Accenture™ iDefense® IntelGraph Intelligence Engine Integration User Guide

Software Version 1.0

Integration Guide

April 27, 2023

30059-03 EN Rev. A

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

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

Table of Contents

Overview

The Accenture iDefense IntelGraph integration with ThreatConnect® allows customers to ingest the IntelGraph feed into ThreatConnect for analysis and response actions. The integration downloads the 21 Fundamentals, as well as Intel Alerts and Intel Reports, into ThreatConnect.

Dependencies

ThreatConnect Dependencies

- ThreatConnect version 6.7 or newer
- 8GB of free memory on Application/Job server
- 10GB minimum of free disk space for data storage if downloading Reports
- Active ThreatConnect Application Programming Interface (API) key

> **Note**: All ThreatConnect dependencies will be provided by default to subscribing ThreatConnect Cloud customers. Customers on Dedicated Cloud and On-Premises instances can enable these settings on the **Account Settings** screen within their ThreatConnect instance.

iDefense Dependencies

- Active subscription to Accenture iDefense IntelGraph with API key

Application Setup and Configuration

1. Install the **Accenture iDefense IntelGraph Intelligence Engine** App via TC Exchange™.
2. Use the ThreatConnect Feed Deployer to set up and configure the **Accenture iDefense IntelGraph Intelligence Engine** App.

   > **Note**: When the App runs for the first time, it will retrieve data for the selected Document type(s) from the past 10 years and data for the selected Fundamental type(s) from the past year.

Configuration Parameters

Parameter Definitions

The parameters defined in Table 1 apply to the configuration parameters available when using the Feed Deployer to configure the App.

Table 1

Name	Description	Required?
Launch Server	Select the server on which the Service corresponding to the Feed API Service App will launch. It is recommended to select **tc-job**	Yes
Fundamental Types	Select the Fundamental type(s) that will be downloaded by the Feed API Service. Only the selected Fundamental types will be downloaded and associated to one another in ThreatConnect.	Yes
Document Types	Select the Document type(s) that will be downloaded by the Feed API Service. Only the selected Document type(s) will be downloaded and associated to one another in ThreatConnect.	Yes
Accenture iDefense IntelGraph Auth Token	The iDefense API authorization token.	Yes

Data Mappings

The data mappings in Table 2 illustrate how data are mapped from the iDefense Fundamental and Document API endpoints into ThreatConnect at a high level.

Table 2

iDefense Fundamental	ThreatConnect Object
Account	adversary:asset:handle
ASN	ASN
Community	Tag
Country	attribute: “Target Country”
Detection Signature	Signature
Domain	Host
File	File
Global Event	Incident
Intelligence Alert	Report
Intelligence Report	Report
IP	Address
Malicious Event	Incident
Malicious Tool	Threat
Malware Family	Threat
Package	N/A
Phish	Email
Region	attribute: “Region” (custom)

Target Organization	Tag
Threat Actor	Adversary
Threat Campaign	Campaign
Threat Group	Adversary
URL	URL
Vertical	Tag
Vulnerability	Tag
Vulnerability Tech	Tag

Troubleshooting

The iDefense IntelGraph 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 iDefense to be initiated.