



ZeroFox Key Incidents for ThreatConnect

Installation and Configuration Guide

V1.0.1 - Oct 15, 2021



Table of Contents

REQUIREMENTS	4
INSTALLATION	5
CONFIGURATION	6
ZeroFox Key Incidents App	6
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
Data Mapping	10
Data Output	11
SAMPLE DATA	12
FURTHER ASSISTANCE	13



OVERVIEW

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

Integration Description

This ZeroFox integration with ThreatConnect allows ThreatConnect users to import Key Incidents along with all of their context from the ZeroFox platform into ThreatConnect.

The ZeroFox Key Incidents 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.

Through each integration job, ZeroFox Key Incidents are imported as Incident Groups to the ThreatConnect platform.



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 Key Incidents data via an API token. This token will be required when creating a new ZeroFox Key Incidents job on the ThreatConnect platform.

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



INSTALLATION

Installing the ZeroFox Key Incidents 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

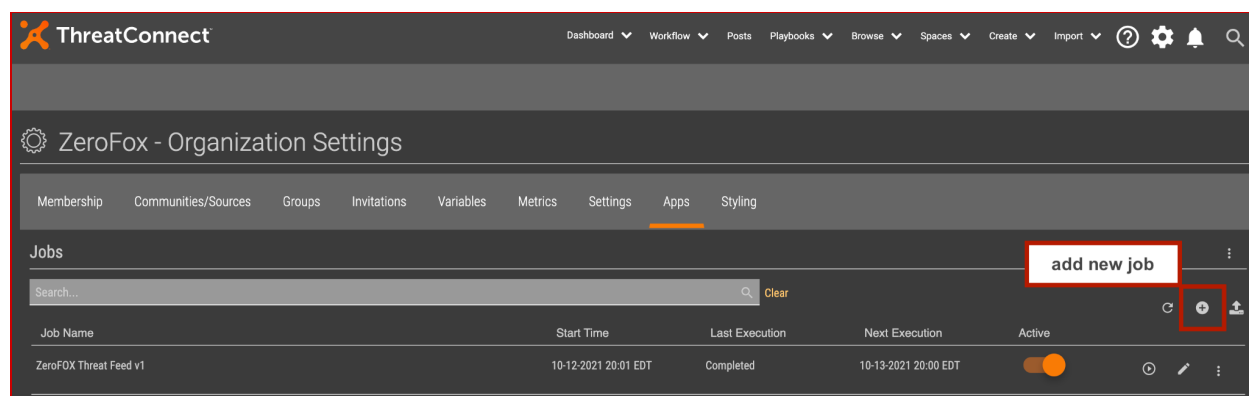
ZeroFox Key Incidents App

Once the ZeroFox Key Incidents 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 Key Incidents 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 Key Incidents 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 Key Incidents API Token: Enter in the API key provided for ZeroFox Key Incidents.

Last Run: This is set to “24 hours ago” by default on your job's initial setup. After your job runs for the first time, this field will automatically update to the time and date the job ran and it will continue looking for data within the last 24 hours on any scheduled run.

Note: Do not change this field's value.



Step 3: Schedule

Here you will enable scheduling options for your new job.

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

By default, the ZeroFox Key Incidents app fetches data within the last 24 hours on all runs.

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

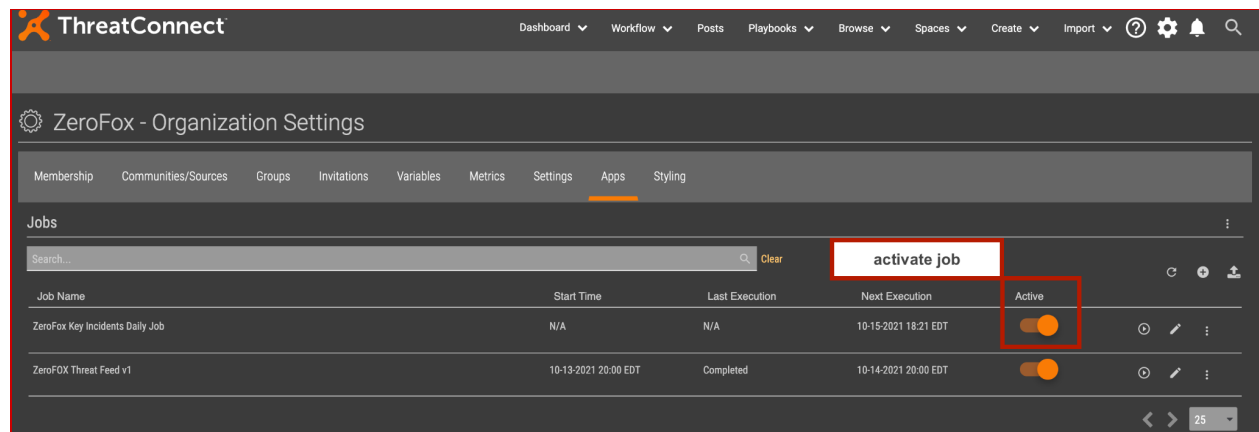
This step allows you to enable notifications that will be triggered by job results: Success, Partial Failure, or Failure. You can choose to include log files with the notification email.

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

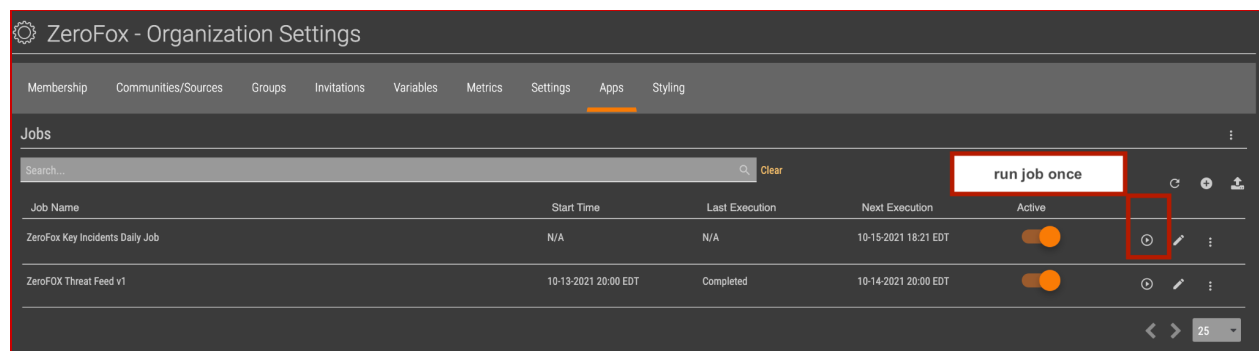


Activating Your Job

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"**.



If you would like to run the job manually, you may start it by clicking on the **"Play"** button of the required job.



Data Mapping

The table below outlines the data objects mapped between the ZeroFox Key Incidents solution and the ThreatConnect platform:

ZeroFox Field	ThreatConnect Field	Examples
Incident ID - Headline	Summary	"CI-33193 - Sydney, Australia: Freedom Day when restrictions lifted on October 11, 2021"
Source	Tag	"Web"
Host	Tag	"www.twitter.com"
Custom Tag	Tag	"Key Incident"
Incident ID	External ID	CI-33193
Tags	Additional Analysis and Context	"Imported, Saved Search, Physical Security, Event Site, Unknown, Analyzed"
Target Type	Additional Analysis and Context	"Company Name, Key Person"
Threat Type	Additional Analysis and Context	"Negative Commentary"
URL	Source	"https://twitter.com/jcostantini/status/1442933438735007746"
Created on	External Date Created	2021-09-20T14:38:02Z
Risk Level	Threat Level	None, Low, Medium, High, Critical

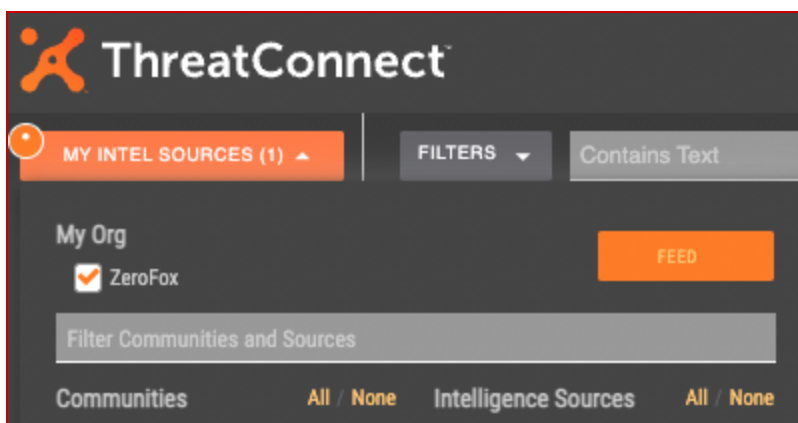
Additional contextual information about each incident will be displayed in the **Description** field:

ZeroFox Fields	ThreatConnect Field	Example
Incident ID Incident Type Headline Analysis	Description	Incident ID: CI-7693 Incident Type: Not Available Headline: Nestle: Github Mention Analysis: A Github posting has been identified containing a Nestle mention. After reviewing the incident and its context, it was sent to your attention.

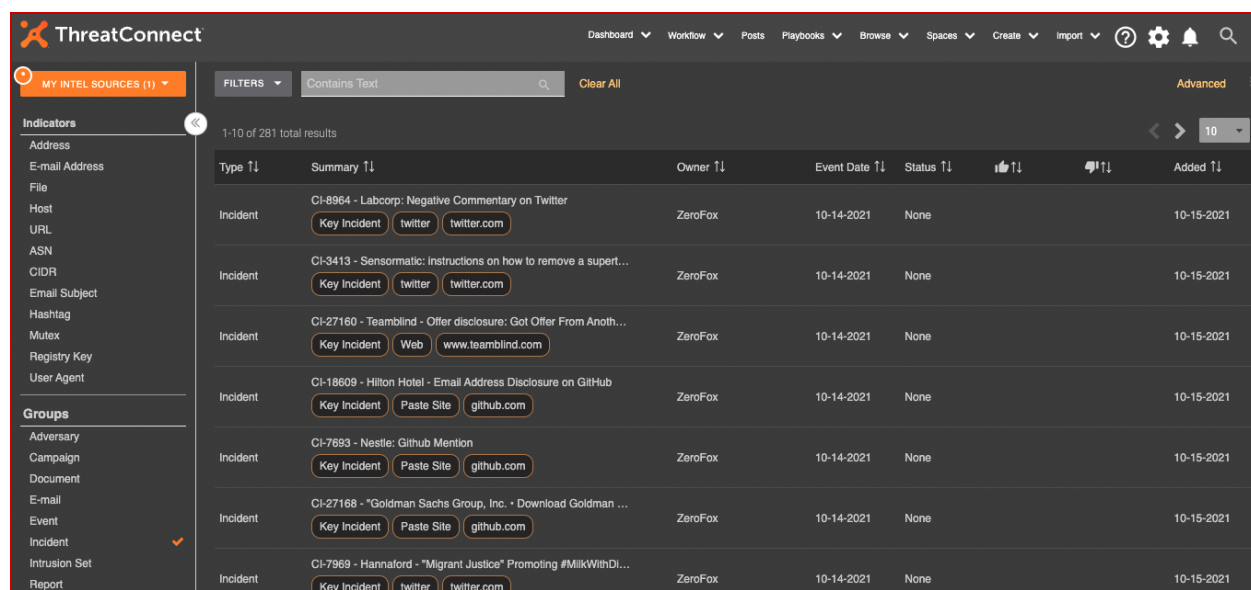
Data Output

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 Key Incidents added as incident groups:



Type	Summary	Owner	Event Date	Status	Added
Incident	Ci-8964 - Labcorp: Negative Commentary on Twitter Key Incident twitter twitter.com	ZeroFox	10-14-2021	None	10-15-2021
Incident	Ci-3413 - Sensormatic: Instructions on how to remove a supert... Key Incident twitter twitter.com	ZeroFox	10-14-2021	None	10-15-2021
Incident	Ci-27160 - Teambind - Offer disclosure: Got Offer From Anoth... Key Incident Web www.teamblind.com	ZeroFox	10-14-2021	None	10-15-2021
Incident	Ci-18609 - Hilton Hotel - Email Address Disclosure on GitHub Key Incident Paste Site github.com	ZeroFox	10-14-2021	None	10-15-2021
Incident	Ci-7693 - Nestle: Github Mention Key Incident Paste Site github.com	ZeroFox	10-14-2021	None	10-15-2021
Incident	Ci-27168 - "Goldman Sachs Group, Inc." Download Goldman ... Key Incident Paste Site github.com	ZeroFox	10-14-2021	None	10-15-2021
Incident	Ci-7969 - Hannaford - "Migrant Justice" Promoting #MilkWithDi... Key Incident twitter twitter.com	ZeroFox	10-14-2021	None	10-15-2021



SAMPLE DATA

FILTERS

Contains Text

Clear All

1-10 of 281 total results

Type TL	Summary TL	Owner TL	Event Date TL
Incident	CI-8964 - Labcorp: Negative Commentary on Twitter Key Incident twitter twitter.com	ZeroFox	10-14-2021
Incident	CI-3413 - Sensomatic: Instructions on how to remove a supertag shared on Twitter Key Incident twitter twitter.com	ZeroFox	10-14-2021
Incident	CI-27160 - Teamblind - Offer disclosure: Got Offer From Another Team In GS Key Incident Web www.teamblind.com	ZeroFox	10-14-2021
Incident	CI-18609 - Hilton Hotel - Email Address Disclosure on Github Key Incident Paste Site github.com	ZeroFox	10-14-2021
Incident	CI-7693 - Nestle: Github Mention Key Incident Paste Site github.com	ZeroFox	10-14-2021
Incident	CI-27168 - "Goldman Sachs Group, Inc." - Download Goldman Sachs vector logo SVG - Logotyp. Key Incident Paste Site github.com	ZeroFox	10-14-2021
Incident	CI-7969 - Hamaford - "Migrant Justice" Promoting #MilkWithDignity Program Key Incident twitter twitter.com	ZeroFox	10-14-2021
Incident	CI-27159 - Teamblind - Offer disclosure: VP Treasury at Dallas Key Incident Web www.teamblind.com	ZeroFox	10-14-2021
Incident	CI-7324 - Continued commentary against Paul Singer over alleged funding of Russia Dossier Key Incident twitter twitter.com	ZeroFox	10-14-2021
Incident	CI-7694 - Nestle: Possible Outage Mention Key Incident twitter twitter.com	ZeroFox	10-14-2021

DELETE

CI-8964 - Labcorp: Negative Commentary on Twitter

Incident ID: CI-8964
Incident Type: Brand Intelligence
Headline: Labcorp: Negative Commentary on Twitter
Analysis: On October 13, 2021, Twitter user @LindseyKarlene posted a tweet containing negative commentary about Labcorp. The user mentioned Labcorp's official Twitter account and explained their dissatisfaction that the Labcorp location they visited only had 1 phlebotomist staffed and that they had to close early.

Type	Owner	Added	Event Date
Incident	ZeroFox	10-15-2021	10-14-2021

Status: None

Tags
[twitter](#)
[twitter.com](#)
[Key Incident](#)

Attributes

Type	Last Modified	Value
External ID	10-15-2021	CI-8964
External Date Created	10-15-2021	2021-10-14T17:48:43Z
Source	10-15-2021	https://twitter.com/LindseyKarlene/status/1448434024532217857
Additional Analysis and Context	10-15-2021	Threat Types: Negative Commentary Target Types: Company Name Tags: Physical Security Package 1, Company Name, Twitter Token Collection, Negative Commentary, Low, Saved Search, Brand Intelligence, Analyzed, Key Incident
Threat Level	10-15-2021	Low

ThreatConnect

Dashboard Workflow Posts Playbooks Browse Spaces Create Import Settings Help

CI-7694 - Nestle: Possible Outage Mention

Q PIVOT DELETE DOWNLOAD PDF

Follow Item

Overview Tasks Activity Associations Sharing Spaces

Description

ZeroFox says:
None
Incident ID: CI-7694
Incident Type:
Headline: Nestle: Possible Outage Mention
Analysis: An October 13, 2021 post by Twitter user (@SplinteredSpace) references a possible outage affecting the Nespresso website. This has been brought to Nestle's attention for situational awareness purposes.

Security Labels
Choose Security Labels

Attributes
External ID
None
CI-7694
Last Updated: 10-15-2021 11:20 EDT by ZeroFox
External Date Created
None
2021-10-14T18:16:19Z
Last Updated: 10-15-2021 11:20 EDT by ZeroFox

Associations

Associated Groups (0)
Associated Indicators (0)
Associated Victim Assets (0)
Associated Artifacts (0)
Associated Cases (0)
Potential Associations (0)

Details

Type	Incident
Added	10-15-2021 11:20 EDT by Integrations api
Event Date	10-14-2021
Status	None (Click here to enter a status)

Tags
Recent Tags...

This document is ZeroFox Confidential and should not be shared or distributed without permission.

© 2021 ZeroFox Inc.



FURTHER ASSISTANCE

If you have any questions about this integration or document, please contact integration-support@zerofox.com