ThreatQuotient

Proofpoint ET CDF User Guide

Version 2.1.1

October 23, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

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

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	2.1.1
Compatible with ThreatQ Versions	>= 4.36.0
Support Tier	ThreatQ Supported

Introduction

Proofpoint ET publishes IP Address and FQDN information in text files. The Proofpoint ET feeds retrieve data using the following endpoints:

- **Proofpoint ET IQRisk Rep List IPs** - `https://rules.emergingthreats.net/{client_key}/reputation/detailed-domainrepdata.txt`
- **Proofpoint ET IQRisk Rep List FQDN** - `https://rules.emergingthreats.net/{client_key}/reputation/detailed-iprepdata.txt`

The integration ingests indicators and indicator attributes into the ThreatQ platform.

Important Notes

- The API uses a client key for authentication.
- The response data is csv-formatted.

Installation

Perform the following steps to install the integration:

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

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration file on your local machine

   > ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to configure and then enable the feed.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

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

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

PARAMETER	DESCRIPTION
Client Key	The Proofpoint ET account client key.

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

Proofpoint ET IQRisk Rep List FQDNs

`https://rules.emergingthreats.net/{client_key}/reputation/detailed-domainrepdata.txt`

CSV Sample Response:

```
domain, category, score, first_seen, last_seen, ports
1928.ga,27,113,2020-02-14,2020-03-02,443
pell.gq,27,87,2020-02-04,2020-02-05,80 443
reae.cf,27,86,2020-03-02,2020-03-02,443
rpam.cf,27,118,2020-03-07,2020-03-07,80
set2.in,1,127,2018-03-11,2020-03-16,80
manip.hk,40,53,2019-12-27,2020-02-08,7777
rotan.tk,27,89,2020-02-07,2020-02-07,80
rreyw.gq,27,38,2019-12-17,2019-12-18,80
shjsc.ml,27,110,2020-02-28,2020-02-28,80
00sbi.icu,27,118,2020-03-07,2020-03-07,80
1ns4n3.de,1,127,2018-03-11,2018-06-18,
7slwb.icu,27,65,2020-01-14,2020-01-14,80
bet365.su,27,87,2020-02-05,2020-02-05,80
bnhaf.net,1,127,2018-03-11,2018-06-18,
btcc.host,1,122,2020-03-03,2020-03-16,80
domsev.ru,4,92,2020-03-02,2020-03-09,80
earcw.icu,27,102,2020-02-20,2020-02-20,80
gkpty.icu,27,107,2020-02-25,2020-02-25,80
himkon.cf,27,80,2020-01-21,2020-01-29,80
molpex.ml,37,77,2016-02-20,2020-03-06,80
p.b5m.com,5,102,2015-03-13,2020-03-11,80
pouiy.xyz,4,27,2020-02-25,2020-02-25,80
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	indicator.value	FQDN	3 (fourth token)	pouiy.xyz	
1 (second token)	indicator.attribute	Category	3 (fourth token)	4	
2 (third token)	indicator.value	Score	3 (fourth token)	27	
3 (fourth token)	indicator.attribute	First Seen	3 (fourth token)	2020-02-25	
4 (fifth token)	indicator.attribute	Last Seen	3 (fourth token)	2020-02-25	
5 (sixth token)	indicator.attribute	Ports	3 (fourth token)	80	The list of ports is separated by spaces
N/A	indicator.attribute	Category Name	3 (fourth token)	Spam,Known Spam Source	
N/A	indicator.attribute	Threat Level	3 (fourth token)	Malicious	

Category Type Mapping

The mapping between the category numbers in Proofpoint ET and ThreatQ Category Name is:

PROOFPOINT ET	THREATQ CATEGORY NAME
1	CnC,Malware Command and Control Server
2	Bot,Known Infected Bot
3	Spam,Known Spam Source
4	Drop,Drop site for logs or stolen credentials
5	SpywareCnC,Spyware Reporting Server
6	OnlineGaming, Questionable Gaming Site
7	DriveBySrc, Driveby Source
9	ChatServer, POLICY Chat Server
10	TorNode, POLICY Tor Node
13	Compromised, Known compromised or Hostile
15	P2P, P2P Node
16	Proxy, Proxy Host
17	IPCheck, IP Check Services
19	Utility, Known Good Public Utility
20	DDoSTarget, Target of a DDoS
21	Scanner, Host Performing Scanning
23	Brute_Forcer, SSH or other brute forcer
24	FakeAV, Fake AV and AS Products
25	DynDNS, Domain or IP Related to a Dynamic DNS Entry or Request
26	Undesirable, Undesirable but not illegal
27	AbusedTLD, Abused or free TLD Related
28	SelfSignedSSL, Self Signed SSL or other suspicious encryption
29	Blackhole, Blackhole or Sinkhole systems
30	RemoteAccessService, GoToMyPC and similar remote access services
31	P2PCnC, Distributed CnC Nodes
33	Parking, Domain or SEO Parked
34	VPN, VPN Server
35	EXE_Source, Observed serving executables
37	Mobile_CnC, Known CnC for Mobile specific Family
38	Mobile_Spyware_CnC, Spyware CnC specific to mobile devices
39	Skype_SuperNode, Observed Skype Bootstrap or Supernode
40	Bitcoin_Related, Bitcoin Mining and related
41	DDoSAttacker, DDoS Source

Threat Attribute Level Mapping

Based on the category, the threat level attribute is set using this map:

PROOFPOINT ET	THREATQ THREAT LEVEL
1	Malicious
2	Malicious
3	Malicious
4	Malicious
5	Suspicious
6	Suspicious
7	Malicious
8	Other
9	Suspicious
10	Suspicious
11	Other
12	Other
13	Malicious
14	Other
15	Suspicious
16	Suspicious
17	Suspicious
18	Other
19	Good
20	Suspicious
21	Malicious
22	Malicious
23	Malicious
24	Malicious
25	Other
26	Suspicious
27	Suspicious
28	Suspicious
29	Malicious
30	Suspicious
31	Malicious
32	Other
33	Suspicious
34	Suspicious
35	Suspicious
36	Other
37	Malicious
38	Suspicious
39	Suspicious
40	Suspicious

Proofpoint ET IQRisk Rep List IPs

`https://rules.emergingthreats.net/{client_key}/reputation/detailed-iprepdata.txt`

CSV Sample Response:

```
ip, category, score, first_seen, last_seen, ports
88.80.5.5,34,111,2018-03-12,2020-03-16,
1.171.8.24,15,97,2013-11-25,2020-03-10,58104
2.58.12.12,16,107,2020-02-24,2020-03-06,
217.23.7.3,1,127,2015-07-31,2020-03-16,443 1530 1680 2800 3003 7836
41.76.24.2,21,87,2018-01-02,2020-03-14,
49.7.43.43,15,122,2019-03-23,2020-03-15,
49.7.43.86,15,107,2019-04-15,2020-03-12,
64.32.8.69,1,81,2018-03-28,2020-03-15,80
68.9.224.8,21,107,2015-02-02,2020-03-15,22 23 445 3389
68.9.81.91,15,122,2015-04-14,2020-03-15,
69.80.99.9,34,127,2018-07-22,2020-03-16,
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	indicator.value	IP Address	3 (fourth token)	69.80.99.9	
1 (second token)	indicator.attribute	Category	3 (fourth token)	34	
2 (third token)	indicator.value	Score	3 (fourth token)	127	
3 (fourth token)	indicator.attribute	First Seen	3 (fourth token)	2020-02-02	
4 (fifth token)	indicator.attribute	Last Seen	3 (fourth token)	2020-02-25	
5 (sixth token)	indicator.attribute	Ports	3 (fourth token)	22 23 445 3389	The list of ports is separated by spaces.
N/A	indicator.attribute	Category Name	3 (fourth token)	Spam,Known Spam Source	
N/A	indicator.attribute	Threat Level	3 (fourth token)	Malicious	

The mapping between the category types in Proofpoint ET and ThreatQ can be found in the Proofpoint ET IQRisk Rep List FQDNs mapping section.

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.

Proofpoint ET IQRisk Rep List FQDNs

METRIC	RESULT
Run Time	2 hours
Indicators	64,000
Indicator Attributes	500,000

Proofpoint ET IQRisk Rep List IPs

METRIC	RESULT
Run Time	2 hours
Indicators	45,000
Indicator Attributes	300,000

Known Issues / Limitations

- A bulk delete of all indicators with the Proofpoint ET IQRisk Rep List IPs and Proofpoint ET IQRisk Rep List FQDNs source is needed before running the 2.1.0 version of the feeds.

Change Log

- Version 2.1.1
  - Resolved an issue where indicator attributes were duplicated when adjusting ingestion time.

    Contact ThreatQ Support, if upgrading from a previous version of the integration, for help deduplicating indicator attributes.

- **Version 2.1.0**
  - Updated the category map and added threat level mapping.

    Perform a bulk delete of all indicators with the Proofpoint ET IQRisk Rep List IPs and Proofpoint ET IQRisk Rep List FQDNs source before running this version of the feed.

- **Version 2.0.0**
  - Added category map and updated mapping.
- **Version 1.0.0**
  - Initial release