ThreatQuotient



Cisco Threat Response Operation User Guide

Version 1.0.0

October 18, 2023

ThreatQuotient

20130 Lakeview Center Plaza Suite 400 Ashburn, VA 20147



Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893



Contents

| Narning and Disclaimer | |
|------------------------|---|
| Support | 4 |
| ntegration Details | 5 |
| ntroduction | |
| nstallation | |
| Configuration | 8 |
| Actions | 9 |
| Enrich | 9 |
| Change Log | |



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.

Copyright © 2023 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.



Support

This integration is designated as ThreatQ Supported.

Support Email: support@threatg.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 1.0.0

Compatible with ThreatQ >= 4.20.0

Versions

Support Tier ThreatQ Supported



Introduction

The Cisco Threat Response Operation for ThreatQuotient enables a user to query Cisco Threat Response for contextual information on a given indicator of compromise.

The operation provides the following action:

• Enrich - queries Cisco Threat Response for any enrichment context it has on an indicator.

The operation is compatible with the following indicator types:

- Email Subject
- MAC Address
- FQDN
- MD5
- I QDIV
- Mutex
- File PathFilename
- SHA-1
- IP Address
- SHA-256
- IPv6 Address
- Username



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 |
|-------------------|--|
| Region | The region of your Cisco Threat Response instance. |
| API Client ID | Your Cisco Threat Response API Client ID. |
| API Client Secret | Your Cisco Threat Response API Client Secret. |

- 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

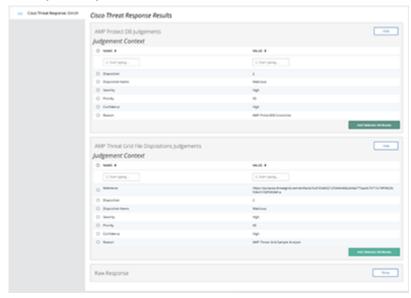
The operation provides the following action:

| ACTION | DESCRIPTION | OBJECT TYPE | OBJECT SUBTYPE |
|--------|---|----------------|---|
| Enrich | Queries Cisco Threat Response for any enrichment context it has on an indicator. | Indicator | Email Subject, FQDN, File Path, Filename, IP Address, IPv6 Address, MAC Address, MD5, Mutex, SHA-1, SHA-256, Username |

Enrich

The Enrich action queries Cisco Threat Response for any enrichment context it has on an indicator.

Example Output





Change Log

- Version 1.0.0
 - Initial release