

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

lter	×	8	Q	Search by n	ame, description or log source identif	ier		+ N		
tatus (5)	Clear									
🗆 ок	5	Log So	ources (10)						
Warning	0		ID	Name	Ύ	Log Source Type	Creation Date	Last Event	Enabled	
Error	1						3 L 05 0000 0 00 MM (707)			
Not Available	4		00	Anomaly	Detection Engine-2 :: qradar732	Anomaly Detection Engine	JUL 25, 2023 8:39 AM (151)		O Un	
Disabled	0		67	Asset Pro	filer-2 :: qradar732	Asset Profiler	Jul 25, 2023 8:39 AM (IST)		© On	
nabled (2)			63	Custom F	ule Engine-8 :: qradar732	Custom Rule Engine	Jul 25, 2023 8:39 AM (IST)		© On	:
Yes	10		69	Health M	etrics-2 :: qradar732	Health Metrics	Jul 25, 2023 8:39 AM (IST)	Aug 9, 2023 4:17 PM (IST)	© On	:
No No	0		68	Search R	esults-2 :: qradar732	Search Results	Jul 25, 2023 8:39 AM (IST)	Aug 9, 2023 4:10 PM (IST)	On	1
og Source Type (9)			64	SIM Audi	t-2 :: qradar732	SIM Audit	Jul 25, 2023 8:39 AM (IST)	Aug 9, 2023 4:10 PM (IST)	🗢 On	
SentinelOne API	2		62	SIM Gen	ric Log DSM-7 :: qradar732	SIM Generic Log DSM	Jul 25, 2023 8:39 AM (IST)		© On	:
Anomaly Detection Engine	1		65	System N	otification-2 :: qradar732	System Notification	Jul 25, 2023 8:39 AM (IST)	Aug 9, 2023 4:17 PM (IST)	© On	:
Asset Profiler	1		112	test		SentinelOne API	Aug 2, 2023 3:54 PM (IST)		💽 0n	:
Custom Rule Engine	1		113	test1		SentinelOne API	Aug 2, 2023 4:48 PM (IST)	Aug 9, 2023 12:13 PM (IST)	💽 0n	:
Health Metrics	1									
SIM Audit	1									
SIM Generic Log DSM	1									
Search Results	1									
Sustem Notification	1									
- System Kouncution	-									
rotocol Type (1)		items	s per page	50 V	1-10 of 10 items			1 \	 1 of 1 pages 	

8. Select Single Log Source.

IBM QRadar Log Source Management				×
How man	y Log Source	s will you be	adding?	
	Single Log Source	Multiple Log Sources		

9. Select SentinelOne API as a log source type.



■ IBM QRadar Log Source Ma	anagement - Add a Single Log Source	×
Select Log Source Type		
O Select Protocol Type	Select a Log Source type	
O Configure Log Source Parameters	Q sentinelone ×	
 Configure Protocol Parameters 	SentinelOne API	
	Step 2: Select Protocol Type]

10. Select protocol type as Syslog.

■ IBM ORadar Log Source	Manaéement - Add a Single Log Source	>	×
Select Log Source Type			
Select Protocol Type	Select a protocol type		
 Configure Log Source Parameters 	Q. Sysied	×	
O Configure Protocol	Syslog		
Falameters	Syslog Redirect		
	TCP Multiline Syslog		
	TLS Syslog		
	UDP Multiline Syslog		
	Step 1: Select Log Source Type	onfigure Log Source Parameters	

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

=	IBM QRadar Log Source Mana	gement - Add a Single Log Source		×
0	Select Log Source Type			
0	Select Protocol Type	Configure the Log Source parameters		
	 Configure Log Source Parameters 	Name *	test	i.
¢	 Configure Protocol Parameters 	The name of the log source.	cog	
		Description An optional description of the log source.		
		Enabled Indicates whether the log source should be enabled.	On On	
		Groups * The groups that this log source will belong to.	Other X	
			Q + Add Group	
		Extension	Select V	
		+ Show More		
		Language * Select the language used for the log source's events to ensure correct and optimized parsing.	English ~	
		Tarset Event Collector *		
		The appliance responsible for receiving and parsing the events from this log source.	additionarchin = 16-115-21-70-17	
		Disconnected Log Collector *	None Available	

≡ IBM QRadar Log Source Man	agement - Add a Single Log Source		×								
 Select Log Source Type Select Protocol Type 	Configure the Log Source parameters										
 IBM QRadar Log Source Management - Select Log Source Type Select Protocol Type Configure Log Source Parameters Configure Protocol Parameters Targe The approximation Shore Credit Wene Coale Shore Shore 	Language * Select the language used for the log source's events to ensure correct and optimized parsing.	tunge * English Contracts events to ensure correct and optimized parsing.									
	Target Event Collector * The appliance responsible for receiving and parsing the events from this log source.	eventcollector0 :: ip-172-31-18-71	~								
	Disconnected Log Collector * The disconnected log collector that this log source will receive events on. * Show More	None Available									
	Credibility * The higher the credibility, the more certain you are that this log source emits reliable events. + Show More	5	<u>~</u>								
	Coalescing Events When a log source entits multiple events which are very similar to one another in a short time span, they'll be coalesced together. • Show More	C On									
	Store Event Payloads Enable to store original event payloads in addition to the normalized record. 4 Show More	Cn Cn									
	Step 2: Select Protocol Type	Step 4: Configure Protocol Parame	eters								

*Suggestion use default values

12. Configure theProtocol parameters



SentinelOne

- * Log Source Identifier value will be some unique value
- 13. Click Finish.
- 14. The created logsource will be enabled.

≡	IBM QRadar Log Source	Manageme	ent									
Filter		×	V	Q id:113	3				×	+	New Log Source	•
Statı	ok	Clear 0	Log So	urces (1)								¢
	Warning	0		ID	Name	\uparrow	Log Source Type	Creation Date	Last Event		Enabled	
	Error	0		113	test		SentinelOne API	27 Oct 2023 07:28 (UTC))		💿 On	+
	Not Available	1										
	Disabled	o										
Enab	led (2)											
	Yes	1										
	No	o										
Log S	ource Type (1)											
	SentinelOne API	1										
Proto	col Type (1)											
	Syslog	1	items	per page 50	\sim	1-1 of 1 it	ems			1 ~	1 of 1 pages	
Grou	n (1)											

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.

+Add New Input	(II) SentinelOne [.]								
Status Name URL Log Source Protocol type Supplicius threats enrichment Malicious threats enrichment Update interval (Seconds) Last data received at Status Actions				+ Add New Inp	put				
14 Frahled Frahled 30 configured Edit Delete	Status Name URL	Log Source	Protocol type	Suspicoius threats enrichment	Malicious threats enrichment	Update interval (Seconds)	Last data received at	Status	Actions
		3		Enabled	Enabled	30		configured	Edit Delete

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

Input Configuration
Input Configuration Name Enter a unique name for the data input URL Console's URL. Example: https://mycompany.sentlinelone.net API Token Enter the User API token generated in the SentlinelOne Console Interval (See) 30 Time interval for input in seconds. Default: 30 seconds Start Time AII Data Orom Date OPEN Choose if to pull all available data or from a specific date Test Connection

- 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.



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.

(ii) s	entine	elOne [.]								
					+ Add New	Input				
Status	Name	URL	Log Source	Protocol type	Suspicolus threats enrichment	Malicious threats enrichment	Update interval (Seconds)	Last data received at	Status	Actions
		and in plates of a links of		ТСР	Enabled	Enabled	30	11:58:39 18/1/2023	configured	Edit Delete
				UDP	Enabled	Enabled	30	19:00:29 12/1/2023	configured	Edit Delete



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.

E IBM QRadar		Ļ	<u>0</u>
Dashboard Offenses Log	Astrily NewookAstrily Assets Reports Roka Valaerabilities Astriin	System Time	: 15:02
Offenses	Display: Twin 👻 Group: Select a group 💿 Comp. 🖉 Revert Nation extensione 🔍 Vee the BM App Exchange for more		0
My Offenses Al Offenses By Category By Source IP By Source IP By Settook Ry Network	Performance Rule Name Group Rule Category Mee Store Rule SentraciOne New SentraciOne New SentraciOne New Cuttors Rule Mee Store Rule New Common Rule Depatch New Event 0 0 User 19 May 5023, 12:06 9 Aug 2023, 07:27 Depatch New Event 0 Depatch New Event 0 0 User 19 May 5023, 12:06 9 Aug 2023, 07:27 Depatch New Event 0 Depatch New Event 0 0 User 19 May 5023, 12:06 9 Aug 2023, 07:27 Mee Common Rule Mee Common Rule Mee Common Rule 0 User 19 May 5023, 12:06 9 Aug 2023, 07:27 Depatch New Event 0 Depatch New Event 0 User 19 May 5023, 12:06 9 Aug 2023, 07:27		
	Note Performance Analysis Notes Performance Analysis This rule has not yet had a detailed analysis. This rule has not yet had a detailed analysis.		•

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 <u>Customer Rule Engine-8</u>
 ;; <u>qradar742</u>
 - and when the event matches ThreatID (custom) is not N/A

ch tests do you wish to perform on incoming events? t Group All	luilding Block
t Group All Export as B Contract Contract Export as B Contract Contra	uilding Block
to filter when the local network is one of the following networks when the destination network is one of the following networks	
when the local network is one of the following networks when the destination network is one of the following networks	
when the destination network is one of the following networks	0
when the IP protocol is one of the following protocols	
when the Event Payload contains this string	
when the source port is one of the following ports	
when the destination port is one of the following ports	
when the remote part is one of the following ports	
when the source IP is one of the following IP addresses	
when the destination IP is one of the following IP addresses	
a (Click on an underlined value to edit it)	



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

Rule Wiza	rd: Rule Respor	ise	
ule Action pose the action(s) to	ake when an event occu	rs that triggers t	this rule
Severity	Set to 🗸	0 ~	
Credibility	Set to 🔗	0 ~	
Relevance	Set to 🗸 🗸	0 ~	
Ensure the dete	cted event is part of an o	flense	
Index of	ense based on Threatl	D (custom)	*
Anno	late this offense:		
🗆 Inclue	le detected events by Th	reatID (custom)	from this point forward, in the offense, for : second(s)
Ile Response pose the response(s)	to make when an event t	riggers this rule	
1			
Enter the details	of the event to dispatch	2	
Enter the details Event Name: Event Description	of the event to dispatch SentinelOne New threat In: SentinelOne New thre	at	
Enter the details Event Name: Event Description Event Details: Severity 5	of the event to dispatch SentinelOne New threat In: SentinelOne New threat Credibility 10 v	at Relevance 10	
Enter the details Event Name: Event Description Event Details: Severity 5 High-Level Co	of the event to dispatch SentineiOne New threat SentineiOne New threat SentineiOne New threat Credibility 10 v tegory: Suspicious Activ	Relevance 10) ↓ rel Category: Suspicious Activity
Enter the details Event Name: Event Description Event Details: Severity 5 High-Level Cr Annotate this	of the event to dispatch SentineiOne New threat SentineiOne New threat Credibility 10 v tegory Suspicious Activ offense:	at Relevance 10 ity v Low-Lev) V rel Category: Suspicious Activity
Enter the details Event Name: Event Description Event Details: Severity 5 High-Level C: Annotate this Ensure the di Index off	of the event to dispatch SentineiOne New threat SentineiOne New threat Credibility 10 v ategory: Suspicious Activ offense upatched event is part of mes based on Threatil	at Relevance 10 ity v Low-Lev an offense 2 (custom)	vel Category: Suspicious Activity
Enter the details Event Name: Event Description Event Details: Severity 5 High-Level Cr. Annotate this Ensure the di- Index official	of the event to dispatch SentineiOne New threat SentineiOne New threat Credibility 10 Credibility 10 ategory: Suspicious Activ offense: Ipatched event is part of Inse based on Threatt	Relevance 10 ity v Low-Lev an offense) (custom)	vel Category: Suspicious Activity

Rule Name	SentinelOne New Threat
Rule Logic	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
Building blocks	None
Rule Action	Ensure the detected event is part of an offense > Indexed based on ThreatID (custom)
Rule Response	Dispatch New Event: Event name: SentinelOne new threat Description: New threat by SentinelOne HLC: Suspicious activity LLC: Suspicious activity • Ensure the dispatched event is part of an offense > Indexed based on ThreatID (custom) • This information should set or replace the name of the associated offense(s)
Response Limiter	None
Notes	None
Dependencies	Sentinelone API Custom Properties: > ThreatID (custom)

- 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

- Event Types: The App has mapping for all SentinelOne event types that were available until Management Console version North Pole GA. You can manually map events from later versions.
- **Threat Property Mapping**: The app has specific rules to give visibility to the main threat properties in the UI. When you open a threat-related event, the main properties automatically show in the QRadar UI.

🔝 Ream to Evert List 🐘 Offices 🔗 Map Evert 🤸 Faller Paulity 👸 Edited Property 🚱 Physical 🔇 Net 💩 Obligation 🔻										
Event Information										
Event Name	New Threat Not Miggland									
Low Level Category	Uninoun Mahare									
Event Description	New Thread Not Milgand									
Magnitude	(3)	(3) Relevance 1 Severity 5 Credibility								
Username										
Start Time	73, 2021, 65359 AM 52021, 65459									
AccountID (custom)	261100									
AccountName (custom)	SentinelOne									
ActivityID (custom)	103/72667302814232									
Agent Updated Version	None									
AgentID (custom)	1065084636959413403									
Comments (custom)	None									
Computer Name (custom)	DESKTOP									
Confidence Level (custom)	malicious									
File Path (custom)	3WanaDecryptor@.exe									
FileID (custom)	N/A									
Filename (custom)	@WaraDoryptor@.exe									
Group Name (custom)	WINTEST									
GroupID (custom)	107794006547100432									
OS Name (custom)	None									
Primary Description (custom)	Thread with confidence level malicious detected: @WanaDecryptor@.exe									
Secondary Description (custom)	455560491									
Site Name (custom)	Jungru									
SiteID (custom)	1841077981340208959									
Threat Classification (custom)	Ransomware									
Threat Classification Source (custom)	Cloud									
ThreatID (custom)	103172667193762328									
User ID (custom)	N/A									
Domain	Default Domain									
ource and Destination Infor	mation									
Source IP	1000000		Destination IP	1001000000						
Source Asset Name	N/A		Destination Asset Name	NA						
Source Port	0	Destination Port	0							
Pre NAT Source IP	Pre NAT Destination IP									
Pre NAT Source Port	0	Pre NAT Destination Port	0							
Post NAT Source IP	Post NAT Destination IP									
Post NAT Source Port	0 Post NAT Destination Port 0									
Source IPv6	0.0.0.0.0.0.0		Destination IPv6	0.0:0.0:0:0:0:0						
Source MAC	00.00.00.00.00		Destination MAC	00:00:00:00:00:00						
Payload Information										

• **Correlate events based on ThreatID**: When you use the SentinelOne recommended custom offense rule, it is easier to find all the related events with one click.

≡ IBM QRadar											¢ o
Dashboard Offenses L	og Activity Network Activity	y Assets Reports	Admin Hello World Pre-Validation								System Time: 2:04 PM
Offenses	All Offenses > Offense 7	71671 (Summary)									
My Offenses	Offense 71671 Barris V. Davis V. Chura Autors V. Anna							• 🐣 Print 🔞			
All Offenses	Magnitude	Lances T			atus 🗟	Relevance 0 Severity 6 Credibility 2					
By Category				01	fense Type	Threat id (cust	om)	1002.570°			
By Source IP	Description	Ev	Event/Flow count 2.046 events and 0 flows in 8 categories								
Du Destination ID	Source IP(s)	Multiple (2)			art	Feb 8, 2021, 10:42:59 AM					
by peschadion in	Destination IP(s)	169.254.3.4			uration	10m 37s					
By Network	Network(s)	other		A	ssigned to	Unassigned					
Rules	Offense Source Summary										
	Custom property value	1071441461506171953									
	Offenses	3							Events/Flows	2,058	
		0									
	Last 5 Notes Creation Control										
	Notes						Us	sername		Creation Date	
	No results were returned.										
	Magnitude		Started 0	Started On		Ended On Duratio		ion	on Events/Flows		
	No results were returned.										
	Source Magn	loc Loc	tion Vulnerability	User	MAG		Weight	Offenses	Destination(s)	Last Event/Flow	Events/Flows
	169	other	No	Unknown	Unknown NIC	0		72,326	0	22d 12h 23m 55s	953,872
	:*: 223	South Korea	No	Unknown	Unknown NIC	0		29	0	23d 3h 9m 51s	20,384
	Top 5 Log Sources										
	Name		Description		Group		Events		Offenses		Total Events
	Custom Rule Engine-8 :: s1_dsm_4	qradar742 Cu	stom Rule Engine			1,023 1,023		73.819 71.903		487,428 474,541	
	Top 5 Users										29 Users

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",

SentinelOne[®]

```
"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,

() SentinelOne

```
"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,
```





"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,

"agentlp": "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,

"dstlp": 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",

"srclp": 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, "totalltems": 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

() SentinelOne

"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":

"eyJpZF9jb2x1bW4iOiAiQWN0aXZpdHkuaWQiLCAiaWRfdmFsdWUiOiAxNTkxMjE5MDc0NTY 4ODE3MTQ3LCAic29ydF9ieV9jb2x1bW4iOiAiQWN0aXZpdHkuaWQiLCAic29ydF9ieV92YWx1 ZSI6IDE1OTEyMTkwNzQ1Njg4MTcxNDcs ICJzb3J0X29yZGVyljogImFzYyJ9",

"totalltems": 15992

}

}