Dragos™ WorldView Integration

Configuration Guide

Software Version 1.0

August 6, 2019

30058-02 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

Dragos WorldView threat intelligence feeds, alerts, reports, and briefings focus on Industrial Control Systems (ICS) threat intelligence, providing information and context that identify the malicious actors and activity targeting industrial control networks globally. The ThreatConnect® integration with Dragos WorldView allows ThreatConnect users to import Reports and Indicators, along with all of their context, from the Dragos WorldView 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.***

Dragos Dependencies

- Active subscription to Dragos WorldView with API Access Token and Secret Key. Customers can generate the API key pair from the **User Profile** page in the Dragos WorldView Portal.

APPLICATION SETUP AND CONFIGURATION

System Administrators should use the ThreatConnect Feed Deployer to set up and configure the Dragos WorldView 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 ThreatConnect API user.
Dragos API Access Token	This parameter is the Dragos WorldView API Access Token.
Dragos API Secret Key	This parameter is the Dragos WorldView API Secret Key.
Destination Owner	This parameter is the name of the Organization in ThreatConnect that will own the data imported from Dragos WorldView.
Last Run (for initial run, enter Start Timestamp)	This parameter is the epoch time of the last time this job ran successfully.
Confidence Rating	This parameter sets a default Confidence Rating on all Indicators downloaded from Dragos WorldView.
Threat Rating	This parameter sets a default Threat Rating on all Indicators downloaded from Dragos WorldView.
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 Dragos WorldView API endpoints into Report and Indicator objects, respectively, in ThreatConnect.

Reports

Table 2

Dragos API Field	ThreatConnect Field
tlp_level	Report: Security Label
title	Report: Name
executive_summary	Attribute: “Description”
updated_at	Attribute: “External Date Last Modified”
release_date	Report: Publish Date
threat_level	Attribute: “Threat Level”
serial	Attribute: “External ID”
tags	Tags
report_link	Attribute: “Source”

Indicators

Table 3

Dragos API Field	ThreatConnect Field
id	Attribute: “External ID”
value	Indicator: Value
indicator_type	Indicator: Type
category	Tags
comment	Attribute: “Description”
first_seen	Attribute: “First Seen”
last_seen	Attribute: “Last Seen”
updated_at	Attribute: “External Date Last Modified”
products	Association: Report

TROUBLESHOOTING

The Dragos WorldView 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 Dragos WorldView API to be initiated.