ThreatQuotient

Cofense Intelligence CDF Guide

Version 1.0.7

March 05, 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	1.0.7
Compatible with ThreatQ Versions	>= 4.35.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/cofense-intelligence

Introduction

Cofense Intelligence delivers high-fidelity phishing indicators and contextual information highlighting attacker tactics across their global criminal operation.

Security teams can easily operationalize Cofense Intelligence indicators in the ThreatQ platform. Indicators of phishing, such as attack vectors and malware families, help analysts in their phishing defense. Automatically deploy prioritized and relevant data to your sensor grid for detection and blocking.

The CDF provides the following feeds:

- **Cofense Intelligence** - retrieves objects from Cofense Intelligence and enrich them with related data.
- **Cofense Intelligence Credential Phishing** - retrieves objects from Cofense Intelligence and enrich them with related data with the possibility to filter based on the malware family.

The integration ingests the following system objects:

- Adversaries
  - Adversary Attributes
- Attachments
- Events
  - Event Attributes
- Indicators
  - Indicator Attributes
- Malware

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:

   All Feeds

PARAMETER	DESCRIPTION
API ID	Your API ID provided by Cofense. Necessary for authentication.
API Key	Your API key provided by Cofense. Necessary for authentication.

   Additional Parameter - Cofense Intelligence

PARAMETER	DESCRIPTION
Ingest Subject Names	When selected, the integration ingests subject names as indicators related to the event.

   Additional Parameter - Cofense Intelligence Credential Phishing

PARAMETER	DESCRIPTION

Ingest Web Components	When selected, the integration ingests web component indicators.
Family Name	Select the objects to query by family name. Only one selection can be used at a time. To ingest phishing data, as the previous versions of the feed did, select the **Credential Phishing** option.

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

Cofense Intelligence

The Cofense Intelligence feed retrieves objects from Cofense Intelligence and enrich them with related data.

```
GET https://www.threathq.com/apiv1/threat/search?threatType=malware
```

Sample Response:


```
{
  "success": true,
  "data": {
    "page": {
      "currentPage": 0,
      "currentElements": 1,
      "totalPages": 1,
      "totalElements": 1
    },
    "threats": [
      {
        "id": 38663,
        "relatedSearchTags": [],
        "feeds": [
          {
            "id": 23,
            "permissions": {
              "WRITE": false,
              "OWNER": false,
              "READ": true
            },
            "displayName": "Cofense"
          }
        ],
        "blockSet": [
          {
            "deliveryMechanism": {
              "mechanismName": "GuLoader",
              "description": "Malware Downloader"
            },
            "impact": "Major",
            "confidence": 0,
            "blockType": "URL",
            "roleDescription": "Location from which a payload is obtained",
            "role": "Payload",
            "data": "https://drive.google.com/u/0/uc?id=1NsGADL4jYjlnVLwjmdivMe3I5yTTalVy&export=download",
            "data_1": {
              "url": "https://drive.google.com/u/0/uc?id=1NsGADL4jYjlnVLwjmdivMe3I5yTTalVy&export=download",
              "domain": "google.com",
              "query": "id=1NsGADL4jYjlnVLwjmdivMe3I5yTTalVy&export=download",
              "path": "/u/0/uc",
              "protocol": "https",
```

```
            "host": "drive.google.com"
          }
        },
        {
          "malwareFamily": {
            "familyName": "Remcos Remote Access Trojan",
            "description": "Remcos is a remote access trojan or RAT, used to take control of a user’s system. It
has multiple capabilities, chief among them is the ability for key logging, information stealing, and audio/visual
monitoring."
          },
          "impact": "Moderate",
          "confidence": 0,
          "blockType": "Domain Name",
          "roleDescription": "Command and control location used by malware",
          "role": "C2",
          "data": "dns.pepsi25.xyz",
          "data_1": "dns.pepsi25.xyz"
        }
      ],
      "campaignBrandSet": [
        {
          "totalCount": 1,
          "brand": {
            "id": 599,
            "text": "UPS"
          }
        }
      ],
      "extractedStringSet": [],
      "domainSet": [],
      "senderEmailSet": [],
      "executableSet": [
        {
          "malwareFamily": {
            "familyName": "Remcos Remote Access Trojan",
            "description": "Remcos is a remote access trojan or RAT, used to take control of a user’s system. It
has multiple capabilities, chief among them is the ability for key logging, information stealing, and audio/visual
monitoring."
          },
          "vendorDetections": [],
          "fileName": "Juei",
          "type": "Download",
          "dateEntered": 1588944174529,
          "severityLevel": "Major",
          "md5Hex": "6dd7c57fd11acea9111b023c27e7eb56"
        },
        {
          "deliveryMechanism": {
            "mechanismName": "GuLoader",
            "description": "Malware Downloader"
          },
          "vendorDetections": [],
          "fileName": "README.EXE",
          "type": "Attachment",
          "ssdeep": "12288:unUo0e4kMU/
NOJF19U9aZqr18iN1uwIoVBXiDjN5dLro6gVZ4glUSamtZsCNisW0:4U96dNOz15Zqr1t3IoTy1CLlGmjs+",
          "dateEntered": 1588941795872,
          "severityLevel": "Major",
          "md5Hex": "b6c8d83223ea073c01d40fafe866466b",
          "sha1Hex": "3341cb5f684cb690e3a92dc8884fcb0c28bf47a3",
          "sha224Hex": "4087a2cee7405842aeb47a0a364e2791d6ca52612bc4865cc42a3dbb",
```

```
            "sha256Hex": "ae3295c31bb70b2970c9acb33c40bae503de989ed9d696842a44c866e7bafa55",
            "sha384Hex":
"b099de38567532dc9675a31d2d6cd1e57bd613d0649c3ec0f9a5ce4ca7efd935113e26c6182ca1b5892a342e1cfcc490",
            "sha512Hex":
"b23ada84e5a6cf6260b05423e637481dbfa9fde7c1462d2b9682715bb8e1865e3e0fffd4978b7a4df17c82384655eebfdfc6b9a6a00380b0dbf3
66fc66ded354",
            "fileNameExtension": "EXE"
          }
        ],
        "senderIpSet": [],
        "senderNameSet": [],
        "spamUrlSet": [],
        "subjectSet": [
          {
            "totalCount": 1,
            "subject": "UPS - Pending delivery"
          }
        ],
        "campaignLanguageSet": [
          {
            "languageDefinition": {
              "isoCode": "en",
              "name": "English",
              "nativeName": "English",
              "family": "Indo-European"
            }
          }
        ],
        "lastPublished": 1588946280590,
        "firstPublished": 1588946277933,
        "label": "Shipping - GuLoader, Remcos RAT",
        "executiveSummary": "UPS-spoofed emails deliver Remcos RAT via GuLoader.",
        "hasReport": true,
        "reportURL": "https://www.threathq.com/api/l/activethreatreport/38663/html",
        "apiReportURL": "https://www.threathq.com/apiv1/t3/malware/38663/html",
        "threatDetailURL": "https://www.threathq.com/p42/search/default?m=38663",
        "threatType": "MALWARE",
        "malwareFamilySet": [
          {
            "familyName": "Remcos Remote Access Trojan",
            "description": "Remcos is a remote access trojan or RAT, used to take control of a user’s system. It has
multiple capabilities, chief among them is the ability for key logging, information stealing, and audio/visual
monitoring."
          }
        ],
        "deliveryMechanisms": [
          {
            "mechanismName": "GuLoader",
            "description": "Malware Downloader"
          }
        ],
        "naicsCodes": []
      },
          ...
    ]
  }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
data.threats[].label/.data.threats[].id	Event.Title	Malware	.data.threats[].firstPublished	Campaign: Shipping - GuLoader, Remcos RAT (38663)	Created by formatting the string `Campaign: {{ value.label }} ({{ value.id }})`
.data.threats[].executiveSummary	Event.Description	N/A	.data.threats[].firstPublished	"UPS-spoofed emails deliver Remcos RAT via GuLoader."	
.data.threats[].threatDetailURL	Event.Attribute	Threat Detail	.data.threats[].firstPublished	https://www.threathq.com/p42/search/default?m=38663	
.data.threats[].malwareFamilySet[].familyName	Event.Attribute	Malware Family	.data.threats[].firstPublished	Remcos Remote Access Trojan	
.data.threats[].campaignBrandSet[].brand.text	Event.Attribute	Brand	.data.threats[].firstPublished	UPS	
.data.threats[].label	Event.Attribute	Label	.data.threats[].firstPublished	Shipping - GuLoader, Remcos RAT	
.data.threats[].reportURL	Event.Attribute	Active Threat Report	.data.threats[].firstPublished	https://www.threathq.com/api/l/activethreatreport/38663/html	
.data.threats[].id	Attachment.Title, Attachment.Name	Attachment	.data.threats[].firstPublished	Campaign: Shipping - GuLoader, Remcos RAT (38663)	Attachment name and title are formatted from . data.threats[].id
.data.threats[].blockSet[].data_1	Indicator.Value	.data.threats[].blockSet[].blockType	.data.threats[].firstPublished	dns.pepsi25.xyz	
.data.threats[].blockSet[].impact	Indicator.Attribute	Impact	.data.threats[].firstPublished	Major	
.data.threats[].blockSet[].role Description	Indicator.Attribute	Role	.data.threats[].firstPublished	Location from which a payload is obtained	
.data.threats[].blockSet[].infrastructure TypeSubclass.description	Indicator.Attribute	SubRole	.data.threats[].firstPublished		
.data.threats[].blockSet[].asn	Indicator.Attribute	ASN	.data.threats[].firstPublished		
.data.threats[].blockSet[].country	Indicator.Attribute	Country	.data.threats[].firstPublished	Canada	
.data.threats[].blockSet[].organization	Indicator.Attribute	Organization	.data.threats[].firstPublished		
.data.threats[].executableSet[].md5Hex	Indicator.Value	MD5	.data.threats[].firstPublished	b6c8d83223ea073c01d40fafe866466b	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.threats[].executableSet[].sha1Hex	Indicator.Value	SHA-1	.data.threats[].firstPublished	3341cb5f684cb690e3a92dc8884fcb0c28bf47a3	
.data.threats[].executableSet[].sha256Hex	Indicator.Value	SHA-256	.data.threats[].firstPublished	ae3295c31bb70b2970c9acb33c40bae503de989ed9d696842a44c866e7bafa55	
.data.threats[].executableSet[].ssdeep	Indicator.Value	ssdeep	.data.threats[].firstPublished	12288:unUo0e4kMU/NOJF19U9aZqr18iN1uwIoVBXiDjN5dLro6gVZ4glUSamtZsCNisW0:4U96dNOz15Zqr1t3IoTy1CLlGmjs	
.data.threats[].executableSet[].sha384Hex	Indicator.Value	SHA-384	.data.threats[].firstPublished	b099de38567532dc9675a31d2d6cd1e57bd613d0649c3ec0f9a5ce4ca7efd935113e26c6182ca1b5892a342e1cfcc490	
.data.threats[].executableSet[].sha512Hex	Indicator.Value	SHA-512	.data.threats[].firstPublished	b23ada84e5a6cf6260b05423e637481dbfa9fde7c1462d2b9682715bb8e1865e3e0fffd4978b7a4df17c82384655eebfdfc6b9a6a00380b0dbf366fc66ded354	
.data.threats[].executableSet[].malwareFamily.familyName	Indicator.Attribute	Malware Family	.data.threats[].firstPublished	Remcos Remote Access Trojan	
.data.threats[].executableSet[].malwareFamily.description	Indicator.Attribute	N/A	.data.threats[].firstPublished	Remcos is a remote access trojan or RAT, used to...	
.data.threats[].executableSet[].fileName	Indicator.Attribute	Filename	.data.threats[].firstPublished	README.EXE	
.data.threats[].executableSet[].type	Indicator.Attribute	Vector	.data.threats[].firstPublished	Attachment	
.data.threats[].executableSet[].executableSubtype.description	Indicator.Attribute	SubRole	.data.threats[].firstPublished		
.data.threats[].malwareFamilySet.familyName	Malware.Value	Malware	.data.threats[].firstPublished	Remcos Remote Access Trojan	
.data.threats[].malwareFamilySet.description	Malware.Description	N/A	N/A	Remcos is a remote access trojan or RAT, used to...	

Cofense Intelligence Credential Phishing

The Cofense Intelligence Credential Phishing feed retrieves objects from Cofense Intelligence and enrich them with related data with the possibility to filter based on the malware family.

```
GET https://www.threathq.com/apiv1/threat/search?malwareFamily=null
```

Sample Response:


```
{
    "success": true,
    "data": {
        "page": {
            "currentPage": 0,
            "currentElements": 30,
            "totalPages": 2706,
            "totalElements": 81153
        },
        "threats": [
            {
                "id": 5496,
                "relatedSearchTags": [],
                "feeds": [
                    {
                        "id": 23,
                        "permissions": {
                            "READ": true,
                            "WRITE": false,
                            "OWNER": false
                        },
                        "displayName": "Cofense"
                    }
                ],
                "blockSet": [
                    {
                        "malwareFamily": {
                            "familyName": "CTB Ransomware",
                            "description": "Encryption ransomware"
                        },
                        "impact": "Major",
                        "confidence": 100,
                        "blockType": "Domain Name",
                        "roleDescription": "Command and control location used by malware",
                        "role": "C2",
                        "data": "zsn5qtrgfpu4tmpg.tor2web.fi",
                        "data_1": "zsn5qtrgfpu4tmpg.tor2web.fi"
                    }
                ],
                "campaignBrandSet": [
                    {
                        "totalCount": 1,
                        "brand": {
                            "id": 577,
                            "text": "Vodafone"
                        }
                    }
```

```
                ],
                "extractedStringSet": [],
                "domainSet": [],
                "senderEmailSet": [],
                "executableSet": [
                    {
                        "malwareFamily": {
                            "familyName": "CTB Ransomware",
                            "description": "Encryption ransomware"
                        },
                        "vendorDetections": [],
                        "fileName": "Fattura AG00003378.pdf.exe",
                        "type": "Attachment",
                        "dateEntered": 1456437633008,
                        "severityLevel": "Major",
                        "md5Hex": "efb280be9a0f11f5eafc7fd49310cf4e",
                        "sha224Hex": "720c963d5a1134e849dda8b1cc26c2435555480a742a5fea734bbd8b",
                        "sha256Hex": "a202b605ec8a1fcac91194d8145fe857ae9da9d5224787c372de74ed38738055",
                        "sha384Hex":
"20318fd2f17129241e34aefe2995e53f9f8d543fa2feecc5094f968dd675e0457cbdb6aa73c2280919a6aeb0aba388b6",
                        "sha512Hex":
"15bf417519387655cf558e073c6868d70d222089e147357fdd0cb07f9a77d55ce87bf5ca2f9dbc55ab7bc82436fe15869254189d552f92defa87
637b355e2c5a",
                        "sha1Hex": "14dd6b59fb38a3c312ae5c380bee0b9f400162d4",
                        "fileNameExtension": "exe"
                    }
                ],
                "senderIpSet": [],
                "senderNameSet": [],
                "spamUrlSet": [],
                "subjectSet": [
                    {
                        "totalCount": 1,
                        "subject": "Vodafone - Recapito Elettronico Fattura nr. AG00003378"
                    }
                ],
                "campaignLanguageSet": [],
                "campaignScreenshotSet": [],
                "lastPublished": 1660157848556,
                "firstPublished": 1456438512972,
                "label": "Vodafone - CTB Locker Encryption Ransomware",
                "executiveSummary": "Imitating a Vodafone template, these Italian-language emails refer to an
electronic invoice instructing the recipient to view the attachment. The attachment is a .zip archive containing an
executable file representing the CTB Locker encryption ransomware that encrypts files on the victim machine and
changes the desktop background to a payment data image. The payment locations for this malware are located on the Tor
web and request payment in Bitcoins, making it impossible to track any payments.",
                "hasReport": true,
                "reportURL": "https://www.threathq.com/api/l/activethreatreport/5496/html",
                "apiReportURL": "https://www.threathq.com/apiv1/t3/malware/5496/html",
                "threatDetailURL": "https://www.threathq.com/p42/search/default?m=5496",
                "threatType": "MALWARE",
                "deliveryMechanisms": [],
                "malwareFamilySet": [
                    {
                        "familyName": "CTB Ransomware",
                        "description": "Encryption ransomware"
                    }
                ],
                "secureEmailGatewaySet": [],
                "naicsCodes": []
            }
```

```
        ]
    }
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.threats[].data.threats[].id	Event.Title	Credential Phishing	.data.threats[].firstPublished	Credential Phishing: 5496	Created by formatting the string `Credential Phishing: {{ value.id }}`
.data.threats[].threatDetailURL	Event.Attribute	Threat Detail	.data.threats[].firstPublished	N/A	N/A
.data.threats[].campaignBrandSet[].brands.text	Event.Attribute	Brand	.data.threats[].firstPublished	Vodafone	N/A
.data.threats[].campaignScreenshotSet[].url	Event.Attribute	Reference Screenshot URL	.data.threats[].firstPublished	N/A	N/A
.data.threats[].ipDetail.ip	Indicator.Value	IP Address	.data.threats[].firstPublished	1.2.3.4	N/A
.data.threats[].ipDetail.asn	Indicator.Attribute	ASN	.data.threats[].firstPublished	N/A	N/A
.data.threats[].ipDetail.asnOrganization	Indicator.Attribute	ASN Organization	.data.threats[].firstPublished	N/A	N/A
.data.threats[].ipdetail.continentCode	Indicator.Attribute	Continent Code	.data.threats[].firstPublished	AS	N/A
.data.threats[].ipDetail.countryIsoCode	Indicator.Attribute	Country ISO Code	.data.threats[].firstPublished	MY	N/A
.data.threats[].ipDetail.countryName	Indicator.Attribute	Country Name	.data.threats[].firstPublished	Malaysia	N/A
.data.threats[].ipDetail.isp	Indicator.Attribute	ISP	.data.threats[].firstPublished	Piradius Net	N/A
.data.threats[].ipDetail.latitude	Indicator.Attribute	Latitude	.data.threats[].firstPublished	2.5000	N/A
.data.threats[].ipDetail.longitude	Indicator.Attribute	Longitude	.data.threats[].firstPublished	112.5000	N/A
.data.threats[].ipDetail.metroCode	Indicator.Attribute	Metro Code	.data.threats[].firstPublished	N/A	N/A
.data.threats[].ipDetail.organization	Indicator.Attribute	Organization	.data.threats[].firstPublished	N/A	N/A
.data.threats[].ipDetail.postalCode	Indicator.Attribute	Postal Code	.data.threats[].firstPublished	N/A	N/A
.data.threats[].ipDetail.subdivisionIsoCode	Indicator.Attribute	Subdivision ISO Code	.data.threats[].firstPublished	N/A	N/A
.data.threats[].ipDetail.subdivisionName	Indicator.Attribute	Subdivsion Name	.data.threats[].firstPublished	N/A	N/A
.data.threats[].ipDetail.timeZone	Indicator.Attribute	Time Zone	.data.threats[].firstPublished	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.threats[].campaignLanguageSet[].languageDefinition.family	Event.Attribute	Language Family	.data.threats[].firstPublished	N/A	N/A
.data.threats[].campaignLanguageSet[].languageDefinition.isoCode	Event.Attribute	Language ISO Code	.data.threats[].firstPublished	N/A	N/A
.data.threats[].campaignLanguageSet[].languageDefinition.name	Event.Attribute	Language Name	.data.threats[].firstPublished	N/A	N/A
.data.threats[].campaignLanguageSet[].languageDefintition.nativeName	Event.Attribute	Language Native Name	.data.threats[].firstPublished	N/A	N/A
.data.threats[].label	Event.TAG	TAG	N/A	N/A	N/A
N/A	Indicator.Attribute	Cofense Type	.data.threats[].firstPublished	Action	Value will always be 'Action'. Applies to indicators from data.threats[].blockSet.data_1
.data.threats[].webComponents[].md5	Indicator.Value	MD5	.data.threats[].firstPublished	N/A	N/A
.data.threats[].webComponents[].sha1	Indicator.Value	SHA-1	.data.threats[].firstPublished	N/A	N/A
.data.threats[].webComponents[].sha256	Indicator.Value	SHA-256	.data.threats[].firstPublished	N/A	N/A
.data.threats[].webComponents[].sha384	Indicator.Value	SHA-384	.data.threats[].firstPublished	N/A	N/A
.data.threats[].webComponents[].sha512	Indicator.Value	SHA-512	.data.threats[].firstPublished	N/A	N/A
.data.threats[].webComponents[].resourceURL.domain	Indicator.Value	FQDN	.data.threats[].firstPublished	N/A	Applies to all hash indicators from .data.threats[].webComponents[].*.
.data.threats[].webComponents[].resourceURL.path	Indicator.Value	URL Path	.data.threats[].firstPublished	N/A	Applies to all hash indicators from .data.threats[].webComponents[].*.
.data.threats[].webComponents[].resourceURL.url	Indicator.Value	URL	.data.threats[].firstPublished	N/A	Applies to all hash indicators from .data.threats[].webComponents[].*. Censored in docs for safety - uncensored in provider response
N/A	Indicator.Attribute	Cofense Type	.data.threats[].firstPublished	Web Component	Value will always be 'Web Component'. Applies to all hash indicators from .data.threats[].webComponents[].*.
.data.threats[].executableSet[].md5Hex	Indicator.Value	MD5	.data.threats[].firstPublished	N/A	N/A
.data.threats[].executableSet[].sha1Hex	Indicator.Value	SHA-1	.data.threats[].firstPublished	N/A	N/A
.data.threats[].executableSet[].sha224Hex	Indicator.Value	SHA-224	.data.threats[].firstPublished	N/A	N/A

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.threats[].executableSet[].sha384Hex	Indicator.Value	SHA-384	.data.threats[].firstPublished	N/A	N/A
.data.threats[].executableSet[].sha512Hex	Indicator.Value	SHA-512	.data.threats[].firstPublished	N/A	N/A
.data.threats[].executableSet[].fileName	Indicator.Value	Filename	.data.threats[].firstPublished	Fattura AG00003378.pdf.exe	N/A
N/A	Indicator.Attribute	Cofense Type	.data.threats[].firstPublished	Executable Component	Value will always be 'Executable Component'. Applies to all indicators from .data.threats[].executableSet[].*.
.data.threats[].executableSet[].fileNameExtension	Indicator.Attribute	File name extension	.data.threats[].firstPublished	exe	Applies to FILENAME indicators
.data.threats[].executableSet[].type	Indicator.Attribute	File Type	.data.threats[].firstPublished	Attachment	Applies to FILENAME indicators
.data.threats[].blockSet.confidence	Indicator.Attribute	Confidence	.data.threats[].firstPublished	N/A	N/A
.data.threats[].blockSet.impact	Indicator.Attribute	Impact	.data.threats[].firstPublished	N/A	N/A
.data.threats[].blockSet.data_1.protocol	Indicator.Attribute	Protocol	.data.threats[].firstPublished	N/A	Applies to URL Path indicators
.data.threats[].blockSet.data_1.domain	Indicator.Value	FQDN	.data.threats[].firstPublished	N/A	N/A
.data.threats[].blockSet.data_1.url	Indicator.Value	URL	.data.threats[].firstPublished	N/A	N/A
.data.threats[].blockSet.data_1.path	Indicator.Value	URL Path	.data.threats[].firstPublished	N/A	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.

Cofense Intelligence

The following metrics is for a 24 hour run.

METRIC	RESULT
Run Time	< 1 minute
Indicators	200
Indicator Attributes	750
Adversaries	5
Adversary Attributes	20
Events	20
Event Attributes	100
Malware	8
Attachments	20

Cofense Intelligence Credential Phishing

The following metrics is for a 24 hour run.

METRIC	RESULT
Run Time	1 min
Indicators	1,749
Indicator Attributes	737
Events	268
Event Attributes	737

Change Log

- **Version 1.0.7**
  - Updated the Cofense Intelligence Credential Phishing feed to reflect a change in the provider's API.
- **Version 1.0.6**
  - Added new configuration filter, **Family Name**, for the Cofense Intelligence Credential Phishing feed.
- **Version 1.0.5**
  - Bug fix on attribute mapping logic for `screenshot` and `phishingURL_1`
  - API Key values are now masked in ThreatQ UI
- **Version 1.0.4**
  - Initial release