ThreatQuotient

ThreatQuotient for Resilient Operation User Guide

Version 1.0.0

November 03, 2023

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	1.2.0
Compatible with ThreatQ Versions	>= 4.47.0
Support Tier	ThreatQ Supported

Introduction

The Resilient Operation for ThreatQuotient enables a ThreatQ user to create Resilient incidents directly from ThreatQ. It also lets you query Resilient from ThreatQ to search if an indicator is related to an incident in Resilient.

The operation provides the following actions:

- **Create -** creates the selected event (from ThreatQ) as an Incident in Resilient.
- **Enrich Indicator -** checks if the indicator is an existing artifact that is related to incidents.

The operation is compatible with Events and Indicators.

Prerequisites

This operation requires users to have an api key set up for resilient with the proper permissions. To execute both actions the api key needs the ability to create and read artifacts and incidents.

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 integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
    - Drag and drop the file into the dialog box
    - Select **Click to Browse** to locate the integration file on your local machine

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

The operation is now installed and will be displayed in the ThreatQ UI. You will still need to configure and then enable the operation.

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 **Operation** option from the *Type* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Host	Enter the hostname or IP address for your Resilient Server.
Email	Enter a Resilient email address to authenticate with your Resilient Server.
Password	Enter the password associated with the above email address.
Organization	Enter the Organization for the specified user from Resilient.
Time Zone	Select the time zone for your Resilient instance. This is used for syncing occurrence dates with ThreatQ.

Custom Attribute Mapping	You can map ThreatQ Attributes to Resilient Custom Fields here. Each mapping is line-delimited, and equals-separated.
	The Resilient Custom Field name must be the programmatic API name (found in Customization Setting)
	Custom Field Mapping Example
	ThreatQ Attribute Name=Resilient Custom Field API Name
	`MITRE Attack Tactic Name=mitre_tactic_name`
	`Threat Confidence=confidence_level`

Custom Object Mapping	You can map ThreatQ Objects to Resilient Custom Fields here. Each mapping is line-delimited, and equals-separated.

PARAMETER	DESCRIPTION
	The Resilient Custom Field name must be the programmatic API name (found in Customization Setting). **Custom Field Mapping Example** ThreatQ Attribute Name=Resilient Custom Field API Name `TTP=mitre_technique_name`

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

Actions

The operation provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Create	Creates the selected event (from ThreatQ) as an Incident in Resilient.	Event	N/A
Enrich Indicator	Checks if the indicator is an existing artifact that is related to incidents.	Indicator	All

Change Log

- **Version 1.1.2**
  - N/A
- **Version 1.0.0**
  - Initial release