



# SentinelOne for QRadar v3.5.x

---

Integration Guide

3 October 2019

Copyright © 2019 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. QRadar and SentinelOne Integration .....	1
1.1. QRadar and SentinelOne Integration Highlights .....	1
2. Requirements .....	5
3. The SentinelOne DSM for QRadar .....	6
3.1. Installing the SentinelOne DSM in QRadar .....	6
3.2. Adding SentinelOne as a Log Source for QRadar .....	9
3.3. Integrating Your QRadar Syslog Server to SentinelOne .....	12
3.4. Seeing SentinelOne Events in QRadar .....	15
4. The SentinelOne App for QRadar .....	21
4.1. Installing the SentinelOne App in QRadar .....	21
4.2. Generate an API Token .....	27
4.3. Adding SentinelOne Management Consoles to the SentinelOne App .....	28
4.4. Using the SentinelOne App .....	29
5. Upgrading From the Beta Version .....	34
6. Advanced Configuration .....	36
6.1. Configuring the Syslog Format .....	36
6.2. Finding SentinelOne Events .....	37
6.3. Regular Expressions for Mapping .....	38
7. Troubleshooting .....	40

# 1. QRadar and SentinelOne Integration

The integration of IBM® QRadar® Security Information and Event Management (SIEM) with SentinelOne® empowers organizations to combine the strengths of QRadar to consolidate, correlate, and aggregate log events and network flow data, with the visibility, detection, response, remediation and forensics capabilities of SentinelOne.

These are the components of this integration:

- **SentinelOne Device Support Module (DSM) for QRadar:** Collects the Syslog output from the SentinelOne Management as a log source for QRadar. Use the QRadar Console to see information in your environment, gathered from SentinelOne.
- **SentinelOne App:** An application running on the QRadar platform enabling you to see information about the endpoints in your environment, taken from SentinelOne, and take action. From the App, you can go to the SentinelOne Management Console.

## 1.1. QRadar and SentinelOne Integration Highlights

After installing and running the SentinelOne DSM and App for QRadar, you can:

- View a list of threats from the SentinelOne App for QRadar Analyze page.

Status	File Name	Endpoint	Created	Updated	Site	Classification	Action Done
✓	BwawWoYU.exe	desktop Enterprise-Desktop	05/05/2019 07:11	05/05/2019 08:02	Demo TEST	Malware	quarantine, kill
✓	CV.exe	desktop Enterprise-Desktop	05/05/2019 07:11	05/05/2019 08:02	Demo TEST	Malware	rollback, quarantine, kill, remediate
✓	CV.exe	desktop Enterprise-Desktop	05/05/2019 07:11	05/05/2019 08:02	Demo TEST	Malware	rollback, quarantine, kill, remediate
✓	CV.exe	desktop Enterprise-Desktop	05/05/2019 07:11	05/05/2019 08:02	Demo TEST	Malware	quarantine, kill
✓	CV.exe	desktop Enterprise-Desktop	05/05/2019 07:11	05/05/2019 08:02	Demo TEST	Malware	quarantine, kill
✓	CV.exe	desktop Enterprise-Desktop	05/05/2019 07:08	05/05/2019 07:09	Demo TEST	Malware	quarantine, kill
✓	CV.exe	desktop Enterprise-Desktop	05/05/2019 07:08	05/05/2019 07:09	Demo TEST	Malware	quarantine, kill
✓	xwURh1MX.exe	desktop Enterprise-Desktop	05/05/2019 06:45	05/05/2019 06:52	Demo TEST	Ransomware	rollback, quarantine, kill, remediate
✓	BwawWoYU.exe	desktop Enterprise-Desktop	05/05/2019 06:45	05/05/2019 06:52	Demo TEST	Ransomware	quarantine, kill
✓	xwURh1MX.exe	desktop Enterprise-Desktop	05/05/2019 06:45	05/05/2019 06:52	Demo TEST	Ransomware	rollback, quarantine, kill, remediate

- View threat details and mitigate threats from the QRadar console. SentinelOne authorized users can also click a hyperlink to the SentinelOne Management Console Forensics page.

IBM QRadar SentinelOne Console

File Info

- File Name: RvawWeYO.exe
- Path: \Device\HarddiskVolume2\Users\adm...

Device

- Device: Enterprise-Desktop
- IP: 192.168.1.100
- Domain: WORKGROUP
- Username: ENTERPRISE-DESK\admin
- Agent version: 3.1.1.12
- Site: Demo TEST
- Group: Default Group

Time

- Created: 05/05/2019 07:11
- Updated: 05/05/2019 08:02

Summary

- Status: mitigated
- SHA1: 0da2192d5b9aaef3a4b02c0c3816f8...
- Threat ID: 619175708896182112
- Detecting engine: pre\_execution
- Classification: Malware
- Signer Identity: N/A
- Group: Default Group
- Management: Demo TEST

Indicators

- Hiding/Stealthiness**  
The majority of sections in this PE have is a sign of obfuscation/packing.
- General**  
This binary imports functions used to raise the process priority.
- Hiding/Stealthiness**  
This binary may contain encrypted/compressed info as measured by high entropy of the sections (>6.8)
- General**  
This binary imports debugger functions

Actions

- Mark as Benign
- Mark as Threat
- Kill
- Quarantine
- Un-quarantine
- Remediate
- Rollback Remediation
- Resolve

- Filter threat lists from the SentinelOne App for QRadar Network page.

IBM QRadar SentinelOne Console

Filter: Search nirg Active All OS All Apply 10 Results

Endpoint Name	Site	Group	Domain	Console Visible IP	Agent Version	Last Logged User	Last Active
nirg-macos-vm1	AcmeHoldings	Default Group	local	192.168.1.100	2.6.5.2559	nirg	23/04/2019 13:25
nirg-centos-dev22	AcmeHoldings	Default Group	local	192.168.1.100	2.6.5.1704		22/04/2019 18:38
nirg-ubuntu-dev23	AcmeHoldings	Default Group	localdomain	192.168.1.100	2.6.5.1704		05/05/2019 09:42
nirg-ubuntu-dev02	AcmeHoldings	Default Group	localdomain	192.168.1.100	2.6.4.1685		22/04/2019 17:32
nirg-ubuntu18-dev19	ABC-Corp	Default Group	unknown	192.168.1.100	3.0.0.305	unknown	03/05/2019 13:24
nirg-rhel7-dev18	ABC-Corp	Default Group	unknown	192.168.1.100	3.0.0.1		02/05/2019 17:04
nirg-ubuntu19-dev31	ABC-Corp	Default Group	local	192.168.1.100	3.0.1.391		02/05/2019 17:02
nirg-debian9-dev34	ABC-Corp	Default Group	sentinel.local	192.168.1.100	3.0.1.391		29/04/2019 18:59
nirg-rhel7-dev21	ABC-Corp	Default Group	unknown	192.168.1.100	3.0.2.400		05/05/2019 09:42

- Disconnect an endpoint from the network and see endpoint associated information, such as the last logged in user and threat history.

The screenshot shows the SentinelOne interface for host 'nirg-macos-vm1'. The top navigation bar includes Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, Admin, and SentinelOne. The host details section shows:

- General:** Agent Version: 2.6.5.2559, Scan Status: none, Memory: 2048, CPU: Intel(R) Core(TM) i9-8950HK CPU @..., Core Count: 2, Disk Encryption: False.
- Network Adapters:** A table with columns Name, IP, and Mac Address. It lists 'utun0' and 'en0'.
- Threats:** A table listing detected threats with columns: Status, File Name, Endpoint, Created, Updated, Site, Classification, and Action Done. Threats include 'vmware-tools-daemon', 'uninstallTools', 'preinstall', 'sh', 'invoices.docx', and 'malware'.

- Use the SentinelOne DSM to create saved searches and dashboards.

The screenshot shows an advanced search in the SentinelOne interface. The search criteria is: `select * from events where LOGSOURCEIPNAME(devicetype) = 'SentinelOne'`. The search results are displayed as a 'Records Matched Over Time' chart and a table.

**Current Statistics:**

- Total Results: 77 (107KB Total)
- Data Files Searched: 60 (6.5MB Total)
- Compressed Data Files Searched: 0 (0B Total)
- Index File Count: 56 (2.7MB Total)
- Duration: 12ms

**Records Matched Over Time:** A line chart showing the number of records matched over time from 7:00 AM to 12:30 PM. The chart shows several peaks, with the highest being around 10:00 AM.

**Table of Results:**

starttime	protocolid	sourceip	logsourceid	qid	sourceport	eventcount	magnitude	identityip	destinationip	destinationport	category	username
1557040490122	255		118	1002250034	0	4	4	0.0.0.0		0	6001	admin
1557040738948	255		118	1002250008	0	2	3	0.0.0.0		0	8008	admin
1557040739848	255		118	1002250145	0	3	3	0.0.0.0		0	8053	admin
1557041294243	255		118	1002250212	0	1	3	0.0.0.0		0	8037	mgmtauto
1557041299105	255		118	1002250213	0	1	3	0.0.0.0		0	8006	N/A
1557040718930	255		118	1002250008	0	1	3	0.0.0.0		0	8008	admin
1557040723948	255		118	1002250010	0	1	4	0.0.0.0		0	6019	admin
1557040723948	255		118	1002250145	0	1	3	0.0.0.0		0	8053	admin
1557040728965	255		118	1002250010	0	1	4	0.0.0.0		0	6019	admin
1557040723948	255		118	1002250145	0	3	3	0.0.0.0		0	8053	admin
1557040723947	255		118	1002250008	0	2	3	0.0.0.0		0	8008	admin
1557040478992	255		118	1002250034	0	1	4	0.0.0.0		0	6001	admin
1557040414087	255		118	1002250188	0	1	5	0.0.0.0		0	8003	Demo-test
1557040414087	255		118	1002250216	0	1	5	0.0.0.0		0	8016	Demo-test
1557040229310	255		118	1002250008	0	1	3	0.0.0.0		0	8008	admin
1557040329310	255		118	1002250034	0	1	4	0.0.0.0		0	6001	admin
1557040329310	255		118	1002250034	0	1	4	0.0.0.0		0	6001	admin
1557040334351	255		118	1002250145	0	1	3	0.0.0.0		0	8053	admin
1557040334351	255		118	1002250008	0	1	3	0.0.0.0		0	8008	admin
1557040340073	255		118	1002250145	0	1	3	0.0.0.0		0	8053	admin
1557040379006	255		118	1002250165	0	1	4	0.0.0.0		0	6019	admin
1557040379006	255		118	1002250165	0	1	4	0.0.0.0		0	6019	admin
1557040488822	255		118	1002250212	0	1	3	0.0.0.0		0	8037	mgmtauto
1557034133925	255		118	1002250213	0	1	3	0.0.0.0		0	8006	N/A
1557030433904	255		118	1002250212	0	1	3	0.0.0.0		0	8037	mgmtauto
1557030459656	255		118	1002250213	0	1	3	0.0.0.0		0	8006	N/A
1557030033957	255		118	1002250003	0	1	3	0.0.0.0		0	8036	dbarc
1557030033957	255		118	1002250003	0	1	3	0.0.0.0		0	8036	N/A

- Use the SentinelOne DSM to classify and parse SentinelOne content rich Syslogs.

IBM QRadar
System Time: 12:51 PM

Dashboard Offenses Log Activity Network Activity Assets Reports Admin SentinelOne

Return to Event List Offense Map Event False Positive Extract Property Previous Next Print Obfuscation

#### Event Information

Event Name	NEW_THREAT_NOT_MITIGATED		
Low Level Category	Unknown Malware		
Event Description			
Magnitude	(4)	Relevance	3
Severity	4	Credibility	5
Username	admin		
Start Time	May 5, 2019, 10:14:50 AM	Storage Time	May 5, 2019, 10:15:50 AM
Log Source Time	May 5, 2019, 10:14:59 AM		
AccountDomain (custom)	WORKGROUP		
Action (custom)	active		
AgentId (custom)	3d68b0d67d67c5e2be83c538d5b9edcea23b81		
Category Description (custom)	New active threat - machine Enterprise-Desktop		
Event Summary (custom)	New active threat - machine Enterprise-Desktop		
File Hash (custom)	Dda2192d5b9aaef3a4b2c0c38f8879496841		
File Path (custom)	\\Device\\HarddiskVolume2\\Users\\admin\\Desktop\\CV.exe		
Filename (custom)	CV.exe		
Hostname (custom)	Enterprise-Desktop		
Service (custom)			
Source Host Name (custom)	Enterprise-Desktop		
Threat Classification (custom)	Malware		
Threat Count (custom)	3		
Threat Id (custom)	61917577631244114		
UNIX path name (custom)	N/A		
deviceHostName (custom)	usea1-purple.sentinelone.net		
eventDesc (custom)	New active threat - machine Enterprise-Desktop		
siteName (custom)	Demo TEST		
sourceDnsDomain (custom)	WORKGROUP		
Domain	Default Domain		

#### Source and Destination Information

Source IP	172.31.2.68	Destination IP	172.31.2.68
Source Asset Name	N/A	Destination Asset Name	N/A
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	Destination IPv6	0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

#### Payload Information

```

utf | hex | base64
-----|-----|-----
Wsp Text
[14-2019-05-05 07:14:58,950 sentinel - CFP:2|sentinelone|Wgnt|Windows 10|deviceAddress=...|deviceHostPgn=usea1-purple.sentinelone.net|deviceHostName=usea1-purple.sentinelone.net|notificationScope=6176|eventId=3911660434620493|siteName=Demo TEST|vendor=sentinelone|originatorName=Enterprise-Desktop|originatorSource=...|...|eventID=19|eventDesc=new active threat - machine Enterprise-Desktop|eventSeverity=1|t=2019-05-05 07:11:20.719922|fileName=\\Device\\HarddiskVolume2\\Users\\admin\\Desktop\\CV.exe|fileHash=Dda2192d5b9aaef3a4b2c0c38f8879496841|threatClassification=Malware|threatClassificationSource=StatC|threatDetectingEngine=Windows_executable|threatClassifier=LOGIC|threatMitigationStatusLabel=active|threatMitigationStatusID=1|threatCommandLineArguments=|threatID=61917577631244114|sourceAgentLastActivityTimestamp=2019-05-05 07:11:20.709401|sourceAgentRegisterTimestamp=2019-01-11 01:38:47.328185|sourceOsWorkstation=connected|sourceOsRevision=17763|sourceOsType=Windows|sourceAgentUtlid=3d68b0d67d67c5e2be83c538d5b9edcea23b81|sourcePgn=WORKGROUP_Enterprise-Desktop|sourceThreatCount=3|sourceMgmtPreceivedAddress=76.244.36.171|sourceDnsDomain=WORKGROUP|sourceHostName=Enterprise-Desktop|sourceUserName=admin|sourceUserId=S-1-5-21-4097623257-2326715497-2399078956-1001|cat=WSMALAR]
                    
```

#### Additional Information

Protocol	255	QID	1002250034
Log Source	Sen...	Event Count	4
Custom Rules	Destination Asset Weight is Low Source Asset Weight is Low Context is Remote to Local		
Custom Rules Partially Matched			
Annotations	Relevance has been decreased by 2 because the destination network weight is low. Relevance has been decreased by 2 because the source network weight is low. Relevance has been increased by 2 because the context is Remote to Local.		
Log Only (Exclude Analytics)	False		

#### Identity Information

Identity Username	N/A	Identity Host Name	N/A
Identity IP	N/A	Identity MAC	N/A
Identity Net Bios Name	N/A	Identity Group Name	N/A
Identity Extended Field	N/A		
Has Identity (Flag)	False		

SentinelOne

SentinelOne for QRadar v3.5.x

4

## 2. Requirements

- QRadar 7.2.8 patch 7 or higher.
- One of these SentinelOne Management versions: Eiffel, Fuji, and above. Versions Central Park and Denali are expected to work although they are End Of Service (EOS).
- SentinelOne App for QRadar.

**Note:** The SentinelOne App is not supported on Internet Explorer.

- DSM Syslog Parsing and Classification for SentinelOne
- In QRadar, allow Syslog TLS, Syslog, or the forwarding of incoming data.
- In SentinelOne, configure Syslog integration.

## 3. The SentinelOne DSM for QRadar

To see SentinelOne logged events in the QRadar Console:

1. Make sure the QRadar Console is installed and running.
2. Install the SentinelOne DSM in QRadar.
3. Add SentinelOne as a log source for QRadar.
4. Integrate your QRadar Syslog Server to SentinelOne.
5. See that SentinelOne events appear on the QRadar Console.

### 3.1. Installing the SentinelOne DSM in QRadar

The SentinelOne DSM enables you to send SentinelOne log events and endpoint data to the QRadar Console.

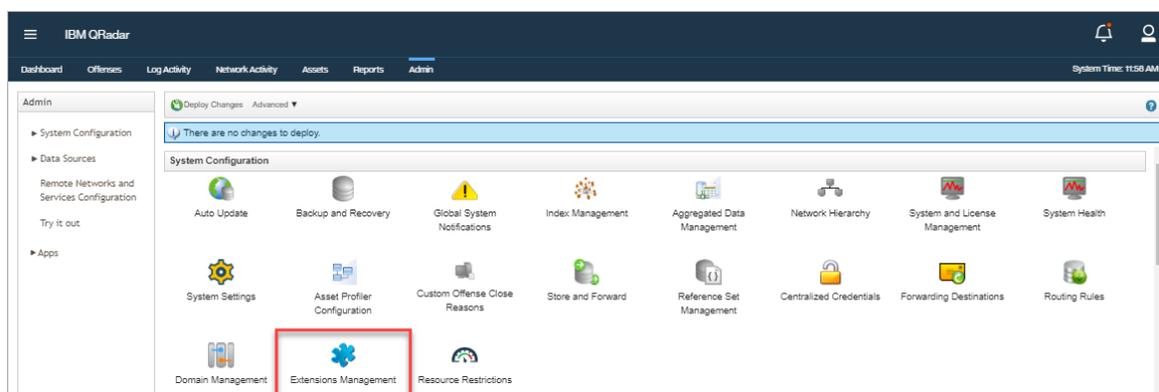
**Important:** If you have an earlier version of the SentinelOne DSM, you must remove it before you install the new DSM. Go to [Upgrading From the Beta Version \[34\]](#) and follow the instructions.

#### To install the SentinelOne DSM:

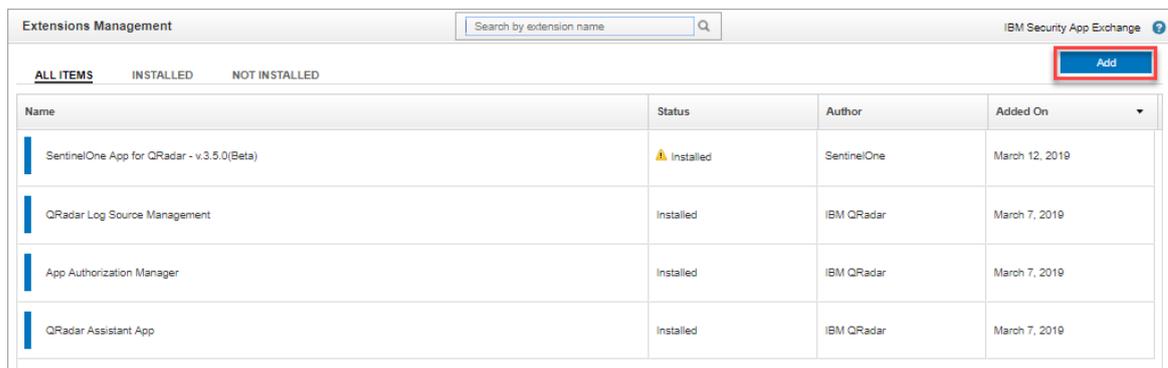
1. Download the SentinelOne DSM ZIP file available on [IBM App Exchange](#).
2. Log in to the QRadar Console as Admin.
3. From the Main menu, click **Admin**.



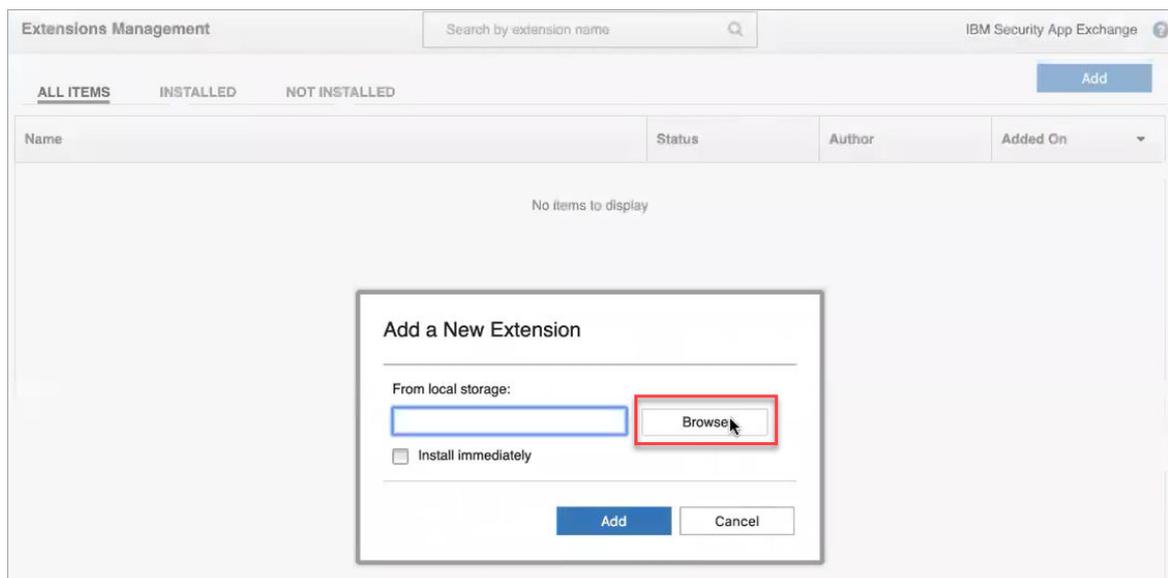
4. Click **Extensions Management**.



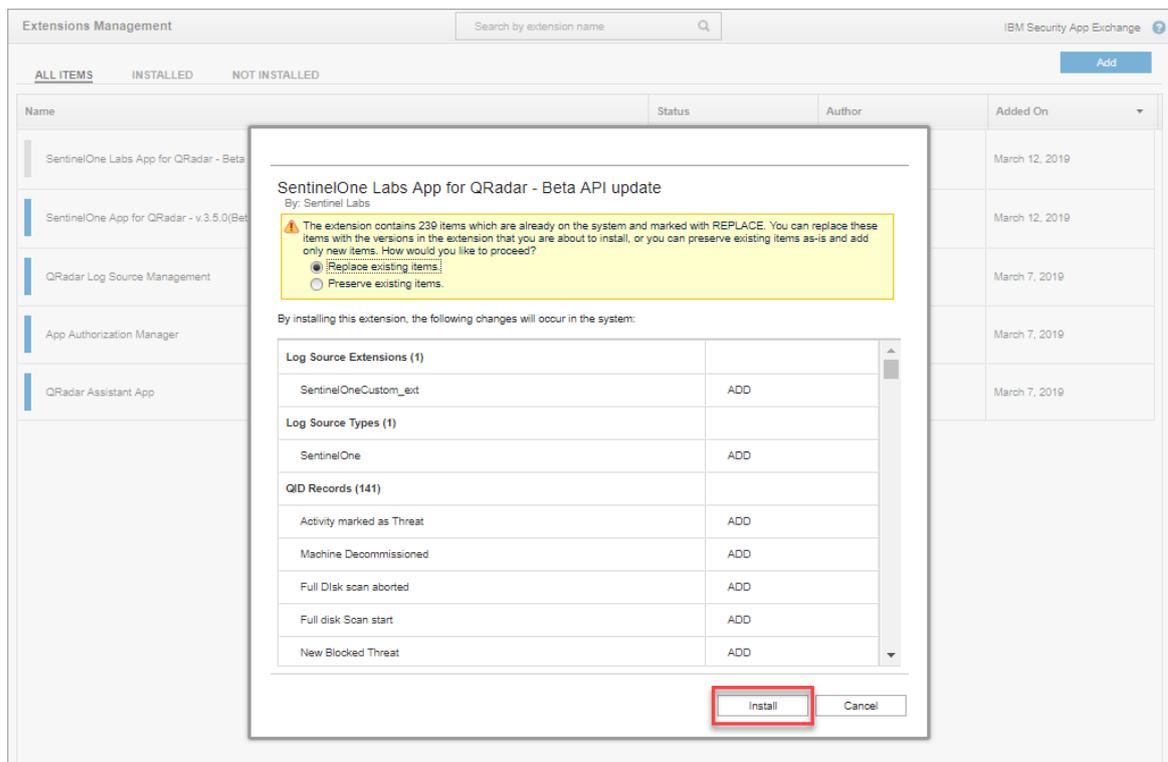
5. In the window that opens, click **Add**.



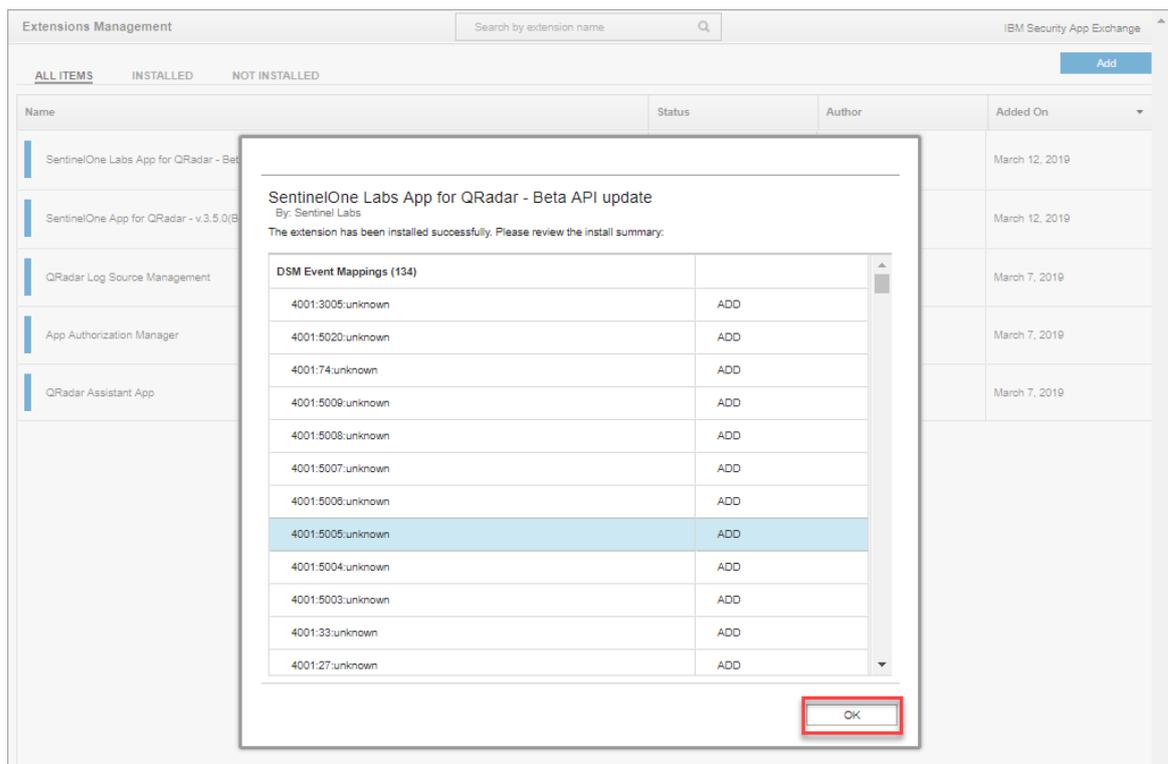
- In the window that opens, click **Browse**. Browse to the location of the downloaded SentinelOne DSM file.



- To immediately install the app, select **Install immediately** and click **Add**.
- Click **Install**.



9. In the window that opens, click **OK**.



The SentinelOne DSM is installed and appears in the list of Extensions.

Extensions Management			
Search by extension name			IBM Security App Exchange
ALL ITEMS	INSTALLED	NOT INSTALLED	Add
Name	Status	Author	Added On
SentinelOne DSM for QRadar - v.3.5.0(Beta)	Installed	Sentinel Labs	March 12, 2019
SentinelOne App for QRadar - v.3.5.0(Beta)	Installed	SentinelOne	March 12, 2019
QRadar Log Source Management	Installed	IBM QRadar	March 7, 2019
App Authorization Manager	Installed	IBM QRadar	March 7, 2019
QRadar Assistant App	Installed	IBM QRadar	March 7, 2019

10. Exit the **Extensions Management** window.

## 3.2. Adding SentinelOne as a Log Source for QRadar

Add each SentinelOne Console as a log source to define how QRadar gets Syslog messages from SentinelOne.

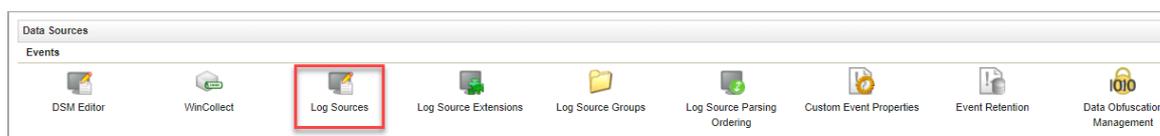
**To add SentinelOne as a log source for QRadar using the TLS syslog protocol:**

Use the TLS Syslog protocol for QRadar to receive encrypted syslog events from SentinelOne.

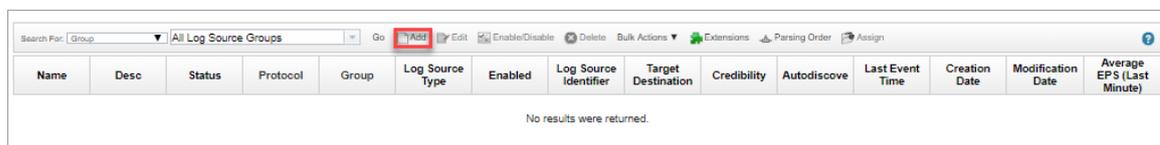
1. Log in to the QRadar Console as Admin.
2. From the Main menu, click **Admin**.



3. Click **Log Sources**.



4. Click **Add**.



5. In the form that opens:

- **Log Source Name:** Enter a unique name of the log source.
- **Log Source Type:** Select **SentinelOne**.

- **Protocol Configuration:** Select **TLS Syslog**. See [TLS syslog protocol configuration options](#).
- **Log Source Identifier:** Enter **sentinel.net**.
- **TLS Listen Port:** Make sure it is set to **6514**.
- **Log Source Extension:** Make sure **SentinelOneCustom\_ext** is selected.

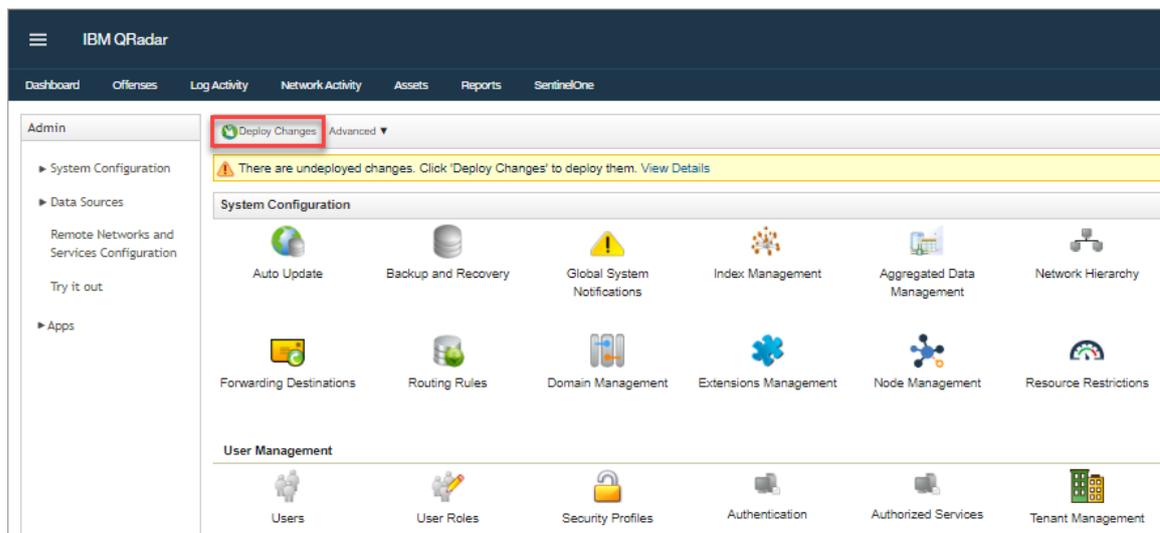
For the other fields, use the default settings or other values according to your environment.

### Add a log source

Log Source Name	SentinelOne
Log Source Description	
Log Source Type	SentinelOne
Protocol Configuration	TLS Syslog
Log Source Identifier	sentinel.net
TLS Listen Port	6514
Authentication Mode	TLS
Certificate Type	Generate Certificate
Maximum Connections	50
TLS Protocols	TLS 1.2 and above
Enabled	<input checked="" type="checkbox"/>
Credibility	5
Target Event Collector	eventcollector0 :: int-qrd-es-dev3
Coalescing Events	<input checked="" type="checkbox"/>
Store Event Payload	<input checked="" type="checkbox"/>
Log Source Language	
Log Source Extension	SentinelOneCustom_ext

Please select any groups you would like this log source to be a member of:

6. Click **Save**.
7. Close the **Log Sources** window.

8. Click **Deploy Changes**.

- Configure a second log source, using either the **Syslog** or **Forwarded** protocol. For instructions, see [To add SentinelOne as a log source for QRadar using the Syslog or Forwarded protocol \[11\]](#).

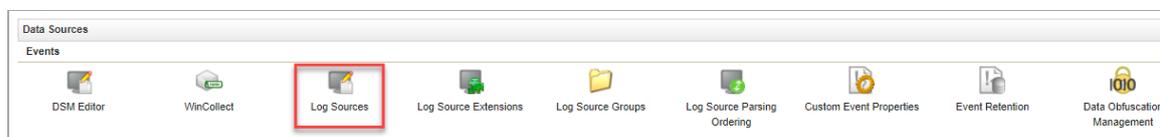
### To add SentinelOne as a log source for QRadar using the Syslog or Forwarded protocol:

Use the Syslog or Forwarded protocol for QRadar to receive unencrypted syslog events from SentinelOne.

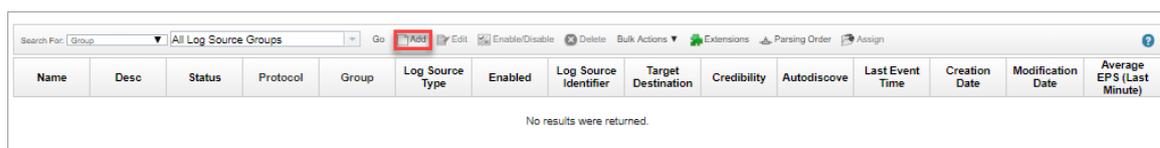
- Log in to the QRadar Console as Admin.
- From the Main menu, click **Admin**.



- Click **Log Sources**.



- Click **Add**.

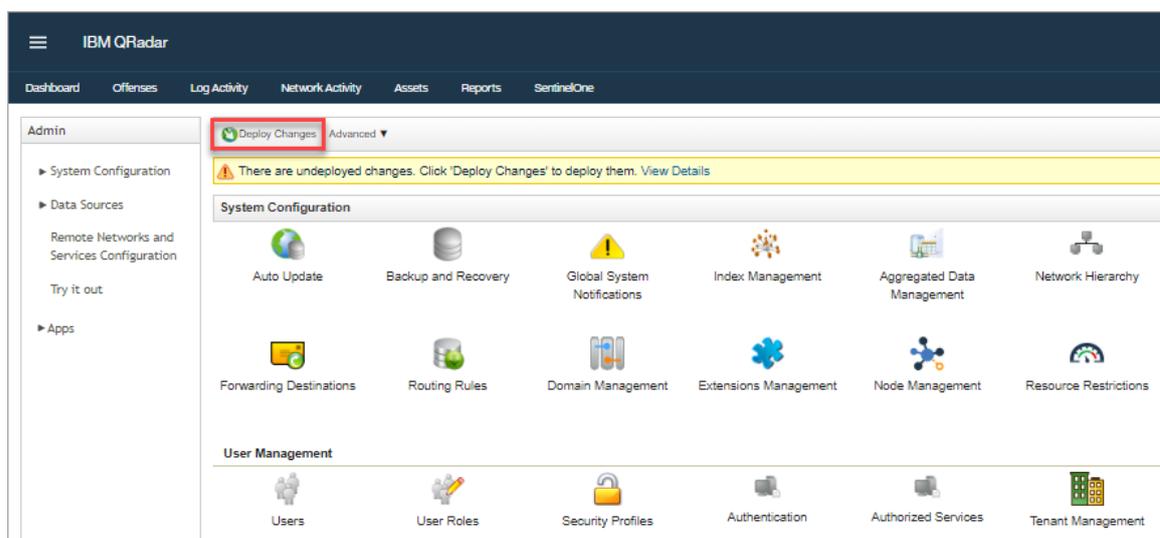


- In the form that opens:

- **Log Source Name:** Enter a unique name of the log source.
- **Log Source Type:** Select **SentinelOne**.
- **Protocol Configuration:** Select **Syslog** or **Forwarded**.
- **Log Source Identifier:** Enter the IP address of the SentinelOne Management Console.
- **Log Source Extension:** Make sure **SentinelOneCustom\_ext** is selected.

For the other fields, use the default settings or other values according to your environment.

6. Click **Save**.
7. Close the **Log Sources** window.
8. Click **Deploy Changes**.



### 3.3. Integrating Your QRadar Syslog Server to SentinelOne

Integrate your QRadar Syslog server to collect SentinelOne logs.

#### To integrate your Syslog server:

1. Open a supported browser on a computer with an active connection to the Internet (or to the On-Prem Management).

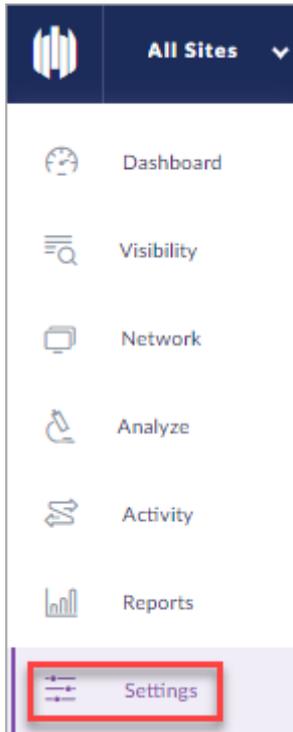
For a list of supported browsers, see [System Requirements](#).

2. In the browser address bar, enter the management console URL provided by the SentinelOne support team (for example, <https://yourcompany.sentinelone.net/>).
3. Enter your username and password, and click **Login**.

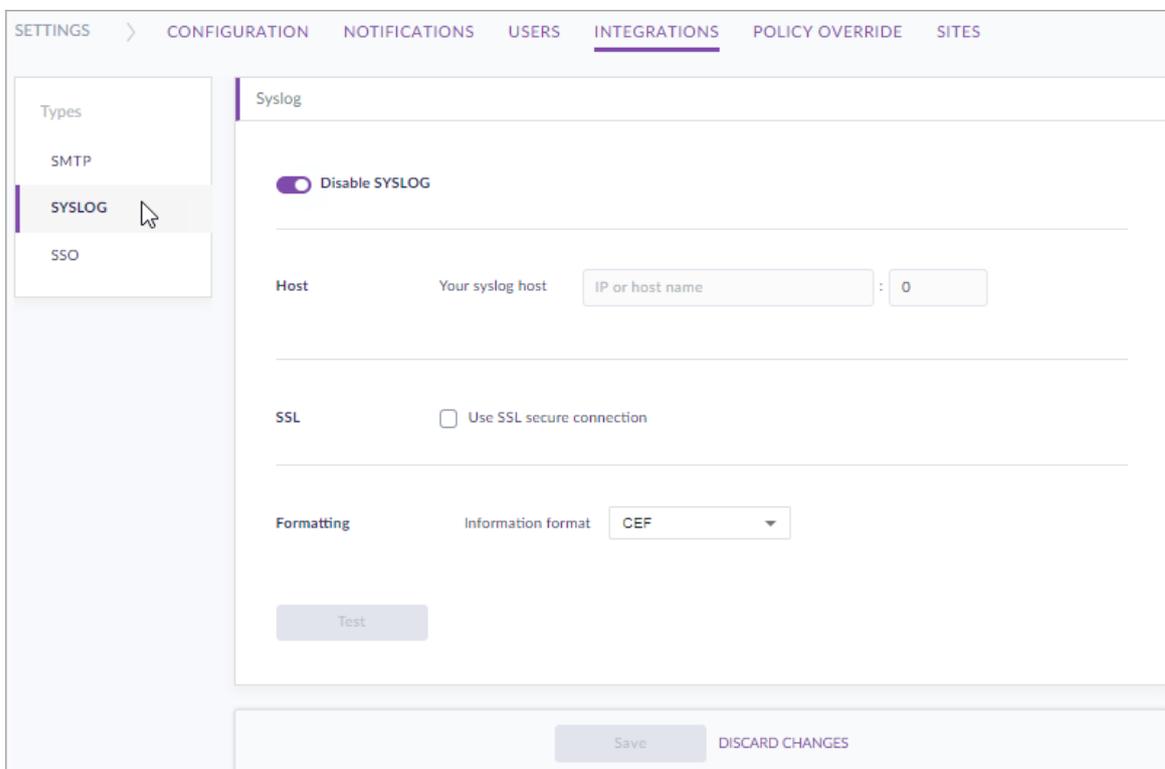
If you want to create a new user for QRadar integration, follow the steps in [Creating New Management Console Users](#) and then log in to the new user.

**Note:** A user with a role of **Site Admin** can mitigate threats from the QRadar Console. A user with a role of **Site Viewer** can view threats but cannot take action.

4. In the SentinelOne Management Console, click **Settings**.



5. If you are a Site or Account Admin, you must select one Site to open Settings.
- 6.
7. Click **SYSLOG**.



8. Click **Enable SYSLOG**.
9. In **Host**, enter the QRadar FQDN or IP address, and its listening port (514 or 6514).
10. To use SSL or TLS channel authentication and privacy, click **Use SSL secure connection**.

If you do not select this, UDP is used.

11. In **Certificate**, you can upload server and client certificates to verify client/server authorization between the SentinelOne Management (client) and the syslog server (server). These options only show if **Use SSL secure connection** is selected. Passphrase certificates are not supported. Make sure you know how the Syslog server is configured, and that you have the correct certificates from that configuration.

The screenshot shows a configuration window with two main sections: **SSL** and **Certificate**.

In the **SSL** section, there is a checkbox labeled "Use SSL secure connection" which is checked. A mouse cursor is pointing at the checkbox.

In the **Certificate** section, there is a heading "Certificates sent from/to the syslog server." followed by the instruction "Choose one out of three verification options: server only, client only or server & client verification". Below this, there are three rows of controls:

- Server certificate    Upload    ?
- Client certificate    Upload    ?
- Client key    Upload

- **Server certificate** - Select and upload a certificate to verify the syslog server identity.
- **Client certificate** - Select and upload a certificate to verify the SentinelOne Management as a client of the syslog server. Use a certificate file with a client key. A Client certificate is necessary if the server requires client authentication.
- **Client key** - Select and upload the client key of a client/server key pair. A Client key is necessary, along with a Client certificate, if the server requires client authentication.

To find the QRadar certificate and key files:

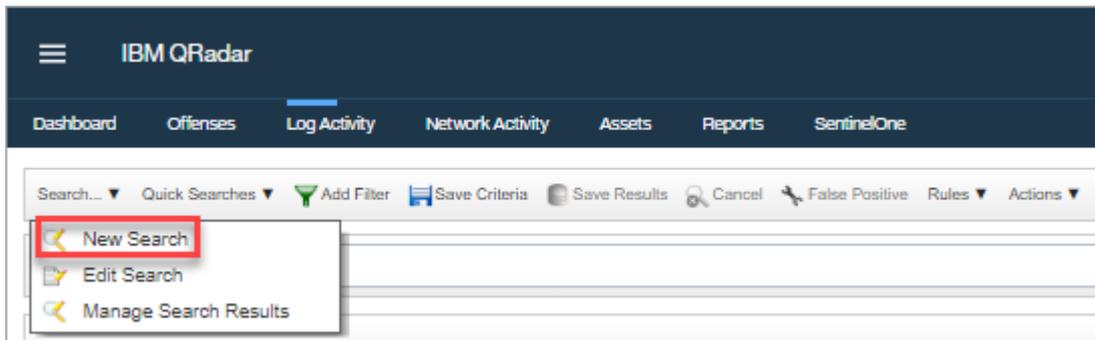
1. Using an SSH session, login to the QRadar Console as root user.
  2. Run: `cd /opt/qradar/conf/trusted_certificates/`
  3. Extract: `syslog-tls.cert` and `syslog-tls.key`.
12. In **Formatting**, select **CEF2**. This format is required to enable integration with the SentinelOne DSM.
  13. To verify connectivity with your QRadar server, click **TEST** to send a test trap.
  14. If the test passed, click **SAVE**.

### 3.4. Seeing SentinelOne Events in QRadar

After the SentinelOne DSM is installed, SentinelOne is added as a log source in QRadar, and your Syslog is integrated, you will see SentinelOne events in the QRadar Console.

#### To see all SentinelOne logged events:

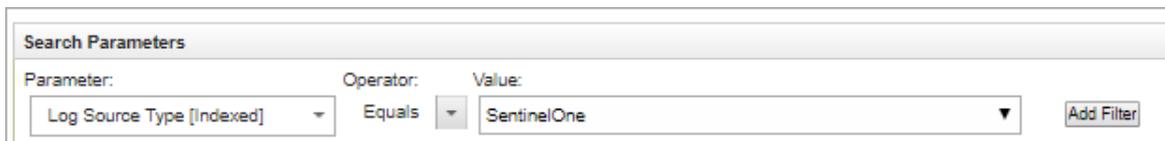
1. In the QRadar Console, click **Log Activity**.
2. Click **Search** and select **New Search**.



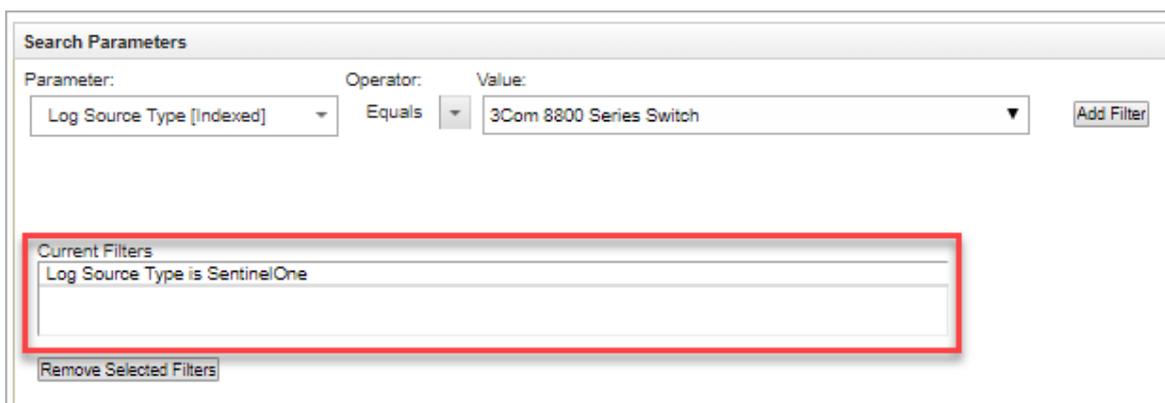
3. In **Search Parameters > Parameter**, select **Log Source Type [Indexed]**.

Make sure **Operator** is set to **Equals**.

Select **SentinelOne** as the **Value**.



4. Click **Add Filter**. The new filter is in the **Current Filters** list.



5. Click **Search**. The QRadar Log Activity shows all log activity sent from SentinelOne to QRadar.

The screenshot shows the IBM QRadar interface with the following elements:

- Navigation:** Dashboard, Offenses, Log Activity, Network Activity, Assets, Reports, SentinelOne.
- Search Bar:** Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions
- Advanced Search:** Start Time: 2/27/2019 3:01 PM End Time: 3/6/2019 3:01 PM. View: Select An Option: Display: Default (Normalized) Results Limit: 1,000.
- Current Filters:** Log Source Type is SentinelOne (Clear Filter)
- Records Matched Over Time:** A line chart showing event counts from Feb 28 to Mar 3. The y-axis ranges from 0 to 500. There are two prominent peaks: one around Feb 28 and another around Mar 2.
- Event Log Table:**

Event Name	Log Source	Event Count	Time	Low Level Category
THREAT_MITIGATION_REPORT_ROLLBACK_SUCCESS	s1	1	Mar 6, 2019, 2:54:56 PM	Notice
THREAT_MITIGATION_REPORT_ROLLBACK_SUCCESS	s1	1	Mar 6, 2019, 2:52:22 PM	Notice
Remediate performed successfully	s1	1	Mar 6, 2019, 2:52:22 PM	Remove Successful
Kill Action performed	s1	1	Mar 6, 2019, 2:52:11 PM	Misc System Event
THREAT_MITIGATION_REPORT_ROLLBACK_SUCCESS	s1	1	Mar 6, 2019, 2:50:11 PM	Notice
NEW_THREAT_NOT_MITIGATED	s1	1	Mar 6, 2019, 2:50:11 PM	Unknown Malware
Remediate performed successfully	s1	1	Mar 6, 2019, 2:47:22 PM	Remove Successful
Kill Action performed	s1	1	Mar 6, 2019, 2:47:11 PM	Misc System Event
THREAT_MITIGATION_REPORT_ROLLBACK_SUCCESS	s1	1	Mar 6, 2019, 2:47:11 PM	Notice
NEW_THREAT_NOT_MITIGATED	s1	1	Mar 6, 2019, 2:42:51 PM	Unknown Malware
THREAT_MITIGATION_REPORT_ROLLBACK_SUCCESS	s1	1	Mar 6, 2019, 2:42:31 PM	Notice
Remediate performed successfully	s1	1	Mar 6, 2019, 2:41:37 PM	Remove Successful
THREAT_MITIGATION_REPORT_ROLLBACK_SUCCESS	s1	1	Mar 6, 2019, 2:41:37 PM	Notice
Kill Action performed	s1	1	Mar 6, 2019, 2:41:26 PM	Misc System Event
NEW_THREAT_NOT_MITIGATED	s1	1	Mar 6, 2019, 2:39:41 PM	Unknown Malware
Threat Marked as resolved	s1	1	Mar 6, 2019, 2:37:11 PM	Remove Successful
THREAT_SUSPICIOUS_RESOLVED	s1	1	Mar 6, 2019, 2:37:11 PM	General Audit Event
THREAT_SUSPICIOUS_RESOLVED	s1	1	Mar 6, 2019, 2:37:11 PM	General Audit Event
- Footer:** Displaying 1 to 40 of 1000 items (Elapsed time: 0:00:00.068)

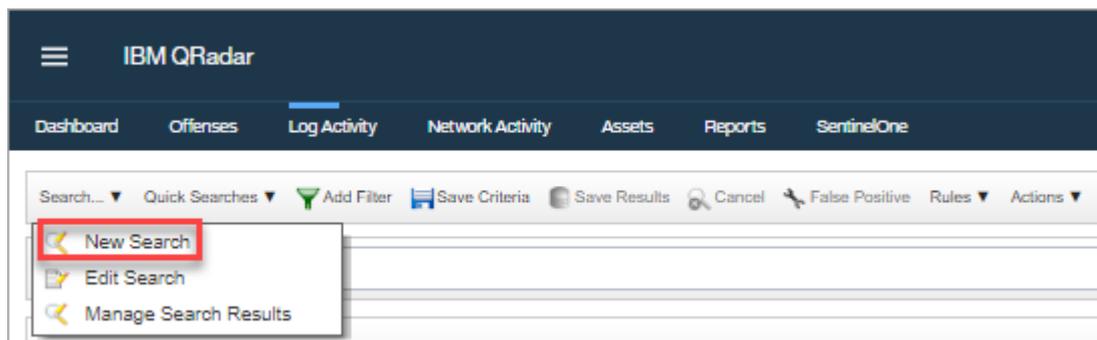
6. Double-click an event row for more details.

Event Information				
Event Name	NEW_THREAT_SUSPICIOUS			
Low Level Category	Suspicious Activity			
Event Description				
Magnitude	<div style="width: 100%; height: 10px; background-color: yellow;"></div>		(4) Relevance	1 Severity
Username	admin			
Start Time	Mar 5, 2019, 4:12:58 PM	Storage Time	Mar 5, 2019, 4:12:58 PM	Log Source Time
AccountDomain (custom)	WORKGROUP			
Action (custom)	active			
AgentId (custom)	b934add3fbc14245692821be0efe09a21273bea			
Category Description (custom)	New Suspicious threat detected - machine mo-win10-pc1			
File Hash (custom)	802498041b393ad1e92a27cfbcf0f882025234dc			
File Path (custom)	\\Device\\HarddiskVolume2\\Users\\admin\\Desktop\\NL_Test_Samples\\CryptoLocker_Symptomatic.exe			
Filename (custom)	CryptoLocker_Symptomatic.exe			
Hostname (custom)	mo-win10-pc1			
Service (custom)				
Threat Classification (custom)	Malware			
Threat Count (custom)	32			
Threat id (custom)	574486387315486036			
UNIX path name (custom)	N/A			
Domain	Default Domain			
Source and Destination Information				
Source IP		Destination IP		
Source Asset Name	N/A	Destination Asset Name		
Source Port	0	Destination Port		
Pre NAT Source IP		Pre NAT Destination IP		
Pre NAT Source Port	0	Pre NAT Destination Port		
Post NAT Source IP		Post NAT Destination IP		
Post NAT Source Port	0	Post NAT Destination Port		
Source IPv6	0:0:0:0:0:0:0	Destination IPv6		
Source MAC	00:00:00:00:00:00	Destination MAC		

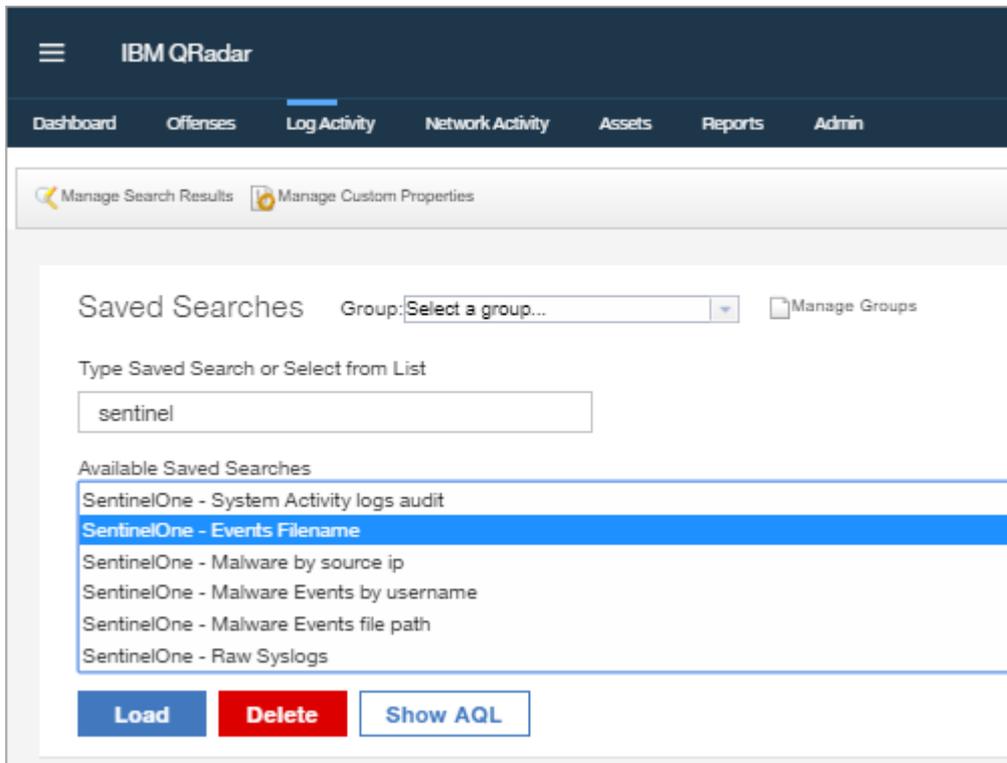
## To use predefined SentinelOne filters:

The SentinelOne DSM comes with SentinelOne predefined saved filters.

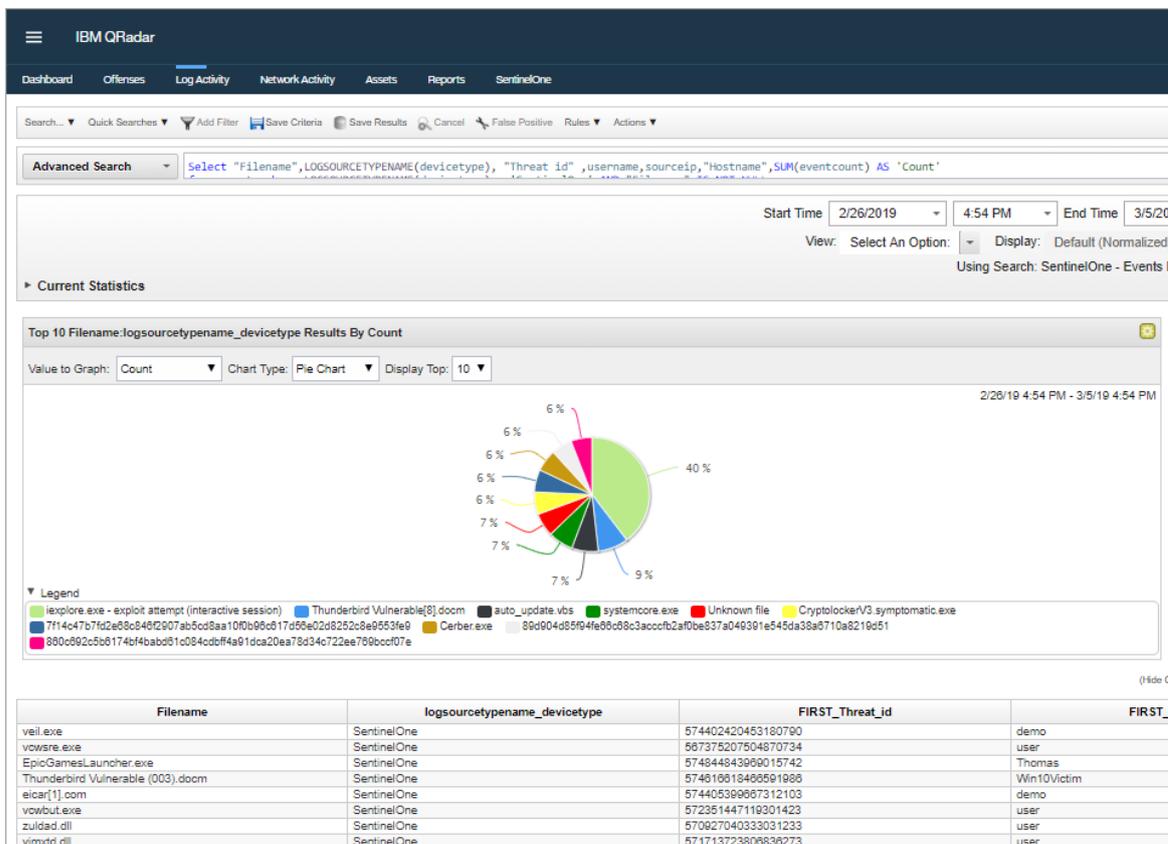
1. In the QRadar Console, click **Log Activity**.
2. Click **Search** and select **New Search**.



3. In **Type Saved Search or Select from List**, enter SentinelOne.



4. Select one of the predefined saved filters.
5. Click **Load**.



- Click an event for more details.

For example, if you selected the **Events Filename** filter, double-click a filename for more details.

The screenshot displays the SentinelOne search interface. At the top, there is a search bar with a query: `SELECT * FROM events WHERE (LOGSOURCETYPE ( devicetype ) = 'SentinelOne' AND Filename IS NOT NULL ) AND Filename &nbsp;= 'Thunderbird Vu'`. Below the search bar, there are filters for Start Time (2/26/2019, 4:54 PM) and End Time (3/5/2019, 4:54 PM). The interface shows a 'Current Statistics' section and a 'Records Matched Over Time' chart. The chart shows a single data point on March 5, 2019, at 2:00 PM, with a value of 2. Below the chart is a table of search results.

starttime	protocolid	sourceip	logsourceid	qid	sourceport	eventcount	magnitude	identityip	destinationip	destinationpor	category	username
1551795146391	255		73	1002250046	0	1	2	0.0.0.0		0	19001	Win10Victim
1551795179622	255		73	1002250032	0	1	4	0.0.0.0		0	7008	Win10Victim

- Double-click an event row for specific details about that event.

Return to Event List | Offense | Map Event | False Positive | Extract Property | Previous | Next | Print | Obfuscation

### Event Information

Event Name	THREAT_STATUS_CHANGED				
Low Level Category	General Audit Event				
Event Description					
Magnitude	(2)	Relevance	1	Severity	1
Credibility	5				
Username	Win10Victim				
Start Time	Mar 5, 2019, 4:12:28 PM	Storage Time	Mar 5, 2019, 4:12:28 PM	Log Source Time	Mar 5, 2019, 4:12:28 PM
AccountDomain (custom)	WORKGROUP				
Action (custom)	active				
Agentid (custom)	E9FF25835C14411BBA799DB4F7531CD400000000				
Category Description (custom)	Threat status changed				
File Hash (custom)	de18928ec32da081038932d80bd5b909b3149b23				
File Path (custom)	\\Device\\HarddiskVolume3\\Users\\Win10Victim\\AppData\\Local\\Microsoft\\Windows\\NetCache\\Content.Outlook\\J00064X3\\Thunderbird Vulnerable (003).docm				
Filename (custom)	Thunderbird Vulnerable (003).docm				
Hostname (custom)	DESKTOP-37TJ1RM				
Service (custom)					
Threat Classification (custom)	Malware				
Threat Count (custom)	1				
Threat id (custom)	574616613466591986				
UNIX path name (custom)	N/A				
Domain	Default Domain				

### Source and Destination Information

Source IP		Destination IP	
Source Asset Name	N/A	Destination Asset Name	N/A
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	0:0:0:0:0:0:0:0	Destination IPv6	0:0:0:0:0:0:0:0
Source MAC	00:00:00:00:00:00	Destination MAC	00:00:00:00:00:00

### Payload Information

utf  hex  base64  
 Wrap Text

## 4. The SentinelOne App for QRadar

To mitigate SentinelOne logged events in the QRadar Console:

1. Make sure the QRadar Console is installed and running.
2. [Add SentinelOne as a log source for QRadar \[9\]](#).
3. [Install the SentinelOne App in QRadar \[21\]](#).
4. [Generate an API Token \[27\]](#).
5. [Add your SentinelOne Management Console to the SentinelOne App \[28\]](#).
6. [View and mitigate SentinelOne events that appear in the App \[29\]](#).

### 4.1. Installing the SentinelOne App in QRadar

The SentinelOne App enables you to mitigate threats from the QRadar Console instead of performing them from the SentinelOne Management Console.

**Note:** The SentinelOne App is not supported on Internet Explorer.

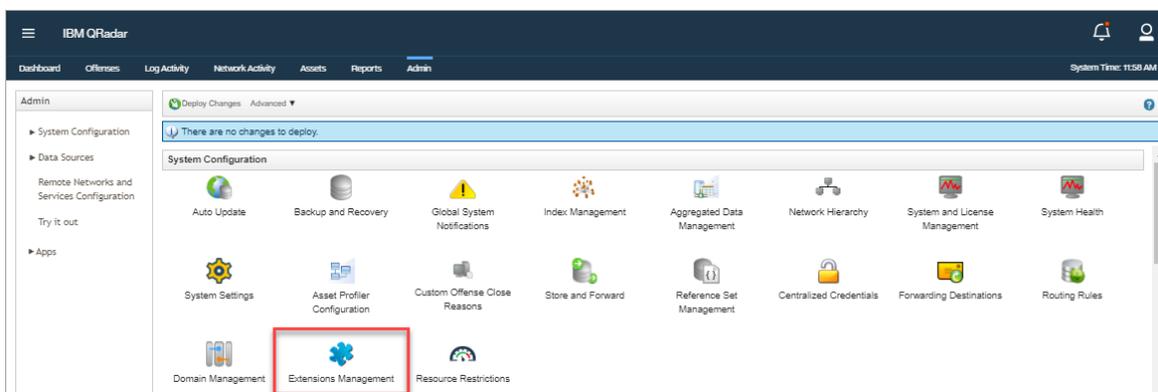
**Important:** If you have an earlier version of the SentinelOne App for QRadar, you must remove it before you install the new app. Go to [Upgrading From the Beta Version \[34\]](#) and follow the instructions.

#### To install the SentinelOne App:

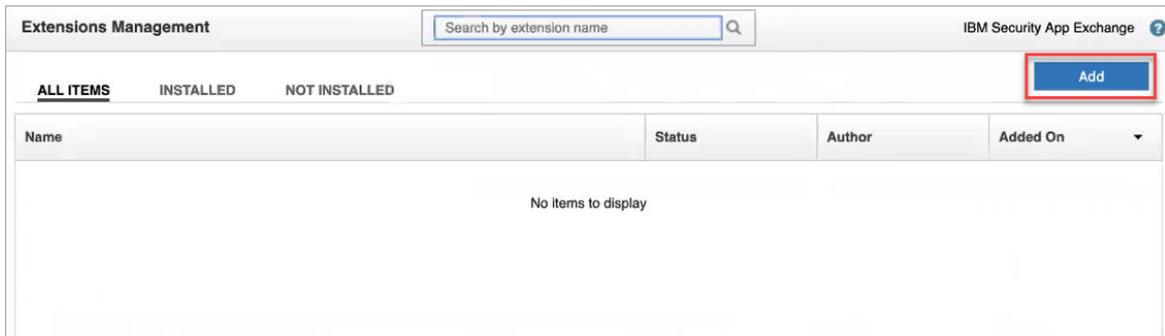
1. Download the SentinelOne App ZIP file available on [IBM App Exchange](#).
2. Log in to the QRadar Console as an Admin.
3. From the Main menu, click **Admin**.



4. Click **Extensions Management**.

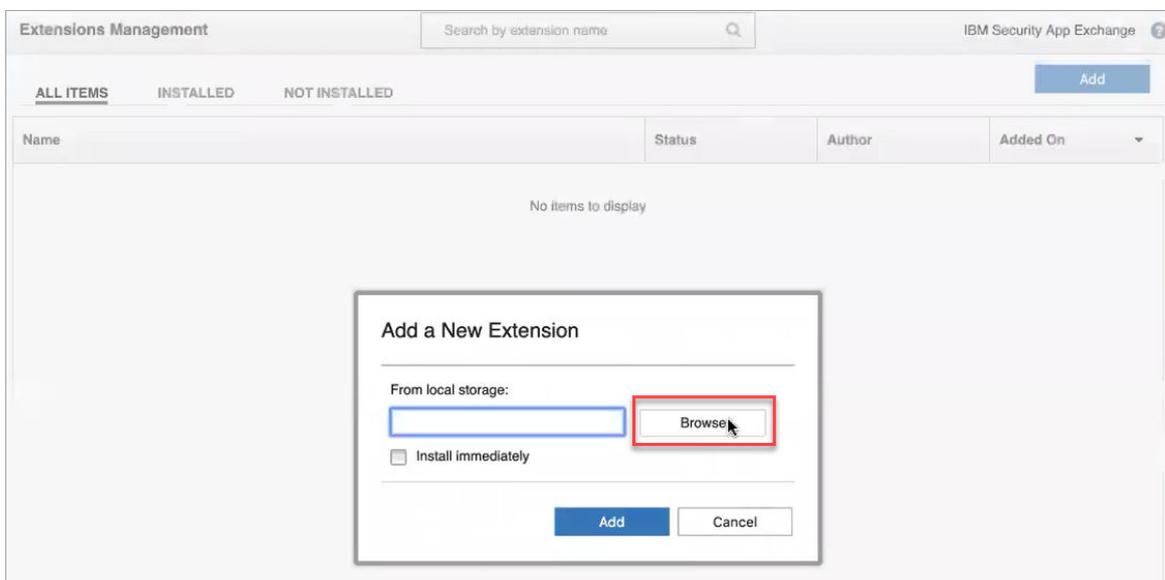


- In the window that opens, click **Add**.



- In the window that opens, click **Browse**. Browse to the location of the downloaded SentinelOne App file.

If you do not see this option, make sure you have the required Admin permissions.



- If you want to immediately install the app, skip to [Step 10](#).

If you want to add the SentinelOne App to the Extensions Management list but install it later, do not select **Install immediately**. Click **Add**.

Extensions Management Search by extension name  IBM Security App Exchange [?](#)

**ALL ITEMS**   INSTALLED   NOT INSTALLED [Add](#)

Name	Status	Author	Added On
QRadar Log Source Management	Installed	IBM QRadar	March 7, 2019
App Authorization Manager	Installed	IBM QRadar	March 7, 2019
QRadar Assistant App	Installed	IBM QRadar	March 7, 2019

**Add a New Extension**

From local storage:

[Browse](#)

Install immediately

[Add](#) [Cancel](#)

Extensions Management Search by extension name  IBM Security App Exchange [?](#)

**ALL ITEMS**   INSTALLED   NOT INSTALLED [Add](#)

Name	Status	Author	Added On
SentinelOne App for QRadar - v.3.5.0(Beta)	⚠ Not Installed	SentinelOne	March 10, 2019
QRadar Log Source Management	Installed	IBM QRadar	March 7, 2019
App Authorization Manager	Installed	IBM QRadar	March 7, 2019
QRadar Assistant App	Installed	IBM QRadar	March 7, 2019

## 8. Select SentinelOne App for QRadar.

Extensions Management Search by extension name  IBM Security App Exchange [?](#)

**ALL ITEMS**   INSTALLED   NOT INSTALLED [Add](#)

Name	Status	Author	Added On
SentinelOne App for QRadar - v.3.5.0(Beta)	⚠ Not Installed	SentinelOne	March 10, 2019
QRadar Log Source Management	Installed	IBM QRadar	March 7, 2019
App Authorization Manager	Installed	IBM QRadar	March 7, 2019
QRadar Assistant App	Installed	IBM QRadar	March 7, 2019

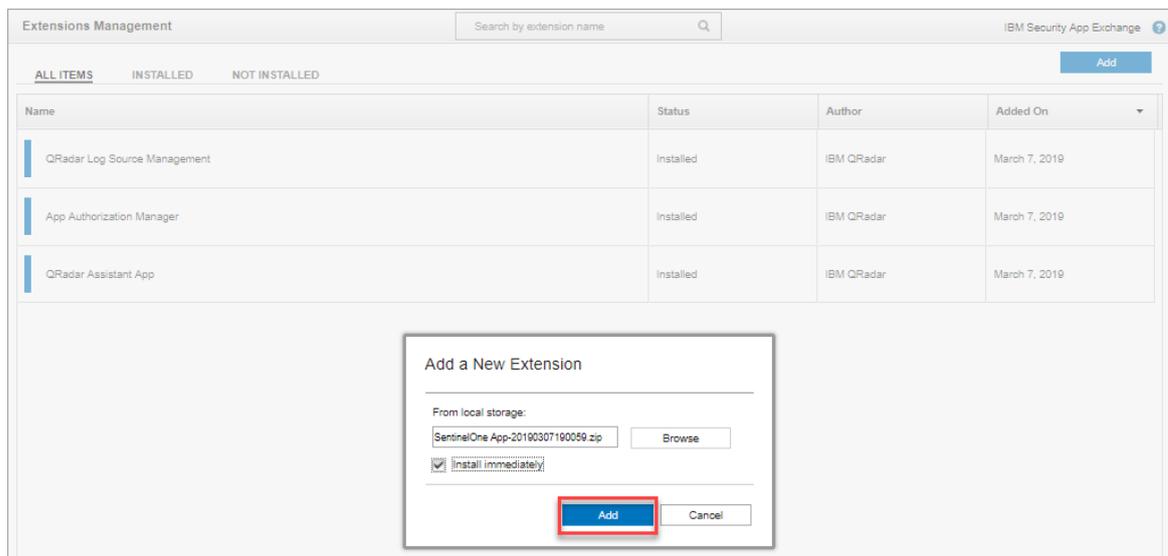
## 9. In the box that opens, click **Install**.

Extensions Management		Search by extension name	IBM Security App Exchange
ALL ITEMS	INSTALLED	NOT INSTALLED	Add
Name	Status	Author	Added On
<p><b>SentinelOne App for QRadar - v.3.5.0(Beta)</b></p> <p>SentinelOne is a next-generation endpoint security product used to protect against all threat vectors. Keep known and unknown malware and other bad programs out of endpoints. SentinelOne combines dynamic whitelisting and blacklisting with advanced static prevention in the form of deep file inspection to block threats before they have a chance to impact your endpoints. Detect and Contain Threats On Execution Lightweight agent monitors all activity and applies machine learning to dynamically detect the most advanced attacks, including exploits, fileless, and sophisticated malware. Upon detection of a new threat, SentinelOne stops its progress by disconnecting the infected device from the network. Immunize Endpoints Post-Execution Use policy-based mitigation to respond to incidents. After stopping attacks, quickly roll back modifications and auto-immunize your endpoints. A 360-degree view of endpoints and threats from inception to termination powers forensics and policy enforcement.</p> <p>Install Delete</p> <p>(More Details...)</p>	Not Installed	SentinelOne	March 10, 2019
QRadar Log Source Management	Installed	IBM QRadar	March 7, 2019
App Authorization Manager	Installed	IBM QRadar	March 7, 2019
QRadar Assistant App	Installed	IBM QRadar	March 7, 2019

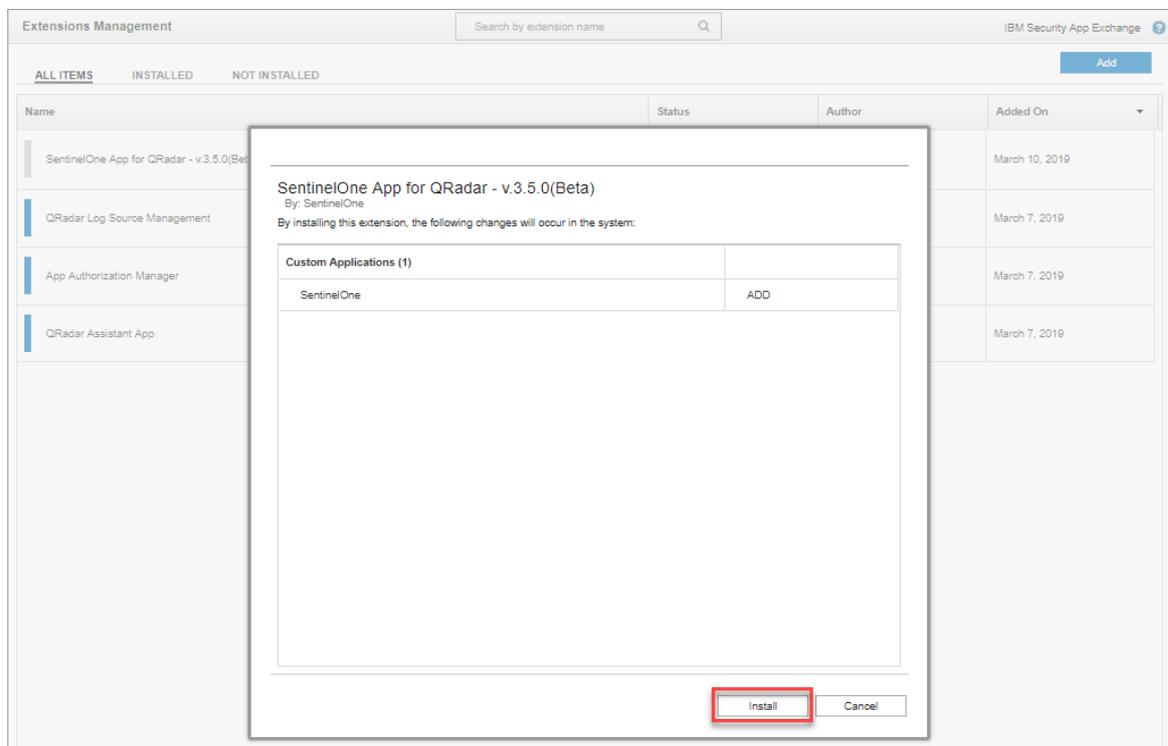
You can click **More Details** to see more information and the installation files.

Extensions Management		Search by extension name	IBM Security App Exchange
ALL ITEMS	INSTALLED	NOT INSTALLED	Add
Name	Status	Author	Added On
<p><b>SentinelOne App for QRadar - v.3.5.0(Beta)</b></p> <p>SentinelOne is a next-generation endpoint security product used to protect against all threat vectors. Keep known and unknown malware and other bad programs out of endpoints. SentinelOne combines dynamic whitelisting and blacklisting with advanced static prevention in the form of deep file inspection to block threats before they have a chance to impact your endpoints. Detect and Contain Threats On Execution Lightweight agent monitors all activity and applies machine learning to dynamically detect the most advanced attacks, including exploits, fileless, and sophisticated malware. Upon detection of a new threat, SentinelOne stops its progress by disconnecting the infected device from the network. Immunize Endpoints Post-Execution Use policy-based mitigation to respond to incidents. After stopping attacks, quickly roll back modifications and auto-immunize your endpoints. A 360-degree view of endpoints and threats from inception to termination powers forensics and policy enforcement.</p> <p>Install Delete</p> <p><b>Contents:</b></p> <ul style="list-style-type: none"> <li>Custom Applications (1)</li> <li>Custom Applications (1)</li> </ul> <p><b>Added By:</b> admin</p> <p><b>Added Date:</b> March 10, 2019</p> <p><b>Version:</b> v.3.5.0(Beta)</p> <p><b>Supported Languages:</b> en_US</p> <p><b>Signed:</b> Not signed</p> <p><b>Support:</b> Contact the extension's author (<a href="mailto:QRadar@SentinelOne.com">QRadar@SentinelOne.com</a>)</p> <p><b>Beta</b></p>	Not Installed	SentinelOne	March 10, 2019
QRadar Log Source Management	Installed	IBM QRadar	March 7, 2019
App Authorization Manager	Installed	IBM QRadar	March 7, 2019
QRadar Assistant App	Installed	IBM QRadar	March 7, 2019

10. To immediately install the app, select **Install immediately** and click **Add**.

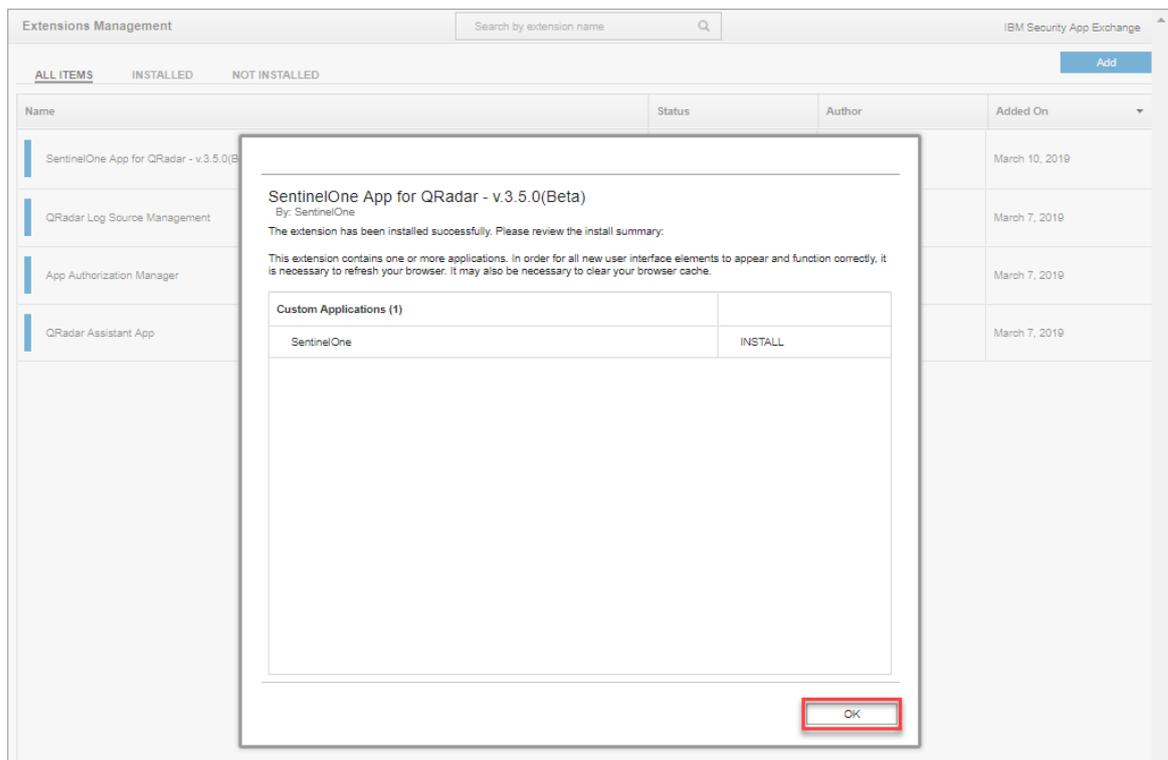


11. In the window that opens, click **Install**.

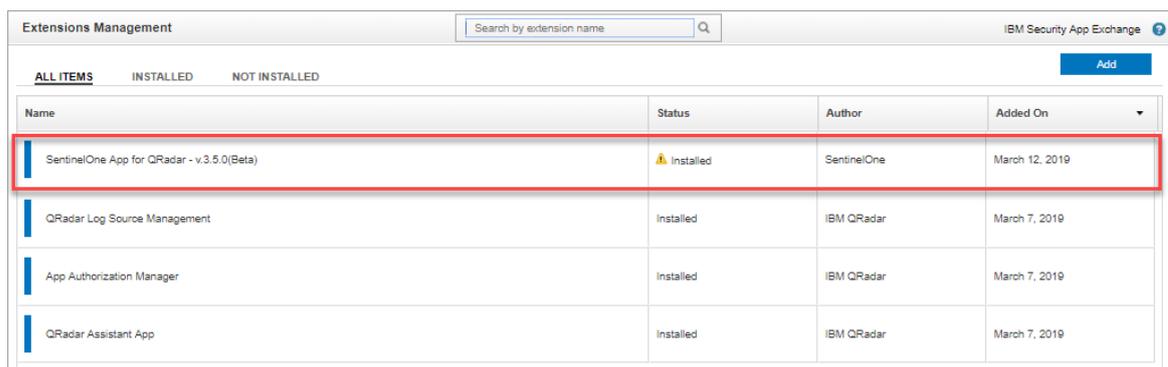


The installation might take a couple of minutes.

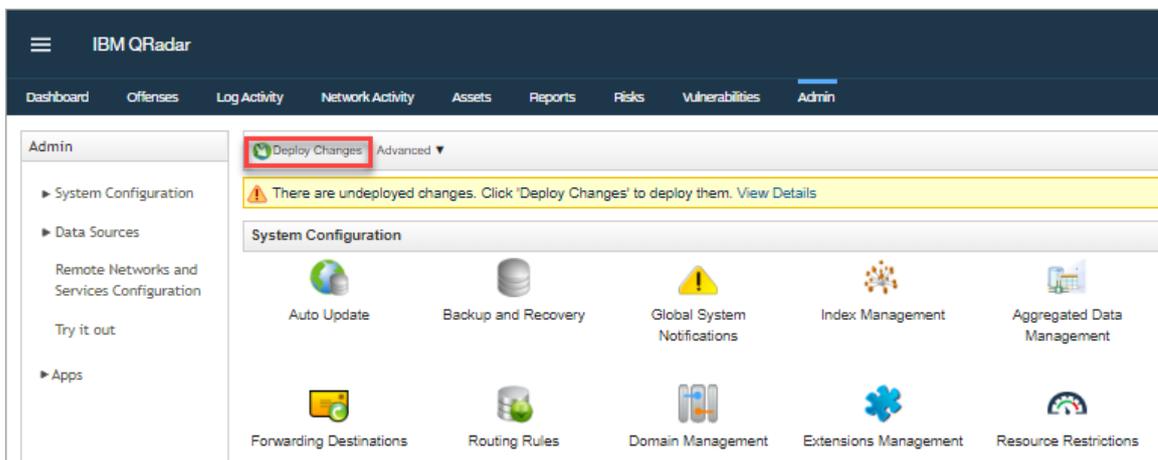
12. When you see the message that the extension installed successfully, click **OK**.



The SentinelOne App is installed and appears in the list of Extensions.



13. Exit the **Extensions Management** window.
14. Click **Deploy Changes** or refresh the QRadar Console screen.



You should see the SentinelOne tab in QRadar.



## 4.2. Generate an API Token

To use the SentinelOne App, you must generate an API token from the SentinelOne Management Console.

**Important:** If you have multiple SentinelOne Management Consoles, you must generate an API Token for each one.

The API token you generate is time limited. To regenerate a new token (and invalidate the old one), log in with the dedicated SentinelOne account. You do not need to create a new account.

### To generate an API Token:

1. In your Management Console, click **Settings > USERS**.

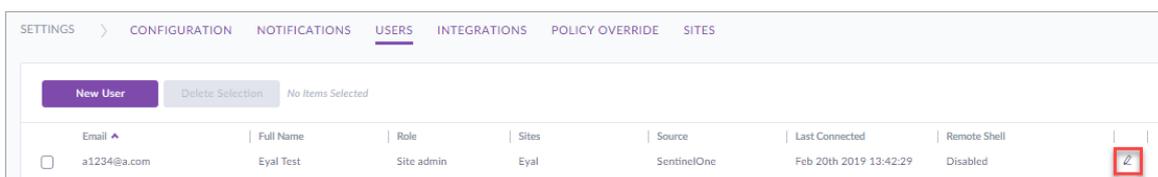


2. Find your user and click its edit button.

If you want to create a new user for QRadar integration, follow the steps in [Creating New Management Console Users](#) and then log in to the new user.

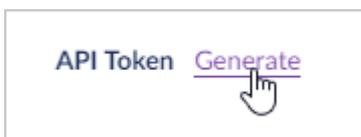
**Note:** A user with a role of **Site Admin** can mitigate threats from the QRadar Console. A user with a role of **Site Viewer** can view threats but cannot take action.

**Note:** You can generate a token only for your own user.



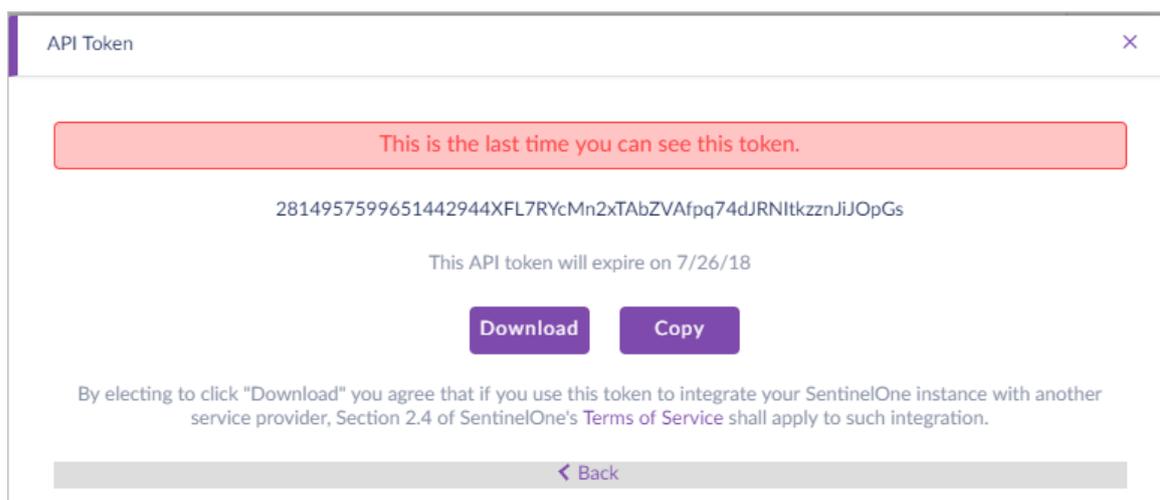
The **Edit User** window opens.

3. In the **API Token** section, click **Generate**.



If you see **Revoke** and **Regenerate**, you already have a token. If you revoke or regenerate it, scripts that use that token will not work. There is no confirmation. **Revoke** removes the token authorization. **Regenerate** revokes the token and generates a new token.

If you click **Generate** or **Regenerate**, a message shows: This is the last time you can see this token. It shows the token string and the date that the token expires.



4. Copy the token or click **Download** to save it.

### 4.3. Adding SentinelOne Management Consoles to the SentinelOne App

To use the SentinelOne App, you must add each SentinelOne Management Console as input for the SentinelOne App.

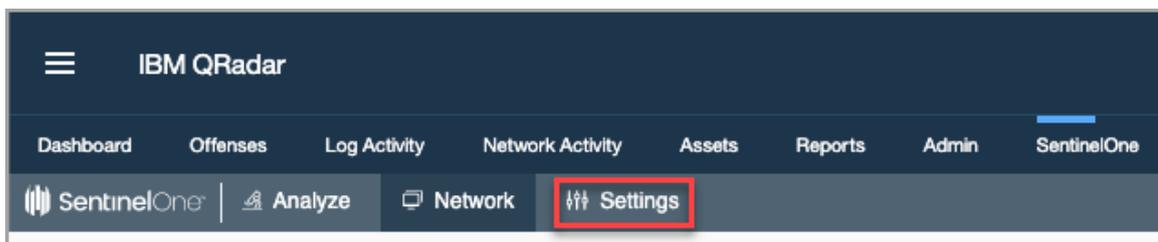
#### To add a SentinelOne Management Console in the SentinelOne App:

**Note:** If you have more than one SentinelOne Management Console, repeat this procedure for each one.

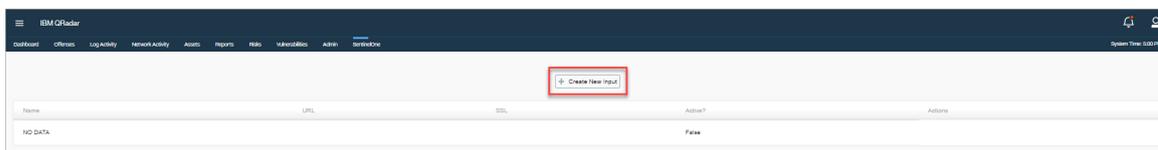
1. Click the **SentinelOne** tab of the QRadar Console.



If you are adding a second SentinelOne Management Console, click the SentinelOne tab of the QRadar Console, and click **Settings**.



2. Click **Create New Input**.



3. In the window that opens, enter:
  - **Name** - The name of the SentinelOne Management Console as it will show in the QRadar Console.
  - **URL** - The URL of the SentinelOne Management Console. For example: `https://xyz.sentinelone.net`.
  - **API Token** - The SentinelOne API token generated in the SentinelOne Console.
  - **SSL Verification** - The default is selected. We strongly recommend you keep this selected to use server certificate verification.
4. Click **Add**.

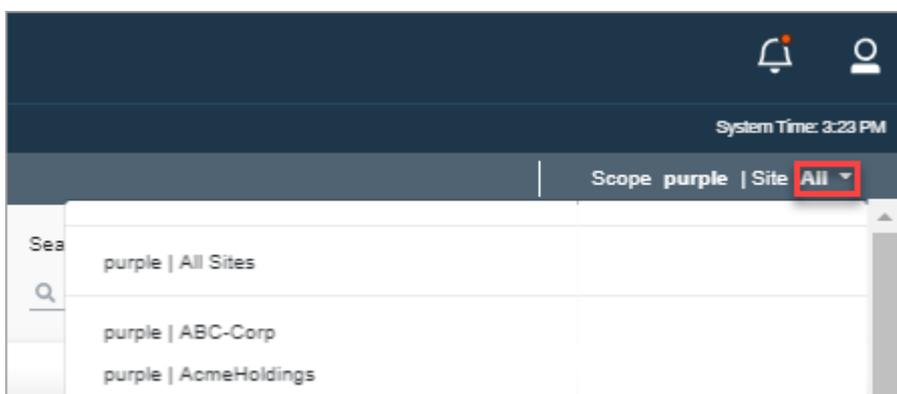
## 4.4. Using the SentinelOne App

The SentinelOne App shows threats collected from your different SentinelOne Sites. The data is from real-time API requests.

### To see and filter threats:

By default, all threats from all sites are shown.

1. Click **SentinelOne > Analyze**.
2. To view threats from a specific site, select the site from the **Site** menu.



- To find specific threats, use the **Filter** and **Search** options, and click **Apply**.

Status	File Name	Endpoint	Created	Updated	Site	Classification	Action Done
✓	Unknown_Sp	www.ibm.com	07/05/2019 10:23	07/05/2019 10:30	vee	Heuristic	quarantine, kill, remediate
✓	Asasb8mouh.doc	www.ibm.com	07/05/2019 10:05	07/05/2019 10:12	vee	PUA	quarantine, kill, remediate
⚠	vowrdm.exe	www.ibm.com	07/05/2019 09:22	07/05/2019 09:33	Andre	Malware	
✓	Basomwara.exe	www.ibm.com	07/05/2019 09:22	07/05/2019 09:33	Andre	Malware	rollback, quarantine, kill, remediate
⚠	Basomwara.exe	www.ibm.com	07/05/2019 09:20	07/05/2019 09:33	Andre	Malware	
⚠	SoloGestel_launcher.exe	www.ibm.com	07/05/2019 08:32	07/05/2019 08:32	Demo IBMxOS	generic/heuristic	
⚠	38.003.0218.0011	www.ibm.com	07/05/2019 00:39	07/05/2019 00:39	memot	Malware	
⚠	word8	www.ibm.com	07/05/2019 00:39	07/05/2019 00:39	memot	Malware	
⚠	ExpGestel_launcher.exe	www.ibm.com	07/05/2019 00:15	07/05/2019 00:15	JPM_Home	Malware	
✓	Thunderbolt_Vulnerabilty.docx	www.ibm.com	05/05/2019 21:29	05/05/2019 21:55	Scott	Malware	rollback, quarantine, kill, remediate

- Click a threat name to view more details about that threat.

## To mitigate a threat:

- Click **SentinelOne > Analyze**.
- Click an item link (for example, a file name) to see its details.
- Optional: Click **Google** or **Virus Total** to see if the hash is known.
- Click **Actions**.

**File Info**

File Name: vowrdm.exe  
Path: I:\Device\HarddiskVolume1\Users\Andre\...

**Device**

Device: WIN7-AMN-DEMO  
IP: 192.168.1.100

Domain: WORKGROUP  
Username: WIN7-AMN-DEMO\Andre Noordam  
Agent version: 3.1.3.38  
Site: Andre  
Group: Default Group

**Time**

Created: 07/05/2019 09:22  
Updated: 07/05/2019 09:33

**Summary**

Status: active

SHA1: 953e01142e4e078048e5e9e69d029f...

Search hash on:

Threat ID: 630891342347922777  
Detections engine: sfs\_detection  
Classification: Malware  
Signer Identity: N/A  
Group: Default Group  
Management: Andre

**Indicators**

**Abnormalities**  
This binary uses non-standard DOS stubs

**Hiding/Stealthiness**  
This binary may contain encrypted/compressed info as measured by high sections (+6.8)

**General**  
This binary creates a System Service

**Actions**

- Mark as Benign
- Mark as Threat
- Kill
- Quarantine
- Un-quarantine
- Remediate
- Rollback Remediation
- Resolve

- Select a mitigation option.

## Mitigation Options:

- Mark as benign** - For false positives. Adds the item to the whitelist, marks the threat as resolved, and removes it from the **Dashboard** view.
- Mark as threat** - Defines the item as a threat in the Dashboard.
- Kill** - Stops processes. Active content in documents, executables, and sub-processes are stopped. The Agent enables Kill for processes that act against normal endpoint behavior or do not fit the actions of the application the process is hiding in.

- **Quarantine** - Stops processes, encrypts the executable, and moves it to a confined path.

If a threat is known, the Agent automatically kills the threat before it can execute. The only mitigation action for you is **Quarantine**.

- **Un-quarantine** - Removes a file from quarantine.
- **Remediate** - (Windows and macOS) Stops processes, quarantines binaries, removes linked libraries, deletes seed files, and restores configuration of the OS, application, and user settings to the state before the attack began.
- **Rollback** - (Windows only) Restores the endpoint to a saved point.

This option is best for ransomware mitigation and disaster recovery. It can remove legitimate work done since the last VSS snapshot.

- **Resolve** - Removes the threat from the Dashboard.

### To see and filter endpoints:

1. Click **SentinelOne > Network**.
2. Use the **Filter** and **Search** options to find specific endpoints, for example, of a specific OS.



Endpoint Name	Site	Group	Domain	Console Visible IP	Agent Version	Last Logged User	Last Active
JOHNATY-WIN-03	Mobesoft	ocean-oact	WORKGROUP	192.168.1.100	2.8.2.5745	user	05/05/2019 22:08
ACORN03000002	manick	Win-Server	WORKGROUP	192.168.1.101	3.0.2.35	PlanPass	01/05/2019 12:40

3. Click **Apply**.
4. Click an endpoint name to view the endpoint details, and threats associated with the endpoint.

### To run an action on an endpoint:

1. Click **SentinelOne > Network**.
2. Use the **Filter** and **Search** options (and click **Apply**) to find specific endpoints on which you will run the action.
3. From the SentinelOne API **Network** tab, click an endpoint. You see the details of that endpoint and its network status.
4. Click **Actions**.

The screenshot shows the SentinelOne console interface for endpoint 'nirg-macos-vm1'. The 'Actions' menu is highlighted in the top right corner. The page displays general system information, network adapters, and a list of threats.

Status	File Name	Endpoint	Created	Updated	Site	Classification	Action Done
Malware	invokes.docx	desktop nirg-macos-vm1	20/05/2019 07:21	20/05/2019 07:25	ABC-Corp	Malware	
Benign	sudo	desktop nirg-macos-vm1	12/05/2019 15:51	12/05/2019 15:52	ABC-Corp	Benign	
Benign	python	desktop nirg-macos-vm1	12/05/2019 12:50	12/05/2019 13:02	ABC-Corp	Benign	
Malware	invokes.docx	desktop nirg-macos-vm1	12/05/2019 12:50	12/05/2019 13:02	ABC-Corp	Malware	
OSX.Malware	malware	desktop nirg-macos-vm1	12/05/2019 12:50	12/05/2019 13:02	ABC-Corp	OSX.Malware	
generic.heuristic	vmware-tools-daemon	desktop nirg-macos-vm1	23/04/2019 12:03	12/05/2019 13:03	ABC-Corp	generic.heuristic	
generic.heuristic	vmware-tools-daemon	desktop nirg-macos-vm1	23/04/2019 12:03	23/04/2019 12:03	ABC-Corp	generic.heuristic	

## 5. Select an action.

### Actions:

- **Full Scan** - Scans the SentinelOne Agent installed on this endpoint. Finds dormant suspicious activity, threats, and compliance violations, that are then mitigated according to the policy.
- **Abort Scan** - Stops scanning the SentinelOne Agent installed on this endpoint.
- **Fetch Logs** - Generates logs of SentinelOne Agent activity on this endpoint.
- **Disconnect** - Disconnects the endpoint from the network. The endpoint can communicate only with the SentinelOne Management Console but not with other components on the network.

## To manage SentinelOne Consoles integrated with QRadar:

1. Click **SentinelOne > Settings** to see a list of SentinelOne Management Consoles integrated with QRadar.
2. If you have more than one SentinelOne Management Console, to integrate a new one with QRadar, click **Create New Input**.
3. To remove the integration of a SentinelOne Management Console, click **delete**.

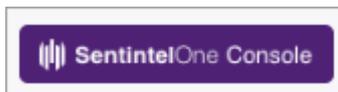
The screenshot shows the IBM QRadar console interface for SentinelOne integration. The 'Create New Input' button is highlighted in the top right corner, and the 'delete' button is highlighted in the bottom right corner of the table.

Name	URL	SSL	Active?	Actions
purple	https://nirg-macos-vm1:443	True	True	delete

## To view threats in the SentinelOne Management Console:

Open the SentinelOne Management Console for more features. For example: Perform more actions on endpoints, view threat attack story lines, and run administrative actions. For a video tour of the Management Console, click [here](#).

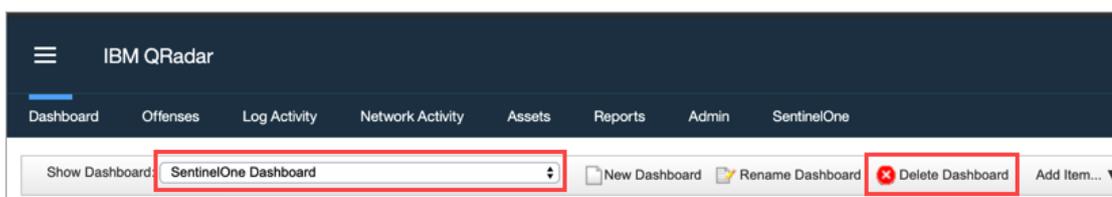
1. Click **SentinelOne> Analyze**.
2. Click an item you want to view from the SentinelOne Management Console.
3. Click the **SentinelOne Console** button.



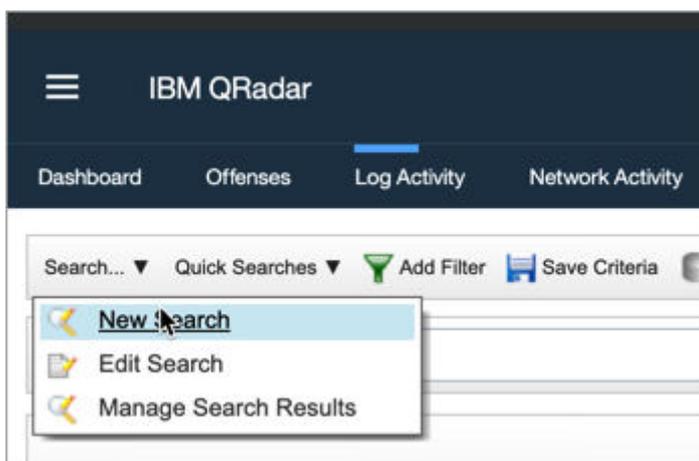
## 5. Upgrading From the Beta Version

**Important:** If you are upgrading from the Beta version, you must first follow this procedure BEFORE installing the latest SentinelOne DSM and App.

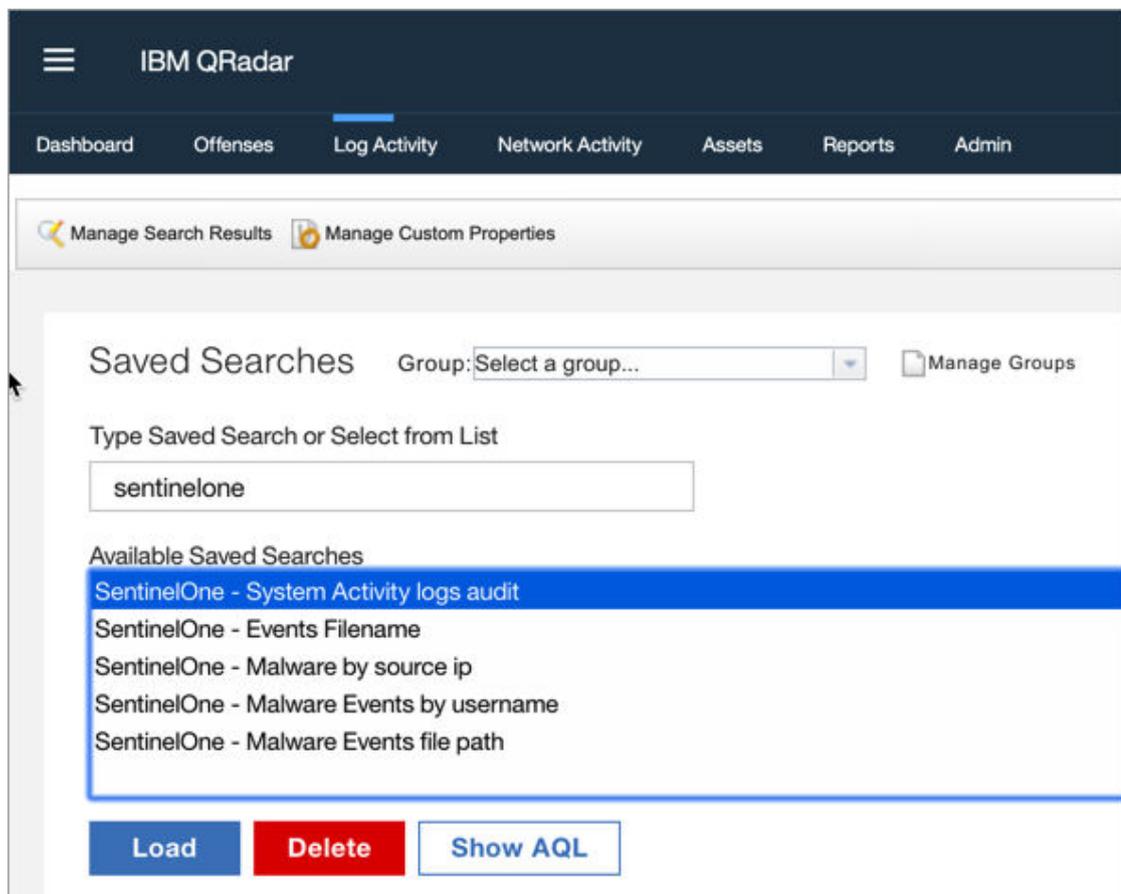
1. Uninstall the existing SentinelOne DSM.
  1. Select **Admin** from the Main menu, and click **Extensions Management**.
  2. Select the SentinelOne DSM from the list, and click **Uninstall**.
2. Uninstall the existing SentinelOne App.
  1. Select **Admin** from the Main menu, and click **Extensions Management**.
  2. Select the SentinelOne App from the list, and click **Uninstall**.
3. Delete the existing SentinelOne Dashboard.
  1. Click **Dashboard** and select **SentinelOne Dashboard**.
  2. Click **Delete Dashboard**.



4. Delete all SentinelOne saved searches.
  1. Click **Log Activity > Search > New Search**.



2. Filter the list of **Available Saved Searches** for **SentinelOne**.
3. Delete all SentinelOne saved searches.



5. Install the SentinelOne DSM for QRadar. Go to [Installing the SentinelOne DSM in QRadar \[6\]](#) and follow the instructions.
6. Install the SentinelOne App for QRadar. Go to [Installing the SentinelOne App in QRadar \[21\]](#) and follow the instructions.

## 6. Advanced Configuration

### 6.1. Configuring the Syslog Format

The Syslog output generated by SentinelOne must be properly parsed to create meaningful and valid log entries in QRadar. The DSM integration maps SentinelOne IDs to QRadar fields. The IDs are from SentinelOne API, version 2.0.



#### NOTE

The Syslog format uses a pipe ( | ) as a delimiter. In this article, it is not a code symbol for "or". Enter the pipe as a shown.

Syntax:

```
CEF:2|SentinelOne|Mgmt|OS|eventID|eventName|eventSeverity|Details
```

#### Valid Values

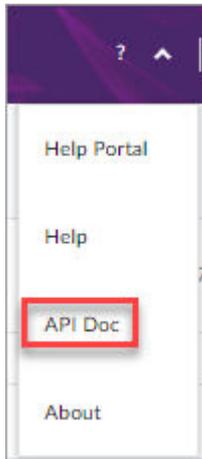
Field	Description	Valid Values	Mapped QRadar Field
Format type and version	Use CEF, version 2, for integration with SentinelOne.	CEF:2	<b>Event Category</b>
SentinelOne	The Company field is hard-coded to SentinelOne.	SentinelOne	<b>SentinelOne</b>
Mgmt	SentinelOne component and version.	Mgmt	<b>Slenvironment</b>
OS	Short name of the operating system of the endpoint.	Windows Linux OS X	<b>SlosName</b>
eventID	Unique ID Of the event. This is matched to the QRadar Event IDs.	<i>integer</i>	<b>Event ID</b>
eventName	Readable text to complement the ID and to headline the event in text.	<i>string</i>	<b>EventDesc</b>
eventSeverity	Threat level, according to SentinelOne intelligence, mapped to the RFC 3164 severity values.	<i>string</i>	
Details	Available on certain alerts, in standard and custom QRadar variables, for correlation when possible.	See next table	

## 6.2. Finding SentinelOne Events

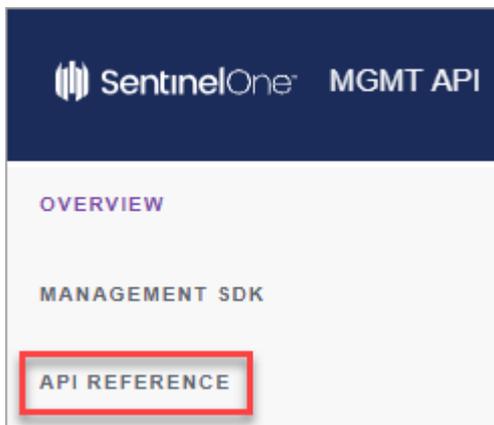
To add SentinelOne events to the QRadar logs, you need a list of the SentinelOne event names and ID numbers.

### To see a complete list of SentinelOne events:

1. Open the SentinelOne Management Console.
2. Click the **Help menu > API Doc.**



3. Click **API REFERENCE.**



4. Click **Activities > Get activities types.**

OVERVIEW

MANAGEMENT SDK

API REFERENCE

Accounts

Activities

**Get activities types**

Get activities

Agent Actions

## Get activities types

**GET** /web/api/v2.0/activities/types

Get a list of activities types.

— Test this endpoint

**RUN ON CONSOLE**

5. Click RUN ON CONSOLE.

The list of activities opens. For example, ID **48** is the event **Agent Recommissioned**.

```

    "id": 46
  },
  {
    "action": "Agent Decommissioned",
    "descriptionTemplate": "Agent {{ computer_name }} automatically d
ecommissioned.",
    "id": 47
  },
  {
    "action": "Agent Recommissioned",
    "descriptionTemplate": "Agent {{ computer_name }} automatically r
ecommissioned.",
    "id": 48
  },
  {
    "action": "Agent Request Uninstall",
    "descriptionTemplate": "Machine named: {{ computer_name }} reques
ted to uninstall SentinelOne agent.",
    "id": 49
  },
  },
}

```

## 6.3. Regular Expressions for Mapping

### Regular Expressions for QRadar Mapping

Field	Regular Expression
Event Category	(CEF):2
S1environment	CEF:2\SentinelOne\\(w+)\.+\.\.+\.\.+\.

Field	Regular Expression
S1osName	CEF:2\SentinelOne\.\+(\.+)\.\.\.\.
Event ID	CEF:2\SentinelOne\.\.\+(\w+)\.\.\.
EventDesc	CEF:2\SentinelOne\.\.\.\+(\.+)\.\.
Log Source Time	\srt\=#arcsightDate\((\S+)\s(\d+)\s(\d+)\s(\d{1,2}):(\d{1,2}):(\d{1,2}))
Source IP	\ssrc=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})
Source Port	\sspt=(\d{1,5})
Source MAC	\ssmac=((?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2})
Destination IP	\sdst=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})
Destination Port	\sdpt=(\d{1,5})
Destination MAC	\sdmac=((?:[0-9a-fA-F]{2}\:){5}[0-9a-fA-F]{2})
Username	\sduid=(\d{1,10})
S1sourceHost	\sshost=(\S+)
S1deviceHost	\sdvchost=(\S+)
S1deviceIP	\sdvc=(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})
Protocol	\sproto=(TCP UDP ICMP GRE)
S1destService	\sdestinationServiceName=(\S+)
S1eventCat	\scat=(\S+)

## 7. Troubleshooting

### Basic SentinelOne App troubleshooting before I open a Support ticket

Here are some solutions to troubleshoot this issue. Do them in the order listed until the problem is solved.

1. See if the **Deploy Changes** button appears in the QRadar dashboard. If it does, click it.
2. Earlier versions of the SentinelOne app should be removed before you install a newer version. Check whether there are two versions of the SentinelOne app installed. (In the QRadar Console, click the **Admin** menu and click **Extensions Management** to see a list of installed extensions.) If there is more than one SentinelOne app installed, uninstall both of them and reinstall one.
3. Uninstall and reinstall the app.

### Why do I not see any SentinelOne events?

Here are some solutions to troubleshoot this issue. Do them in the order listed until the problem is solved.

1. See if the **Deploy Changes** button appears in the QRadar dashboard. If it does, click it.
2. Check the Log Source configuration settings. In the QRadar Console, click the **Admin** menu and click Log Sources. Make sure **Log Source Extension** is set to the SentinelOne extension.
3. Check the Syslog settings. In the SentinelOne Management Console, click **Settings > Integrations > Syslog**. Make sure that **Formatting** is set to **CEP2**.
4. Contact SentinelOne Support.

### Why do I see an Unknown event?

An Unknown event is collected and parsed, but is not mapped or categorized to a specific log source.

If you see a SentinelOne log event marked as **Unknown**, you can manually add it to the QRadar system using the correct SentinelOne activity type and ID. For a list of SentinelOne activity types, see [Finding SentinelOne Events \[37\]](#).

### What information should I submit to SentinelOne Support when opening a ticket?

1. URL of your SentinelOne Management Console.
2. QRadar version and build number. This information is available from the QRadar Console. From the Dashboard tab, select **Help > About**.
3. The SentinelOne DSM version, and SentinelOne App version, installed on the QRadar Console.
  - a. Log in to the QRadar Console as Admin.
  - b. From the Admin tab, in the System Configuration group, click **Extensions Management**.
  - c. Search for the SentinelOne extensions, and write their version numbers.

4. A detailed description of what occurred, and how to reproduce it.
5. What you expected compared to what you saw.
6. A screen capture showing the issue or on-screen error message.
7. A screen capture of the log source configuration.
  - a. Log in to the QRadar Console as Admin.
  - b. From the Admin tab, in the Events group, click **Log Sources**.
  - c. Double-click the log source to open the edit screen and take a screen capture.
8. A screen capture of the incorrect event. Double-click an event in the **Log Activity** tab to view the Event Summary, and submit a screen capture.
9. Steps taken by the user or administrator to try and resolve the issue.
10. The QRadar support package tar.gz file.
  - a. Using SSH, log in to the QRadar Console as the root user.
  - b. Run: `sudo /opt/qradar/support/get_logs.sh -a`
  - c. Attach the generated `/store/LOGS/XXXX.tar.gz` file to the support ticket.  
For example: `logs_qrd-dev-test3_20190505_3620c115.tar.gz`
11. An export of the log files.
  - a. Log in to the QRadar Console as Admin.
  - b. From the **Admin** tab, click **System and License Management**.
  - c. Select the QRadar appliances that you want to collect logs from in the user interface. If you do not select any appliance, the default action is to collect logs from the QRadar Console.
  - d. Select **Actions > Collect Log Files**.
  - e. Click **Collect Log Files**. The log collection process starts and the status bar will update when log collection is complete.
  - f. Click **Download** and save the file.
  - g. Attach the log to your support ticket.
12. A Full XML export from the **Log Activity** tab on the QRadar Console. Explain the events that appear to be parsing incorrectly in the description of your service request.
  - a. From the QRadar Console, click the **Log Activity** tab.
  - b. Click the **View** drop-down and select a time interval.
  - c. Review the filtered events to ensure that it contains your issue or concern.
  - d. From the navigation menu, select **Actions > Export to XML > Full Export (All Columns)**.
  - e. Attach the XML event export.

**Checklist before sending email to SentinelOne Support:**

The email to SentinelOne Support includes:

- [ ] URL of the SentinelOne Management Console
- [ ] QRadar version and build number
- [ ] SentinelOne DSM version number
- [ ] SentinelOne App version number
- [ ] A detailed description of what occurred, and how to reproduce it
- [ ] What you expected compared to what you saw
- [ ] A screen capture showing the issue or on-screen error message
- [ ] A screen capture of the log source configuration.
- [ ] A screen capture of the incorrect event
- [ ] Steps taken to try and resolve the issue
- [ ] Attachment of the QRadar support package tar.gz file
- [ ] Attachment of the exported log files
- [ ] Attachment of the XML exported Log Activity tab

**How do I contact SentinelOne Support?**

Phone: +1-855-868-3733 select Option 2

Web: [support.sentinelone.com](https://support.sentinelone.com)

Email: [Support@sentinelone.com](mailto:Support@sentinelone.com)