



# ZeroFox ThreatIntel for ThreatConnect Installation and Configuration Guide

**V1.0.7 - May 11, 2022**



# Table of Contents

<b>REQUIREMENTS</b>	<b>4</b>
<b>INSTALLATION</b>	<b>5</b>
<b>CONFIGURATION</b>	<b>6</b>
<b>ZeroFox ThreatIntel App</b>	<b>6</b>
Creating a New Job	6
Step 1: Program	7
Step 2: Parameters	7
Step 3: Schedule	8
Step 4: Output	8
Activating Your Job	9
<b>Data Mapping</b>	<b>10</b>
<b>Data Output</b>	<b>11</b>
<b>SAMPLE DATA</b>	<b>12</b>
<b>FURTHER ASSISTANCE</b>	<b>13</b>



# OVERVIEW

This document describes how to configure the **ZeroFox ThreatIntel App for ThreatConnect**.

The ZeroFox ThreatIntel integration makes up a group of integration solutions with ThreatConnect, including ThreatIntel and Key Incidents integrations.

## Integration Description

This ZeroFox integration with ThreatConnect allows ThreatConnect users to import threat intelligence data along with all of their context from the ZeroFox platform into ThreatConnect.

The ZeroFox ThreatIntel integration is a Threat Intelligence Feed type of integration that can be enabled as a standalone job or using ThreatConnect's Feed Deployer, which adds the feed to your current list of Intelligence sources.

The ZeroFox ThreatIntel app can leverage multiple threat intelligence endpoints to ingest data into the ThreatConnect platform, depending on the user's access and scope within the ZeroFox ThreatIntel API.



# REQUIREMENTS

## ThreatConnect Platform Requirements

On the ThreatConnect side you will need at least one ThreatConnect Platform API user.

## ZeroFox Platform Requirements

To enable this integration you will need access to ZeroFox ThreatIntel data via an API token. This token will be required when creating a new ZeroFox ThreatIntel job on the ThreatConnect platform.

Please contact your ZeroFox representative for assistance with API credentials or access.



# INSTALLATION

## Installing the ZeroFox app on ThreatConnect

For installation instructions, refer to ThreatConnect's Administration Guide (Install an App).

For assistance throughout this process please contact your ThreatConnect customer success representative.

# CONFIGURATION

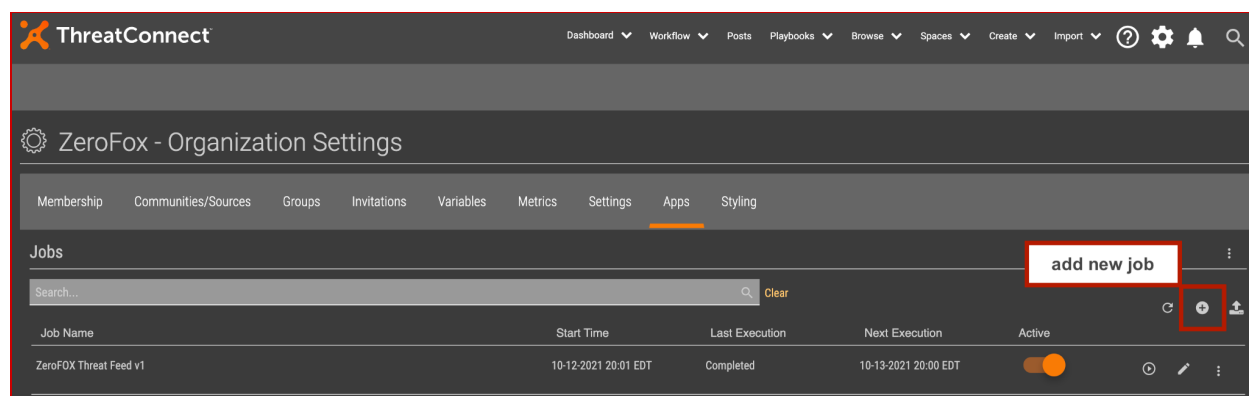
## ZeroFox ThreatIntel App

Once the ZeroFox ThreatIntel App has been installed, the integration can be enabled as a standalone job or via ThreatConnect's Feed Deployer. This user guide walks you through the process of configuring a standalone job instance. However, the process of adding a new source via the Feed Deployer is relatively similar as it requires the same configurations.

## Creating a New Job

Verify the ZeroFox ThreatIntel app is installed.

From your Organization Settings, under the Apps tab, click + to add a new job.



A pop-up window will appear with a series of steps to create a new job, including job parameters and scheduling options.



## Step 1: Program

Under **Job Name** enter in a name for your new job and under the **Run Program** dropdown menu select “ZeroFox ThreatIntel Feed”.

## Step 2: Parameters

This step allows you to enter specific information required to enable your job.

**Api User:** Select the ThreatConnect API user.

**ThreatConnect Owner:** Select the ThreatConnect owner required for this job. This may be an organization or a feed source already created in your account.

**Log Level:** Select the log level desired for this job (ThreatConnect specific).

**ZeroFox Threat Intelligence API Username:** Enter in the username provided for the ZeroFox ThreatIntel API.

**ZeroFox Threat Intelligence API Password:** Enter in the password provided for the ZeroFox ThreatIntel API.

**Last Run:** Set to “1 day ago” by default on initial run. This field should not be changed.

**ZeroFox Threat Intelligence Endpoint:** Select the endpoints you would like to enable and that you have access to.

**ZeroFox Debug Mode:** This feature allows you to enable ZeroFox Debug Mode. When left on, the app will only ingest a small amount of data to limit the app run time (specially helpful for testing purposes).

**ZeroFox Domain for Compromised Credentials:** Domain name filtering for the compromised credentials data feed.



### Step 3: Schedule

Here you will enable scheduling options for your new job.

Suggested schedule setting for the ZeroFox ThreatIntel app is **daily** at any desired time.

By default, the ZeroFox app fetches data within the last 24 hours for every run.

ThreatConnect

Add Job

1 Program 2 Parameters 3 Schedule 4 Output

Scheduled job timezone "America/New\_York"

Schedule: Daily

At: 22:00

Every: 1 hour hour between: 10:00 PM and: Midnight

ThreatConnect

Add Job

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

### Step 4: Output

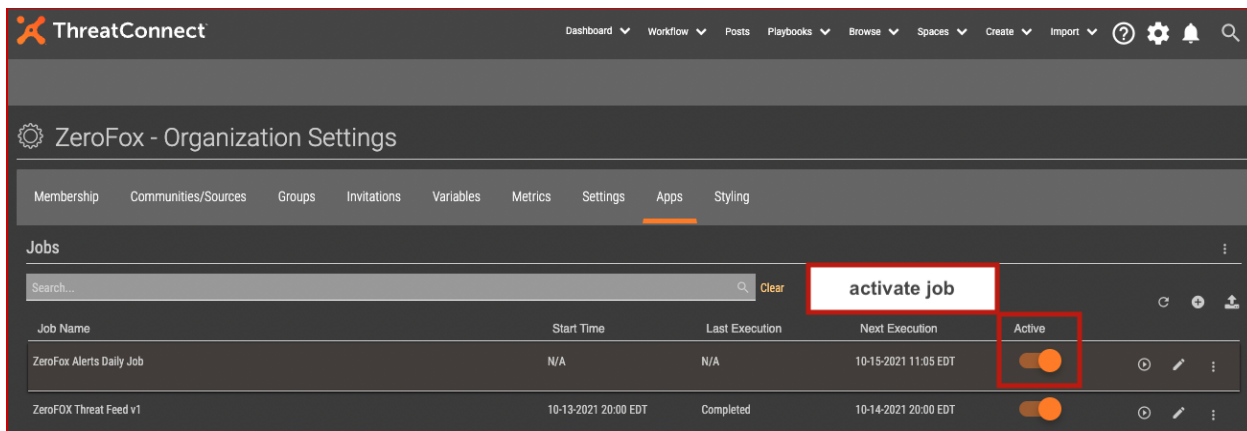
This step allows you to enable notifications that will be triggered by job results: Success, Partial Failure, or Failure. You can choose to include log files with the notification email.

When you are ready to continue, click **Save**.



## Activating Your Job

To activate your new job, within the Apps tab, click on the **“Active”** slider of the required job. The job will run on the next scheduled time as shown under **“Next Execution”** and it will look for ThreatIntel that occurred in the past 24 hours.



ThreatConnect







ZeroFox - Organization Settings

Membership Communities/Sources Groups Invitations Variables Metrics Settings **Apps** Styling

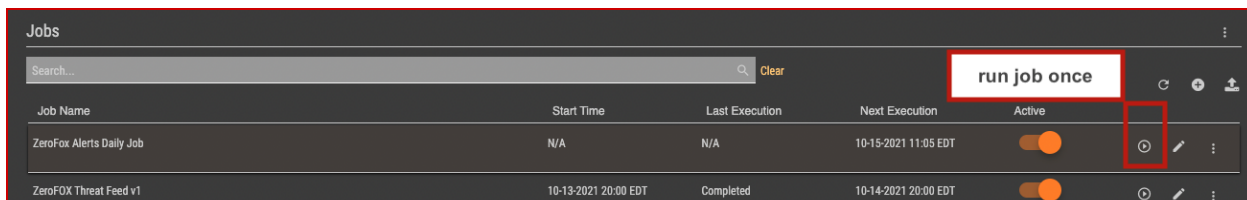
**Jobs**

Search... Clear

activate job

Job Name	Start Time	Last Execution	Next Execution	Active	
ZeroFox Alerts Daily Job	N/A	N/A	10-15-2021 11:05 EDT	<input checked="" type="checkbox"/>	  
ZeroFOX Threat Feed v1	10-13-2021 20:00 EDT	Completed	10-14-2021 20:00 EDT	<input checked="" type="checkbox"/>	  







If you would like to run the job manually, you may start it by clicking on the **“Play”** button of the required job. This action will also look for ThreatIntel that occurred in the last 24 hours.



**Jobs**

Search... Clear

run job once

Job Name	Start Time	Last Execution	Next Execution	Active	
ZeroFox Alerts Daily Job	N/A	N/A	10-15-2021 11:05 EDT	<input checked="" type="checkbox"/>	  
ZeroFOX Threat Feed v1	10-13-2021 20:00 EDT	Completed	10-14-2021 20:00 EDT	<input checked="" type="checkbox"/>	  

## Data Mapping

Below are ZeroFox CTI data objects mapped to ThreatConnect fields. Each Threat Intelligence endpoint will map to a ThreatConnect group or indicator depending on its most closely matched representation.

BOTNET			
ZeroFox Field	ThreatConnect Field	Possible Value Examples	ThreatConnect Group
ip_address	Description	"101.18.80.96"	Threat
listed_at	External Date Created	"2022-04-05T15:55:53Z"	
bot_name	Description	"andromeda"	

DISRUPTION			
ZeroFox Field	ThreatConnect Field	Possible Value Examples	ThreatConnect Group
url	Description	"hxxp://micro-strategy.io"	Threat
fqdn	Additional Analysis and Context	"micro-strategy.io"	
ip	Additional Analysis and Context	"185.186.52.238"	
host	Additional Analysis and Context	"GENIUS-GUARD Genius Guard, GB"	
registrar	Additional Analysis and Context	"Registrar of domain names REG.RU LLC"	
threat_type	Threat Type	"Trademark"	
http_status	Additional Analysis and Context	200	
asn	Additional Analysis and Context	16509	
iana	Additional Analysis and Context	1606	
created_at	External Date Created	"2021-08-11T01:18:16.658914Z"	
updated_at	External Date Last Modified	"2021-08-11T01:18:16.658914Z"	
category	Description	"domains"	
network	Description	"domains"	

EXPLOITS			
ZeroFox Field	ThreatConnect Field	Possible Value Examples	ThreatConnect Group
created_at	External Date Created	"2021-08-11T01:18:16.658914Z"	Vulnerability
cve	Description	"CVE-2017-5754"	
url	Description	"https://github.com/ionescu007/SpecuCheck"	
exploit	Additional Analysis and Context	"/*++\r\n\r\nCopyright (c) Alex Ionescu. All rights reserved.\r\n\r\nModule Name:\r\n\r\n\r\n"	

VULNERABILITIES			
ZeroFox Field	ThreatConnect Field	Possible Value Examples	ThreatConnect Group
description	Description	"CWD ~root command in ftpd allows root access."	Vulnerability
created_at	External Date Created	"2021-08-11T01:18:16.658914Z"	
updated_at	External Date Last Modified	"2021-08-11T01:18:16.658914Z"	
cve	Description	"CVE-2017-5754"	

C2 DOMAINS			
ZeroFox Field	ThreatConnect Field	Possible Value Examples	ThreatConnect Indicator
domain	Host	https://bl1we4t.xyz/	Host
port	Description	80	
tags	Tags	"evasion, persistence"	
ip_addresses	Additional Analysis and Context	"101.18.80.96"	
created_at	External Date Created	"2021-08-11T01:18:16.658914Z"	
updated_at	External Date Last Modified	"2021-08-11T01:18:16.658914Z"	

PHISHING			
ZeroFox Field	ThreatConnect Field	Possible Value Examples	ThreatConnect Group

scanned	Source Date Time	"1970-01-19T19:41:27.989000Z"	Campaign
domain	Description	"hutsjwt.com"	
url	Description	"https://hutsjwt.com/css/mbt"	
cert	Additional Analysis and Context	"authority": "cPanel, Inc.", "Fingerprint": "871B3BD9A98E83573B8368DFDB09629 D4E1777BB", "issued": "2021-05-09T00:00:00Z"	
host	Additional Analysis and Context	"ip": "164.138.221.136", "asn": 201200, "geo": "BG"	

MALWARE			
ZeroFox Field	ThreatConnect Field	Possible Value Examples	ThreatConnect Group
created_at	External Date Created	"2021-04-22T17:40:10Z"	Malware
family	Additional Analysis and Context	"family": ["dcrat", "fickerstealer", "redline"]	
md5	Description	563107b1df2a00f4ec868acd9e08a205	
sha1	Description	9cb9c91d66292f5317aa50d92e38834861 e9c9b7	
sha256	Description	bf2bd257dde4921ce83c7c1303f9f81 e53c2775d3c373ced482b22eb8a9	
sha512	Description	99a8d247fa435c4cd95be7bc64c7dd6e38 2371f3a3c160aac3995fd705e4fd3f6622c2 3784a4ae3457c87536347d15eda3f08aa6 16450778a99376df540d74d1	
tags	Tags	"family:dcrat"	
c2	Additional Analysis and Context	"sodaandcoke.top:80"	
botnet	Additional Analysis and Context	"gamut"	

RANSOMWARE			
ZeroFox Field	ThreatConnect Field	Possible Value Examples	ThreatConnect Group
created_at	External Date Created	"2021-04-22T17:40:10Z"	Malware
md5	Description	563107b1df2a00f4ec868acd9e08a205	
sha1	Description	9cb9c91d66292f5317aa50d92e38834861 e9c9b7	

sha256	Description	bf2bd257dde4921ce83c7c1303fafe7f9f81e53c2775d3c373ced482b22eb8a9	
sha512	Description	99a8d247fa435c4cd95be7bc64c7dd6e382371f3a3c160aac3995fd705e4fd3f6622c23784a4ae3457c87536347d15eda3f08aa616450778a99376df540d74d1	
ransom_note	Additional Analysis and Context	"==== Welcome. HB-Technik. ====-\r\n\r\n[+] Whats Happen? [+]\r\n\r\nYour files are encrypted, and currently unavailable."	
ransomware_name	Additional Analysis and Context	"sodinokibi"	
tags	Tags	"tags": ["family:sodinokibi", "persistence", "ransomware"]	

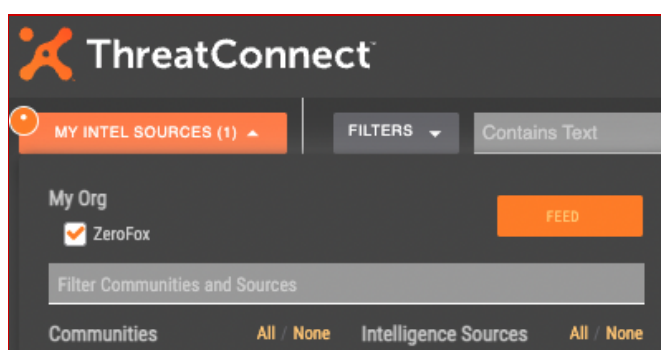
EMAIL ADDRESS			
ZeroFox Field	ThreatConnect Field	Possible Value Examples	ThreatConnect Group
created_at	External Date Created	"2021-04-22T17:40:10Z"	Email
email	Description	"Az@gcmce.com"	
domain	Description	"https://gcmce.com/"	
tags	Tags	"family:agenttesla"	

EMAIL ADDRESS			
ZeroFox Field	ThreatConnect Field	Possible Value Examples	ThreatConnect Group
created_at	External Date Created	"2021-04-22T17:40:10Z"	Compromised Credentials
domain	Description	"zerofox.com"	
email	Description	"jsmith@zerofox.com"	
username	Description	"jsmith"	
breach_name	Description	"KnifeCenter Data Breach"	
impacted_domain	Description	"knifecenter.com"	

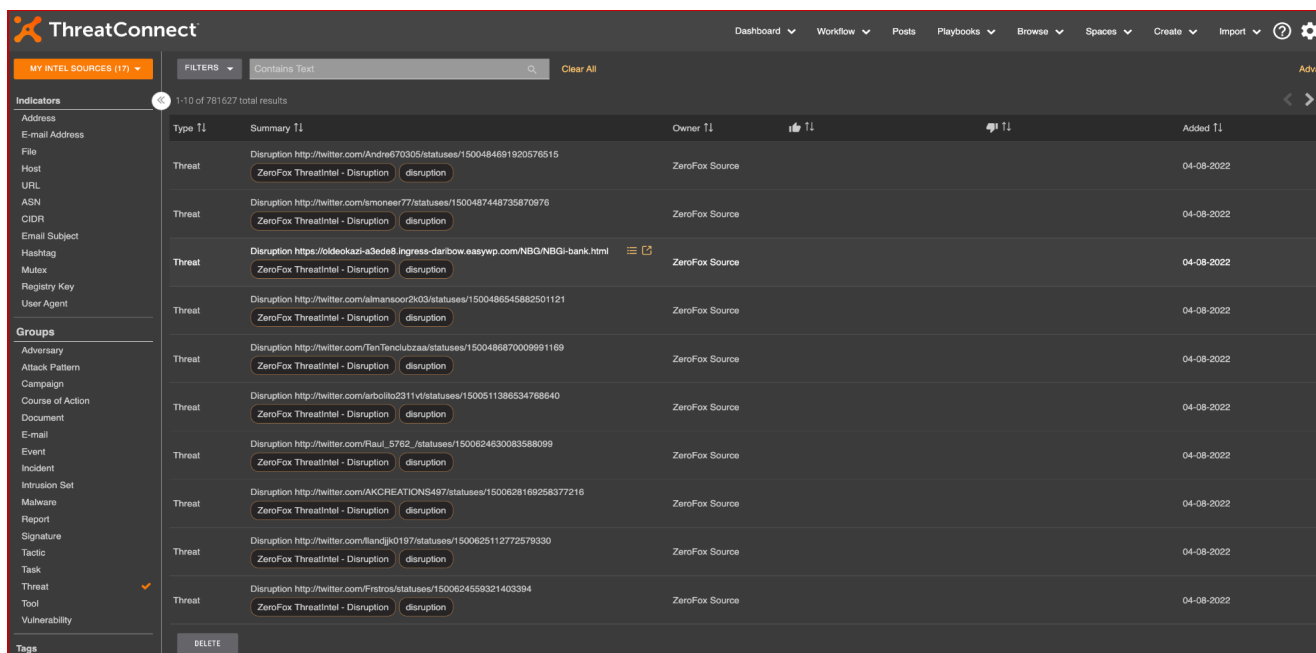
# Data Output

## ThreatConnect Platform

To browse through the data that has been collected and added to the ThreatConnect platform, click the **Browse>Groups** option on the main menu and under the **"My Intel Sources"** dropdown menu select the organization or source where the ZeroFox incidents were added to.



You will see a list of ZeroFox ThreatIntel data added as groups or indicators:



Type TL	Summary TL	Owner TL	TL	TL	Added TL
Threat	Disruption http://twitter.com/Andre670305/statuses/1500484891920576515 ZeroFox ThreatIntel - Disruption disruption	ZeroFox Source			04-08-2022
Threat	Disruption http://twitter.com/moneer77/statuses/1500487448735870976 ZeroFox ThreatIntel - Disruption disruption	ZeroFox Source			04-08-2022
Threat	Disruption https://oldeokazi-a3ede8.ingress-daribow.easyp.com/NBG/NBG-bank.html ZeroFox ThreatIntel - Disruption disruption	ZeroFox Source			04-08-2022
Threat	Disruption http://twitter.com/almansoor2k03/statuses/1500486545882501121 ZeroFox ThreatIntel - Disruption disruption	ZeroFox Source			04-08-2022
Threat	Disruption http://twitter.com/TenTencubzaa/statuses/1500486870009991169 ZeroFox ThreatIntel - Disruption disruption	ZeroFox Source			04-08-2022
Threat	Disruption http://twitter.com/arbolto2311v/statuses/1500511386534768640 ZeroFox ThreatIntel - Disruption disruption	ZeroFox Source			04-08-2022
Threat	Disruption http://twitter.com/Raul_5762/statuses/1500624630083588099 ZeroFox ThreatIntel - Disruption disruption	ZeroFox Source			04-08-2022
Threat	Disruption http://twitter.com/AKCREATIONS497/statuses/1500628169258377216 ZeroFox ThreatIntel - Disruption disruption	ZeroFox Source			04-08-2022
Threat	Disruption http://twitter.com/landjk0197/statuses/150062511272579330 ZeroFox ThreatIntel - Disruption disruption	ZeroFox Source			04-08-2022
Threat	Disruption http://twitter.com/Frstros/statuses/1500624559321403394 ZeroFox ThreatIntel - Disruption disruption	ZeroFox Source			04-08-2022



## FURTHER ASSISTANCE

If you have any questions about this integration or document, please contact [integration-support@zerofox.com](mailto:integration-support@zerofox.com)