ThreatQuotient

A Securonix Company

Have I Been Pwned Action

Version 1.0.0

June 28, 2026

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: tq-support@securonix.com
Web: https://ts.securonix.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: tq-support@securonix.com
Support Web: https://ts.securonix.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	>= 5.29.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The **Have I Been Pwned Action Bundle** enables ThreatQ users to enrich email address indicators with breach intelligence from the Have I Been Pwned (HIBP) platform. By querying the HIBP breached account endpoint, the action identifies known data breaches associated with an email address and enriches the indicator with breach-related context to support credential exposure investigations and incident response.

The integration provides the following action:

- **Have I Been Pwned - Lookup** - queries the Have I Been Pwned (HIBP) breached account endpoint using a submitted email address and returns details of known data breaches associated with the account.

The integration is compatible with Email Address type Indicators and returns enriched indicators and indicator attributes.

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A Have I Been Pwned API Key for production HTTP lookups.
- A data collection containing the Email Address indicator type objects.

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 action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

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

You will still need to configure the action.

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 **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

   The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

PARAMETER	DESCRIPTION
API Key	Enter your Have I Been Pwned API key which is required when the HTTP source is enabled.
Include Unverified Results	Enable this parameter to include HIBP breaches that have not been independently verified. This parameter is enabled by default.
Enable SSL Certificate Verification	Enable this parameter if the action should validate the host-provided SSL certificate.
Disable Proxies	Enable this parameter if the action should not honor proxies set in the ThreatQ UI.
Objects Per Run	Enter the max number of objects to process per run. The default value is `1000`.

5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Have I Been Pwned - Lookup	Retrieve HIBP breaches for an email address	Indicator	Email Address

Have I Been Pwned - Lookup

The Have I Been Pwned – Lookup action queries the Have I Been Pwned (HIBP) breached account endpoint using a submitted email address to identify known data breaches associated with the account.

```
GET https://haveibeenpwned.com/api/v3/breachedaccount/{email}
```

Sample Response:

```
[
  {
    "Name": "Adobe",
    "Title": "Adobe",
    "Domain": "adobe.com",
    "BreachDate": "2013-10-04",
    "PwnCount": 152445165,
    "Description": "In October 2013, 153 million Adobe accounts were
breached with email addresses, password hints and encrypted passwords
exposed.",
    "DataClasses": [
      "Email addresses",
      "Password hints",
      "Passwords",
      "Usernames"
    ],
    "IsVerified": true,
    "IsFabricated": false,
    "IsSensitive": false,
    "IsRetired": false,
    "IsSpamList": false
  }
]
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
.Name	Indicator.Attribute	Breach Name	Adobe
.Title	Indicator.Attribute	Breach Title	Adobe
.BreachDate	Indicator.Attribute	Breach Date	2013-10-04
.PwnCount	Indicator.Attribute	Pwn Count	152445165
.IsVerified	Indicator.Attribute	Is Verified	Yes
.IsSensitive	Indicator.Attribute	Is Sensitive	No

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
.IsRetired	Indicator.Attribute	Is Retired	No
.IsSpamList	Indicator.Attribute	Is Spam List	No
.IsFabricated	Indicator.Attribute	Is Fabricated	No
.Domain	Indicator.Attribute	Breached Domain	adobe.com
.Description	Indicator.Attribute	Description	Adobe: ...
.DataClasses[]	Indicator.Attribute	Breached Data	Email addresses

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

METRIC	RESULT
Run Time	2 minutes
Indicator	2
Indicator Attributes	35

Change Log

- **Version 1.0.0**
  - Initial release