



Seqrite Threat Intel Integration Guide

www.seqrite.com

Copyright & License Information

© 2026 Quick Heal Technologies Limited. All Rights Reserved.

No part of this publication may be reproduced, duplicated, or modified in any form or incorporated into any information retrieval system, electronic or any other media or transmitted in any form without prior permission of Quick Heal Technologies Limited; having its registered address at Solitaire Business Hub, 7th floor, Office No. 7010 C & D, Viman Nagar, Pune – 411 014, Maharashtra, India.

Marketing, distribution or use by anyone barring the people authorized by Quick Heal Technologies Limited is liable to legal prosecution.

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

- 1. Copyright & License Information 2
- 2. Seqrite Threat Intel 4
- 3. Introduction..... 5
- 4. SIEM Integration 6
 - QRadar Integration 6
- 5. SOAR Integration 9
 - XSOAR Integration 9

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

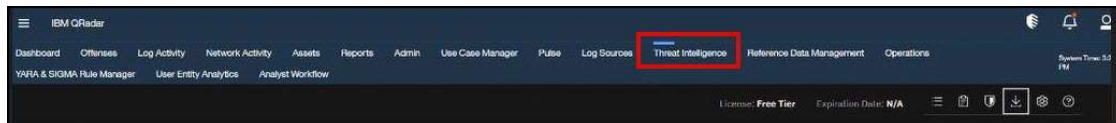
SIEM (Security Information and Event Management) is a platform that collects normalizes and analyzes security event data from an organization's IT infrastructure.

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

QRadar Integration

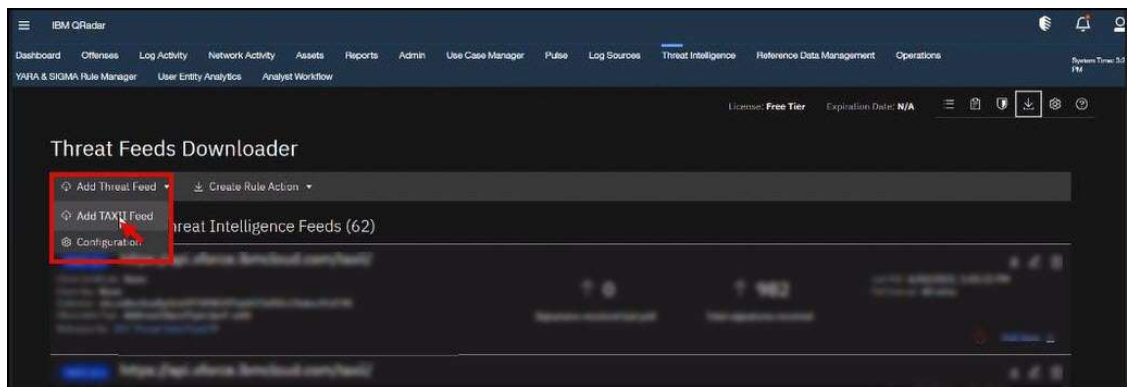
Steps for Seqrite Threat Intel and QRadar integration are given below:

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.segrite.com/taxii/root/collections>
 - TAXII 2.1: <https://sti.segrite.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.)

Add TAXII Feed

Connection | Parameters | Summary

TAXII Endpoint: **Version:**

Authentication Method: HTTP Basic

Username: **Password:**

If you need to add a Client Certificate, please upload the PEM file below.

Client Certificate

[Choose file](#)

Client Key

[Choose file](#)

[Previous](#) [Next](#) [Cancel](#)

5. Go to **Parameter** section.

IBM QRadar

Dashboard | Offenses | Log Activity | Network Activity | Assets | Reports | Risks | Vulnerabilities | Admin | Pulse | Use Case Manager | Niscom Networks Vantage | **Threat Intelligence**

License: Free Tier | Expiration Date: N/A

Threat Feeds D

[Add Threat Feed](#)

Configured Threa

No configured threat feeds

Items per page: 5 | 0-0

Configured Rule

No configured rules

Items per page: 5 | 0-0

Add TAXII Feed

Connection | **Parameter** | Summary

Collections: **Observable Type:**

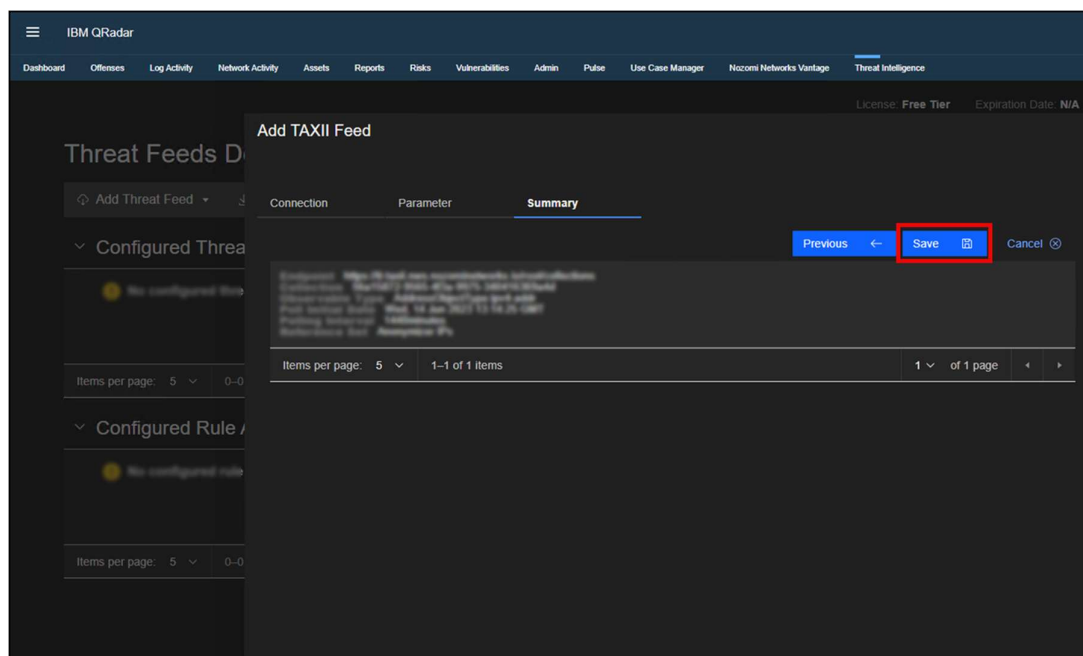
Polling Intervals: **Poll Initial Date:**

Reference Set: [Reference Set Management](#) [Add](#)

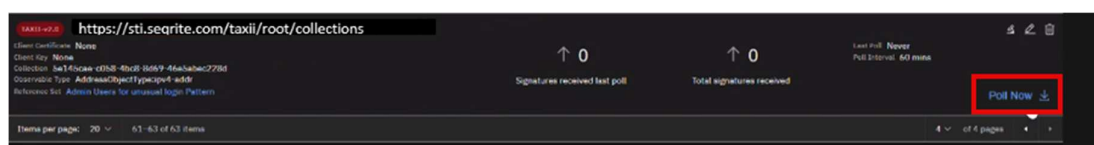
Endpoint:
Collection:
Observable Type:
Poll Initial Date:
Polling Interval:
Reference Set:

Items per page: 3 | 1-1 of 1 items | 1 of 1 page | [Previous](#) [Next](#) [Cancel](#)

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



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



QRadar integration is now complete.

SOAR Integration

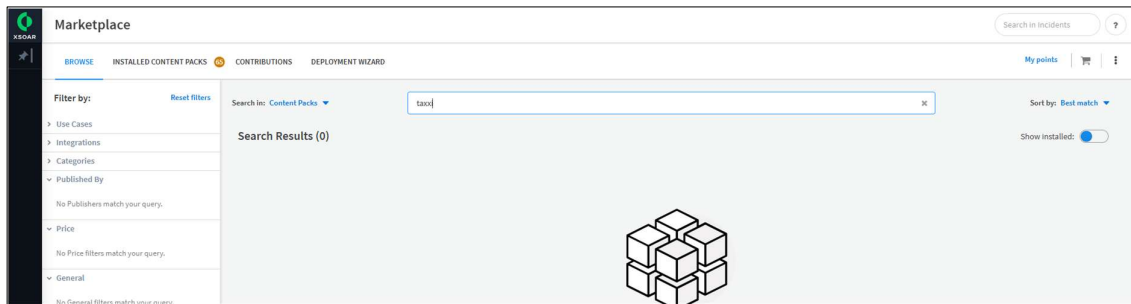
SOAR is a platform that brings security tools together in one platform. It automates tasks that are repetitive or time-consuming and manages incident workflows.

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

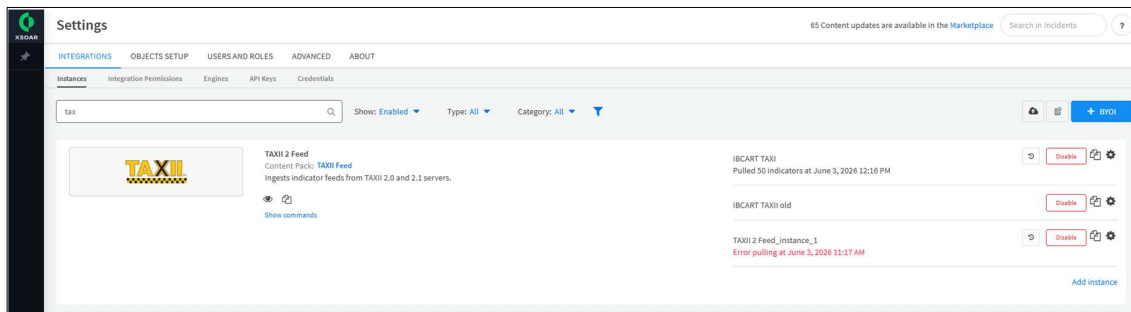
XSOAR Integration

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**.

TAXII 2 Feed

☐ Bypass exclusion list ⓘ

Discovery Service URL (e.g. https://example.net/taxii2) *

[Switch to credentials](#)

Username / API Key

Password

API Root to Use ⓘ

Collection Name To Fetch Indicators From ⓘ

☒ Incremental Feed ⓘ
☐ Full Feed Fetch ⓘ

Max Indicators Per Fetch (disabled for Full Feed Fetch) ⓘ

☐ Delete

[Help](#)
[Test results](#)

Using API Token Authentication

In order to use the integration with an API token you'll first need to change the Username / API Key field to `_api_token_key`. Following this step, you can now enter the API Token into the Password field - this value will be used as an API key.

Using Custom Authentication Header

In case the TAXII 2 server you're trying to connect to requires a custom authentication header, you'll first need to change the Username / API Key field to `_header`; and the custom header name, e.g. `_header:custom_auth`. Following this step, you can now enter the custom authentication header value into the Password field - this value will be used as a custom authentication header.

Complex Observation Mode

Two or more Observation Expressions MAY be combined using a complex observation operator such as "AND", "OR", and "FOLLOWEDBY", e.g. `[IP = 'b'] AND [URL = 'd']`. These relationships are not represented in CORTEX XSOAR threat intel management indicators. You can opt to create them while ignoring these relations, or you can opt to ignore these expressions - if you choose to ignore these expressions, then no indicators will be created for complex observations.

API Roots and Collections

Each TAXII server may contain more than one API root with different collections. If the

[Test](#)
[Cancel](#)
[Save & exit](#)

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

TAXII 2 Feed
 Command Profile: TAXII Feed
 Imports indicator feeds from TAXII 2.0 and 2.1 servers.

[Show commands](#)

OKAPI TAXII
 Pulled 50 indicators at June 4, 2020 12:21 PM

OKAPI TAXII and
 TAXII 2 Feed_instance_1
 Error pulling at June 4, 2020 12:28 PM

[Add instance](#)