

ThreatQuotient



ZeroFox CDF Guide

Version 1.1.0

July 05, 2022

ThreatQuotient

11400 Commerce Park Dr., Suite 200
Reston, VA 20191

 ThreatQ Supported

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

Contents

Support	4
Versioning.....	5
Introduction	6
Installation Guide	7
Configuration	8
ThreatQ Mapping	10
ZeroFox Alerts (Feed).....	10
ZeroFox Campaigns (Feed)	15
Get Related Indicators (Supplemental).....	15
ZeroFox Indicators (Feed)	17
Indicator Type Mapping	18
Average Feed Runs.....	20
Known Issues/Limitations	22
Change Log.....	23

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.

Copyright © 2022 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

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.

Versioning

- Current integration version: 1.1.0
- Supported on ThreatQ versions $\geq$ 4.50.0

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 Guide

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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

ZeroFox - ALL Feeds

PARAMETER	DESCRIPTION
-----------	-------------

API Token	Your ZeroFox API Token.
-----------	-------------------------

ZeroFox Alerts

PARAMETER	DESCRIPTION
-----------	-------------

Severity Filter	Specify which alerts to ingest based on their severity levels.
-----------------	--

Status Filter	Specify which alerts to ingest based on their status.
---------------	---

ZeroFox Campaigns

PARAMETER	DESCRIPTION
-----------	-------------

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

ZeroFox Indicators**PARAMETER****DESCRIPTION****Privacy Levels**

Specify which campaigns or indicators to ingest based on their privacy level.

Threat Levels

Specify which indicators to ingest based on their threat level.

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>

```
{
  "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/r12rybmrht5k7890b3g93i7sifh9epsupwe2xmy5h82jyvf8dtznzbnbr20n2eri.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",
    }
  ]
}
```

[illegible]

```

\"entityID\": 1163869,\n          \"images\": [\n          {\n          \"field\":\n          \"content.domain.screenshot\", \n          \"item\": \"https://storage.restpack.io/screenshot/\n          0b38694ae1f34d41c4ddfd53cf6f3df9aff607b48f855276983c83c03067cee\" \n          }, \n          \"network\": \"domains\", \n          \"relation\": \"search_query\", \n          \"serviceOrigin\": \"analyst-\n          console\", \n          \"subtype\": \"unspecified\", \n          \"texts\": null, \n          \"type\":\n          \"page\", \n          \"urls\": null \n          }, \n          \"language-detection\": {\n          \"confidence\": 0.9999961125, \n          \"detected_language\": \"en\", \n          \"detection_method\":\n          \"languageProbability\", \n          \"language_probability\": {\n          \"en\":\n          0.9999961125 \n          }, \n          \"text\": \"acme-corporation.com\" \n          }, \n          \"nlp-\n          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 ] ],\n          [ [ 170, 665 ], [ 206, 679 ] ], [ [ 214, 664 ], [ 308, 683 ] ], [ [ 197, 727 ], [ 242, 740 ] ], [ [ 247, 727 ],\n          [ 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/\n          0b38694ae1f34d41c4ddfd53cf6f3df9aff607b48f855276983c83c03067cee\" \n          }, \n          \"image_overlays\": [\n          {\n          \"image_url\":\n          \"https://storage.restpack.io/screenshot/0b38694ae1f34d41c4ddfd53cf6f3df9aff607b48f855276983c83c03067cee\", \n          \"image_width\": 800, \n          \"image_height\": 650, \n          \"image_highlights\": [], \n          \"image_discovered_text\": \"Register Lost password? Privacy Policy\" \n          }, \n          \"occurrences\": [\n          {\n          \"origin\": null, \n          \"term\": \"acme-\n          corporation.com\" \n          }, \n          ],\n          \"status\": \"Open\", \n          \"timestamp\": \"2021-10-04T04:55:00+00:00\", \n          \"rule_name\": \"Advanced Domain Analysis - Full String Match\", \n          \"last_modified\": \"2021-10-04T05:14:12Z\", \n          \"protected_locations\": null, \n          \"darkweb_term\": null, \n          \"business_network\": null, \n          \"reviewed\": true, \n          \"escalated\": true, \n          \"network\": \"domains\", \n          \"protected_social_object\": null, \n          \"notes\": \"Impersonation - Name\", \n          \"reviews\": [\n          {\n          \"id\": 204501, \n          \"label\": \"NOT_HELPFUL\", \n          \"alert\": 135985017, \n          \"created_by\": \"\", \n          \"timestamp\": \"2021-06-29T11:42:10Z\" \n          }, \n          {\n          \"id\": 204502, \n          \"label\": \"IRRELEVANT\", \n          \"alert\": 135985017, \n          \"created_by\": \"\", \n          \"timestamp\": \"2021-06-29T11:48:17Z\" \n          }\n          ], \n          \"rule_id\": 38161, \n          \"entity_account\": null, \n          \"entity_email_receiver_id\": null, \n          \"tags\": [\n          \"a-record\", \n          \"matching-term\", \n          \"live-domain\", \n          \"test\", \n          \"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
<code>.alerts[].alert_type/rule_name/severity/id</code>	Event.Title	Alert	<code>.alerts[].timestamp</code>	[Search Query] Inferred Vulnerability (Severity: Medium; ID: 142919722)	Key values are concatenated to form title
<code>.alerts[].content_created_at</code>	Event.Happened_at	N/A	<code>.alerts[].timestamp</code>	2021-04-21T18:05:16+00:00	N/A
<code>.alerts[].offending_content_url</code>	Related Indicator.Value	URL	<code>.alerts[].timestamp</code>	http://acme-corporation.com	This is not always present
<code>.alerts[].perpetrator.url</code>	Related Indicator.Value	URL	<code>.alerts[].timestamp</code>	http://acme-corporation.com	This is not always present
<code>.alerts[].tags[]</code>	Event.Tag	N/A	<code>.alerts[].timestamp</code>	a-record	N/A
<code>.alerts[].perpetrator.name</code>	Event.Attribute	Perpetrator Name	<code>.alerts[].timestamp</code>	Concealed	N/A
<code>.alerts[].perpetrator.username</code>	Event.Attribute	Perpetrator Username	<code>.alerts[].timestamp</code>	Jake	N/A
<code>.alerts[].perpetrator.url</code>	Event.Attribute	Perpetrator URL	<code>.alerts[].timestamp</code>	http://acme-corporation.com	N/A
<code>.alerts[].perpetrator.type</code>	Event.Attribute	Perpetrator Type	<code>.alerts[].timestamp</code>	page	N/A
<code>.alerts[].perpetrator.network</code>	Event.Attribute	Perpetrator Network	<code>.alerts[].timestamp</code>	domains	N/A
<code>.alerts[].alert_type</code>	Event.Attribute	Alert Type	<code>.alerts[].timestamp</code>	search query	N/A
<code>.alerts[].assignee</code>	Event.Attribute	Assignee	<code>.alerts[].timestamp</code>	Kishaas	N/A
<code>.alerts[].darkweb_term</code>	Event.Attribute	Dark Web Term	<code>.alerts[].timestamp</code>	N/A	N/A
<code>.alerts[].entity_term</code>	Event.Attribute	Entity Term	<code>.alerts[].timestamp</code>	N/A	N/A
<code>.alerts[].escalated</code>	Event.Attribute	Escalated	<code>.alerts[].timestamp</code>	True	Mapped to True or False
<code>.alerts[].reviewed</code>	Event.Attribute	Reviewed	<code>.alerts[].timestamp</code>	False	Mapped to True or False
<code>.alerts[].network</code>	Event.Attribute	Network Source	<code>.alerts[].timestamp</code>	domains	N/A
<code>.alerts[].notes</code>	Event.Attribute	Note	<code>.alerts[].timestamp</code>	Impersonation - Name	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>.alerts[].reviews.label</code>	Event.Attribute	Alert Review	<code>.alerts[].timestamp</code>	NOT_HELPFUL	N/A
<code>.alerts[].rule_name</code>	Event.Attribute	Rule Name	<code>.alerts[].timestamp</code>	Advanced Domain Analysis - Full String Match	N/A
<code>.alerts[].severity</code>	Event.Attribute	Severity	<code>.alerts[].timestamp</code>	4	Mapped to string-value
<code>.alerts[].status</code>	Event.Attribute	Status	<code>.alerts[].timestamp</code>	Open	N/A
<code>.alerts[].entity.name</code>	Event.Attribute	Targeted Entity	<code>.alerts[].timestamp</code>	Acme Corporation	N/A
<code>.alerts[].asset.name</code>	Event.Attribute	Targeted Asset	<code>.alerts[].timestamp</code>	Acme Corporation	N/A
<code>.alerts[].offending_content_url</code>	Event.Attribute	Offending Content URL	<code>.alerts[].timestamp</code>	http://acme-corporation.com	N/A
<code>.alerts[].asset.labels.name</code>	Event.Attribute	Targeted Asset Label	<code>.alerts[].timestamp</code>	Brand	N/A
<code>.alerts[].entity.labels.name</code>	Event.Attribute	Targeted Entity Label	<code>.alerts[].timestamp</code>	Brand	N/A
<code>.alerts[].protected_social_object</code>	Event.Attribute	Protected Social Object	<code>.alerts[].timestamp</code>	N/A	N/A
<code>.alerts[].id</code>	Event.Attribute	ZeroFox Link	<code>.alerts[].timestamp</code>	https://cloud.zerofox.com/alerts/135985017	N/A

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>

```
{
  "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[].create_d_at	file_hash_sha256	This will be mapped
results[].value	Indicator.Value	N/A	results[].create_d_at	http://109.230.199.227	N/A
results[].classifications[].name	Indicator.Attribute	Classification	results[].create_d_at	Domain	For each item in array
results[].privacy_level	Indicator.Attribute	Privacy Level	results[].create_d_at	Private	Converted to title casing
results[].threat_level	Indicator.Attribute	Threat Level	results[].create_d_at	High	Converted to title casing
results[].zf_alert_id	Indicator.Attribute	ZeroFox Alert ID	results[].create_d_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>

```
{
  "next": "https://tg-api.zerofox.com/indicators/?cursor=cD0yMDE5LTEyLTA1KzE0JTNBMDAlM0ExMy43MzY1NDU1MkIwMCUzQTAW",
  "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 Runs



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

METRIC	RESULT
Indicator Attributes	9571

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 1.1.0**
 - Added ZeroFox Alerts feed.
- **Version 1.0.0**
 - Initial Release