ThreatQuotient

ThreatQ Object Operation Guide

Version 1.0.1

May 31, 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	1.0.1
Compatible with ThreatQ Versions	>= 5.15.0
Support Tier	ThreatQ Supported

Introduction

ThreatQ Object operation allows a ThreatQ user to interact with objects in complex ways to better manage the Threat Library.

The operation provides the following actions:

- **Clone** - creates a new object based on the original.
- **Inherit from Children** - bubble-up relationships and other context from child relationships.

The operation is compatible with the following system objects:

- Event
- Campaign
- Attack Pattern
- Malware
- Exploit Target
- Asset
- Tool
- Adversary
- TTP
- Report
- Intrusion Set
- Course Of Action
- Signature
- Vulnerability
- Identity
- Incident
- Indicator

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. Review any additional settings, make any changes if needed, and click on **Save**.
5. 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
Object Clone	Creates a new object based on the original.	All Seeded ThreatQ System Objects	N/A
Object Inherit from Children	Bubble-up relationships and other context from child relationships.	All Seeded ThreatQ System Objects	N/A

Object Clone

The Object Clone action creates a new object based on the original.

Configuration Options

The following configuration options are available after selecting the action:

CONFIGURATION	DESCRIPTION
New Value / Name / Title (Optional)	The new value (or title/name) to give to the cloned object. If none provided, a prefix will be added. Example: `<original value> - CLONE`.
Cloned Object Type	Select the type of object to clone this object to. The default is the original object type.
Copy Selected Relationships	Select the relationships to copy to the cloned object.
Copy Tags	Enabling this will copy all tags to the cloned object.
Copy Attributes	Enabling this will copy all attributes (including their sources) to the cloned object.
Relate Cloned Object to Original	Enabling this will relate the cloned object to the original object.

Object Inherit from Children

The Object Inherit from Children action bubble-ups relationships and other context from child relationships.

Configuration Options

The following configuration options are available after selecting the action:

CONFIGURATION	DESCRIPTION
Select the objects you want to inherit context from	Select which objects you'd like context inherited from.
Select the sub-relationships you'd like to inherit	Select which objects you'd like to inherited from this object's sub-relationships.
Inherit Tags	Would you like tags to be bubbled-up to this object?

Change Log

- **Version 1.0.1**
  - Updated the hostname for all requests.
  - Updated the minimum ThreatQ version to 5.15.0. This was incorrectly reported as 5.14.0 in a previous announcement.
- **Version 1.0.0**
  - Initial release