ThreatQuotient

ThreatQ Tasks Action

Version 1.0.0

May 20, 2025

ThreatQuotient

20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support

Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document "as is", without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠️ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.1
Compatible with ThreatQ Versions	>= 5.12.1
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The ThreatQ Tasks Action integration allows the automatic creation and assignment of tasks in ThreatQ for incoming data.

The integration provides the following action:

- **ThreatQ - Create Tasks** - automatically creates tasks for incoming intelligence objects.

The action is compatible with the following system object types:

- Adversaries
- Assets
- Attack Patterns
- Campaigns
- Courses of Action
- Events
- Exploit
- Targets
- Identities
- Incidents
- Intrusion Sets
- Malware
- Reports
- Tools
- TTPs
- Vulnerabilities

> This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following object types:
    - Adversaries
    - Assets
    - Attack Patterns
    - Campaigns
    - Courses of Action
    - Events
    - Exploit
    - Targets
    - Identities
    - Incidents
    - Intrusion Sets
    - Malware
    - Reports
    - Tools
    - TTPs
    - Vulnerabilities

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
   - Drag and drop the zip file into the dialog box
   - Select **Click to Browse** to locate the zip file on your local machine

> ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
Task Title	Enter a title for the tasks that will be created.
Task Description	Enter a description for the tasks that will be created. HTML markup is supported.
Priority	Select the priority of the task. Options include: ◦ Low ◦ Medium *(Default)* ◦ High
Status	Select the status of the task. Options include: ◦ ToDo *(Default)* ◦ In Progress ◦ Review ◦ Done
Assignee	Select the user that will be assigned the task. Options include: ◦ Specific User *(Default)* ◦ Least Assigned ◦ Unassigned

PARAMETER	DESCRIPTION
	📝 The `Least Assigned` logic considers the total number of tasks already assigned to users. For example, there are two users in the pool. User A has 3 existing Tasks assigned to him and User B has zero existing tasks. If the there are two new tasks, the action will assign them to User B using this logic to maintain an even distribution.
Assigned User	Enter the user that will be assigned the task(s). Entry format will based on your ThreatQ version: • **ThreatQ Version >= 6.7.0** - enter the user's display name in this parameter. • **ThreatQ Version < 6.7.0** - enter the user's username or email. 📝 This parameter is only accessible if you selected `Specific User` for the **Assignee** parameter.
Assignee Pool	Enter the users that that will be included in the pool to be assigned the task(s). Entry format will based on your ThreatQ version: • **ThreatQ Version >= 6.7.0** - enter the user's display name in this parameter. • **ThreatQ Version < 6.7.0** - enter the user's username or email. 📝 This parameter is only accessible if you selected `Least Assigned` for the **Assignee** parameter.
Due In X Days	Optional - Enter a due date, in the form of days, for the task. The default value is `0`, which is for no due date.
Allow Manual Execution	Enabling this parameter will result in allowing the action to be run manually. When running manually, the entire data collection will be processed. This parameter is disabled by default as to prevent creating duplicate tasks en masse.
Objects Per Run	The number of objects to process per run of the workflow.

Configuration

Overview

This action will take the objects from a data collection and create a new task for each object. This may be useful for automate tasking for your analysts.

WARNING, ensure that your Threat Library data collection contains a reasonable amount of objects (less is better) as this action will create a task for each object.

NOTE, by default, since tasks are not de-duplicated, this action will not operate when run manually.

Task Configuration

Task Title

Enter a title for the tasks that will be created.

Task Description

Enter a description for the tasks that will be created. HTML is supported.

Priority

Medium

Select the priority of the task.

Status

ToDo

Select the status of the task.

Assignee

Specific User

Select the user that will be assigned the task

Assigned User

Enter the display name (>= v5.7.0) or username/email (< v5.7.0) of the user that will be assigned the task.

Due In X Days (Optional)

0

Additional Information

Integration Type: Action
Version:
Action ID: 1
Accepted Data Types:
Adversaries
Assets
Attack Pattern
Campaign
Course of Action
Events
Exploit Target
Identity
Incident
Intrusion Set
Malware
Report
Tool
TTP
Vulnerability

5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
`ThreatQ - Create Tasks`	Creates a new task for each object in a data collection	Adversaries, Assets, Attack Patterns, Campaigns, Courses of Action, Events, Exploit Targets, Identities, Incidents, Intrusion Sets, Malware, Reports, Tools, TTPs, Vulnerabilities	N/A

ThreatQ - Create Tasks

The ThreatQ - Create Tasks action will take a data collection and create a task for each object in the collection. The task will be assigned to the user specified in the configuration (or unassigned).

> There is no mapping for this action. For each object a new task is created and related to it.

Use Case Example

Scenario 1

1. An organization receives reports from different vendors everyday.
2. The manager wants to automatically create tasks to assign to each analyst for each report that comes in.
3. The manager selects `Least Assigned` as the **Assignee** and enters each analyst in the **Assignee Pool** parameter.
4. Tasks will be divided equally among the analysts.

Scenario 2

1. An organization receives alerts from different vendors everyday regarding typosquatting, potential phishing, and/or other malicious activities.
2. The manager wants to assign these alerts to a specific analyst who specializes in these areas.
3. The manager selects `Specific User` as the **Assignee** and enters the analyst in the **Assigned User** parameter.
4. The tasks will assigned to specified analyst.

Change Log

- **Version 1.0.0**
    - Initial release