ThreatQuotient

Phishlabs Feed Implementation Guide

Version 1.0.0

Tuesday, December 3, 2019

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, December 3, 2019

Contents

Versioning

- Current integration version `1.0.0`
- Supported on ThreatQ versions >= `4.24.0`

Introduction

The Phishlabs feed ingests threat intelligence data from the following endpoint:

- https://caseapi.phishlabs.com/idapi/v1/incidents/:service

Notes:

- Uses basic HTTP authentication based on email address and API key.

  > ThreatQuotient does not issue third-party credentials. Contact Phishlabs for the required credentials.

- Time constrained data fetching is possible.

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 **Phishlabs** 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
Email Address	The vendor-supplied email address.
API Key	The vendor-supplied API Key.
Service	Service name used to filter incidents. Defaults to **EIR**.

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

ThreatQ Mapping

The Phishlabs feed provides an API that users can use to extract data in JSON format.

JSON Response Sample


```
{
    "metadata": {
        "count": 1
    },
    "incidents": [
        {
            "id": "INC0763488",
            "service": "EIR",
            "title": "Fwd: CONFIRMATION OF YOUR OVERDUE
PAYMENT BY ATTACHE FILE",
            "description": "",
            "status": "Closed",
            "details": {
                "caseType": "Payload",
                "classification": "Do Not Engage",
                "subClassification": "Do Not Engage",
                "severity": null,
                "emailReportedBy": "Billy Smith <bsmith@ph-
ishlabs.com>",
                "submissionMethod": "Forwarded",
                "sender": "Billy Smith <bsmith@ph-
ishlabs.com>",
                "emailBody": "\"\\r\\n\\r\\nBilly
Smith\\r\\n843-283-7421\\r\\n\\r\\nBegin forwarded
```

```
message:\\r\\n\\r\\nFrom: UN ECOSOC / 2019 <chin-
a@medicalcables.eu>\\r\\nDate: November 17, 2019 at 5:22:31 PM
EST\\r\\nSubject: CONFIRMATION OF YOUR OVERDUE PAYMENT BY
ATTACHE FILE\\r\\nReply-To: <services@etscc.com>\\r\\n\\r\\n
[External]\\r\\nDear Sir/Madam, Please confirm the attache mes-
sage file for more information regard of your payment. Best
Regards, World Bank Group Finance Ministry\\r\\n\\r\\nExternal
email\\r\\n\\r\\nForward suspicious emails to bad@ph-
ishlabs.com\\r\\n\"",
                "urls": [
                    {
                        "url": "http://purl.or-
g/dc/elements/1.1/",
                        "malicious": false,
                        "maliciousDomain": false
                    },
                    {
                        "url": "https://www.un-
.org/press/en/2005/ik486.doc.htm",
                        "malicious": false,
                        "maliciousDomain": false
                    },
                    {
                        "url": "http://www.un.org/",
                        "malicious": false,
                        "maliciousDomain": false
                    },
                    {
                        "url":
```

```
"http://ns.adobe.com/xap/1.0/mm/",
                        "malicious": false,
                        "maliciousDomain": false
                    },
                    {
                        "url": "http://ns.adobe.com/pdf/1.3/",
                        "malicious": false,
                        "maliciousDomain": false
                    },
                    {
                        "url": "http://www.w3.org/1999/02/22-
rdf-syntax-ns#",
                        "malicious": false,
                        "maliciousDomain": false
                    },
                    {
                        "url": "http://ns.adobe.com/xap/1.0/",
                        "malicious": false,
                        "maliciousDomain": false
                    }
                ],
                "attachments": [
                    {
                        "fileName": "ATT00001.htm",
                        "mimeType": "text/html",
                        "md5": "07cbbf25d210d17c6d-
f7ce17695a8f5f",
                        "sha256":
```

```
"e19f4d5b6a2341e3ba9437f152f4f6739f-
d8a0842fbc36d531ffa7ec938a289f",
                        "malicious": false
                    }
                ],
                "furtherReviewReason": null,
                "offlineUponReview": false
            },
            "created": "2019-11-17T22:23:16Z",
            "modified": "2019-11-17T22:37:27Z",
            "closed": "2019-11-17T22:37:27Z",
            "duration": 852
        }
    ]
}
```

The mapping table is below.

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
incidents.title	incident.value	Value	"Fwd: CONFIRMATION OF YOUR OVERDUE PAYMENT BY ATTACHE FILE"	
incidents.description	incident.description	Description	""	
incidents.created	incident.published_at	Published At	"2019-11-17T22:23:16Z"	
incidents.id	incident.attribute	ID	"INC0763488"	
incidents.details.caseType	incident.attribute	Case Type	"Payload"	
incidents.details.classification	incident.attribute	Classification	"Do Not Engage"	
incidents.details.subClassification	incident.attribute	Subclassification	"Do Not Engage"	
incidents.details.severity	incident.attribute	Severity	"Low"	
incidents.details.emailReportedBy	incident.attribute	Email Reported By	"Billy Smith bsmith@phishlabs.com"	

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
incidents.details.emailBody	incident.attribute	Email Body	""\r\n\r\nBilly Smith\r\n843-283-7421\r\n\r\nBegin forwarded..."	
incidents.details.submissionMethod	incident.attribute	Submission Method	"Forwarded"	
incidents.details.sender	incident.attribute	Sender	"Billy Smith bsmith@phishlabs.com"	
incidents.details.furtherReviewReason	incident.attribute	Further Review Reason	"reason example	
incidents.details.offlineUponReview	incident.attribute	Offline Upon Review	false	
incidents.status	incident.attribute	Status	"Closed"	
incident.modified	incident.attribute	Modified At	"2019-11-17T22:23:16Z"	
incident.closed	incident.attribute	Closed At	"2019-11-17T22:23:16Z"	
incident.duration	incident.attribute	Duration	852	

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
incident.service	incident.attribute	Service	"EIR"	
incident.details.urls	related indicators	Indicator		see URL Indicators mappings
incident.details.attachments	related indicators	Indicator		see Attachments Indicators mappings

URL Indicator Mappings

JSON response sample


```
[{
    "url": "http://purl.org/dc/elements/1.1/",
    "malicious": false,
    "maliciousDomain": false
},
{
    "url": "https://www.un.org/press/en/2005/ik486.doc.htm",
    "malicious": false,
    "maliciousDomain": false
},
{
    "url": "http://www.un.org/",
    "malicious": false,
    "maliciousDomain": false
}]
```

The mapping table is below.

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
url	indicator.value	Value	http://purl.org/dc/elements/1.1/	
malicious	indicator.attribute	Malicious URL	false	
maliciousDomain	indicator.attribute	Malicious Domain	true	

Attachment Indicators Mappings

JSON Response Sample

```
[{
    "fileName": "ATT00001.htm",
    "mimeType": "text/html",
    "md5": "07cbbf25d210d17c6df7ce17695a8f5f",
    "sha256": "e19f4d5b6a2341e3ba9437f152f4f6739f-
d8a0842fbc36d531ffa7ec938a289f",
    "malicious": false
}]
```

The mapping table is below.

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
fileName	indicator.value	Value	ATT00001.htm	Indicator of type "Filename"
md5	indicator.value	Value	07cbbf25d210d17c6df7ce17695a8f5f	Indicator of type "MD5"
sha256	indicator.value	Value	e19f4d5b6a2341e3ba9437f152f4f6739fd8a0842fbc36d531ffa7ec938a289f	Indicator of type "SHA-256"
malicious	indicator.attribute	Malicious Domain	true	
mimeType	indicator.attribute	Mime Type	text/html	
* An indicator of type Filename, MD5 and SHA-256 will be created from the values of the fields "fileName", "sha256" and "md5". Each of these indicators will have the attributes from the fields "malicious" and "mimeType".				