ThreatQuotient

Carbon Black Response Operation Guide

Version 1.2.0

Thursday, June 18, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: Support.threatq.com

Phone: 703.574.9893

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.

Contents

Warning and Disclaimer **2**
Contents **3**
Versioning **4**
Introduction **5**
Preface 5
Audience 5
Scope 5
Installation **6**
Configuration **7**
Usage **8**
MD5 8
Domains, IP Addresses & MD5 8
Change Log **9**

Versioning

- Current integration version: 1.2.0
- Supported on ThreatQ versions: 3.6 or greater

Introduction

The ThreatQuotient for Carbon Black Response Operation provides users with the ability to interact with Carbon Black Response in two ways. First, it allows users to blacklist MD5 hashes within Carbon Black Response, directly from ThreatQ. Second, it allows users to query Carbon Black Response to see if an indicator (IP Address, FQDN, or MD5) has been found in any Threat Reports.

Preface

This guide provides the information necessary to implement the ThreatQuotient for Carbon Black Response Operation. This document is not specifically intended as a site reference guide. It is assumed that the implementation engineer has experience installing and commissioning the ThreatQuotient Apps and integrations covered within the document, as well as the experience necessary to troubleshoot at a basic level.

Audience

This document is intended for use by the following parties:

- ThreatQ and Security Engineers.
- ThreatQuotient Professional Services Project Team & Engineers.

Scope

This document covers the implementation of the application only

Installation

Perform the following steps to install the operation:

Note: *The same steps can be used to upgrade the operation to a new version.*

1. Download the operation .whl file.
2. Log into your ThreatQ instance.
3. Click on the **Settings** icon and select **Operations Management**.
4. Click on the **Install Operation** button.
5. Upload the operation file using one of the following methods:
6. Drag and drop the file into the dialog box
7. Select **Click to Browse** to locate the operation file on your local machine

   Note: *ThreatQ will inform you if the operation already exists on the platform and will require user confirmation before proceeding.*

The operation will be added to your list of installed operations. You will still need to configure and enable the operation.

Configuration

Note: *ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other operation-related credentials.*

To configure the operation:

1. Click on the **Settings** icon and select **Operations Management**.
2. Locate the operation and click on **Operation Settings**.
3. Enter the following configuration parameters:

Parameter	Description
Carbon Black Response Host	The Carbon Black Response Host IP address.
API Token	The Carbon Black Response API Key.

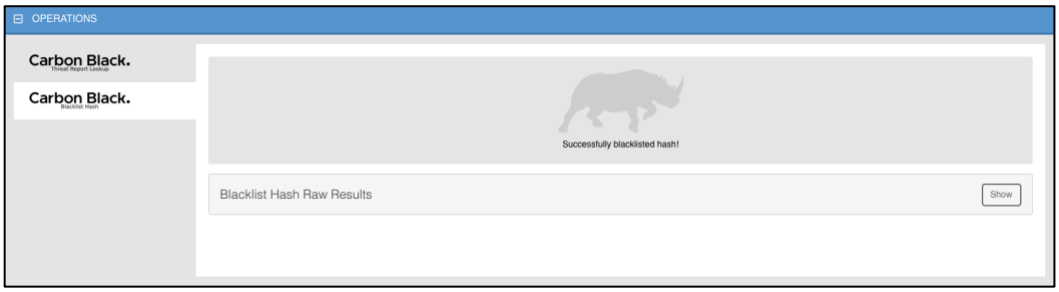
4. Click on **Save Changes**.
5. Click on the toggle switch to the left of the operation name to enable the operation.

Usage

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

MD5

1. For MD5's, you will get the operation to Blacklist the hash.
2. By clicking the operation, the hash will then be added to the banned hashes section found in the Carbon Black Response server/portal, by going to the very last icon in the side bar, labelled, "Banned Hashes."



Domains, IP Addresses & MD5

1. For Domains, IPs, and MD5s, you will get the operation to do a Threat Report Lookup:
    - For lookups on an indicator that is found in a report, the operation will show all the reports it is found in, as well as any related indicators from the same report.
    - Lookups where an indicator is not found in any report and make sure the response fits accordingly; no errors.
2. Threat Report Lookup enables you to relate the indicators and attributes (links) successfully to the main indicator where the operation is being run.

Change Log

Version	Details
1.2.0	• Added the ability to execute a Binary Search for hashes from within ThreatQ • Added the ability to execute a Process Search for hashes from within ThreatQ • Operation now allows users to lookup if hashes have been banned • Operation now allows users to specify their port.
1.0.0	Initial Release