ZeroFox Alerts for ThreatConnect

Installation and Configuration Guide

V1.0.1 - Oct 13, 2021

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

OVERVIEW

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

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

Integration Description

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

Within ZeroFox, an alert provides information about a potential threat to an entity in order to help analyze social-media-based threat indicators such as profiles, pages, posts, and comments from a number of different sources.

The ZeroFox Alerts 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 alerts are imported as Incident Groups to the ThreatConnect platform and they include contextual data similar to what you would see on the ZeroFox Platform for all alerts.

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

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

INSTALLATION

ThreatConnect Platform

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

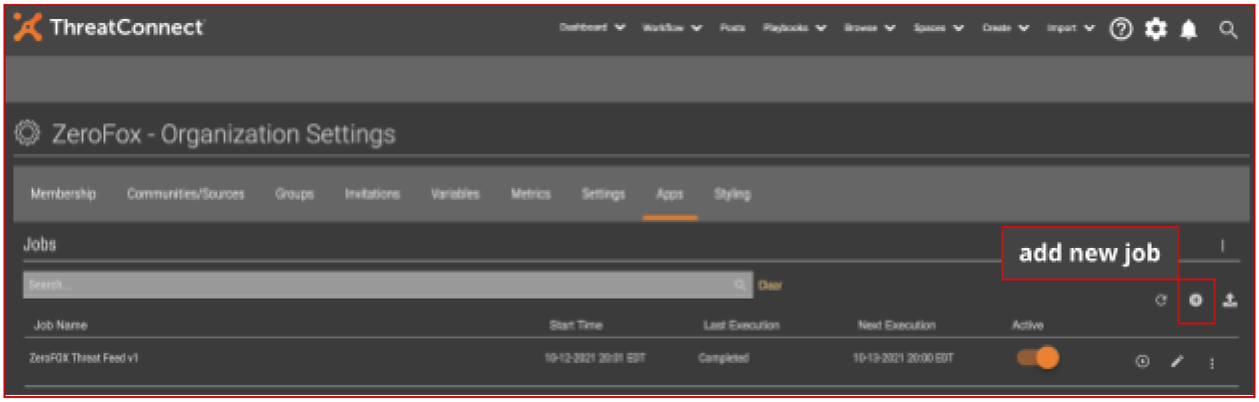
ZeroFox Alerts App

Once the ZeroFox Alerts 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.

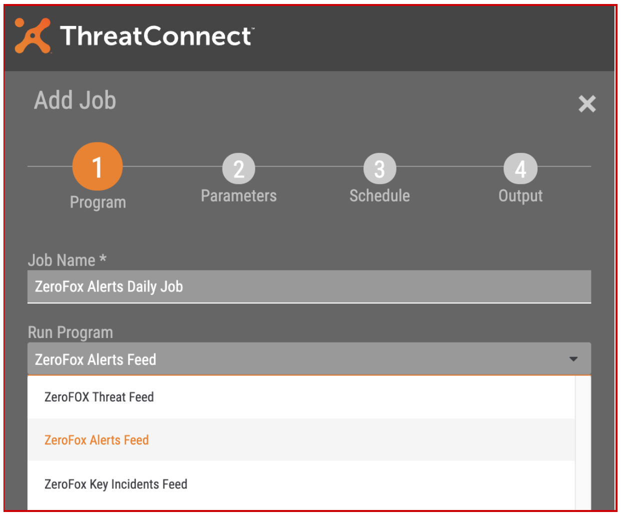


Job Name	Start Time	Last Execution	Next Execution	Active
ZeroFOX Threat Feed v1	10-12-2021 20:01 EDT	Completed	10-13-2021 20:00 EDT	

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

Step 1: Program

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



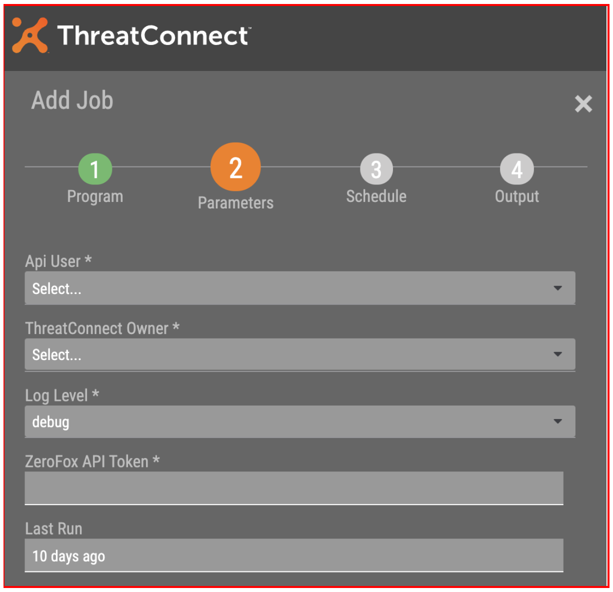
Job Name *
ZeroFox Alerts Daily Job

Run Program
ZeroFox Alerts Feed

- ZeroFOX Threat Feed
- ZeroFox Alerts Feed
- ZeroFox Key Incidents Feed

Step 2: Parameters

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



Api User *
Select...

ThreatConnect Owner *
Select...

Log Level *
debug

ZeroFox API Token *

Last Run
10 days ago

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 API Token: Enter in the API key provided for ZeroFox Alerts.

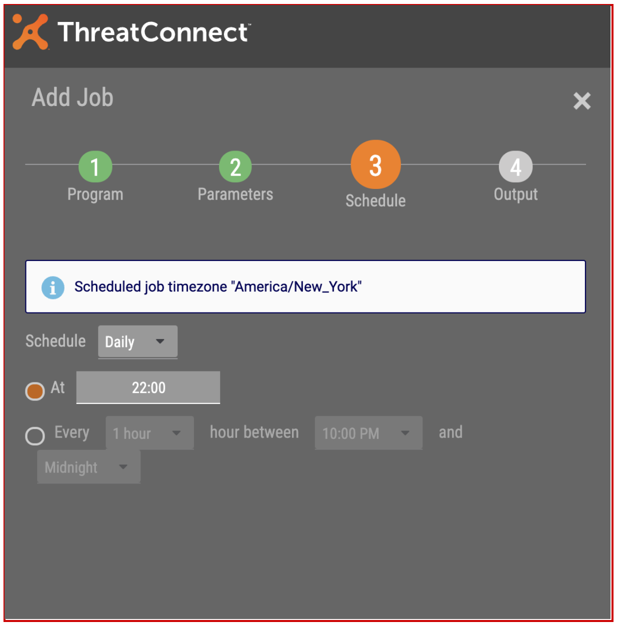
Last Run: Upon your job’s initial setup, this field will be set to “10 Days ago” to look for historical data. On subsequent runs, this field will be updated automatically to the date and time when the app last ran.

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 that occurred in the last 24 hours instead.

Step 3: Schedule

Here you will add scheduling information for your new job.

Suggested schedule setting for the ZeroFox Alerts app is **daily** at any desired time, since by default, the ZeroFox app fetches data within the last 24 hours after the initial run.

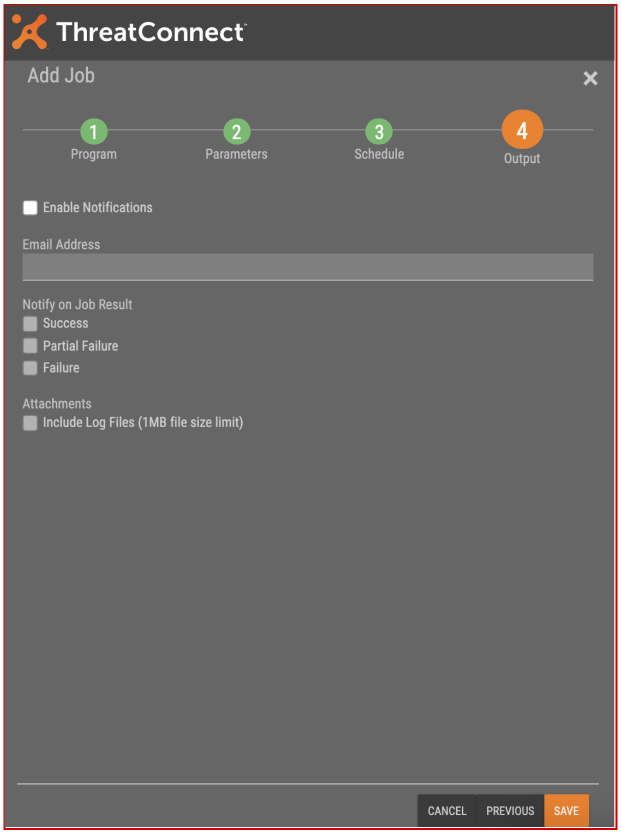


Scheduled job timezone "America/New_York"

Schedule: Daily

● At 22:00

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



□ Enable Notifications

Email Address

Notify on Job Result
□ Success
□ Partial Failure
□ Failure

Attachments
□ Include Log Files (1MB file size limit)

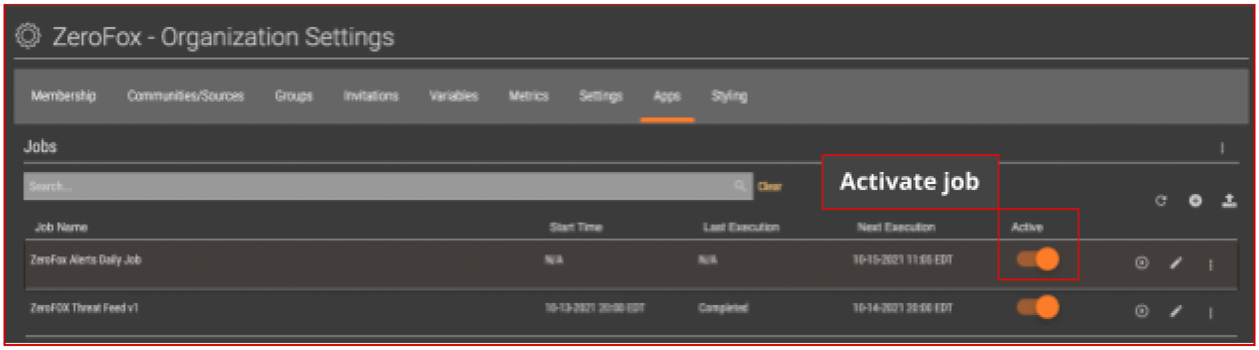
Step 4: Output

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.

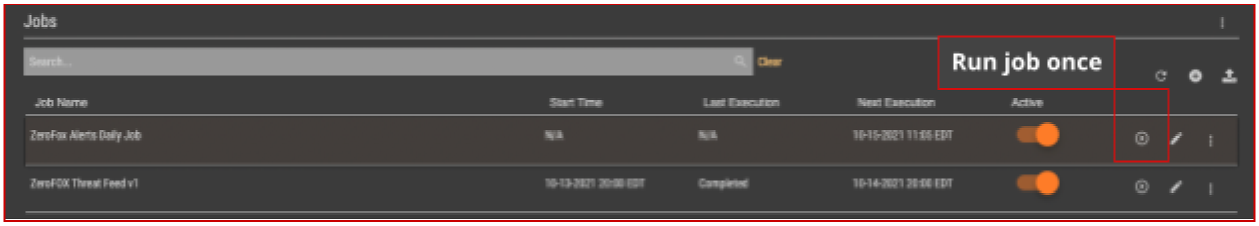

ZeroFox - Organization Settings

Jobs

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	●
ZeroFOX Threat Feed v1	10-13-2021 20:00 EDT	Completed	10-14-2021 20:00 EDT	●

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.

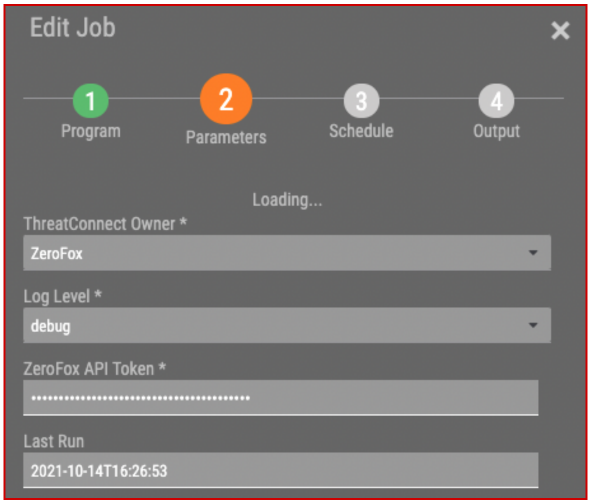


Jobs

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	●
ZeroFOX Threat Feed v1	10-13-2021 20:00 EDT	Completed	10-14-2021 20:00 EDT	●

After the initial run, the app's **"Last Run"** setting will be updated to the time and date when the application ran, and it will look for alerts that occurred in the last 24 hours on each scheduled run that follows.


Edit Job

ThreatConnect Owner *: ZeroFox

Log Level *: debug

ZeroFox API Token *: ••

Last Run: 2021-10-14T16:26:53

Data Mapping

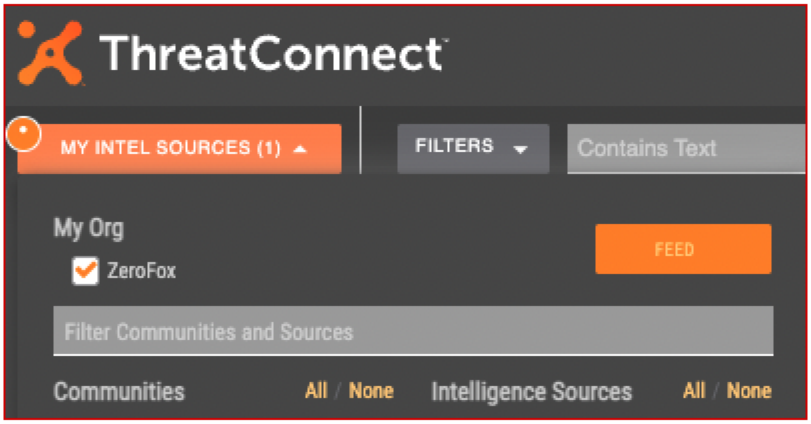
The table below outlines the data objects mapped between the ZeroFox Alerts solution and the ThreatConnect platform:

ZeroFox Field	ThreatConnect Field	Examples
Label Name	Tag	“Executive”
Alert Type	Tag	“search query”, “impersonating account”
Network	Tag	“Twitter”, “Facebook”
Alert ID	External ID	“147964163”
Cloud URL	Additional Analysis and Context	“https://cloud.zerofox.com/alerts/147964163”
Offending Content URL	Source	“http://twitter.com/executemalware/status/1”
Timestamp	External Date Created	2021-09-20T14:38:02Z
Severity	Threat Level	Info, Low, Medium, High, or Critical.

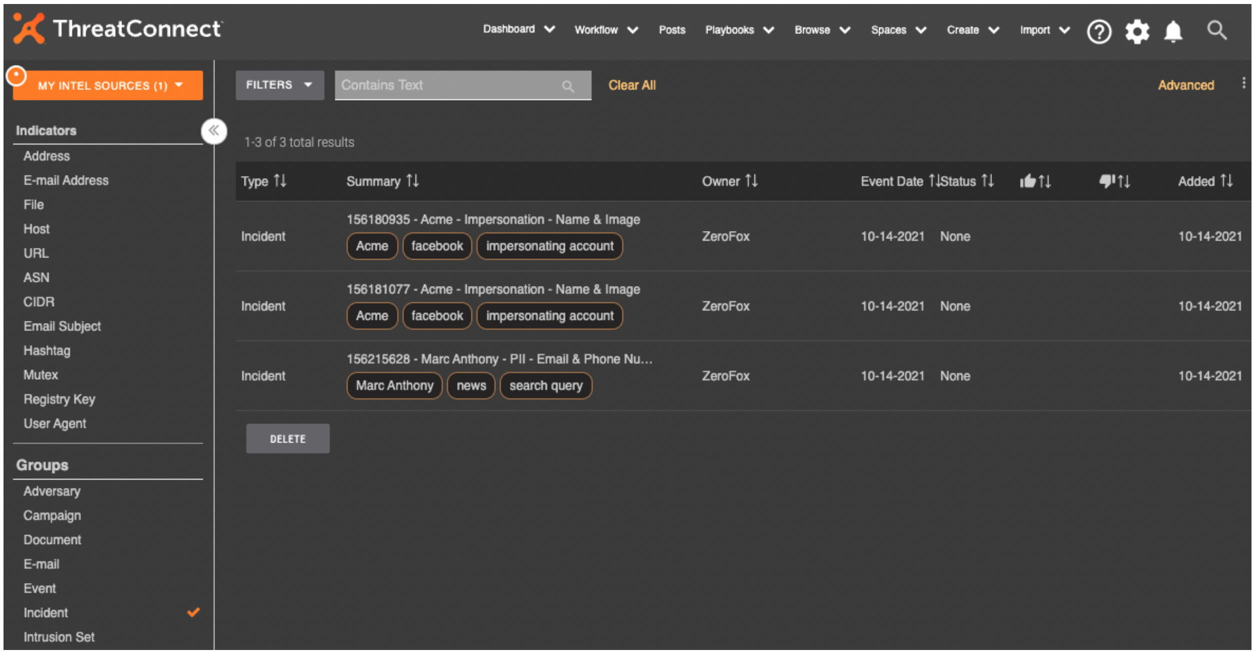
Data Output

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 alerts added as incident groups to the ThreatConnect platform:

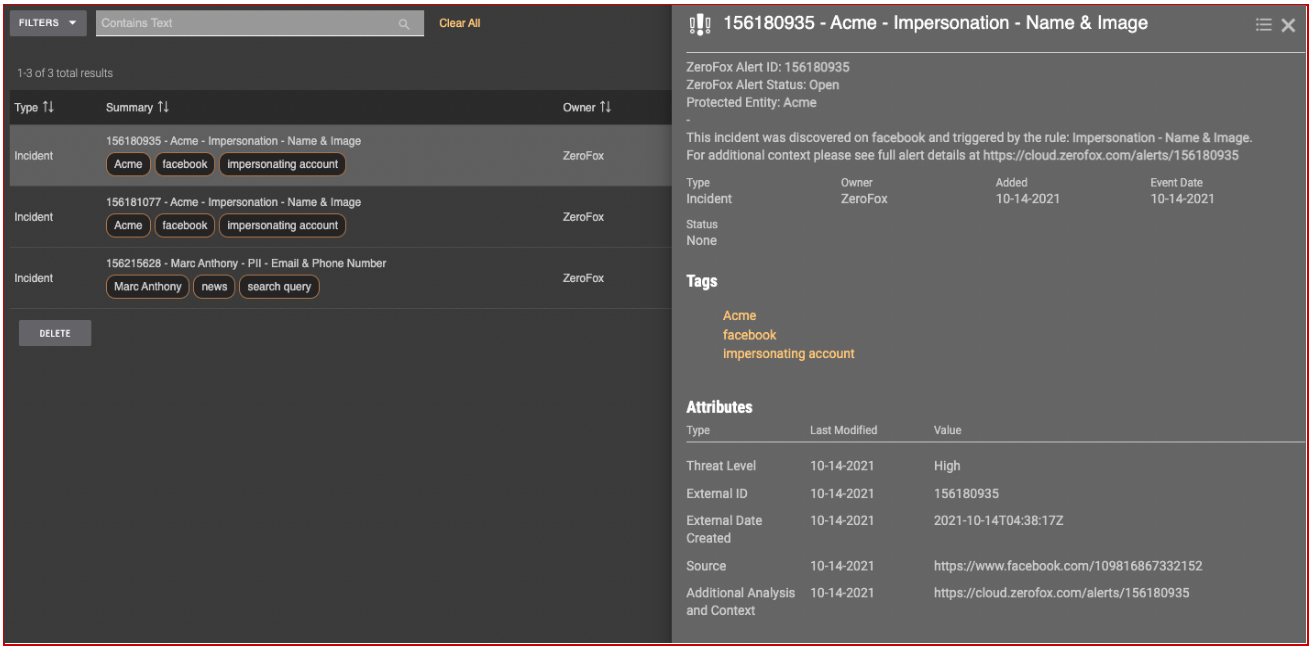


1-3 of 3 total results

Type ↑↓	Summary ↑↓	Owner ↑↓	Event Date ↑↓	Status ↑↓	👍↑↓	👎↑↓	Added ↑↓
Incident	156180935 - Acme - Impersonation - Name & Image Acme facebook impersonating account	ZeroFox	10-14-2021	None			10-14-2021
Incident	156181077 - Acme - Impersonation - Name & Image Acme facebook impersonating account	ZeroFox	10-14-2021	None			10-14-2021
Incident	156215628 - Marc Anthony - PII - Email & Phone Nu... Marc Anthony news search query	ZeroFox	10-14-2021	None			10-14-2021

ZEROFOX®

SAMPLE DATA



1-3 of 3 total results

Type	Summary	Owner
Incident	156180935 - Acme - Impersonation - Name & Image Acme facebook impersonating account	ZeroFox
Incident	156181077 - Acme - Impersonation - Name & Image Acme facebook impersonating account	ZeroFox
Incident	156215628 - Marc Anthony - PII - Email & Phone Number Marc Anthony news search query	ZeroFox

156180935 - Acme - Impersonation - Name & Image

ZeroFox Alert ID: 156180935
ZeroFox Alert Status: Open
Protected Entity: Acme
-
This incident was discovered on facebook and triggered by the rule: Impersonation - Name & Image.
For additional context please see full alert details at https://cloud.zerofox.com/alerts/156180935

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

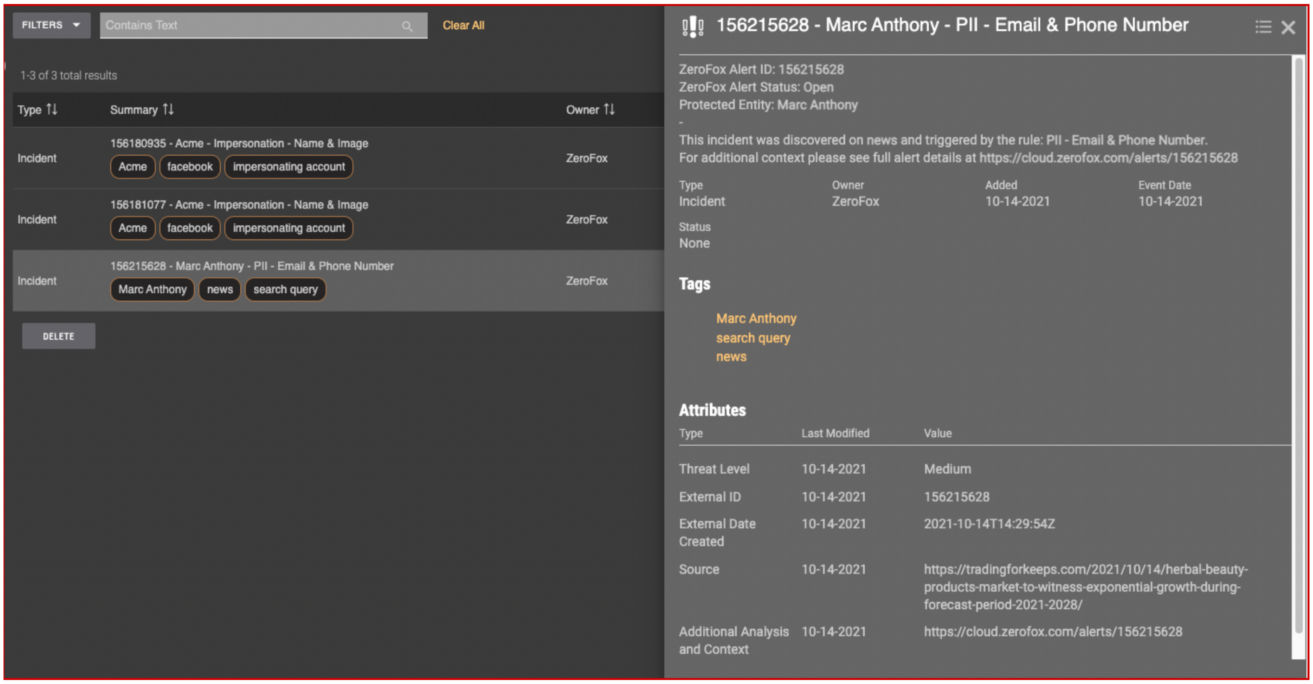
Status
None

Tags

Acme
facebook
impersonating account

Attributes

Type	Last Modified	Value
Threat Level	10-14-2021	High
External ID	10-14-2021	156180935
External Date Created	10-14-2021	2021-10-14T04:38:17Z
Source	10-14-2021	https://www.facebook.com/109816867332152
Additional Analysis and Context	10-14-2021	https://cloud.zerofox.com/alerts/156180935



1-3 of 3 total results

Type	Summary	Owner
Incident	156180935 - Acme - Impersonation - Name & Image Acme facebook impersonating account	ZeroFox
Incident	156181077 - Acme - Impersonation - Name & Image Acme facebook impersonating account	ZeroFox
Incident	156215628 - Marc Anthony - PII - Email & Phone Number Marc Anthony news search query	ZeroFox

156215628 - Marc Anthony - PII - Email & Phone Number

ZeroFox Alert ID: 156215628
ZeroFox Alert Status: Open
Protected Entity: Marc Anthony
-
This incident was discovered on news and triggered by the rule: PII - Email & Phone Number.
For additional context please see full alert details at https://cloud.zerofox.com/alerts/156215628

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

Status
None

Tags

Marc Anthony
search query
news

Attributes

Type	Last Modified	Value
Threat Level	10-14-2021	Medium
External ID	10-14-2021	156215628
External Date Created	10-14-2021	2021-10-14T14:29:54Z
Source	10-14-2021	https://tradingforkeeps.com/2021/10/14/herbal-beauty-products-market-to-witness-exponential-growth-during-forecast-period-2021-2028/
Additional Analysis and Context	10-14-2021	https://cloud.zerofox.com/alerts/156215628

FURTHER ASSISTANCE

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