Symantec
by Broadcom Software

Broadcom Threat Intelligence: TAXII Integration Guide for QRadar

September 2023

Table of Contents

Documentation Legal Notice

This Documentation, which includes embedded help systems and electronically distributed materials, (hereinafter referred to as the “Documentation”) is for your informational purposes only and is subject to change or withdrawal by Broadcom at any time. This Documentation is proprietary information of Broadcom and may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of Broadcom.

If you are a licensed user of the software product(s) addressed in the Documentation, you may print or otherwise make available a reasonable number of copies of the Documentation for internal use by you and your employees in connection with that software, provided that all Broadcom copyright notices and legends are affixed to each reproduced copy.

The right to print or otherwise make available copies of the Documentation is limited to the period during which the applicable license for such software remains in full force and effect. Should the license terminate for any reason, it is your responsibility to certify in writing to Broadcom that all copies and partial copies of the Documentation have been returned to Broadcom or destroyed.

TO THE EXTENT PERMITTED BY APPLICABLE LAW, BROADCOM PROVIDES THIS DOCUMENTATION “AS IS” WITHOUT WARRANTY OF ANY KIND, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT WILL BROADCOM BE LIABLE TO YOU OR ANY THIRD PARTY FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FROM THE USE OF THIS DOCUMENTATION, INCLUDING WITHOUT LIMITATION, LOST PROFITS, LOST INVESTMENT, BUSINESS INTERRUPTION, GOODWILL, OR LOST DATA, EVEN IF BROADCOM IS EXPRESSLY ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

The use of any software product referenced in the Documentation is governed by the applicable license agreement and such license agreement is not modified in any way by the terms of this notice.

The manufacturer of this Documentation is Broadcom Inc.

Provided with “Restricted Rights.” Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

Introduction

This document provides information on how to integrate the Broadcom Threat Intelligence TAXII feeds with QRadar.

For more information on the TAXII service, see the Broadcom Threat Intelligence: TAXII Overview.

To get started, see Getting Your Symantec Enterprise Security Complete (SESC) Credentials.

Getting Your Symantec Enterprise Security Complete (SESC) Credentials

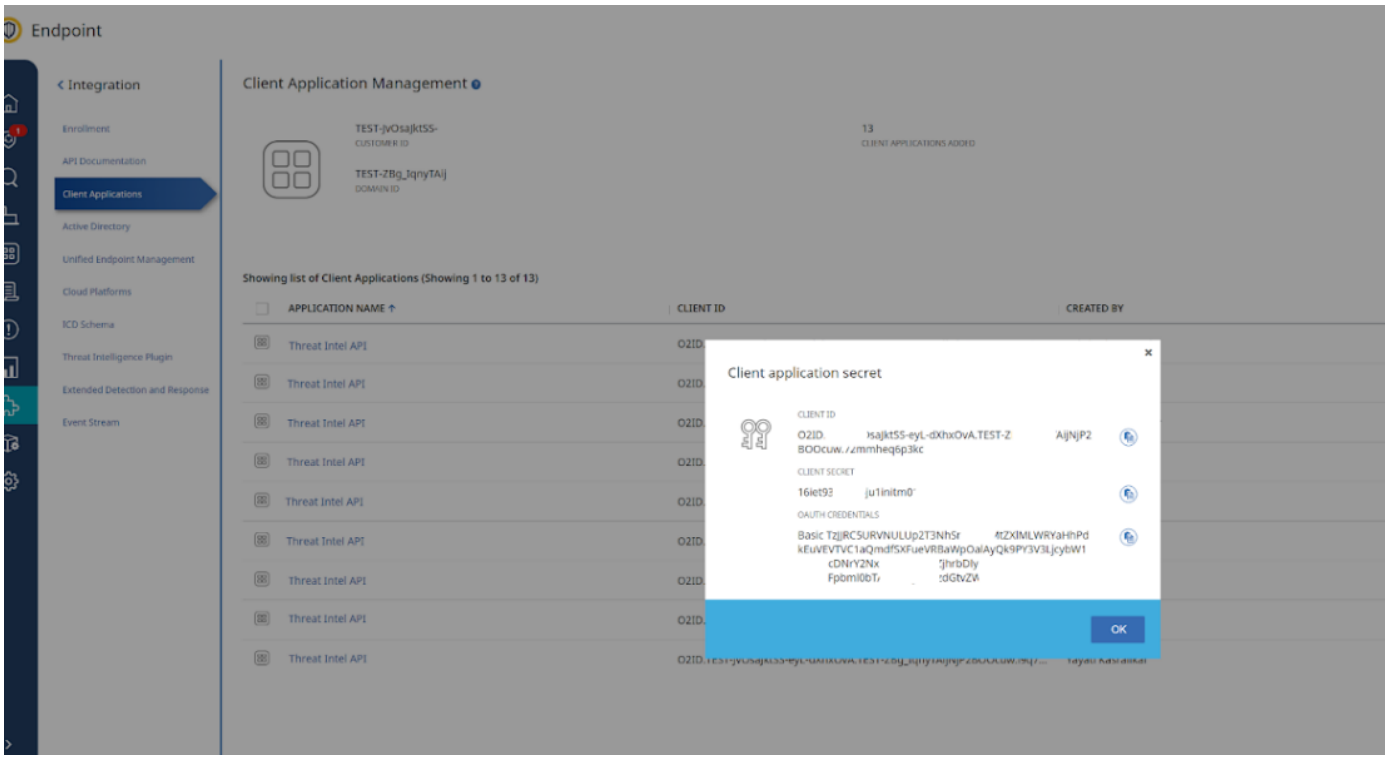
You can obtain your credentials by logging into the Symantec Enterprise Security Complete (SESC) cloud console.

NOTE

Without credentials, you cannot integrate the Broadcom Threat Intelligence TAXII feeds with QRadar.

To get your Symantec Enterprise Security Complete (SESC) credentials

1. Log on to https://sep.securitycloud.symantec.com/.
2. In the sidebar, click **Integration.**
3. On the Integration page, click **Client Applications**.
4. On the Client Application Management page, do one of the following:
   a) Select an existing application in the grid.
   b) Click **Add** to add a new client application name.
5. Complete the setup, and then select the new application in the grid. In the application flyout pane, click **Client Secret** to view and copy both the client_id and the client_secret to the Clipboard.



TAXII URL

Type the URL for the TAXII polling service according to the region, as indicated in the following table.

Region	Endpoint
Global	https://**api.sep**.securitycloud.symantec.com/v1/threat-intel/taxii11/poll
EU	https://**api.sep.eu**.securitycloud.symantec.com/v1/threat-intel/taxii11/poll
India	https://**api.sep.in**.securitycloud.symantec.com/v1/threat-intel/taxii11/poll

You can determine which region to use by logging into your SESC tenant and going to **Integration > API Documentation** to see what documentation is available there.

The Broadcom Threat Intelligence Collections

The Broadcom Threat Intelligence collections vary in size and can contain large numbers of indicators.

Collection	Approximate size
threat-alert	Approximately one new report is added each week. Each report contains dozens of indicators.
malicious-uri	Approximately ten thousand indicators **per day**.
malicious-file	Approximately eight thousand indicators **per day**.

Configuring QRadar

T use the Broadcom Threat Intelligence TAXII feeds with QRadar, you must install the IBM® QRadar® Threat Intelligence app. This app pulls in threat intelligence feeds by using the open standard STIX and TAXII formats, and lets you deploy the data to create custom rules for correlation, searching, and reporting.

For example, you can use the app to import public collections of dangerous IP addresses from IBM X-Force Exchange and create a rule to raise the magnitude of any offense that includes IP addresses from that watch list.

For more information, refer to the following IBM documentation resources:

- https://www.ibm.com/docs/en/qradar-common?topic=checklist-installing-qradar-threat-intelligence
- https://www.ibm.com/docs/en/qradar-on-cloud?topic=tokens-adding-authorized-service-token

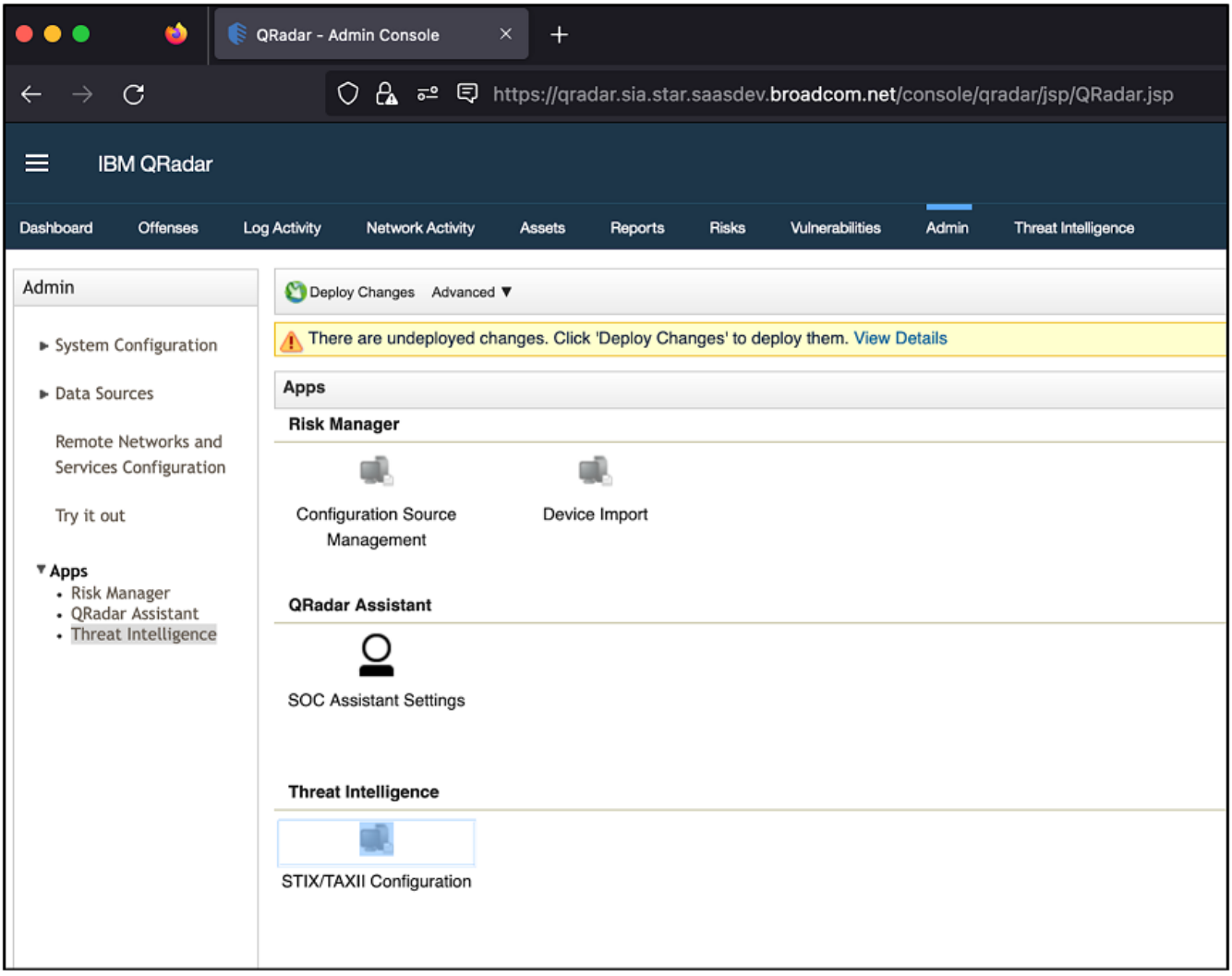
Adding and Configuring Feeds

To integrate the Broadcom Threat Intelligence feeds with QRadar, you must add and configure the feeds properly.

Refer to your QRadar documentation for any changes to these procedures.

To add and configure feeds

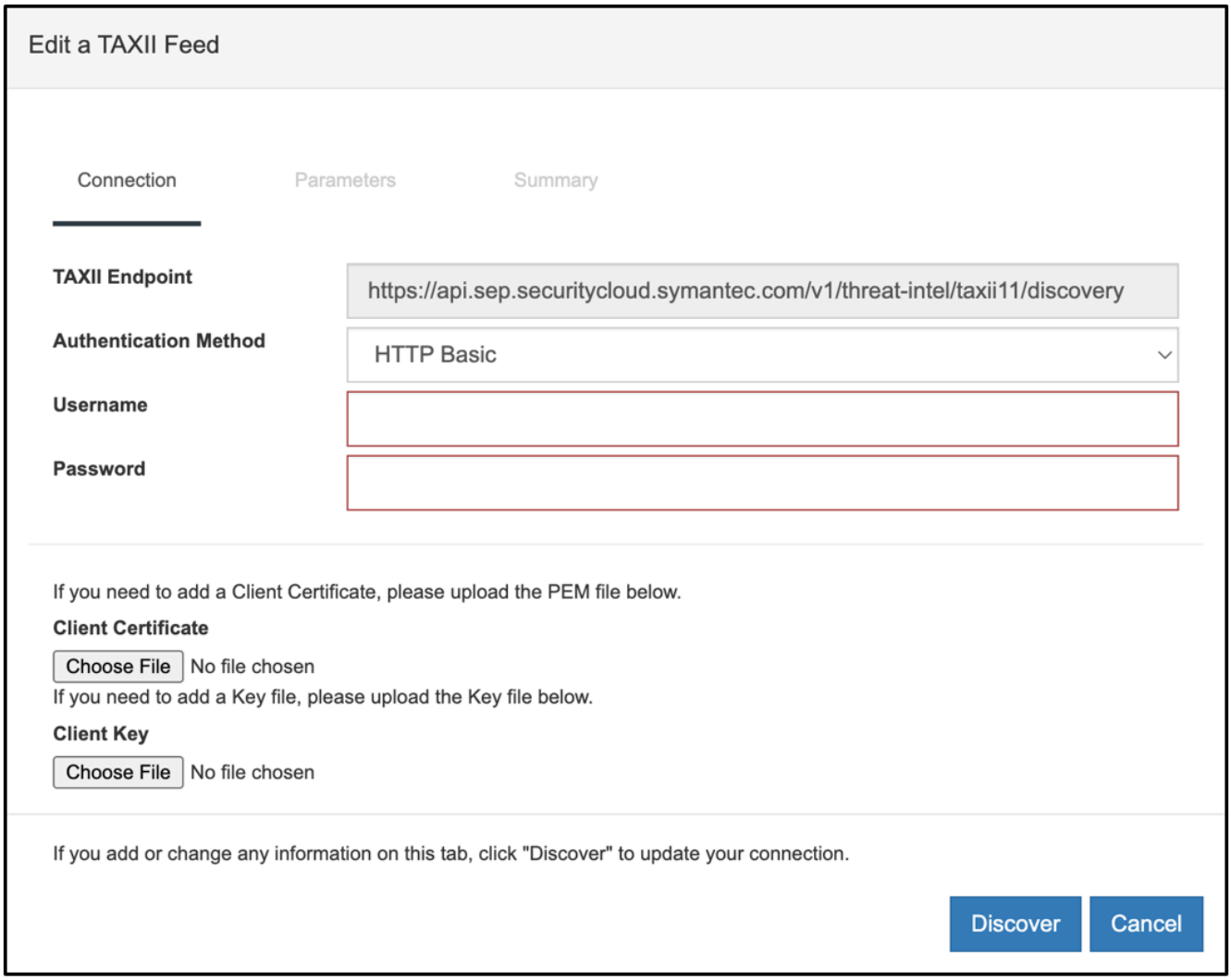
1. In the IBM QRadar console, on the navigation menu, click **Admin > Apps > Threat Intelligence**.
2. Under Threat Intelligence, click **STIX/TAXII Configuration**.



3. In the Edit a TAXII Feed window, click the **Connection** tab, and then configure the following options:

TAXII Endpoint	Type the URL of the TAXII server for your region. For example: https://api.sep.securitycloud.symantec.com/v1/threat-intel/taxii11/discovery
Authentication Method	Select **HTTP Basic** in the drop-down list.
Username	Type the client_id value.

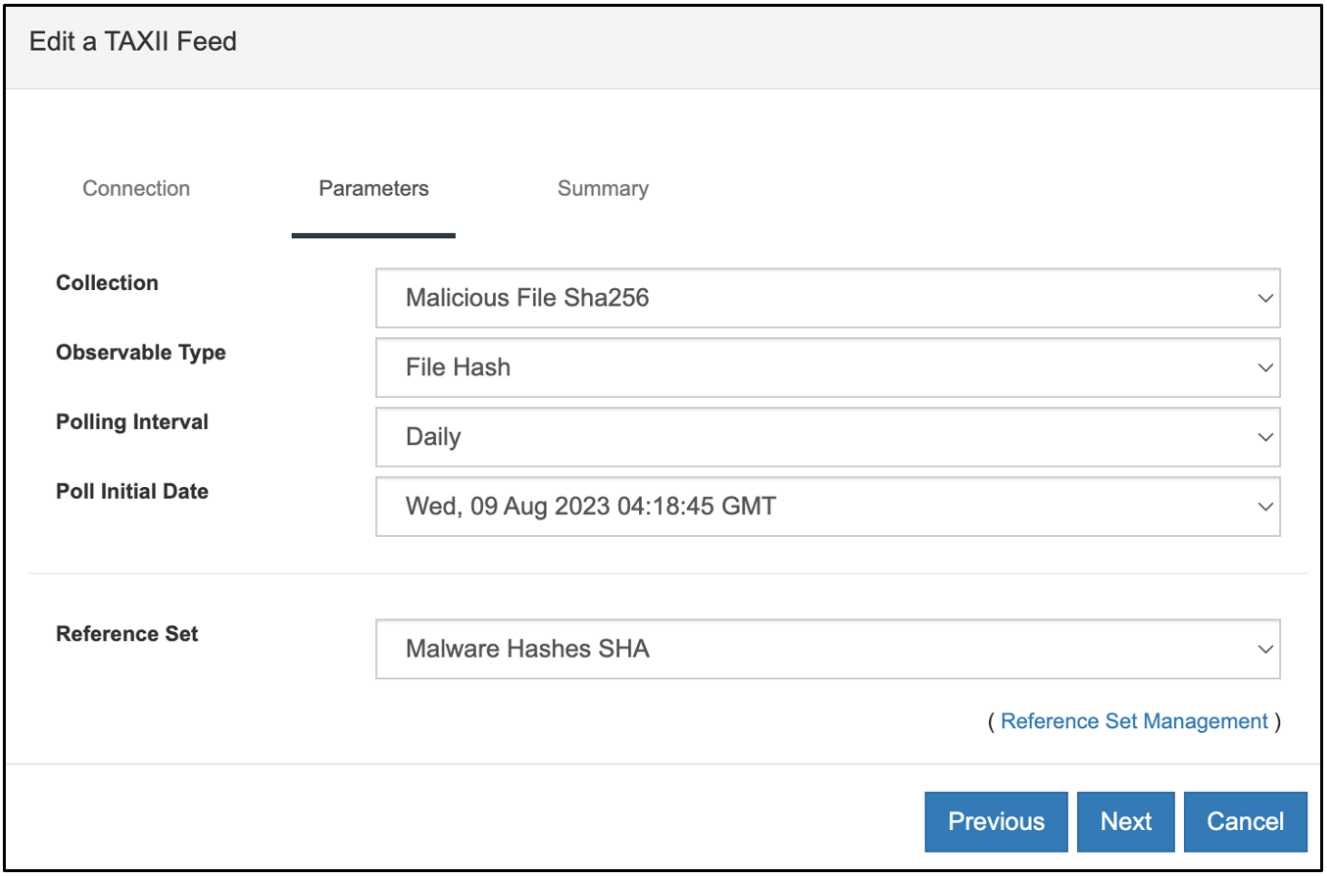
Password	Type the client_secret value.
Client Certificate	Not applicable.
Client Key	Not applicable.



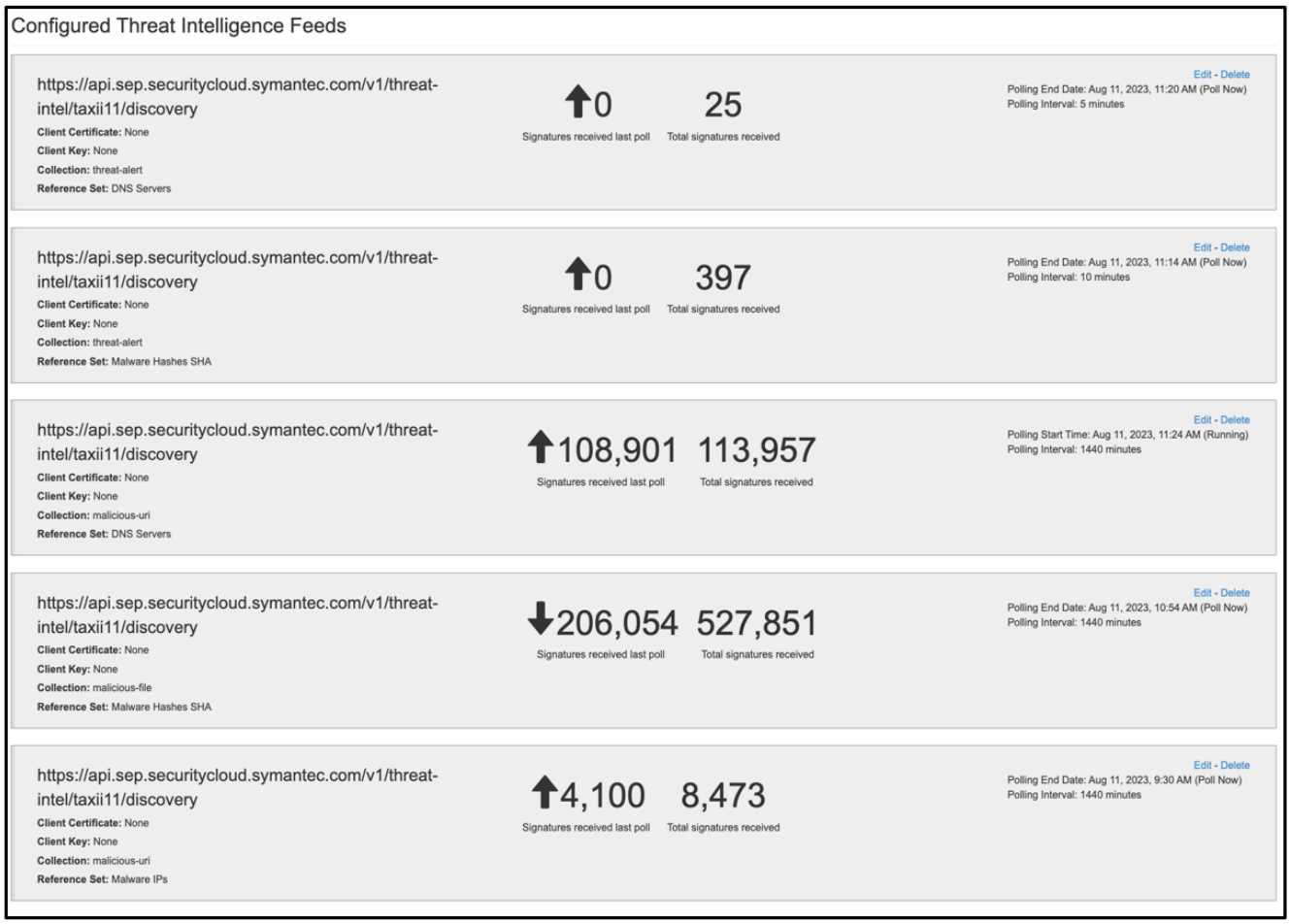
4. Click **Discover**.
5. In the Edit a TAXII Feed window, click the **Parameters** tab, and then configure the following options:

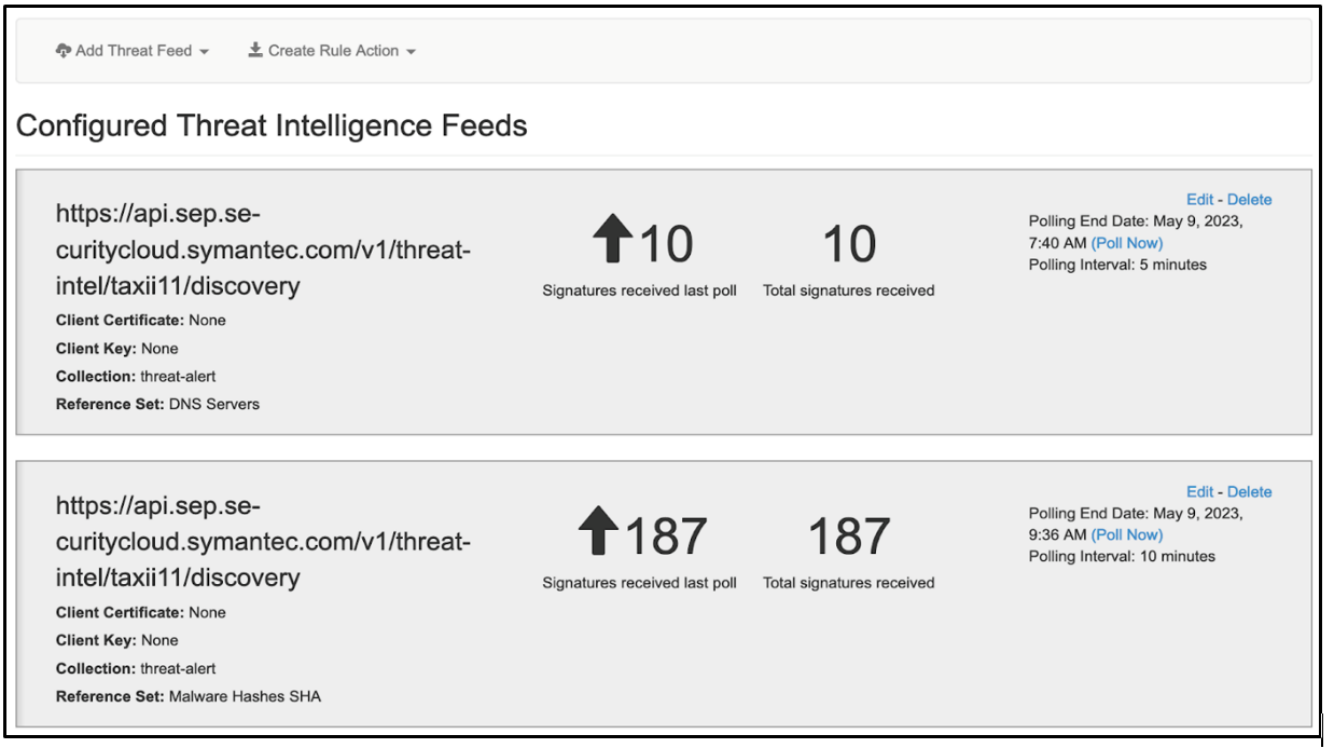
Collection	Use a collection that is specified in The Broadcom Threat Intelligence Collections.
Observable Type	An observable is a STIX schema component that specifies a suspicious object. Only observables of this type are used. All others are ignored. • For the `malicious-file` collection, use File Hash. • For the `malicious-uri` collection, use Domain name or IPv4 Address. • For the `threat-alert` collection, use malware File Hash, Domain name, or IPv4 Address.
Polling Interval	The Broadcom Threat Intelligence feeds are updated daily so you can set the polling interval to every 24 hours.

Poll Initial Date	• For the `malicious-uri` and `malicious-file` feeds, Symantec recommends that you use a poll initial date 24 hours older than the current date. The maximum lookback period for the uri feeds is 10 days. • For the `threat-alert` feed, you can sepcify an older earliest value.
Reference Set	• For the `malicious-file` collection, use Malware Hashes SHA. • For the `malicious-uri` collection, use Malware IPs or DNS server. • For the `threat-alert` collection, use malware Malware Hashes SHA, Malware IPs, or DNS server. **Note:** If you want to add elements to a dedicated reference set, you must set it up in advance. For more information about reference sets, see the IBM QRadar Administration Guide.



6. Click **Add**. You can add unlimited multiple collections to the same TAXII endpoint, or you can continue to create this feed.
7. When you finish creating the feeds, click **Next**.
8. In the window, click the **Summary** tab to check your configuration parameters before you implement the threat intelligence feed. You can **Edit** or **Delete** any feeds.





9. When you are finished, click **Save**.

Troubleshooting

You can use the following instructions to troubleshoot issues when integrating the Broadcom Threat Intelligence TAXII feeds with the IBM® QRadar® SIEM Console:

- https://www.ibm.com/docs/en/qradar-common?topic=app-troubleshooting-qradar-threat-intelligence
- https://www.ibm.com/support/pages/qradar-threat-intelligence-app-troubleshooting-polling-issues

Frequently Asked Questions

Question	Answer
What version of TAXII is supported?	The TAXII 1.1 specification is supported.
What version of STIX is supported?	The STIX 1.2 schema is supported.


Symantec
by Broadcom Software