ThreatQuotient

Proofpoint TAP CDF User Guide

Version 1.1.0

November 28, 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	1.1.0
Compatible with ThreatQ Versions	>= 5.10.0
Support Tier	ThreatQ Supported

Introduction

The Proofpoint TAP (Targeted Attack Protection) CDF allows you to ingest and relate the emails of users who have clicked on malicious links, as well as these malicious links and their senders from the Proofpoint TAP SIEM endpoint.

The integration provides the following feed:

- **Proofpoint TAP Events** - ingests and relates the emails of users who have clicked on malicious links.
- **Proofpoint TAP Campaigns** - ingests data about campaigns.
- **Proofpoint TAP Emails** - ingests data about emails.

The integration ingests the following system objects:

- Adversary
- Campaigns
- Corporate Emails (custom object)
- Events
- Incidents
- Indicators
    - Indicator Attributes
- Malware
- TTP

Prerequisites

The integration requires the following:

- Proofpoint TAP Principal.
- Proofpoint TAP Secret.
- The Corporate Email custom object installed on your ThreatQ instance.

Corporate Email Custom Object

The integration requires the Corporate Email custom object.

Use the steps provided to install the Corporate Email custom object.

> ⚠ When installing the custom objects, be aware that any in-progress feed runs will be cancelled, and the API will be in maintenance mode.

1. Download the integration zip file from the ThreatQ Marketplace and unzip its contents.
2. SSH into your ThreatQ instance.
3. Navigate to tmp directory:

   ```
   cd /tmp/
   ```

4. Create a new directory:

   ```
   mkdir proofpoint_tap_cdf
   ```

5. Upload the **corporate_email.json** and **install.sh** script into this new directory.
6. Create a new directory called **images** within the proofpoint_tap_cdf directory.

   ```
   mkdir images
   ```

7. Upload the corporate_emails.svg.
8. Navigate to the **/tmp/proofpoint_tap_cdf**.

   The directory should resemble the following:

   - tmp
     - **proofpoint_tap_cdf**
       - **corporate_email.json**
       - **install.sh**
       - **images**
         - **corporate_email.svg**
9. Run the following command to ensure that you have the proper permissions to install the custom object:

   ```
   chmod +x install.sh
   ```

10. Run the following command:

```
sudo ./install.sh
```

> You must be in the directory level that houses the install.sh and json files when running this command.

The installation script will automatically put the application into maintenance mode, move the files to their required directories, install the custom object, update permissions, bring the application out of maintenance mode, and restart dynamo.

11. Remove the temporary directory, after the custom object has been installed, as the files are no longer needed:

```
rm -rf proofpoint_tap_cdf
```

Installation

The CDF requires the installation of the Corporate Email custom object before installing the actual CDF. See the Prerequisites chapter for more details. The custom object must be installed prior to installing the CDF. Attempting to install the CDF without the custom object will cause the CDF install process to fail.

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 zip file.
3. Extract the contents of the zip and install the required Corporate Email custom object.
4. Navigate to the integrations management page on your ThreatQ instance.
5. Click on the **Add New Integration** button.
6. Upload the yaml 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.
7. 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 parameters under the **Configuration** tab:

All Feeds

PARAMETER	DESCRIPTION
Proofpoint TAP Principal	Your Proofpoint TAP Principal.
Proofpoint TAP Secret	Your Proofpoint TAP Secret.

TAP Campaigns - Additional Parameters

PARAMETER	DESCRIPTION
Fetch Full Threat (IOC) Details	Enabling this will fetch the full details for a given threat.  This will increase the amount of requests and time that the feed will require.
Fetch Campaign Forensics	Enabling this will fetch the forensics for each campaign.  This will increase the amount of requests and time that the feed will require to process the data.
Fetch IOCs	Enable/Disable the ingestion of IOCs.

TAP Emails - Additional Parameter

PARAMETER	DESCRIPTION
Threat Status	Specify which threat statuses will be returned in the data. **Active**, **Cleared**, and **False Positive** threat statuses are accepted. If no value is specified, active and cleared threats are returned.

TAP Events - Additional Parameters

PARAMETER	DESCRIPTION
Event Type Filter	Specify which types of message events to ingest threats from. Options include: ◦ Clicks Blocked (Clicks to URL threats which were blocked) ◦ Clicks Permitted (Clicks to URL threats which were permitted) ◦ Messages Blocked (Messages with threats which were quarantined by PPS) ◦ Messages Delivered (Messages with threats which were delivered by PPS)
Threat Status Filter	Specify which threat statuses will be returned in the data. If no value is specified, active and cleared threats are returned. Options include: ◦ Active ◦ Cleared ◦ False Positive
Classification Filter	Specify the classifications required for the threat to be ingested. Options include: ◦ Malware ◦ Phishing ◦ Spam ◦ Impostor (for BEC/Message Text Threats) ◦ TOAD (Telephone-Oriented Attack Delivery)
Require Score	Enabling this will ignore any threats that do not have a score for any classifications.
Ingest Recipient Email Address	Enabling this will ingest the recipient email address as a ThreatQ Object, related to the threat.
Threat Types (IOCs)	Select the threat types (IOCs) you want to be ingested into ThreatQ. Options include: ◦ URLs ◦ Attachments (Hashes) ◦ Email Addresses ◦ Sender Email Addresses

PARAMETER	DESCRIPTION
	◦ Sender IP Addresses

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.

See the Known Issues / Limitations chapter of this guide if you plan on performing manual runs with the feeds included with this integration.

ThreatQ Mapping

Proofpoint TAP Events

The Proofpoint TAP Events feed allows a user to ingest and relate the emails of users who have clicked on malicious links, as well as these malicious links and their senders from the Proofpoint TAP SIEM endpoint.

```
GET https://tap-api-v2.proofpoint.com/v2/siem/all
```

Sample Response:


```
{
  "clicksPermitted": [
    {
      "url": "https://kul.ink/LyZu",
      "classification": "spam",
      "clickTime": "2021-03-29T18:08:16.000Z",
      "threatTime": "2021-03-30T15:36:54.000Z",
      "userAgent": "Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0)
like Gecko",
      "campaignId": "",
      "id": "b92f6d79-aeec-4bc4-8fdb-ee9929f96856",
      "clickIP": "167.239.221.85",
      "sender": "roger73martinez@yahoo.com",
      "recipient": "john.doe@example.com",
      "senderIP": "78.159.108.31",
      "GUID": "21utHx_zcMEWcrZJEwVt8h-HU7GtkcVF",
      "threatID":
"4d07e404b62d36aa6cf7c1712f12ee00836be10942abf1740090b88ea209019b",
      "threatURL": "https://threatinsight.proofpoint.com/011ae236-5630-b11c-
efa9-799e8c978947/threat/email/
4d07e404b62d36aa6cf7c1712f12ee00836be10942abf1740090b88ea209019b",
      "threatStatus": "active",
      "messageID": "<01000nhxALbx7pjR-6XpAKxD-HLCE-0x1m-gqMY-
VQ3KUl2DOGJT-000000@email.amazonses.com>"
    }
  ],
  "clicksBlocked": [
    {
      "url": "https://kul.ink/ZyQ",
      "classification": "malware",
      "clickTime": "2021-03-29T18:08:16.000Z",
      "threatTime": "2021-03-30T15:36:54.000Z",
      "userAgent": "Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0)
like Gecko",
      "campaignId": "",
      "id": "e12f6d79-aeec-4bc4-8fdb-ee9929f96856",
```

```
      "clickIP": "168.239.221.85",
      "sender": "roger73martinez@yahoo.com",
      "recipient": "john.doe@example.com",
      "senderIP": "78.159.108.32",
      "GUID": "21utHx_zcMEWcrZJEwVt8h-HU7GtkcVF",
      "threatID":
"4d07e404b62d36aa6cf7c1712f12ee00836be10942abf1740090b88ea209019b",
      "threatURL": "https://threatinsight.proofpoint.com/781ae236-5630-b11c-
efa9-799e8c978947/threat/email/
4d07e404b62d36aa6cf7c1712f12ee00836be10942abf1740090b88ea209019b",
      "threatStatus": "active",
      "messageID": "<01000nhxALbx7pjR-6XpAKxD-HLCE-0x1m-gqMY-
VQ3KUl2DOGJT-000000@email.amazonses.com>"
    }
  ],
  "messagesDelivered": [
    {
      "spamScore": 0,
      "phishScore": 0,
      "threatsInfoMap": [
        {
          "threatID":
"79f5a059efa25ad815a7bfd4bac4b33168bd205e09ecd3029fee1e8c902017e3",
          "threatStatus": "active",
          "classification": "malware",
          "threatUrl": "https://threatinsight.proofpoint.com/bad9882e-b042-
c1ed-7a8c-dd948a40e9a7/threat/email/
79f5a059efa25ad815a7bfd4bac4b33168bd205e09ecd3029fee1e8c902017e3",
          "threatTime": "2023-08-15T13:18:59.000Z",
          "threat": "https://ads.associationmediagroup.com/
redirect_alink.spark?
ALID=12884&ID=172818&utm_source=msba%20weekly&utm_medium=email&campaign=2399",
          "campaignID": null,
          "threatType": "url"
        }
      ],
      "messageTime": "2023-08-15T13:07:26.000Z",
      "impostorScore": 0,
      "malwareScore": 0,
      "cluster": "exampleofcompanyinc_hosted",
      "subject": "MSBA Mourns Passing of Past President Seymour Stern, Join
the\r\n A2JCâ€™s Delivery of Legal Services Committee, ABA Formal Op.\r\n 505
Denounces Nonrefundable Fees, & More",
      "quarantineFolder": null,
      "quarantineRule": null,
      "policyRoutes": [
        "default_inbound"
      ],
      "modulesRun": [
        "av",
```

```
        "dkimv",
        "spf",
        "spam",
        "dmarc",
        "pdr",
        "urldefense"
      ],
      "messageSize": 118278,
      "headerFrom": "MSBA Weekly <msbaweekly@msba.org>",
      "headerReplyTo": null,
      "fromAddress": [
        "msbaweekly@msba.org"
      ],
      "ccAddresses": [],
      "replyToAddress": [],
      "toAddresses": [
        "john.doe@example.com"
      ],
      "xmailer": null,
      "messageParts": [
        {
          "disposition": "inline",
          "sha256":
"90884d87582fdd68f9b969cc28592bd74376869b533707625fedb237b01bfa32",
          "md5": "ff53861b753d20f37f27bc8f528ab03d",
          "filename": "text.html",
          "sandboxStatus": null,
          "oContentType": "text/html",
          "contentType": "text/html"
        },
        {
          "disposition": "inline",
          "sha256":
"7879b9e594f5db07b9ff987e5df82350b111686b8e10bd8504fa604b8e4b5491",
          "md5": "a40421f586719b827b5ac730142ca5ba",
          "filename": "text.txt",
          "sandboxStatus": null,
          "oContentType": "text/plain",
          "contentType": "text/plain"
        }
      ],
      "completelyRewritten": true,
      "id": "f9d43162-91f1-60ce-5219-d06a48c39b65",
      "QID": "37FA0mQ2014303",
      "GUID": "a_KclEU5OcHxiRjFeDUSRZEN-iflZ5cZ",
      "sender": "83242fbb75c8-000000@mail.msba.org",
      "recipient": [
        "john.doe@example.com"
      ],
      "senderIP": "23.251.231.70",
```

```
      "messageID": "<01000189f94ee762-
b92e97d0-2aab-44b8-84c5-83242fbb75c8-000000@email.amazonses.com>"
    }
  ],
  "messagesBlocked": [
    {
      "spamScore": 0,
      "phishScore": 0,
      "threatsInfoMap": [
        {
          "threatID":
"ddbb3051ccbb43a985bb3dc98da57ee2380892a248853b2a5a1f0a77c3e10201",
          "threatStatus": "active",
          "classification": "malware",
          "threatUrl": "https://threatinsight.proofpoint.com/bad9882e-b042-
c1ed-7a8c-dd948a40e9a7/threat/email/
ddbb3051ccbb43a985bb3dc98da57ee2380892a248853b2a5a1f0a77c3e10201",
          "threatTime": "2023-07-04T00:30:19.000Z",
          "threat": "appy.thelittlehappythings.com/ga/click/",
          "campaignID": null,
          "threatType": "url"
        }
      ],
      "messageTime": "2023-08-15T13:18:10.000Z",
      "impostorScore": 0,
      "malwareScore": 100,
      "cluster": "exampleofcompanyinc_hosted",
      "subject": "ER Doctor just went public with a shocking study he found.",
      "quarantineFolder": "Inbound Malware",
      "quarantineRule": "inbound_malware",
      "policyRoutes": [
        "default_inbound"
      ],
      "modulesRun": [
        "av",
        "dkimv",
        "spf",
        "spam",
        "dmarc",
        "pdr",
        "urldefense"
      ],
      "messageSize": 9005,
      "headerFrom": "\"sleeping pills\"
<leoneljblalock@lit.thelittlehappythings.com>",
      "headerReplyTo": "leoneljblalock@lit.thelittlehappythings.com",
      "fromAddress": [
        "leoneljblalock@lit.thelittlehappythings.com"
      ],
      "ccAddresses": [],
```

```
      "replyToAddress": [
        "leoneljblalock@lit.thelittlehappythings.com"
      ],
      "toAddresses": [
        "john.doe@example.com"
      ],
      "xmailer": null,
      "messageParts": [
        {
          "disposition": "inline",
          "sha256":
"c9cf8b9799e3eb9972b87baf75d22b518bca885d2424c273c838a88934ee3322",
          "md5": "488bdfe713c2e6eae01ff4129fb2f2a0",
          "filename": "text.html",
          "sandboxStatus": null,
          "oContentType": "text/html",
          "contentType": "text/html"
        }
      ],
      "completelyRewritten": false,
      "id": "320e7e53-71a0-1d54-86e6-9a7a4374c5eb",
      "QID": "3sg9b3r3hh-1",
      "GUID": "Gg9EOkeeyWN_5K4Ql3rnCnk4RCgQbxbs",
      "sender": "403625345=8@lit.thelittlehappythings.com",
      "recipient": [
        "john.doe@example.com"
      ],
      "senderIP": "161.97.93.90",
      "messageID":
"<mid-2af6eb34d77f189d523324ff1ca38096-379@lit.thelittlehappythings.com>"
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.messagesDelivered[].threatsInfoMap[].threat	Related Indicator.Value	.messagesDelivered[].threatsInfoMap[].threatType	.messagesDelivered[].threatsInfoMap[].threatTime	https://ads.associationmediagroup.com/redirect_alink.spark?ALID=128...	Indicator type computed by using `Proofpoint Threat Type Mapping`
.messagesDelivered[].threatsInfoMap[].classification	Related Indicator.Attribute	Classification	.messagesDelivered[].threatsInfoMap[].threatTime	malware	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.messagesDelivered[].malwareScore	Related Indicator.Attribute	Malware Score	.messagesDelivered[].threatsInfoMap[].threatTime	0	If `.messagesDelivered[].threatsInfoMap[].classification` is `malware`. Updated if it already exists.
.messagesDelivered[].spamScore	Related Indicator.Attribute	Spam Score	.messagesDelivered[].threatsInfoMap[].threatTime	0	If `.messagesDelivered[].threatsInfoMap[].classification` is `spam`. Updated if it already exists.
.messagesDelivered[].phishScore	Related Indicator.Attribute	Phish Score	.messagesDelivered[].threatsInfoMap[].threatTime	0	If `.messagesDelivered[].threatsInfoMap[].classification` is `phish`. Updated if it already exists.
.messagesDelivered[].impostorScore	Related Indicator.Attribute	Impostor Score	.messagesDelivered[].threatsInfoMap[].threatTime	0	If `.messagesDelivered[].threatsInfoMap[].classification` is `impostor`. Updated if it already exists.
.messagesDelivered[].recipient, .	Event.Title	N/A	.messagesDelivered[].messageTime	`[Delivered] john.doe@example.com received a suspicious`	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
messagesDelivered[].sender				`message from sender, 83242fbb75c8-000000@mail.msba.org`	
N/A	Event.Type	N/A	N/A	Incident	All the events have type `Incident`
.messagesDelivered[].id	Event.Attribute	Proofpoint ID	.messagesDelivered[].messageTime	f9d43162-91f1-60ce-5219-d06a48c39b65	N/A
.messagesDelivered[].cluster	Event.Attribute	Cluster	.messagesDelivered[].messageTime	exampleofcompanyinc_hosted	N/A
.messagesDelivered[].quarantineFolder	Event.Attribute	Quarantine Folder	.messagesDelivered[].messageTime	N/A	N/A
.messagesDelivered[].subject	Event.Attribute	Subject	.messagesDelivered[].messageTime	MSBA Mourns Passing of Past President Seymour Stern...	N/A
.messagesDelivered[].impostorScore	Event.Attribute	Impostor Score	.messagesDelivered[].messageTime	0	Updated if it already exists.
.messagesDelivered[].spamScore	Event.Attribute	Spam Score	.messagesDelivered[].messageTime	0	Updated if it already exists.
.messagesDelivered[].phishScore	Event.Attribute	Phish Score	.messagesDelivered[].messageTime	0	Updated if it already exists.
.messagesDelivered[].malwareScore	Event.Attribute	Malware Score	.messagesDelivered[].messageTime	0	Updated if it already exists.
.messagesBlocked[].threatsInfoMap[].threat	Related Indicator.Value	.messagesBlocked[].threatsInfoMap[].threatType	.messagesBlocked[].threatsInfoMap[].threatTime	appy.thelittlehappythings.com/ga/click/	Indicator type computed by using `Proofpoint Threat Type Mapping`
.messagesBlocked[].threatsInfoMap[].classification	Related Indicator.Attribute	Classification	.messagesBlocked[].threatsInfoMap[].threatTime	malware	N/A
.messagesBlocked[].malwareScore	Related Indicator.Attribute	Malware Score	.messagesBlocked[].threatsInfoMap[].threatTime	100	If `.messagesDelivered[].threatsInfoMap[].classification` is `malware`.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					Updated if it already exists.
.messagesBlocked[].spamScore	Related Indicator.Attribute	Spam Score	.messagesBlocked[].threatsInfoMap[].threatTime	0	If `.messagesDelivered[].threatsInfoMap[].classification` is `spam`. Updated if it already exists.
.messagesBlocked[].phishScore	Related Indicator.Attribute	Phish Score	.messagesBlocked[].threatsInfoMap[].threatTime	0	If `.messagesDelivered[].threatsInfoMap[].classification` is `phish`. Updated if it already exists.
.messagesBlocked[].impostorScore	Related Indicator.Attribute	Impostor Score	.messagesBlocked[].threatsInfoMap[].threatTime	0	If `.messagesDelivered[].threatsInfoMap[].classification` is `impostor`. Updated if it already exists.
.messagesBlocked[].recipient, .messagesBlocked[].sender	Event.Title	N/A	.messagesBlocked[].messageTime	`[Blocked] john.doe@example.com received a suspicious message from sender, 403625345=8@lit.thelittlehappythings.com`	N/A
.messagesBlocked[].id	Event.Attribute	Proofpoint ID	.messagesBlocked[].messageTime	320e7e53-71a0-1d54-86e6-9a7a4374c5eb	N/A
.messagesBlocked[].cluster	Event.Attribute	Cluster	.messagesBlocked[].messageTime	exampleofcompanyinc_hosted	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.messagesBlocked[].quarantineFolder	Event.Attribute	Quarantine Folder	.messagesBlocked[].messageTime	Inbound Malware	N/A
.messagesBlocked[].subject	Event.Attribute	Subject	.messagesBlocked[].messageTime	ER Doctor just went public with a shocking study he found.	N/A
.messagesBlocked[].impostorScore	Event.Attribute	Impostor Score	.messagesBlocked[].messageTime	0	Updated if it already exists.
.messagesBlocked[].spamScore	Event.Attribute	Spam Score	.messagesBlocked[].messageTime	0	Updated if it already exists.
.messagesBlocked[].phishScore	Event.Attribute	Phish Score	.messagesBlocked[].messageTime	0	Updated if it already exists.
.messagesBlocked[].malwareScore	Event.Attribute	Malware Score	.messagesBlocked[].messageTime	100	Updated if it already exists.
.clicksPermitted[].recipient, .clicksPermitted[].sender	Event.Title	N/A	.clicksPermitted[].clickTime	`[Permitted] john.doe@example.com clicked a link classified as spam, from sender roger73martinez@yahoo.com`	N/A
.clicksPermitted[].classification	Event.Attribute	Classification	.clicksPermitted[].clickTime	spam	N/A
.clicksPermitted[].campaignId	Event.Attribute	Campaign ID	.clicksPermitted[].clickTime	N/A	N/A
.clicksPermitted[].id	Event.Attribute	Proofpoint ID	.clicksPermitted[].clickTime	b92f6d79-aeec-4bc4-8fdb-ee9929f96856	N/A
.clicksPermitted[].threatURL	Event.Attribute	Proofpoint Threat URL	.clicksPermitted[].clickTime	https://threatinsight.proofpoint.com/011ae236-5630-b11c-efa9-799e8c978947...	N/A
.clicksPermitted[].clickIP	Event.Attribute	Click External IP	.clicksPermitted[].clickTime	167.239.221.85	N/A
.clicksBlocked[].recipient, .clicksBlocked[].sender	Event.Title	N/A	.clicksPermitted[].clickTime	`[Blocked] john.doe@example.com clicked a link classified as malware, from sender roger73martinez@yahoo.com`	N/A
.clicksBlocked[].classification	Event.Attribute	Classification	.clicksPermitted[].clickTime	malware	N/A
.clicksBlocked[].campaignId	Event.Attribute	Campaign ID	.clicksPermitted[].clickTime	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.clicksBlocked[].id	Event.Attribute	Proofpoint ID	.clicksPermitted[].clickTime	e12f6d79-aeec-4bc4-8fdb-ee9929f96856	N/A
.clicksBlocked[].threatURL	Event.Attribute	Proofpoint Threat URL	.clicksPermitted[].clickTime	https://threatinsight.proofpoint.com/781ae236-5630-b11c-efa9-799e8c978947...	N/A
.clicksBlocked[].clickIP	Event.Attribute	Click External IP	.clicksPermitted[].clickTime	168.239.221.85	N/A
.messagesDelivered[].recipient	Related Corporate_Email.Value	N/A	N/A	john.doe@example.com	If user config `Ingest Recipient Email Addresses` is enabled
.messagesBlocked[].recipient	Related Corporate_Email.Value	N/A	N/A	john.doe@example.com	If user config `Ingest Recipient Email Addresses` is enabled
.clicksPermitted[].recipient	Related Corporate_Email.Value	N/A	N/A	john.doe@example.com	If user config `Ingest Recipient Email Addresses` is enabled
.clicksBlocked[].recipient	Related Corporate_Email.Value	N/A	N/A	john.doe@example.com	If user config `Ingest Recipient Email Addresses` is enabled
.clicksPermitted[].url	Related Indicator.Value	URL	N/A	https://kul.ink/LyZu	If user config `Threat Types (IOCs)` contains `URLs`
.clicksBlocked[].url	Related Indicator.Value	URL	N/A	https://kul.ink/ZyQ	If user config `Threat Types (IOCs)`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					contains `URLs`
.messagesDelivered[].sender	Related Indicator.Value	Email Address	N/A	83242fbb75c8-000000@mail.msba.org	If user config `Threat Types (IOCs)` contains `Sender Email Addresses`
.messagesBlocked[].sender	Related Indicator.Value	Email Address	N/A	403625345=8@lit.thelittlehappythings.com	If user config `Threat Types (IOCs)` contains `Sender Email Addresses`
.clicksPermitted[].sender	Related Indicator.Value	Email Address	N/A	roger73martinez@yahoo.com	If user config `Threat Types (IOCs)` contains `Sender Email Addresses`
.clicksBlocked[].sender	Related Indicator.Value	Email Address	N/A	roger73martinez@yahoo.com	If user config `Threat Types (IOCs)` contains `Sender Email Addresses`
.messagesDelivered[].senderIP	Related Indicator.Value	IP Address	N/A	23.251.231.70	If user config `Threat Types (IOCs)` contains `Sender IP Addresses`
.messagesBlocked[].senderIP	Related Indicator.Value	IP Address	N/A	161.97.93.90	If user config `Threat Types (IOCs)` contains `Sender`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					`IP Addresses`
.clicksPermitted[].senderIP	Related Indicator.Value	IP Address	N/A	78.159.108.31	If user config `Threat Types (IOCs)` contains `Sender IP Addresses`
.clicksBlocked[].senderIP	Related Indicator.Value	IP Address	N/A	78.159.108.32	If user config `Threat Types (IOCs)` contains `Sender IP Addresses`

Threat Type Matching

PROOFPOINT THREAT TYPE	THREATQ INDICATOR TYPE	NOTES
url	URL	N/A
attachment	MD5, SHA-1, SHA-256, SHA-384, SHA-512	Mapping performed based on hash length.
messageText	Email Address	N/A

Proofpoint TAP Campaigns

The Proofpoint TAP Campaigns feed allows users to pull specific details about a campaign.

`GET https://tap-api-v2.proofpoint.com/v2/campaign/ids`

Sample Response:

This feed extracts the campaign ID (campaigns[].id) and sends it to the supplemental feeds: Proofpoint TAP - Fetch Campaign by ID, Proofpoint TAP - Fetch Forensics.


```
{
    "campaigns": [
        {
            "id": "4de2b1f5-81a3-58d9-834f-7e4c944f73c0",
            "lastUpdatedAt": "2023-08-11T00:30:15.000Z"
        }
    ]
}
```

Proofpoint TAP - Fetch Threat by ID (supplemental)

The Fetch Threat by ID supplemental feed ingests information about campaigns.

`GET https://tap-api-v2.proofpoint.com/v2/campaign/{CAMPAIGN_ID}`

Sample Response:


```
{
   "id": "4de2b1f5-81a3-58d9-834f-7e4c944f73c0",
   "name": "Grandoreiro | TA2725 | URLs | \"n0t49083\" | BR | 9-14 August
2023",
   "description": "Emails with Portuguese language NF-e lures containing links
to a rar file containing an MSI file with a final payload of Grandoreiro, a
trojan designed to steal personal and banking information. This campaign is
geofenced to Brazil.\n\nExample senders:\n<pre>\nDepartamento De
Emissao&lt;grupo@c1.nf7329.com&gt;\nDepartamento De
Emissao&lt;grupo@c11.ntffs32992.com&gt;\n</pre>\n\nExample subjects:
\n<pre>\nEmissao de Registro NF-E- 09/08/2023\n</pre>\n\n\n\n**Landing
Page**\n\n - http://86.203.178.68.host.secureserver.net/.n0t49083/\n\n -
https://pronotaid2023747343.blob.core.windows.net/%24web/
ElectricNf24f2023.rar\n",
   "startDate": "2023-08-09T00:00:00.000Z",
   "notable": false,
   "actors": [
      {
         "id": "3ba7ed7e-c62b-4009-b736-a1e190ad31b2",
         "name": "TA2725"
      }
   ],
   "families": [
      {
         "id": "1c76a23b-5d2f-4ec8-bb37-cff693e73419",
         "name": "Malware"
      }
   ],
   "malware": [
      {
         "id": "5b27a23b-5d2f-4ec8-bb37-cff693e73023",
         "name": "IceID"
      }
   ],
   "techniques": [
      {
         "id": "0d3494d8-efad-4fe8-a947-760f0a50a8d9",
         "name": "Geofencing"
      },
      {
         "id": "70a76992-2be1-4a70-a96b-2824c4428113",
         "name": "Social Engineering"
      }
```

```
   ],
   "brands": [],
   "campaignMembers": [
      {
         "id":
"91d97d8d0e4dd1354c4d0a00f97717c6c165480002e3176fcc5c65bc4ca2e786",
         "threat": "http://86.203.178.68.host.secureserver.net/.n0t49083/?
hash=enrico.almeida@edenred.com",
         "threatStatus": "active",
         "type": "url",
         "threatTime": "2023-08-13T08:50:26.000Z"
      },
      {
         "id":
"b806ab4b6034d2fef208fc2996ee14bb18368c65add2b5ec4939bc49e9366e02",
         "threat": "http://86.203.178.68.host.secureserver.net/.n0t49083/?
hash=elisa.dimer@embratec.com.br",
         "threatStatus": "active",
         "type": "url",
         "threatTime": "2023-08-13T09:06:23.000Z"
      }
   ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.name	Campaign.Value	N/A	value.startDate	Grandoreiro..	N/A
.description	Campaign.Description	N/A	N/A	Emails with Portuguese language NF-e...	N/A
.id	Campaign.Attribute	Campaign ID	value.startDate	4de2b1f5-81a3-58d9-834f-7e4c944f73c0	N/A
.families[].name	Campaign.Attribute	Campaign Family	value.startDate	Malware	N/A
.brands[].name	Campaign.Attribute	Affected Brand	value.startDate	N/A	N/A
.notable	Campaign.Attribute	Is Notable	value.startDate	False	Updated if it already exists.
.actors[].name	Related Adversary.Name	N/A	value.startDate	TA2725	N/A
.malware[].name	Related Malware.Value	N/A	value.startDate	IceID	N/A
.techniques[].name	Related TTP.Value	N/A	value.startDate	Geofencing	N/A
.campaignMembers[].threat	Related Indicator.Value	.campaignMembers[].type	value.campaignMembers[].threatTime	http://86.203.178.68.host.secureserver.net/.n0t49083/...	Indicator type computed by using `Proofpoint Threat`

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					Type Mapping

Proofpoint TAP - Fetch Threat by ID (supplemental)

The Fetch Threat by ID feed ingests information about threats (indicators) sent in campaigns.

`GET https://tap-api-v2.proofpoint.com/v2/threat/summary/{THREAT_ID}`

Sample Response:


```
{
    "id": "91d97d8d0e4dd1354c4d0a00f97717c6c165480002e3176fcc5c65bc4ca2e786",
    "identifiedAt": "2023-08-11T00:30:15.000Z",
    "name": "29e1885a1a422f2963630c515518085dc75f24d3f3adaf87896684af47d1a64a",
    "type": "attachment",
    "category": "malware",
    "status": "active",
    "severityScore": 105,
    "attackSpread": 273,
    "notable": false,
    "verticallyTargeted": false,
    "geoTargeted": false,
    "actors": [
        {
            "id": "3ba7ed7e-c62b-4009-b736-a1e190ad31b2",
            "name": "TA2725"
        }
    ],
    "families": [
        {
            "id": "69a63403-f478-40f6-a4cb-3d2ffb85b98e",
            "name": "Keylogger"
        }
    ],
    "malware": [
        {
            "id": "4b500558-23d0-4a9b-901a-1cb4cf8a21fb",
            "name": "AgentTesla"
        }
    ],
    "techniques": [
        {
            "id": "e8eae353-317b-4211-8a87-7d4b6baf9f2c",
            "name": "PDF"
        },
        {
            "id": "e48835be-e1b5-4e20-a1aa-d1a85494067c",
            "name": "Compressed Executable"
        }
    ],
    "brands": [
        {
            "id": "c9fed353-317b-4211-8a87-6a3b6baf9f2c",
```

```
            "name": "Some Brand Name"
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.category	Related Indicator.Attribute	Category	value.campaign Members[].threatTime	malware	N/A
.severityScore	Related Indicator.Attribute	Severity	value.campaign Members[].threatTime	105	Updated if it already exists.
.attackSpread	Related Indicator.Attribute	Attack Spread	value.campaign Members[].threatTime	273	Updated if it already exists.
.notable	Related Indicator.Attribute	Is Notable	value.campaign Members[].threatTime	False	Updated if it already exists.
.verticallyTargeted	Related Indicator.Attribute	Is Vertically Targeted	value.campaign Members[].threatTime	False	Updated if it already exists.
.geoTargeted	Related Indicator.Attribute	Is Geographically Targeted	value.campaign Members[].threatTime	False	Updated if it already exists.
.families[].name	Related Indicator.Attribute	Malware Type	value.campaign Members[].threatTime	Keylogger	N/A
.malware[].name	Related Indicator.Attribute	Malware Family	value.campaign Members[].threatTime	AgentTesla	N/A
.techniques[].name	Related Indicator.Attribute	Technique	value.campaign Members[].threatTime	PDF	N/A
.actors[].name	Related Indicator.Attribute	Related Actor	value.campaign Members[].threatTime	TA2725	N/A
.brands[].name	Related Indicator.Attribute	Affected Brand	value.campaign Members[].threatTime	Some Brand Name	N/A
.id	Related Indicator.Attribute	Threat ID	value.campaign Members[].threatTime	91d97d8d0e4dd1354c4d0a00f97717c6c165480002e3176fcc5c65bc4ca2e786	N/A

Proofpoint TAP - Fetch Forensics (Supplemental)

The Fetch Forensics Supplemental feed ingests forensics information about a campaign if the user field Fetch Campaign Forensics is enabled.

```
GET https://tap-api-v2.proofpoint.com/v2/forensics?campaignId={CAMPAIGN_ID}
```

Sample Response:


```
{
   "generated": "2023-08-16T19:03:50.378Z",
   "reports": [
      {
         "scope": "CAMPAIGN",
         "id": "6d91144e-204f-4bee-8e87-f1ae598e8da1",
         "name": "AgentTesla | PDF Attachments | \"adobeuplate\" | 15 August
2023",
         "forensics": [
            {
               "type": "attachment",
               "display": "Malicious attachment with SHA-256:
6e164c98d26cbff1cd1b3935b236a2fe228a011a197b7d3763f6803210d19f1e",
               "engine": "iee",
               "malicious": true,
               "time": 0,
               "what": {
                  "sha256":
"6e164c98d26cbff1cd1b3935b236a2fe228a011a197b7d3763f6803210d19f1e",
                  "blacklisted": true
               },
               "platforms": [
                  {
                     "name": "Win10",
                     "os": "win",
                     "version": "win10"
                  }
               ]
            },
            {
               "type": "behavior",
               "display": "ET INFO Windows Powershell User-Agent Usage",
               "engine": "iee",
               "malicious": false,
               "note": "ET INFO Windows Powershell User-Agent Usage",
               "time": 0,
               "what": {
                  "rule": "etpro_2033355"
               },
               "platforms": [
                  {
                     "name": "Win10",
```

```
                    "os": "win",
                    "version": "win10"
                }
            ]
        }
    ]
  }
]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.reports[].forensics[].what.sha256	Indicator.Value	SHA-256	N/A	6e164c98d26cbff1cd1b3935b236a2fe228a011a197b7d3763f6803210d19f1e	If `.reports[].forensics[].type` is `attachment`, `file` or `url`
.reports[].forensics[].what.md5	Indicator.Value	MD5	N/A	N/A	If `.reports[].forensics[].type` is `attachment`, `file` or `url`
.reports[].forensics[].what.fqdn	Indicator.Value	FQDN	N/A	N/A	If `.reports[].forensics[].type` is `dns`
.reports[].forensics[].what.ips	Indicator.Value	IP Address	N/A	N/A	If `.reports[].forensics[].type` is `dns`
.reports[].forensics[].what.ip	Indicator.Value	IP Address	N/A	N/A	If `.reports[].forensics[].type` is `url`
.reports[].forensics[].what.path	Indicator.Value	File Path	N/A	N/A	If `.reports[].forensics[].type` is `dropper` or `file`
.reports[].forensics[].what.url	Indicator.Value	URL	N/A	N/A	If `.reports[].forensics[].type` is `dropper` or `url`
.reports[].forensics[].what.name	Indicator.Value	Mutex	N/A	N/A	If `.reports[].forensics[].type` is `mutex`
.reports[].forensics[].what.key	Indicator.Value	Registry Key	N/A	N/A	If `.reports[].forensics[].type` is `registry`
.reports[].forensics[].what.key	Indicator.Value	Registry Key	N/A	N/A	If `.reports[].forensics[].type` is `registry`
.reports[].forensics[].what.blacklisted	Indicator.Attribute	Is Blacklisted	N/A	True	N/A
.reports[].forensics[].type	Indicator.Attribute	Type	N/A	attachment	N/A
.reports[].forensics[].what.port	Indicator.Attribute	Port	N/A	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.reports[].forensics[].what.protocol	Indicator.Attribute	Protocol	N/A	N/A	N/A
N/A	Indicator.Attribute	Is Malicious	N/A	True	Always true because non-malicious data is filtered out.
.reports[].forensics[].display, .reports[].forensics[].platforms	Related Campaign.Description	N/A	N/A	True	If `.reports[].forensics[].type` is `behavior`.
.reports[].forensics[].what.url	Related Campaign.Description	N/A	N/A	True	If `.reports[].forensics[].type` is `screenshot`.

Proofpoint TAP Emails

`GET https://tap-api-v2.proofpoint.com/v2/siem/all`

Sample Response:


```
{
  "clicksPermitted": [
    {
      "url": "https://kul.ink/LyZu",
      "classification": "spam",
      "clickTime": "2021-03-29T18:08:16.000Z",
      "threatTime": "2021-03-30T15:36:54.000Z",
      "userAgent": "Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0)
like Gecko",
      "campaignId": "",
      "id": "b92f6d79-aeec-4bc4-8fdb-ee9929f96856",
      "clickIP": "12.12.12.12",
      "sender": "",
      "recipient": "user1@example.com",
      "senderIP": "78.159.108.31",
      "GUID": "21utHx_zcMEWcrZJEwVt8h-HU7GtkcVF",
      "threatID":
"4d07e404b62d36aa6cf7c1712f12ee00836be10942abf1740090b88ea209019b",
      "threatURL": "https://threatinsight.proofpoint.com/011ae236-5630-b11c-
efa9-799e8c978947/threat/email/123",
      "threatStatus": "active",
      "messageID": "<01000nhxALbx7pjR-6XpAKxD-HLCE-0x1m-gqMY-
VQ3KUl2DOGJT-000000@email.amazonses.com>"
    },
    {
      "url": "https://kul.ink/LyZu",
      "classification": "spam",
      "clickTime": "2021-03-29T17:53:39.000Z",
      "threatTime": "2021-03-30T15:36:54.000Z",
      "userAgent": "Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0)
like Gecko",
      "campaignId": "",
      "id": "037333e0-c162-4c3e-9579-e2d870197e79",
      "clickIP": "12.12.12.12",
      "sender": "",
      "recipient": "user1@example.com",
      "senderIP": "78.159.108.27",
      "GUID": "Xfa7pjHNgP-hexGor7RIlyZepOYHBDI_",
      "threatID":
"4d07e404b62d36aa6cf7c1712f12ee00836be10942abf1740090b88ea209019b",
      "threatURL": "https://threatinsight.proofpoint.com/011ae236-5630-b11c-
efa9-799e8c978947/threat/email/123",
      "threatStatus": "active",
      "messageID": "<01000CIc2hlQgxeY-VRkGfep-Flge-Awkx-VbdI-
```

```
maz8c7lXnV3A-000000@email.amazonses.com>"
    },
    {
      "url": "https://drive.google.com/file/d/
1e2Hov_WTbQ21WuXujDXe1R1kFQVuUkFD/view?usp=sharing",
      "classification": "phish",
      "clickTime": "2021-03-27T18:13:19.000Z",
      "threatTime": "2021-03-30T16:20:12.000Z",
      "userAgent": "Mozilla/5.0 (Windows NT 6.3; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/89.0.4389.90 Safari/537.36 Edg/89.0.774.57",
      "campaignId": "",
      "id": "08493af3-5207-4347-845b-938ecc85e723",
      "clickIP": "12.12.12.12",
      "sender": "user1@example.com",
      "recipient": "user1@example.com",
      "senderIP": "66.163.191.147",
      "GUID": "lC4DCoxP2ydvf9Grk2JA9h4OZfk1rj6_",
      "threatID":
"4ed0ba2a159f3e774346185a9a454ca5c24908685d697b2cd3d91c9fc3bfe7d4",
      "threatURL": "https://threatinsight.proofpoint.com/011ae236-5630-b11c-
efa9-799e8c978947/threat/email/123",
      "threatStatus": "cleared",
      "messageID": "<1902302406.673823.1616768722115@mail.yahoo.com>"
    },
  ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.clicksPermitted[].url	Indicator.Value	URL	https://kul.ink/LyZu	N/A
.clicksPermitted[].recipient	Corporate_Email.Value	N/A	user1@example.com	N/A
.clicksPermitted[].sender	Indicator.Value	Email Address	roger73martinez@yahoo.com	N/A
.clicksPermitted[].clickTime	Incident.started_at	N/A	"2021-03-29T18:08:16.000Z"	N/A

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 Events

METRIC	RESULT
Run Time	1 minute
Corporate Emails	80
Indicators	212
Indicator Attributes	283
Incidents	120

Proofpoint Campaigns

METRIC	RESULT
Run Time	1 minute
Campaign	1
Campaign Attributes	3
Indicators	3

METRIC	RESULT
Indicator Attributes	21
Adversary	1
Malware	1
TTP	2

Proofpoint Emails

METRIC	RESULT
Run Time	1 minute
Corporate Emails	80
Indicators	212

Known Issues / Limitations

- Manual Runs - the following are known limitations when performing manual runs:
  - The time range must be within the last 7 days.
  - The feeds will only fetch time ranges of 48 hours or less, starting from the end date.
  - The start time must be at least 1 minute before the end time.

Change Log

- **Version 1.1.0**
  - Added two new feeds:
    - Proofpoint TAP Campaigns
    - Proofpoint TAP Events
  - Updated the Integration name to Proofpoint TAP CDF.
  - Added a new Known Issues / Limitations entry regarding manual runs.
  - Updated the minimum ThreatQ version to 5.10.0.
- **Version 1.0.0**
  - Initial release