



# ZeroFox Domains for ThreatConnect

## Installation and Configuration Guide

V1.0.1 - Dec 21, 2021



# Table of Contents

<b>REQUIREMENTS</b>	<b>4</b>
<b>INSTALLATION</b>	<b>5</b>
<b>CONFIGURATION</b>	<b>6</b>
<b>ZeroFox Alerts 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 Domains App for ThreatConnect**.

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

## Integration Description

This ZeroFox integration with ThreatConnect allows ThreatConnect users to import domain data from the ZeroFox Domain feed into ThreatConnect.

The ZeroFox Domains 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.

ZeroFox Domains are mapped as ThreatConnect Host indicator objects.



# 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 Domains feed via an API token. This token will be required when creating a new ZeroFox Domains 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

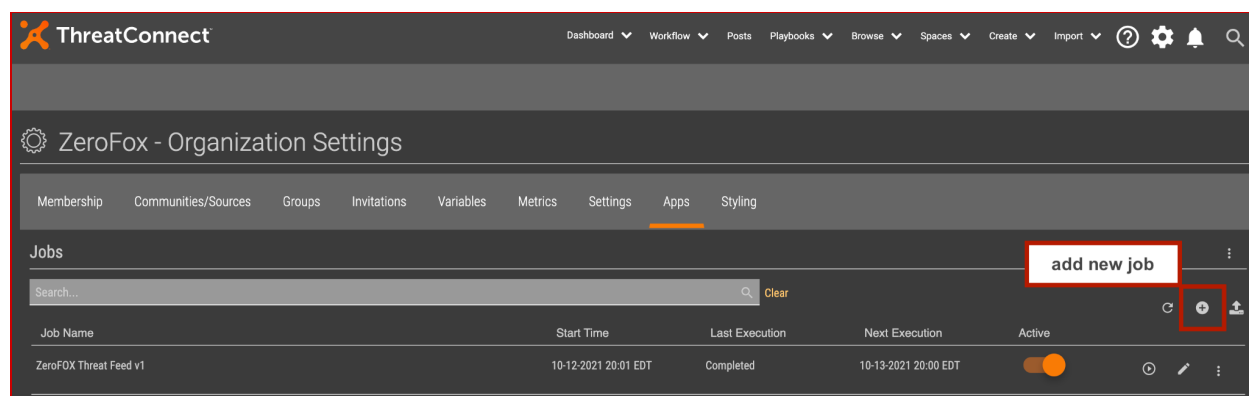
## ZeroFox Alerts App

Once the ZeroFox Domains 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 Alerts app is installed.

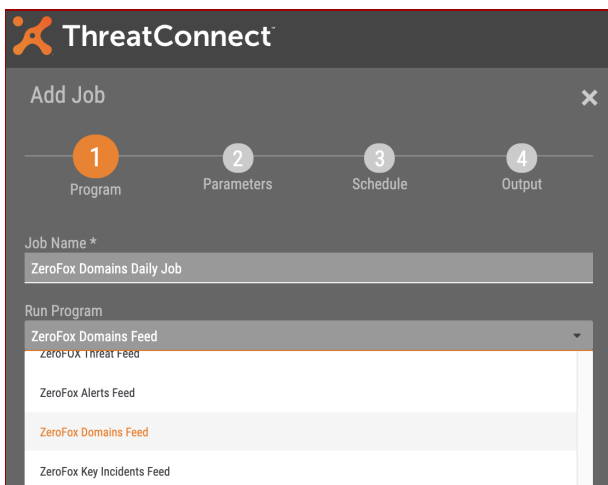
From your Organization Settings, under the Apps tab, click + to add a new job.



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

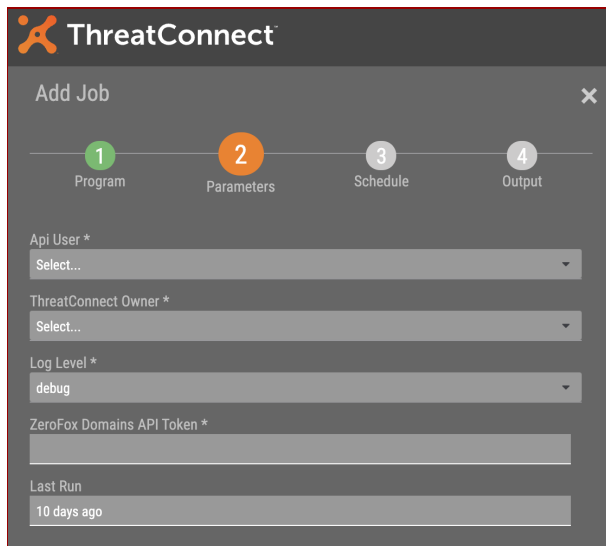
## Step 1: Program

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

**ZeroFox Domains API Token:** Enter in the API key provided for ZeroFox Domains Feed.

**Last Run:** Upon your job's initial setup, this field will be set to “10 Days ago” to look for historical data. On subsequent runs, this field will be updated automatically to the date and time when the app last ran.

**Note:** Do not change the “**Last Run**” field. If you would like the app to not look for historical data on your initial job run, you may change this field to “**1 day ago**” to check for alerts in the last 24 hours instead, on your initial run.



### Step 3: Schedule

Here you will enable scheduling options for your new job.

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

By default, the ZeroFox Domains app fetches data within the last 24 hours after the initial 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

CANCEL PREVIOUS SAVE

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

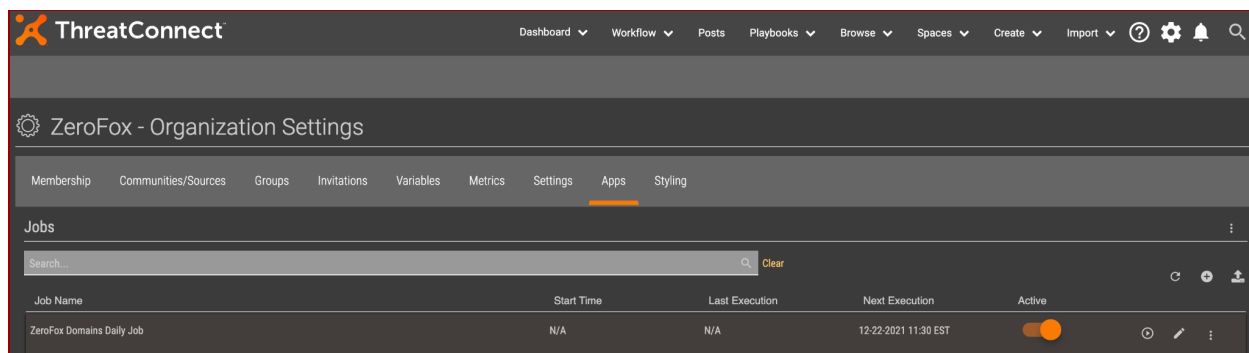
This step allows you to enable notifications that will be triggered by job results: Success, Partial Failure, or Failure. You can choose to include log files with the notification email.

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



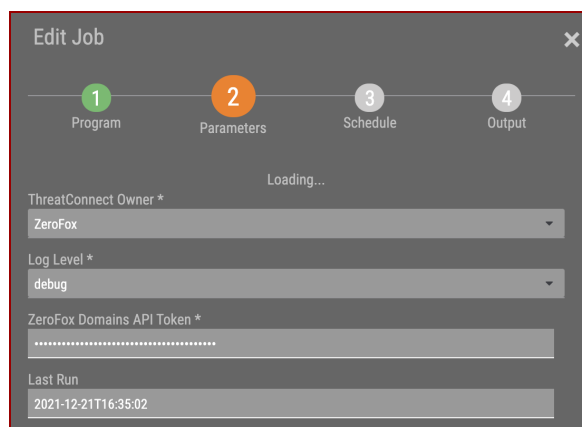
## Activating Your Job

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 alerts that occurred in the last 10 days, since this would be the first run.



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 alerts that occurred in the last 10 days.

After your job’s initial run, its **“Last Run”** field will be updated to the time and date when the job ran. On future runs your job will look for alerts that occurred in the last 24 hours.



## Data Mapping

The table below outlines the data objects mapped between the ZeroFox Domains Feed and the ThreatConnect platform:

ZeroFox Field	ThreatConnect Field	Examples
Domain	Summary	"augen-praxisklinik-rostock.de"
Tags	Tag	"spyware", "trojan"
Domain ID	External ID	"2369"
IP Addresses	Additional Analysis and Context	85.13.155.177
Updated At	External Date Last Modified	2021-09-20T14:38:02Z
Created At	External Date Created	2021-09-20T14:38:02Z

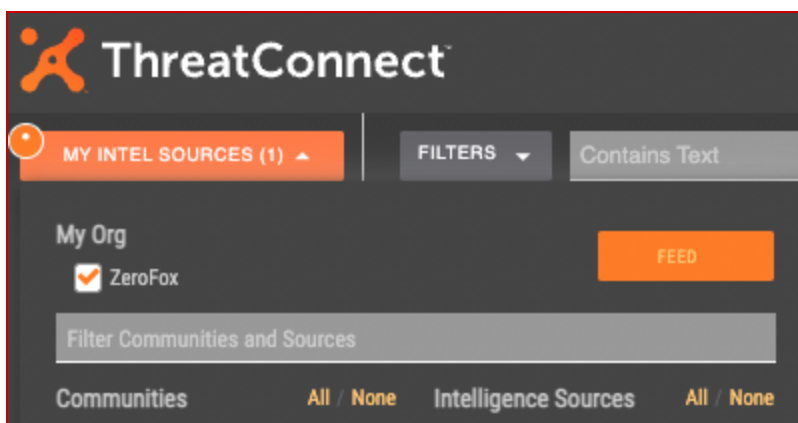
Additional information about each domain is displayed in the **Description** field:

ZeroFox Fields	ThreatConnect Field	Example
Domain ID Domain Port	Description	<b>Domain ID:</b> 2369 <b>Domain:</b> https://augen-praxisklinik-rostock.de <b>Port:</b> 80

# Data Output

## ThreatConnect Platform

To browse through the data that has been ingested 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 domains added as host indicators to the ThreatConnect platform:

ThreatConnect										
<div> <div>MY INTEL SOURCES (1)</div> <div>FILTERS</div> <div>Contains Text</div> <div>Clear All</div> <div>Advanced</div> </div>										
Indicators	1-10 of 259 total results									
Address	Type	Summary	Owner	Threat Rating	ThreatAssess	Obs	F/P	Added	Modified	
E-mail Address	Host	augen-praxisklinik-rostock.de ZeroFox Domains evasion family:sodinokibi +4 more...	ZeroFox Domains	5	--	--	--	12-21-2021	12-21-2021	
File	Host	egobiakita.xyz ZeroFox Domains collection family:lokibot +5 more...	ZeroFox Domains	5	516	--	--	12-18-2021	12-18-2021	
URL	Host	showroomrezamotor.com ZeroFox Domains collection family:lokibot +4 more...	ZeroFox Domains	5	503	--	--	12-18-2021	12-18-2021	
ASN	Host	linm.thebt.xyz ZeroFox Domains family:oski infostealer +2 more...	ZeroFox Domains	5	516	--	--	12-17-2021	12-17-2021	
CIDR	Host	kaminscy.com ZeroFox Domains evasion family:sodinokibi +2 more...	ZeroFox Domains	5	440	--	--	12-17-2021	12-17-2021	
Email Subject	Host	marietteaernoudts.nl ZeroFox Domains evasion family:sodinokibi +2 more...	ZeroFox Domains	5	440	--	--	12-17-2021	12-17-2021	
Hashtag	Host	ligiercenter-sachsen.de ZeroFox Domains evasion family:sodinokibi +2 more...	ZeroFox Domains	5	440	--	--	12-17-2021	12-17-2021	
Mutex										
Registry Key										
User Agent										
Groups										
Adversary										
Attack Pattern										
Campaign										
Course of Action										
Document										
E-mail										
Event										
Incident										

# SAMPLE DATA

FILTERS

Contains text

Clear All

1-10 of 259 total results

Type ↑↓

Summary ↑↓

Host

augen-praxisklinik-rostock.de

ZeroFox Domains evasion family:sodinokibi +4 more...

Host

egobiakita.xyz

ZeroFox Domains collection family:lokibot +5 more...

Host

showroomrezamotor.com

ZeroFox Domains collection family:lokibot +4 more...

Host

linm.thetxt.xyz

ZeroFox Domains family:oski infostealer +2 more...

Host

kaminscy.com

ZeroFox Domains evasion family:sodinokibi +2 more...

Host

marietteaernoudts.nl

ZeroFox Domains evasion family:sodinokibi +2 more...

Host

ligiercenter-sachsen.de

ZeroFox Domains evasion family:sodinokibi +2 more...

Host

geisterradler.de

ligiercenter-sachsen.de

Status set by CAL

Domain ID: 2343

Domain: ligiercenter-sachsen.de

Port: 80

Type

Host

Owner

ZeroFox Domains

Added

12-17-2021

Last Modified

12-17-2021

DNS

Not Active

Whois

Not Active

ThreatAssess

440

Medium

Recent False Positive Reported

Impacted by Recent Observations

Threat Rating

Critical

Confidence Rating

100% Confirmed

Tags

family:sodinokibi ransomware evasion persistence

FILTERS

Contains Text

Clear All

0 of 259 total results

e ↑↓

Summary ↑↓

t

augen-praxisklinik-rostock.de

ZeroFox Domains evasion family:sodinokibi +4 more...

t

egobiakita.xyz

ZeroFox Domains collection family:lokibot +5 more...

t

showroomrezamotor.com

ZeroFox Domains collection family:lokibot +4 more...

t

linm.thetxt.xyz

ZeroFox Domains family:oski infostealer +2 more...

t

kaminscy.com

ZeroFox Domains evasion family:sodinokibi +2 more...

t

marietteaernoudts.nl

ZeroFox Domains evasion family:sodinokibi +2 more...

t

ligiercenter-sachsen.de

ZeroFox Domains evasion family:sodinokibi +2 more...

augen-praxisklinik-rostock.de

Status set by CAL

Attributes

Type	Last Modified	Value
Additional Analysis and Context	12-21-2021	IP Addresses: 85.13.155.177 213.133.104.49 2a01:4f8:d0a:274e::2
External ID	12-21-2021	2369
External Date Last Modified	12-21-2021	2021-12-21T08:26:27Z
External Date Created	12-21-2021	2021-12-21T08:26:27Z

CAL™ Insights

Trends

7 days

30 days

Daily False Positives

Daily Impressions

Daily Observations



## FURTHER ASSISTANCE

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