ThreatQuotient

Phishlabs CDF User Guide

Version 1.1.0

October 18, 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	>= 4.24.0
Support Tier	ThreatQ Supported

Introduction

The Phishlabs CDF ingests a comprehensive list of Indicators and their related IOCs. The integration provides the following feed:

- **Phishlabs** - ingests indicators and related IOCs.

The integration ingests the following system objects:

- Incidents
  - Incident Attributes
- Indicators
  - Indicator Attributes

Installation

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
Email Address	Your Phishlabs account email address.
API Key	Your Phishlabs account API key.
Service	The service name used to filter incidents. The default setting is "EIR".

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

Phishlabs

The Phishlabs feed ingests indicators and related IOCs.

Sample Response:


```
{
    "metadata": {
        "count": 1
    },
    "incidents": [
        {
            "id": "INC0763488",
            "service": "EIR",
            "title": "Fwd: CONFIRMATION OF YOUR OVERDUE PAYMENT BY ATTACHE
FILE",
            "description": "Incident description",
            "status": "Closed",
            "details": {
                "caseType": "Payload",
                "classification": "Do Not Engage",
                "subClassification": "Do Not Engage",
                "severity": null,
                "emailReportedBy": "Billy Smith <bsmith@phishlabs.com>",
                "submissionMethod": "Forwarded",
                "sender": "Billy Smith <bsmith@phishlabs.com>",
                "emailBody": "\"\\r\\n\\r\\nBilly Smith\\r\\n843-283-7421\\r\
\n\\r\\nBegin forwarded message:\\r\\n\\r\\nFrom: UN ECOSOC / 2019
<china@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 message 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@phishlabs.com\\r\\n\"",
                "urls": [
                    {
                        "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
                    },
                    {
                        "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": "07cbbf25d210d17c6df7ce17695a8f5f",
                        "sha256":
"e19f4d5b6a2341e3ba9437f152f4f6739fd8a0842fbc36d531ffa7ec938a289f",
                        "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
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.incidents[].title, .incidents[].id	incident.value	N/A	.incidents[].created	"Fwd: CONFIRMATION OF YOUR OVERDUE PAYMENT BY ATTACHE FILE - INC0763488"	An incident's in th `{{title}} -` `.incidents[]` has a value; ot `.incidents`
.incidents[].description	incident.description	N/A	.incidents[].created	"Incident description"	
.incidents[].id	incident.attribute	ID	.incidents[].created	"INC0763488"	
.incidents[].details.caseType	incident.attribute	Case Type	.incidents[].created	"Payload"	
.incidents[].details.classification	incident.attribute	Classification	.incidents[].created	"Do Not Engage"	
.incidents[].details.subClassification	incident.attribute	Subclassification	.incidents[].created	"Do Not Engage"	
.incidents[].details.severity	incident.attribute	Severity	.incidents[].created	"Low"	
.incidents[].details.emailReportedBy	incident.attribute	Email Reported By	.incidents[].created	"Billy Smith bsmith@phishlabs.com"	
.incidents[].details.emailBody	incident.attribute	Email Body	.incidents[].created	""\r\n\r\nBilly Smith\r\n843-283-7421\r\n\r\nBegin forwarded..."	
.incidents[].details.submissionMethod	incident.attribute	Submission Method	.incidents[].created	"Forwarded"	
.incidents[].details.sender	incident.attribute	Sender	.incidents[].created	"Billy Smith bsmith@phishlabs.com"	
.incidents[].details.furtherReviewReason	incident.attribute	Further Review Reason	.incidents[].created	"reason example	
.incidents[].details.offlineUponReview	incident.attribute	Offline Upon Review	.incidents[].created	false	
.incidents[].status	incident.attribute	Status	.incidents[].created	"Closed"	
.incidents[].modified	incident.attribute	Modified At	.incidents[].created	"2019-11-17T22:23:16Z"	
.incidents[].closed	incident.attribute	Closed At	.incidents[].created	"2019-11-17T22:23:16Z"	
.incidents[].duration	incident.attribute	Duration	.incidents[].created	852	
.incidents[].service	incident.attribute	Service	.incidents[].created	"EIR"	
.incidents[].details.urls	indicator.value	URL	.incidents[].created		see URL In m
.incidents[].details.attachments	indicator.value	Filename / MD5 / SHA-256	.incidents[].created		see Atta Indicators m
.incidents[].details.sender	indicator.value	Email Address	.incidents[].created	"bsmith@phishlabs.com"	this indicator i by extracting t incidents.detail

URL Indicator Mapping

Sample Response:

```
[
  {
    "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
}
]
```

ThreatQuotient provides the following default mapping:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES
url	indicator.value	URL	"http://purl.org/dc/elements/1.1/"
malicious	indicator.attribute	Malicious URL	false
maliciousDomain	indicator.attribute	Malicious Domain	true

Attachment Indicators Mapping

Sample Response:

```
[
  {
    "fileName": "ATT00001.htm",
    "mimeType": "text/html",
    "md5": "07cbbf25d210d17c6df7ce17695a8f5f",
    "sha256":
"e19f4d5b6a2341e3ba9437f152f4f6739fd8a0842fbc36d531ffa7ec938a289f",
    "malicious": false
}
]
```

ThreatQuotient provides the following default mapping:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
leName	indicator.value	Filename	"ATT00001.htm"	Indicator of type "Filename"
md5	indicator.value	MD5	"07cbbf25d210d17c6df7ce17695a8f5f"	Indicator of type "MD5"
sha256	indicator.value	SHA-256	"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".

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.

Phishlabs

METRIC	RESULT
Run Time	1 minute
Indicators	1,017
Indicator Attributes	3,175
Incidents	194
Incidents Attributes	2,687

Change Log

- **Version 1.1.0**
  - Parse out an Email Address Indicator from the Sender Attribute (if it contains an email address)
  - Append `ID` to the `Title` to make it unique: `{Title} - {ID}`
- **Version 1.0.0**
  - Initial release