6.20.0

The ThreatQuotient team is pleased to announce the availability of ThreatQ version 6.20.0. 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 6.20.0.

NEW/UPDATED FEATURES

Threat Research Agent | AI-Assisted Report Templates

AI-Assisted Report Templates are now available for the Threat Research Agent, enabling analysts to create reusable, standardized report templates for AI-generated reports. Templates organize AI prompts into configurable sections, ensuring consistent, high-quality reports while allowing templates to be categorized, customized for individual investigations, and reused across teams. Generated reports can be saved directly to the Threat Library as Report objects or exported as PDF for sharing. See the AI-Assisted Report Templates topic for more details.

Threat Research Agent | Insights Button

The Threat Research Agent now offers two ways to generate AI-driven insights directly from an object's details page through the **Insights** button. Hovering over the button now displays two options:

- **Quick** – Generates an AI-powered summary of the selected object directly in the chat.
- **Full** – Opens the report generation dialog to create a comprehensive AI-generated report for the selected object.

Dashboard Widget Refresh Intervals

Dashboard widgets now offer shorter automatic refresh options, giving users more control over how frequently dashboard data updates. The widget settings now include 2 and 5 minute refresh presets, helping teams keep dashboard views more current for time-sensitive monitoring and analysis.

IPv6 CIDR Support

ThreatQ now includes expanded IPv6 CIDR support with a new `CIDR Block - IPv6` indicator type. This allows users to work with IPv6 CIDR ranges in both compressed and expanded notation, with values normalized into a consistent network CIDR format.

This update also improves IPv6 CIDR matching for whitelist and containment checks by storing the calculated start and end range bounds needed for accurate comparisons. Related API field naming has been clarified to use `range_start` terminology, making IPv6 CIDR range data easier to understand and maintain.

Customer-Provided TLS Certificates

ThreatQ Hosted environments now support deployments that use a customer-provided hostname and SSL certificate. This allows customers to access their hosted ThreatQ environment through their own domain while using a certificate and private key supplied by their organization. The update also ensures hosted deployments can override the default ThreatQ hostname where needed, helping align the user-facing URL and certificate details with the customer's domain configuration.

NOTABLE BUG FIXES

The following list of issues and bugs that have been resolved with ThreatQ v6.20.0.

- **Dashboard Widgets** - Fixed an issue where Dashboard Pie Chart and Bar Chart widgets could return no results when grouped by Workflow Runs, even when matching workflow run data existed in the Threat Library. Dashboard widgets now correctly display results for objects with populated Workflow Runs values.
- **Threat Library** - Fixed an issue in Threat Library where the Related Vulnerability count could display `0` for Report objects even when valid vulnerability relationships existed.
- **Feed Runs** - Fixed an issue where closing a feed run could return a `400` error if its temporary feed run tables had already been cleaned up, such as after a scheduler restart.
- **Simple Authentication Operations** - Fixed an issue introduced in ThreatQ v6.18.0 that prevented Operations using `simple_auth` authentication from executing successfully.
- **Object Details Navigation** - Fixed an issue where navigation options in the Object Details page sidebar were not clickable across object types. Users can now select sidebar sections to navigate to the corresponding areas of an object's details page as expected.
- **LDAP Group Migration** - Fixed an upgrade issue that could occur when migrating LDAP Groups to Roles in environments containing custom groups.

- **Platform Reliability** - Fixed an issue where malformed custom feed definitions could cause Dynamo feed processing to fail without clearly surfacing the error and could prevent other feeds from running. Dynamo now handles invalid feed configuration more safely, improving feed processing reliability and reducing the risk of system-wide feed disruption from a single malformed feed.
- **Dashboard Performance** - Improved dashboard performance by optimizing widget caching and simplifying cache management.

Security and System Updates

The following updates have been made with ThreatQ v6.20.0:

- **Operations** - Updated API response handling to better protect sensitive Operation configuration data. This security update helps ensure credentials and other protected configuration values are not exposed in object detail responses.
- **Security Hardening for Export Templates** - Security hardening has been added for export template handling. Export template functions have been restricted to a smaller set than historically allowed to reduce risk and improve platform safeguards.

  

  If you encounter issues with export templates that worked in prior ThreatQ versions, please contact Support for help reviewing and reconciling the affected template.

- **API Error Handling** - Improved error handling for Solr connection failures to ensure connection issues are reported and handled more reliably. This security update helps prevent invalid connection states and improves overall application stability when backend search services encounter errors.
- **Authentication Security** - Improved authentication messaging to provide more consistent, non-specific responses during sign-in attempts. This security update helps better protect user account information and strengthens the overall authentication experience.
- **Multi-Factor Authentication** - Enhanced MFA validation protections to better limit repeated invalid verification attempts. This security update strengthens authentication safeguards and helps protect accounts from excessive MFA validation retries.
- **User API Security** - Strengthened authorization controls for user-related API access. This security update helps ensure users can only access account information they are permitted to view, improving protection of user profile and configuration data.
- **Password Security** - Improved password management form handling to better protect credential data during user creation and updates. This security update

strengthens how sensitive password fields are submitted and reduces the risk of unintended credential exposure.

- **File Permissions** - Improved default storage permissions for ThreatQ-managed deployment directories to better align with customer security and compliance requirements. This security update strengthens least-privilege handling for application-managed storage and helps reduce audit risk in hardened environments.
- **Lodash Dependency Update** - Lodash was updated from `4.17.21` to `4.18.1`. This update resolves CVE-2025-13465.

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