LOGPOINT

Integrations

StixTaxii

*V*6.3.1

CONTENTS

CHAPTER

ONE

STIXTAXII

StixTaxii is a threat intelligence source that fetches Cyber Threat Intelligence (CTI) data written in *STIX* format from a *TAXII* server. You can enrich incoming logs of Logpoint with this fetched data by using the Threat Intelligence process command.

StixTaxii support *STIX/TAXII* versions 1.0, 2.0 and 2.1.

CHAPTER

TWO

INSTALLING STIXTAXII

Prerequisites

- LogPoint v7.6.0 or later
- Threat Intelligence v6.4.0 or later

To install StixTaxii:

1. Download the .pak file from the *Download* section in Release Notes.
2. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
3. Click **Import**.
4. **Browse** to the downloaded .pak file.
5. Click **Upload**.

After installing StixTaxii, you can find it under *Settings >> System Settings>> Plugins*.

CHAPTER

THREE

UNINSTALLING STIXTAXII

You must first remove StixTaxii configuration and then uninstall it.

To remove the configurations:

1. Go to *Settings >> Configuration* from the navigation bar and click **STIX/TAXII**.
2. Click **Settings** and disable **Enable Source**.
3. Click **Submit**.

To uninstall StixTaxii:

1. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
2. Click the **Uninstall** (🗑) icon in **Actions** of StixTaxii.

CHAPTER

FOUR

CONFIGURING STIXTAXII

Go to *Settings >> Configuration* from the navigation bar and click **STIX/TAXII**.

4.1 General Information

General Information consists of all the details about the fetched Cyber Threat Intelligence (CTI) data. You can find the total number of data fetched in **Total Records** and the status of fetched data in **Status**. You can also find the most recent attempt made to fetch data in **Last Fetch Attempt** and the last date and time when data was successfully fetched in **Last Fetch Date**.

1. Go to *Settings >> Configuration* from the navigation bar and click **STIX/TAXII**.
2. Click **General Information**.

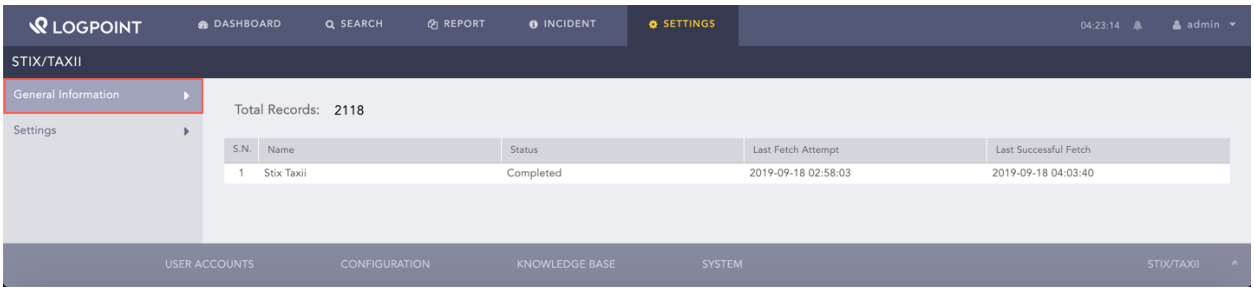

Fig. 1: General Information

4.2 Settings

For StixTaxii to fetch data, an initial setup where details like server endpoints, authentication credentials and data filtering options must be configured. You can perform this setup from Settings.

1. Go to *Settings >> Configuration* from the navigation bar and click **STIX/TAXII**.

2. Click **Settings**.
3. Select **Enable Source** to activate StixTaxii.
4. Enter the **Discovery URL**, which is the location of the discovery service in the *TAXII* server.
5. Select a *STIX* **Version**.

    5.1. If you select **1.X**, you must also select the **Fetch From** date. StixTaxii fetches data from the specified date.

    5.2. If you select **2.0** and **2.1**, you can **Enable Pagination** to separate data fetching into pages.

        5.2.1. Select the number of data to be retrieved in a page in **Fetch Per Page**.

6. Select **Fetch Interval** in either hours or days.
7. Select **Enable Basic Authentication** if the *TAXII* server uses basic authentication.
8. In **User Credentials**, enter *TAXII* server **User Name** and **Password**.
9. Select **Enable SSL Authentication** if the *TAXII* server uses SSL authentication.
10. In **SSL Configuration**:

    10.1. Upload the SSL certificate file in the **Certification File**.

    10.2. Upload the SSL key file in the **Certificate Key**.

    10.3. If you configured a password for SSL key decryption, enter it in **Key Password**. If you didn't configure a password, leave it empty.

11. Select **Enable Proxy** to use a proxy server.
12. In **Proxy Configuration**:

    12.1. Enter the proxy server **IP** address and the **Port** number.

    12.2. Select either **HTTP** or **HTTPS** protocol.

13. Click **Submit**.

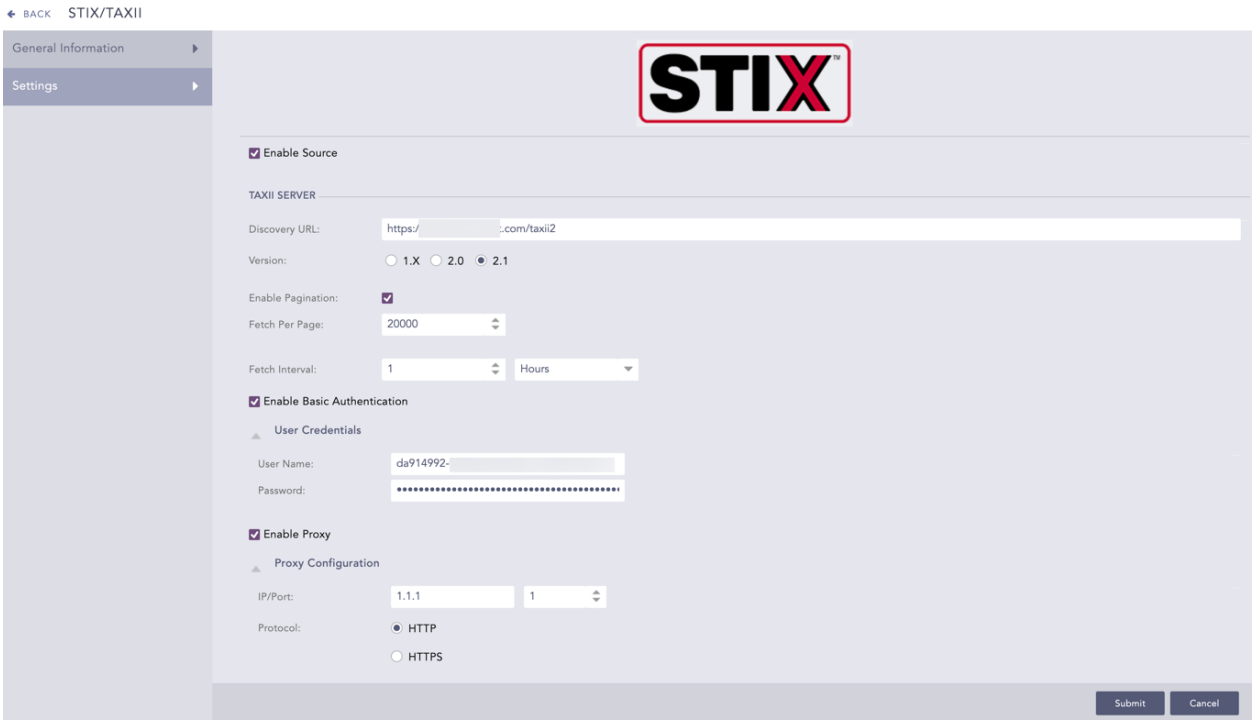

Fig. 2: Configuring STIX