ThreatQuotient

ArcSight Case Management CDF Guide

Version 1.0.0

August 03, 2021

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.

TOC

Versioning

- Current integration version: `1.0.5`
- Supported on ThreatQ versions >= `4.35.0`

Introduction

The Cofense Intelligence version 1.0.5 integration includes two feeds:

- Cofense Intelligence

  > This integration provides an update to the existing Cofense Intelligence feed that is seeded with the platform.

- Cofense Intelligence Credential Phishing

> Time constrained data fetching is possible.

> Feeds use basic HTTP authentication based on API ID and Key.

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 **Cofense Intelligence** feeds 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 parameters under the **Configuration** tab:

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

Additional Parameter - Cofense Intelligence

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

Additional Parameter - Cofense Intelligence Credential Phishing

PARAMETER	DESCRIPTION
Ingest Web Components	When checked, ingests web component indicators.

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

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


```
{
  "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": []
      },
          ...
    ]
  }
}
```


ThreatQ provides the following default mapping for the 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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					`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	
.data.threats[].executableSet[].sha1Hex	Indicator.Value	SHA-1	.data.threats[].firstPublished	3341cb5f684cb690e3a92dc8884fcb0c28bf47a3	
.data.threats[].executableSet[].sha256Hex	Indicator.Value	SHA-256	.data.threats[].firstPublished	ae3295c31bb70b2970c9acb33c40bae503d	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
				e989ed9d696842a44c866e 7bafa55	
.data.threats[].executableSet[].ssdeep	Indicator.Value	ssdeep	.data.threats[]. firstPublished	12288:unUo0e4kMU/NOJF19 U9aZqr18iN1u wIoVBXiDjN5dLr o6gVZ4glUSamtZsCNisW0:4 U96dNOz15Zqr1 t3IoTy1CLlGmjs	
.data.threats[].executableSet[]. sha384Hex	Indicator.Value	SHA-384	.data.threats[]. firstPublished	b099de38567532dc9675a31 d2d6cd1e57bd61 3d0649c3ec0f 9a5ce4ca7efd935113e26c6182 ca1b5892a342 e1cfcc490	
.data.threats[].executableSet[]. sha512Hex	Indicator.Value	SHA-512	.data.threats[]. firstPublished	b23ada84e5a6cf6260b0542 3e637481dbfa9f de7c1462d2b96 82715bb8e1865e3e0fffd497 8b7a4df17c8238 4655eebfdfc6b9 a6a00380b0dbf366fc66ded354	
.data.threats[].executableSet[].malware Family.familyName	Indicator.Attribute	Malware Family	.data.threats[]. firstPublished	Remcos Remote Access Trojan	
.data.threats[].executableSet[].malware Family.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[]. executable Subtype.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...	

Average Feed Run - Cofense Intelligence (24h run):

METRIC	RESULT
Run Time	< 1 minute
Indicators	200

METRIC	RESULT
Indicator Attributes	750
Adversaries	5
Adversary Attributes	20
Events	20
Event Attributes	100
Malware	8
Attachments	20

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 Credential Phishing

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


```
{
  "success": true,
  "data": {
    "page": {
      "currentPage": 0,
      "currentElements": 5,
      "totalPages": 6,
      "totalElements": 30
    },
    "threats": [
      {
        "id": 29849346,
        "brands": [
          {
            "id": 535,
            "text": "Netflix"
          }
        ],
        "feeds": [
```

```
    {
      "id": 42,
      "permissions": {
        "WRITE": false,
        "OWNER": false,
        "READ": true
      },
      "displayName": "Cofense Open Source"
    }
  ],
  "kits": [],
  "title": "Netflix",
  "screenshot": {
    "url": "https://www.threathq.com/apiv1/screenshot/29849346",
    "url_1": {
      "url": "https://www.threathq.com/apiv1/screenshot/29849346",
      "domain": "threathq.com",
      "path": "/apiv1/screenshot/29849346",
      "protocol": "https",
      "host": "www.threathq.com"
    }
  },
  "firstDate": 1588945216890,
  "lastDate": 1588945216890,
  "confirmedDate": 1588945808107,
  "ipDetail": {
    "ip": "111.90.156.123",
    "lookupOn": 1588696613965,
    "latitude": 2.5000,
    "longitude": 112.5000,
    "continentName": "Asia",
    "continentCode": "AS",
    "countryName": "Malaysia",
    "countryIsoCode": "MY",
    "isp": "Piradius Net",
    "organization": "Piradius Net"
  },
  "threatDetailURL": "https://www.threathq.com/p42/search/default?p=29849346",
  "confirmationData": {
    "confirmingUrlId": 29849348
  },
  "messageHeaders": [],
  "language": {
    "languageDefinition": {
      "isoCode": "en",
      "name": "English",
      "nativeName": "English",
      "family": "Indo-European"
    },
    "probability": 0.9999965436645388
  },
  "threatType": "PHISH",
  "isConfirmedPhishingWebsite": "YES",
  "processingState": "ANALYZED",
  "webComponents": [
    {
      "fileSize": 95962,
      "resourceURL": {
        "domain": "infonex47.com",
        "path": "/js/jquery-1.11.3.min.js",
        "protocol": "http",
```

```
            "host": "infonex47.com",
            "url": "http://infonex47.com/js/jquery-1.11.3.min.js"
          },
          "md5": "13c0a5055cca7b2463b2f73701960b9e",
          "sha1": "e6082a7b52db82604ac446d2e6a32cb5af263781",
          "sha224": "fd337ec060000d557c6fd7f0b5a9aad342de7e4f863cafd5dd2aee49",
          "sha256": "20e11ce61890c08c0529911822233c9023ebc367df6c1050dec105e2b9628104",
          "sha384":
"da10f33f2ca65415d27ce78ad7c151cf839072c7308313043bc5fe667504ec32eec4942d44c3bb9f72da5e389e5869c4",
          "sha512":
"2fa08436b5f748776d265944595a59581c6b06eb6eb239626de3338e0819b45852ead29d4997dc1f86dfbfb1b5d39dbd4dc9e44e6e38ba9f6006
628710546ef9"
        }
      ],
      "reportedURLs": [
        "http://infonex47.com/alldetails.html"
      ],
      "phishingURL": "http://infonex47.com/alldetails.html",
      "actionURLs": [],
      "actionURLs_1": [],
      "reportedURLs_1": [
        {
          "urlSeverity": "Major",
          "urlConfidence": "High",
          "hostSeverity": "Moderate",
          "hostConfidence": "High",
          "domainSeverity": "Minor",
          "domainConfidence": "High",
          "domain": "infonex47.com",
          "path": "/alldetails.html",
          "protocol": "http",
          "host": "infonex47.com",
          "url": "http://infonex47.com/alldetails.html"
        }
      ],
      "phishingURL_1": {
        "urlSeverity": "Major",
        "urlConfidence": "High",
        "hostSeverity": "Moderate",
        "hostConfidence": "High",
        "domainSeverity": "Minor",
        "domainConfidence": "High",
        "ipSeverity": "Minor",
        "ipConfidence": "High",
        "domain": "infonex47.com",
        "path": "/alldetails.html",
        "protocol": "http",
        "host": "infonex47.com",
        "url": "http://infonex47.com/alldetails.html"
      }
    },
        ...
  ]
 }
}
```


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.threats[].title/.data.threats[].id	Event.Title	Credential Phishing	.data.threats[].firstDate	Credential Phishing: Netflix (29849346)	Created by formatting the string `Credential Phishing: {{ value.title}} ({{ value.id }})`
.data.threats[].threatDetailURL	Event.Attribute	Threat Detail	.data.threats[].firstDate		
.data.threats[].brands.text	Event.Attribute	Brand	.data.threats[].firstDate	UPS	
.data.threats[].screenshot.url	Event.Attribute	Reference Screenshot URL	.data.threats[].firstDate	https://www.threathq.com/apiv1/screenshot/29849346	
.data.threats[].ipDetail.ip	Indicator.Value	IP Address	.data.threats[].firstDate	1.2.3.4	
.data.threats[].ipDetail.asn	Indicator.Attribute	ASN	.data.threats[].firstDate		
.data.threats[].ipDetail.asn Organization	Indicator.Attribute	ASN Organization	.data.threats[].firstDate		
.data.threats[].ipdetail.continent Code	Indicator.Attribute	Continent Code	.data.threats[].firstDate	AS	
.data.threats[].ipDetail.countryIso Code	Indicator.Attribute	Country ISO Code	.data.threats[].firstDate	MY	
.data.threats[].ipDetail.country Name	Indicator.Attribute	Country Name	.data.threats[].firstDate	Malaysia	
.data.threats[].ipDetail.isp	Indicator.Attribute	ISP	.data.threats[].firstDate	Piradius Net	
.data.threats[].ipDetail.latitude	Indicator.Attribute	Latitude	.data.threats[].firstDate	2.5000	
.data.threats[].ipDetail.longitude	Indicator.Attribute	Longitude	.data.threats[].firstDate	112.5000	
.data.threats[].ipDetail.metroCode	Indicator.Attribute	Metro Code	.data.threats[].firstDate		
.data.threats[].ipDetail.postalCode	Indicator.Attribute	Postal Code	.data.threats[].firstDate		
.data.threats[].ipDetail. subdivisionIsoCode	Indicator.Attribute	Subdivision ISO Code	.data.threats[].firstDate		
.data.threats[].ipDetail. subdivisionName	Indicator.Attribute	Subdivsion Name	.data.threats[].firstDate		
.data.threats[].ipDetail.timeZone	Indicator.Attribute	Time Zone	.data.threats[].firstDate		
.data.threats[].language.language Definition.family	Event.Attribute	Language Family	.data.threats[].firstDate	Indo-European	
.data.threats[].language.language Definition.isoCode	Event.Attribute	Language ISO Code	.data.threats[].firstDate	en	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.data.threats[].language.language Definition.name	Event.Attribute	Language Name	.data.threats[]. firstDate	English	
.data.threats[].language.language Defintition. nativeName	Event.Attribute	Language Native Name	.data.threats[]. firstDate	English	
.data.threats[].phishingURL_1. domain	Indicator.Value	URL	.data.threats[]. firstDate	infonext87.com	
.data.threats[].phishingURL_1.url	Indicator.Value	URL	.data.threats[]. firstDate	hxxp://infonext87.com/ alldetails.html	URL censored in docs for safety - uncensored in provider response
.data.threats[].phishingURL_1.path	Indicator.Value	URL Path	.data.threats[]. firstDate	/alldetails.html	
.data.threats[].phishingURL_1. domainConfidence	Indicator.Attribute	Domain Confidence	.data.threats[]. firstDate	High	
.data.threats[].phishingURL_1. domainSeverity	Indicator.Attribute	Domain Severity	.data.threats[]. firstDate	Minor	
.data.threats[].phishingURL_1.url Confidence	Indicator.Attribute	URL Confidence	.data.threats[]. firstDate	High	
.data.threats[].phishingURL_1.url Severity	Indicator.Attribute	URL Severity	.data.threats[]. firstDate	Moderate	
.data.threats[].phishingURL_1. protocol	Indicator.Attribute	Protocol	.data.threats[]. firstDate	http	
.data.threats[].reportedURLs_1. domainConfidence	Indicator.Attribute	Confidence	.data.threats[]. firstDate	High	
.data.threats[].reportedURLs_1. domainSeverity	Indicator.Attribute	Severity	.data.threats[]. firstDate	Moderate	
.data.threats[].reportedURLs_1.url Confidence	Indicator.Attribute	Confidence	.data.threats[]. firstDate	High	
.data.threats[].reportedURLs_1.url Severity	Indicator.Attribute	Severity	.data.threats[]. firstDate	Moderate	
.data.threats[].reportedURLs_1. protocol	Indicator.Attribute	Protocol	.data.threats[]. firstDate	http	
N/A	Indicator.Attribute	Cofense URL Type	.data.threats[]. firstDate	Action	Value will be one of 'Action', 'Phishing', or 'Reported', depending on the URL type as given by the provider.
.data.threats[].webComponents[ ].md5	Indicator.Value	MD5	.data.threats[]. firstDate	7b3042a2d8f6a351a228f11 52b560302	
.data.threats[].webComponents []].sha1	Indicator.Value	SHA-1	.data.threats[]. firstDate	693a5d1e3cb90fd8bdec53e 4f4000d19e1dc1152	
.data.threats[].webComponents []].sha256	Indicator.Value	SHA-256	.data.threats[]. firstDate	ba892f7903e737d06c952be 4ed3266746ed5e109037 7fbc5d2ac975626c4533a	
.data.threats[].webComponents []].sha384	Indicator.Value	SHA-384	.data.threats[]. firstDate	e3437366a3c034a4cfe458131 e91de42e970e3d70f7a57a	

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
				8d7888e295432ef465b 0c7ae7edd981b9476bcacbb6005da6	
.data.threats[].webComponents[].sha512	Indicator.Value	SHA-512	.data.threats[].firstDate	200089b4b93f1fdd393da32c37e 812daeb53b16c2311 2befa442fa65520dfded076 e18f278b4cb080040825649f448cd2 5e0a28352efef34 a8ecd83f35712b65	
.data.threats[].webComponents[].resourceURL.domain	Indicator.Value	FQDN	.data.threats[].firstDate	nflxext.com	Applies to all hash indicators from .data.threats[].web Components[].*.
.data.threats[].webComponents[].resourceURL.path	Indicator.Value	URL Path	.data.threats[].firstDate	/ffe/siteui/fonts/nf-icon-v1-88.woff	Applies to all hash indicators from .data.threats[].web Components[].*.
.data.threats[].webComponents[].resourceURL.url	Indicator.Value	URL	.data.threats[].firstDate	hxxps://assets.nflxext.com/ffe/siteui/fonts/nf-icon-v1-88.woff	Applies to all hash indicators from . data.threats[].web Components[].*.Censored in docs for safety -uncensored in provider response
N/A	Indicator.Attribute	Cofense Type	.data.threats[].firstDate	Web Component	Value will always be 'Web Component'. Applies to all hash indicators from .data.threats[].web Components[].*.

Average Feed Run - Cofense Intelligence Credential Phishing (24h run):

METRIC	RESULT
Run Time	5.5 hours
Indicators	13000
Indicator Attributes	20000
Events	200

METRIC	RESULT
Event Attributes	1600

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.

Change Log

- Version 1.0.5
  - Bugfix on attribute mapping logic for `screenshot` and `phishingURL_1`
  - API Key values are now masked in ThreatQ UI
- Version 1.0.4
  - Initial Release