Amazon GuardDuty® Integration

Configuration Guide

Software Version 1.0

July 27, 2021

30075-01 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

The ThreatConnect® integration with Amazon GuardDuty is designed to upload IPv4 and IPv6 Address Indicators from ThreatConnect to Threat Intel Sets and Trusted IP Sets in GuardDuty. Several filters are available to narrow the scope of Indicators retrieved from ThreatConnect, including Threat Rating, Confidence Rating, owner, Indicator type, and Tags.

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 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.

Amazon GuardDuty Dependencies

- Active Amazon GuardDuty subscription with API token

CONFIGURATION PARAMETERS

Parameter Definition

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

Table 1

Name	Description
API User	This parameter is the API user that will retrieve data from ThreatConnect.
AWS Access Key	This parameter is the Amazon Web Services™ (AWS) Access Key. It is used for authentication.
AWS Secret Key	This parameter is the AWS Secret Key. It is used for authentication.
AWS Region	This parameter is the AWS Region.
S3 Bucket	This parameter is the S3 Bucket that connects to AWS.
Set List Type	This parameter is the type of set (**Threat Intel Set** or **Trusted IP Set**) to which the Indicators from ThreatConnect will be uploaded in GuardDuty.
Intel Set Name	This parameter is the name displayed in all findings that are generated by activity involving Addresses included in the set.
Owners	This parameter is a multi-select dropdown list of ThreatConnect owners on which to filter.
Indicator Types	This parameter provides the ThreatConnect Indicator types on which to filter.

Minimum ThreatAssess Score	This parameter is the minimum ThreatAssess score that an Indicator must have in order to be uploaded.
Minimum Confidence Rating	This parameter is the minimum Confidence Rating that an Indicator must have in order to be uploaded.
Minimum Threat Rating	This parameter is the minimum Threat Rating that an Indicator must have in order to be uploaded.
False Positive Threshold	This parameter is the lowest number of false positives that will prevent an Indicator from being uploaded.
Tag Filter	This parameter provides the Tags that will be added to the Threat Intel Set or Trusted IP Set in GuardDuty.
Modified Since	This parameter is the date on which the GuardDuty set was last modified.
Logging Level	This parameter is the logging level for the app (recommended value: **INFO**).