



ThreatConnect – Cofense Intelligence Integration User Guide

Version 3.0.0

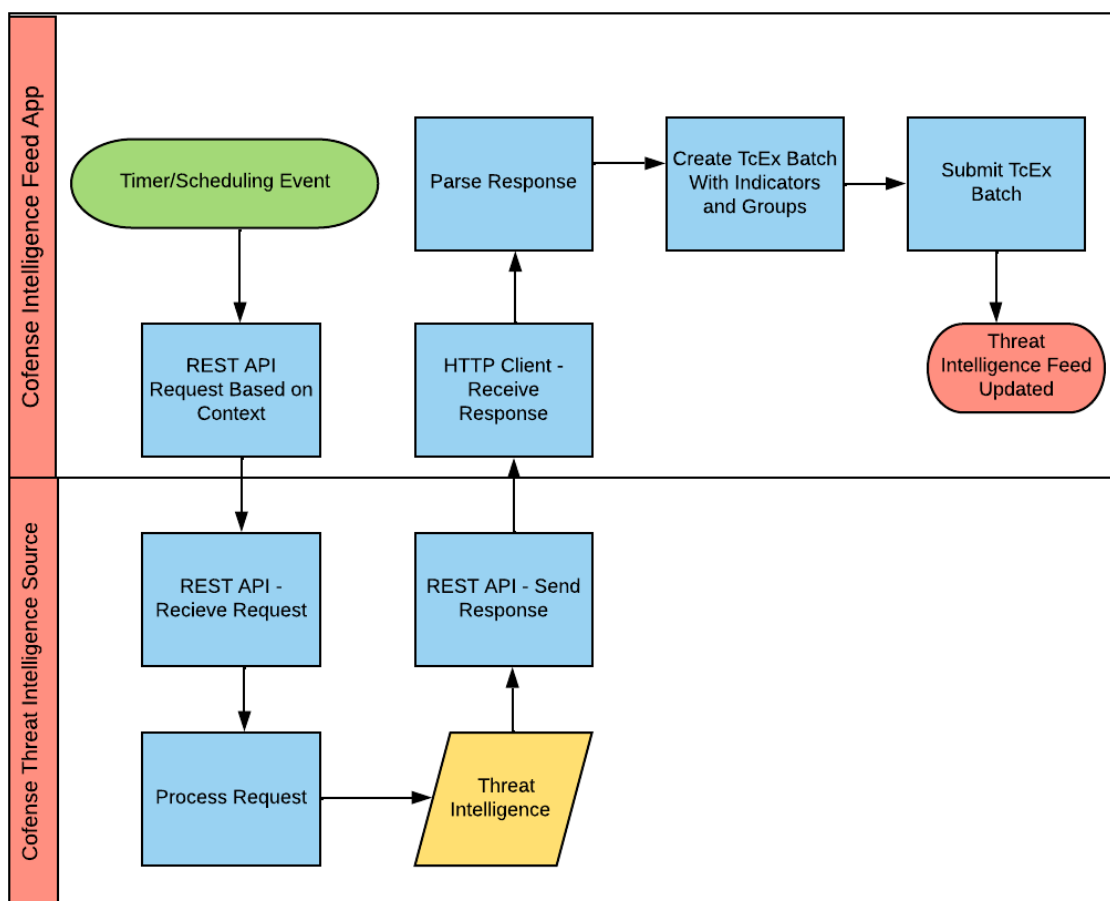
Contents

Introduction	3
Release Notes	4
Data Mapping	4
Configuration Requirements	4
Job App Installation	4
ThreatConnect Job Configuration	4
Program Screen	5
Parameter Screen	6
Schedule Screen	7
Output Screen	8
Feed Deployer Instructions	9
Browsing Cofense Intelligence Feed	14
Browsing Indicators	14
IP Address Feed	14
Host Feed	15
Email Address Feed	15
File Feed	16
URL Feed	16
Browsing Groups	17
Document	17
Threat	18
Browsing Intel Finished Reports	18
Support	18

Introduction

The ThreatConnect platform ingests and maps Cofense Intelligence phishing threats. Cofense Intelligence is human-verified phishing intelligence that includes actionable phishing indicators, and contextual reports behind the threat. Security teams ingest Cofense Intelligence which include the latest phishing indicators identified globally. Credential phishing, malware, ransomware, and BEC attacks, are a few examples, provided to customers to operationalize in their SOC. Each phishing indicator corresponds with a human-verified impact rating and is a high-fidelity source of phishing intelligence that security teams can use with confidence. Cofense offers phishing intelligence to empower security teams to make informed strategic decisions against today's phishing attacks.

This integration consists of consuming the Cofense Threat Intelligence feed and importing the data as indicators, groups into the ThreatConnect Platform as a Threat Intelligence feed. A high-level run of the Cofense Threat Intelligence feed is shown below.



Release Notes

App Version	Release Date	Details
1.0.0		Initial Release.
3.0.0		Updated to TcEX 3.0.0

Data Mapping

The table below documents the data mapping that takes place between the Cofense Threat Intelligence data and the ThreatConnect Platform.

Cofense Threat Intelligence Feed	ThreatConnect Field/Object
Threat ID general information	Threat or Indicator
Active Threat Report for Threat ID	Document
Finished Intelligence Document	Document
WatchList IPv4	Indicator of type Address
WatchList Email Addresses	Indicator of type Email Address
WatchList URL	Indicator of type URL
WatchList Domain	Indicator of type Host
Malware Artifacts	Indicator of type File

Configuration Requirements

1. Access to a ThreatConnect Platform Instance
2. ThreatConnect API user

Job App Installation

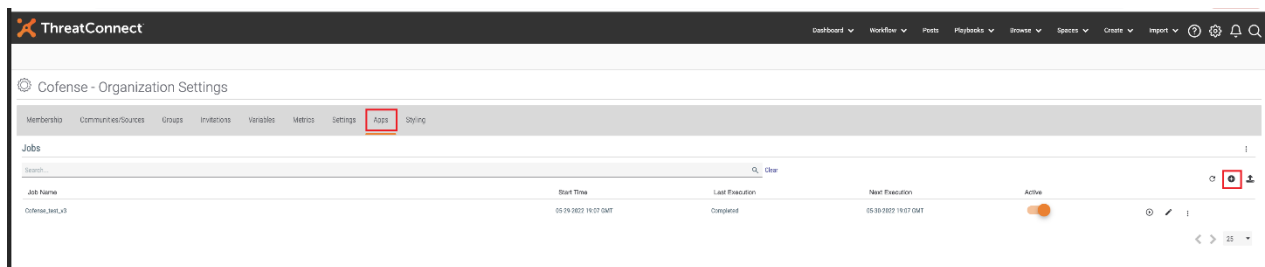
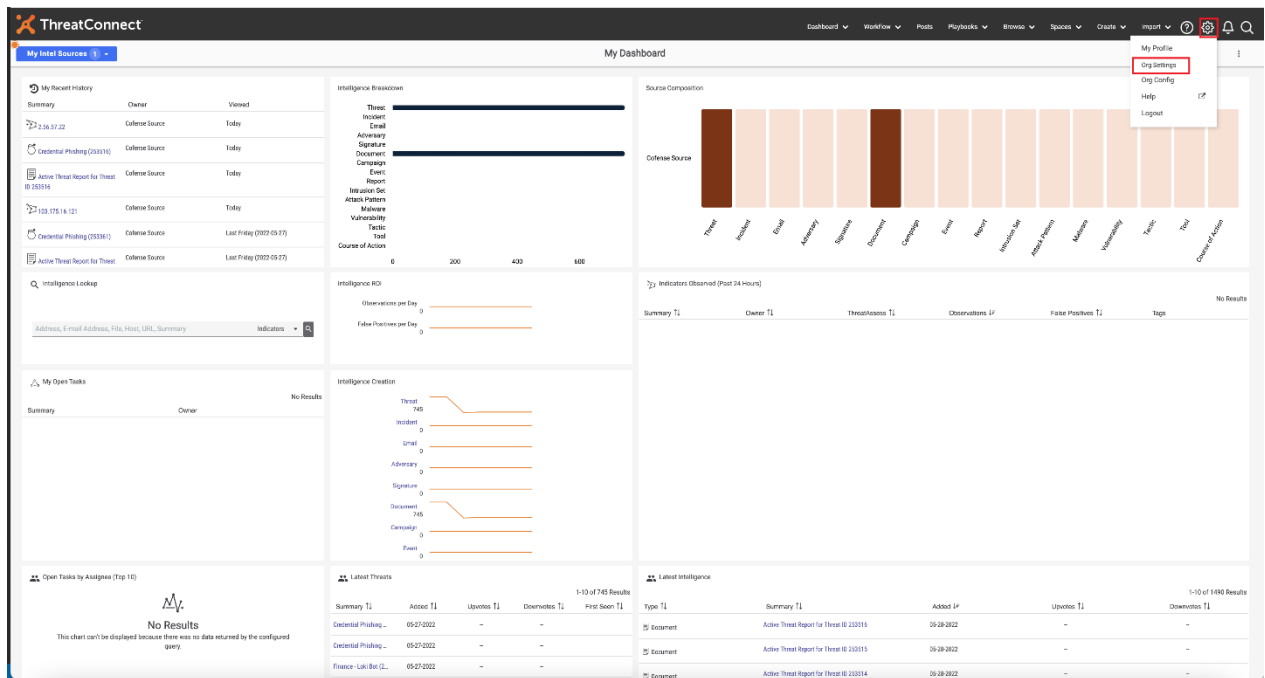
For download and installation instructions, please refer to the ThreatConnect System Administration Guide (Install an App). The App is available on GitHub [here](#). For more information, contact your ThreatConnect Customer Success representatives.

ThreatConnect Job Configuration

ThreatConnect Platform allows customers to run jobs on a scheduled basis. Once the package has been installed, the customer enabled to run the Cofense Threat Intelligence feed as frequently as they desire. By default, the App will run daily.

Note: These steps are not necessary if the app was deployed using Feed Deployer as the job would have already been configured.

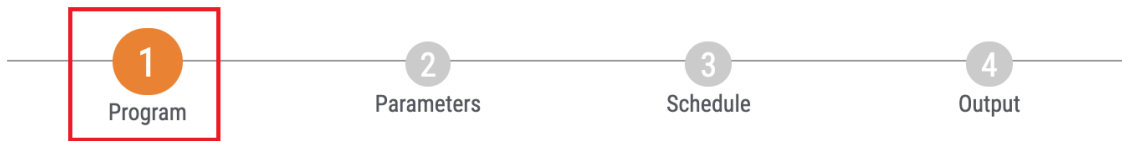
- Go to the gear in the top right corner in the ThreatConnect platform then **Org Settings > Apps**.
- Click on the + to create a new job



Program Screen

- Enter the Job Name (Ex: Cofense).
- Select the Run program as a “Cofense Intelligence v3” from the dropdown.
- Click NEXT.

Add Job



Job Name *

cofense

Run Program

Cofense Intelligence v3

BAE Threat Intelligence

Bambenek Consulting Feed

Cisco Umbrella

Cisco Umbrella Enforcement

Cofense Intelligence

Cofense Intelligence v3

CANCEL

NEXT

Parameter Screen

- For API User, click on the down arrow and select your organization (Required – Username of Cofense Intelligence API credentials that will be used)
- For ThreatConnect Default Org Name click on dropdown arrow as mentioned in the image. (Required - This parameter is the organization name with which the incoming Indicators will be associated)

- For Cofense Intelligence API Base URL (Required -Ex: <https://www.threathq.com/apiv1>)
- Cofense Intelligence API Username (Required – Username of Cofense Intelligence API credentials that will be used)
- Cofense Intelligence API Password (Required – Password of Cofense Intelligence API credentials that will be used.)
- Cofense Intelligence Initial Ingestion Date (YYYY-MM-DD) (Required – How far back to perform the initial ingestion of Cofense Intelligence. Cofense Intelligence recommends 1 to 3 months.)
- ThreatConnect Group Type to Use (Required – Which ThreatConnect Group type to use for organizing each Cofense Intelligence Threat ID. Choices are Threat or Incident (default is Threat)
- Cofense Intelligence Position: This parameter tracks the position this integration is at in Cofense Intelligence after initial ingestion. This value could be accessed or populated for troubleshooting, so it is exposed
- Click NEXT

Schedule Screen

- Depending on your environment, you can schedule the feed at daily hours, weekly etc., select the appropriate values from the dropdown menu.
- Click NEXT

1 Program 2 Parameters 3 Schedule 4 Output

Scheduled job timezone "Asia/Kolkata"

Schedule

☒ At

☐ Every hour between and

CANCEL PREVIOUS **NEXT**

Output Screen

- If you want to be notified on job results, click the box next to Enable Notifications, enter an email address for the notifications to be sent, and which notifications that you want and if you want a log file attached.
- Click SAVE

The screenshot shows a four-step configuration wizard. The steps are: 1. Program, 2. Parameters, 3. Schedule, and 4. Output. Step 4 is the active step, indicated by an orange circle. Below the steps, there are several configuration options:

- ☐ Enable Notifications
- Email Address:
- Notify on Job Result
 - ☐ Success
 - ☐ Partial Failure
 - ☐ Failure
- Attachments
 - ☐ Include Log Files (1MB file size limit)

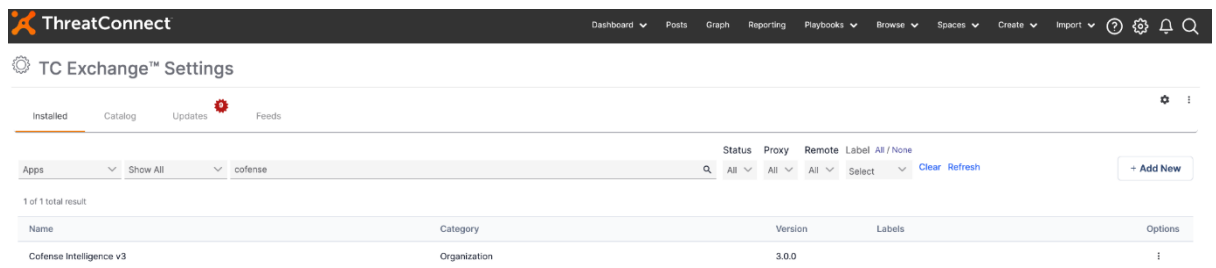
At the bottom right, there are three buttons: CANCEL, PREVIOUS, and SAVE. The SAVE button is highlighted with a red rectangle.

- Once the Job has been saved, we can find our job on Jobs under Apps
- Click on the slider under Active to activate the job.
- Here we can observe the Start Time and Next Execution time and Last Execution Status as well. If you want to run the job at this time, click on the play button in the options tab.

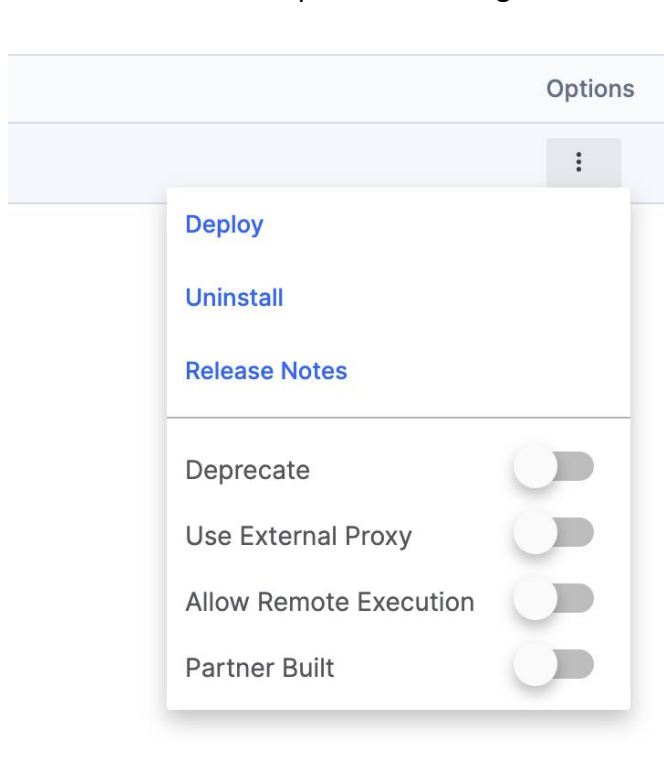
Feed Deployer Instructions

For users that want an easy experience with deploying the Cofense Intelligence Version 3 feed, follow these steps below.

1. Navigate to the TC Exchange Settings area of the ThreatConnect Platform and go to the installed tab. Filter by Apps and type in Cofense in the search bar.



2. Click on the ... under options on the right side and select deploy.



3. The first page of the feed deployer menu will show up. The Sources to Create section will populate automatically with “Cofense Source”. For the Owners section, choose the organization that the source will be created in.

Feed Deployer

Source Parameters Variables Confirm

Sources to Create

Cofense Source

Owner

ThreatConnect PM Team

Note: This operation will overwrite the job for this feed in the selected owner.

☒ Activate Deprecation

☒ Create Attributes

Next

CANCEL DEPLOY

- Click “Next” to advance to the Parameters Tab.

Feed Deployer

Source Parameters Variables Confirm

Cofense Intelligence API Base URL *

https://www.threatq.com/apiv1

Cofense Intelligence API Username *

Cofense Intelligence API Password *

Cofense Intelligence Initial Ingestion Date (YYYY-MM-DD) *

ThreatConnect Group Type to Use *

Back

Next

CANCEL DEPLOY

Source Parameters Variables Confirm

ThreatConnect Group Type to Use *

Threat

Cofense Intelligence Position

Malware Intelligence Stream *

☒

Brand Intelligence Stream *

☒

< Back

> Next

CANCEL DEPLOY

5. The following Parameters need to be filled in:

- a. For Cofense Intelligence API Base URL (Required -Ex: <https://www.threathq.com/apiv1>)
 - b. Cofense Intelligence API Username (Required – Username of Cofense Intelligence API credentials that will be used)
 - c. Cofense Intelligence API Password (Required – Password of Cofense Intelligence API credentials that will be used.)
 - d. Cofense Intelligence Initial Ingestion Date (YYYY-MM-DD) (Required – How far back to perform the initial ingestion of Cofense Intelligence. Cofense Intelligence recommends 1 to 3 months.)
 - e. ThreatConnect Group Type to Use (Required – Which ThreatConnect Group type to use for organizing each Cofense Intelligence Threat ID. Choices are Threat or Incident (default is Threat)
 - f. Cofense Intelligence Position: This parameter tracks the position this integration is at in Cofense Intelligence after initial ingestion. This value could be accessed or populated for troubleshooting, so it is exposed
 - g. Malware Intelligence Stream Checkbox
 - i. Select this checkbox if Malware Intelligence should be included in the feed.
 - h. Brand Intelligence Steam Checkbox
 - i. Select this checkbox if Barnd Intelligence should be included in the feed.
6. Click Next, once the parameters have been filled in.
7. Click next on the variable tab as there are no variables to fill in.
8. Once on the Confirm tab, click the deploy button to deploy the Cofense Intelligence Version 3 feed.

- If the feed has already been deployed on the system in the same org, an error such as below will show up. Select the “Confirm Deployment Over Existing Source” checkbox to redeploy the job and deactivate the previous feed deployer job.

Feed Deployer

Source

Parameters

Variables

Confirm

Source currently has a job for this feed, deploying this feed will disable the existing job. Any currently running jobs should be killed.

☒ Run Feeds after deployment
☒ Activate Feeds after deployment
 Sources to be created:

Cofense Source

Deprecation will be activated.
 Attributes will be created.
☐ Confirm Deployment Over Existing Source

Back

CANCEL

DEPLOY

- Once deployed, a job should show up by the name of “Cofense Intelligence V3” under Organization Settings -> Apps.
- Note that any feeds deactivated by the feed deployer will be shown as well.

ThreatConnect PM Team

ThreatConnect PM Team - Organization Settings

Membership

Communities/Sources

Groups

Invitations

Activity

Variables

Metrics

Settings

Email

Apps

Styling

Jobs

cofense

Clear

Job Name	Start Time	Last Execution	Next Execution	Active	
Cofense Intelligence v3	09-15-2023 02:00 GMT	Completed	09-15-2023 04:00 GMT	<input checked="" type="checkbox"/>	
Cofense Intelligence v3 v3 (Deactivated by Feed Deployer)	09-15-2023 00:00 GMT	Completed	Off	<input type="checkbox"/>	

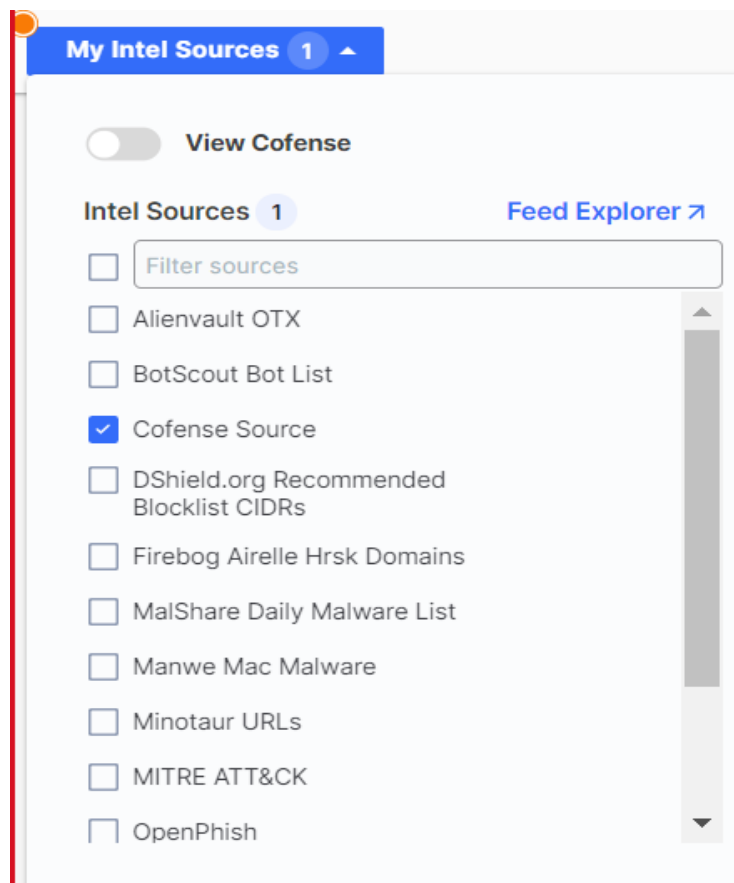
- The created Job will start and run automatically.

Browsing Cofense Intelligence Feed

For guidance on general browsing of indicators and groups in the ThreatConnect Platform, please refer to the article below:

<https://training.threatconnect.com/learn/article/browse-kb-article>

Navigate to the browse page and check to make sure that the Cofense Source Feed is checked.



Browsing Indicators

IP Address Feed

To browse **IP Address Feed** from Cofense Intelligence, select Address Indicator.

The screenshot shows the ThreatConnect interface with the 'Hosts' feed selected. The left sidebar lists various indicators, and the main table displays a list of hosts. The right panel provides detailed information for a selected host, including a threat rating of 241 (Medium), a confidence rating of Confirmed, and a list of attributes and associated indicators.

Host Feed

To browse **Hosts Feed** from Cofense Intelligence, select Host Indicator.

The screenshot shows the ThreatConnect interface with the 'Email Address' feed selected. The left sidebar lists various indicators, and the main table displays a list of email addresses. The right panel provides detailed information for a selected email address, including a threat rating of 503 (High), a confidence rating of Confirmed, and a list of attributes and associated indicators.

Email Address Feed

To browse **Email Address Feed** from Cofense Intelligence, select Email Address Indicator.

The screenshot shows the ThreatConnect interface with the 'Email Address' indicator selected. The table lists various email addresses from the 'Colense Intelligence' source, all with a threat rating of 503 (High). The details panel on the right shows the specific indicator for 'droidyandex@centralefiltris.cl' with a threat rating of 503 (High) and a confidence rating of 'Confirmed'.

Type	Summary	Owner	Threat Rating	ThreatAssess	Obs
Email Address	droidyandex@centralefiltris.cl	Colense Intelligence	503	High	-
Email Address	hunkun@vub.be	Colense Intelligence	503	High	-
Email Address	info2@bunnet.ru	Colense Intelligence	503	High	-
Email Address	sakee@powerfactory.com	Colense Intelligence	503	High	-
Email Address	sakee@power2.ru	Colense Intelligence	503	High	-
Email Address	potemkin@sunrisebbs.com	Colense Intelligence	503	High	-
Email Address	werner.wagner@esens.com	Colense Intelligence	503	High	-
Email Address	marat.sulyayev@com	Colense Intelligence	503	High	-
Email Address	king@ethereum-exchange.com	Colense Intelligence	382	High	-
Email Address	king@ethereum-exchange.com	Colense Intelligence	503	High	-

File Feed

To browse **File Feed** from Cofense Intelligence, select File Indicator.

The screenshot shows the ThreatConnect interface with the 'File' indicator selected. The table lists various file hashes from the 'Colense Intelligence' source, all with a threat rating of 503 (High). The details panel on the right shows the specific indicator for 'FD5BE840876D9A8CE05D990159D74B:23193D6AC6A6B49DBA17C8C0438FFA38D6BF1175F' with a threat rating of 503 (High) and a confidence rating of 'Confirmed'.

Type	Summary	Owner	Threat Rating	ThreatAssess	Obs
File	FD5BE840876D9A8CE05D990159D74B:23193D6AC6A6B49DBA17C8C0438FFA38D6BF1175F	Colense Intelligence	503	High	-
File	A4A787F7E4E8C0F8E2C8628E3C0B	Colense Intelligence	503	High	-
File	018D3EC4265128872CE8F96148EE	Colense Intelligence	503	High	-
File	68E76B3E23D88C217103C8BC246:83C8B3C8E30A88B83F0C70A88772C4A7009	Colense Intelligence	503	High	-
File	15887286A8371F762D43B180C812	Colense Intelligence	503	High	-
File	7D8B0A677A56161207D8740A7425	Colense Intelligence	503	High	-
File	2AF3826A4B1100C77E11AB8933	Colense Intelligence	503	High	-
File	0EE5A0C62078C8B0AC8F44D1D0DE7:9775A58778B3C1C1C274FE4AECBAAC0378B2	Colense Intelligence	645	High	-
File	1ED862C45332281930313D85428:FUEVFC2B18C78C3410F4645A4F248B03A	Colense Intelligence	503	High	-
File	C3F86E5104FCC7879F1C3E8A7D0C3A:863775D5F3E4033D3F8AC31860C7E74799	Colense Intelligence	503	High	-

URL Feed

To browse **URL Feed** from Cofense Intelligence, select URL Indicator.

The screenshot displays the ThreatConnect interface. On the left, a sidebar lists various indicators such as Address, File, Host, URL, ASN, and Groups. The 'URL' indicator is selected. The main panel shows a list of indicators with columns for Type, Summary, Owner, Threat Rating, Threat Score, and Obs. The 'URL' indicator is highlighted. On the right, a detailed view of the selected indicator is shown, including a Threat Rating of 503 (High), a Confidence Score of 100% (Confirmed), and a list of attributes and associated intel.

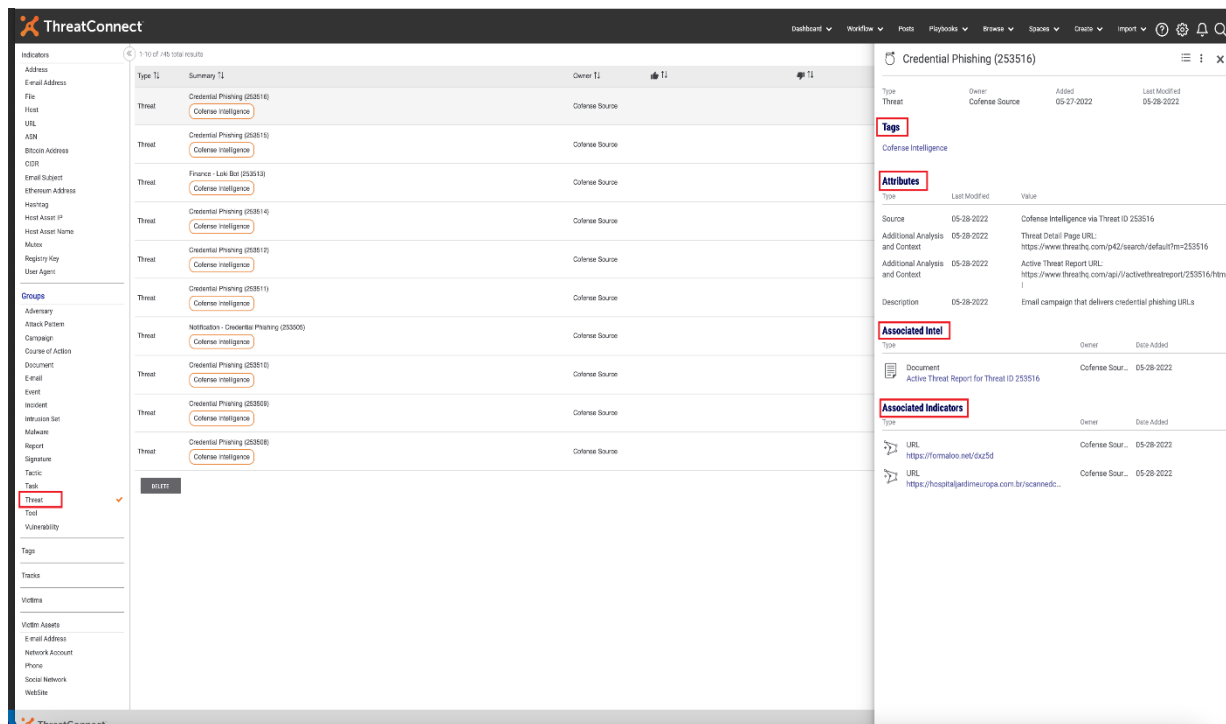
Browsing Groups Document

To browse **Document** from Cofense Intelligence, select Document Group.

The screenshot displays the ThreatConnect interface. On the left, a sidebar lists various indicators such as Address, File, Host, URL, ASN, and Groups. The 'Document' indicator is selected. The main panel shows a list of documents with columns for Type, Format, Summary, Owner, and Threat Rating. The 'Document' indicator is highlighted. On the right, a detailed view of the selected document is shown, including a File Information section, a Threat Rating of 100% (Confirmed), and a list of attributes and associated intel.

Threat

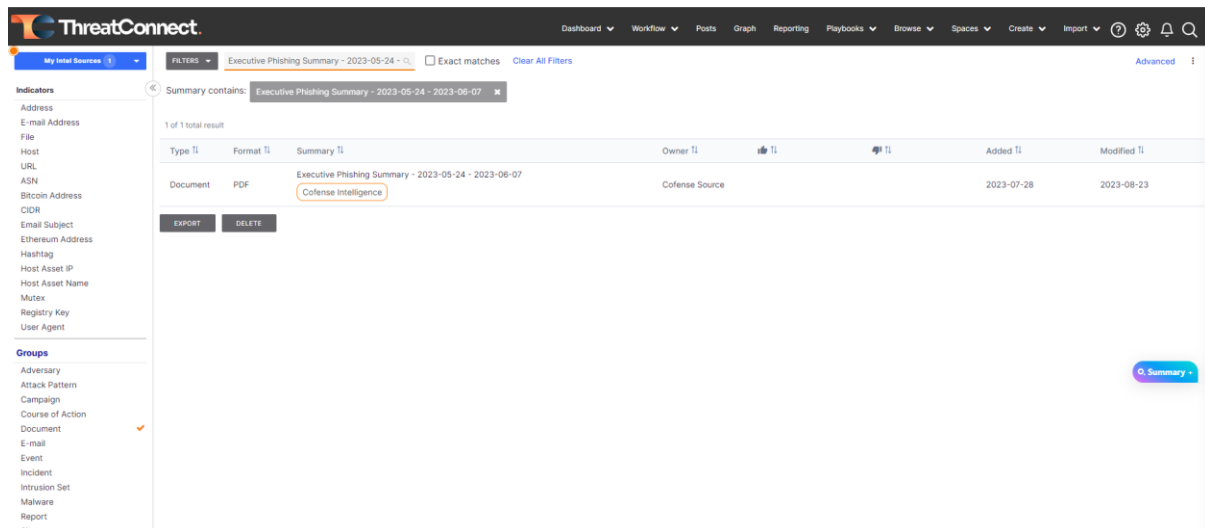
To browse **Threat** from Cofense Intelligence, select Threat Group.



The screenshot shows the ThreatConnect interface. On the left, the 'Threat' group is selected under the 'Groups' section. The main panel displays a list of threats, with 'Credential Phishing (253516)' highlighted. The right panel shows the details for this threat, including its type (Threat), owner (Cofense Source), and added date (05-27-2022). The 'Attributes' section lists various details such as Source, Additional Analysis, and Description. The 'Associated Intel' section shows a document titled 'Active Threat Report for Threat ID 253516'. The 'Associated Indicators' section lists two URLs: 'https://formaloo.net/dx5d' and 'https://hospitaladmeurges.com.br/scanned...'.

Browsing Intel Finished Reports

To browse **Intel Finished Reports** from Cofense Intelligence, select Document Group.



The screenshot shows the ThreatConnect interface. On the left, the 'Document' group is selected under the 'Groups' section. The main panel displays a list of documents, with 'Executive Phishing Summary - 2023-05-24 - 2023-06-07' highlighted. The right panel shows the details for this document, including its type (Document), format (PDF), owner (Cofense Source), and added date (2023-07-28). The 'Attributes' section lists various details such as Source, Additional Analysis, and Description. The 'Associated Intel' section shows a document titled 'Active Threat Report for Threat ID 253516'. The 'Associated Indicators' section lists two URLs: 'https://formaloo.net/dx5d' and 'https://hospitaladmeurges.com.br/scanned...'.

Support

For assistance with this App, to report a bug, or feature requests please contact us via the following.

Support Portal	https://cofense.com/contact-support/
Email	support@cofense.com