ThreatQuotient

ZeroFox CDF

Version 1.2.0

October 07, 2024

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	1.2.0
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The ZeroFox integration allows a ZeroFox user to ingest campaigns and indicators from ZeroFox. Ingested intelligence can be filtered down by privacy level (for campaigns), and threat level (for indicators).

The integration provides the following feeds:

- **ZeroFox Alerts** - ingests new Event objects and related Indicators.
- **ZeroFox Campaigns** - ingests new Campaign objects and related Indicators.
- **ZeroFox Indicators** - ingests new Indicator objects.

The following system object types are ingested by the integration:

- Events
  - Event Attributes
- Campaigns
  - Campaign Attributes
- Indicators
  - Indicator 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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the 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. Select the individual feeds to install, when prompted, and click **Install**. The feed(s) 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).

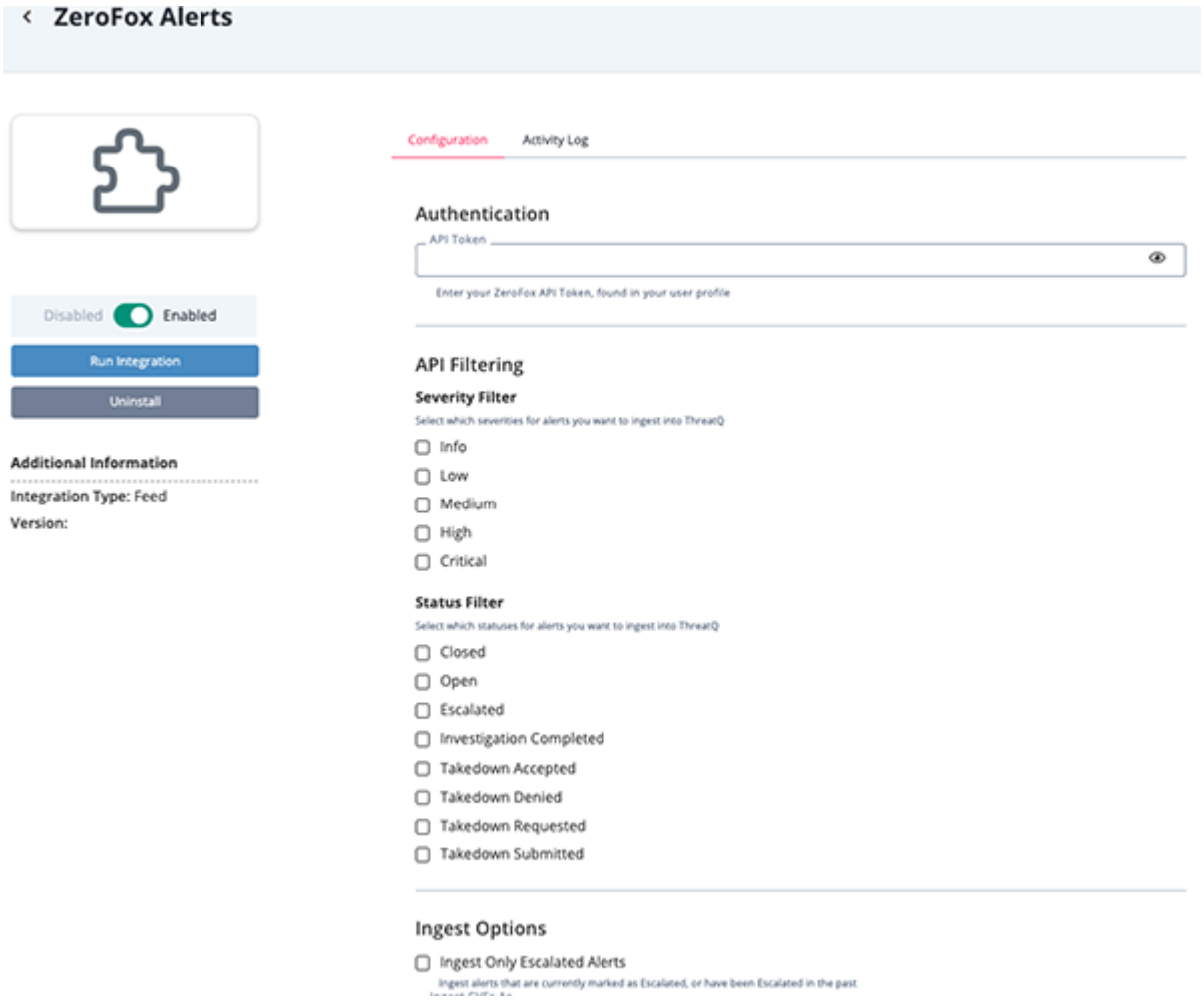
   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

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

ZeroFox Alerts

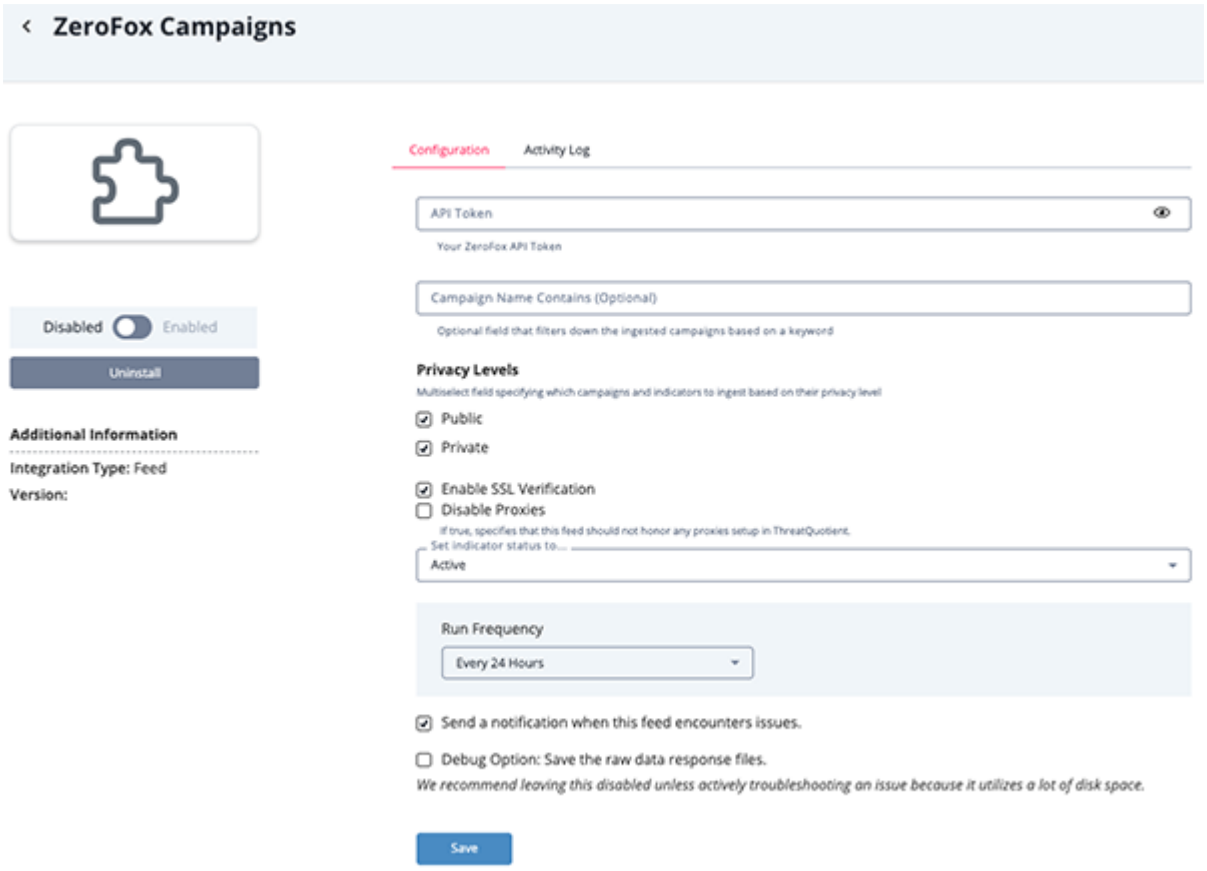
PARAMETER	DESCRIPTION
API Token	Your ZeroFox API Token.
Severity Filter	Specify which alerts to ingest based on their severity levels. Options include: ◦ Info ◦ Low ◦ Medium ◦ High ◦ Critical
Status Filter	Specify which alerts to ingest based on their status. Options include: ◦ Closed ◦ Open ◦ Escalated ◦ Investigation Completed ◦ Takedown Accepted ◦ Takedown Denied ◦ Takedown Requested ◦ Takedown Submitted

PARAMETER	DESCRIPTION
Ingest Only Escalated Alerts	Enable this option to ingest alerts that are currently marked as Escalated, or have been Escalated in the past.
Ingest CVEs As	Select which entity type to ingest CVEs as in the ThreatQ platform. Options include: ◦ Vulnerabilities (default) ◦ Indicators (Type: CVE)
Context Filter	Select which pieces of context to ingest with each alert. This allows you pick and choose what your organization needs to see with each alert, leaving out anything that isn't relevant. Options include: ◦ Alert Type (default) ◦ Tags (default) ◦ Assignee (default) ◦ Dark Web Term (default) ◦ Entity Term (default) ◦ Escalated (default) ◦ Reviewed (default) ◦ Network Source (default) ◦ Notes (default) ◦ Alert Review (default) ◦ Rule Name (default) ◦ Status (default) ◦ Severity (default) ◦ Targeted Entity (default) ◦ Targeted Asset (default) ◦ Targeted Asset Label (default) ◦ Targeted Entity Label (default) ◦ Protected Social Object ◦ Affected Products (default) ◦ Affected Vendors (default) ◦ Perpetrator Name ◦ Perpetrator Username ◦ Perpetrator Network
Enable SSL Verification	Enable this option if the feed should verify the SSL certificate.
Disable Proxies	Enable this option to have the feed ignore proxies set in the ThreatQ UI.


ZeroFox Alerts
Disabled
Enabled
Run Integration
Uninstall
Additional Information
Integration Type: Feed
Version:
Configuration
Activity Log
Authentication
API Token
Enter your ZeroFox API Token, found in your user profile
API Filtering
Severity Filter
Select which severities for alerts you want to ingest into ThreatQ
Info
Low
Medium
High
Critical
Status Filter
Select which statuses for alerts you want to ingest into ThreatQ
Closed
Open
Escalated
Investigation Completed
Takedown Accepted
Takedown Denied
Takedown Requested
Takedown Submitted
Ingest Options
Ingest Only Escalated Alerts
Ingest alerts that are currently marked as Escalated, or have been Escalated in the past

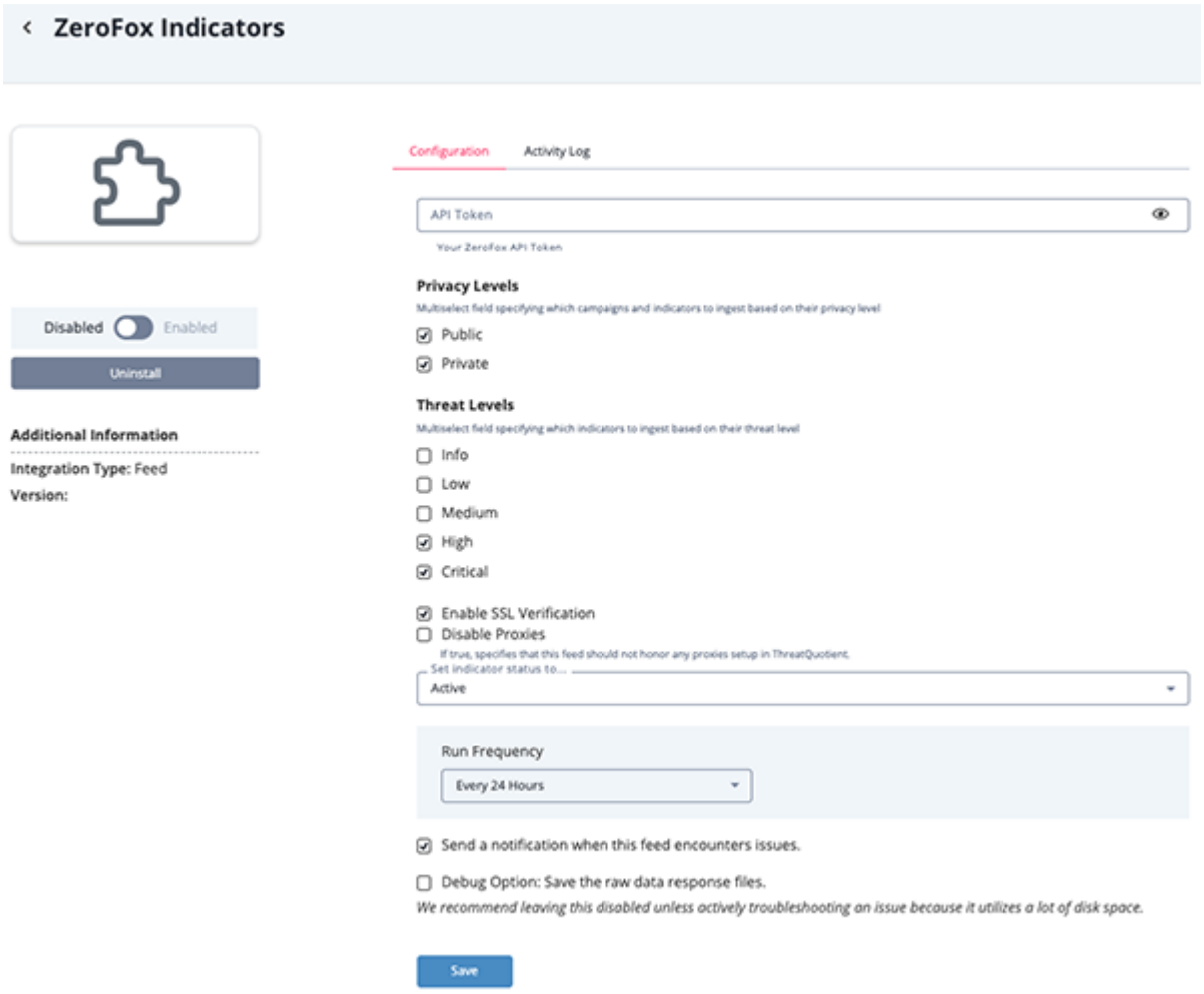
ZeroFox Campaigns

PARAMETER	DESCRIPTION
API Token	Your ZeroFox API Token.
Campaign Name Contains (Optional)	Optional field to allow you to filter down the ingested campaigns based on a keyword.
Privacy Levels	Specify which campaigns or indicators to ingest based on their privacy level. Options include **Public** and **Private**.
Enable SSL Verification	Enable this option if the feed should verify the SSL certificate.
Disable Proxies	Enable this option to have the feed ignore proxies set in the ThreatQ UI.


ZeroFox Campaigns
Disabled
Enabled
Uninstall
Additional Information
Integration Type: Feed
Version:
Configuration
Activity Log
API Token
Your ZeroFox API Token
Campaign Name Contains (Optional)
Optional field that filters down the ingested campaigns based on a keyword
Privacy Levels
Multiselect field specifying which campaigns and indicators to ingest based on their privacy level
Public
Private
Enable SSL Verification
Disable Proxies
If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.
Set Indicator status to...
Active
Run Frequency
Every 24 Hours
Send a notification when this feed encounters issues.
Debug Option: Save the raw data response files.
We recommend leaving this disabled unless actively troubleshooting an issue because it utilizes a lot of disk space.
Save

ZeroFox Indicators

PARAMETER	DESCRIPTION
API Token	Your ZeroFox API Token.
Privacy Levels	Specify which campaigns or indicators to ingest based on their privacy level. Options include **Public** and **Private**.
Threat Levels	Specify which indicators to ingest based on their threat level. Option include: ◦ Info ◦ Low ◦ Medium ◦ High ◦ Critical
Enable SSL Verification	Enable this option if the feed should verify the SSL certificate.
Disable Proxies	Enable this option to have the feed ignore proxies set in the ThreatQ UI.



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

ZeroFox Alerts (Feed)

This feed automatically pulls brand alerts from the ZeroFox API.

`GET https://api.zerofox.com/1.0/alerts`

Sample Response:


```
{
    "count": 5,
    "next": null,
    "previous": null,
    "page_size": 100,
    "num_pages": 1,
    "alerts": [
        {
            "alert_type": "search query",
            "logs": [
                {
                    "id": 238682352,
                    "timestamp": "2021-09-28T17:36:48+00:00",
                    "actor": "ZeroFox Platform Specialist",
                    "subject": "",
                    "action": "cancel takedown"
                },
                {
                    "id": 228353522,
                    "timestamp": "2021-08-18T04:36:52+00:00",
                    "actor": "api_metronlabs",
                    "subject": "",
                    "action": "request takedown"
                }
            ],
            "offending_content_url": "http://acme-corporation.com",
            "asset_term": null,
            "assignee": "Kishaas",
            "entity": {
                "id": 1163869,
                "name": "Acme Corporation",
                "image": "https://cdn.zerofox.com/media/entityimages/
rl2rybmrht5k7890b3g93i7sifh9epsupwe2xmy5h82jyvf8dtnzbwnbr20n2eri.jpg",
                "labels": [
                    {
                        "id": 2036277,
                        "name": "Brand"
                    }
                ],
```

```
                "entity_group": {
                    "id": 6397,
                    "name": "Default"
                }
            },
            "entity_term": null,
            "content_created_at": "2021-04-21T18:05:16+00:00",
            "id": 135985017,
            "severity": 4,
            "perpetrator": {
                "name": "Concealed",
                "display_name": "Concealed",
                "id": 199987205,
                "url": "http://acme-corporation.com",
                "content": "",
                "type": "page",
                "timestamp": "2021-04-21T18:05:16+00:00",
                "network": "domains",
                "username": "Jake"
            },
            "rule_group_id": 457,
            "asset": {
                "id": 1163869,
                "name": "Acme Corporation",
                "image": "https://cdn.zerofox.com/media/entityimages/
rl2rybmrht5k7890b3g93i7sifh9epsupwe2xmy5h82jyvf8dtnzbwnbr20n2eri.jpg",
                "labels": [
                    {
                        "id": 2036277,
                        "name": "Brand"
                    }
                ],
                "entity_group": {
                    "id": 6397,
                    "name": "Default"
                }
            },
            "metadata": "{\n          \"ai_confidence_display\": [\n
{\n              \"color\": \"#0072ce\",\n              \"detections\": [\n
{\n                  \"confidence\": 0.9999945766507031,\n
\"label\": \"English\"\n                }\n              ],\n
\"icon\": \"chat\",\n              \"name\": \"Language
Detection\"\n            }\n          ],\n\n          \"alert_modal\": {\n
\"a_records\": [\"web.netzerv.com A 13.58.70.70\"],\n\n
\"analysis\": 1,\"live\": true,\"mx_records\": [],\n            \"redirects\":
[\n              \"acme-corporation.com/wp-login.php?redirect_to=acme-
corporation.com\",\n              \"acme-corporation.com\"\n            ],\n
\"screenshot\": \"https://storage.restpack.io/screenshot/
0b38694ae1f34d41c4ddfda53cf6f3df9aff607b48f855276983c83c03067cee\",\n
\"whois\": \"% IANA WHOIS server\\\\n% for more information on IANA, visit
```

```
http://www.iana.org\\\\n% This query returned 1 object\\\\n\\\\nrefer:
whois.verisign-grs.com\\\\n\\\\ndomain:       COM\\\\n\\\\norganisation:
VeriSign Global Registry Services\\\\naddress:      12061 Bluemont Way\\\
\naddress:      Reston Virginia 20190\\\\naddress:      United States\\\\n\\\
\ncontact:      administrative\\\\nname:         Registry Customer Service\\\
\norganisation: VeriSign Global Registry Services\\\\naddress:      12061
Bluemont Way\\\\naddress:      Reston Virginia 20190\\\\naddress:      United
States\\\\nphone:        +1 703 925-6999\\\\nfax-no:       +1 703 948 3978\\\
\ne-mail:       info@verisign-grs.com\\\\n\\\\ncontact:      technical\\\
\nname:         Registry Customer Service\\\\norganisation: VeriSign Global
Registry Services\\\\naddress:      12061 Bluemont Way\\\\naddress:      Reston
Virginia 20190\\\\naddress:      United States\\\\nphone:        +1 703
925-6999\\\\nfax-no:       +1 703 948 3978\\\\ne-mail:       info@verisign-
grs.com\\\\n\\\\nnserver:      A.GTLD-SERVERS.NET 192.5.6.30
2001:503:a83e:0:0:0:2:30\\\\nnserver:      B.GTLD-SERVERS.NET 192.33.14.30
2001:503:231d:0:0:0:2:30\\\\nnserver:      C.GTLD-SERVERS.NET 192.26.92.30
2001:503:83eb:0:0:0:0:30\\\\nnserver:      D.GTLD-SERVERS.NET 192.31.80.30
2001:500:856e:0:0:0:0:30\\\\nnserver:      E.GTLD-SERVERS.NET 192.12.94.30
2001:502:1ca1:0:0:0:0:30\\\\nnserver:      F.GTLD-SERVERS.NET 192.35.51.30
2001:503:d414:0:0:0:0:30\\\\nnserver:      G.GTLD-SERVERS.NET 192.42.93.30
2001:503:eea3:0:0:0:0:30\\\\nnserver:      H.GTLD-SERVERS.NET 192.54.112.30
2001:502:8cc:0:0:0:0:30\\\\nnserver:      I.GTLD-SERVERS.NET 192.43.172.30
2001:503:39c1:0:0:0:0:30\\\\nnserver:      J.GTLD-SERVERS.NET 192.48.79.30
2001:502:7094:0:0:0:0:30\\\\nnserver:      K.GTLD-SERVERS.NET 192.52.178.30
2001:503:d2d:0:0:0:0:30\\\\nnserver:      L.GTLD-SERVERS.NET 192.41.162.30
2001:500:d937:0:0:0:0:30\\\\nnserver:      M.GTLD-SERVERS.NET 192.55.83.30
2001:501:b1f9:0:0:0:0:30\\\\nds-rdata:     30909 8 2
E2D3C916F6DEEAC73294E8268FB5885044A833FC5459588F4A9184CFC41A5766\\\\n\\\
\nwhois:        whois.verisign-grs.com\\\\n\\\\nstatus:       ACTIVE\\\
\nremarks:      Registration information: http://www.verisigninc.com\\\\n\\\
\ncreated:      1985-01-01\\\\nchanged:      2017-10-05\\\\nsource:       IANA\
\\\n\\\\n\\\\n\"\n          },\n\n          \"enrichment\": {\n
\"analysis-message-mapper\": {\n              \"enterpriseID\": 5031,\n
\"entityID\": 1163869,\n              \"images\": [\n                {\n
\"field\": \"content.domain.screenshot\",\n                \"item\":
\"https://storage.restpack.io/screenshot/
0b38694ae1f34d41c4ddfda53cf6f3df9aff607b48f855276983c83c03067cee\"\n
     }\n              ],\n              \"network\": \"domains\",\n
\"relation\": \"search_query\",\n              \"serviceOrigin\": \"analyst-
console\",\n              \"subtype\": \"unspecified\",\n
\"texts\": null,\n              \"type\": \"page\",\n              \"urls\":
null\n            },\n            \"language-detection\": {\n
\"confidence\": 0.9999961125,\n              \"detected_language\": \"en\",\n
\"detection_method\": \"languageProbability\",\n
\"language_probability\": {\n                \"en\":
0.9999961125\n              },\n              \"text\": \"acme-
corporation.com\"\n            },\n            \"nlp-utils\": {\n
\"lemmatized_and_stop_words_filter\": \"acme-corporation.com\",\n
\"nlp_model\": \"en\"\n            },\n            \"ocr-analysis\": {\n
\"data\": [\n                {\n                  \"details\": {\n
\"bounding_boxes\": [ [ [ 203, 599 ], [ 275, 618 ] ], [ [ 170, 665 ], [ 206,
```

```
679 ] ], [ [ 214, 664 ], [ 308, 683 ] ], [ [ 197, 727 ], [ 242, 740 ] ],
[ [ 247, 727 ], [ 283, 740 ] ] ],\n                    \"confidences\":
[ 0.96, 0.96, 0.96, 0.96, 0.77 ],\n                    \"height\": 900,\n
\"width\": 800,\n                    \"words\": [\n
\"Register\",\n                    \"Lost\",\n
\"password?\",\n                     \"Privacy\",\n
\"Policy\"\n                    ]\n                },\n
\"image\": \"https://storage.restpack.io/screenshot/
0b38694ae1f34d41c4ddfda53cf6f3df9aff607b48f855276983c83c03067cee\"\n
      }\n              ]\n            }\n          },\n\n
\"image_overlays\": [\n           {\n             \"image_url\": \"https://
storage.restpack.io/screenshot/
0b38694ae1f34d41c4ddfda53cf6f3df9aff607b48f855276983c83c03067cee\",\n
\"image_width\": 800,\n              \"image_height\": 650,\n
\"image_highlights\": [],\n              \"image_discovered_text\": \"Register
Lost password? Privacy Policy\"\n           }\n          ],\n\n
\"occurrences\": [\n           {\n              \"origin\": null,\n
\"term\": \"acme-corporation.com\"\n           }\n          ]\n        }",
            "status": "Open",
            "timestamp": "2021-10-04T04:55:00+00:00",
            "rule_name": "Advanced Domain Analysis - Full String Match",
            "last_modified": "2021-10-04T05:14:12Z",
            "protected_locations": null,
            "darkweb_term": null,
            "business_network": null,
            "reviewed": true,
            "escalated": true,
            "network": "domains",
            "protected_social_object": null,
            "notes": "Impersonation - Name",
            "reviews": [
                {
                    "id": 204501,
                    "label": "NOT_HELPFUL",
                    "alert": 135985017,
                    "created_by": "",
                    "timestamp": "2021-06-29T11:42:10Z"
                },
                {
                    "id": 204502,
                    "label": "IRRELEVANT",
                    "alert": 135985017,
                    "created_by": "",
                    "timestamp": "2021-06-29T11:48:17Z"
                }
            ],
            "rule_id": 38161,
            "entity_account": null,
            "entity_email_receiver_id": null,
            "tags": [
                "a-record",
```

```
                "matching-term",
                "live-domain",
                "test",
                "tag",
                "skopje"
            ]
        }
    ]
}
```

ThreatQ provides the following default mapping for this feed:

These mappings are based on the data pulled from the `alerts` list from the API response

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.alerts[].alert_type/rule_name/severity/id`	Event.Title	Alert	`.alerts[].timestamp`	`[Search Query] Inferred Vulnerability | Acme Corp | Vulnerabilities (Severity: Medium; ID: 142919722)`	Key values are concatenated to form title
`.alerts[].content_created_at`	Event.Happened_at	N/A	`.alerts[].timestamp`	`2021-04-21T18:05:16+00:00`	N/A
`.alerts[].offending_content_url`	Related Indicator.Value	URL or FQDN	`.alerts[].timestamp`	`http://acme-corporation.com`	This is not always present. Will be an FQDN if `.network == 'domains'`
`.alerts[].perpetrator.url`	Related Indicator.Value	URL	`.alerts[].timestamp`	`http://acme-corporation.com`	This is not always present
`.alerts[].tags[]`	Event.Tag	N/A	`.alerts[].timestamp`	`a-record`	Configurable
`.alerts[].perpetrator.name`	Event.Attribute	Perpetrator Name	`.alerts[].timestamp`	`Concealed`	Configurable
`.alerts[].perpetrator.username`	Event.Attribute	Perpetrator Username	`.alerts[].timestamp`	`Jake`	Configurable
`.alerts[].perpetrator.network`	Event.Attribute	Perpetrator Network	`.alerts[].timestamp`	`domains`	Configurable
`.alerts[].alert_type`	Event.Attribute	Alert Type	`.alerts[].timestamp`	`search query`	Configurable
`.alerts[].assignee`	Event.Attribute	Assignee	`.alerts[].timestamp`	`Kishaas`	Updatable, Configurable
`.alerts[].darkweb_term`	Event.Attribute	Dark Web Term	`.alerts[].timestamp`	N/A	Configurable
`.alerts[].entity_term`	Event.Attribute	Entity Term	`.alerts[].timestamp`	N/A	Configurable

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.alerts[].escalated`	Event.Attribute	Escalated	`.alerts[].timestamp`	`True`	Mapped to `True` or `False`, Updatable, Configurable
`.alerts[].reviewed`	Event.Attribute	Reviewed	`.alerts[].timestamp`	`False`	Mapped to `True` or `False`, Updatable, Configurable
`.alerts[].network`	Event.Attribute	Network Source	`.alerts[].timestamp`	`domains`	Configurable
`.alerts[].notes`	Event.Attribute	Note	`.alerts[].timestamp`	`Impersonation - Name`	Configurable
`.alerts[].reviews.label`	Event.Attribute	Alert Review	`.alerts[].timestamp`	`NOT_HELPFUL`	Configurable
`.alerts[].rule_name`	Event.Attribute	Rule Name	`.alerts[].timestamp`	`Advanced Domain Analysis - Full String Match`	Configurable
`.alerts[].severity`	Event.Attribute	Severity	`.alerts[].timestamp`	`4`	Mapped to string-value, Configurable
`.alerts[].status`	Event.Attribute	Status	`.alerts[].timestamp`	`Open`	Updatable, Configurable
`.alerts[].entity.name`	Event.Attribute	Targeted Entity	`.alerts[].timestamp`	`Acme Corporation`	Configurable
`.alerts[].asset.name`	Event.Attribute	Targeted Asset	`.alerts[].timestamp`	`Acme Corporation`	Configurable
`.alerts[].asset.labels.name`	Event.Attribute	Targeted Asset Label	`.alerts[].timestamp`	`Brand`	Configurable
`.alerts[].entity.labels.name`	Event.Attribute	Targeted Entity Label	`.alerts[].timestamp`	`Brand`	Configurable
`.alerts[].protected_social_object`	Event.Attribute	Protected Social Object	`.alerts[].timestamp`	N/A	Configurable
`.alerts[].metadata.alert_reasons[].value.text_content`	Event.Attribute	Affected Product	`.alerts[].timestamp`	`adobe_flashplayer`	When the alert reason type is `Product`, Configurable
`.alerts[].metadata.alert_reasons[].value.text_content`	Event.Attribute	Affected Vendor	`.alerts[].timestamp`	`google`	When the alert reason type is `Vendor`, Configurable
`.alerts[].metadata.alert_reasons[].value.text_content`	Event.Vulnerability	N/A	`.alerts[].timestamp`	`CVE-2024-12345`	When the alert reason type is `Vulnerability Name`

Severity Map

METRIC	VALUE
1	Info
2	Low
3	Medium
4	High
5	Critical

ZeroFox Campaigns (Feed)

This feed will ingest campaigns and indicators from ZeroFox's API.

`GET https://tg-api.zerofox.com/campaigns`

Sample Response:


```
{
  "next": null,
  "previous": null,
  "results": [
    {
      "id": 115,
      "name": "Phishing Domains - Apple and Amazon",
      "privacy_level": "public",
      "description": "Phishing Domains - Apple and Amazon",
      "url_descriptions": [],
      "created_at": "2019-12-03T20:13:39.593334Z",
      "updated_at": "2019-12-03T20:13:39.593355Z"
    },
    {
      "id": 114,
      "name": "Amazon India Phishing Site",
      "privacy_level": "public",
      "description": "Amazon India Impersonator Site",
      "url_descriptions": [],
      "created_at": "2019-12-03T18:20:13.473048Z",
      "updated_at": "2019-12-03T18:20:13.473076Z"
    }
  ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
results[].name	Campaign.Value	N/a	results[].created_at	Phishing Domains - Apple and Amazon	N/A
results[].description	Campaign.Description	N/A	results[].created_at	Amazon India Impersonator Site	N/A
results[].privacy_level	Campaign.Attribute	Privacy Level	results[].created_at	Public	Converted to title casing

Get Related Indicators (Supplemental)

This supplemental feed will ingest only indicators related to ingested campaigns.

`GET https://tg-api.zerofox.com/campaigns/{id}/list_indicators`


```
{
  "next": null,
  "previous": null,
  "results": [
    {
      "id": 2404244,
      "indicator_type": "non-social",
      "value": "http://109.230.199.227",
      "network": "all",
      "classifications": [],
      "campaigns": [
        {
          "id": 105,
          "name": "Cybercriminal Group FIN7 Updates Toolset",
          "privacy_level": "public",
          "description": "FIN7, a notorious cybercriminal group with
significant resources that target the retail, restaurant and hotel industries,
has been deploying new tools within their arsenal. Incident responders at
FireEye's Mandiant released a post outlining two new tools - dubbed RDFSNIFFER
and BOOSTWRITE. BOOSTWRITE is an in memory dropper for malware, and RDFSNIFFER
is a malicious DLL that hijacks a remote administration client built by NCR
Corporation.",
          "url_descriptions": [],
          "created_at": "2019-10-10T17:54:16.318585Z",
          "updated_at": "2019-10-10T17:54:16.318615Z"
        }
      ],
      "privacy_level": "public",
      "created_at": "2019-10-10T17:59:42.701910Z",
      "updated_at": "2019-10-10T17:59:42.707703Z",
      "threat_level": "high",
      "expired": "false",
      "ttl": "2020-02-07T17:59:42.701910Z",
      "zf_alert_id": null
    },
    {
      "id": 2404243,
      "indicator_type": "file_hash_sha256",
      "value":
"18cc54e2fbdad5a317b6aeb2e7db3973cc5ffb01bbf810869d79e9cb3bf02bd5",
      "network": "all",
      "classifications": [],
      "campaigns": [
        {
```

```
          "id": 105,
          "name": "Cybercriminal Group FIN7 Updates Toolset",
          "privacy_level": "public",
          "description": "FIN7, a notorious cybercriminal group with
significant resources that target the retail, restaurant and hotel industries,
has been deploying new tools within their arsenal. Incident responders at
FireEye's Mandiant released a post outlining two new tools - dubbed RDFSNIFFER
and BOOSTWRITE. BOOSTWRITE is an in memory dropper for malware, and RDFSNIFFER
is a malicious DLL that hijacks a remote administration client built by NCR
Corporation.",
          "url_descriptions": [],
          "created_at": "2019-10-10T17:54:16.318585Z",
          "updated_at": "2019-10-10T17:54:16.318615Z"
        }
      ],
      "privacy_level": "public",
      "created_at": "2019-10-10T17:59:21.140847Z",
      "updated_at": "2019-10-10T17:59:21.146710Z",
      "threat_level": "high",
      "expired": "false",
      "ttl": "2020-02-07T17:59:21.140847Z",
      "zf_alert_id": null
    }
  ]
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
results[].indicator_type	Indicator.Type	SHA-256	results[].created_at	file_hash_sha256	This will be mapped
results[].value	Indicator.Value	N/A	results[].created_at	http://109.230.199.227	N/A
results[].classifications[].name	Indicator.Attribute	Classification	results[].created_at	Domain	For each item in array
results[].privacy_level	Indicator.Attribute	Privacy Level	results[].created_at	Private	Converted to title casing
results[].threat_level	Indicator.Attribute	Threat Level	results[].created_at	High	Converted to title casing
results[].zf_alert_id	Indicator.Attribute	ZeroFox Alert ID	results[].created_at	12345	This can be null

ZeroFox Indicators (Feed)

This feed will ingest indicators from ZeroFox's API.

`GET https://tg-api.zerofox.com/indicators`

Sample Response:


```
{
  "next": "https://tg-api.zerofox.com/indicators/?
cursor=cD0yMDE5LTEyLTA1KzE0JTNBMDAlM0ExMy43MzY1NDUlMkIwMCUzQTAw",
  "previous": null,
  "results": [
    {
      "id": 2550745,
      "indicator_type": "non-social",
      "value": "http://43.247.68.165/",
      "network": "all",
      "classifications": [
        {
          "id": 73,
          "name": "Twitter - Phishing Listener",
          "privacy_level": "public",
          "created_at": "2018-07-16T16:01:25.636504Z",
          "updated_at": "2018-07-16T16:01:25.636522Z"
        }
      ],
      "campaigns": [],
      "privacy_level": "public",
      "created_at": "2019-12-05T15:31:20.925689Z",
      "updated_at": "2019-12-05T15:31:20.929551Z",
      "threat_level": "medium",
      "expired": "false",
      "ttl": "2020-04-03T15:31:20.925689Z"
    }
  ]
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
results[].indicator_type	Indicator.Type	SHA-256	results[].created_at	file_hash_sha256	View indicator mapping table below
results[].value	Indicator.Value	N/A	results[].created_at	http://109.230.199.227	N/A
results[].classifications[].name	Indicator.Attribute	Classification	results[].created_at	Domain	For each item in array
results[].privacy_level	Indicator.Attribute	Privacy Level	results[].created_at	Private	Converted to title casing
results[].threat_level	Indicator.Attribute	Threat Level	results[].created_at	High	Converted to title casing
results[].expired	Indicator.Attribute	Is Expired	results[].created_at	False	Mapped to `True` or `False`

Indicator Type Mapping

Mapped (ZeroFox -> ThreatQ):

PROVIDER FIELD VALUE	THREATQ FIELD VALUE
non-social	URL
email	Email Address
file_hash_md5	MD5
file_hash_sha1	SHA-1
file_hash_sha256	SHA-256
ipv4_address	IP Address
domain	FQDN

Unmapped:

PROVIDER FIELD VALUE	VALUE
profile	Twitter profiles, forum profiles, etc.
post	Twitter posts, forum posts, etc.
page	Facebook pages
hashtag	Twitter hashtags
phonenumber	Phone numbers
btc_wallet	BTC wallet IDs

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.

ZeroFox Alerts

METRIC	RESULT
Run Time	1 min
Events	5
Event Attributes	60
Indicators	5

ZeroFox Campaigns and Get Related Indicators

METRIC	RESULT
Run Time	3 mins
Campaign	6
Campaign Attributes	12
Indicators	3,184
Indicator Attributes	9,571

ZeroFox Indicators

METRIC	RESULT
Run Time	1 min
Indicators	185
Indicator Attributes	926

Known Issues / Limitations

- Depending on whether you are ingesting public or private data, files may be downloaded, even if no data is ingested. This is because the public/private filtering happens at the integration code level instead of the API level.
- The ZeroFox Alerts feed may not take the same API key as the other feeds

Change Log

- **Version 1.2.0**
  - Added the following configuration parameters to all feeds: **Enable SSL Verification** and **Disable Proxies**.
  - Added the following configuration parameters to the ZeroFox Alerts feed:
    - **Only Ingest Escalated Alerts** - only ingest alerts marked as escalated or have been escalated in the past.
    - **Ingest CVEs As** - select how to ingest CVEs.
    - **Context Filter** - select the pieces of context to ingest with each alert.
  - Performed the following updates to the ZeroFox Alerts feed:
    - Improved the Event Title attribute to contain the following additional information:
      - Target Asset/Entity
      - Source Network
    - Added HTML rich text descriptions to the Event objects.
    - The following attributes will now be included in the description:
      - Offending Content URL
      - Perpetrator URL
      - Perpetrator Type
    - Added the ability to:
      - extract and relate vulnerabilities (CVEs) from the alert metadata.
      - extract affected products/vendors from the alert metadata into attributes.
      - extract compromised account credentials from the alert metadata into the description.
    - Added the ability to update single-value attributes.
    - The perpetrator URL will no longer be added as a related indicator.
    - The Offending content URL will no longer be added as a related indicator if it's a ZeroFox URL.
    - The ZeroFox Alert Link attribute has been moved to the description as a hyperlink.
    - Added better handling for situations where there are multiple notes in an alert.
    - Multiple notes will now be divided into multiple attributes.
  - Updated the minimum ThreatQ version to 5.12.1.
- **Version 1.1.2**
  - Resolved an issue where users encountered a `TypeError ('Cannot parse argument of type None.')` error.
- **Version 1.1.1**
  - Updated the integration for improved handle incomplete metadata JSON responses and the offending content URL field.
- **Version 1.1.0**
  - Added ZeroFox Alerts feed.
- **Version 1.0.0**
  - Initial Release