

# ThreatQuotient



## QRadar Operation User Guide

**Version 1.4.0**

December 17, 2023

### **ThreatQuotient**

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 **ThreatQ Supported**

### **Support**

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

# Contents

Warning and Disclaimer ..... 3

Support ..... 4

Integration Details..... 5

Introduction ..... 6

Prerequisites ..... 7

    QRadar Authentication Token ..... 7

Installation..... 8

Configuration ..... 9

Actions ..... 11

    Run Parameters ..... 11

Known Issues / Limitations ..... 12

Change Log ..... 13

# 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@threatq.com](mailto: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	1.4.0
Compatible with ThreatQ Versions	>= 4.26.0
Support Tier	ThreatQ Supported

# Introduction

The QRadar Operation provides a historical look up of events related to IP Address, FQDN, and URL type Indicators.

The operation provides the following action:

- **Search** - performs a historical look up of events related to the submitted object.

The operation is compatible with IP Address, FQDN, and URL type Indicators.

# Prerequisites

Review the following requirements before attempting to install or upgrade the QRadar operation.

## QRadar Authentication Token

You must have a **valid QRadar Authorization Token** for each of the QRadar systems you want to run the operation against. You can generate an Auth Token in the QRadar UI by navigating Admin > Authorized Services > Add Authorized Services.

# 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 Configuration	<p>Enter your host and sec_token configuration settings in the field provided. Each entry should contain the following:</p> <ul style="list-style-type: none"> <li>◦ <b>QRadar Instance Name</b> - the name that you want it to show up as in the system. Note that at least the first 10 characters should be unique.</li> <li>◦ <b>host</b> - the host (with scheme) to the QRadar instance you want to run the operation against.</li> <li>◦ <b>sec-token</b> - the authorized service token from the QRadar instance you want to run the operation against.</li> </ul> <p>Example:</p> <pre>QRadar 1:   host: https://10.10.10.10   sec_token: 5b579449-5864-4a17-8dcf-82865ea89244 QRadar 2:   host: https://10.10.10.11   sec_token: 8dcf5864-9449-5b57-5ea8-4a1792448286</pre>
Days to Search	The number of days for the historical lookup.
Record Limit	Enter a value to limit the return results. The default value is 100.
Verify SSL	Enable this option to verify SSL when connecting to QRadar.
First Results	Enable this option to see the 100 earliest results. If this option is not enabled, you will see the 100 latest results.

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
Search	Performs a historical look up of events related to the submitted object.	Indicator	IP Address, FQDN, URL

## Run Parameters

The following parameters are available when you select the operation's action to run against an object:

PARAMETER	DESCRIPTION
Days to Query	<p>Enter how many days back from the current date to query.</p> <div>  <p>The value is limited by the <b>Days to Search</b> parameter set on the operation's configuration settings.</p> </div>
Start Date	Start date for a date range query. Format must be Y-m-d H:M:S (Example: 2022-01-01 00:00:00)
End Date	End date for a date range query. Format must be Y-m-d H:M:S (Example: 2022-01-01 00:00:00)
Dry Run	Disable this option in order to automatically upload returned indicators to ThreatQ.

## Known Issues / Limitations

- Version 1.3.0 introduced the ability to to run the operation against multiple instances at one time. You may experience technical limitations when performing the operation against more than one appliance.

# Change Log

- **Version 1.4.0**
  - You are no longer required to create and link a separate configuration file in order to install/use the operation. This information can now be entered from the configuration screen via the new **Host Configuration** parameter field.
    - Removed the **Config** parameter from the configuration screen.
    - Added **Host Configuration** parameter field to the configuration screen.
  - Added the following run configuration parameters for the Search action:
    - Dry Run
    - Days to Query
    - Start Date
    - End Date



See the [Run Parameters](#) section of this guide for more details.

- **Version 1.3.1**
  - Fixed a dependency issue.
- **Version 1.3.0**
  - Added the ability to allow the operation to be run against multiple instances at the same time.
- **Version 1.2.2**
  - Modified the SQL query.
  - Improved Logging.
  - Added new configuration option, **Limit**, to allow you to limit the number of records returned.
- **Version 1.2.0**
  - Initial release