ThreatQuotient

Enzoic CDF 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
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 CDF for ThreatQ enables the automatic ingestion of all public exposures, or exposures pertaining to a particular domain. These exposures will be ingested as Events, which can be used to alert you of any new exposures that are discovered.

The integration provides the following feeds:

- **Enzoic Exposures -** ingests all public Exposures from the Enzoic API.
- **Enzoic Exposures by Domain -** ingests all Exposures and users for a specified domain from the Enzoic API.

The integration ingests the following system object types:

- Identities
    - Identity Attributes
- Events
    - Event Attributes

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:

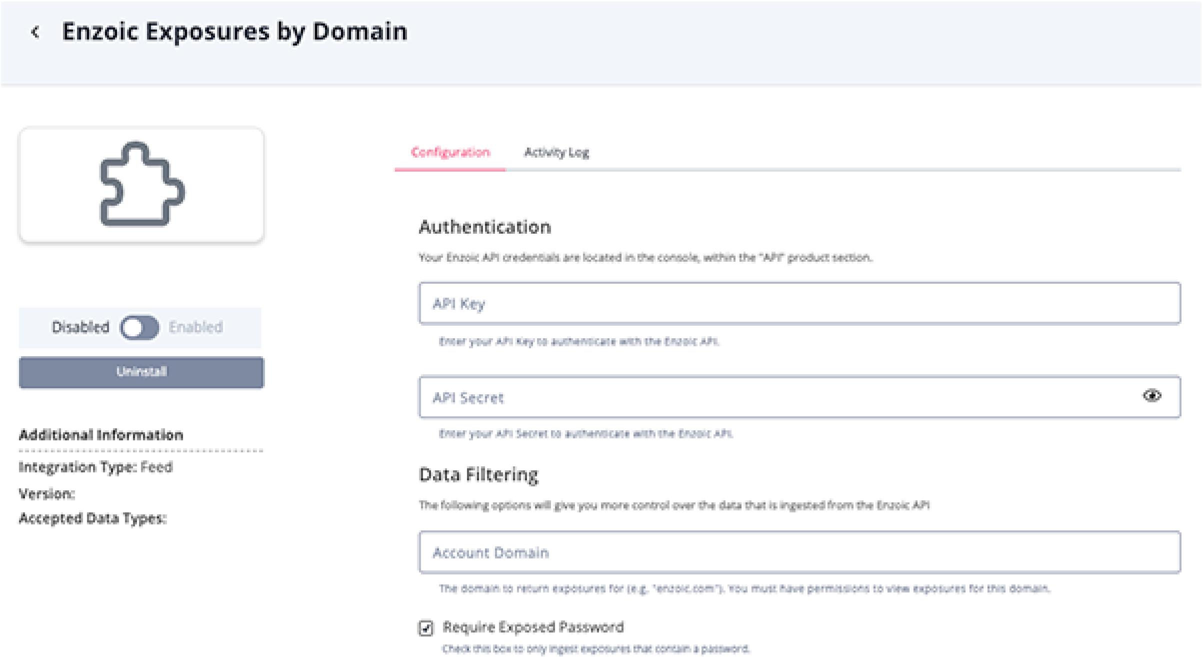
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
API Key	Your Enzoic API Key.
API Secret	Your Enzoic API Secret.
Require Exposed Password	When enabled, the feeds will only ingest exposures that contain a password.
Require Category *(Exposures feed only)*	When enabled, the feed will only ingest exposures that contain a category. **Example**: Exposures listed as `Unspecified` will not be ingested.
Minimum Entries *(Exposures feed only)*	The minimum number of entries an exposure must have in order to be ingested into the platform.
Minimum Affected Domains *(Exposures feed only)*	The minimum number of affected domains an exposure must have in order to be ingested into the platform.
Account Domain *(Exposures by Domain feed only)*	The domain to return exposures.

PARAMETER	DESCRIPTION
	You must have permission to view exposures for the domain.



< Enzoic Exposures by Domain

Additional Information

Integration Type: Feed

Version:

Accepted Data Types:

Authentication

Your Enzoic API credentials are located in the console, within the "API" product section.

API Key

Enter your API Key to authenticate with the Enzoic API.

API Secret

Enter your API Secret to authenticate with the Enzoic API.

Data Filtering

The following options will give you more control over the data that is ingested from the Enzoic API

Account Domain

The domain to return exposures for (e.g. "enzoic.com"). You must have permissions to view exposures for this domain.

☑ Require Exposed Password

Check this box to only ingest exposures that contain a password.

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.

ThreatQ Mapping

Enzoic Exposures

The Enzoic Exposures feed ingests all public Exposures from the Enzoic API.

`GET https://api.enzoic.com/v1/exposures-by-date`

Sample Response:

```
{
  "count": 3,
  "pagingToken": null,
  "exposures": [
    {
      "category": "Unspecified",
      "date": "2023-05-16T00:00:00.000Z",
      "dateAdded": "2023-05-16T07:02:13.000Z",
      "domainsAffected": 10,
      "entries": 60,
      "exposedData": ["Emails", "Passwords"],
      "id": "64632a759c64dcd3258785f0",
      "passwordType": "Cleartext",
      "source": "Messaging Services",
      "sourceFileCount": 1,
      "sourceURLs": ["telegram client"],
      "title": "Telegram File Download #2528 on Channel #-1001780683792"
    },
    {
      "category": "Unspecified",
      "date": "2023-05-16T00:00:00.000Z",
      "dateAdded": "2023-05-16T10:54:30.000Z",
      "domainsAffected": 2,
      "entries": 59,
      "exposedData": ["Emails", "Passwords"],
      "id": "646360e61368b1a3e91333f8",
      "passwordType": "Cleartext",
      "source": "Messaging Services",
      "sourceFileCount": 1,
      "sourceURLs": [],
      "title": "Telegram Message #45216 on Channel #-1001227389993"
    },
    {
      "category": "Unspecified",
      "date": "2023-05-16T00:00:00.000Z",
      "dateAdded": "2023-05-16T13:08:57.000Z",
      "domainsAffected": 4,
      "entries": 9,
      "exposedData": ["Emails", "Passwords"],
      "id": "646380694b721434189ae7e5",
      "passwordType": "Cleartext",
      "source": "Messaging Services",
      "sourceFileCount": 1,
      "sourceURLs": [],
      "title": "Telegram File Download #2531 on Channel #-1001780683792"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

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

Enzoic Exposures by Domain

The Enzoic Exposures by Domain feed ingests all Exposures & users for a specified domain, from the Enzoic API.

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

Sample Response:

```
{
  "count": 1,
  "pagingToken": "598e5b844eb6d82ea07c5783",
  "users": [
    {
      "username": "sample@email.tst",
      "exposures": ["57dc11964d6db21300991b78"]
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

> The majority of the mapping for this feed will be under the **Enzoic Exposure by ID** supplemental feed.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES	
`.users[].username`	Identity.Value	N/A	N/A	N/A	N/A	N/A
N/A	Identity.Attribute	Is Exposed	N/A	N/A	`true`	N/A

Enzoic Exposures by ID Supplemental

The Enzoic Exposures by ID supplemental feed fetches a given Exposure by ID from the Enzoic API.

`GET https://api.enzoic.com/v1/exposure-details?id={ exposure_id }`

Sample Response:

```
{
  "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 feed:

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

Average Feed Run

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

Enzoic Exposures

METRIC	RESULT
Run Time	1 minute
Events	3
Event Attributes	21

Enzoic Exposures by Domain

METRIC	RESULT
Run Time	1 minute
Identities	3
identity Attributes	3
Events	3
Event Attributes	21

Known Issues / Limitations

- **Enzoic Exposures -** due to an Enzoic API limitation, the exposure feed can only return exposures found in the past 30 days.

Change Log

- **Version 1.0.0**
    - Initial release