
servicenow

Safe harbor notice for forward-looking statements

This presentation may contain "forward-looking" statements that are based on our beliefs and assumptions and on information currently available to us only as of the date of this presentation. Forward-looking statements involve known and unknown risks, uncertainties, and other factors that may cause actual results to differ materially from those expected or implied by the forward-looking statements. Further information on these and other factors that could cause or contribute to such differences include, but are not limited to, those discussed in the section titled "Risk Factors," set forth in our most recent Annual Report on Form 10-K and Quarterly Report on Form 10-Q and in our other Securities and Exchange Commission filings. We cannot guarantee that we will achieve the plans, intentions, or expectations disclosed in our forward-looking statements, and you should not place undue reliance on our forward-looking statements. The information on new products, features, or functionality is intended to outline our general product direction and should not be relied upon in making a purchasing decision, is for informational purposes only, and shall not be incorporated into any contract, and is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. The development, release, and timing of any features or functionality described for our products remains at our sole discretion. We undertake no obligation, and do not intend, to update the forward-looking statements.

TISC Overview

Threat Intelligence Security Center (TISC) provides technology solution for aggregation, management and operationalization of threat intelligence. The platform has capabilities to collect and process various threat intelligence feeds and a workspace to analyse, collaborate, action, and share the necessary information.

Key features

- Data collection from different sources and in various formats.
- Integrations with OSINT and Premium Feeds.
- Data processing to normalize, de-duplicate, and aggregate data.
- Threat Intelligence Library, a repository for curated intelligence with basic automated correlation, internal Intelligence and observable Enrichment operations.
- Customizable threat score calculator for observables.
- Threat Analyst workbench with MITRE ATT&CK Framework for threat hunting and case investigations.
- Integration with ServiceNow Security Incident Response (SIR)

ServiceNow Confidential

Recorded Future – STIX/TAXII Feed Configuration

Understanding STIX TAXII

Structured Threat Information Expression (STIX) is a language and serialization format used to exchange cyber threat intelligence (CTI). Trusted Automated Exchange of Intelligence Information (TAXII) is a protocol used to exchange cyber threat intelligence (CTI) over HTTPS.

With STIX, all aspects of suspicion, compromise, and attribution are represented as objects and descriptive relationships. STIX information can be visually represented for an analyst or stored as JSON to be quickly machine readable.

Cyber Threat Intelligence (CTI) was chartered to define a set of information representations and protocols to address the need to model, analyze, and share cyber threat intelligence. The CTI is primarily focused on development and standardization of Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII).

Configure a new TAXII Feed

You can maintain TAXII feeds for sharing STIX-formatted information. Each TAXII feed contains one or more TAXII collections.

Before you begin
Role required: sn_sec_tisc.admin

Procedure

1. Navigate to **Workspaces** > **Threat Intelligence Security Center**.
2. Click on **Integrations** icon.
3. Select **Threat Intel Feeds** > **STIX TAXII** > **TAXII Feeds**.

   Note: Configure TAXII feed to serve as a profile for all the TAXII Collections within.

4. Click **Configure new source**.
   The Configure new TAXII Feed page is displayed.
5. On the form, fill in the fields.

Recorded Future – STIX/TAXII Feed Configuration

Create New Data Source

Field	Description
Name	Enter a name for the feed.
Description	Description of the feed.
Source Type	The type of source such as Open Source, Premium Source, and so on provided for the feed. The available source types are: ◦ Government ◦ ISACs ◦ Open Source ◦ Premium Source ◦ Other Source
Logo	Attach the logo of the source feed.
Industry	Select the industry category such as Aerospace, Agriculture, and so on.

Fill in the fields in the Configuration section, as appropriate.

Configuration

Field	Description
TAXII Version	Select the TAXII Version of the TAXII server that needs to be configured. Supported versions are 2.0 and 2.1.
Configuration Type	Provide a configuration type to fetch TAXII collections. Available values are: ◦ **Discovery Service URL**: Choose Discovery Service URL to fetch collections from all available API roots within the discovery service of the TAXII server. ◦ **API Root URL**: Choose API Root URL to fetch collections from the specific API root of the TAXII server.
Authentication	Select the required option from the drop down list if the authentication is required. The available options are: ◦ **None**: Select this option if there is no authentication required. ◦ **API Key**: Select this option to provide username and passowrd. ◦ **Basic**: Select this option to provide an API key. ◦ **Choose a REST message**: Select this option for any other type of

servicenow
Limited Access Release
Features in the release may or may not be productized

Field	Description
	authentication. The REST message options are: ▪ **Use REST Message**: Select this box if you need a REST message to build a pre-build REST Message. If you don't select then this will use the value in endpoint field. Click the lookup icon, and select the REST message from the list. ▪ **REST Method**: Select this box if you need a REST method. Click the lookup icon, and select the REST method from the list. **Note:** The REST message and REST method fields become available when the REST message option is selected.
URL	Enter either the TAXII Server Discovery Service URL or specific API Root URL based on the selected configuration type.
Advanced section	
Advanced	Select the check box to choose a different Integration script and Report Processor. Make sure the chosen scripts are compatible with the selected TAXII version. Based on the TAXII version and authentication, these scripts are auto populated by default.
Integration script	Invokes a call to the REST Endpoint URL API using the authentication parameters such as authentication type: User name/ Password/API Key and the headers to be passed with the request, and then the script fetches the observables or indicators STIX data that are available for the specific feed.

Limited Availability - Confidential - Do not distribute

ServiceNow Confidential

Recorded Future – STIX/TAXII Feed Configuration

Field	Description
	Note: The data that is fetched is the raw data only (no records are created) which will be attached to the integration process and can then be viewed under the **Integration Run** section. Within the base system following are the custom scripts includes, which are provisioned within the application for the integrations scripts: ◦ TAXIIV2_0QueryParamAPIKeyIntegrationScript ◦ TAXIIV2_0BasicAuthIntegrationScript ◦ TAXIIV2_1QueryParamAPIKeyIntegrationScript ◦ TAXIIV2_1BasicAuthIntegrationScript The default integration script is based on the feed type that you select. The script includes runs a simple REST call, saves the response as an attachment, and then returns the attachment to the processor.
Report processor	The report processor invokes a call to the REST Endpoint URL. Within the base system below is the custom scripts includes, which is provisioned within the application for the integrations scripts, **TAXIIV2CollectionDataProcessor**.

Fill in the fields in the Scheduling section, as appropriate.

Scheduling

Field	Description
Run Frequency of Collections	The scheduling interval which will be applied to the TAXII collection records. Run frequency for a TAXII collection can be modified in the TAXII collection form view if required. **Note:** This setting will be applied as default to all the TAXII collections that are fetched. There is an option to override the setting in TAXII Collections if required. For more information, see Scheduled Jobs and how to Automatically run a script of your choosing.

servicenow
Limited Access Release
Features in the release may or may not be productized

Field	Description
Fetch Data From	The start date from when the data needed to be fetched. **Note:** Scheduled runs will fetch data incrementally starting from this date onwards.

6. Click **Validate Connection**
   An information message is displayed that the TAXII Feed connection is successful. To fetch the collections proceed to the next step.
7. Click **Get TAXII Collections**.

   Note: If there are any errors, then an error message is displayed that an error occurred while fetching TAXII collections and check logs for more details.

   The TAXII Collections are displayed under the TAXII Collections section, and they are disabled by default.
8. Enable the TAXII Collections to retrieve the STIX objects available in these TAXII collections.

Limited Availability

ServiceNow Confidential

Benefits

- Provides **early warnings** about emerging threats and vulnerabilities. This allows organizations to proactively defend against potential attacks before they become widespread.
- Provides **contextualized information** about threats, offering a deeper understanding of the threat landscape, including the tactics, techniques, and procedures (TTPs) employed by threat actors.
- Deliver **customized and Actionable** Insights tailored to an organization's specific industry, geography, and technology stack.
- Provides **real-time updates** on the latest threats, vulnerabilities, and indicators of compromise (IoCs).
- Offers **comprehensive coverage**, monitoring a wide range of sources including the dark web, open-source intelligence, and closed forums..
- Provides valuable **Incident Response Support** by offering additional context and information that helps organizations understand the scope and severity of an incident, facilitating a more effective and targeted response.


servicenow