ThreatConnect™

ThreatConnect® App for ServiceNow® Security Operations

User Guide

Software Version 1.0

November 19, 2019

30062-01 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 app for ServiceNow Security Operations queries ThreatConnect intelligence and analytics collections using the Threat Lookup and Enrich Observables capabilities in ServiceNow. These features give analysts working inside ServiceNow the information they need to get relevant and actionable insights from intelligence sources within ThreatConnect.

EXAMPLE USE CASES

Threat Intelligence

- Operationalize intelligence from ThreatConnect into other parts of the security organization.

SOC/IR

- Provide SOC analysts working in ServiceNow the information they need to get relevant and actionable insights from intelligence sources within ThreatConnect.

GETTING STARTED

Dependencies

ThreatConnect Dependencies

- ThreatConnect license with an API key (any version)

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

ServiceNow Dependencies

- ServiceNow Security Incident Response
- ServiceNow Orchestration
- ServiceNow Threat Intelligence
- ThreatConnect Activity Pack for ServiceNow Orchestration
- ServiceNow MID Server (optional for ThreatConnect On Premises instances)

Installation and Configuration

The ThreatConnect app for ServiceNow Security Operations can be installed from the ServiceNow Store or from within ServiceNow by using the **System Applications** menu. After installing the app, follow these steps to configure the ThreatConnect Threat Lookup and Enrich Observables capabilities:

1. Select **Integration Configurations** from the **Integrations** section of the **Security Operations** menu (Figure 1) to go to the **Security Integrations** page.

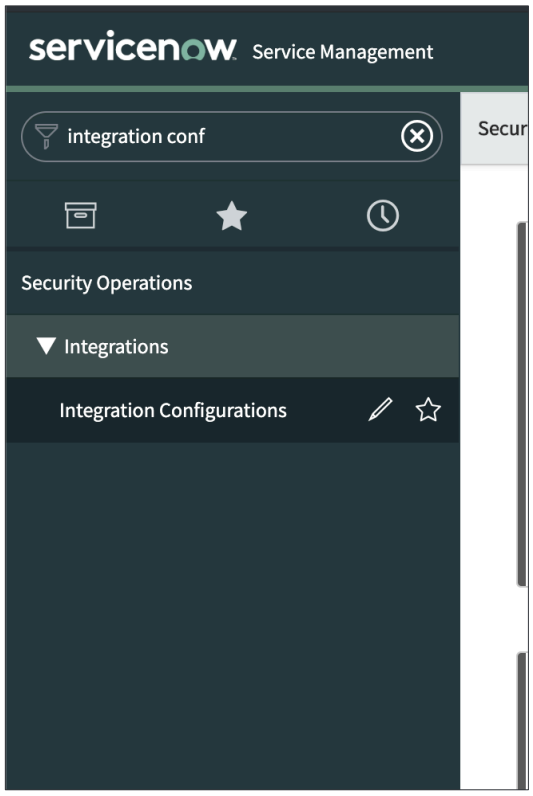

Figure 1

2. On the **Security Integrations** page, click **Configure** on the **ThreatConnect** card (Figure 2).

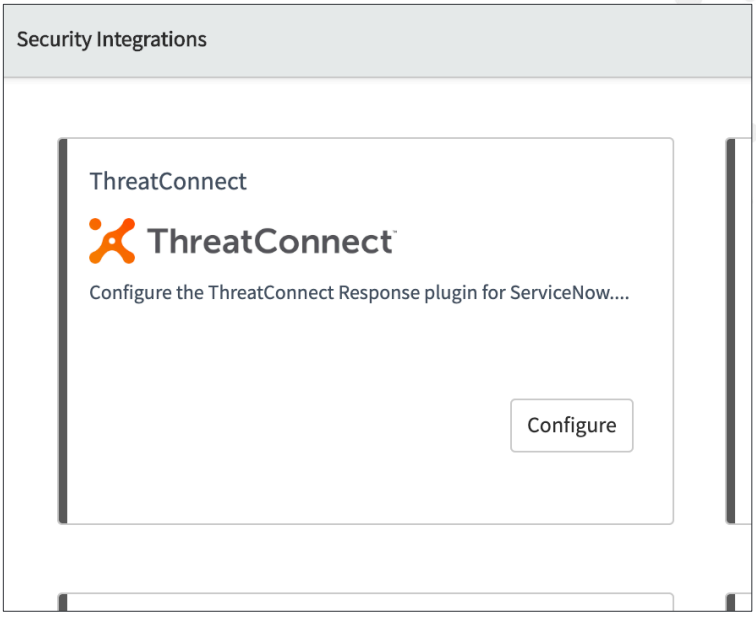

Figure 2

3. Configuration options for the ThreatConnect Response plugin for ServiceNow will be displayed (Figure 3).

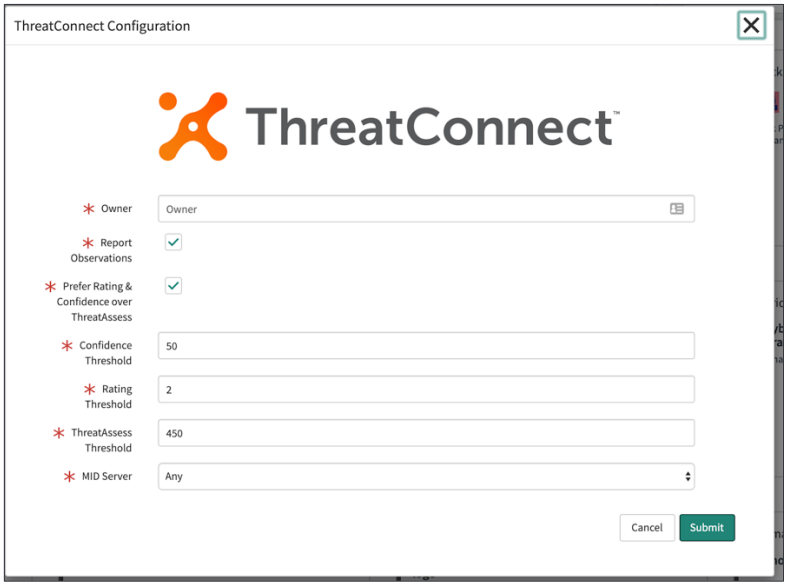

Figure 3

- **Owner**: Enter the ThreatConnect owner to use for the Threat Lookup and Enrich Observables capabilities. If this field is left blank, then the default owner for the API user will be used.
- **Report Observations**: If this checkbox is selected, then an observation will be recorded for any Indicator found in ThreatConnect during the Enrich Observables operation.

- **Prefer Rating & Confidence over ThreatAssess**: If this checkbox is selected, the Indicator's Threat Rating and Confidence Rating will be used to make the determination in the Threat Lookup implementation rather than the Indicator's ThreatAssess score.
- **Confidence Threshold**: Enter the Confidence Rating threshold above which an Indicator will be considered "malicious" by the Threat Lookup implementation.
- **Rating Threshold**: Enter the Threat Rating threshold above which an Indicator will be considered "malicious" by the Threat Lookup implementation.
- **ThreatAssess Threshold**: Enter the ThreatAssess threshold above which an Indicator will be considered "malicious" by the Threat Lookup implementation.
- **MID Server**: Select the MID Server to use for requests to ThreatConnect.

Follow these steps to show data from the Enrich Observables implementation:

1. Navigate to any Security Incident. From the menu, select **Configure** and then **Related Lists** (Figure 4).

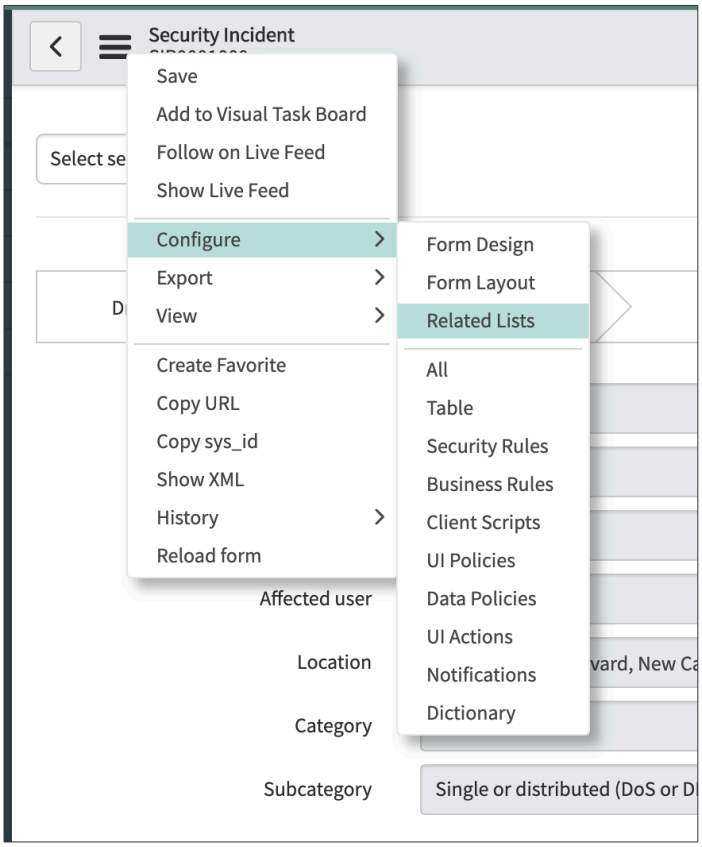

Figure 4

2. Move **ThreatConnect Enrichment Results** to the **Selected** list, and then place it directly after **Compromised User Info** (Figure 5). Click the **Save** button.

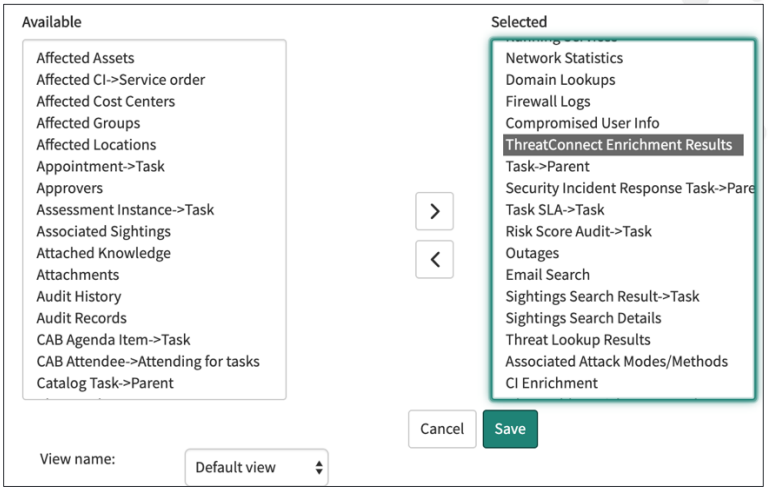

Figure 5

3. Navigate to **UI Scripts** under the **System UI** menu. Find and edit the script named **sn_si.SecurityIncidentConstants** (Figure 6).

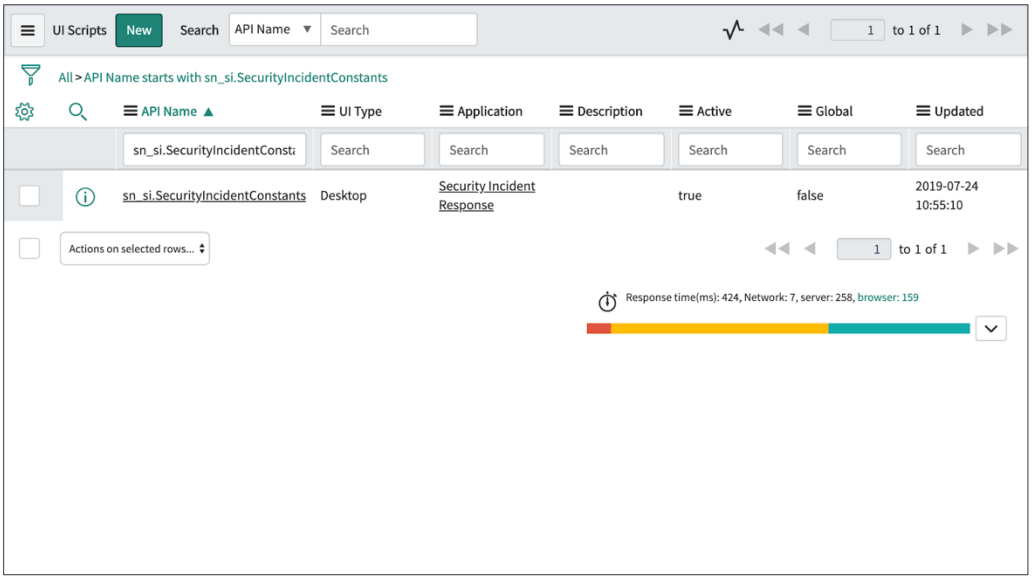

Figure 6

4. Edit the **Script** input by adding the following new element to the end of the **ENRICHMENT_DATA** array (Figure 7):

```
"REL:dd0fc6d6dbb27b001908176a489619d3", // ThreatConnect Enrichments
```

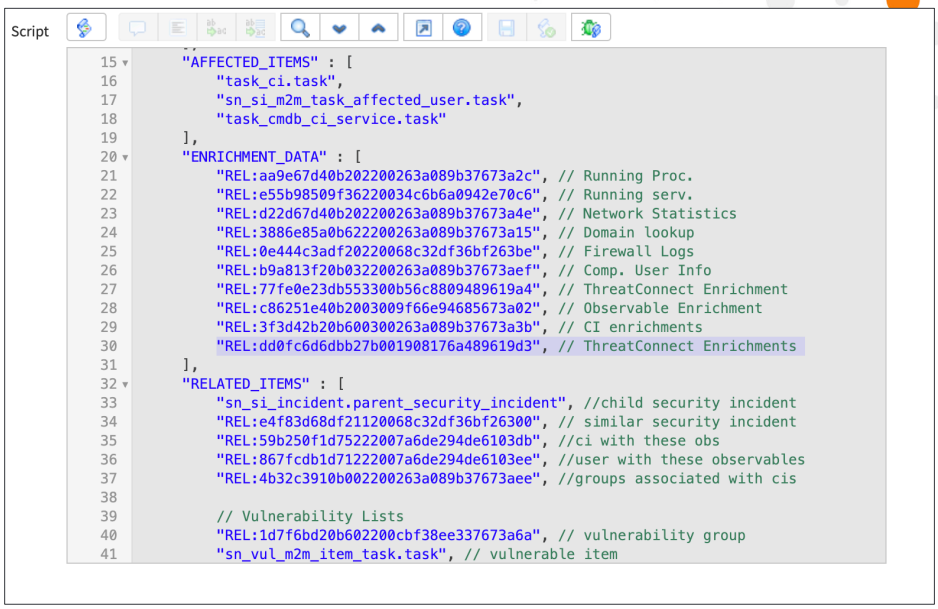

Figure 7

5. Click the **Update** button at the top right of the screen (Figure 8).

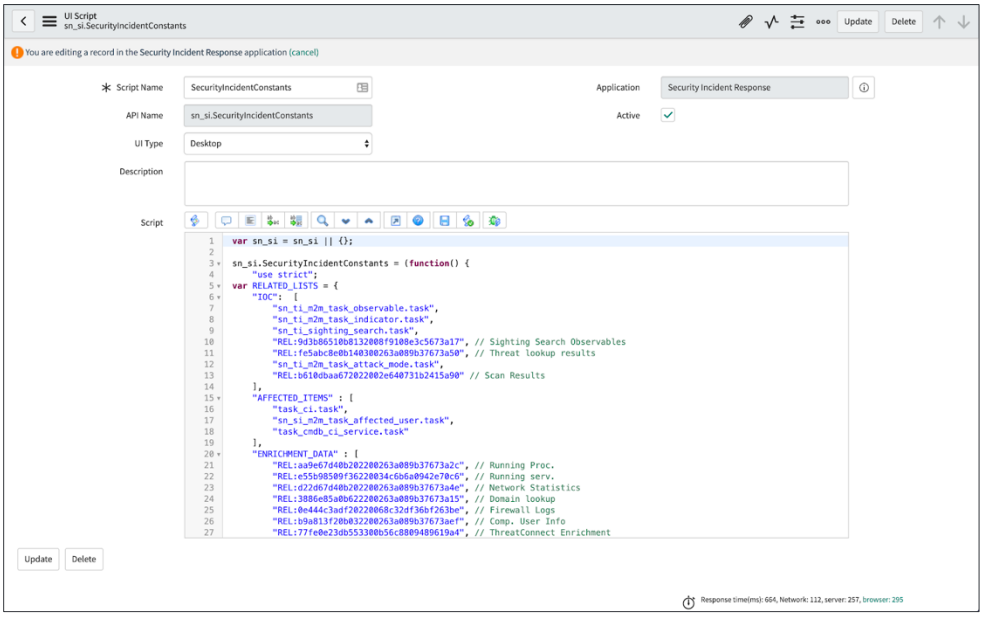

Figure 8

USAGE

When an observable is added to a Security Incident, the ThreatConnect Threat Lookup and Enrich Observables workflows will be automatically run. To see ThreatConnect Threat Lookup data, view any Security Incident and then scroll to the **Threat Lookup Results** related list (Figure 9).

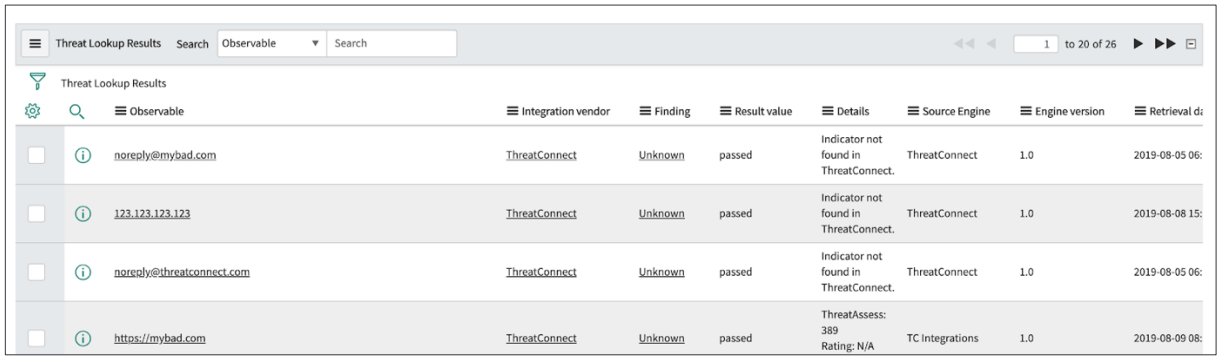

Figure 9

To view ThreatConnect Enrichment data, scroll to the **ThreatConnect Enrichment Results** related list (Figure 10), or, if tabbed forms are enabled, select **Show Enrichment Data** in the **Related Links** list.

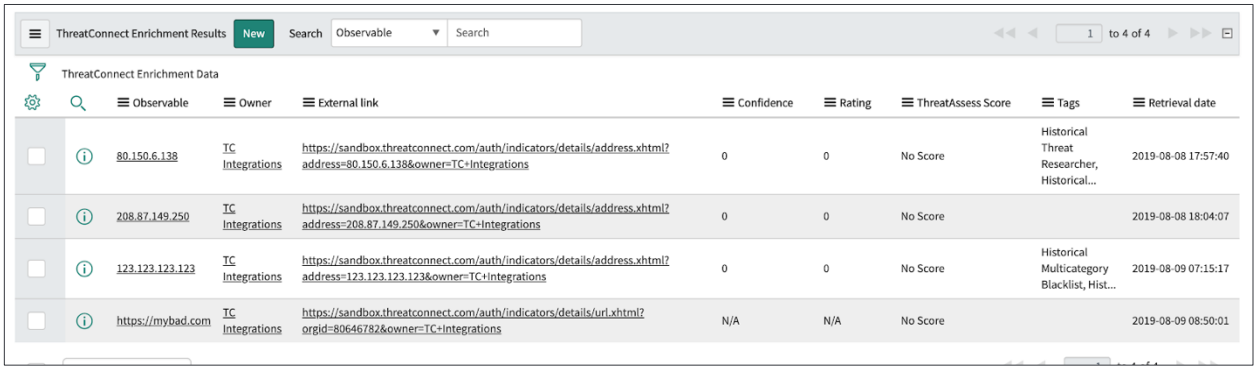

Figure 10