



# ThreatConnect – Cofense Intelligence Integration User Guide

Version 3.0.0

## Release Notes

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

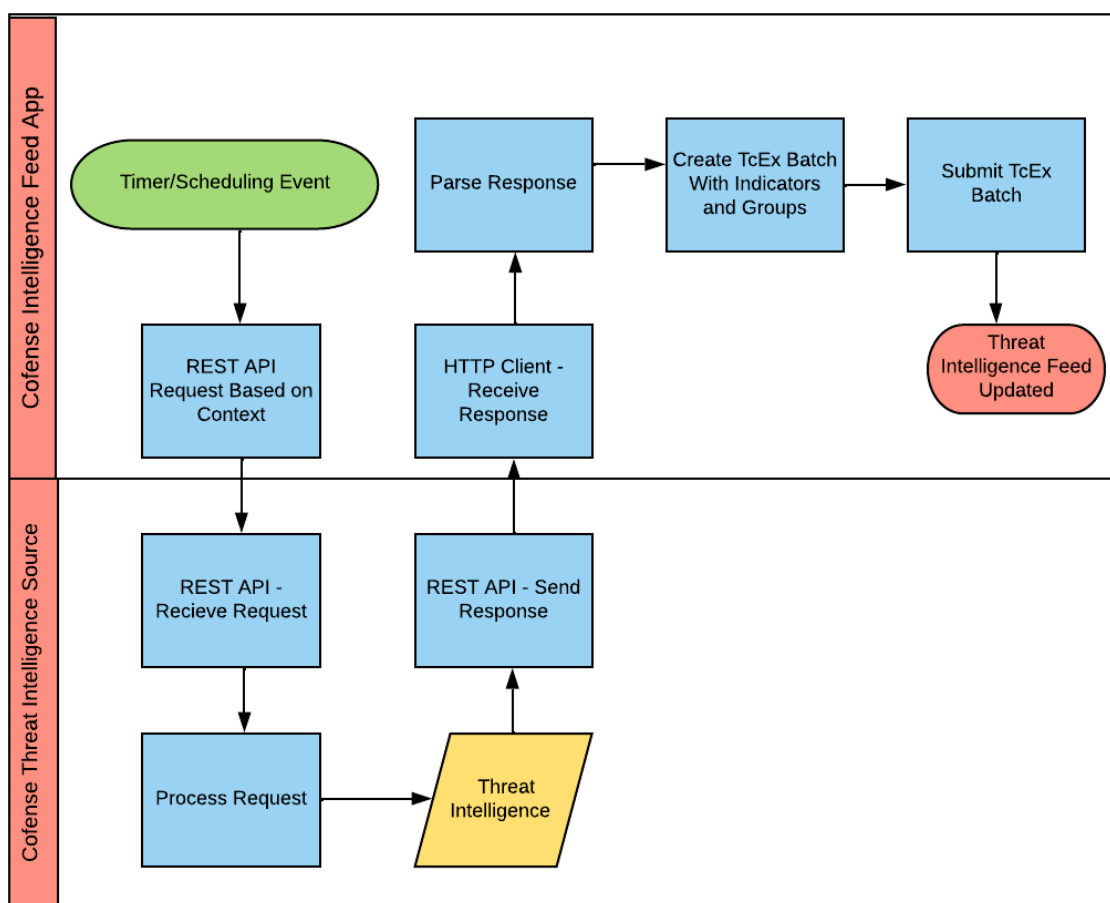
## Contents

<b>Introduction</b>	3
<b>Release Notes</b>	1
<b>Data Mapping</b>	4
<b>Configuration Requirements</b>	4
<b>Job App Installation</b>	4
<b>ThreatConnect Job Configuration</b>	4
Program Screen	6
Parameter Screen	7
Schedule Screen	8
Output Screen	9
<b>Browsing Cofense Consulting Feed</b>	10
<b>Browsing Indicators</b>	11
IP Address Feed	11
Host Feed	11
Email Address Feed	12
File Feed	12
URL Feed	13
<b>Browsing Groups</b>	14
Document	14
Threat	14
<b>Cofense Intelligence Ratings</b>	15
Indicator Threat Rating Mapping – Cofense to ThreatConnect	15
<b>Support</b>	16

## 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.



## 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

**ThreatConnect**

My Dashboard

Org Settings

My Recent History

Summary	Owner	Viewed
2.2.26.17.22	Cofense Source	Today
Cofense Phishing (233316)	Cofense Source	Today
Active Threat Report for Threat ID 233316	Cofense Source	Today
103.175.18.121	Cofense Source	Today
Cofense Phishing (233316)	Cofense Source	Last Friday (2022-05-07)
Active Threat Report for Threat	Cofense Source	Last Friday (2022-05-07)

Intelligence Breakdown

Source Composition

Intelligence ROI

Intelligence Creation

Open Tasks by Assignee (Top 10)

Latest Threats

Latest Intelligence

**ThreatConnect**

Cofense - Organization Settings

App

Jobs

Job Name	Start Time	Last Execution	Next Execution	Active
Cofense_int_v3	05-19-2022 18:07 GMT	Completed	05-19-2022 18:07 GMT	Active

## Program Screen

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

**ThreatConnect**

### Add Job ×

1 **Program** 2 Parameters 3 Schedule 4 Output

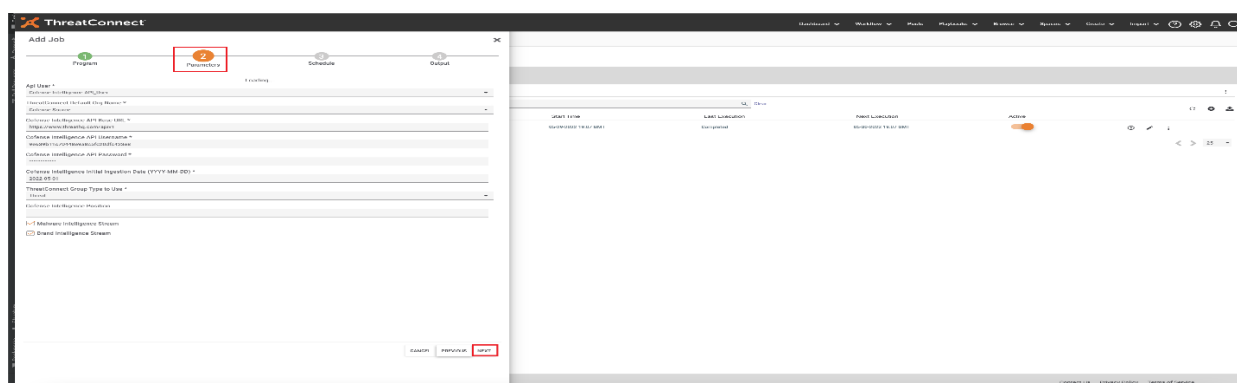
**Job Name \***  
cofense

**Run Program**  
Cofense Intelligence v3  
BAE Threat Intelligence  
Bambenek Consulting Feed  
Cisco Umbrella  
Cisco Umbrella Enforcement  
Cofense Intelligence  
Cofense Intelligence v3

**CANCEL** **NEXT**

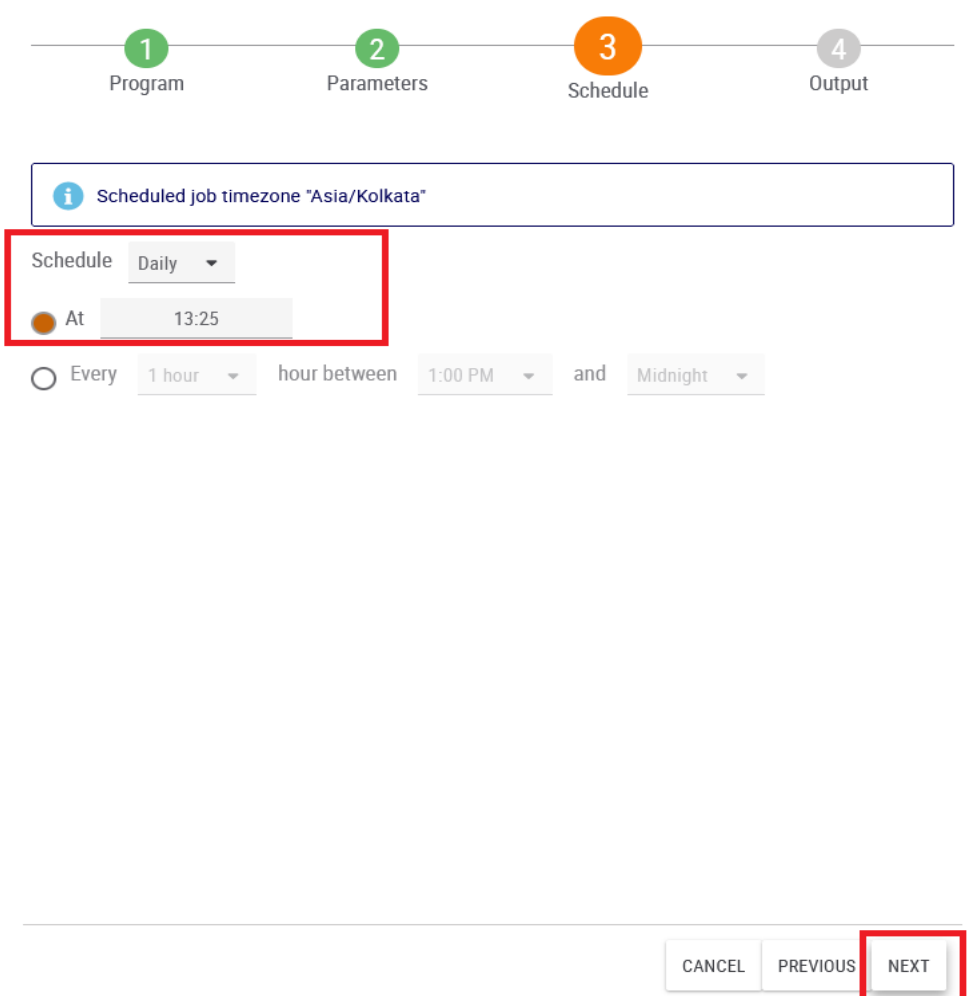
## Parameter Screen

- 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

*i* Scheduled job timezone "Asia/Kolkata"

Schedule Daily ▼

☒ At 13:25

☐ Every 1 hour ▼ hour between 1:00 PM ▼ and Midnight ▼

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

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

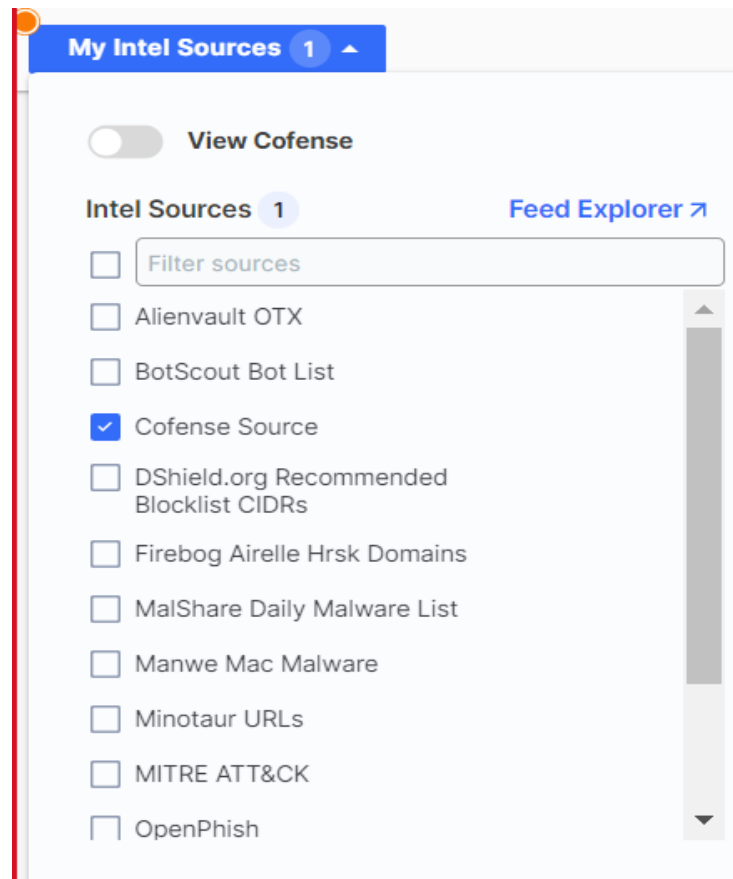
- Once the Job has been saved, we can find our job on Jobs under Apps
- Click on the slider under Active to activate the job.
- Here we can observe the Start Time and Next Execution time and Last Execution Status as well. If you want to run the job at this time, click on the play button in the options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

The screenshot displays the ThreatConnect interface with the 'Indicators' section selected. The 'Address' indicator is chosen, showing a list of IP addresses. The right-hand panel provides detailed information for a selected indicator, including a threat rating of 'Low' (241), a confirmed status, and various attributes like source, additional analysis, and description. The 'Associated Intel' and 'Associated Indicators' sections are also visible.

Type	Summary	Owner	Version	Threat Rating	ThreatAssess	Obs
Address	256.67.22	Cofense Source	IPv4	Low	241	---
Address	103.175.16.121	Cofense Source	IPv4	Low	383	---
Address	64.44.134.266	Cofense Source	IPv4	Low	381	---
Address	68.233.238.105	Cofense Source	IPv4	Low	412	---

**Threat Rating:** 241 Medium

**Confidence Rating:** Confirmed

**Tags:** Cofense Intelligence

**Attributes:**

Type	Last Modified	Value
Source	05-28-2022	Cofense Intelligence via Threat ID 253110
Additional Analysis and Context	05-28-2022	Threat Detail Page URL: <a href="https://www.threatq.com/p42/search/default.htm?c253110">https://www.threatq.com/p42/search/default.htm?c253110</a>
Additional Analysis and Context	05-28-2022	Active Threat Report URL: <a href="https://www.threatq.com/api/v/activethreatreport/253110.htm">https://www.threatq.com/api/v/activethreatreport/253110.htm</a>
Additional Analysis and Context	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	Cofense Sour...	05-27-2022

**Associated Indicators:**

Type	Owner	Date Added
File	Cofense Sour...	05-28-2022
File	Cofense Sour...	05-28-2022
EmailAddress	Cofense Sour...	05-28-2022
File	Cofense Sour...	05-28-2022
URL	Cofense Sour...	05-28-2022

## Host Feed

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

The screenshot displays the ThreatConnect interface with the 'Indicators' section selected. The 'Host' indicator is chosen, showing a list of hostnames. The right-hand panel provides detailed information for a selected indicator, including a threat rating of 'Moderate' (503), a confirmed status, and various attributes like source, additional analysis, and description. The 'Associated Intel' and 'Associated Indicators' sections are also visible.

Type	Summary	Owner	Version	Threat Rating	ThreatAssess	Obs
Host	www.jiangsuck.com	Cofense Source		Moderate	503	---
Host	www.madebox.info	Cofense Source		Moderate	516	---
Host	www.apnigh.com	Cofense Source		Moderate	503	---
Host	www.kitchenapplianceshop.com	Cofense Source		Moderate	503	---
Host	www.adresscommerce.com	Cofense Source		Moderate	503	---
Host	www.cargat.com	Cofense Source		Moderate	503	---
Host	www.kyghupersons.com	Cofense Source		Moderate	503	---
Host	www.Biqua.net	Cofense Source		Moderate	503	---
Host	www.men.roa	Cofense Source		Moderate	503	---
Host	www.odanterior.com	Cofense Source		Moderate	503	---

**Threat Rating:** 503 High

**Confidence Rating:** Confirmed

**Tags:** Cofense Intelligence

**Attributes:**

Type	Last Modified	Value
Source	05-27-2022	Cofense Intelligence via Threat ID 253357
Additional Analysis and Context	05-27-2022	Threat Detail Page URL: <a href="https://www.threatq.com/p42/search/default.htm?c253357">https://www.threatq.com/p42/search/default.htm?c253357</a>
Additional Analysis and Context	05-27-2022	Active Threat Report URL: <a href="https://www.threatq.com/api/v/activethreatreport/253357.htm">https://www.threatq.com/api/v/activethreatreport/253357.htm</a>
Additional Analysis and Context	05-27-2022	C2 Command and control location used by malware (Threat ID 253357)
Description	05-27-2022	FormBook: FormBook is a browser focused keylogger coded in ASM/C. It can record keystrokes, form input, clipboard contents, take screenshots, and recover stored credentials from many different applications. (Threat ID 253357)

**Associated Intel:**

Type	Owner	Date Added
Threat Order - FormBook (253357)	Cofense Sour...	05-27-2022

**Associated Indicators:**

Type	Owner	Date Added
File	Cofense Sour...	05-27-2022

## 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 main table lists several email addresses, each with a 'Threat Rating' of 503 (Critical) and a 'Confidence Rating' of 'Confirmed'. The right sidebar provides detailed information for the selected email address, including a 'ThreatAssess' section with a '503 High' rating, 'Tags' (Cofense Intelligence), 'Attributes' (Source, Additional Analysis, and Context), 'Associated Intel' (Threat: Shipping - CVE-2017-11882, Outloader, Agent T...), and 'Associated Indicators' (File: FD5B840876D9A8CE05D990159074B: 23193DE6AE6B49DBA17C8C0438FFA38D6BF1175F).

## File Feed

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

The screenshot shows the ThreatConnect interface with the 'File' indicator selected. The main table lists several file hashes, each with a 'Threat Rating' of 503 (Critical) and a 'Confidence Rating' of 'Confirmed'. The right sidebar provides detailed information for the selected file hash, including a 'ThreatAssess' section with a '503 High' rating, 'Tags' (Cofense Intelligence), 'Attributes' (Source, Additional Analysis, and Context), 'Associated Intel' (Threat: Finance - Loki Bot (253513)), and 'Associated Indicators' (URL: http://sempersu.us/gg/11/rn.php).

## URL Feed

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

**ThreatConnect**

Dashboard Workflow Reports Playbooks Integrations Spaces Create Import Settings Status set by

My Intel Sources 1-10 of 2493 total results

Pictures Summary Contains Exact matches Clear All Filters

Type T1	Summary T1	Owner T1	Threat Rating T1	ThreatAssess T1	Ota T1
URL	https://hospitaljardineuropa.com.br/scannedconfirmation/ <b>Confidence Intelligence</b>	Confense Source	★★★★★	503	-
ASN	https://formaloo.net/dx5d <b>Confence Intelligence</b>	Confense Source	★★★★★	485	-
URL	https://api.gripeponse.com/best5f8fa6527be18dafc7828108ba51a7d7~Q2rdaAweshtenre_slnzVL <b>Confence Intelligence</b>	Confense Source	★★★★★	485	-
URL	https://romasaguest-my.sharepoint.com/:443ra3gipersonalpatencia_blanco_omasa_esv6ak8Mh_BUFGm_hCqgtUkUalga... <b>Confence Intelligence</b>	Confense Source	★★★★★	428	-
URL	https://api-grip-microservices.tallfun.com/ <b>Confence Intelligence</b>	Confense Source	★★★★★	485	-
URL	https://riepscrymes.com/?file=index.php <b>Confence Intelligence</b>	Confense Source	★★★★★	485	-
URL	https://apiappcloudr1.bencokapp.com/ <b>Confence Intelligence</b>	Confense Source	★★★★★	485	-
URL	https://api-grip-35aaa-assad-qdrca-cal.icd.app/ <b>Confence Intelligence</b>	Confense Source	★★★★★	485	-
URL	https://rs.geO7FM9 <b>Confence Intelligence</b>	Confense Source	★★★★★	503	-
URL	https://retelnet-my.sharepoint.com/:o:lqpersonalephank_gatl_conEjZ2HOKZUmGpaWYBumtmbnDg?uiid21... <b>Confence Intelligence</b>	Confense Source	★★★★★	426	-

Groups: Adversary, Attack Pattern, Campaign, Course of Action, Document, e-mail, Event, Incident, Intrusion Set, Malware, Report, Signature, Trick, Task, Threat, Tool, Vulnerability

Tags:

Victim Assets: e-mail Address, Network Account, Phone, Social Network

---

### https://hospitaljardineuropa.com.br/scannedconfirmation/

Status set by

**ThreatAssess**

Recent False Positive Reported  
Impacted by Recent Observations

503 High

Threat Rating: ★★★★★ Critical

Confidence Rating: ★★★★★ Confirmed

**Tags**: Confense Intelligence

**Attributes**:

Type	Last Modified	Value
Source	05-28-2022	Confense intelligence via Threat ID 253516
Additional Analysis and Context	05-28-2022	Threat Detail Page URL: https://www.threatiq.com/p42/search/default?tm=253516
Additional Analysis and Context	05-28-2022	Active Threat Report URL: https://www.threatiq.com/api/v1/active/threatreport/253516.htm#1
Additional Analysis and Context	05-28-2022	Credential Phishing: Credential Phishing (Threat ID 253516)
Description	05-28-2022	Credential Phishing: An instance of credential phishing (Threat ID 253516)

**Associated Intel**:

Type	Owner	Date Added
Threat: Credential Phishing (253516)	Confense Sour.	05-27-2022

**Associated Indicators**:

Type	Owner	Date Added
URL: https://formaloo.net/dx5d	Confense Sour.	05-28-2022

▼ CAL™ Insights

▼ Trends

# Browsing Groups Document

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

The screenshot shows the ThreatConnect interface. On the left, the 'Groups' sidebar is expanded, and 'Document' is selected. The main table displays a list of documents, all of which are 'Active Threat Report for Threat ID 253516' from 'Cofense Intelligence'. The right-hand pane shows the details for 'Active Threat Report for Threat ID 253516'. It includes sections for 'File Information' (Type: Document, Owner: Cofense Source, Added: 05-28-2022, Last Modified: 05-28-2022), 'Tags' (Cofense Intelligence), 'Attributes' (Type, Last Modified, Value), and 'Associated Intel' (Type: Threat, Owner: Cofense Source, Data Added: 05-27-2022).

# Threat

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

The screenshot shows the ThreatConnect interface. On the left, the 'Groups' sidebar is expanded, and 'Threat' is selected. The main table displays a list of threats, all of which are 'Credential Phishing (253516)' from 'Cofense Intelligence'. The right-hand pane shows the details for 'Credential Phishing (253516)'. It includes sections for 'Tags' (Cofense Intelligence), 'Attributes' (Type, Last Modified, Value), 'Associated Intel' (Type: Document, Owner: Cofense Source, Data Added: 05-28-2022), and 'Associated Indicators' (Type: URL, Owner: Cofense Source, Data Added: 05-28-2022).

## Cofense Intelligence Ratings

Cofense Intelligence is human-verified phishing intelligence. Indicators produced and consumed by customers, have been through Cofense's review and therefore should be considered high confidence. Below are indicator ratings in relation to ThreatConnect. In addition, all Cofense Intelligence IOCs will be high confidence, and carry the Confidence Rating – 100% Confirmed.

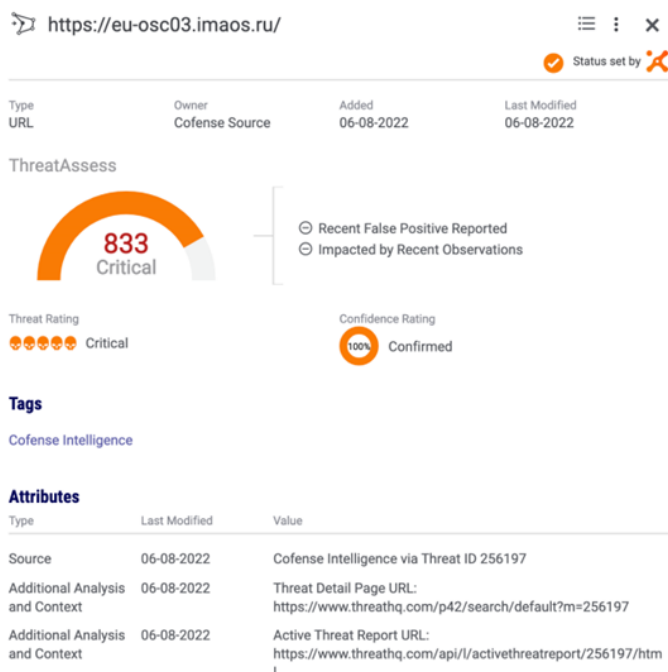
Cofense Intelligence indicators use threat impacting ratings with URLs, domains, files, and IPs:

- Major
- Moderate
- Minor
- None

### Indicator Threat Rating Mapping – Cofense to ThreatConnect

- Major: Critical(5 skulls),
- Moderate: Moderate(3 skulls)
- Minor: Low(2 skulls)
- None: Suspicious(1 skull)

The example below is an URL indicator, designated by Cofense with a Major impact rating. In addition, Cofense Intelligence will always be 100% confirmed in the Confidence Rating field.



## Support

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

<b>Support Portal</b>	<a href="https://cofense.com/contact-support/">https://cofense.com/contact-support/</a>
<b>Email</b>	<a href="mailto:support@cofense.com">support@cofense.com</a>