ThreatQuotient

Proofpoint ET OSINT Guide

Version 1.0.0

Tuesday, November 10, 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.

Contents

Versioning

- Current integration version: 1.0.0
- Supported on ThreatQ versions: 4.3.0 or greater

Introduction

The Proofpoint ET OSINT feeds retrieve data using the following endpoints:

- Proofpoint ET Block IP
- Proofpoint ET Compromised IPs

Proofpoint ET publishes IP Address and CIDR Block threat data in a text format. The API called for these feeds does not require a client key for authentication.

Installation

Perform the following steps to install the integration:

Note: *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

   Note: 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

Note: *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. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** tab (optional).
3. Click on the integration to open its details page.
4. Review the Settings configuration, make any changes if needed, and click on **Save**.
5. Click on the toggle switch to the left of the integration name to enable it.

ThreatQ Mapping

Proofpoint ET Block IP

```
GET https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt
```

Text response sample:

```
100.14.117.137
100.37.240.62
100.6.23.40
101.187.104.105
101.187.81.254
101.187.97.173
101.50.232.218
102.182.93.220
103.106.236.83
103.109.78.174
103.122.75.218
103.127.165.250
103.13.224.53
103.133.66.57
```

ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
0 (first token)	Indicator.value	IP Address or CIDR Block	100.14.117.137	If data contains "/" the indicator type will be CIDR Block, else "IP Address"'

Proofpoint ET Compromised IP

This supplemental feed will fetch the full analysis report JSON from Threat Grid's API

```
GET https://rules.emergingthreats.net/blockrules/compromised-ips.txt
```

Text response sample

```
{101.231.124.6
101.36.118.86
101.69.200.162
101.69.247.6
101.81.136.34
101.81.137.93
101.86.133.244
101.96.89.207
102.176.160.30
103.101.52.48
103.123.8.75
```

ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples
0 (first token)	Indicator.value	IP Address	100.231.124.6

Average Run Time

Note: *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 Block IP

Metric	Result
Run Time	3 minutes
Indicators	2,300

Proofpoint ET Compromised IP

Metric	Result
Run Time	2 minutes
Indicators	1,000

Change Log

Version	Details
1.0.0	Initial Release