Icon

Description automatically generated with low confidence

**ThreatConnect – Cofense Intelligence Integration User Guide**

**Version 3.0.0**

Contents

[**Introduction** 3](#_Toc145671781)

[**Release Notes** 4](#_Toc145671782)

[**Data Mapping** 4](#_Toc145671783)

[**Configuration Requirements** 4](#_Toc145671784)

[**Job App Installation** 4](#_Toc145671785)

[**ThreatConnect Job Configuration** 4](#_Toc145671786)

[**Program Screen** 5](#_Toc145671787)

[**Parameter Screen** 6](#_Toc145671788)

[**Schedule Screen** 7](#_Toc145671789)

[**Output Screen** 8](#_Toc145671790)

[**Feed Deployer Instructions** 9](#_Toc145671791)

[**Browsing Cofense Intelligence Feed** 14](#_Toc145671792)

[**Browsing Indicators** 14](#_Toc145671793)

[**IP Address Feed** 14](#_Toc145671794)

[**Host Feed** 15](#_Toc145671795)

[**Email Address Feed** 15](#_Toc145671796)

[**File Feed** 16](#_Toc145671797)

[**URL Feed** 16](#_Toc145671798)

[**Browsing Groups** 17](#_Toc145671799)

[**Document** 17](#_Toc145671800)

[**Threat** 18](#_Toc145671801)

[**Browsing Intel Finished Reports** 18](#_Toc145671802)

[**Support** 18](#_Toc145671803)

# **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.

Diagram

Description automatically generated

# **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**

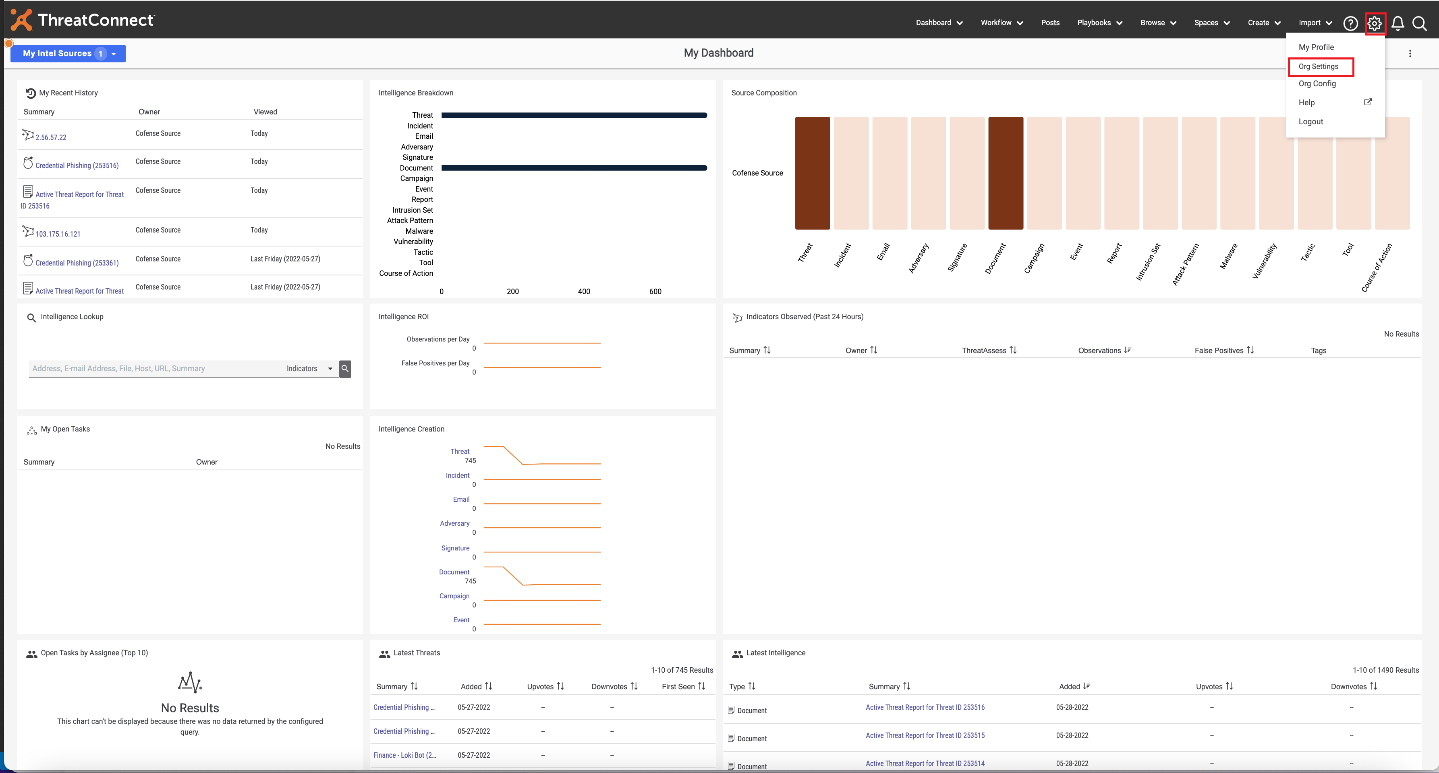
For download and installation instructions, please refer to the ThreatConnect System Administration Guide (Install an App). The App is available on GitHub [here](https://github.com/ThreatConnect-Inc/threatconnect-jobs/tree/master/apps/Cofense-Intelligence-v3). For more information, contact your ThreatConnect Customer Success representatives.

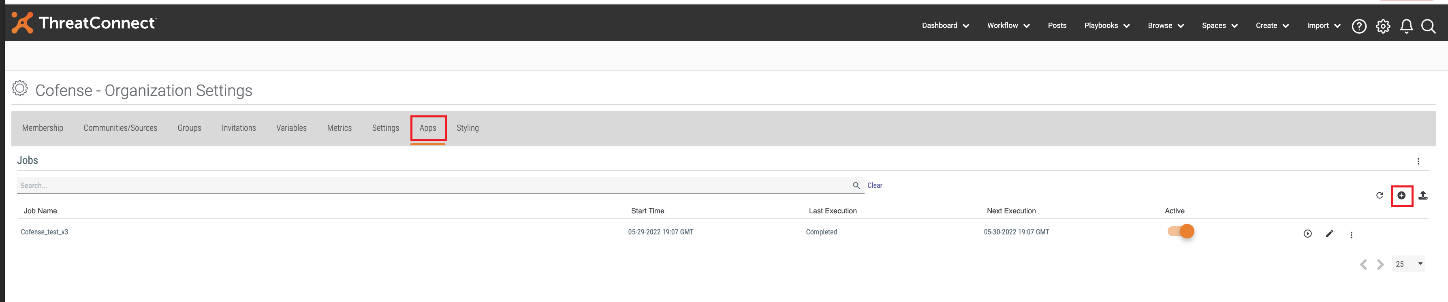
# **ThreatConnect Job Configuration**

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**

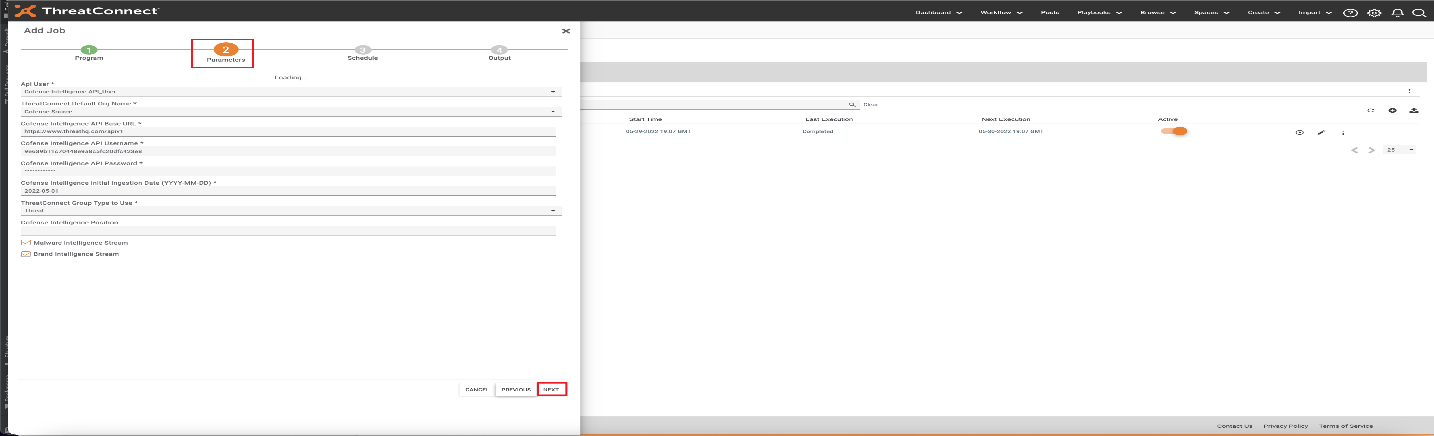
* Enter the Job Name (Ex: Cofense).
* Select the Run program as a “Cofense Intelligence v3” from the dropdown.
* Click NEXT.

Graphical user interface, application

Description automatically generated

## **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

Graphical user interface, text, application, email

Description automatically generated

## **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

Graphical user interface, application

Description automatically generated

* 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.

A screenshot of a computer

Description automatically generated

1. Click on the … under options on the right side and select deploy.

A screenshot of a computer

Description automatically generated

1. 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.

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. The following Parameters need to be filled in:
   1. For Cofense Intelligence API Base URL (Required -Ex: https://www.threathq.com/apiv1 )
   2. Cofense Intelligence API Username (Required – Username of Cofense Intelligence API credentials that will be used)
   3. Cofense Intelligence API Password (Required – Password of Cofense Intelligence API credentials that will be used.)
   4. 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.)
   5. 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)
   6. 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
   7. Malware Intelligence Stream Checkbox
      1. Select this checkbox if Malware Intelligence should be included in the feed.
   8. Brand Intelligence Steam Checkbox
      1. Select this checkbox if Barnd Intelligence should be included in the feed.
2. Click Next, once the parameters have been filled in.
3. Click next on the variable tab as there are no variables to fill in.
4. Once on the Confirm tab, click the deploy button to deploy the Cofense Intelligence Version 3 feed.
5. 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.

A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated

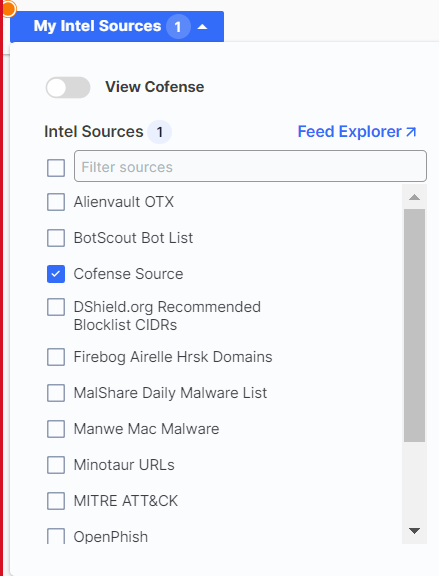
1. The created Job will start and run automatically.

# **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**

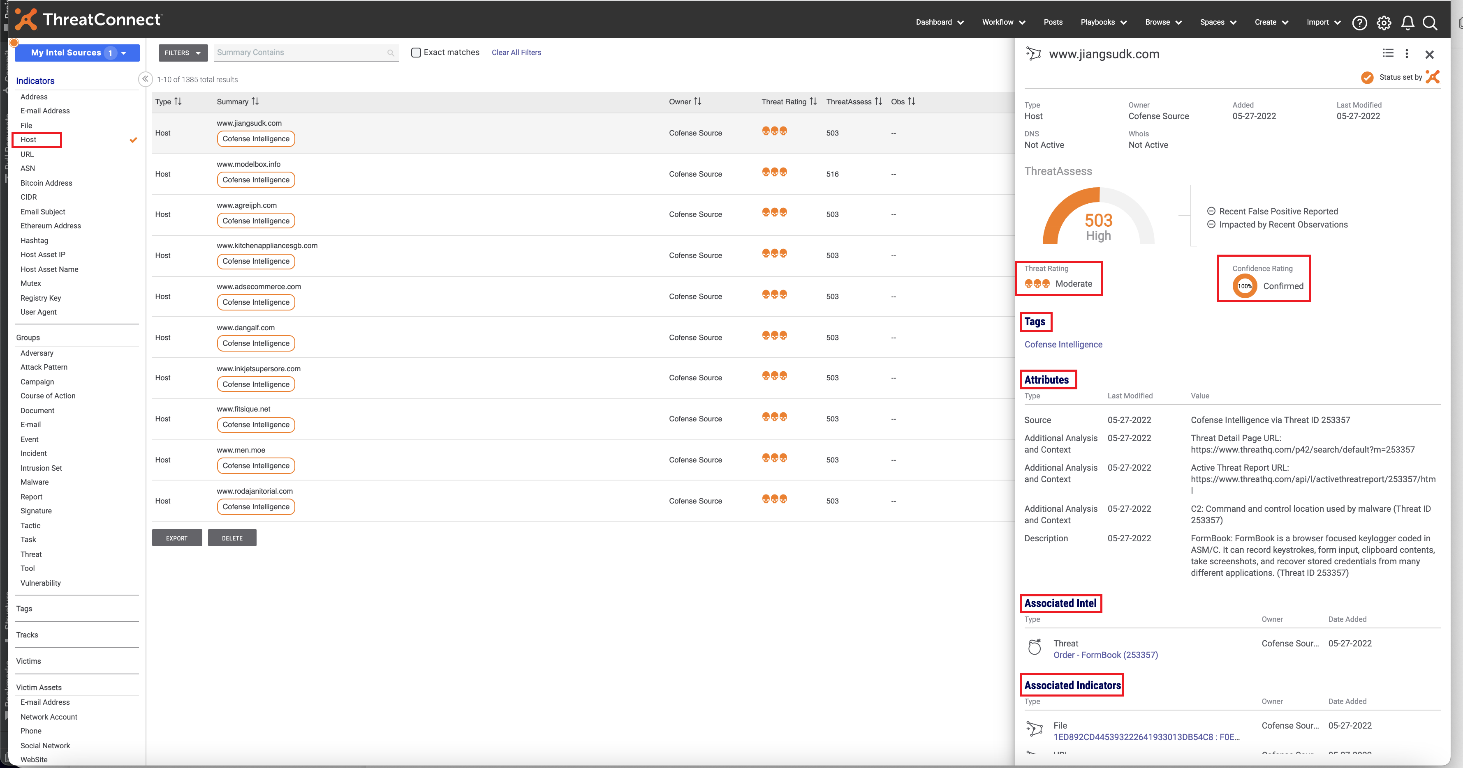
To browse **IP Address Feed** from Cofense Intelligence, select Address Indicator.

Graphical user interface, application, email

Description automatically generated

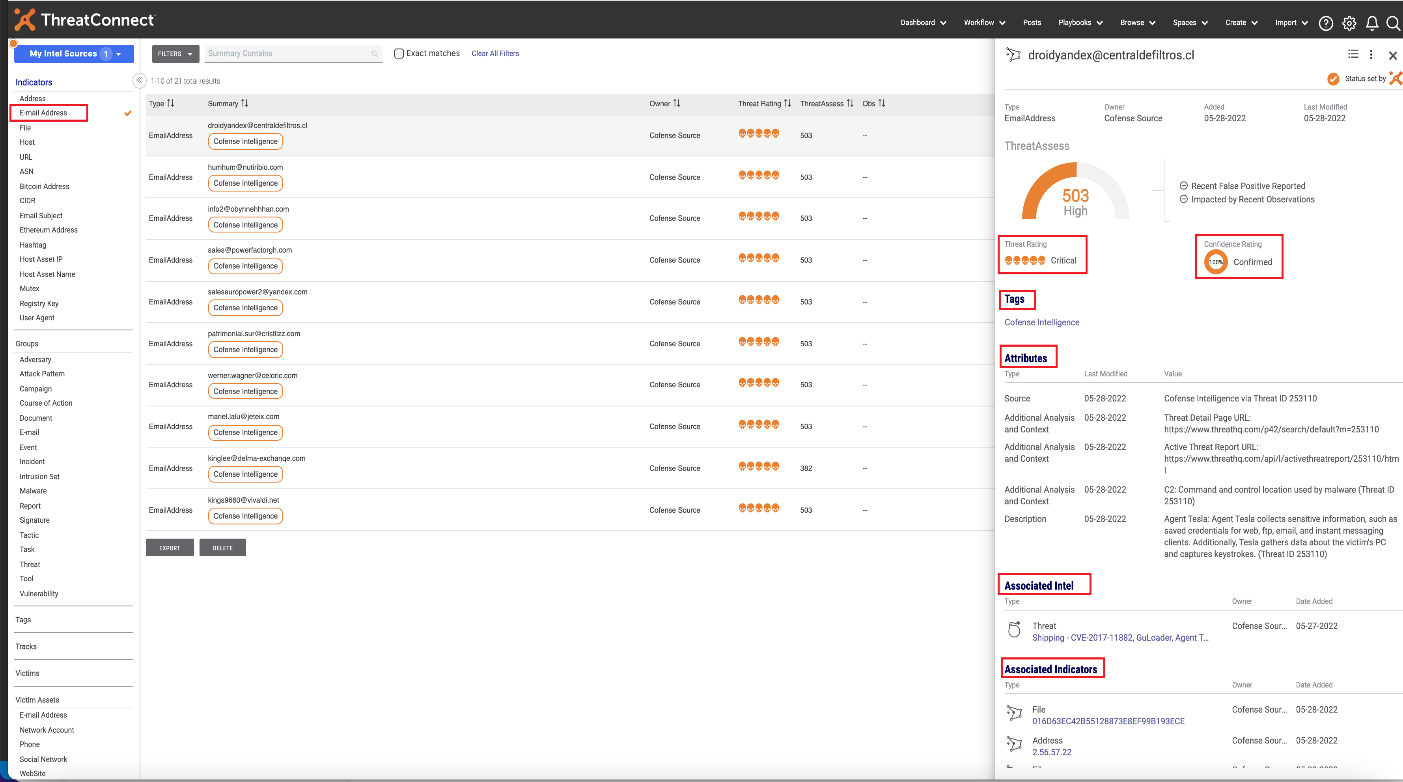
## **Host Feed**

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



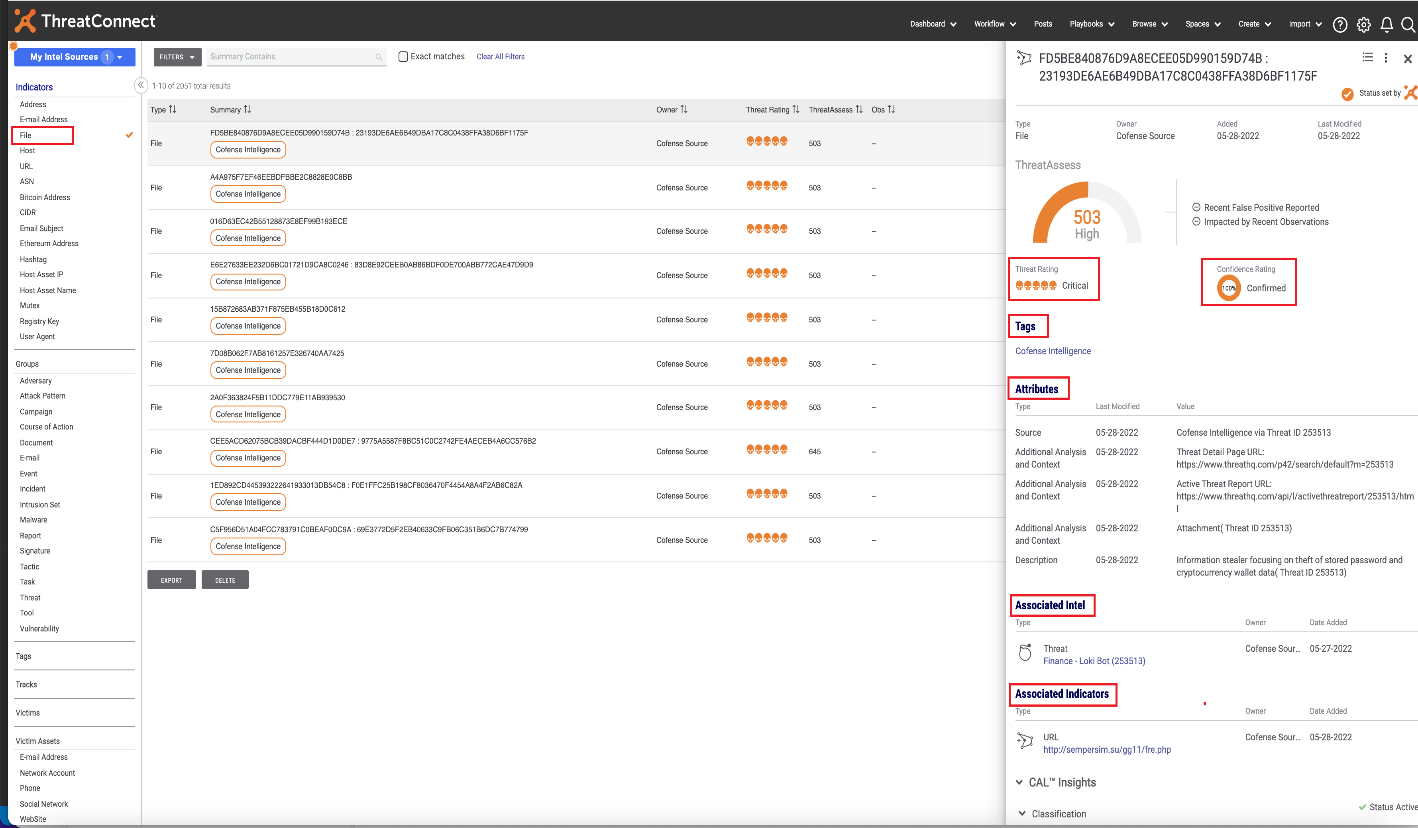
## **Email Address Feed**

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



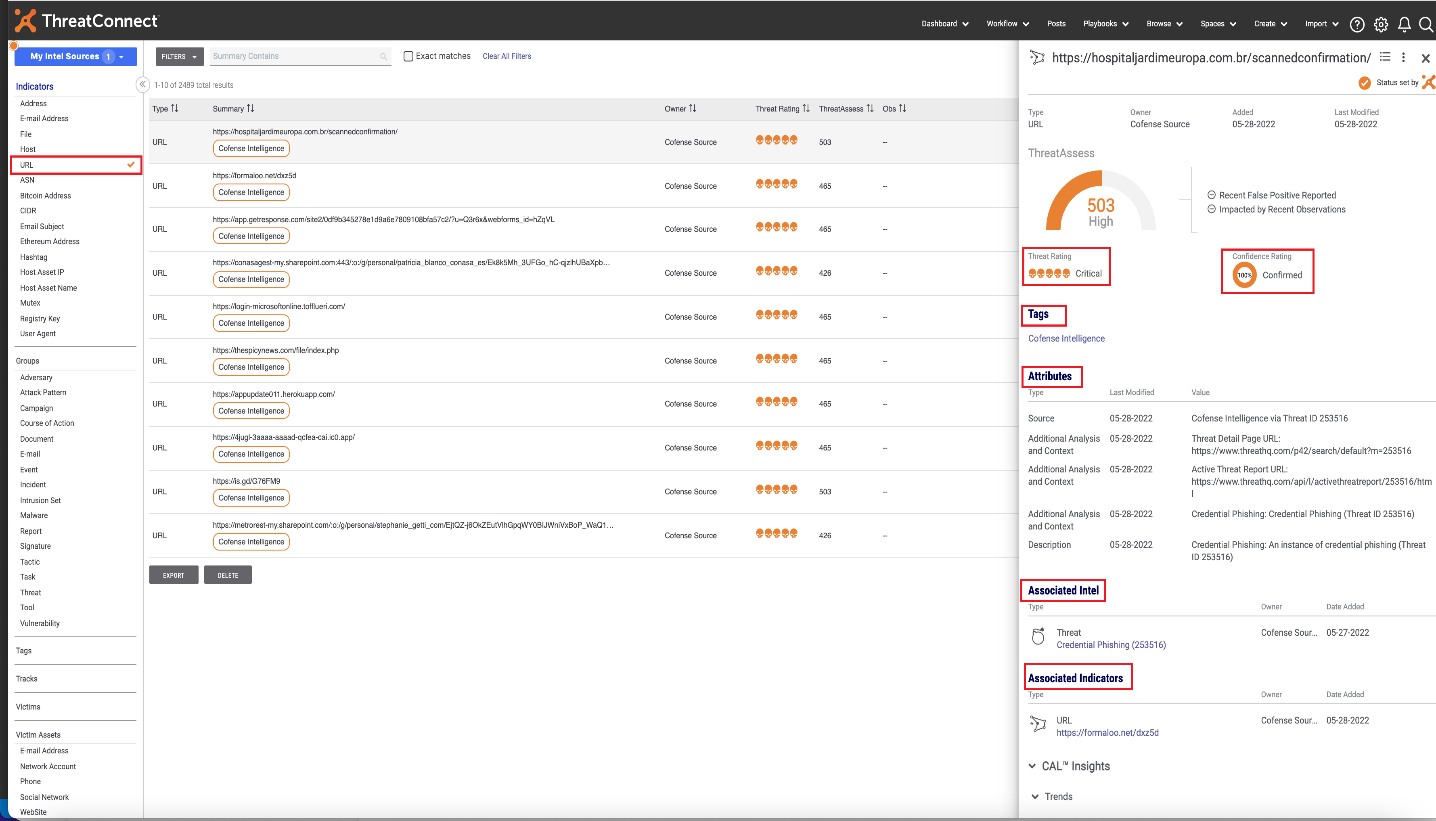
## **File Feed**

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



## **URL Feed**

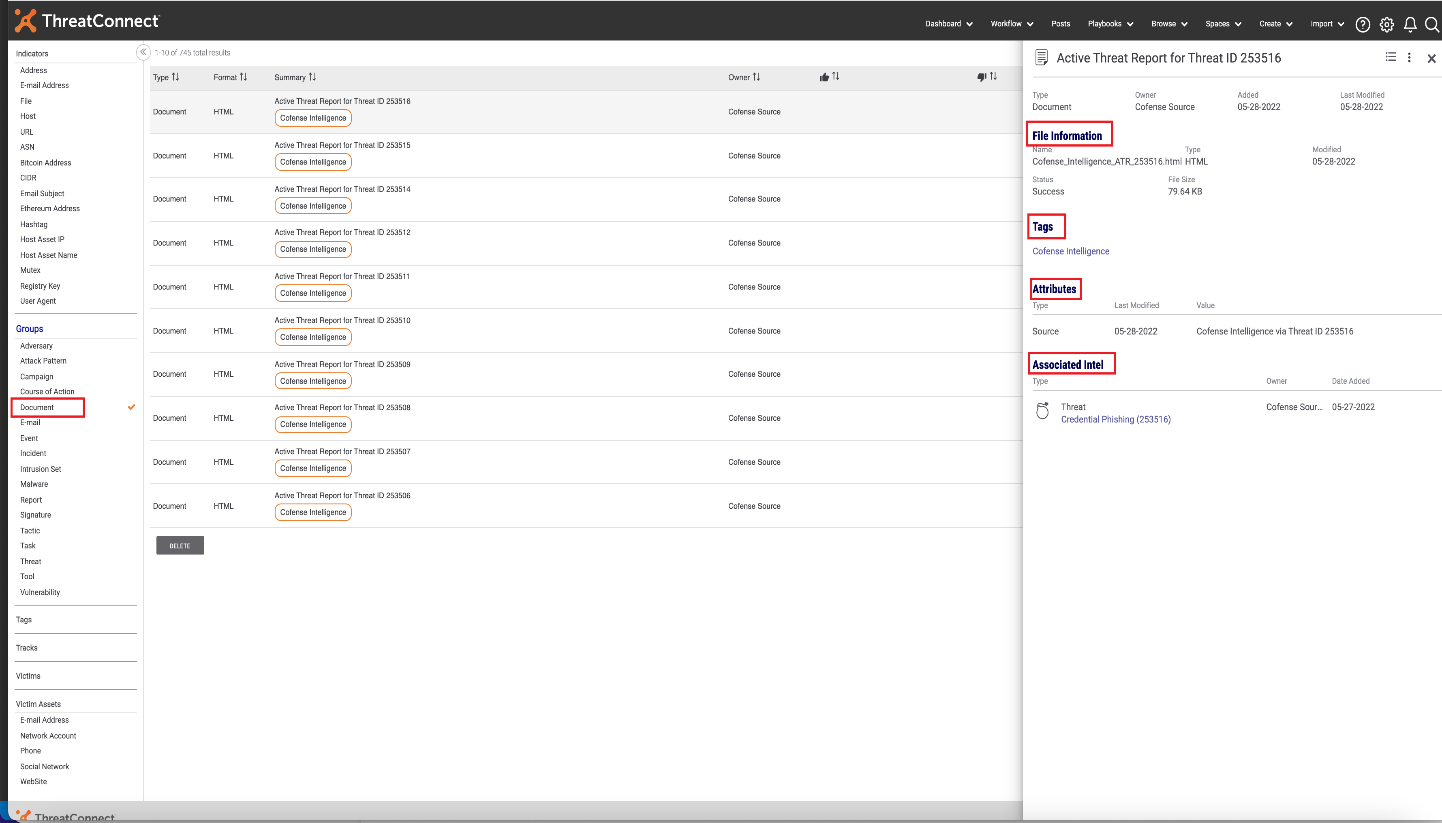
To browse **URL Feed** from Cofense Intelligence, select URL Indicator.



# **Browsing Groups**

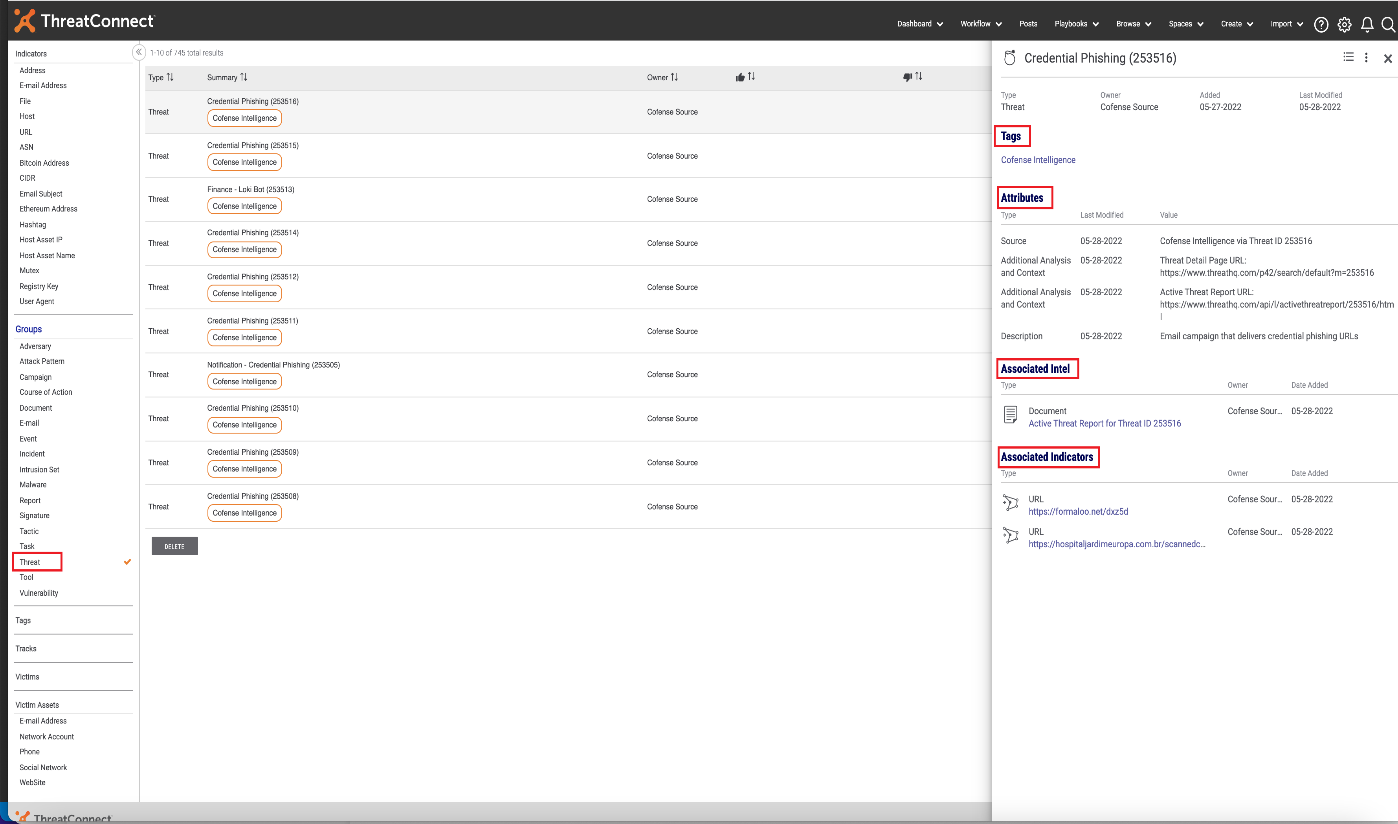
## **Document**

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



## **Threat**

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



# **Browsing Intel Finished Reports**

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

A screenshot of a computer

Description automatically generated

# **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](mailto:support@cofense.com) |