



# SentinelOne Connector for QRadar

Version 2.0.0

10 Aug 2023

Copyright © 2023 SentinelOne

This document contains SentinelOne proprietary information owned by Sentinel Labs, Inc. ("SentinelOne"), and is provided for use only in connection with SentinelOne's Endpoint Protection Platform. This document may also contain confidential information, and may not be reproduced or otherwise used without the express permission of SentinelOne. SentinelOne reserves the right to amend this document in its sole discretion. SentinelOne® and the SentinelOne logos are the registered and unregistered trademarks of Sentinel Labs, Inc. The SentinelOne Solutions are protected under various state and federal laws, including without limitation, US Patent Nos. 9,710,648 and 10,102,374. Please contact SentinelOne with questions.

# Table of Contents

1. SentinelOne Connector for QRadar	4
2. Requirements for the QRadar Connector App	4
3. Configuring QRadar Connector App Integration	5 - 8
4. Main Capabilities of QRadar Connector App	9
5. API for QRadar Connector App	10 - 19

## SentinelOne Connector for QRadar

The SentinelOne QRadar Connector App empowers organizations to combine the strengths of their QRadar deployments to collect, monitor, analyze, and visualize massive streams of machine data with the detection, response, remediation, and forensics capabilities of SentinelOne EPP.

The Application uses SentinelOne REST APIs to fetch information about threat events and activities from the SentinelOne Console and ingest them into QRadar. It also indexes the events in QRadar by converting them into the proper CEF formatted messages. The app pulls data every 30 seconds by default (frequency can also be customized).

The app can connect with multiple SentinelOne Consoles, either On-Prem and cloud deployments, and multiple scopes on the same Console. Administrators can view all connected Consoles or a specific Console. Managed Security Service Providers (MSSPs) can split the different sources to use different QRadar collectors to manage multiple QRadar licenses for customer requirements.

**Event Types:** The App has mapping for all SentinelOne event types that were available up to Management Console version North Pole GA. You can manually map events from later versions.

Features of the SentinelOne QRadar Connector App:

- Extend real-time threat prevention, detection, and investigation to all endpoints, on network or off.
- Streamline multi-console deployments with integrated analysis and management.
- Understand network-wide trends and behavioral patterns to make more informed decisions through custom searches and reports.
- Enrich threats data and triage indicators with 3rd party applications in QRadar.
- Simplify deployment complexity and operational overheads with an integrated console for monitoring and management.
- Leverage the SentinelOne API for increased reliability of information.
- Support the TCP protocol also while sending the data to Qradar.
- Added a dropdown for the logsource selector in the configuration to select any log source which falls under the SentinelOne API.

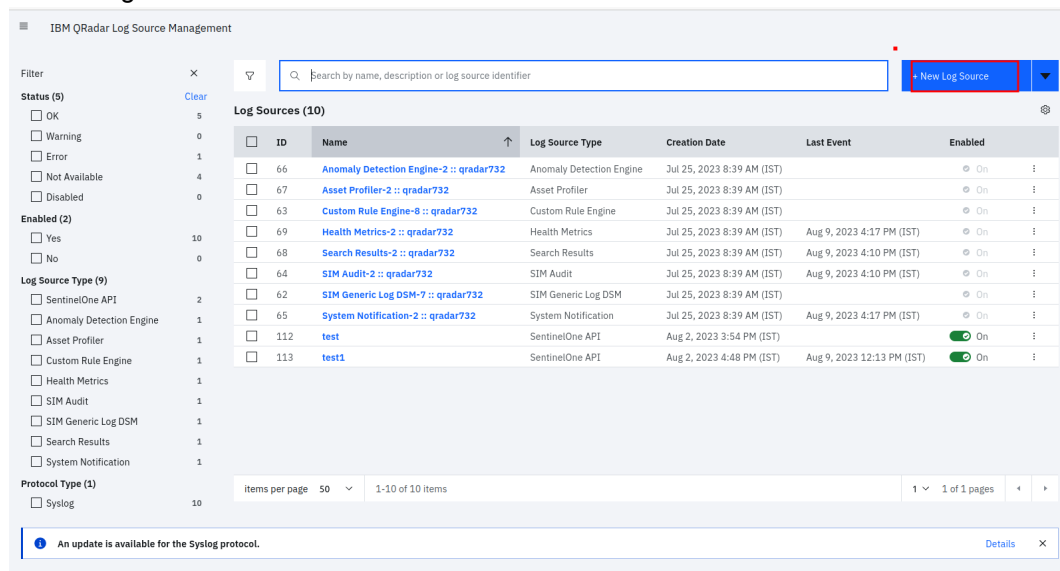
## Requirements for the QRadar Connector App

- The SentinelOne QRadar Connector App is compatible with QRadar and QRoc.
- SentinelOne Management Console version Kauai and later (API 2.1).
- The external SentinelOne DSM app is not required, it won't be used by connector App as it contains its own DSM.

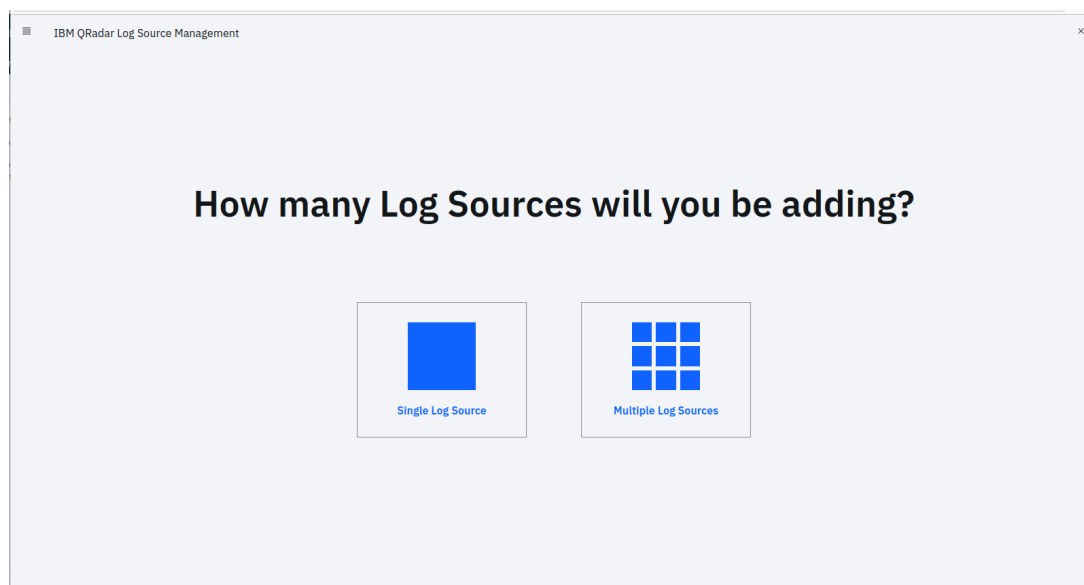
## Configuring QRadar Connector App Integration

### To Create a Logsource (Prerequisite):

1. Download the Qradar logsource Management App from the IBM App Exchange. If the app is already installed continue to step 2.
2. Log in to the **QRadar** console.
3. Click **Admin > Extensions Management**.
4. Click **Add**, upload the App package, and follow the installation wizard.
5. Click **Admin > Deploy Changes**.
6. Scroll to the bottom of the page and click **Qradar Logsource Management App**.
7. Click New Logsource



8. Select Single Log Source.



9. Select SentinelOne API as a log source type.

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

## Select a Log Source type

Search: sentinelone

SentinelOne API

Step 2: Select Protocol Type

10. Select protocol type as Syslog.

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

## Select a protocol type

Search: Syslog

Syslog

Syslog Redirect

TCP Multiline Syslog

TLS Syslog

UDP Multiline Syslog

Step 1: Select Log Source Type

Step 3: Configure Log Source Parameters

## 11. Configure the Log Source Parameters, provide the required fields while configuring.

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

### Configure the Log Source parameters

**Name \***  
The name of the log source.

**Description**  
An optional description of the log source.

**Enabled**  
Indicates whether the log source should be enabled.

☒ On

**Groups \***  
The groups that this log source will belong to.

Other X

Q + Add Group

**Extension**  
Log Source Extensions perform post-processing of events after default parsing has occurred.  
[+ Show More](#)

**Language \***  
Select the language used for the log source's events to ensure correct and optimized parsing.

**Target Event Collector \***  
The appliance responsible for receiving and parsing the events from this log source.

**Disconnected Log Collector \***  
The disconnected log collector that this log source will receive events on.

IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

### Configure the Log Source parameters

**Language \***  
Select the language used for the log source's events to ensure correct and optimized parsing.

**Target Event Collector \***  
The appliance responsible for receiving and parsing the events from this log source.

**Disconnected Log Collector \***  
The disconnected log collector that this log source will receive events on.

**Credibility \***  
The higher the credibility, the more certain you are that this log source emits reliable events.  
[+ Show More](#)

**Coalescing Events**  
When a log source emits multiple events which are very similar to one another in a short time span, they'll be coalesced together.  
[+ Show More](#)

☒ On

**Store Event Payloads**  
Enable to store original event payloads in addition to the normalized record.  
[+ Show More](#)

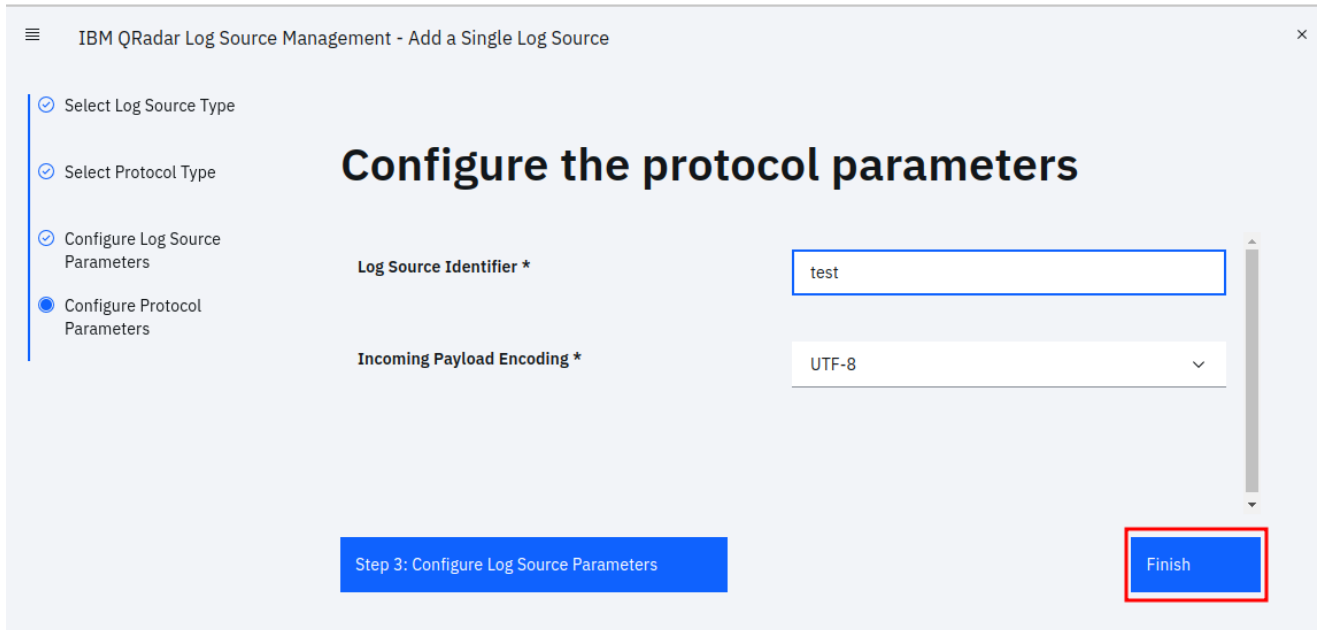
☒ On

Step 2: Select Protocol Type

Step 4: Configure Protocol Parameters

\*Suggestion use default values

## 12. Configure the Protocol parameters



IBM QRadar Log Source Management - Add a Single Log Source

Select Log Source Type

Select Protocol Type

Configure Log Source Parameters

Configure Protocol Parameters

### Configure the protocol parameters

Log Source Identifier \*

Incoming Payload Encoding \*

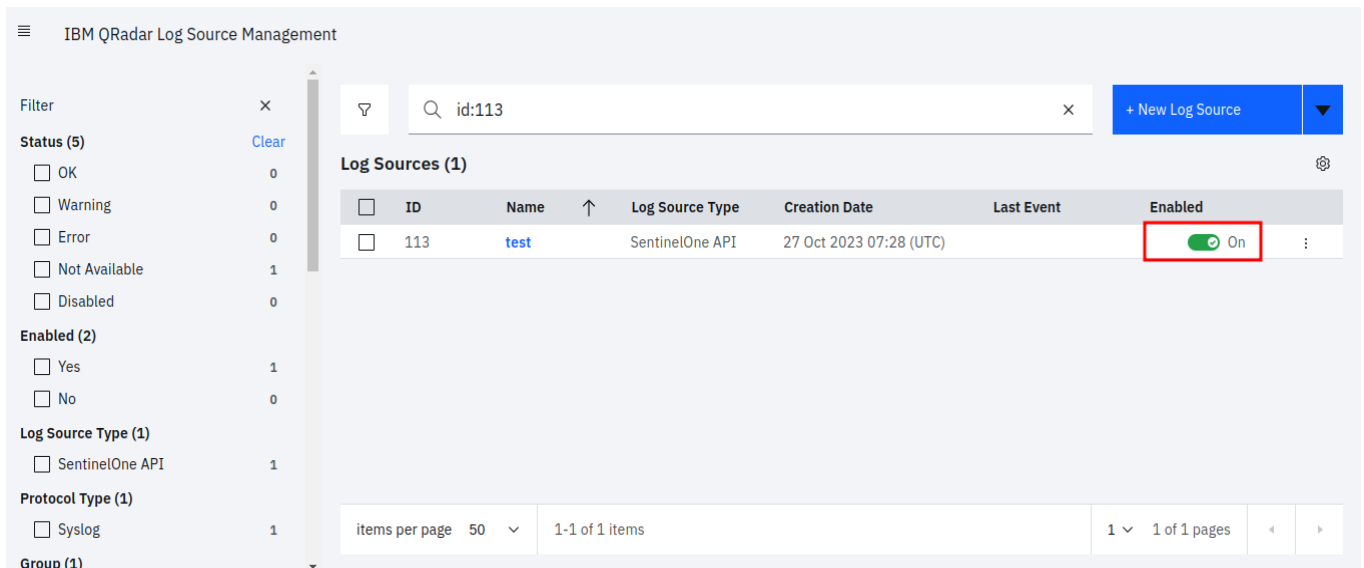
Step 3: Configure Log Source Parameters

Finish

\* Log Source Identifier value will be some unique value

13. Click Finish.

14. The created logsource will be enabled.



IBM QRadar Log Source Management

Filter

Status (5)

OK 0

Warning 0

Error 0

Not Available 1

Disabled 0

Enabled (2)

Yes 1

No 0

Log Source Type (1)

SentinelOne API 1

Protocol Type (1)

Syslog 1

Group (1)

id:113

+ New Log Source

### Log Sources (1)

ID	Name	Log Source Type	Creation Date	Last Event	Enabled
113	test	SentinelOne API	27 Oct 2023 07:28 (UTC)		On

items per page 50 1-1 of 1 items 1 1 of 1 pages

15. Deploy the changes.

## To Install the Connector App:

1. Download the SentinelOne QRadar Connector App from the [IBM App Exchange](#).

The App supports QRadar and QRoc

2. Log in to the **QRadar console**.

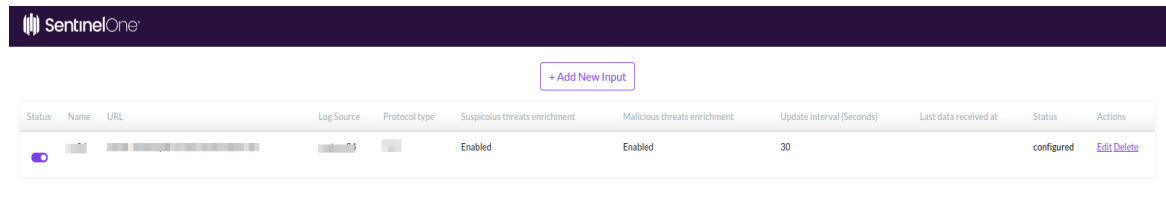
3. Click **Admin > Extensions Management**.

4. Click **Add**, upload the App package, and follow the installation wizard.

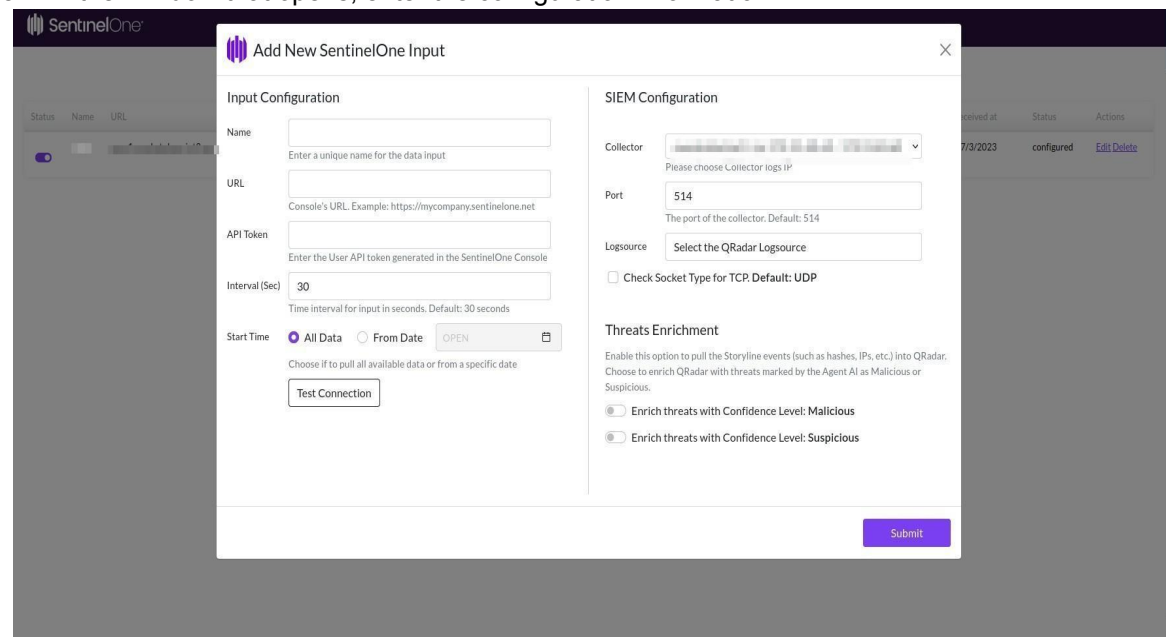


5. Click **Admin > Deploy Changes**.
6. Scroll to the bottom of the page and click **SentinelOne Configuration**.
7. Click **Add New Input**.

This adds SentinelOne Consoles to QRadar.



8. In the Window that opens, enter the configuration information.



- In QRadar, select a **Collector** from the list
  - In QRoc, enter the IP of the **Collector**.
9. To make sure the input is accurate, click **Test Connection**.
  10. Select the QRadar collector and port.
  11. Select a log source.  
You must **Deploy Changes** before you can access the log Source.
  12. Make sure the log source is selected and its port is correct.  
Once the log source is used, it is then disabled or removed from the list. Each logSource can be used for a single input only. Select the Logsource which was created recently.
  13. Select the protocol type for getting data into Qradar with **UDP (Default) or TCP**.
  14. In the **Threats Enrichment** section, select the levels of threat indicators for Suspicious and Malicious threats.

SentinelOne gives a score to different indicators based on Static AI and Dynamic AI. If the score is high, the threat indicator has a confidence level of Malicious. If the score is low, the object has a confidence level of Benign. If the score is higher than benign, but lower than malicious, the object has a confidence level of Suspicious. You can change this option at any time.

15. Click **Submit**.

A new row shows in **Disable Status**.

16. Click **Admin > Deploy Changes**.

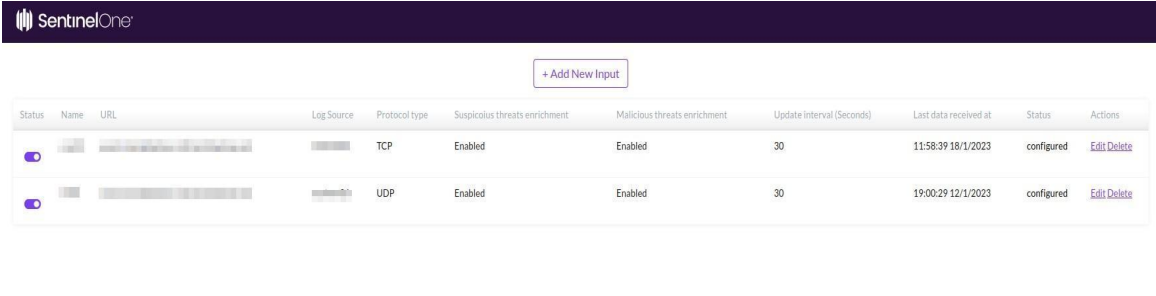
17. Open the **SentinelOne Connector** page, and click **Enable** on the new SentinelOne input.

The status updates to **Active** and the **Last Data Received** column shows the current date and time.

18. Add more inputs or close the page.

19. Open the **Log Activity** tab and see new events arrive in the QRadar console.

**Note:** The QRadar Connector App runs on a different container. If you do not get events, verify with IBM that they are not blocking traffic from the container.



The screenshot shows the SentinelOne Connector configuration interface. At the top, there is a dark purple header with the SentinelOne logo. Below the header, there is a button labeled "+ Add New Input". The main content area displays a table with two rows of configuration data. Each row has a toggle switch on the left, followed by columns for Name, URL, Log Source, Protocol type, Suspicious threats enrichment, Malicious threats enrichment, Update interval (Seconds), Last data received at, Status, and Actions.

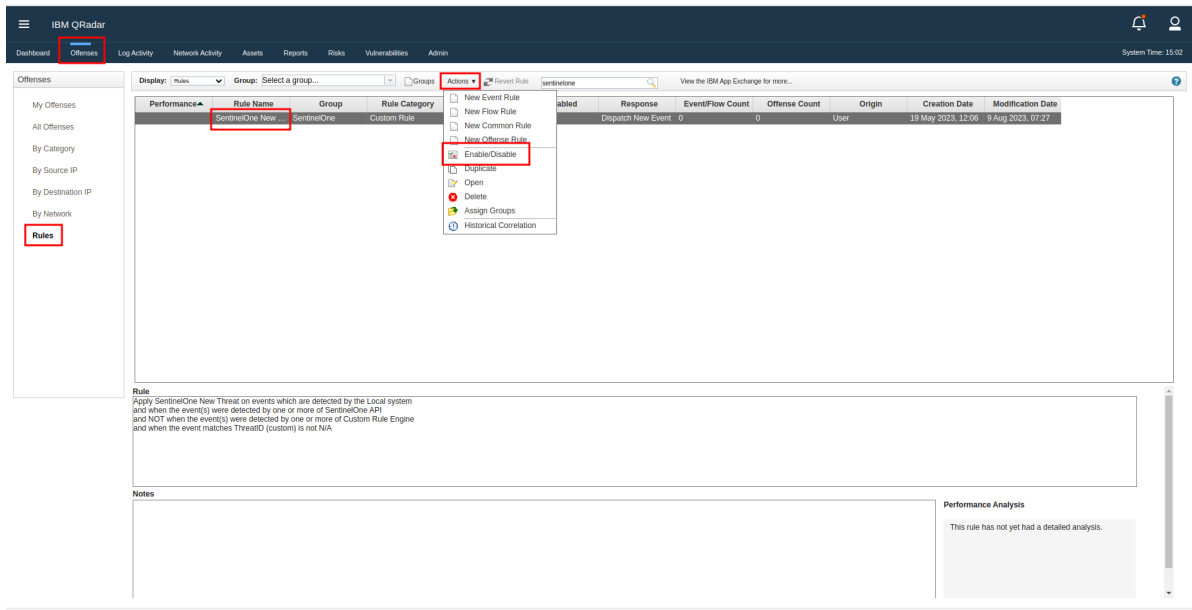
Status	Name	URL	Log Source	Protocol type	Suspicious threats enrichment	Malicious threats enrichment	Update interval (Seconds)	Last data received at	Status	Actions
<input checked="" type="checkbox"/>	[Redacted]	[Redacted]	[Redacted]	TCP	Enabled	Enabled	30	11:58:39 18/1/2023	configured	<a href="#">Edit</a> <a href="#">Delete</a>
<input checked="" type="checkbox"/>	[Redacted]	[Redacted]	[Redacted]	UDP	Enabled	Enabled	30	19:00:29 12/1/2023	configured	<a href="#">Edit</a> <a href="#">Delete</a>

## Recommended rule to leverage SentinelOne data:

**Important Note:** The **SentinelOne New Threat** rule is available in Qradar Connector v2.0.0 and above.

### To Enable the Rule:

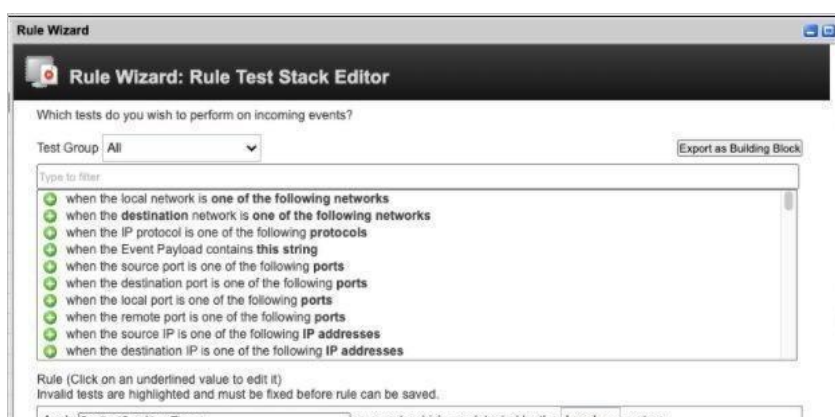
1. Login into your **Qradar** console.
2. Click **Offenses > Rules**.
3. Enter **SentinelOne** in the Search filter.
4. Select the **SentinelOne New Threat** rule.
5. Click **Actions > Enable**.



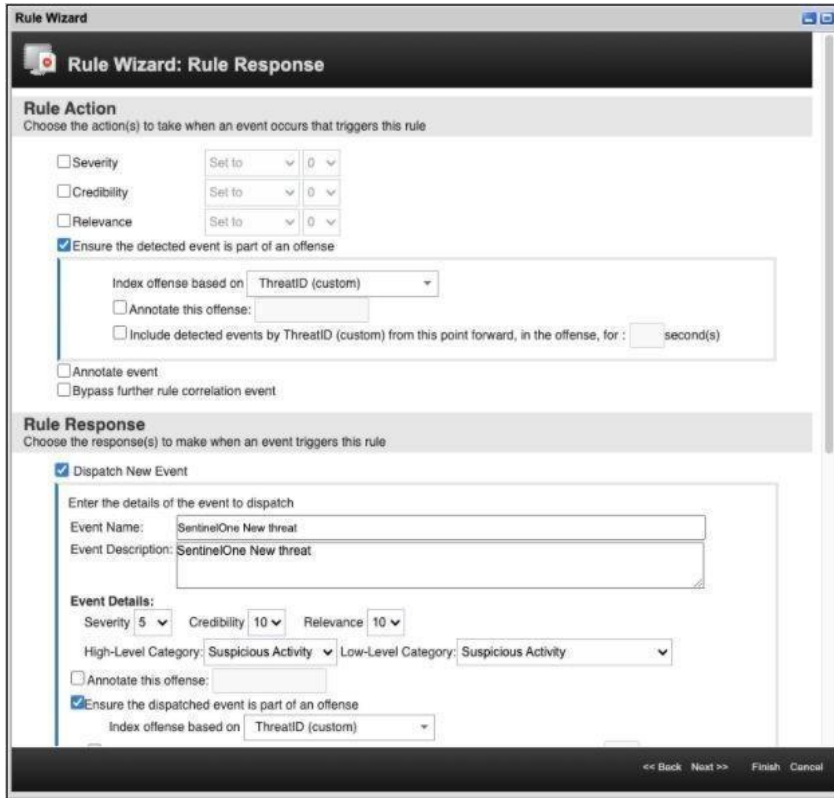
**These steps are required for enabling the rules when for Connector version below v2.0.0:**

To correlate and search for threat events easily, we recommend you use a custom offense rule.

1. Open the **Offenses** tab and click **Rules**.
2. From the **Actions** menu, click **New Event Rule**.
3. In the Rule Wizard, select and edit the values to target SentinelOne events:
  - and when the event(s) were detected by one or more of SentinelOne API
  - and NOT when the event(s) were detected by one or more of Customer Rule Engine-8 :: qradar742
  - and when the event matches ThreatID (custom) is not N/A



4. In the Rule Response window, add these properties:



Rule Name	SentinelOne New Threat
Rule Logic	<b>And when the event(s) were detected by one or more of SentinelOne API And when the event matches ThreatID (custom) is not N/A</b>
Building blocks	None
Rule Action	<b>Ensure the detected event is part of an offense &gt; Indexed based on ThreatID (custom)</b>
Rule Response	<b>Dispatch New Event:</b> <b>Event name: SentinelOne new threat</b> <b>Description: New threat by SentinelOne</b> <b>HLC: Suspicious activity</b> <b>LLC: Suspicious activity</b> <ul style="list-style-type: none"> <li>• <b>Ensure the dispatched event is part of an offense &gt; Indexed based on ThreatID (custom)</b></li> <li>• <b>This information should set or replace the name of the associated offense(s)</b></li> </ul>
Response Limiter	None
Notes	None
Dependencies	<b>Sentinelone API Custom Properties: &gt; ThreatID (custom)</b>

5. **Optional:** To begin watching events immediately, click **Enable this rule**.
6. Review the Rule Summary and click **Finish**.

- ## Main Capabilities of the QRadar Connector App

## API for QRadar Connector App

**QRadar :**

**GET :** config/event\_sources/log\_source\_management/log\_source\_types/{id}

Retrieves log source type by id.

**Response :**

```
{
  "Supported_language_ids" : [
    1], "Internal" : false,
  "Log_source_extension_id"
:1, "Protocol_types" : [
  {
    "Protocol_id" : 0,
    "Documented" : false
  },
  {
    "Protocol_id" : 0,
    "Documented" : false
  }
],
  "Custom" : true,
  "Name" : "SentinelOne
API", "Id" : 4001,
  "Version": null,
  "Uuid" : "4ef6c3b2-1931-4b14-b55c-0ff45ad7001c"
}
```

**GET :**

**config/deployment/hosts**

Retrieves the list of deployed

hosts. **Response :** [ "events",

"flows",

```
"simarc",
```

```
"statistics
```

```
"
```

```
]
```

#### **GET : config/event\_sources/event\_collectors**

Retrives list of all event collectors

#### **Response :**

```
[
```

```
{
```

```
  "Name" : "eventcollector0 ::
```

```
  ip-172-31-40-69", "Host_id" : 53,
```

```
  "Componenet_name" :
```

```
  "eventcollector0", "Id" : 7
```

```
}
```

```
]
```

POST : config/event\_sources/log\_source\_management/log\_sources/

Creates a new log source

Json data is required i.e; log\_source\_data.

#### **Response :**

```
{
```

```
  "coalesce_events":
```

```
  true, "credibility": 42,
```

```
  "deleted": true,
```

```
  "description":
```

```
  "String",
```

```
  "disconnected_log_collector_id":
```

```
  42, "enabled": true,
```

```
  "gateway":
```

```
  true,
```

```
"group_ids": [  
  42  
],  
"id": 42,  
"language_id": 42,  
"log_source_extension_id": 42,  
"name": "String", "parsing_order":  
42, "protocol_parameters": [  
  {  
    "id": 42,  
    "name": "String",  
    "value": "String"  
  }  
],  
"protocol_type_id": 42,  
"requires_deploy": true,  
"sending_ip": "String",  
"store_event_payload": true,  
"target_event_collector_id":  
42,  
"type_id": 42,  
"wincollect_external_destination_ids  
": [  
  42  
],  
"wincollect_internal_destination_id": 42  
}
```



**GET: /config/event\_sources/log\_source\_management/log\_source\_types'?filter=name%3D%22{}%22'**

Retrieves a list of log sources according to the logSource type id like sentinelone,cybereason etc.

**Sample Response :**

```
{
  "sending_ip":
    "169.254.3.8", "internal":
    false,
    "protocol_parameters": [
      {
        "name":
          "incomingPayloadEncoding", "id":
          1,
        }
    ],
    {
      "name": "identifier", "id": 0,
      "value": "SentinelOne"
    }
  ],
  "description": "UnityOne
device", "coalesce_events":
true, "enabled": true,
  "parsing_order": 1,
  "average_eps":0,
  "group_ids": [
    0
  ],
  "credibility": 5,
  "id": 264,
  "store_event_payload": true,
  "target_event_collector_id": 7,
  "protocol_type_id": 0,
```

```
"language_id": 1,
"creation_date": 1676961225355,
"wincollect_external_destination_ids": null,
"log_source_extension_id": null,
"name": "UnityOne @ SentinelOne",
"modified_date": 1676961225355,
"auto_discovered": true,
"type_id": 19,
"last_event_time": 1676980886909,
"requires_deploy": false,
"gateway": false,
"wincollect_internal_destination_id": null,
"status": {
  "last_updated": 0
  "messages": [
    {
      "severity": "ERROR",
      "text": "Events have not been received from this Log Source in over 720
minutes.", "timestamp": null
    }
  ],
}
```

**Sentinelone API :****GET - /threats/{threat\_id}/explore/events**

Get all threat events.

Response :

```
{
  "data": [
    {
      "activeContentFileId": null,
      "activeContentHash": null,
      "activeContentPath": null,
      "agentDomain": "myguest.virtualbox.org",
      "agentGroupId": "1594943021508472481",
      "agentId": "1620860299252988044",
      "agentInfected": true,
      "agentIp": "117.96.237.188",
      "agentIsActive": true,
      "agentIsDecommissioned": false,
      "agentMachineType": "server",
      "agentName": "Ubuntu-Engineering",
      "agentNetworkStatus": "connected",
      "agentOs": "linux",
      "agentUuid": "43b99a99-09b0-7c54-5b69-822cbc34a928",
      "agentVersion": "22.3.3.11",
      "connectionStatus": null,
      "createdAt": "2023-02-20T14:59:07.999000Z",
      "direction": null,
      "dnsRequest": null,
      "dnsResponse": null,
      "dstIp": null,
      "dstPort": null,
      "eventType": "Process Creation",
```

```
"fileFullName": null,  
"fileSha1": "9df2e83b282ec552ad53e4d1bfb192f2c55f8d5f",  
"fileSha256": null,  
"fileSize": null,  
"fileType": null,  
"hasActiveContent": null,  
"id": "1624675162219761759",  
"indicatorCategory": null,  
"indicatorDescription": null,  
"indicatorMetadata": null,  
"indicatorName": null,  
"loginsBaseType": null,  
"loginsUserName": null,  
"md5": null,  
"networkMethod": null,  
"networkSource": null,  
"networkUrl": null,  
"objectType": "process",  
"oldFileMd5": null,  
"oldFileName": null,  
"oldFileSha1": null,  
"oldFileSha256": null,  
"parentPid": null,  
"parentProcessName": null,  
"parentProcessUniqueKey": null,  
"pid": "2922",  
"processCmd": null,  
"processDisplayName": "gedit",  
"processGroupId": "45593bcb-4be1-2bd0-8e03-3eaaafc047c7",  
"processImagePath": null,  
"processImageSha1Hash": "9df2e83b282ec552ad53e4d1bfb192f2c55f8d5f",
```

"processIntegrityLevel": null,  
"processIsRedirectedCommandProcessor": null,  
"processIsWow64": null,  
"processName": "gedit",  
"processRoot": "True",  
"processSessionId": null,  
"processStartTime": null,  
"processSubSystem": null,  
"processUniqueKey": "45593bcb-4be1-2bd0-8e03-3eaaafc047c7\_2922",  
"processUserName": null,  
"protocol": null,  
"publisher": null,  
"registryClassification": null,  
"registryId": null,  
"registryPath": null,  
"relatedToThreat": true,  
"rpId": null,  
"sha1": "9df2e83b282ec552ad53e4d1bfb192f2c55f8d5f",  
"sha256": null,  
"signatureSignedInvalidReason": null,  
"signedStatus": null,  
"siteName": "Test",  
"srcIp": null,  
"srcPort": null,  
"storyline": "45593bcb-4be1-2bd0-8e03-3eaaafc047c7",  
"taskName": null,  
"taskPath": null,  
"threatStatus": "marked\_as\_benign",  
"tid": null,  
"trueContext": "45593bcb-4be1-2bd0-8e03-3eaaafc047c7",  
"user": null,

```
"verifiedStatus": null

}
]

"pagination": { "nextCursor": null, "totalItems": 2
}

}
```

### **GET - /web/api/v2.0/activities**

Get the activities, and their data.

#### **Response :**

```
{
  "data": [
    {
      "accountId": null,
      "accountName": null,
      "activityType": 26,
      "activityUuid": "1a845274-8ea1-42b1-9a21-f257d8ab092a",
      "agentId": null,
      "agentUpdatedVersion": null,
      "comments": "Union Square#59",
      "createdAt": "2023-01-05T11:08:15.398123Z",
      "data": {
        "accountName": null,
        "buildVersion": "Union Square#59",
        "fullScopeDetails": "Global",
        "fullScopeDetailsPath": "Global",
        "groupName": null,
        "ipAddress": null,
        "scopeLevel": "Global",
        "scopeName": "",
        "siteName": null
      },
    },
  ],
}
```

```
"description": null,
"groupId": null,
"groupName": null,
"hash": null,
"id": "1591219074568817147",
"osFamily": null,
"primaryDescription": "The management console was updated with build Union Square#59.",
"secondaryDescription": null,
"siteId": null,
"siteName": null,
"threatId": null,
"updatedAt": "2023-01-05T11:08:15.386498Z",
"userId": null
}

],
"pagination": { "nextCursor":
"eyJpZF9jb2x1bW4iOiAiQWN0aXZpdHkuaWQiLCIAiaWRfdmFsdWUiOiAiAxNTkxMjE5MDc0NTY
4ODE3MTQ3LCAic29ydF9ieV9jb2x1bW4iOiAiQWN0aXZpdHkuaWQiLCIAic29ydF9ieV92YWx1
ZSI6IDE1OTEyMTkwNzQ1Njg4MTcxNDcsICJzb3J0X29yZGVyIjogImFzYyJ9",
"totalItems": 15992
}
}
```