ThreatQuotient

Proofpoint ET Feeds Guide

Version 2.0.0

Tuesday, May 5, 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: Tuesday, May 5, 2020

Contents

Versioning

- Current integration version `2.0.0`
- Supported on ThreatQ versions >= `4.36.0`

Introduction

The Proofpoint ET integration replaces the Emerging Threats **IQRisk Rep List FQDNs** and **IQRisk Rep List IPs** commercial feeds that were seeded with previous versions of the ThreatQ platform. Upgrading your ThreatQ platform to version 4.36 or greater will remove the aforementioned feeds. Existing intelligence data previously ingested will remain on the platform and will appear as Proofpoint ET. You will have to download and install the new Proofpoint ET integration from the ThreatQuotient Marketplace.

Proofpoint ET publishes IP Address and FQDN information in text files using the following endpoints:

- Proofpoint ET IQRisk Rep List IPs
- Proofpoint ET IQRisk Rep List FQDN

Notes:

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

Installation

Perform the following steps to install the feed:

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 **Proofpoint ET** feed 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 feed 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 feed under the **Commercial** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
Client Key	The Proofpoint ET account client key.

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

ThreatQ Mapping

Proofpoint ET IQRisk Rep List FQDNs

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

CSV response sample:

```
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
```

The mapping table is below:

ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples
indicator.value	FQDN		3 (fourth token)	pouiy.xyz
indicator.attribute	Category		3 (fourth token)	4
indicator.value	Score		3 (fourth token)	27
indicator.attribute	First Seen		3 (fourth token)	2020-02-25
indicator.attribute	Last Seen		3 (fourth token)	2020-02-25
indicator.attribute	Ports		3 (fourth token)	80
indicator.attribute	Category Name		3 (fourth token)	Botcc Port-grouped

Category Name Mapping

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

ProofPoint ET	ThreatQ Category Name
1	Activex
2	Attack Response
3	Botcc (Bot Command and Control)
4	Botcc Portgrouped
5	Chat
6	CIArmy
7	Compromised
8	Current Events
9	Decoder-events
10	Deleted
11	DNS
12	DOS
13	Drop
14	Dshield
15	Exploit
16	Files
17	FTP
18	Games
19	HTTP-Events
20	ICMP

ProofPoint ET	ThreatQ Category Name
21	ICMP_info
22	IMAP
23	Inappropriate
24	Malware
25	Misc.
26	Mobile Malware
27	Netbios
28	P2P
29	Policy
30	POP3
31	RBN & RBN-malvertisers
32	RPC
33	SCADA
34	SCADA_special
35	SCAN
36	Shellcode
37	SMTP
38	SMTP-events
39	SNMP
40	SQL

ProofPoint ET	ThreatQ Category Name
41	Stream-events
42	TELNET
43	TFTP
44	TLS-Events
45	TOR
46	Trojan
47	User Agents
48	VOIP
49	Web Client
50	Web Server
51	Web Specific Apps
52	WORM

Proofpoint ET IQRisk Rep List IPs

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

CSV response sample:

```
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,
```

The mapping table is below:

ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples
indicator.value	IP Address		3 (fourth token)	69.80.99.9
indicator.attribute	Category		3 (fourth token)	34
indicator.value	Score		3 (fourth token)	127
indicator.attribute	First Seen		3 (fourth token)	2020-02-02
indicator.attribute	Last Seen		3 (fourth token)	2020-02-25
indicator.attribute	Ports		3 (fourth token)	22 23 445 3389
indicator.attribute	Category Name		3 (fourth	SCADA_

ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples
			token)	special

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

Change Log

- **Version 2.0**
  - Updated name to ProofPoint ET
  - Added data mapping for Category Names
- **Version 1.0**
  - Initial release