ThreatQuotient

Zvelo CDF User Guide

Version 1.1.0

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	1.1.0
Compatible with ThreatQ Versions	>= 4.27.0
Support Tier	ThreatQ Supported

Introduction

The Zvelo CDF provides contextual datasets, premium phishing and malicious threat intelligence.

The integration provides the following feeds:

- **Zvelo PhishBlocklist** - ingests phishing threats from Zvelo that are enriched with additional metadata attributes.
- **Zvelo Malicious Detailed Detection** - ingests malicious threat intelligence data from Zvelo that is enriched with additional metadata attributes.
- **Zvelo Threats** - ingests malicious IoCs from Zvelo, that are enriched with additional metadata attributes.

The integration ingests the following system objects:

- Indicators
    - Indicator Attributes

Prerequisites

The Zvelo CDF requires the following:

- Zvelo API Client ID
- Zvelo Client Secret

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.

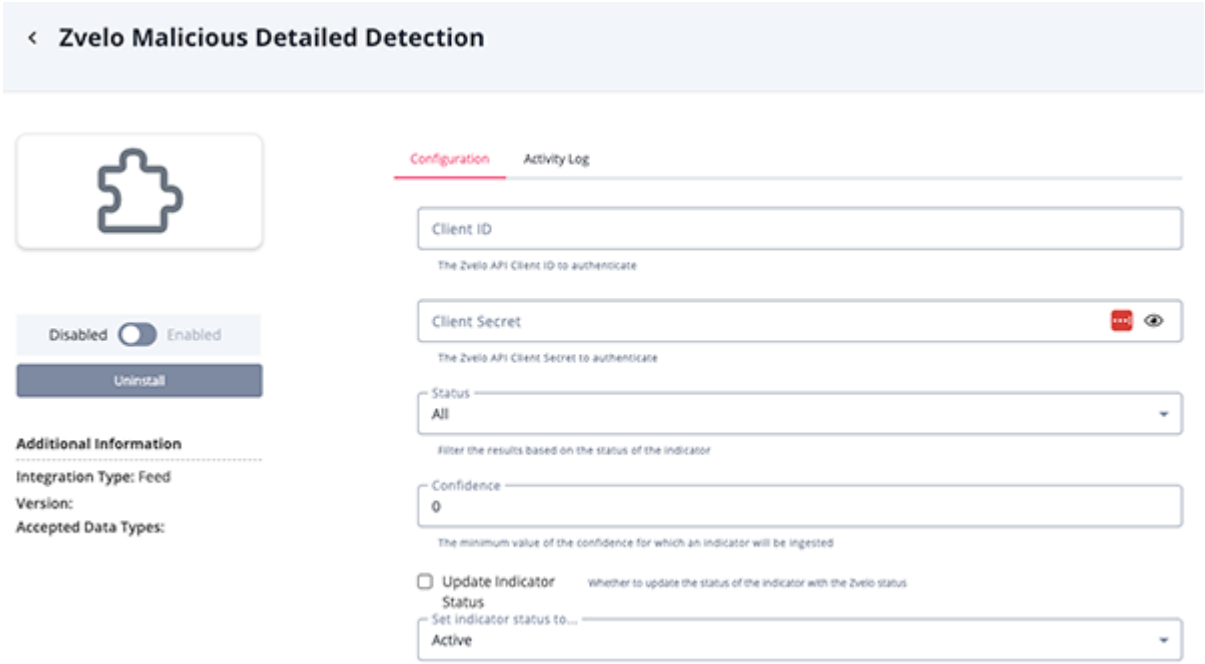
To configure the integration:

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
Client ID	Your Zvelo API Client ID to authenticate.
Client Secret	Your Zvelo API Client Secret to authenticate.
Status	Filter the results based on the status of the indicator. Options include: ◦ All (default) ◦ Active ◦ Inactive
Confidence	The minimum value of the confidence for which an indicator will be ingested. The default value for this parameter is **0**.
Update Indicator Status	Select whether to update the status of the indicator with the Zvelo status. This parameter is disabled by default. See the Known Issues section for further details on this parameter option.



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

Zvelo PhishBlocklist

The Zvelo PhishBlocklist feed ingests phishing threats from Zvelo, that are enriched with additional metadata attributes.

```
GET https://api.zvelo.io/v1/phish
```


```
{
    "_meta": {
        "version": "1",
        "request_id": "2RHnGMyFWZJla85CRRigTAxdvMb",
        "generated_at": "2023-06-16T11:42:57.666041272Z",
        "requested_query": ""
    },
    "_response_part": {
        "page_no": 1,
        "num_pages": 2
    },
    "phish_info": {
        "phish": [
            {
                "ip_info": [
                    {
                        "ip": "2606:4700::6812:375"
                    },
                    {
                        "ip": "104.18.3.117"
                    }
                ],
                "url": "http://uspssitechange.com/",
                "discovered_date": "2023-06-16T11:12:49Z",
                "brand": "usps",
                "confidence_level": 80,
                "last_active_date": "2023-06-16T11:12:49Z",
                "status": "inactive",
                "last_verified_date": "2023-06-16T11:38:47.625155Z"
            }
        ]
    }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.phish_info.phish[].url	Indicator.Value	URL	.phish_info.phish[].discovered_date	http://uspssitechange.com/	N/A
.phish_info.phish[].ip_info[].ip	Related Indicator.Value	IP Address / IPv6 Address	.phish_info.phish[].discovered_date	104.18.3.117	N/A
.phish_info.phish[].brand	Indicator.Attribute, Related Indicator.Attribute	Brand	.phish_info.phish[].discovered_date	usps	N/A
.phish_info.phish[].confidence_level	Indicator.Attribute, Related Indicator.Attribute	Confidence Level	.phish_info.phish[].discovered_date	80	N/A
.phish_info.phish[].last_active_date	Indicator.Attribute, Related Indicator.Attribute	Last Active Date	.phish_info.phish[].discovered_date	2023-06-16T11:12:49Z	The attribute value is updated at ingestion
.phish_info.phish[].last_verified_date	Indicator.Attribute, Related Indicator.Attribute	Last Verified Date	.phish_info.phish[].discovered_date	2023-06-16T11:38:47.625155Z	The attribute value is updated at ingestion

Zvelo Malicious Detailed Detection

The Zvelo Malicious Detailed Detection feed ingests malicious threat intelligence data from Zvelo, that is enriched with additional metadata attributes.

`GET https://api.zvelo.io/v1/malicious`


```
{
    "_meta": {
        "version": "1",
        "request_id": "2RQLffZwjb3WIPVmNUlhWecTHue",
        "generated_at": "2023-06-19T12:24:22.717062214Z",
        "requested_query": ""
    },
    "_response_part": {
        "page_no": 0,
        "num_pages": 1
    },
    "malicious_info": {
      "malicious": [
            {
                "ip_info": [
                    {
                        "ip": "117.213.42.81"
                    }
                ],
                "url": "http://117.213.42.81/Mozi.m/",
                "discovered_date": "2023-06-19T11:40:28Z",
                "confidence_level": 100,
                "last_active_date": "2023-06-19T11:40:28Z",
                "status": "active",
                "last_verified_date": "2023-06-19T11:40:28.558398Z"
            }
        ]
    }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.phish_info.phish[].url	Indicator.Value	URL	.phish_info.phish[].discovered_date	http://uspssitechange.com/	N/A
.phish_info.phish[].ip_info[].ip	Related Indicator.Value	IP Address / IPv6 Address	.phish_info.phish[].discovered_date	104.18.3.117	N/A
.phish_info.phish[].brand	Indicator.Attribute, Related Indicator.Attribute	Brand	.phish_info.phish[].discovered_date	usps	N/A
.phish_info.phish[].confidence_level	Indicator.Attribute, Related Indicator.Attribute	Confidence Level	.phish_info.phish[].discovered_date	80	N/A
.phish_info.phish[].last_active_date	Indicator.Attribute, Related Indicator.Attribute	Last Active Date	.phish_info.phish[].discovered_date	2023-06-16T11:12:49Z	The attribute value is updated at ingestion
.phish_info.phish[].last_verified_date	Indicator.Attribute, Related Indicator.Attribute	Last Verified Date	.phish_info.phish[].discovered_date	2023-06-16T11:38:47.625155Z	The attribute value is updated at ingestion

Zvelo Threats

The Zvelo Threats feed ingests threats (IOCs) from Zvelo's API. These IOCs may be phishing URLs, C2 servers, or other types of threats.

```
GET https://api.zvelo.io/v1/threat
```


```
{
  "_meta": {
    "version": "1",
    "request_id": "2VGItRIlDpUxCicOiWhCCXxGZD1",
    "generated_at": "2023-09-11T18:16:44.427844289Z",
    "requested_query": ""
  },
  "_response_part": {
    "page_no": 0,
    "num_pages": 1
  },
  "threat_info": {
    "threat": [
      {
        "id": "bb5793b2-25dd-436b-b3b8-9c87836da1c7",
        "ioc": "39.105.50.248:443",
        "ioc_type": "ip",
        "threat_type": "command and control",
        "malware_family": "covenant",
        "ip_info": [
          {
            "ip": "39.105.50.248"
          }
        ],
        "discovered_date": "2022-08-04T09:02:19Z",
        "confidence_level": 100,
        "last_active_date": "2023-09-11T05:07:24Z",
        "status": "active",
        "last_verified_date": "2023-09-11T05:07:24Z",
        "updated_at": "2023-09-11T05:08:57.248228Z",
        "action": "u"
      }
    ]
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.ioc	Indicator.Value	Based on `.ioc_type` value	.discovered_date	`39.105.50.248`	N/A
.ip_info[].ip	Related Indicator.Value	IP Address / IPv6 Address	.discovered_date	N/A	N/A
.malware_family	Indicator.Attribute, Related Indicator.Attribute	Malware Family	.discovered_date	`covenant`	N/A
.confidence	Indicator.Attribute, Related Indicator.Attribute	Confidence	.discovered_date	`100`	N/A
.threat_type	Indicator.Attribute, Related Indicator.Attribute	Threat Type	.discovered_date	`command and control`	N/A
.last_active_date	Indicator.Attribute, Related Indicator.Attribute	Last Active Date	.discovered_date	2023-09-11T05:07:24Z	The attribute value is updated at ingestion
.last_verified_date	Indicator.Attribute, Related Indicator.Attribute	Last Verified Date	.discovered_date	2023-09-11T05:07:24Z	The attribute value is updated at ingestion
.updated_at	Indicator.Attribute, Related Indicator.Attribute	Updated At	.discovered_date	2023-09-11T05:08:57.248228Z	The attribute value is updated at ingestion

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.

Zvelo PhishBlocklist

METRIC	RESULT
Run Time	1 minute
Indicators	170
Indicator Attributes	1,019

Zvelo Malicious Detailed Detection

METRIC	RESULT
Run Time	1 minute
Indicators	87
Indicator Attributes	409

Zvelo Threats

METRIC	RESULT
Run Time	1 minute
Indicators	873
Indicator Attributes	6,499

Known Issues / Limitations

- The **Run Frequency** should be set to **Hourly** as the Zvelo API limits the time range to an hour.
- In order for the **Status of the Indicator** to be updated, confirm that the Active status is not **protected from feed override**. This can be set from the **Object Management** page on your ThreatQ instance.

Change Log

- **Version 1.1.0**
  - Added new feed: **Zvelo Threats**.
- **Version 1.0.0**
  - Initial release