ThreatQuotient

ThreatQuotient for Carbon Black Defense 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	1.0.0
Compatible with ThreatQ Versions	>= 3.6.0
Support Tier	ThreatQ Supported

Introduction

The ThreatQuotient for Carbon Black Defense Operation allows a ThreatQ user to query their Carbon Black Defense instance for any sensors/devices that have generated events containing an indicator.

The operation provides the following action:

- **Query Sensor Events -** retrieves sensor data from the Carbon Black Defense API.

The operation is compatible with Filename and SHA-256 indicator types.

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

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

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
Carbon Black Defense API Host	The Host or IP of your Carbon Black Defense instance.
API Key	Carbon Black Defense API Key. ⚠ Do not include the Connector ID.
Connector ID	The value will be appended to the API key for authentication.

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
Query Sensor Events	Retrieves sensor data from the Carbon Black Defense API.	Indicator	Filename, SHA-256

Usage

The following section covers the use of the ThreatQuotient for Carbon Black Defense Operation.

1. Navigate to a suitable indicator found in ThreatQ that is to be scanned.
2. Navigate to the Operations section on the left hand side.

> A Carbon Black Defense entry will be available.

3. Click the Carbon Black Defense entry to run the operation, you will be presented with a popup window asking for two further pieces of information.
   a. How far back do you want to search?: These are pre-set fields, set by Carbon Black Defense's API. Select one.
   b. Max number of results to show: The Carbon Black Defense API may return a ton of results (> 1k), so this option is here to limit the number of events returned.

> The total number of events found will show as a statistic, but the event details will not be pulled after the max number is reached.

Change Log

- **Version 1.0.0**
  - Initial release