

ThreatQuotient



Recorded Future Operation Guide

Version 1.3.0

August 29, 2022

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

Integration Details..... 5

Introduction 6

Installation..... 7

Configuration 8

Actions 9

Change Log..... 10

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 © 2022 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@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	1.3.0
Compatible with ThreatQ Versions	>= 4.35.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https:// marketplace.threatq.com/ details/recorded-future- operation

Introduction

The ThreatQuotient for Recorded Future Operation allows a ThreatQ user to add geolocation attributes and related indicators (if available) of IP Addresses within ThreatQ.

The operation provides the following actions:

- **Enrich** - provides enrichment of the selected object.
- **Intel Card Link** - links to the Recorded Future Intel Card.

The operation is compatible with the following indicator types:

- CVE
- FQDN
- IP Address
- MD5
- SHA-1
- SHA-256
- SHA-384
- SHA-512

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
Hostname	The hostname for the API.
Hostname Port	The port for the Recorded Future host.
Recorded Future API Key	The API Access Key provided by Recorded Future.

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
Enrich	Provides enrichment of the selected object.	Indicator	CVE, FQDN, IP Address, MD5, SHA-1, SHA-256, SHA-384, SHA-512
Intel Card Link	Links to the Recorded Future Intel Card.	Indicator	CVE, FQDN, IP Address, MD5, SHA-1, SHA-256, SHA-384, SHA-512

Change Log

- **Version 1.3.0**
 - Removed the ability to pull related vulnerabilities due to some vulnerabilities not having a proper value. This would cause an error when ThreatQ attempted to ingest the information.
- **Version 1.2.0**
 - Added enrichment of CVE objects.
 - Added the ability to pull related vulnerabilities from Recorded Future
- **Version 1.0.0**
 - Initial release