



Proofpoint™ ET Pro Signatures Integration Configuration Guide

Software Version 1.0

December 23, 2021

30076-01 EN Rev. A



©2021 ThreatConnect, Inc.

ThreatConnect® is a registered trademark of ThreatConnect, Inc.

Proofpoint™ is a trademark of Proofpoint, Inc.





Table of Contents

OVERVIEW	4
DEPENDENCIES	4
ThreatConnect Dependencies	4
Proofpoint Dependencies.....	4
CONFIGURATION PARAMETERS	5
Parameter Definition.....	5





OVERVIEW

The ThreatConnect® integration with Proofpoint ET Pro Signatures is designed to pull signatures from Proofpoint ET Pro Ruleset in Suricata and/or Snort format for writing into ThreatConnect.

DEPENDENCIES

ThreatConnect Dependencies

- ThreatConnect version 6.0.0 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 under the Account Settings menu within their Private Instance of ThreatConnect or locally in their On Premises setup. Job creation can be done either in an On Premises installation or on a ThreatConnect Environment Server.

Proofpoint Dependencies

- Active Proofpoint ET Pro Signatures oinkcode. This item is provided to customers via email after the purchase of Proofpoint ET Pro and can also be retrieved from the Proofpoint ET Admin Portal.





CONFIGURATION PARAMETERS

Parameter Definition

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

Table 1

Name	Description	Required?
Api User	The name of the ThreatConnect API user.	Yes
Proofpoint ET Pro Signatures oinkcode	The Proofpoint ET Pro Signatures oinkcode.	Yes
Suricata Version	Either Suricata or Snort version must be included.	No
Snort Version	Either Suricata or Snort version must be included.	No
Owner	The ThreatConnect data owner that will be receiving the Suricata or Snort rules.	Yes
Logging Level	The level used to determine the verbosity of the logging output for the application.	Yes
Advanced Settings	Use this field for advanced settings, such as allowing the job to trigger Playbook apps.	No