ZeroFOX® Threat Feed Integration

User Guide

Software Version 1.0

August 3, 2020

30057-02 EN Rev. A

ThreatConnect, Inc.
3865 Wilson Blvd., Suite 550, Arlington, VA 22203

P: 1.800.965.2708 | F: .703.229.4489
www.ThreatConnect.com

Table of Contents

OVERVIEW

ZeroFOX Threat Feed is a valuable resource for blocking and analyzing social-media-based threat indicators such as profiles, pages, posts, and comments from a number of different sources.

The ThreatConnect® integration with ZeroFOX Threat Feed allows ThreatConnect customers to import Campaigns and Indicators, along with all of their context, from the ZeroFOX Threat Feed into ThreatConnect.

DEPENDENCIES

ThreatConnect Dependencies

- ThreatConnect version 5.6 or newer
- Active ThreatConnect Application Programming Interface (API) key

NOTE: All ThreatConnect dependencies will be provided by default to subscribing ThreatConnect Cloud customers. Private Instance customers can enable these settings during configuration on the** Account Settings **screen within their Private Instance of ThreatConnect.

ZeroFOX Dependencies

- Active subscription to ZeroFOX Threat Feed with API key

APPLICATION SETUP AND CONFIGURATION

System Administrators should use the ThreatConnect Feed Deployer to set up and configure the ZeroFOX Threat Feed app. See the "Feed Deployment" sub-section of the "Apps and Jobs" section of the *ThreatConnect System Administration Guide* for instructions on how to use the Feed Deployer. On the **Confirm** screen, uncheck the **Run Jobs after deployment** and **Activate Jobs after deployment** checkboxes. It is highly recommended to review the app configuration prior to running or activating the Job.

CONFIGURATION PARAMETERS

Parameter Definition

The parameters defined in Table 1 apply to the configuration parameters during the job-creation process.

Table 1

Name	Description
ThreatConnect API Access ID	This parameter is the name of the API user in ThreatConnect.
Destination Owner	This parameter is the name of the Organization in ThreatConnect that will own the data imported from ZeroFOX.
ZeroFox API Token	This parameter is the ZeroFOX API token.
Last Run (for initial run, enter Start Timestamp)	This parameter is the epoch time of the last time this job ran successfully.
Indicator Confidence Rating	This parameter sets a default Confidence Rating on all Indicators downloaded from ZeroFOX.
Logging Level	This parameter is the logging level for the app (recommended value: **info**).

DATA MAPPING

The data mappings in Table 2 and Table 3 illustrate how data are mapped from the ZeroFOX API endpoints into Campaign and Indicator objects, respectively, in ThreatConnect.

Campaigns

Table 2

ZeroFOX API Field	ThreatConnect Field
id	Attribute: “External ID”
name	Campaign: Name
privacy_level	Campaign: Security Label
description	Attribute: “Description”
url_descriptions	Attribute: “Additional Analysis and Context”
created_at	Attribute: “External Date Created”
updated_at	Attribute: “External Date Last Modified”

Indicators

Table 3

ZeroFOX API Field	ThreatConnect Field
id	Attribute: “External ID”
Indicator_type	Indicator: Type Attribute: “URL Type”
value	Indicator: Value
network	Tags
privacy_level	Indicator: Security Label
zf_alert_id	Attribute: “Source”
threat_level	Indicator: Threat Rating
classifications	Tags
campaigns	Association: Campaign
ttl	Attribute: “External Date Expires”
expired	Indicator: Active
created_at	Attribute: “External Date Created”
updated_at	Attribute: “External Date Last Modified”

TROUBLESHOOTING

The ZeroFOX Threat Feed integration is a Python®-based app that requires certificate verification. Organizations using SSL inspection solutions will need to import their internal CA certificate to the OS-trusted root certificate store in order for the connection to ZeroFOX to be initiated.