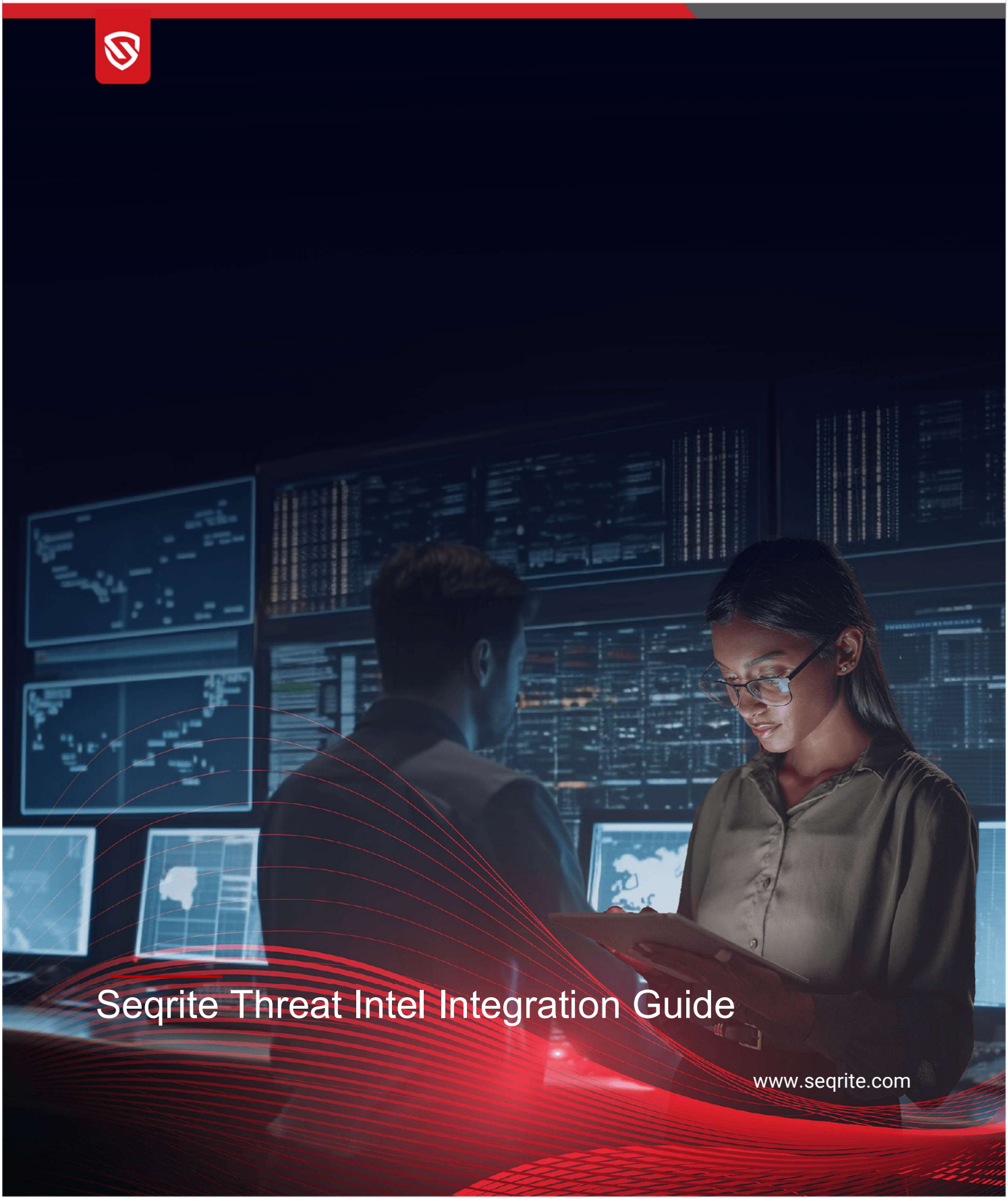
Seqrite Threat Intel

SEQRITE



Seqrite Threat Intel Integration Guide

www.seqrite.com

Copyright & License Information

Trademarks

Seqrite Threat Intel is a trademark of Quick Heal Technologies Limited. All third-party trademarks are owned by their respective third-party owners.

License Terms

Access to and use of Seqrite Threat Intel is subject to end-user's acceptance of the Seqrite Master End-User License Agreement. The license terms can be found at www.seqrite.com/eula.

Contents

Seqrite Threat Intel

Seqrite Threat Intel processes and detects millions of threats every day and stores this information in its secure databases. This information contains traditional indicators of compromise (IoCs), information on threat actors, suspicious domains and IP addresses, malware hashes, and more.

Seqrite makes this information available through the TAXII servers in STIX format to external customers and enterprises who can query this information and feed it to their security tools and platforms to block threats or gain visibility on upcoming cyber threats.
Information about malicious files, domain, IP Address and URLs can be polled from Seqrite labs through the TAXII services.

Introduction

This document explains how to integrate Seqrite Threat Intel with various cyber security solutions such as SIEM, SOAR and other solutions.
This integration helps to:

- Improve detection and response through monitoring and automation.
- Enable data sharing between SIEM and SOAR.

SIEM Integration

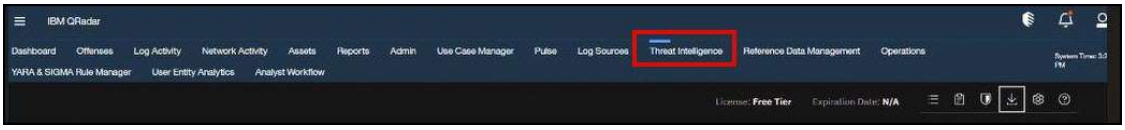
SIEM (Security Information and Event Management) is a platform that collects normalizes and analyzes security event data from an organization's IT infrastructure.

SIEM tools like QRadar help detect suspicious activity, correlate events, and generate alerts for potential threats.

QRadar Integration

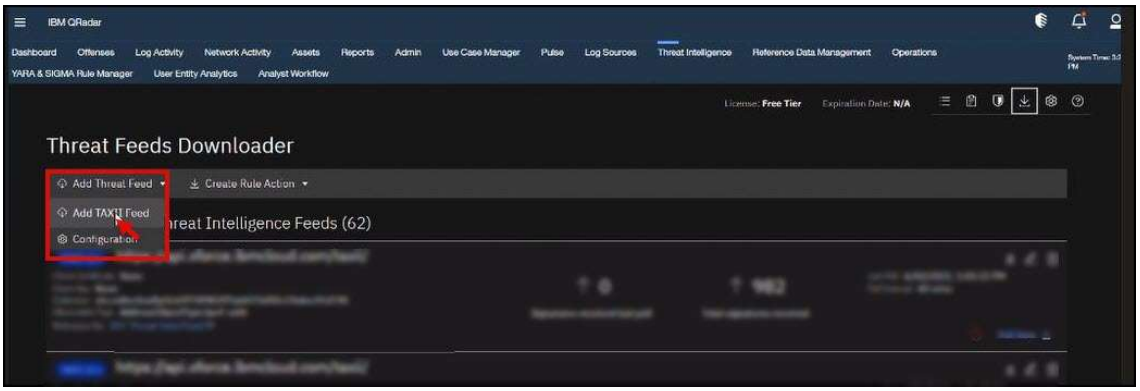
Steps for Seqrite Threat Intel and QRadar integration are given below:

1. Login to **QRadar** console.
2. Navigate to the **Threat Intelligence** tab**.**



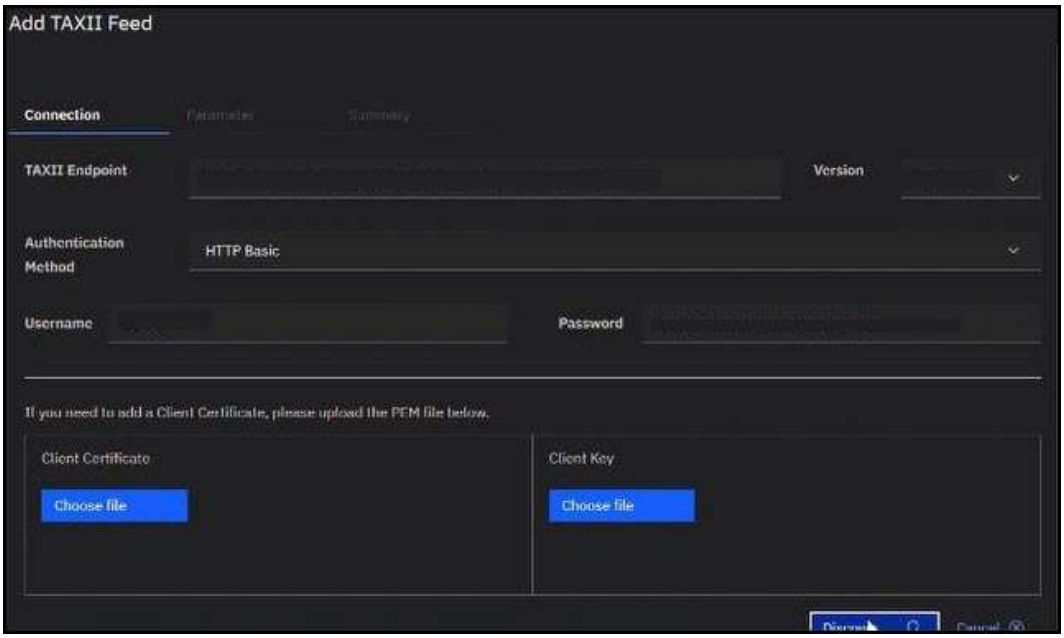
The **Threat Feeds Downloader** page appears.

3. Select **Add Threat Feed** >> **Add TAXII Feed**.

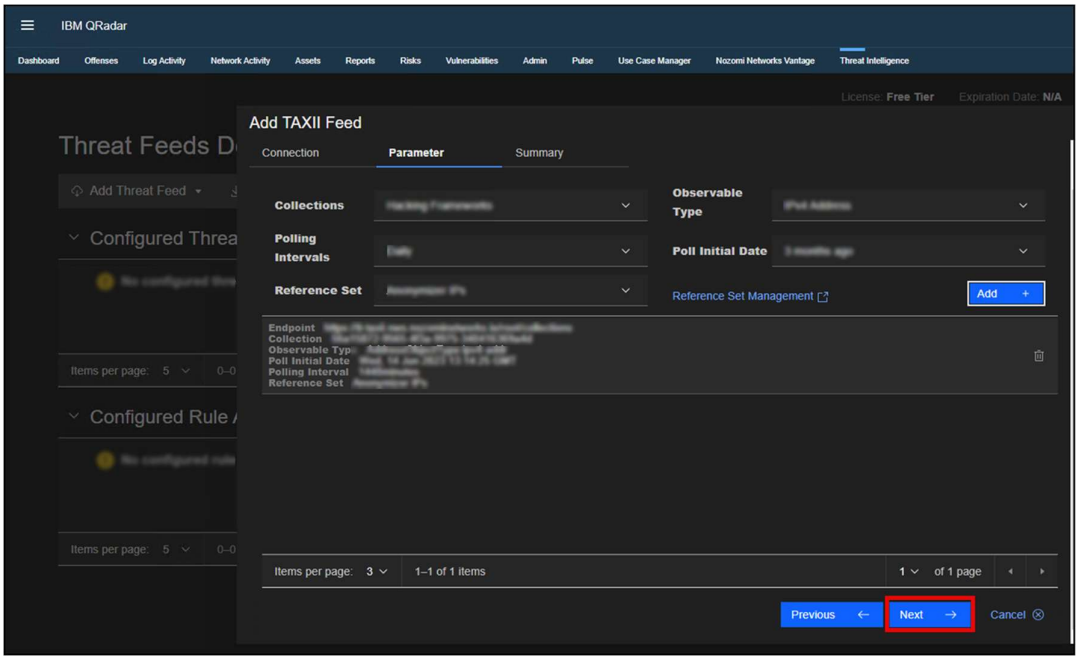


4. In the **Connection** section, enter following details and click **Discover**.

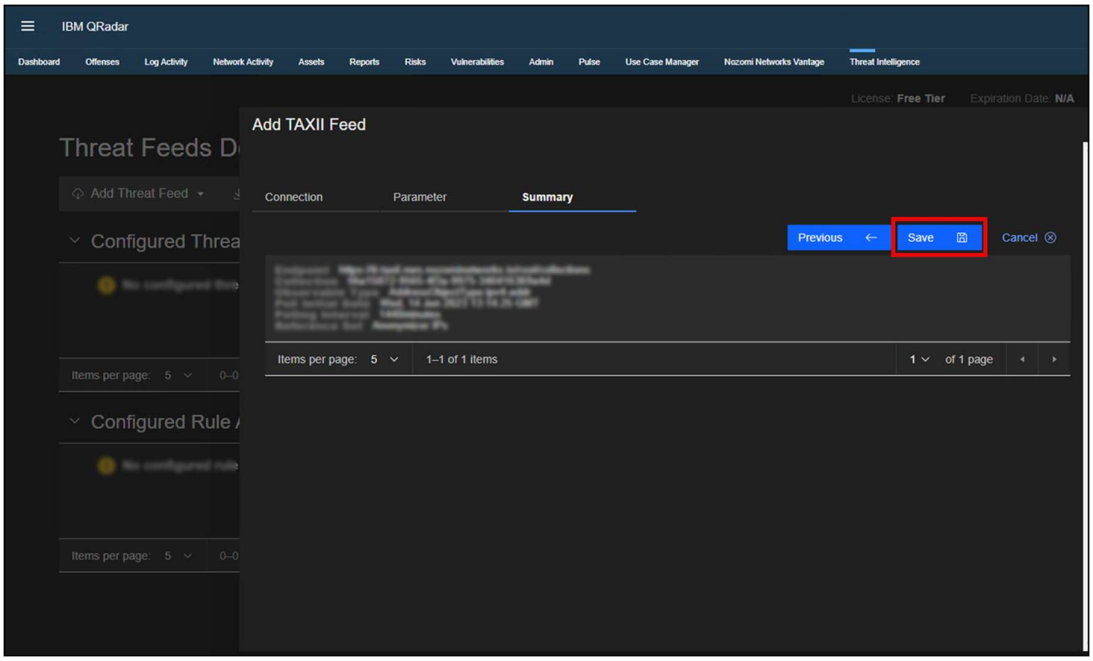
- TAXII Endpoint:
  - TAXII 2.0: https://sti.seqrite.com/taxii/root/collections
  - TAXII 2.1: https://sti.seqrite.com/taxii2/root/collections
- Authentication:
  You can authenticate in either of the following methods:
  - Username/Password
  - Bearer Token (A secure token available on the Seqrite Threat Intel portal.)



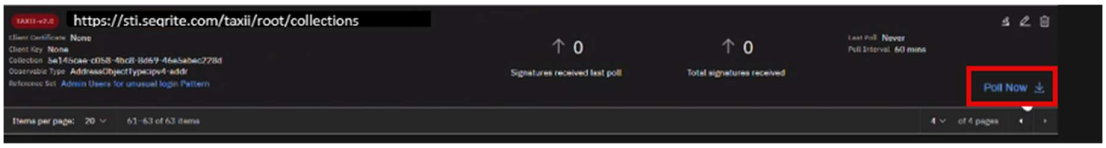
5. Go to **Parameter** section.



6. From the **Collections** dropdown, select ioc./select the applicable option.
7. From the **Observable Type** dropdown, select the appropriate indicator type.
8. Click **Add**.
9. In the **Summary** section, click **Save**.



10. Click **Poll Now** to start collecting indicators.



QRadar integration is now complete.

SOAR Integration

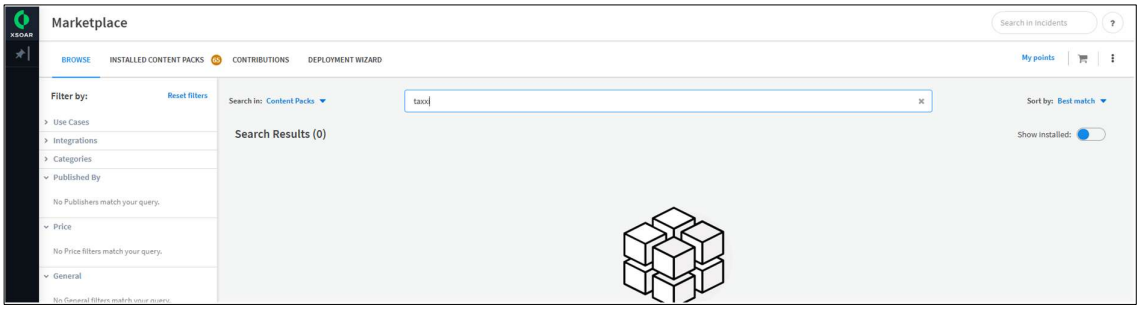
SOAR is a platform that brings security tools together in one platform. It automates tasks that are repetitive or time-consuming and manages incident workflows.

SOAR tools like XSOAR automates incident response and integrates security tools for faster, consistent workflows.

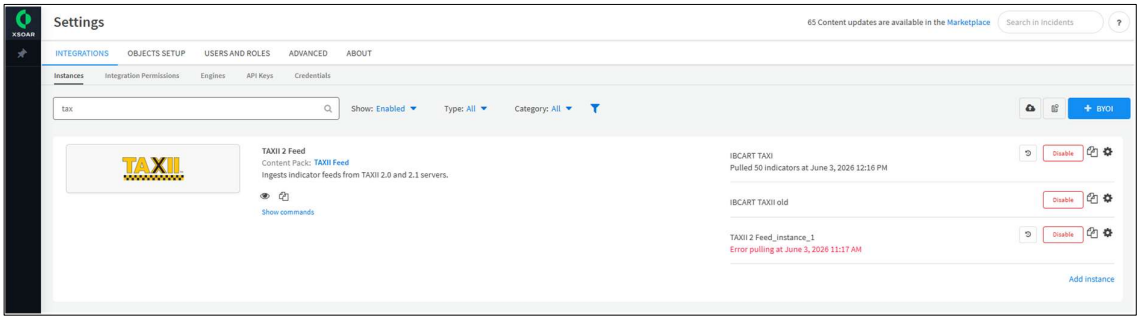
XSOAR Integration

Steps for Seqrite Threat Intel and XSOAR integration are given below:

1. **Log in** to the XSOAR platform and navigate to the **Marketplace**.
2. Search for TAXII installation package in the search box.

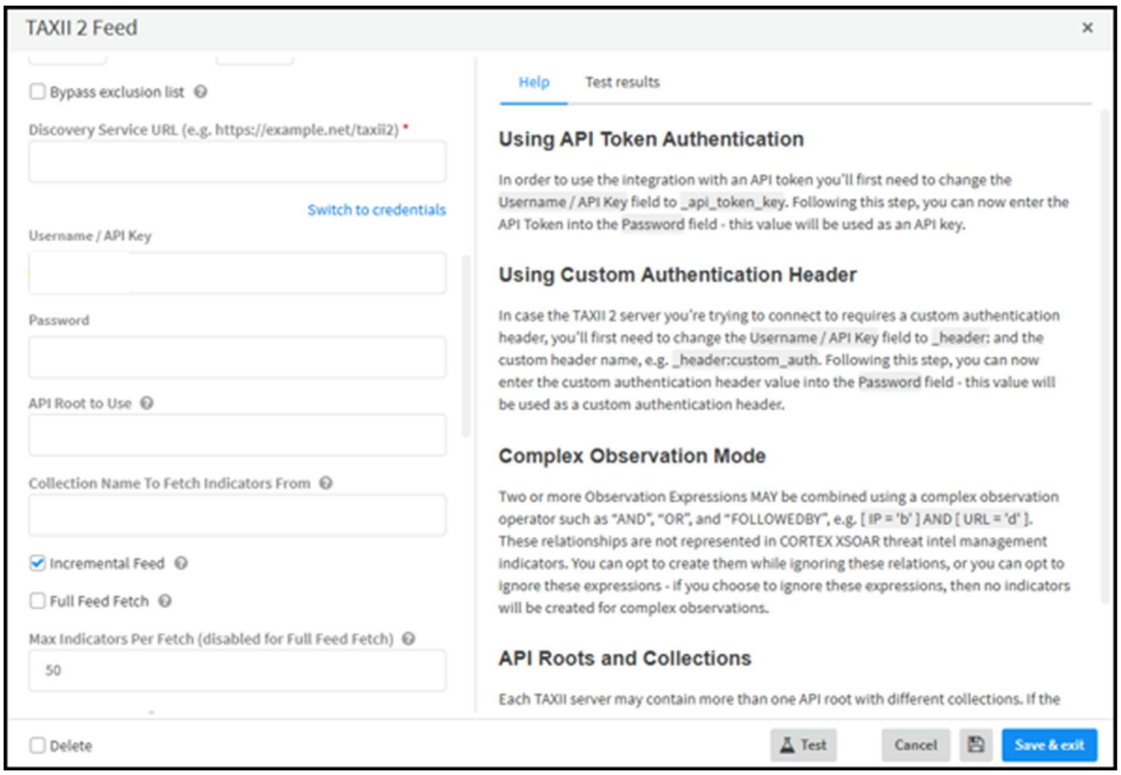


3. Select the app to install.



4. Configure TAXII Feed.

I. Provide connection details.
II. Enter Sachet URL, username, password, and then click **Save & exit**.



Once the integration is complete, XSOAR successfully pulls the threat feed from Seqrite Threat Intel.