ThreatQuotient

Cofense Triage CDF Guide

Version 1.1.3

May 22, 2022

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Support **4**
Versioning **5**
Introduction **6**
Installation **7**
Configuration **8**
ThreatQ Mapping **10**
Cofense Triage 10
Cofense Triage Owner (supplemental) 13
Cofense Triage Report (supplemental) 14
Cofense Triage Domains (supplemental) 18
Cofense Triage Hostnames (supplemental) 20
Cofense Triage URLS (supplemental) 22
Cofense Triage Rules (supplemental) 24
Indicator Type 26
Status and Threat Type 26
Average Feed Run **27**
Known Issues / Limitations **28**
Change Log **29**

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.

Versioning

- Current integration version: `1.1.3`
- Compatible with ThreatQ versions >= `4.38.0`

Introduction

The Confense Triage CDF for ThreatQ ingests Identities, Indicators, Reports and Signature objects as well as their attributes. Cofense Triage, a phishing-specific incident response platform, helps stop active phishing attacks in progress. By leveraging real-time, internally reported attack intelligence from conditioned users, Cofense Triage makes it easy to stop phishing attacks in progress by eliminating the noise of the abuse mailbox, automating standard responses, and orchestrating across other security systems to quickly respond to and eliminate phishing threats.

The integration provides the following feeds:

- **Cofense Triage** - fetches all the indicator present on the Cofense DB.
- **Cofense Triage Owner (supplemental)** - fetches related Identities and their attributes to a given Indicator Id.
- **Cofense Triage Report (supplemental)** - fetches related Reports and their attributes to a given Indicator Id.
- **Cofense Triage Domains (supplemental)** - fetches related FQDNs to a given Report Id.
- **Cofense Triage Hostnames (supplemental)** - fetches related FQDNs to a given Report Id.
- **Cofense Triage URLS (supplemental)** - fetches related URLs to a given Report Id.
- **Cofense Triage Rules (supplemental)** - fetches related Rules and their attributes to a given Report Id.

The integration ingests the following system objects:

- Identities
  - Identity Attributes
- Indicators
  - Indicator Attributes
- Reports
  - Report Attributes
- Signatures
  - Signature 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:

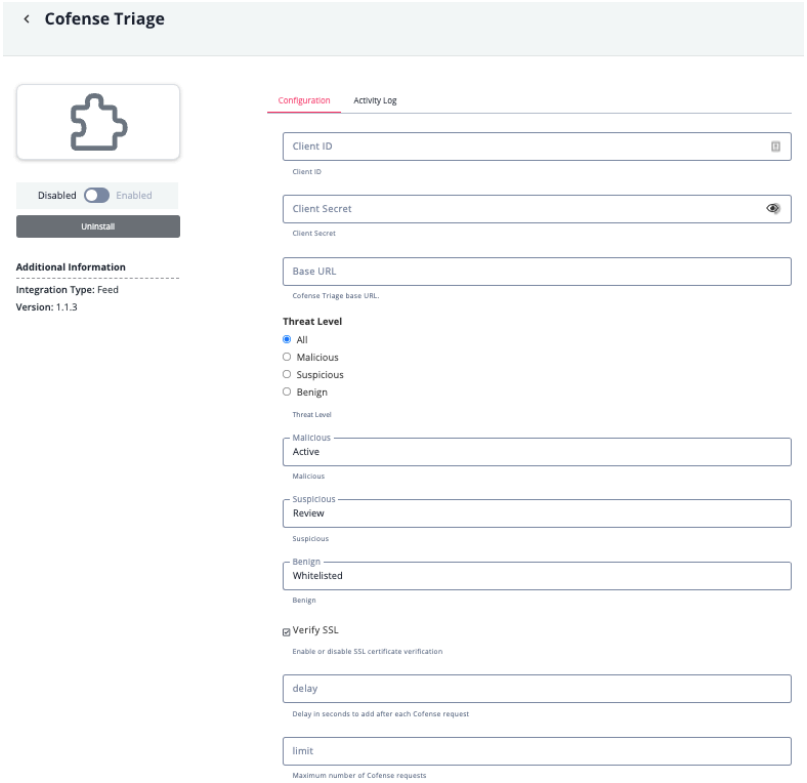
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameter under the **Configuration** tab:

PARAMETER	DESCRIPTION
Client ID	Your Cofense Client ID.
Client Secret	Your Cofense Client Secret.
Base URL	The Cofense Triage base URL. Example: `https://www.exampledomain.com/public/api`
Threat Level	Use this option to filter the response based on the threat. Options include: ◦ All (default) ◦ Malicious ◦ Suspicious ◦ Benign

PARAMETER	DESCRIPTION
Malicious	Set the custom mapping status for Malicious indicators.
Suspicious	Set the custom mapping status for Suspicious indicators.
Benign	Set the custom mapping status for Benign indicators.
Verify SSL	Enable or disable verification of the server's SSL certificate.
Delay	Delay in seconds to add after each Cofense request. See the Known Issues / Limitations chapter for more details on this parameter.
Request Limit	The maximum number of Cofense requests. See the Known Issues / Limitations chapter for more details on this parameter.



5. Review the **Settings** configuration, 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

Cofense Triage

The Cofense Triage feed fetches all the indicator present on the Cofense DB.

`GET {{base_url}}/api/public/v2/threat_indicators`

Sample Response:


```
{
  "data":[
    {
            "id": "20",
            "type": "threat_indicators",
            "links": {
                "self": "https://reltest6.phishmecloud.com/api/public/v2/threat_indicators/20"
            },
            "attributes": {
                "threat_level": "Malicious",
                "threat_type": "Header",
                "threat_value": "To:service@1105media.com",
                "threat_source": "Triage-UI",
                "created_at": "2020-11-02T16:12:47.426Z",
                "updated_at": "2020-11-02T16:12:47.439Z"
            },
            "relationships": {
                "owner": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/threat_indicators/20/relationships/
owner",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/threat_indicators/20/owner"
                    },
                    "data": {
                        "type": "operators",
                        "id": "2"
                    }
                },
                "reports": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/threat_indicators/20/relationships/
reports",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/threat_indicators/20/reports"
                    }
                },
                "comments": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/threat_indicators/20/relationships/
comments",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/threat_indicators/20/comments"
                    }
                }
            }
```

```
        },
        {
            "id": "24",
            "type": "threat_indicators",
            "links": {
                "self": "https://reltest6.phishmecloud.com/api/public/v2/threat_indicators/24"
            },
            "attributes": {
                "threat_level": "Suspicious",
                "threat_type": "URL",
                "threat_value": "https://pages.egress.com/UnsubscribePage.html?
mkt_unsubscribe=1&mkt_tok=eyJpIjoiTUdKak5XUm1OekEyTkRrMCIsInQiOiJpd0ZzUEFvUlRBeWljb1RtTWEvRHpWRGtGNGplbDB2RTNYek1VOEI
ycG11VzVKbHFIdEw4U1loUXhmQlFiV2NBcGFvbmRyaGZ1b1lvaGNiM3FqOUk3WXlFeTV1OEcxampUcTI3N2ZPOHpYWm1WUi9JcHQzVS9ybFJOT1E3NURJ
TCJ9?utm_medium=email&utm_source=marketo&utm_campaign=Event-(ISC)2SecurityCongress-11-20",
                "threat_source": "Triage-UI",
                "created_at": "2020-11-03T19:35:20.636Z",
                "updated_at": "2020-11-03T19:35:20.643Z"
            },
            "relationships": {
                "owner": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/threat_indicators/24/relationships/
owner",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/threat_indicators/24/owner"
                    },
                    "data": {
                        "type": "operators",
                        "id": "2"
                    }
                },
                "reports": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/threat_indicators/24/relationships/
reports",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/threat_indicators/24/reports"
                    }
                },
                "comments": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/threat_indicators/24/relationships/
comments",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/threat_indicators/24/comments"
                    }
                }
            }
        }],
  "meta": {
        "record_count": 4794,
        "page_count": 240
    }
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data[].attributes.threat_value`	Indicator.Value	`.data[].attributes.threat_type`	`.data[].attributes.created_at`	To:service@1105media.com	The ThreatQ Object Type is determinate by the value on the `threat_type` key
`.data[].id`	Indicator.Attribute	ID	`.data[].attributes.created_at`	20	N/A
`.data[].attributes.threat_level`	Indicator.Attribute	Threat Level	`.data[].attributes.created_at`	Malicious	N/A
`.data[].attributes.threat_source`	Indicator.Attribute	Threat Source	`.data[].attributes.created_at`	Triage-UI	N/A
`.data[].relationships.owner.data.id`	Indicator.Attribute	Operator ID	`.data[].attributes.created_at`	2	N/A

Cofense Triage Owner (supplemental)

The Cofense Triage Owner supplemental feed fetches related Identities and their attributes to a given Indicator Id.

```
GET {{base_url}}/api/public/v2/threat_indicators/{id}/owner
```

Sample Response:


```
{
    "data": {
        "id": "2",
        "type": "operators",
        "links": {
            "self": "https://reltest6.phishmecloud.com/api/public/v2/operators/2"
        },
        "attributes": {
            "email": "mike.saurbaugh@cofense.com",
            "first_name": "Mike",
            "last_name": "Saurbaugh",
            "nickname": "MikeSaurbaugh",
            "time_zone": "Eastern Time (US & Canada)"
        }
    }
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data.attributes.email`	Identity.Value	N/A	N/A	mike.saurbaugh@cofense.com	Only for `.data.type` == operator
`.data.attributes.name`	Identity.Value	N/A	N/A	XSOAR_CDS_OP	Only for `.data.type` != operator
`.data.type`	Identity.Attribute	Owner Type	N/A	operators	N/A
`.data.attributes.first_name`	Identity.Attribute	First Name	N/A	Mike	Only for `.data.type` == operator
`.data.attributes.last_name`	Identity.Attribute	Last Name	N/A	Saurbaugh	Only for `.data.type` == operator
`.data.attributes.nickname`	Identity.Attribute	Nickname	N/A	MikeSaurbaugh	Only for `.data.type` == operator
`.data.attributes.time_zone`	Identity.Attribute	Time Zone	N/A	Eastern Time (US & Canada)	Only for `.data.type` == operator
`.data.attributes.grant_type`	Identity.Attribute	Grant Type	N/A	client_credentials	Only for `.data.type` != operator

Cofense Triage Report (supplemental)

The Cofense Triage Report supplemental feed fetches related Reports and their attributes to a given Indicator Id.

`GET {{base_url}}/api/public/v2/threat_indicators/{id}/reports`

Sample Response:


```
{"data":[{
            "id": "650",
            "type": "reports",
            "links": {
                "self": "https://reltest6.phishmecloud.com/api/public/v2/reports/650"
            },
            "attributes": {
                "location": "Inbox",
                "risk_score": 99,
                "from_address": "mike.saurbaugh@cofense.com",
                "subject": "Re: Suspicious domain testing - 12/3",
                "received_at": "2020-12-03T20:22:41.000Z",
                "reported_at": "2020-12-03T20:22:39.000Z",
                "raw_headers": "Date: Thu, 03 Dec 2020 20:23:09 +0000\r\nFrom: Mike.Saurbaugh@cofense.com\r\nTo:
Mike.Saurbaugh@cofense.com\r\nMessage-ID:
<5fc9492d6fd6_27a2adc002fd9cc89058@ip-10-132-9-81.ec2.internal.mail>\r\nSubject: Re: Suspicious domain testing -
12/3\r\nMime-Version: 1.0\r\nContent-Type: multipart/mixed;\r\n boundary=\"--
==_mimepart_5fc9492d6cbb_27a2adc002fd9cc8897b\";\r\n charset=UTF-8\r\nContent-Transfer-Encoding: 7bit",
                "text_body": "Adding a new domain to see if this updates the SIR 13867\r\n\r\nSuspicious
domain<atis.ug>\r\n\r\n\r\nFrom: Mike Saurbaugh <Mike.Saurbaugh@cofense.com>\r\nDate: Saturday, October 31, 2020 at
11:43 AM\r\nTo: Mike Saurbaugh <Mike.Saurbaugh@cofense.com>\r\nSubject: Suspicious domain testing\r\n\r\nThis is a s
suspicious domain<http://zavagilsanti.com/>\r\n\r\nwww.google.com<http://www.google.com>\r\n\r\n\r\n\r\n",
                "html_body": "<html xmlns:o=\"urn:schemas-microsoft-com:office:office\" xmlns:w=\"urn:schemas-
microsoft-com:office:word\" xmlns:m=\"http://schemas.microsoft.com/office/2004/12/omml\" xmlns=\"http://www.w3.org/
TR/REC-html40\">\r\n<head>\r\n<meta http-equiv=\"Content-Type\" content=\"text/html; charset=utf-8\">\r\n<meta
name=\"Generator\" content=\"Microsoft Word 15 (filtered medium)\">\r\n<style><!--\r\n/* Font Definitions */
\r\n@font-face\r\n\t{font-family:\"Cambria Math\";\r\n\tpanose-1:2 4 5 3 5 4 6 3 2 4;}\r\n@font-face\r\n\t{font-
family:Calibri;\r\n\tpanose-1:2 15 5 2 2 2 4 3 2 4;}\r\n/* Style Definitions */\r\np.MsoNormal, li.MsoNormal,
div.MsoNormal\r\n\t{margin:0in;\r\n\tfont-size:12.0pt;\r\n\tfont-family:\"Calibri\",sans-serif;}\r\na:link,
span.MsoHyperlink\r\n\t{mso-style-priority:99;\r\n\tcolor:#0563C1;\r\n\ttext-decoration:underline;}
\r\nspan.EmailStyle19\r\n\t{mso-style-type:personal-reply;\r\n\tfont-family:\"Calibri\",sans-serif;
\r\n\tcolor:windowtext;}\r\n.MsoChpDefault\r\n\t{mso-style-type:export-only;\r\n\tfont-size:10.0pt;}\r\n@page
WordSection1\r\n\t{size:8.5in 11.0in;\r\n\tmargin:1.0in 1.0in 1.0in 1.0in;}
\r\ndiv.WordSection1\r\n\t{page:WordSection1;}\r\n--></style>\r\n</head>\r\n<body lang=\"EN-US\" link=\"#0563C1\"
vlink=\"purple\" style=\"word-wrap:break-word\">\r\n<div class=\"WordSection1\">\r\n<p class=\"MsoNormal\"><span
style=\"font-size:11.0pt\">Adding a new domain to see if this updates the SIR 13867<o:p></o:p></span></p>\r\n<p
class=\"MsoNormal\"><span style=\"font-size:11.0pt\"><o:p> </o:p></span></p>\r\n<p class=\"MsoNormal\"><span
style=\"font-size:11.0pt\"><a href=\"atis.ug\">Suspicious domain</a><o:p></o:p></span></p>\r\n<p
class=\"MsoNormal\"><span style=\"font-size:11.0pt\"><o:p> </o:p></span></p>\r\n<p class=\"MsoNormal\"><span
style=\"font-size:11.0pt\"><o:p> </o:p></span></p>\r\n<div style=\"border:none;border-top:solid #B5C4DF
1.0pt;padding:3.0pt 0in 0in 0in\">\r\n<p class=\"MsoNormal\"><b><span style=\"color:black\">From: </span></b><span
style=\"color:black\">Mike Saurbaugh &lt;Mike.Saurbaugh@cofense.com&gt;<br>\r\n<b>Date: </b>Saturday, October 31,
2020 at 11:43 AM<br>\r\n<b>To: </b>Mike Saurbaugh &lt;Mike.Saurbaugh@cofense.com&gt;<br>\r\n<b>Subject: </
b>Suspicious domain testing<o:p></o:p></span></p>\r\n</div>\r\n<div>\r\n<p class=\"MsoNormal\"><span style=\"font-
size:11.0pt\"><o:p> </o:p></span></p>\r\n</div>\r\n<p class=\"MsoNormal\"><span style=\"font-size:11.0pt\">This
is a s suspicious <a href=\"http://zavagilsanti.com/\">\r\ndomain</a> </span><o:p></o:p></p>\r\n<p
class=\"MsoNormal\"><span style=\"font-size:11.0pt\"> </span><o:p></o:p></p>\r\n<p class=\"MsoNormal\"><span
```

```
style=\"font-size:11.0pt\"><a href=\"http://www.google.com\">www.google.com</a></span><o:p></o:p></p>\r\n<p
class=\"MsoNormal\"><span style=\"font-size:11.0pt\"> </span><o:p></o:p></p>\r\n<p class=\"MsoNormal\"><span
style=\"font-size:11.0pt\"> </span><o:p></o:p></p>\r\n<p class=\"MsoNormal\"><span style=\"font-
size:11.0pt\"> </span><o:p></o:p></p>\r\n</div>\r\n</body>\r\n</html>\r\n",
                "md5": "eaea121360915c67881538ea6de6f7ba",
                "sha256": "041a71be56a31c975b7a29763ff1d5a114b78c05f6dcb1816efb34ad0971fd5c",
                "match_priority": 4,
                "attachments_count": 0,
                "comments_count": 0,
                "rules_count": 2,
                "urls_count": 2,
                "tags": [],
                "categorization_tags": [],
                "processed_at": "2022-02-18T11:28:08.885Z",
                "created_at": "2020-12-03T20:23:09.071Z",
                "updated_at": "2022-02-02T21:20:25.344Z"
            },
            "relationships": {
                "assignee": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/relationships/assignee",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/assignee"
                    },
                    "data": null
                },
                "category": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/relationships/category",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/category"
                    },
                    "data": null
                },
                "cluster": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/relationships/cluster",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/cluster"
                    },
                    "data": {
                        "type": "clusters",
                        "id": "182"
                    }
                },
                "reporter": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/relationships/reporter",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/reporter"
                    },
                    "data": {
                        "type": "reporters",
                        "id": "24"
                    }
                },
                "attachment_payloads": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/relationships/
attachment_payloads",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/attachment_payloads"
                    }
                },
                "attachments": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/relationships/
```

```
attachments",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/attachments"
                    }
                },
                "domains": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/relationships/domains",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/domains"
                    }
                },
                "headers": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/relationships/headers",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/headers"
                    }
                },
                "hostnames": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/relationships/
hostnames",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/hostnames"
                    }
                },
                "urls": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/relationships/urls",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/urls"
                    }
                },
                "rules": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/relationships/rules",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/rules"
                    }
                },
                "threat_indicators": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/relationships/
threat_indicators",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/threat_indicators"
                    }
                },
                "comments": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/relationships/comments",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/comments"
                    }
                }
            },
            "meta": {
                "risk_score_summary": {
                    "integrations": 75,
                    "vip": 5,
                    "reporter": 15,
                    "rules": 4
                }
            }
        }]}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data[].attributes.subject`	Report.Title	N/A	`.data[].attributes.created_at`	Re: Suspicious domain testing - 12/3`	N/A
`.data[].attributes.text_body`	Report.Description	N/A	`.data[].attributes.created_at`	Adding a new domain to see...	N/A
`.data[].id`	Report.Attribute	ID	`.data[].attributes.created_at`	650	N/A
`.data[].attributes.location`	Report.Attribute	Location	`.data[].attributes.created_at`	Inbox	N/A
`.data[].attributes.risk_score`	Report.Attribute	Risk Score	`.data[].attributes.created_at`	99	N/A
`.data[].attributes.received_at`	Report.Attribute	Received At	`.data[].attributes.created_at`	2020-12-03T20:22:41.000Z	N/A
`.data[].attributes.reported_at`	Report.Attribute / Report.Happened At	Reported At	`.data[].attributes.created_at`	2020-12-03T20:22:39.000Z	N/A
`.data[].attributes.raw_headers`	Report.Attribute	Report Headers	`.data[].attributes.created_at`	Date: Thu, 03 Dec...	N/A
`.data[].attributes.processed_at`	Report.Attribute	Processed At	`.data[].attributes.created_at`	2022-02-18T11:28:08.885Z	N/A
`.data[].attributes.from_address`	Related.Indicator	Email Address	`.data[].attributes.created_at`	mike.saurbaugh@cofense.com	N/A
`.data[].attributes.md5`	Related.Indicator	MD5	`.data[].attributes.created_at`	eaea121360915c67881538ea6de6f7ba	N/A
`.data[].attributes.sha256`	Related.Indicator	SHA-256	`.data[].attributes.created_at`	041a71be56a31c975b7a29763ff1d5a114b78c05f6dcb1816efb34ad0971fd5c	N/A

Cofense Triage Domains (supplemental)

The Cofense Triage Domains supplemental feed fetches related FQDNs to a given Report Id.

```
GET {{base_url}}/api/public/v2/reports/{{id}}/domains
```

Sample Response:


```
{
    "data": [
        {
            "id": "126",
            "type": "domains",
            "links": {
                "self": "https://reltest6.phishmecloud.com/api/public/v2/domains/126"
            },
            "attributes": {
                "domain": "1105info.com",
                "created_at": "2020-10-21T20:57:15.836Z",
                "updated_at": "2020-10-21T20:57:15.836Z"
            },
            "relationships": {
                "clusters": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/domains/126/relationships/clusters",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/domains/126/clusters"
                    }
                },
                "hostnames": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/domains/126/relationships/
hostnames",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/domains/126/hostnames"
                    }
                },
                "reports": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/domains/126/relationships/reports",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/domains/126/reports"
                    }
                },
                "urls": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/domains/126/relationships/urls",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/domains/126/urls"
                    }
                }
            }
        }
    ],
    "meta": {
        "record_count": 2,
        "page_count": 1
    },
    "links": {
        "first": "https://reltest6.phishmecloud.com/api/public/v2/reports/267/domains?
```

```
page%5Bnumber%5D=1&page%5Bsize%5D=20",
        "last": "https://reltest6.phishmecloud.com/api/public/v2/reports/267/domains?
page%5Bnumber%5D=1&page%5Bsize%5D=20"
    }
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data[].attributes.domain`	Related.Indicator	FQDN	`.data[].attributes.created_at`	1105info.com	N/A

Cofense Triage Hostnames (supplemental)

The Cofense Triage Hostnames supplemental feed fetches related FQDNs to a given Report Id.

```
GET {{base_url}}/api/public/v2/reports/{{id}}/hostnames
```

Sample Response:


```
{
    "data": [
        {
            "id": "199",
            "type": "hostnames",
            "links": {
                "self": "https://reltest6.phishmecloud.com/api/public/v2/hostnames/199"
            },
            "attributes": {
                "hostname": "download.1105media.com",
                "risk_score": 21,
                "created_at": "2020-10-21T20:57:15.833Z",
                "updated_at": "2020-12-03T23:50:14.357Z"
            },
            "relationships": {
                "domain": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/hostnames/199/relationships/domain",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/hostnames/199/domain"
                    },
                    "data": {
                        "type": "domains",
                        "id": "126"
                    }
                },
                "clusters": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/hostnames/199/relationships/
clusters",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/hostnames/199/clusters"
                    }
                },
                "reports": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/hostnames/199/relationships/
reports",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/hostnames/199/reports"
                    }
                },
                "urls": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/hostnames/199/relationships/urls",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/hostnames/199/urls"
                    }
                }
            }
        }
    ],
```

```
    "meta": {
        "record_count": 3,
        "page_count": 1
    },
    "links": {
        "first": "https://reltest6.phishmecloud.com/api/public/v2/reports/267/hostnames?
page%5Bnumber%5D=1&page%5Bsize%5D=20",
        "last": "https://reltest6.phishmecloud.com/api/public/v2/reports/267/hostnames?
page%5Bnumber%5D=1&page%5Bsize%5D=20"
    }
}
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data[].attributes.hostname`	Related.Indicator	FQDN	`.data[].attributes.created_at`	download.1105media.com	N/A

Cofense Triage URLS (supplemental)

The Cofense Triage URLS supplemental feed fetches related URLs to a given Report Id.

```
GET {{base_url}}/api/public/v2/reports/{{id}}/urls
```

Sample Response:


```
{
    "data": [
        {
            "id": "1983",
            "type": "urls",
            "links": {
                "self": "https://reltest6.phishmecloud.com/api/public/v2/urls/1983"
            },
            "attributes": {
                "url": "https://1105info.com/portal/wts/ucmcmQefnvybb%5Ee8byzfycv0EyvdaBy2TV%5ENnnaXp",
                "risk_score": null,
                "created_at": "2020-10-21T20:57:15.846Z",
                "updated_at": "2020-10-21T20:57:15.846Z"
            },
            "relationships": {
                "domain": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/urls/1983/relationships/domain",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/urls/1983/domain"
                    }
                },
                "hostname": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/urls/1983/relationships/hostname",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/urls/1983/hostname"
                    },
                    "data": {
                        "type": "hostnames",
                        "id": "199"
                    }
                },
                "clusters": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/urls/1983/relationships/clusters",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/urls/1983/clusters"
                    }
                },
                "integration_submissions": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/urls/1983/relationships/
integration_submissions",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/urls/1983/
integration_submissions"
                    }
                },
                "reports": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/urls/1983/relationships/reports",
```

```
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/urls/1983/reports"
                    }
                }
            }
        }
    ],
    "meta": {
        "record_count": 9,
        "page_count": 1
    },
    "links": {
        "first": "https://reltest6.phishmecloud.com/api/public/v2/reports/267/urls?
page%5Bnumber%5D=1&page%5Bsize%5D=20",
        "last": "https://reltest6.phishmecloud.com/api/public/v2/reports/267/urls?
page%5Bnumber%5D=1&page%5Bsize%5D=20"
    }
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data[].attributes.url`	Related.Indicator	URL	`.data[].attributes.created_at`	https://1105info.com/portal/wts/ucmcmQefnvybb%5Ee8byzfycv0EyvdaBy2TV%5ENnnaXp	N/A

Cofense Triage Rules (supplemental)

The Cofense Triage Rules supplemental feed fetches related Rules and their attributes to a given Report Id.

```
GET {{base_url}}/api/public/v2/reports/{{id}}/rules
```


```
{
    "data": [
        {
            "id": "2589",
            "type": "rules",
            "links": {
                "self": "https://reltest6.phishmecloud.com/api/public/v2/rules/2589"
            },
            "attributes": {
                "name": "test_rule3",
                "description": "Rule of S",
                "priority": 1,
                "tags": [
                    "tag3"
                ],
                "scope": "Header",
                "author_name": "KetulPatel_CDS",
                "rule_context": "Unknown",
                "active": true,
                "content": "meta:\n  time_to_live=\"Forever\"\n  rule_context=\"Unknown\"\nstrings: \n  $forward=/
Subject:.+(fwd?|re) ?:/ nocase\ncondition:\n  $forward\n",
                "time_to_live": "Forever",
                "share_with_cofense": false,
                "reports_count": 91,
                "imported_at": null,
                "created_at": "2021-04-29T05:22:24.175Z",
                "updated_at": "2021-04-29T05:22:24.175Z"
            },
            "relationships": {
                "cluster_context": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/rules/2589/relationships/
cluster_context",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/rules/2589/cluster_context"
                    },
                    "data": null
                },
                "report_context": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/rules/2589/relationships/
report_context",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/rules/2589/report_context"
                    },
                    "data": null
                },
                "owner": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/rules/2589/relationships/owner",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/rules/2589/owner"
                    },
```

```
                    "data": {
                        "type": "operators",
                        "id": "9"
                    }
                },
                "clusters": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/rules/2589/relationships/clusters",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/rules/2589/clusters"
                    }
                },
                "reports": {
                    "links": {
                        "self": "https://reltest6.phishmecloud.com/api/public/v2/rules/2589/relationships/reports",
                        "related": "https://reltest6.phishmecloud.com/api/public/v2/rules/2589/reports"
                    }
                }
            }
        }
    ],
    "meta": {
        "record_count": 1,
        "page_count": 1
    },
    "links": {
        "first": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/rules?
page%5Bnumber%5D=1&page%5Bsize%5D=20",
        "last": "https://reltest6.phishmecloud.com/api/public/v2/reports/650/rules?
page%5Bnumber%5D=1&page%5Bsize%5D=20"
    }
}
```


ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
`.data[].attributes.name`	Rule.Name	Custom	`.data[].attributes.created_at`	test_rule3	N/A
`.data[].attributes.description`	Rule.Description	N/A	`.data[].attributes.created_at`	Rule of S	N/A
`.data[].attributes.content`	Rule.Value	N/A	`.data[].attributes.created_at`	meta:\n time_to_live...	N/A
`.data[].attributes.tags`	Rule.Tag	N/A	`.data[].attributes.created_at`	tag3	N/A
`.data[].id`	Rule.Attribute	Rule ID	`.data[].attributes.created_at`	2589	N/A
`.data[].attributes.author_name`	Rule.Attribute	Author Name	`.data[].attributes.created_at`	KetulPatel_CDS	N/A
`.data[].attributes.scope`	Rule.Attribute	Scope	`.data[].attributes.created_at`	Header	N/A

Indicator Type

The mapping between the indicator types in Cofense Triage and ThreatQ is as follows:

COFENSE TRIAGE	THREATQ
Header	Email Subject
Hostname	FQDN
MD5	MD5
SHA256	SHA-256
URL	URL

Status and Threat Type

You can enter custom mapping between the status of the indicator and threat type. The default ones are:

COFENSE TRIAGE	THREATQ
Malicious	Active
Suspicious	Review
Benign	Whitelisted

Average Feed Run

METRIC	RESULT
Run Time	2 minutes
Reports	58
Report Attributes	457
Signatures	2
Signature Attributes	6
Identities	5
Identity Attributes	13
Indicators	521
Indicators Attributes	560

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.

Known Issues / Limitations

- Due to the large amount of data and Cofense's variable HTTP request limit rate, you should use the **Delay** and **Limit** parameters in the CDF's Configuration page to avoid 401 errors.

Change Log

- **Version 1.1.3**
  - Added two new configuration options:
    - **Delay** - add a delay after each Cofense HTTP requests.
    - **Request Limit** - limit the maximum number of Cofense HTTP requests.
  - Added pagination support back into the integration due to the introduction of the new configuration options listed above.
- **Version 1.1.2**
  - Fixed an issue where the SSL certificate was not respected when making supplemental calls.
  - Fixed an issue where users encountered an `Error fetching data from provider: ClientResponseError("401, message='Too Many Requests",)` error message when performing a run.
  - Removed pagination support due to the large data set. See the Known Issues / Limitations chapter for more details.
- **Version 1.1.1**
  - Added the Verify SSL configuration option to the configuration page. See the Configuration chapter for more details.
- **Version 1.1.0**
  - Updated the API to version 2.
- **Version 1.0.2**
  - When Threat Level is specified as 'All', the `level` param is no longer included in the API request