ThreatConnect® Activity Pack for ServiceNow® Orchestration

User Guide

Software Version 1.0

June 6, 2022

30063-01 EN Rev. B

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 Activity Pack for ServiceNow Orchestration provides a set of activities that can be leveraged from ServiceNow Orchestration workflows to interact with ThreatConnect's API and Playbooks. These activities provide a broad set of functionalities that can be used for automating threat intelligence and SOC/IR processes.

The following activities are available:

- Create ThreatConnect Incident
- Create ThreatConnect Indicator
- Get ThreatConnect Incident
- Get ThreatConnect Indicator
- Filter ThreatConnect Indicators
- ThreatConnect API Client
- Run ThreatConnect Playbook

EXAMPLE USE CASES

Threat Intelligence

- Look up intelligence in ThreatConnect and use the results in ServiceNow Orchestration workflows.
- Create ThreatConnect Tasks and Incidents from ServiceNow.
- Share ServiceNow Incidents and Observables back to ThreatConnect to generate new intelligence.

SOC/IR

- Trigger a Playbook in ThreatConnect from a ServiceNow workflow. Use the results to make further decisions in ServiceNow or update an Incident for an analyst's review.
- Increase confidence in automated decisions by leveraging ThreatConnect's intelligence collection as part of containment and response actions.

GETTING STARTED

Dependencies

ThreatConnect Dependencies

- ThreatConnect private instance with Playbooks (required for "Run ThreatConnect Playbook" activity)
- ThreatConnect license with API key (required for all other activities)

  NOTE: An Organization Administrator will need to create an API user within the Organization prior to ServiceNow interfacing with the ThreatConnect API. See the "Creating an API User" section of Creating User Accounts for instructions on creating an API user.

ServiceNow Dependencies

- ServiceNow Orchestration

Installation and Configuration

Users can install the ThreatConnect Orchestration Activity Pack from the ServiceNow Store or from within ServiceNow by using the **System Applications** menu.

After installing the application, follow these steps to configure the ThreatConnect Orchestration application:

1. Click **API Credentials** in the **ThreatConnect** menu (Figure 1) to view the **API Credentials** form (Figure 2).

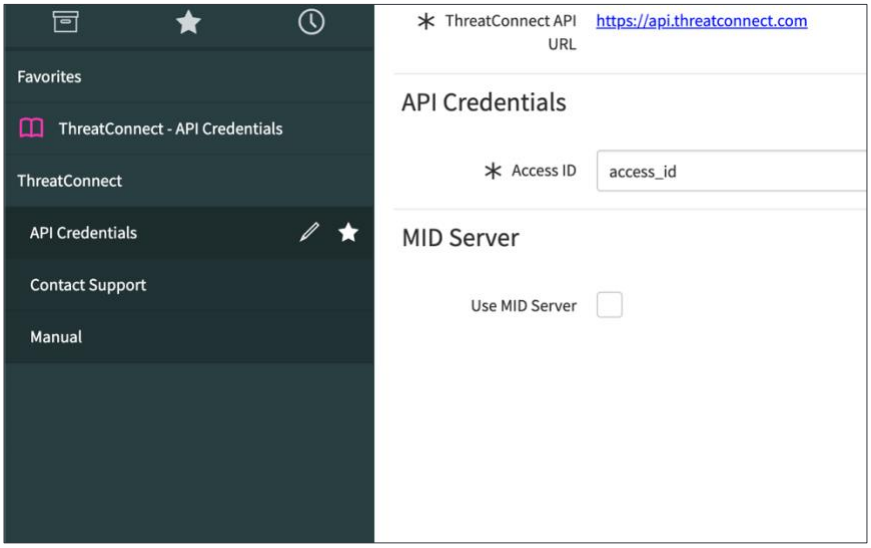

Figure 1

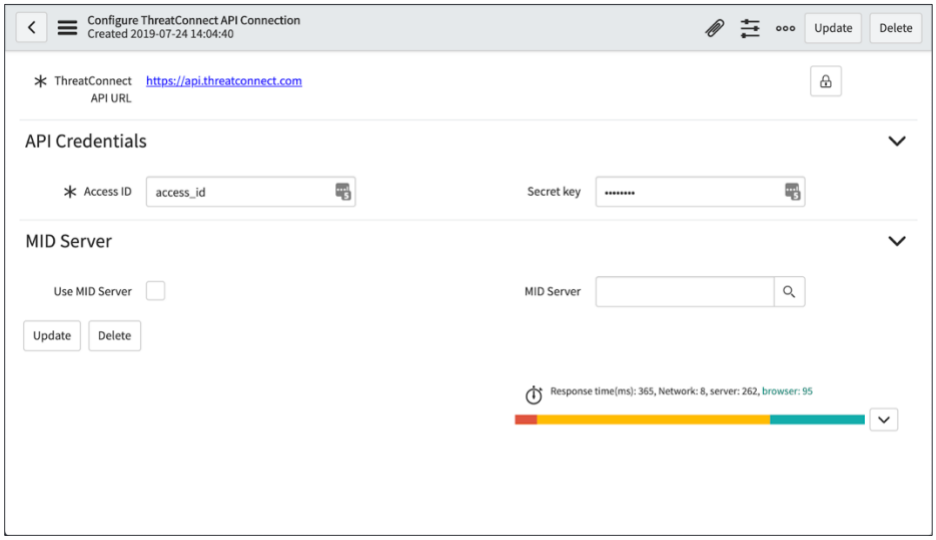

Figure 2

2. Input the **ThreatConnect API URL**, **Access ID**, and **Secret Key**. Then click the **Update** button in the upper right of the screen.

3. ThreatConnect activities can be found in the Workflow Editor by clicking the **Custom** tab and expanding the **ThreatConnect Activity Pack for Orchestration** section (Figure 3).

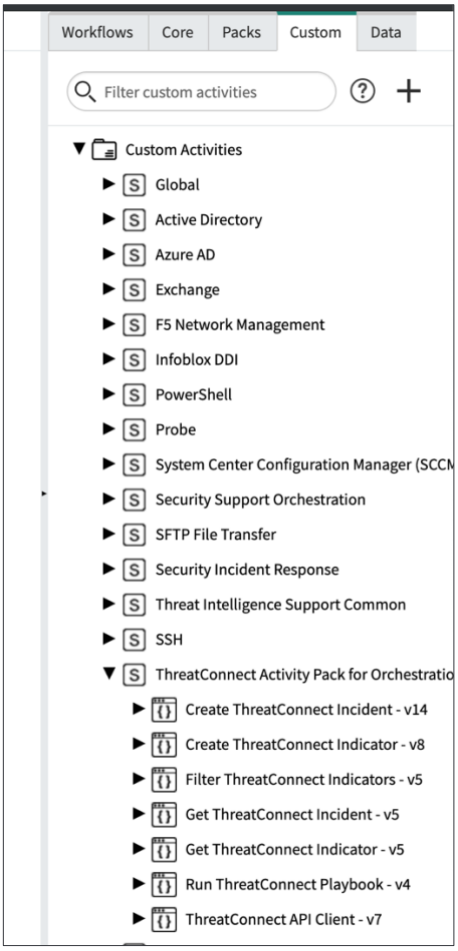

Figure 3

ACTIVITIES

Create ThreatConnect Incident

This activity creates an Incident Group in ThreatConnect. If desired, it can add Attributes, Tags, and Security Labels to the Incident. Table 1 provides the input parameters for the activity.

Table 1

Name	Description
Name	*Required* – This parameter is the name of the Incident.
Event Date	*Required* – This parameter is the event date of the Incident. It must be in the appropriate format. See https://docs.threatconnect.com/en/latest/rest_api/v2/groups/groups.html#group-fields.
Status	This parameter is the status of the Incident. It must be a valid Incident status in ThreatConnect. See https://docs.threatconnect.com/en/latest/rest_api/v2/groups/groups.html#group-fields.
Attributes	This parameter is an array of Attributes to add to the Incident. **Type** is the Attribute type, **Value** is the Attribute value, and **Displayed** (default value: **true**) is an optional field controlling display of the Attribute in ThreatConnect.
Tags	This parameter is an array of Tags to apply to the Incident.
Security Labels	This parameter is an array of Security Labels to apply to the Incident. Each Security Label must already exist in ThreatConnect.
Owner	This parameter is the owner in which to create the Incident. If left blank, the default owner will be the owner of the API account.

Table 2 provides the output variables for the activity.

Table 2

Name	Description
success	This variable will have a value of **true** (the Incident was successfully created) or **false** (the Incident was not successfully created).
id	This variable is the ID of the Incident (valid only when the **success** variable has a value of **true**).
raw_response	This variable is a String containing the raw response from ThreatConnect.
json_response	This variable is a JSON object containing the raw response from ThreatConnect.

Create ThreatConnect Indicator

This activity creates an Indicator in ThreatConnect. If desired, it can add Attributes, Tags, and Security Labels to the Indicator. Table 3 provides the input parameters for the activity.

Table 3

Name	Description
API Branch	*Required* – This parameter is the name of the API branch for the Indicator type. ***Note: This parameter is used to determine the type of Indicator. As such, it must match the API branch of an Indicator type defined in ThreatConnect.***
Fields	*Required* – This parameter is the Indicator fields for the desired Indicator type (e.g., for an Address Indicator, an **ip** field is required).
Attributes	This parameter is an array of Attributes to add to the Indicator. **Type** is the Attribute type, **Value** is the Attribute value, and **Displayed** (default value: **true**) is an optional field controlling display of the Attribute in ThreatConnect.
Tags	This parameter is an array of Tags to apply to the Indicator.
Security Labels	This parameter is an array of Security Labels to apply to the Incident. Each Security Label must already exist in ThreatConnect.
Owner	This parameter is the owner in which to create the Indicator. If left blank, the default owner will be the owner of the API account.
MID Server Name	This parameter is the MID server to use (if any) for this request.

Table 4 provides the output variables for the activity.

Table 4

Name	Description
success	This variable will have a value of **true** (the Indicator was successfully created) or **false** (the Indicator was not successfully created).
indicator	This variable is a JSON object containing the Indicator.
raw_response	This variable is a String containing the raw response from ThreatConnect.
json_response	This variable is a JSON object containing the raw response from ThreatConnect.

Filter ThreatConnect Indicators

This activity retrieves Indicators from ThreatConnect using the filter API. It returns one or more results. Table 5 provides the input parameters for the activity.

Table 5

Name	Description
API Branch	*Required* – This parameter is the name of the API branch to which to apply filters. **/indicators** is the default value and will filter Indicators of all types. **/indicators/addresses** will filter only Address Indicators.
Filters	*Required* – This parameter is the filters to apply. See https://docs.threatconnect.com/en/latest/rest_api/v2/indicators/indicators.html#filtering-indicators.
Or Filters	If this parameter is enabled, multiple filters will be treated with "or" logic. If it is not enabled, multiple filters will be treated with "and" logic.
Owner	This parameter is the ThreatConnect owner from which to retrieve Indicators.

Table 6 provides the output variables for the activity.

Table 6

Name	Description
success	This variable will have a value of **true** (the API call succeeded) or **false** (the API call failed).
indicator	This variable is an array of returned Indicators in JSON object format.
raw_response	This variable is an array of Strings containing the raw responses from ThreatConnect.
json_response	This variable is a JSON object containing the raw responses from ThreatConnect.

Get ThreatConnect Incident

This activity retrieves an Incident from ThreatConnect by name or by ID. If both name and ID are given, ID will be used. Note that if a name is used, more than one Incident will be retrieved from ThreatConnect if more than one Incident with that name exists in the specified owner. Table 7 provides the input parameters for the activity.

Table 7

Name	Description
Name	This parameter is the name of the Incident to retrieve.
ID	This parameter is the ID of the Incident to retrieve.
Include Additional	If this parameter is enabled, Attributes, Security Labels, and Tags for the Incident will be retrieved.
Owner	This parameter is the ThreatConnect owner from which to retrieve the Incident.

Table 8 provides the output variables for the activity.

Table 8

Name	Description
success	This variable will have a value of **true** (the Incident was successfully retrieved) or **false** (the Incident was not successfully retrieved).
raw_response	This variable is a String containing the raw response from ThreatConnect.
json_response	This variable is a JSON object containing the raw response from ThreatConnect.
incident	This variable is a JSON object containing the retrieved Incident.

Get ThreatConnect Indicator

This activity retrieves an Indicator from ThreatConnect. This activity always outputs a maximum of one result, whereas the "Filter ThreatConnect Indicators" activity may output more than one result. Table 9 provides the input parameters for the activity.

Table 9

Name	Description
Indicator	This parameter is the Indicator to retrieve.
Api Branch	This parameter is the API branch for the Indicator type.
Include Additional	If this parameter is enabled, Attributes, Security Labels, and Tags for the Indicator will be retrieved.
Owner	This parameter is the ThreatConnect owner from which to retrieve the Indicator.

Table 10 provides the output variables for the activity.

Table 10

Name	Description
success	This variable will have a value of **true** (the Indicator was successfully retrieved) or **false** (the Indicator was not successfully retrieved).
raw_response	This variable is a String containing the raw response from ThreatConnect.
json_response	This variable is a JSON object containing the raw response from ThreatConnect.
indicator	This variable is a JSON object containing the retrieved Indicator.

Run ThreatConnect Playbook

This activity triggers a ThreatConnect Playbook with a WebHook Trigger. Table 11 provides the input parameters for the activity.

Table 11

Name	Description
Playbook URL	This parameter is the URL for the Playbook's WebHook Trigger.
HTTP Method	This parameter is the HTTP method to use.
Request Body	This parameter is the data to send to the Playbook in the request body.
Query Parameters	This parameter is the data to send to the Playbook as query parameters.
Playbook Username	This parameter is the username for accessing the Playbook.
Playbook Password	This parameter is the password for accessing the Playbook.

Table 12 provides the output variables for the activity.

Table 12

Name	Description
response_status	This variable is the HTTP status code returned by the Playbook.
raw_response	This variable is a String containing the raw response from ThreatConnect.
json_response	This variable is a JSON object containing the raw response from ThreatConnect.

ThreatConnect API Client

This activity provides general-purpose access to the ThreatConnect API. Table 13 provides the input parameters for the activity.

Table 13

Name	Description
Path	This parameter is the URL path to which to send a request. This value will be appended to **ThreatConnect API URL** as defined in the **API Credentials** form.
HTTP Method	This parameter is the HTTP method to use for the request.
Body	This parameter is the data to send in the request body.
Query Parameters	This parameter is the data to send to the Playbook as query parameters.

Table 14 provides the output variables for the activity.

Table 14

Name	Description
success	This variable will have a value of true (the request was successful) or false (the request was not successful).
raw_response	This variable is a String containing the raw response from ThreatConnect.
json_response	This variable is a JSON object containing the raw response from ThreatConnect.