



ThreatConnect® App for ServiceNow® Security Operations

User Guide

Software Version 1.0

November 19, 2019

30062-01 EN Rev. A



©2019 ThreatConnect, Inc.

ThreatConnect® is a registered trademark of ThreatConnect, Inc.

ServiceNow® is a registered trademark of ServiceNow, Inc.





Table of Contents

OVERVIEW	4
EXAMPLE USE CASES	4
Threat Intelligence.....	4
SOC/IR.....	4
GETTING STARTED	4
Dependencies	4
ThreatConnect Dependencies	4
ServiceNow Dependencies	5
Installation and Configuration.....	6
USAGE	11



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.

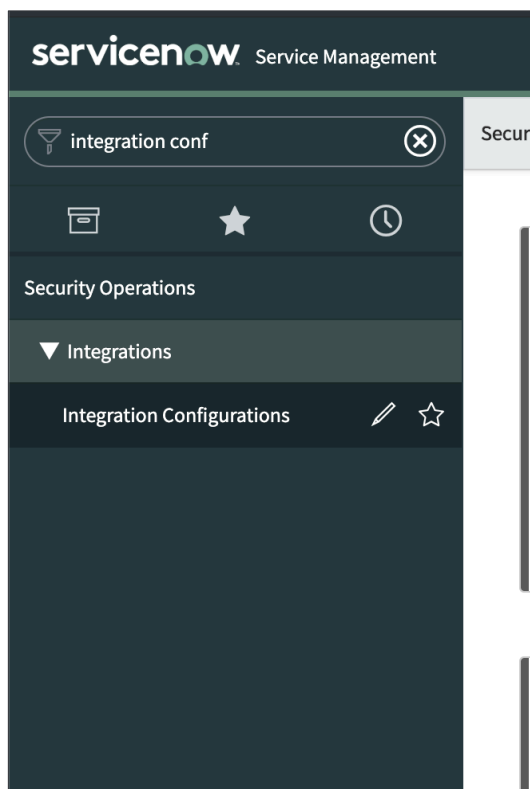


Figure 1

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

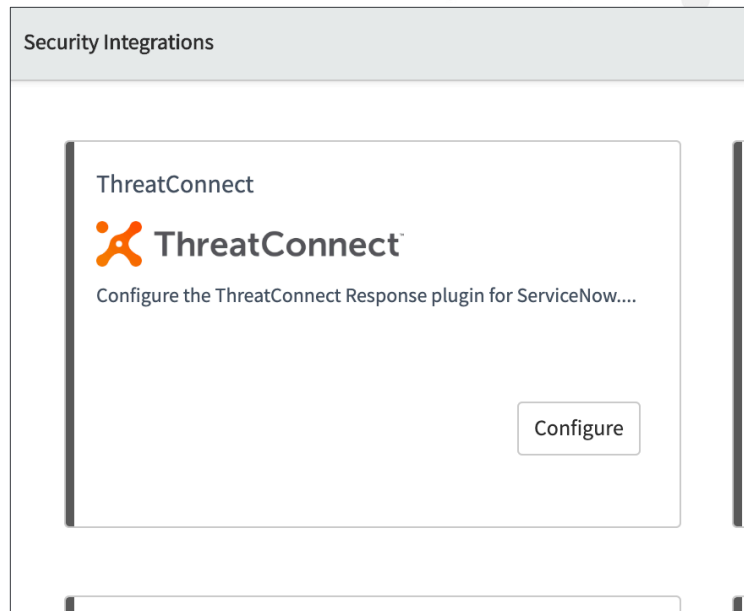


Figure 2

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

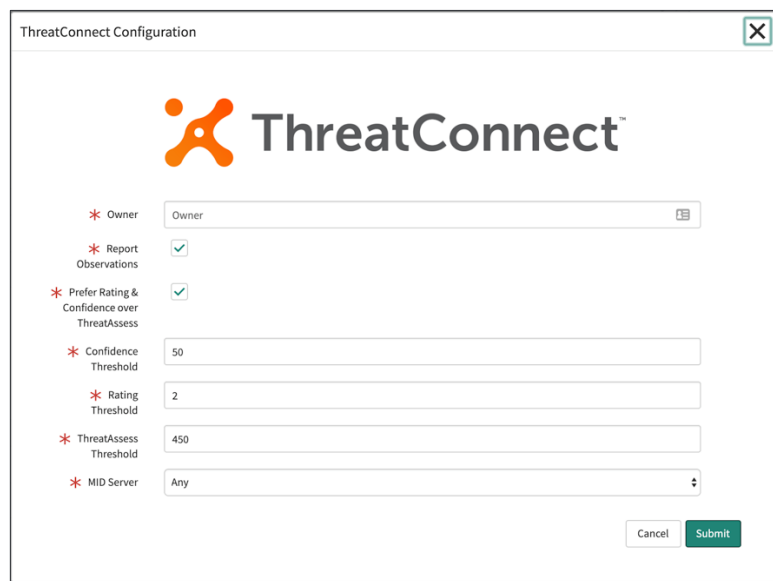


Figure 3

- **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).

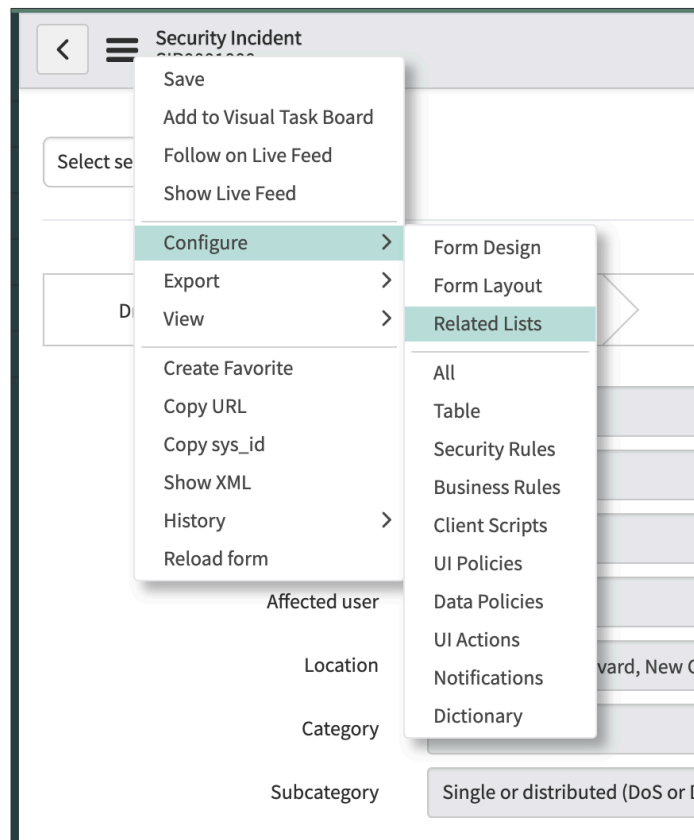


Figure 4

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

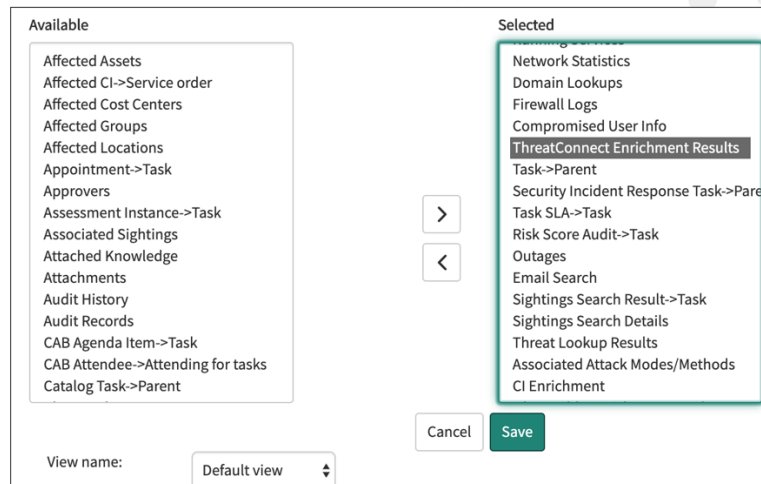


Figure 5

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

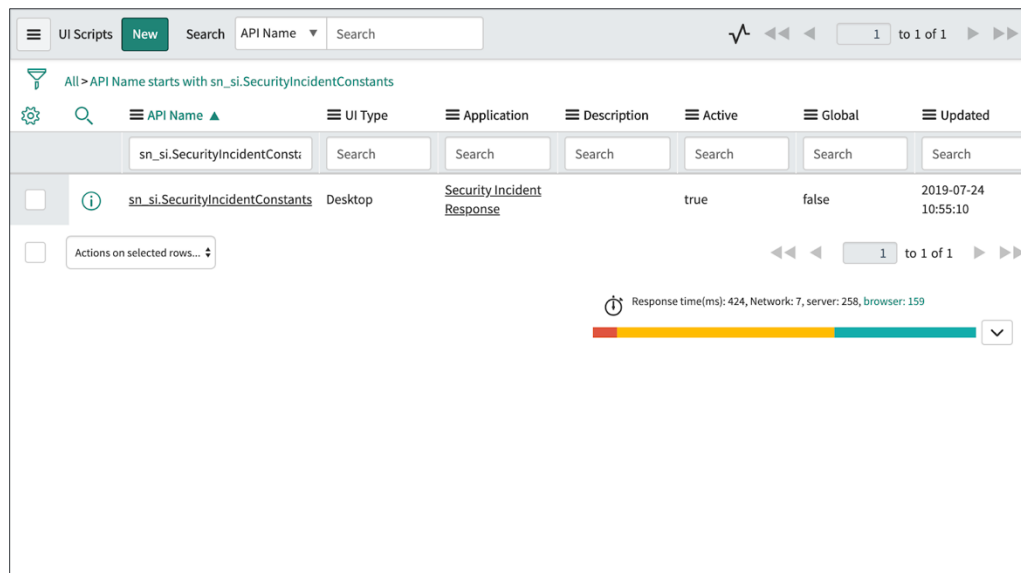


Figure 6

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
```



```
Script
15  "AFFECTED_ITEMS" : [
16    "task_ci.task",
17    "sn_si_m2m_task_affected_user.task",
18    "task_cmdb_ci_service.task"
19  ],
20  "ENRICHMENT_DATA" : [
21    "REL:aa9e67d40b202200263a089b37673a2c", // Running Proc.
22    "REL:e55b98509f36220034c6b6a0942e70c6", // Running serv.
23    "REL:d22d67d40b202200263a089b37673a4e", // Network Statistics
24    "REL:3886e85a0b622200263a089b37673a15", // Domain lookup
25    "REL:0e444c3adf20220068c32df36bf263be", // Firewall Logs
26    "REL:b9a813f20b032200263a089b37673aef", // Comp. User Info
27    "REL:77fe0e23db553300b56c8809489619a4", // ThreatConnect Enrichment
28    "REL:c86251e40b2003009f66e94685673a02", // Observable Enrichment
29    "REL:3f3d42b20b600300263a089b37673a3b", // CI enrichments
30    "REL:dd0fc6d6bb27b001908176a489619d3", // ThreatConnect Enrichments
31  ],
32  "RELATED_ITEMS" : [
33    "sn_si_incident.parent_security_incident", //child security incident
34    "REL:e4f83d68df21120068c32df36bf26300", // similar security incident
35    "REL:59b250f1d75222007a6de294de6103db", //ci with these obs
36    "REL:867fcd1d71222007a6de294de6103ee", //user with these observables
37    "REL:4b32c3910b002200263a089b37673aee", //groups associated with cis
38
39    // Vulnerability Lists
40    "REL:1d7f6bd20b602200cbf38ee337673a6a", // vulnerability group
41    "sn_vul_m2m_item_task.task", // vulnerable item
```

Figure 7

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

UI Script
sn_si.SecurityIncidentConstants

You are editing a record in the Security Incident Response application (cancel)

* Script Name: SecurityIncidentConstants Application: Security Incident Response

API Name: sn_si.SecurityIncidentConstants Active: ☒

UI Type: Desktop

Description:

Script

```
1  var sn_si = sn_si || {};
```

```
2  sn_si.SecurityIncidentConstants = (function() {
```

```
3  "use strict";
```

```
4  var RELATED_LISTS = {
```

```
5  "IOC": [
```

```
6    "sn_ti_m2m_task_observable.task",
```

```
7    "sn_ti_m2m_task_indicator.task",
```

```
8    "sn_ti_sighting_search.task",
```

```
9    "REL:9d3b6510b6132008f91806c5673a17", // Sighting Search Observables
```

```
10    "REL:fesabc8e0b140380263a089b37673a50", // Threat lookup results
```

```
11    "sn_ti_m2m_task_attack_mode.task",
```

```
12    "REL:b618dbaa672022002640731b2415a908" // Scan Results
```

```
13  ],
```

```
14  "AFFECTED_ITEMS" : [
```

```
15    "task_ci.task",
```

```
16    "sn_si_m2m_task_affected_user.task",
```

```
17    "task_cmdb_ci_service.task"
```

```
18  ],
```

```
19  "ENRICHMENT_DATA" : [
```

```
20    "REL:aa9e67d40b202200263a089b37673a2c", // Running Proc.
```

```
21    "REL:e55b98509f36220034c6b6a0942e70c6", // Running serv.
```

```
22    "REL:d22d67d40b202200263a089b37673a4e", // Network Statistics
```

```
23    "REL:3886e85a0b622200263a089b37673a15", // Domain lookup
```

```
24    "REL:0e444c3adf20220068c32df36bf263be", // Firewall Logs
```

```
25    "REL:b9a813f20b032200263a089b37673aef", // Comp. User Info
```

```
26    "REL:77fe0e23db553300b56c8809489619a4", // ThreatConnect Enrichment
```

```
27  ]
```

Update Delete

Response time(ms): 664, Network: 112, server: 257, browser: 265

Figure 8



Threat Lookup Results									
Threat Lookup Results									
Observable	Integration vendor	Finding	Result value	Details	Source Engine	Engine version	Retrieval date		
noreply@mybad.com	ThreatConnect	Unknown	passed	Indicator not found in ThreatConnect.	ThreatConnect	1.0	2019-08-05 06:00		
123.123.123.123	ThreatConnect	Unknown	passed	Indicator not found in ThreatConnect.	ThreatConnect	1.0	2019-08-08 15:00		
noreply@threatconnect.com	ThreatConnect	Unknown	passed	Indicator not found in ThreatConnect.	ThreatConnect	1.0	2019-08-05 06:00		
https://mybad.com	ThreatConnect	Unknown	passed	ThreatAssess: 389 Rating: N/A	TC Integrations	1.0	2019-08-09 08:00		

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