ThreatQuotient

ZeroFox Feeds Implementation Guide

Version 1.0.0

Wednesday, January 22, 2020

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

Support

Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

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.

Last Updated: Wednesday, January 22, 2020

Contents

ZeroFox Feeds Implementation Guide 1

Warning and Disclaimer 2

Contents 3

Introduction 4

Versioning 5

Installation 6

Configuration 7

ThreatQ Mapping 9

ZeroFox Campaigns 9

Get Campaigns 9

Get Related Indicators (Supplemental) 12

ZeroFox Indicators 16

Indicator Type Mapping 19

Introduction

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

There are two feeds included:

- ZeroFox Campaigns
- ZeroFox Indicators

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.21.0`

Installation

Perform the following steps to install the feeds:

> The same steps can be used to upgrade the feed to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **ZeroFox** feeds file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Incoming feeds**.
5. Click on the **Add New Feed** button.
6. Upload the feeds file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the feed 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.

   The feed will be added to the **Commercial** tab for Incoming Feeds. 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 feed-related credentials.

To configure the feed:

1. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feeds under the **Commercial** tab.
3. Click on the **Feed Settings** link for each feed.
4. Under the **Connection** tab, enter the following configuration parameters:

ZeroFox Campaigns

Parameter	Description
API Token	Your ZeroFox API Token.
Campaign Name Contains	An optional field that allow you to filter down the ingested campaigns based on a keyword.
Privacy Levels	A multi-select field that allows you to specify which campaigns and indicators to ingest based on their privacy level.

ZeroFox Indicators

Parameter	Description
API Token	Your ZeroFox API Token.
Privacy Levels	A multi-select field that allows you to specify which campaigns and indicators to ingest based on their privacy level.

Parameter	Description
Threat Levels	A multi-select field that allows you to specify which indicators to ingest based on their threat level.

5. Click on **Save Changes**.
6. Click on the toggle switch to the left of each feed name to enable the feeds.

ThreatQ Mapping

ZeroFox Campaigns

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

Get Campaigns

`GET /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:

ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples
Object	Campaign	N/A
Value	Campaign	Phishing Domains - Apple and Amazon
Attribute	Description	Amazon India Impersonator Site
Attribute	Privacy Level	Public
Published At	Source	2019-12-03T18:20:13.473048Z

Get Related Indicators (Supplemental)

This supplemental feed will ingest only indicators related to ingested campaigns

`GET /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": "18cc54e2f-
bdad5a317b6aeb2e7db3973cc5ffb01bbf810869d79e9cb3bf02bd5",
      "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, res-
taurant and hotel industries, has been deploying new tools
within their arsenal. Incident responders at FireEye's Man-
diant 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:

ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples
Object	Indicator	N/A
Indicator Type	N/A	file_hash_sha256
Value	Indicator	http://109.230.199.227
Attribute	Classification	Domain
Attribute	Privacy Level	Private
Published At	Source	2019-10-10T17:59:21.140847Z
Attribute	Threat Level	High
Attribute	ZeroFox Alert ID	12345

ZeroFox Indicators

This feed will ingest indicators from ZeroFox's API

`GET /indicators`

```
{
  "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:

ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples
Object	Indicator	N/A
Indicator Type	N/A	file_hash_sha256
Value	Indicator	http://109.230.199.227
Attribute	Classification	Domain
Attribute	Privacy Level	Private
Published At	Source	2019-10-10T17:59:21.140847Z
Attribute	Threat Level	High

Indicator Type Mapping

The table below provides indicator type mapping from ZeroFox to ThreatQ.

ZeroFox	ThreatQ Indicator Type
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

The following table contains data that is not mapped to ThreatQ indicator types:

ZeroFox	Details
profile	Twitter profiles, forum profiles, etc.
post	Twitter posts, forum posts, etc.
page	Facebook pages
hashtag	Facebook pages
phonenumber	Phone numbers
btc_wallet	BTC wallet IDs