



ThreatConnect – Cofense Intelligence Integration User Guide

Version 3.0.0

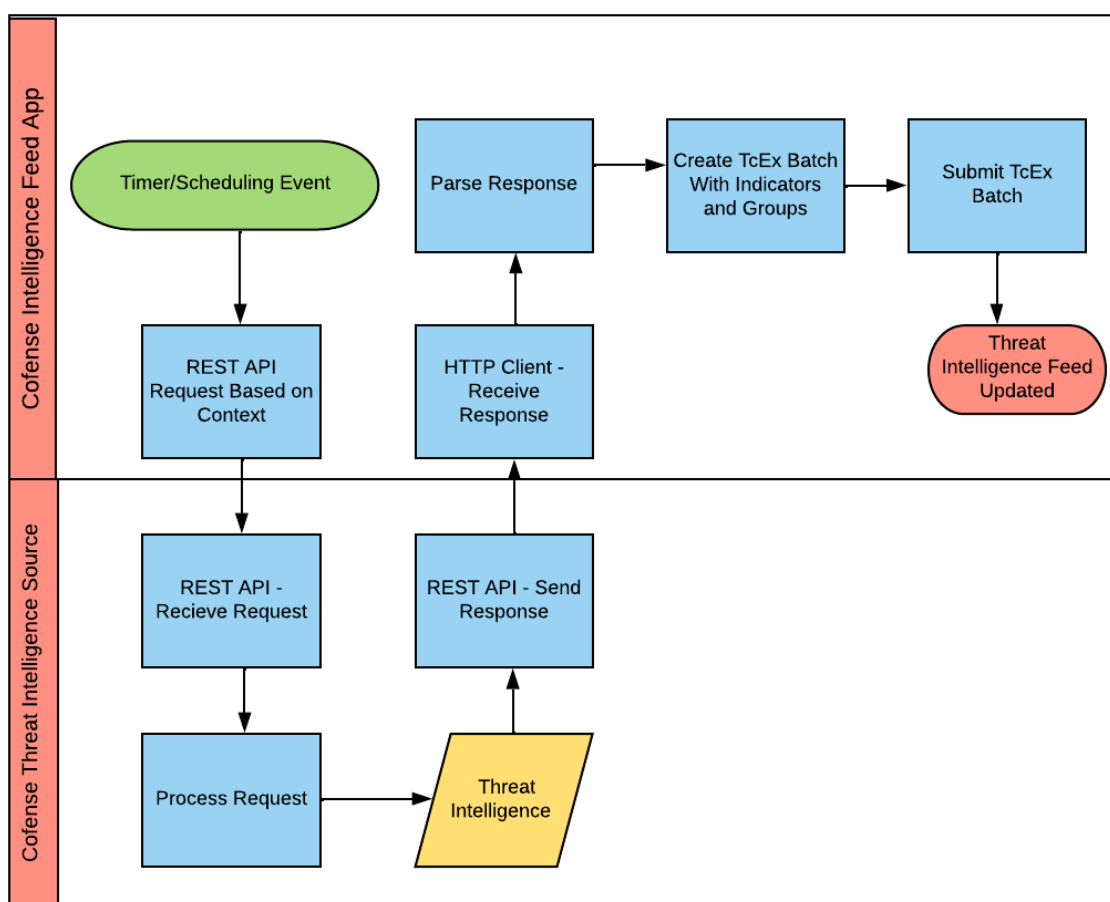
Contents

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
Browsing Cofense Consulting Feed	9
Browsing Indicators	10
IP Address Feed	10
Host Feed	11
Email Address Feed	11
File Feed	11
URL Feed.....	12
Browsing Groups.....	13
Document.....	13
Threat	13
Support.....	14

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
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

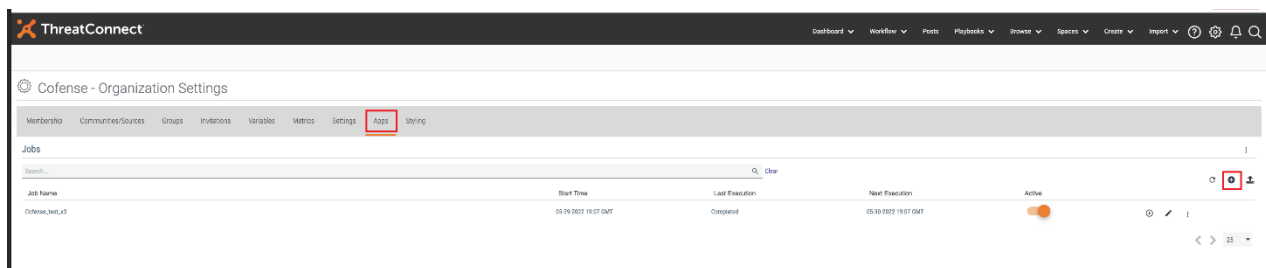
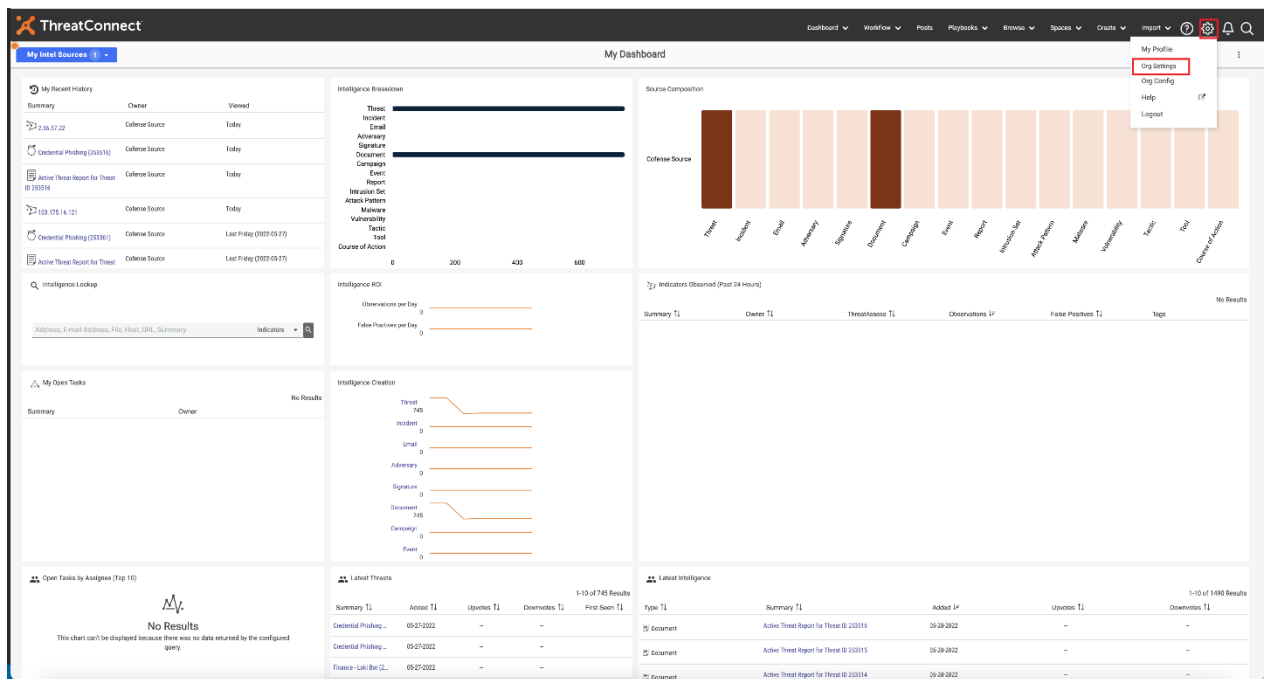
For download and installation instructions, please refer to the ThreatConnect System Administration Guide (Install an App). For more information, contact your ThreatConnect Customer Success representatives.

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

The screenshot shows the ThreatConnect 'Add Job' configuration interface. The 'Configure' tab is selected, displaying various configuration fields for a new job. A red box highlights the 'NEXT' button at the bottom right of the configuration pane. The right-hand pane displays a table with columns for Job ID, Name, Status, and Last Run, showing a single job entry.

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

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

1
Program

2
Parameters

3
Schedule

4
Output

☐ Enable Notifications

Email Address

Notify on Job Result
☐ Success
☐ Partial Failure
☐ Failure

Attachments
☐ Include Log Files (1MB file size limit)

CANCEL

PREVIOUS

SAVE

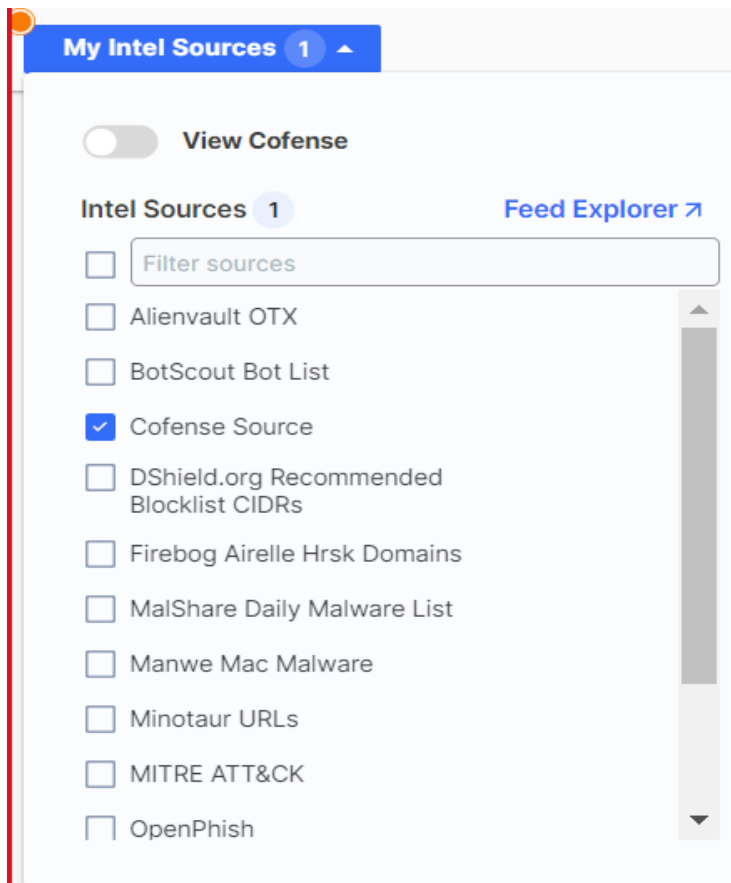
- Once the Job has been saved, we can find our job on Jobs under Apps
- Click on the slider under Active to activate the job.
- Here we can observe the Start Time and Next Execution time and Last Execution Status as well. If you want to run the job at this time, click on the play button in the options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

Browsing Cofense Consulting 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.

Type	Summary	Owner	Version	Threat Rating	Threats	One
Address	2.56.87.22	Cofense Source	IPv4	241		
Address	103.175.16.121	Cofense Source	IPv4	388		
Address	64.44.130.206	Cofense Source	IPv4	381		
Address	68.233.238.105	Cofense Source	IPv4	412		

Threat Rating: 241 Medium

Confidence Rating: Confirmed

Attributes:

- Source: 05-28-2022 Cofense Intelligence via Threat ID 253110
- Additional Analysis and Content: 05-28-2022 Threat Detail Page URL: <https://www.threatconnect.com/p2/research/default.htm?threatid=253110>
- Additional Analysis and Content: 05-28-2022 Active Threat Report URL: <https://www.threatconnect.com/api/v2/threatreport/253110.htm>
- Additional Analysis and Content: 05-28-2022 Payload: Location from which a payload is obtained (Threat ID 253110)
- Description: 05-28-2022 CVE-2017-11882: Microsoft Office exploit taking advantage of flaw in Microsoft Equation Editor allowing for arbitrary code execution (Threat ID 253110)

Associated Intel:

Type	Owner	Date Added
Threat Shipping - CVE 2017-11882, GULoader, Agent T...	Cofense Sour...	05-27-2022

Associated Indicators:

Type	Owner	Date Added
File 016D5A36C4395512887388F98163CE	Cofense Sour...	05-28-2022
File AAA975F7EF46E83F88E2C8828E0C8B	Cofense Sour...	05-28-2022
EmailAddress droidyanden@centralidafitros.d	Cofense Sour...	05-28-2022
File 66E27633E2232048D6172109C802246_83...	Cofense Sour...	05-28-2022
URL http://2.56.87.22/ndrpe.exe	Cofense Sour...	05-28-2022

Host Feed

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

The screenshot shows the ThreatConnect interface. On the left, the 'Indicators' sidebar has 'Host' selected. The main table displays a list of host indicators, all sourced from 'Cofense Intelligence'. The right pane shows the details for the host 'www.jiangsuck.com'. It includes a 'ThreatAssess' gauge showing a '503 High' rating, a 'Threat Rating' of 'Moderate', and a 'Confidence Rating' of 'Confirmed'. Below this, there are sections for 'Tags', 'Attributes', 'Associated Intel', and 'Associated Indicators'.

Type	Summary	Owner	Threat Rating	ThreatScore	Obs
Host	www.jiangsuck.com	Cofense Intelligence	503	High	0
Host	www.madebounfo	Cofense Intelligence	516	High	0
Host	www.apnigh.com	Cofense Intelligence	503	High	0
Host	www.kitchenapplianceguy.com	Cofense Intelligence	503	High	0
Host	www.adsscomm.com	Cofense Intelligence	503	High	0
Host	www.dangof.com	Cofense Intelligence	503	High	0
Host	www.miguelgarcia.com	Cofense Intelligence	503	High	0
Host	www.Bloose.net	Cofense Intelligence	503	High	0
Host	www.men.roa	Cofense Intelligence	503	High	0
Host	www.odysseia.com	Cofense Intelligence	503	High	0

Email Address Feed

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

The screenshot shows the ThreatConnect interface. On the left, the 'Indicators' sidebar has 'Email Address' selected. The main table displays a list of email address indicators, all sourced from 'Cofense Intelligence'. The right pane shows the details for the email address 'droidyandex@centraledifilros.cl'. It includes a 'ThreatAssess' gauge showing a '503 High' rating, a 'Threat Rating' of 'Critical', and a 'Confidence Rating' of 'Confirmed'. Below this, there are sections for 'Tags', 'Attributes', 'Associated Intel', and 'Associated Indicators'.

Type	Summary	Owner	Threat Rating	ThreatScore	Obs
EmailAddress	droidyandex@centraledifilros.cl	Cofense Intelligence	503	High	0
EmailAddress	humbun@nubio.com	Cofense Intelligence	503	High	0
EmailAddress	info@barnesandnoble.com	Cofense Intelligence	503	High	0
EmailAddress	saee@powerfactory.com	Cofense Intelligence	503	High	0
EmailAddress	sales@power2byd.com	Cofense Intelligence	503	High	0
EmailAddress	potomental@nortel.com	Cofense Intelligence	503	High	0
EmailAddress	www@agor@centraledifilros.cl	Cofense Intelligence	503	High	0
EmailAddress	marcel@alyssa.com	Cofense Intelligence	503	High	0
EmailAddress	king@ed@extra-exchange.com	Cofense Intelligence	382	High	0
EmailAddress	king@ed@extra-exchange.com	Cofense Intelligence	303	High	0

File Feed

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

The screenshot displays the ThreatConnect interface. On the left, the 'Indicators' sidebar is visible with 'File' selected. The main table shows a list of indicators, all of which are 'File' type and sourced from 'Cofense Intelligence'. The right-hand panel provides a detailed view of a selected indicator (ID: 23193DE6AE6B49DBA17C8C0438FFA3B06B1175F). It includes a 'ThreatAssess' section with a '503 High' rating, a 'Tags' section with 'Cofense Intelligence', and an 'Attributes' table listing source, analysis, and description. Below this, 'Associated Intel' and 'Associated Indicators' are also shown.

URL Feed

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

This screenshot shows the ThreatConnect interface with 'URL' selected in the 'Indicators' sidebar. The main table lists various URL indicators, all sourced from 'Cofense Intelligence'. The right-hand panel details a specific URL indicator (ID: https://hospitaljardimeuropa.com.br/scannedconfirmation/). It features a 'ThreatAssess' section with a '503 High' rating, a 'Tags' section with 'Cofense Intelligence', and an 'Attributes' table. The 'Associated Intel' and 'Associated Indicators' sections are also present, showing related threat intelligence.

Browsing Groups

Document

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

The screenshot shows the ThreatConnect interface. On the left sidebar, the 'Document' group is selected under the 'Groups' section. The main table displays a list of documents, each with columns for Type, Format, Summary, and Owner. The right sidebar shows details for 'Active Threat Report for Threat ID 253516', including File Information, Tags, Attributes, Associated Intel, and Associated Indicators.

Type	Format	Summary	Owner
Document	HTML	Active Threat Report for Threat ID 253516	Cofense Source
Document	HTML	Active Threat Report for Threat ID 253515	Cofense Source
Document	HTML	Active Threat Report for Threat ID 253514	Cofense Source
Document	HTML	Active Threat Report for Threat ID 253512	Cofense Source
Document	HTML	Active Threat Report for Threat ID 253511	Cofense Source
Document	HTML	Active Threat Report for Threat ID 253510	Cofense Source
Document	HTML	Active Threat Report for Threat ID 253509	Cofense Source
Document	HTML	Active Threat Report for Threat ID 253508	Cofense Source
Document	HTML	Active Threat Report for Threat ID 253507	Cofense Source
Document	HTML	Active Threat Report for Threat ID 253506	Cofense Source

Threat

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

The screenshot shows the ThreatConnect interface. On the left sidebar, the 'Threat' group is selected under the 'Groups' section. The main table displays a list of threats, each with columns for Type, Summary, and Owner. The right sidebar shows details for 'Credential Phishing (253516)', including Tags, Attributes, Associated Intel, and Associated Indicators.

Type	Summary	Owner
Threat	Credential Phishing (253516)	Cofense Source
Threat	Credential Phishing (253515)	Cofense Source
Threat	France - Lark Bar (253513)	Cofense Source
Threat	Credential Phishing (253514)	Cofense Source
Threat	Credential Phishing (253512)	Cofense Source
Threat	Credential Phishing (253511)	Cofense Source
Threat	Notification - Credential Phishing (253505)	Cofense Source
Threat	Credential Phishing (253510)	Cofense Source
Threat	Credential Phishing (253509)	Cofense Source
Threat	Credential Phishing (253508)	Cofense Source

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