ThreatQuotient

Enzoic Action User Guide

Version 1.0.0

October 30, 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	>= 5.20.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

Enzoic is a security platform that helps prevent account takeover and fraud through compromised credential detection and password policy enforcement.

The Enzoic Action for ThreatQ enables the automatic search for exposures, given a dynamic list of usernames/emails. Organizations will be able to use this action to submit a list of usernames/emails and receive a list of exposures for each of them in the form of ThreatQ Events. This allows organizations to monitor their users' exposure and take action to prevent account takeovers.

The integration provides the following TQO action:

- **Enzoic - Check User Exposures** - locates exposures for the given usernames/emails

The action is compatible with Indicators (Username, Email Address) and Identities system objects.

The action returns the following enriched system objects:

- Events
- Indicators (Username, Email Address)
- Identities

> 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 data collection containing at least one of the follow object types:
  - Username or Email type indicators
  - Identities
- An Enzoic API Key

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

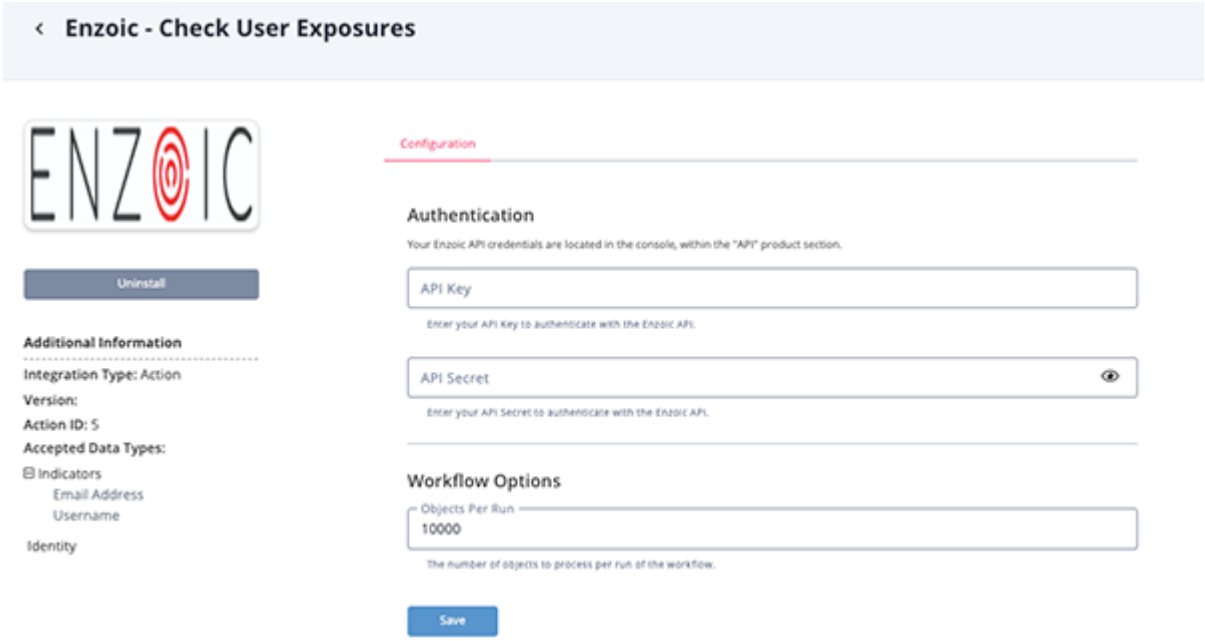
> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

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 API Key to authenticate with the Enzoic API.
API Secret	Enter your API Secret to authenticate with the Enzoic API.
Objects per Run	The number of objects to process per run of the workflow. The default value is **10000**.



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

Actions

The following actions are available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Enzoic - Check User Exposures	Checks identities for exposures	Indicator, Identity	Indicator: Username, Email Address

Enzoic - Check User Exposures

The Check User Exposures action checks email addresses and usernames indicator types, as well as identities, submitted to the Enzoic API to check for exposures. Any exposures identified are then ingested back into the ThreatQ platform in the form of Events.

`GET https://api.enzoic.com/v1/exposures-for-usernames`

Sample Response:


```
[
  {
    "username": "frank@corp.co",
    "usernameHash": "51885d3cc1b6f144455e9d25661ca34b9f945b5540b61cb41cf56381950bf50b",
    "count": 1,
    "exposures": [
      {
        "id": "57dc11964d6db21300991b78",
        "title": "funsurveys.net",
        "entries": 5123,
        "date": "2015-05-01T00:00:00.000Z",
        "category": "Manufacturing",
        "source": "Cybercrime Forums",
        "passwordType": "Cleartext",
        "exposedData": ["Emails", "Passwords"],
        "dateAdded": "2016-09-16T15:36:54.000Z",
        "sourceURLs": ["https://www.someplace.com"],
        "domainsAffected": 683,
        "sourceFileCount": 1
      }
    ]
  }
]
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.username`	Indicator.Value or Identity.Value	N/A	N/A	`user@threatq.com`	N/A
`.exposures[].title`	Event.Title	Exposure	`.exposures[].dateAdded`	`funsurveys.net`	N/A
`.exposures[].category`	Event.Attribute	Category	`.exposures[].dateAdded`	`Manufacturing`	N/A
`.exposures[].domainsAffected`	Event.Attribute	Domains Affected	`.exposures[].dateAdded`	`683`	If the attribute already exists, the value will be updated.
`.exposures[].entries`	Event.Attribute	Entries	`.exposures[].dateAdded`	`5123`	If the attribute already exists, the value will be updated.
`.exposures[].exposedData`	Event.Attribute	Exposed Data	`.exposures[].dateAdded`	`Emails`	N/A
`.exposures[].passwordType`	Event.Attribute	Exposed Password Type	`.exposures[].dateAdded`	`Cleartext`	N/A
`.exposures[].source`	Event.Attribute	Source	`.exposures[].dateAdded`	`Cybercrime Forums`	N/A
`.exposures[].sourceURLs[]`	Event.Attribute	Source URL	`.exposures[].dateAdded`	N/A	N/A
N/A	Identity.Attribute or Indicator.Attribute	Is Exposed	`.exposures[].dateAdded`	`true`	N/A

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	1 minute
Events	1
Event Attributes	7
Identities	4
Indicator Attributes	4

Change Log

- **Version 1.0.0**
  - Initial release