ThreatQuotient

Proofpoint TAP Emails CDF Guide

Version 1.0.0 rev-a

August 15, 2022

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

Integration Details 5
Introduction 6
Prerequisites 7
Corporate Email Custom Object 7
Installation 9
Configuration 10
ThreatQ Mapping 11
Proofpoint TAP ClicksPermitted 11
Average Feed Run 13
Known Issues / Limitations 14
Change Log 15

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	1.0.0
Compatible with ThreatQ Versions	>= 4.40.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/proofpoint-tap-emails

Introduction

The Proofpoint TAP (Targeted Attack Protection) Emails 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 ClicksPermitted** - `https://tap-api-v2.proofpoint.com/v2/siem/all`

The integration ingests the following system objects:

- Corporate Emails
- Incidents
- Indicators
    - Indicator Attributes

Prerequisites

Review the integration prerequisites before attempting to install the integration.

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 custom object 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 a 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 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 parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Proofpoint TAP Principal	The Proofpoint TAP Principal.
Proofpoint TAP Secret	The Proofpoint TAP Secret.
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.

   > You will have to set the time range by clicking Run Integration. See the Known Issues / Limitations section for further details.

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 TAP ClicksPermitted

`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.

With Time Range (UTC): 03/30/2021 04:11pm to 03/30/2021 05:12pm

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

Known Issues / Limitations

- The time range must be within the last 7 days and the start time must be before the end time by at least 1 minute.
- The feed only fetches time ranges of 48 hours or less, starting from the end date.

Change Log

- **Version 1.0.0 rev-a**
  - Guide Update - Updated the corporate email definition. Updated the guide to include new custom boject installation process.
- **Version 1.0.0**
  - Initial release