

ThreatQuotient



ThreatQuotient for Have I Been Pwned Operation User Guide

Version 1.0.0

October 28, 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 3

Support 4

Integration Details..... 5

Introduction 6

Installation..... 7

Configuration 8

Actions 9

 Lookup..... 9

Change Log..... 11

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

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	>= 4.26.0
Support Tier	ThreatQ Supported

Introduction

The Have I Been Pwned Operation for ThreatQuotient enables a ThreatQ user to query Have I Been Pwned for any breaches for a given account.

The operation provides the following action:

- **Lookup** - queries Have I Been Pwned for any breaches associated with the selected email address.

The operation is compatible with IP Address type Indicators.

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 parameter under the **Configuration** tab:

PARAMETER

DESCRIPTION

API Key

Your Have I Been Pwned API Key.

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
Lookup	Queries Have I Been Pwned for any breaches associated with the queried email address.	Indicator	IP Address

Lookup

The Lookup action queries Have I Been Pwned for any breaches associated with the queried email address.

Example Output

 Have I Been Pwned: Lookup

Account found in 7 breaches!

Breach: 000webhost

Showing 1 to 15 of 15

Row count: 25 ▾

<input type="checkbox"/> NAME ▾	VALUE ▾
<input type="text" value="Start typing..."/>	<input type="text" value="Start typing..."/>
<input type="checkbox"/> Breached Data	Email addresses
<input type="checkbox"/> Breached Data	IP addresses
<input type="checkbox"/> Breached Data	Names
<input type="checkbox"/> Breached Data	Passwords
<input type="checkbox"/> Description	000webhost: In approximately March 2015, the free web hosting provider 000webhost suffered a major data breach that exposed almost 15 million customer records. The data was sold and traded before 000webhost was alerted in October. The breach included names, email addresses and plain text passwords.
<input type="checkbox"/> Is Spam List	No
<input type="checkbox"/> Breach Title	000webhost
<input type="checkbox"/> Breached Domain	000webhost.com
<input type="checkbox"/> Is Sensitive	No
<input type="checkbox"/> Breach Date	2015-03-01
<input type="checkbox"/> Pwn Count	14936670
<input type="checkbox"/> Breach Name	000webhost
<input type="checkbox"/> Is Retired	No
<input type="checkbox"/> Is Fabricated	No
<input type="checkbox"/> Is Verified	Yes

Add Attribute

Breach: Canva

Showing 1 to 16 of 16

Row count: 25 ▾

<input type="checkbox"/> NAME ▾	VALUE ▾
<input type="text" value="Start typing..."/>	<input type="text" value="Start typing..."/>
<input type="checkbox"/> Breached Data	Email addresses
<input type="checkbox"/> Breached Data	Geographic locations
<input type="checkbox"/> Breached Data	Names
<input type="checkbox"/> Breached Data	Passwords
<input type="checkbox"/> Breached Data	Usernames
<input type="checkbox"/> Description	Canva: In May 2019, the graphic design tool website Canva suffered a data breach that impacted 137 million subscribers. The exposed data included email addresses, usernames, names, cities of residence and passwords stored as bcrypt hashes for users not using social logins. The data was provided to HIBP by a source who requested it be attributed to "JimScott.Sec@protonmail.com".
<input type="checkbox"/> Is Spam List	No
<input type="checkbox"/> Breach Title	Canva
<input type="checkbox"/> Breached Domain	canva.com
<input type="checkbox"/> Is Sensitive	No
<input type="checkbox"/> Breach Date	2019-05-24
<input type="checkbox"/> Pwn Count	137272116
<input type="checkbox"/> Breach Name	Canva
<input type="checkbox"/> Is Retired	No
<input type="checkbox"/> Is Fabricated	No
<input type="checkbox"/> Is Verified	Yes

Add Attribute

Change Log

- Version 1.0.0
 - Initial release