servicenow

APPLICATION INSTALLATION AND CONFIGURATION GUIDE

Recorded Future for Threat Intelligence Security Center

servicenow

Table of Contents

servicenow

1. Overview

This guide will help customers install and configure the Recorded Future for Threat Intelligence Security Center (TISC) application on their ServiceNow instance. It also details any application dependencies.

2. Application Dependencies

- Threat Intelligence Security Center

3. User Roles

This application uses the default security roles of the Threat Intelligence Security Center to handle app permissions.

- **sn_sec_tisc.admin** - Required to configure the application.
- **sn_sec_tisc.analyst** - Required to run the application.

4. Installation and Configuration

1. Search for 'Recorded Future for Threat Intelligence Security Center' application in the ServiceNow store
2. Click on 'View Details' and Install the application
3. Make sure the current user has the **sn_sec_tisc.admin** role before continuing with below steps
4. Go to the Integrations section in the Threat Intelligence Security Center within ServiceNow
5. Goto 'All Integrations' under Enrichment Integrations
6. Click on 'Configure new enrichment' button and select 'Observable Enrichment' capability
7. Click Next and select 'Recorded Future for Threat Intelligence Security Center' from the list of available integrations
8. You will be redirected to 'Create New Enrichment Integration' page for 'Recorded Future for Threat Intelligence Security Center'
9. Provide the following details:
    a. Name: Input an appropriate name for the integration
    b. API Key: Input the Recorded Future API token here
10. Click on Save to create the enrichment integration

5. Testing the configuration

Perform the following steps for enrichment of an indicator to test the connection and ensure successful configuration:

1. Make sure the current user has either the **sn_sec_tisc.admin** or the **sn_sec_tisc.analyst** role before continuing with below steps
2. Go to the 'Threat Intel Library' section in 'Threat Intelligence Security Center'
3. Click on the value of an indicator of a supported type (eg. IPv4 address)
4. Go to the 'Enrichment Results' section and click on 'Observable Enrichment Results'
5. Click on the 'Run Observable Enrichment' button and select the integration created in section 3 before submitting the enrichment operation
6. If the configuration is successful, you should see a new record under 'Observable Enrichment Results'
7. Click on the Number of the new record created post enrichment operation using your integration and verify if you are able to fetch the context from Recorded Future

6. Support and Troubleshooting

1. If you see errors while saving the integration in section 3, make sure the following fields are populated:
    a. API Token: with a valid API token from Recorded Future.
    b. API URL: set to the default value **https://api.recordedfuture.com/gw**
2. If you are having issues with the data or with the connection to the Recorded Future API, please contact support@recordedfuture.com

End of Document