ThreatConnect™

Proofpoint™ ET Intelligence Reputation List Integration

User Guide

Software Version 1.0

November 1, 2019

30064-01 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

Proofpoint ET Intelligence Reputation List threat intelligence feeds focus on IP and domain reputation data, providing information and context that identify malicious activity worldwide. The ThreatConnect® integration with Proofpoint ET Intelligence Reputation List allows ThreatConnect users to import Address and Host Indicators, along with all of their context, from the Proofpoint ET Intelligence Reputation List API 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.

Proofpoint Dependencies

- Active subscription to Proofpoint ET Intelligence Reputation List subscription code with API access. Customers can retrieve their subscription code from the **Subscriptions** page in the Proofpoint ET Admin Portal.

APPLICATION SETUP AND CONFIGURATION

System Administrators should use the ThreatConnect Feed Deployer to set up and configure the Proofpoint ET Intelligence Reputation List 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
Proofpoint ET Intelligence Reputation List Subscription Code	This parameter is the Proofpoint ET Intelligence Reputation List Subscription Code.
Destination Owner	This parameter is the name of the Organization in ThreatConnect that will own the data imported from the Proofpoint ET Intelligence Reputation List.
Indicator Types to Collect	This parameter sets the types of Indicators that will be imported from Proofpoint ET Intelligence Reputation List.
Action for Removed Indicators	This parameter determines the action to be applied to Indicators that have been removed from the Proofpoint ET Intelligence Reputation List.
Threat Rating	This parameter sets a default Threat Rating on all Indicators downloaded from the Proofpoint ET Intelligence Reputation List.
Confidence Rating	This parameter sets a default Confidence Rating on all Indicators downloaded from the Proofpoint ET Intelligence Reputation List.
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 Proofpoint ET Intelligence Reputation List API into Address and Host objects, respectively, in ThreatConnect.

Table 2

Proofpoint API Field	ThreatConnect Field
ip	Indicator: Value
category	Tags
score	Attribute: “External Score”, Rating
first_seen	Attribute: “First Seen”
last_seen	Attribute: “Last Seen”

Table 3

Proofpoint API Field	ThreatConnect Field
domain	Indicator: Value
category	Tags
score	Attribute: “External Score”, Rating
first_seen	Attribute: “First Seen”
last_seen	Attribute: “Last Seen”

TROUBLESHOOTING

The Proofpoint ET Intelligence Reputation List 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 the Proofpoint ET Intelligence Reputation List API to be initiated.