ThreatConnect® Transform Pack

Transform Setup & Documentation

Revision: April 4, 2018

MALFORMITYLABS

Table of Contents

Background

This document will provide the information required in order to successfully install your ThreatConnect® Transform Pack and associated entities. It also serves as a full transform reference document that can be used to explore the different types of analysis that are made possible with the transforms and machines. The document will be updated and redistributed as new transforms are added to the ThreatConnect Seed.

Software Requirements:
- Valid commercially licensed copies of the Maltego Client

Installing the Seed

Prior to using your ThreatConnect transforms, you will need to import the seed and discover the necessary transforms and configuration data, which include entities, icons, and machines.

In the Maltego Transform Hub, locate the ThreatConnect seed entry.

Highlight the entry and select 'Install'. You can either choose to enter your credentials now or wait until your first transform run. To enter them now, select 'Details' and then 'Settings'.
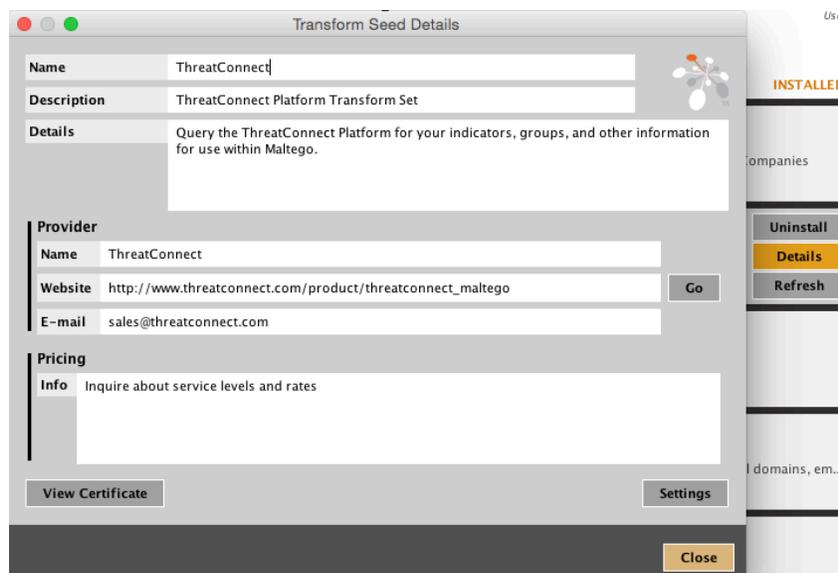
You can then enter your Secret Key and Access ID for the ThreatConnect API.

Transform Overview

The transforms discussed in this section are provided through your ThreatConnect seed. They are grouped according to input entity type. You will be required to enter your ThreatConnect API ID and Security Key prior to the first use.
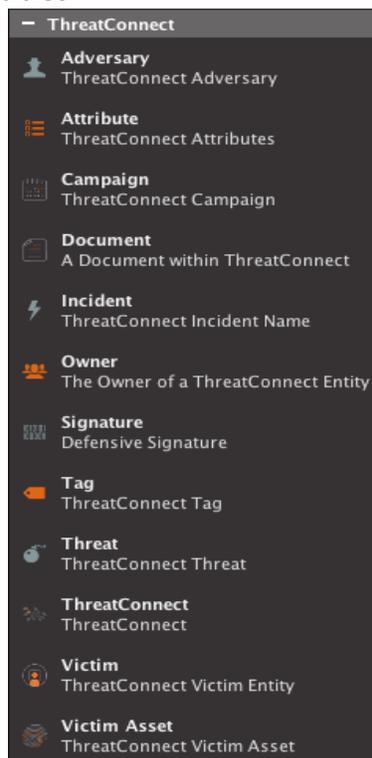
Group Entity Requirements

Within ThreatConnect, Groups consist of Adversaries, Campaigns, Documents, Emails, Incidents, Signatures, Tasks, and Threats. When these Groups are created as outgoing entities from a previously run transform, there are no special requirements. However, in order to create a fresh Group entity from the Maltego palette and be able to successfully run ThreatConnect transforms against it, you must provide a value in the 'ID' property.

Property View		>> ✕
▼ Properties		
Type	Adversary	
Adversary	-	...
owner		...
ID		...

This property is used to query the ThreatConnect API and is currently required for Group transforms.

ThreatConnect-Specific Entities

ThreatConnect

Adversary
ThreatConnect Adversary

Attribute
ThreatConnect Attributes

Campaign
ThreatConnect Campaign

Document
A Document within ThreatConnect

Incident
ThreatConnect Incident Name

Owner
The Owner of a ThreatConnect Entity

Signature
Defensive Signature

Tag
ThreatConnect Tag

Threat
ThreatConnect Threat

ThreatConnect
ThreatConnect

Victim
ThreatConnect Victim Entity

Victim Asset
ThreatConnect Victim Asset

MALFORMITYLABS

Transform Listing

Transform Name	Input Entity	Output Entity
tcASN2Victim	AS	Victim
tcASN2VictimAsset	AS	Victim Asset
tcASNAdversary	AS	Adversary
tcASNAttributes	AS	Attributes
tcASNCampaign	AS	Campaign
tcASNDocument	AS	Document
tcASNEmail	AS	Email
tcASNGroups	AS	Multiple
tcASNIncidents	AS	Incident
tcASNOwners	AS	Owners
tcASNSignature	AS	Signature
tcASNTag	AS	Tag
tcASNThreat	AS	Threat
tcAdversary2ASN	Adversary	AS
tcAdversary2Adversary	Adversary	Adversary
tcAdversary2Attributes	Adversary	Attributes
tcAdversary2CIDR	Adversary	Netblock
tcAdversary2Campaign	Adversary	Campaign
tcAdversary2Document	Adversary	Document
tcAdversary2Domain	Adversary	Domain
tcAdversary2Email	Adversary	Email Address
tcAdversary2EmailGroup	Adversary	Email
tcAdversary2File	Adversary	Hash
tcAdversary2Groups	Adversary	Multiple
tcAdversary2IP	Adversary	IP Address
tcAdversary2Incident	Adversary	Incident
tcAdversary2Indicators	Adversary	Multiple
tcAdversary2Mutex	Adversary	Mutex
tcAdversary2RegistryKey	Adversary	Registry Entry
tcAdversary2Signature	Adversary	Signature
tcAdversary2Tags	Adversary	Tag
tcAdversary2Threat	Adversary	Threat
tcAdversary2URL	Adversary	URL
tcAdversary2UserAgent	Adversary	User Agent
tcAdversary2VictimAsset	Adversary	Victim Asset
tcAdversary2Victims	Adversary	Victim

tcCIDR2Victim	Netblock	Victim
tcCIDR2VictimAsset	Netblock	Victim Asset
tcCIDRAdversary	Netblock	Adversary
tcCIDRAttributes	Netblock	Attributes
tcCIDRCampaign	Netblock	Campaign
tcCIDRDocument	Netblock	Document
tcCIDREmail	Netblock	Email
tcCIDRGroups	Netblock	Multiple
tcCIDRIncidents	Netblock	Incident
tcCIDROwners	Netblock	Owners
tcCIDRSignature	Netblock	Signature
tcCIDRTag	Netblock	Tag
tcCIDRThreat	Netblock	Threat
tcCampaign2ASN	Campaign	AS
tcCampaign2Adversary	Campaign	Adversary
tcCampaign2Attributes	Campaign	Attributes
tcCampaign2CIDR	Campaign	Netblock
tcCampaign2Campaign	Campaign	Campaign
tcCampaign2Document	Campaign	Document
tcCampaign2Domain	Campaign	Domain
tcCampaign2Email	Campaign	Email Address
tcCampaign2EmailG	Campaign	Email
tcCampaign2File	Campaign	Hash
tcCampaign2Groups	Campaign	Multiple
tcCampaign2IP	Campaign	IP Address
tcCampaign2Incident	Campaign	Incident
tcCampaign2Indicators	Campaign	Multiple
tcCampaign2Mutex	Campaign	Mutex
tcCampaign2RegistryKey	Campaign	Registry Entry
tcCampaign2Signature	Campaign	Signature
tcCampaign2Tags	Campaign	Tag
tcCampaign2Threat	Campaign	Threat
tcCampaign2URL	Campaign	URL
tcCampaign2UserAgent	Campaign	User Agent
tcCampaign2VictimAssets	Campaign	Victim Asset
tcCampaign2Victims	Campaign	Victim
tcDocument2ASN	Document	AS
tcDocument2Adversary	Document	Adversary
tcDocument2Attributes	Document	Attributes

tcDocument2CIDR	Document	Netblock
tcDocument2Campaign	Document	Campaign
tcDocument2Document	Document	Document
tcDocument2Domain	Document	Domain
tcDocument2Email	Document	Email Address
tcDocument2EmailAddresses	Document	Email
tcDocument2File	Document	Hash
tcDocument2Groups	Document	Multiple
tcDocument2IP	Document	IP Address
tcDocument2Incident	Document	Incident
tcDocument2Indicators	Document	Multiple
tcDocument2Mutex	Document	Mutex
tcDocument2RegistryKey	Document	Registry Entry
tcDocument2Signature	Document	Signature
tcDocument2Tags	Document	Tag
tcDocument2Threat	Document	Threat
tcDocument2URL	Document	URL
tcDocument2UserAgent	Document	User Agent
tcDocument2VictimAssets	Document	Victim Asset
tcDocument2Victims	Document	Victim
tcDomain2Victim	Domain	Victim
tcDomain2VictimAsset	Domain	Victim Asset
tcDomainAdversary	Domain	Adversary
tcDomainAttributes	Domain	Attributes
tcDomainCampaign	Domain	Campaign
tcDomainDocument	Domain	Document
tcDomainEmail	Domain	Email
tcDomainGroups	Domain	Multiple
tcDomainIncidents	Domain	Incident
tcDomainOwners	Domain	Owners
tcDomainSignature	Domain	Signature
tcDomainTag	Domain	Tag
tcDomainThreat	Domain	Threat
tcDuplicateDomain	Domain	Domain
tcDuplicateEmailAddr	Email Address	Email Address
tcDuplicateFile	Hash	Hash
tcDuplicateIP	IPv4 Address	IP Address
tcDuplicateURL	URL	URL
tcEmail2ASN	Email	AS

tcEmail2Adversary	Email	Adversary
tcEmail2Attributes	Email	Attributes
tcEmail2CIDR	Email	Netblock
tcEmail2Campaign	Email	Campaign
tcEmail2Document	Email	Document
tcEmail2Domain	Email	Domain
tcEmail2Email	Email	Email
tcEmail2EmailAddress	Email	Email Address
tcEmail2File	Email	Hash
tcEmail2Groups	Email	Multiple
tcEmail2IP	Email	IP Address
tcEmail2Incident	Email	Incident
tcEmail2Indicators	Email	Multiple
tcEmail2Mutex	Email	Mutex
tcEmail2RegistryKey	Email	Registry Entry
tcEmail2Signature	Email	Signature
tcEmail2Tags	Email	Tag
tcEmail2Threat	Email	Threat
tcEmail2URL	Email	URL
tcEmail2UserAgent	Email	User Agent
tcEmail2Victim	Email Address	Victim
tcEmail2VictimAsset	Email Address	Victim Asset
tcEmail2VictimAssets	Email	Victim Asset
tcEmail2Victims	Email	Victim
tcEmailAddressEmail	Email Address	Email
tcEmailAdversary	Email Address	Adversary
tcEmailAttributes	Email Address	Attributes
tcEmailCampaign	Email Address	Campaign
tcEmailDocument	Email Address	Document
tcEmailGroups	Email Address	Multiple
tcEmailIncidents	Email Address	Incident
tcEmailOwners	Email Address	Owners
tcEmailSignature	Email Address	Signature
tcEmailTag	Email Address	Tag
tcEmailThreat	Email Address	Threat
tcFile2Victim	Hash	Victim
tcFile2VictimAsset	Hash	Victim Asset
tcFileAdversary	Hash	Adversary
tcFileAttributes	Hash	Attributes

tcFileCampaign	Hash	Campaign
tcFileDocument	Hash	Document
tcFileEmail	Hash	Email
tcFileGroups	Hash	Multiple
tcFileIncidents	Hash	Incident
tcFileOwners	Hash	Owners
tcFileSignature	Hash	Signature
tcFileTag	Hash	Tag
tcFileThreat	Hash	Threat
tcGetASN	AS	AS
tcGetAddress	IPv4 Address	IP Address
tcGetAdversaries	Owner	Adversary
tcGetAllTags	Registry Entry	Tag
tcGetAllTags	Netblock	Tag
tcGetAllTags	IPv4 Address	Tag
tcGetAllTags	URL	Tag
tcGetAllTags	Domain	Tag
tcGetAllTags	AS	Tag
tcGetAllTags	Hash	Tag
tcGetAllTags	Mutex	Tag
tcGetAllTags	User Agent	Tag
tcGetAllTags	Email Address	Tag
tcGetCIDR	Netblock	Netblock
tcGetCampaigns	Owner	Campaign
tcGetDocuments	Owner	Document
tcGetEmail	Email Address	Email Address
tcGetEmails	Owner	Email
tcGetFile	Hash	Hash
tcGetGroups	Owner	Multiple
tcGetHost	Domain	Domain
tcGetIncidents	Owner	Incident
tcGetMutex	Mutex	Mutex
tcGetOwners	ThreatConnect	Owners
tcGetRegistryKey	Registry Entry	Registry Entry
tcGetResolutions	Domain	IP Address
tcGetSignatures	Owner	Signature
tcGetTags	Owner	Tag
tcGetThreats	Owner	Threat
tcGetURL	URL	URL

tcGetUserAgent	User Agent	User Agent
tcGetVictims	ThreatConnect	Victim
tcIP2Victim	IPv4 Address	Victim
tcIP2VictimAsset	IPv4 Address	Victim Asset
tcIPAdversary	IPv4 Address	Adversary
tcIPAttributes	IPv4 Address	Attributes
tcIPCampaign	IPv4 Address	Campaign
tcIPDocument	IPv4 Address	Document
tcIPEmail	IPv4 Address	Email
tcIPGroups	IPv4 Address	Multiple
tcIPIncidents	IPv4 Address	Incident
tcIPOwners	IPv4 Address	Owners
tcIPSignature	IPv4 Address	Signature
tcIPTag	IPv4 Address	Tag
tcIPThreat	IPv4 Address	Threat
tcIncident2ASN	Incident	AS
tcIncident2Adversary	Incident	Adversary
tcIncident2Attributes	Incident	Attributes
tcIncident2CIDR	Incident	Netblock
tcIncident2Campaign	Incident	Campaign
tcIncident2Document	Incident	Document
tcIncident2Domain	Incident	Domain
tcIncident2Email	Incident	Email Address
tcIncident2EmailGroup	Incident	Email
tcIncident2File	Incident	Hash
tcIncident2Groups	Incident	Multiple
tcIncident2IP	Incident	IP Address
tcIncident2Incident	Incident	Incident
tcIncident2Indicators	Incident	Multiple
tcIncident2Mutex	Incident	Mutex
tcIncident2RegistryKey	Incident	Registry Entry
tcIncident2Signature	Incident	Signature
tcIncident2Tags	Incident	Tag
tcIncident2Threat	Incident	Threat
tcIncident2URL	Incident	URL
tcIncident2UserAgent	Incident	User Agent
tcIncident2VictimAssets	Incident	Victim Asset
tcIncident2Victims	Incident	Victim
tcMutex2Victim	Mutex	Victim

tcMutex2VictimAsset	Mutex	Victim Asset
tcMutexAdversary	Mutex	Adversary
tcMutexAttributes	Mutex	Attributes
tcMutexCampaign	Mutex	Campaign
tcMutexDocument	Mutex	Document
tcMutexEmail	Mutex	Email
tcMutexGroups	Mutex	Multiple
tcMutexIncidents	Mutex	Incident
tcMutexOwners	Mutex	Owners
tcMutexSignature	Mutex	Signature
tcMutexTag	Mutex	Tag
tcMutexThreat	Mutex	Threat
tcOwner2ASN	Owner	AS
tcOwner2CIDR	Owner	Netblock
tcOwner2Domain	Owner	Domain
tcOwner2EmailAddress	Owner	Email Address
tcOwner2File	Owner	Hash
tcOwner2IPAddress	Owner	IP Address
tcOwner2Indicators	Owner	Multiple
tcOwner2Mutex	Owner	Mutex
tcOwner2RegistryKey	Owner	Registry Entry
tcOwner2URL	Owner	URL
tcOwner2UserAgent	Owner	User Agent
tcRegistryKey2Victim	Registry Entry	Victim
tcRegistryKey2VictimAsset	Registry Entry	Victim Asset
tcRegistryKeyAdversary	Registry Entry	Adversary
tcRegistryKeyAttributes	Registry Entry	Attributes
tcRegistryKeyCampaign	Registry Entry	Campaign
tcRegistryKeyDocument	Registry Entry	Document
tcRegistryKeyEmail	Registry Entry	Email
tcRegistryKeyGroups	Registry Entry	Multiple
tcRegistryKeyIncidents	Registry Entry	Incident
tcRegistryKeyOwners	Registry Entry	Owners
tcRegistryKeySignature	Registry Entry	Signature
tcRegistryKeyTag	Registry Entry	Tag
tcRegistryKeyThreat	Registry Entry	Threat
tcSignature2ASN	Signature	AS
tcSignature2Adversary	Signature	Adversary
tcSignature2Attributes	Signature	Attributes

tcSignature2CIDR	Signature	Netblock
tcSignature2Campaign	Signature	Campaign
tcSignature2Document	Signature	Document
tcSignature2Domain	Signature	Domain
tcSignature2Email	Signature	Email Address
tcSignature2EmailGroup	Signature	Email
tcSignature2File	Signature	Hash
tcSignature2Groups	Signature	Multiple
tcSignature2IP	Signature	IP Address
tcSignature2Incident	Signature	Incident
tcSignature2Indicators	Signature	Multiple
tcSignature2Mutex	Signature	Mutex
tcSignature2RegistryKey	Signature	Registry Entry
tcSignature2Signature	Signature	Signature
tcSignature2Tags	Signature	Tag
tcSignature2Threat	Signature	Threat
tcSignature2URL	Signature	URL
tcSignature2UserAgent	Signature	User Agent
tcSignature2VictimAssets	Signature	Victim Asset
tcSignature2Victims	Signature	Victim
tcSubmitDomain	Domain	None
tcSubmitEmailAddress	Email Address	None
tcSubmitFile	Hash	None
tcSubmitIP	IPv4 Address	None
tcSubmitURL	URL	None
tcTag2ASN	Tag	AS
tcTag2Adversaries	Tag	Adversary
tcTag2CIDR	Tag	Netblock
tcTag2Campaigns	Tag	Campaign
tcTag2Documents	Tag	Document
tcTag2Email	Tag	Email
tcTag2EmailAddresses	Tag	Email Address
tcTag2Files	Tag	Hash
tcTag2Groups	Tag	Multiple
tcTag2Hosts	Tag	Domain
tcTag2IPAddresses	Tag	IP Address
tcTag2Incidents	Tag	Incident
tcTag2Indicators	Tag	Multiple
tcTag2Mutex	Tag	Mutex

tcTag2RegistryKey	Tag	Registry Entry
tcTag2Signatures	Tag	Signature
tcTag2Threats	Tag	Threat
tcTag2URLs	Tag	URL
tcTag2UserAgent	Tag	User Agent
tcThreat2ASN	Threat	AS
tcThreat2Adversary	Threat	Adversary
tcThreat2Attributes	Threat	Attributes
tcThreat2CIDR	Threat	Netblock
tcThreat2Campaign	Threat	Campaign
tcThreat2Document	Threat	Document
tcThreat2Domain	Threat	Domain
tcThreat2Email	Threat	Email Address
tcThreat2EmailGroup	Threat	Email
tcThreat2File	Threat	Hash
tcThreat2Groups	Threat	Multiple
tcThreat2IP	Threat	IP Address
tcThreat2Incident	Threat	Incident
tcThreat2Indicators	Threat	Multiple
tcThreat2Mutex	Threat	Mutex
tcThreat2RegistryKey	Threat	Registry Entry
tcThreat2Signature	Threat	Signature
tcThreat2Tags	Threat	Tag
tcThreat2Threat	Threat	Threat
tcThreat2URL	Threat	URL
tcThreat2UserAgent	Threat	User Agent
tcThreat2VictimAssets	Threat	Victim Asset
tcThreat2Victims	Threat	Victim
tcURL2Victim	URL	Victim
tcURL2VictimAsset	URL	Victim Asset
tcURLAdversary	URL	Adversary
tcURLAttributes	URL	Attributes
tcURLCampaign	URL	Campaign
tcURLDocument	URL	Document
tcURLEmail	URL	Email
tcURLGroups	URL	Multiple
tcURLIncidents	URL	Incident
tcURLOwners	URL	Owners
tcURLSignature	URL	Signature

tcURLTag	URL	Tag
tcURLThreat	URL	Threat
tcUserAgent2Victim	User Agent	Victim
tcUserAgent2VictimAsset	User Agent	Victim Asset
tcUserAgentAdversary	User Agent	Adversary
tcUserAgentAttributes	User Agent	Attributes
tcUserAgentCampaign	User Agent	Campaign
tcUserAgentDocument	User Agent	Document
tcUserAgentEmail	User Agent	Email
tcUserAgentGroups	User Agent	Multiple
tcUserAgentIncidents	User Agent	Incident
tcUserAgentOwners	User Agent	Owners
tcUserAgentSignature	User Agent	Signature
tcUserAgentTag	User Agent	Tag
tcUserAgentThreat	User Agent	Threat
tcVictimASNs	Victim	AS
tcVictimAdversaries	Victim	Adversary
tcVictimAssets	Victim	Victim Asset
tcVictimCIDRBlocks	Victim	Netblock
tcVictimCampaign	Victim	Campaign
tcVictimDocuments	Victim	Document
tcVictimDomains	Victim	Domain
tcVictimEmailAddresses	Victim	Email Address
tcVictimEmails	Victim	Email
tcVictimFiles	Victim	Hash
tcVictimIPs	Victim	IP Address
tcVictimIncidents	Victim	Incident
tcVictimMutexes	Victim	Mutex
tcVictimRegistryKeys	Victim	Registry Entry
tcVictimSignatures	Victim	Signature
tcVictimThreats	Victim	Threat
tcVictimURLs	Victim	URL
tcVictimUserAgents	Victim	User Agent