SentinelOne for QRadar v3.5.x

Integration Guide

3 October 2019

Table of Contents

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.

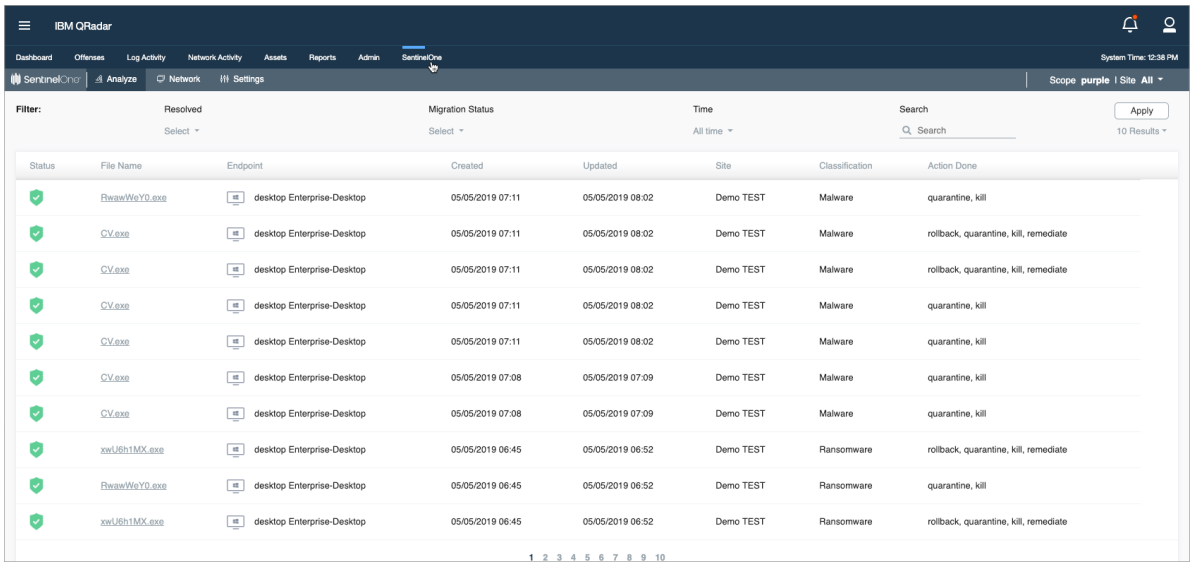
These are the components of this integration:

- **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.

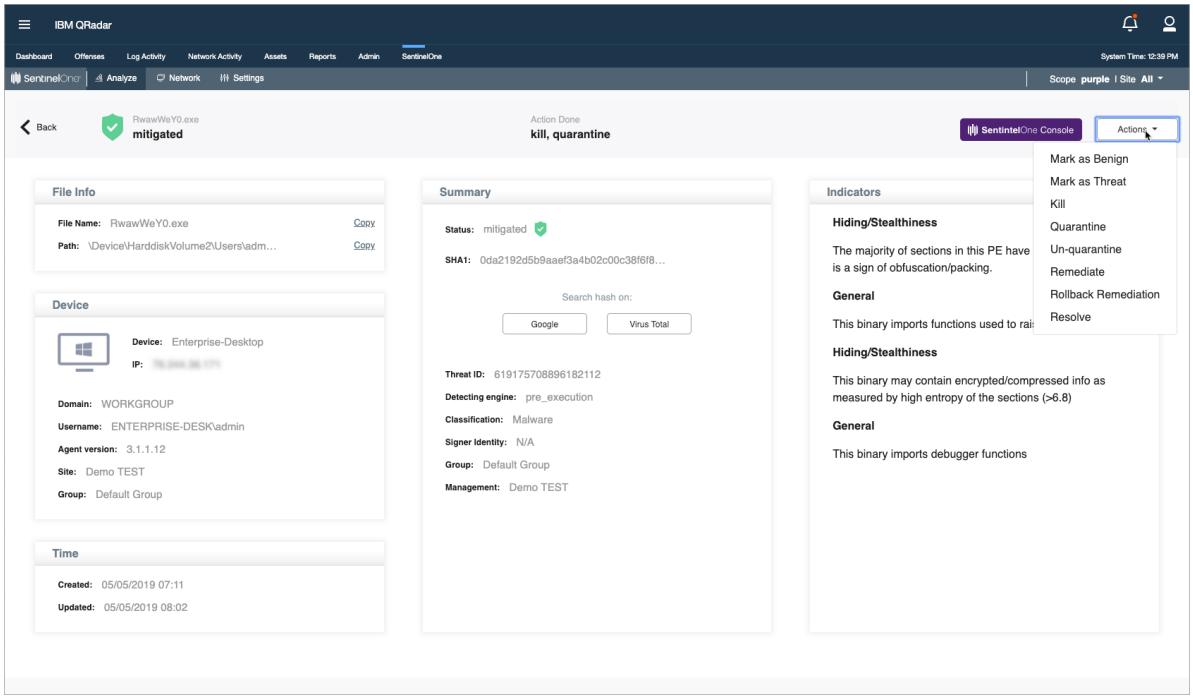
1.1. QRadar and SentinelOne Integration Highlights

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

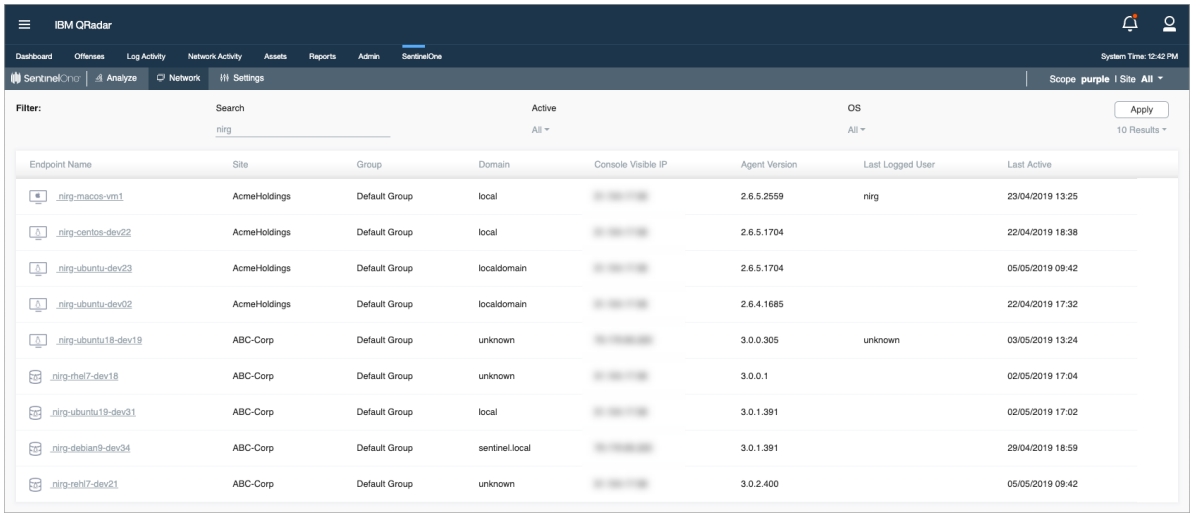
- View a list of threats from the SentinelOne App for QRadar Analyze page.



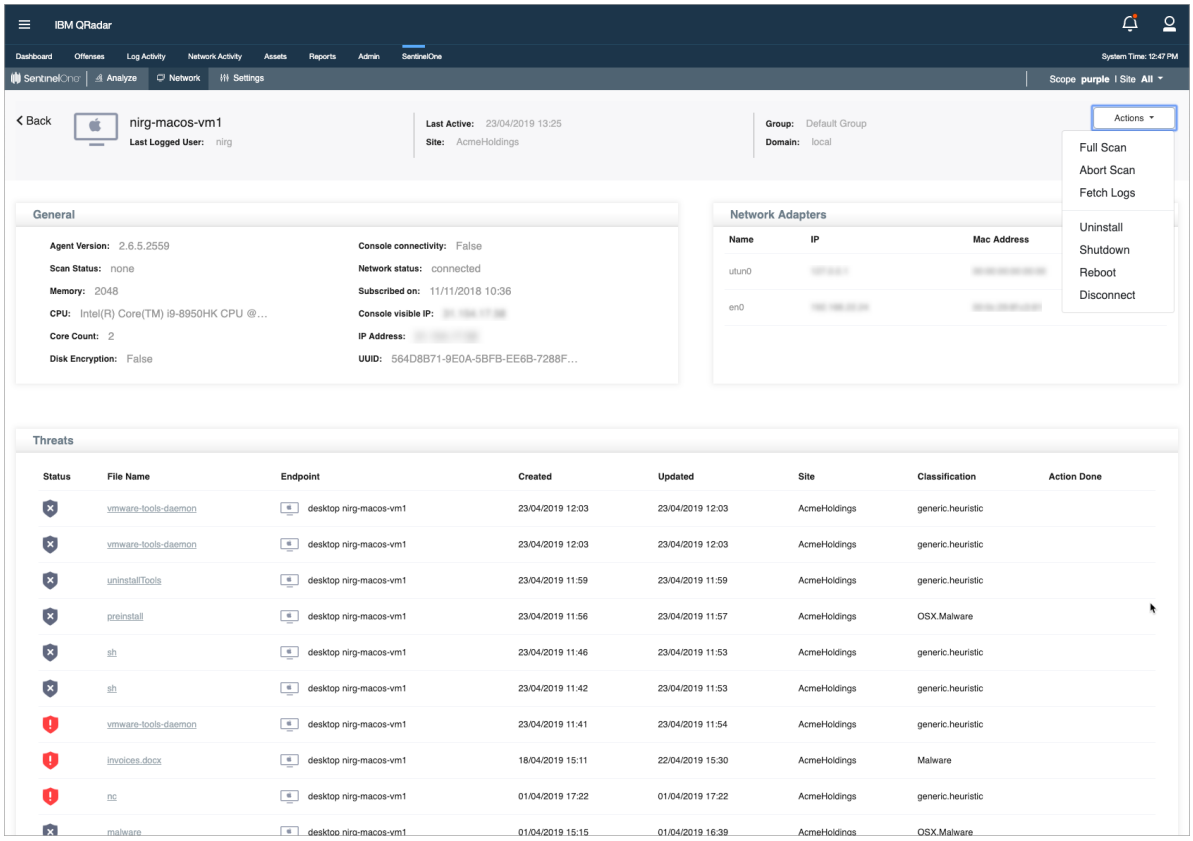
- View threat details and mitigate threats from the QRadar console. SentinelOne authorized users can also click a hyperlink to the SentinelOne Management Console Forensics page.



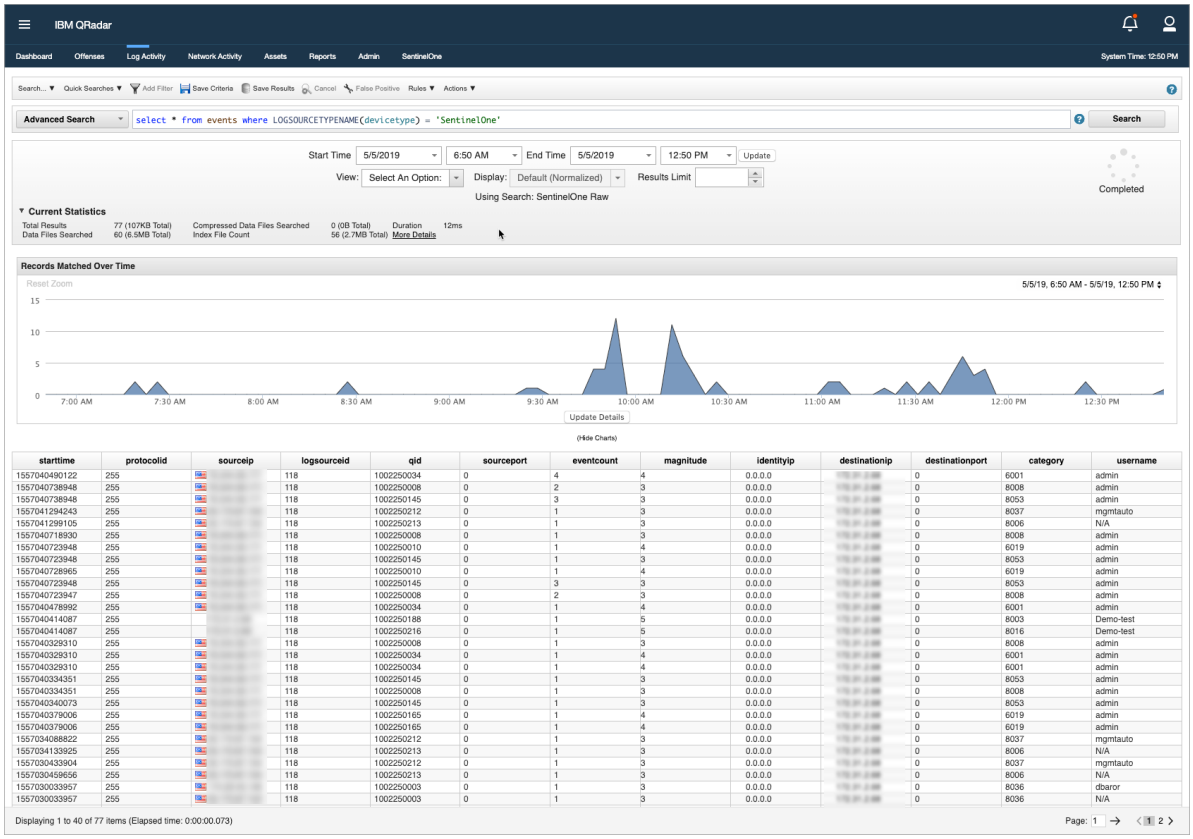
- Filter threat lists from the SentinelOne App for QRadar Network page.



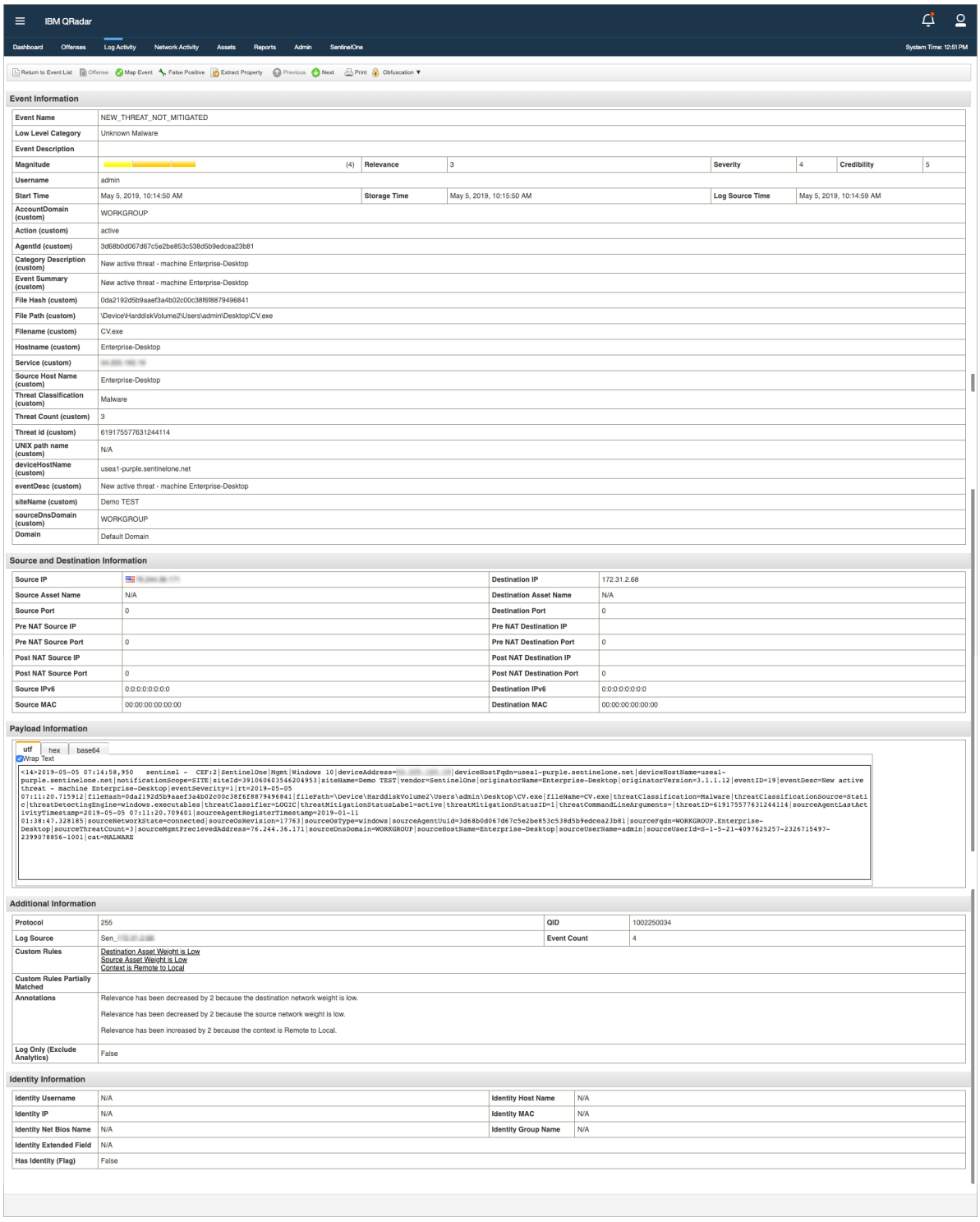
- Disconnect an endpoint from the network and see endpoint associated information, such as the last logged in user and threat history.



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



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



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

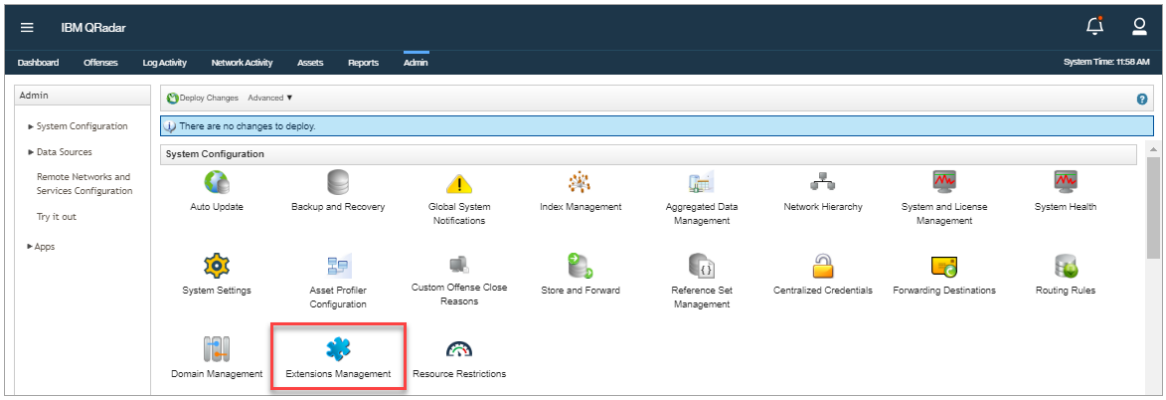
The SentinelOne DSM enables you to send SentinelOne log events and endpoint data to the QRadar Console.

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.

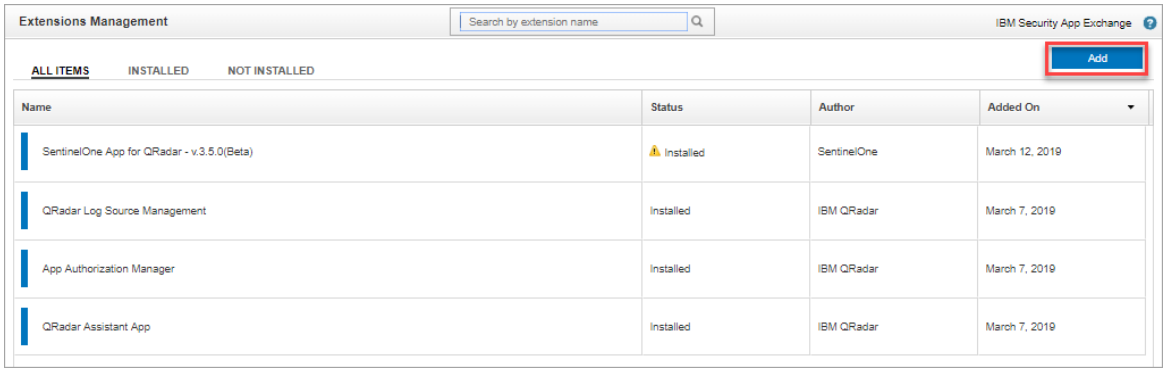
To install the SentinelOne DSM:

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**.

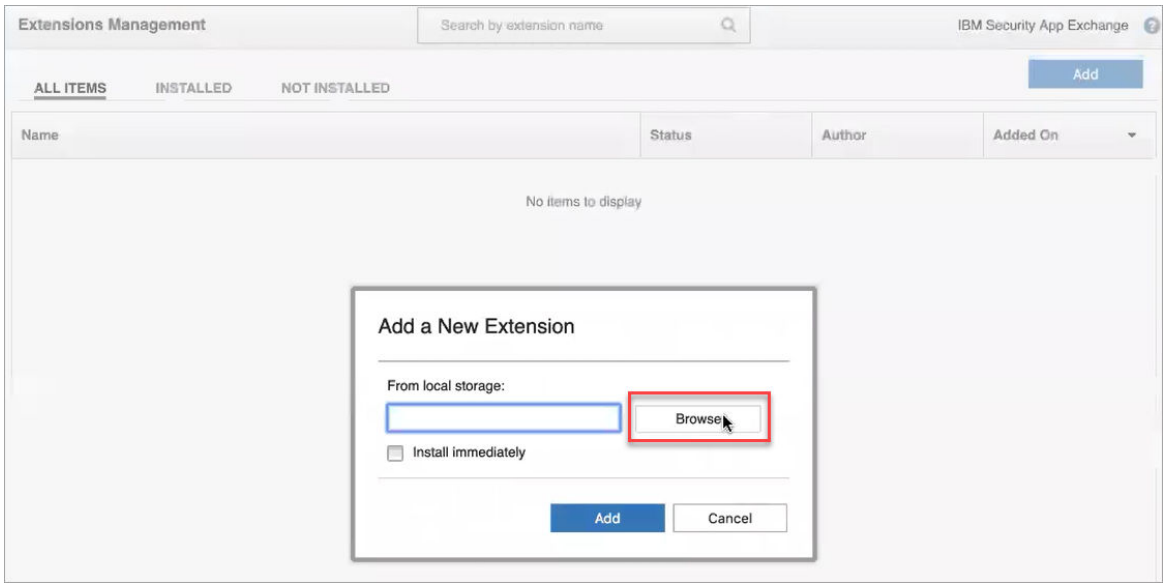
4. Click **Extensions Management**.



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

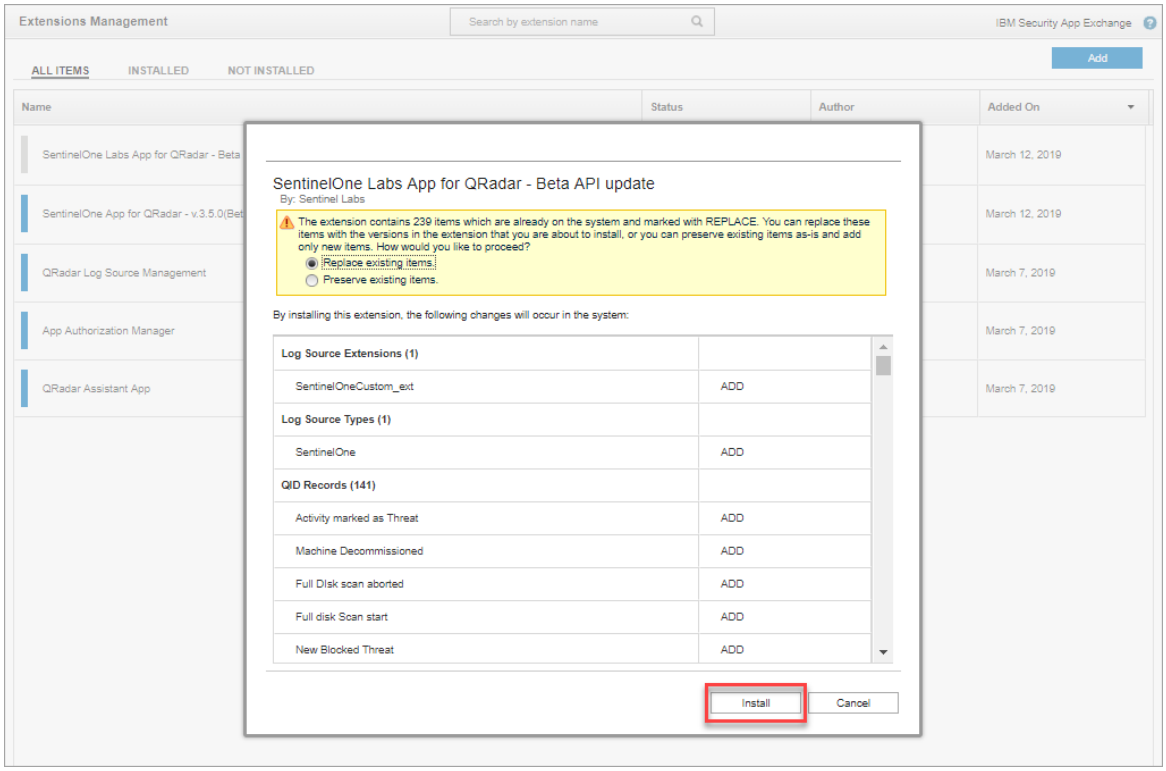


6. In the window that opens, click **Browse**. Browse to the location of the downloaded SentinelOne DSM file.

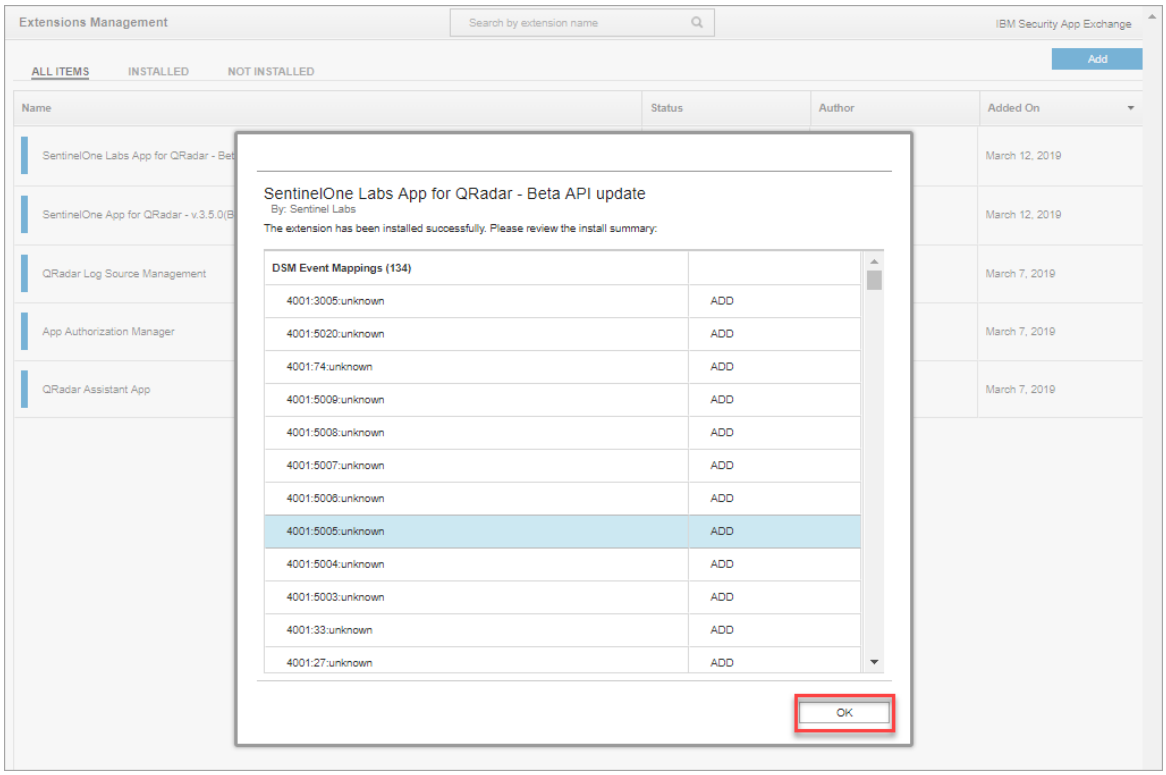


7. To immediately install the app, select **Install immediately** and click **Add**.

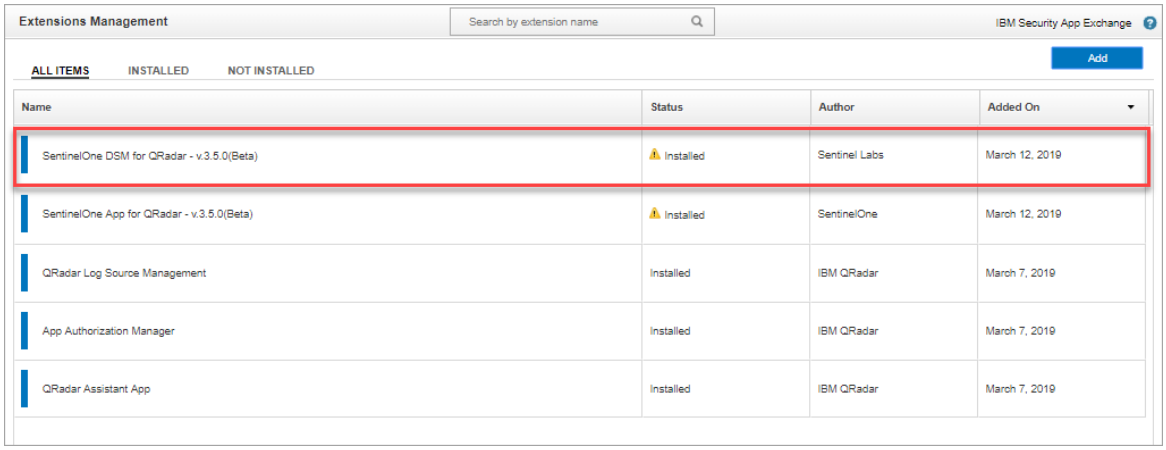
8. Click **Install**.



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



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



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

3.2. Adding SentinelOne as a Log Source for QRadar

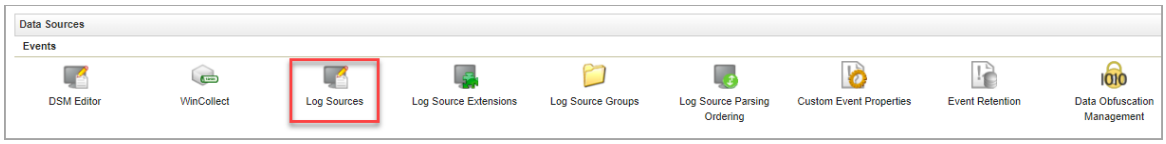
Add each SentinelOne Console as a log source to define how QRadar gets Syslog messages from SentinelOne.

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

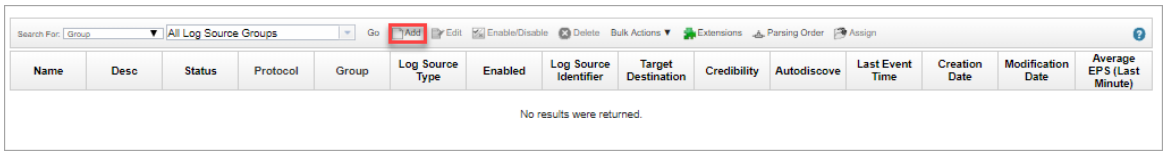
Use the TLS Syslog protocol for QRadar to receive encrypted syslog events from SentinelOne.

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

3. Click **Log Sources**.



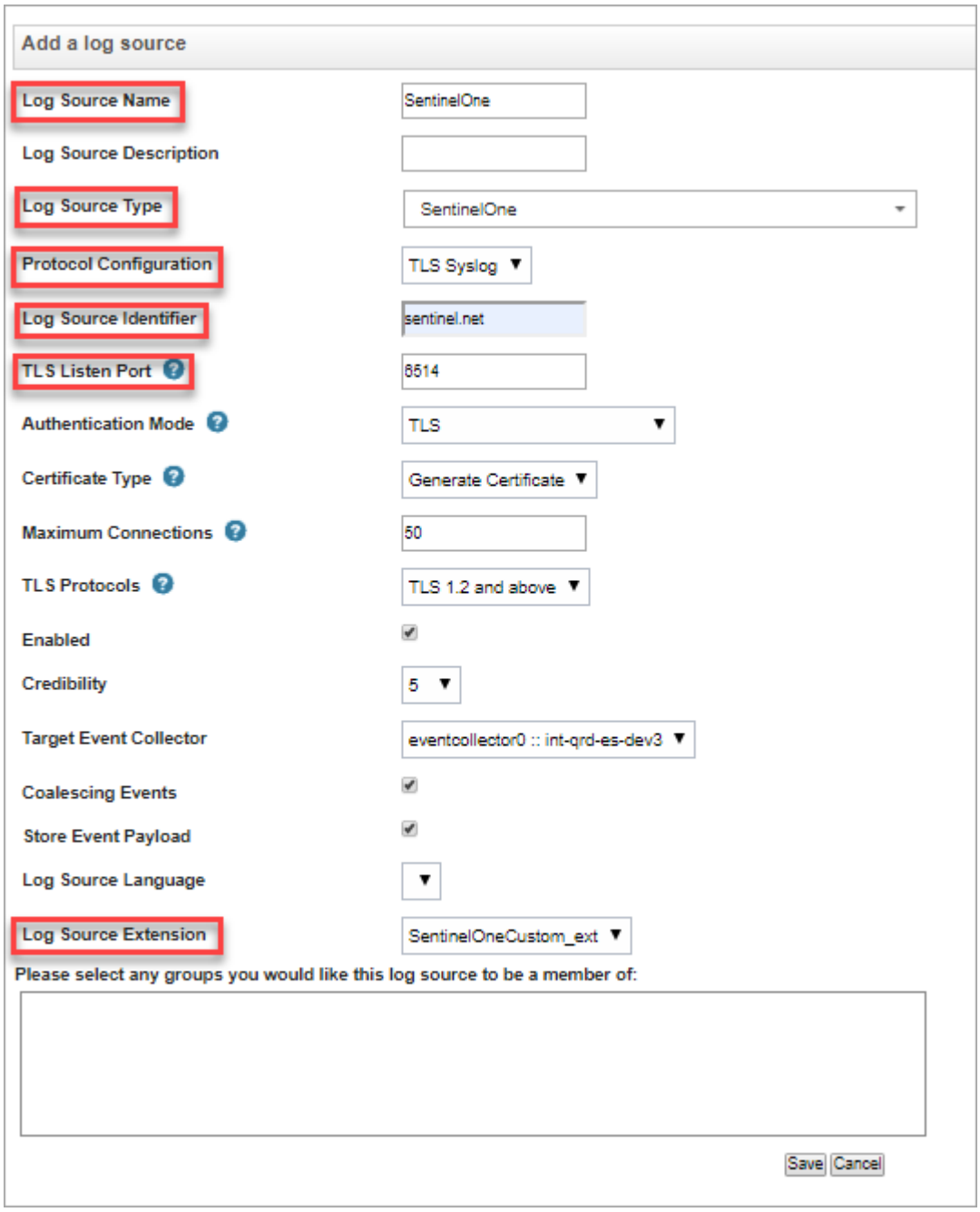
4. Click **Add**.



5. In the form that opens:
   - **Log Source Name:** Enter a unique name of the log source.
   - **Log Source Type:** Select **SentinelOne**.

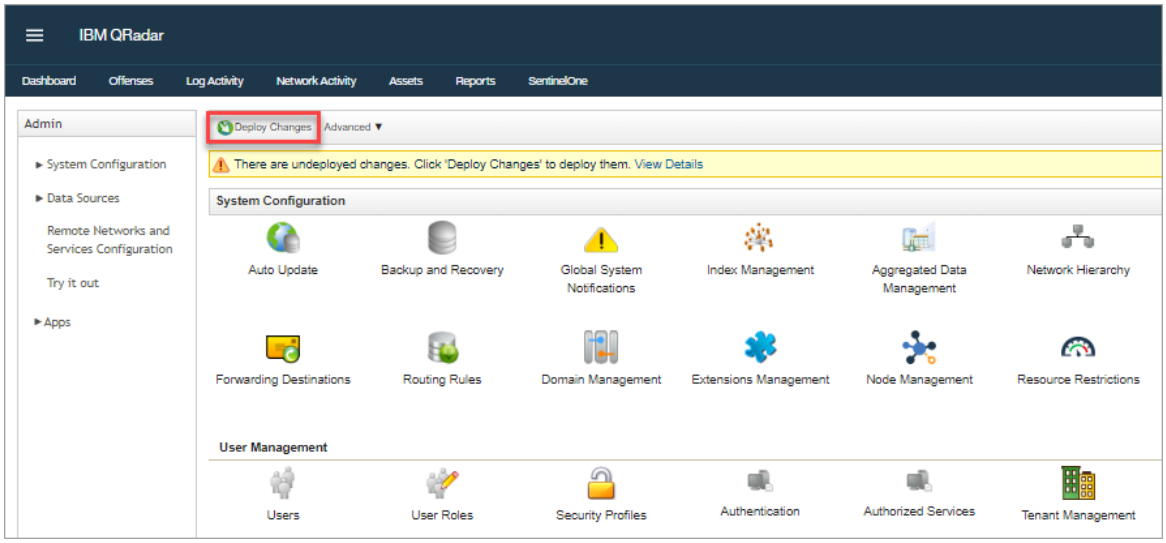
- **Protocol Configuration:** Select **TLS Syslog**. See TLS syslog protocol configuration options.
- **Log Source Identifier:** Enter **sentinel.net**.
- **TLS Listen Port**: Make sure it is set to **6514**.
- **Log Source Extension:** Make sure **SentinelOneCustom_ext** is selected.

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



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

8. Click **Deploy Changes**.



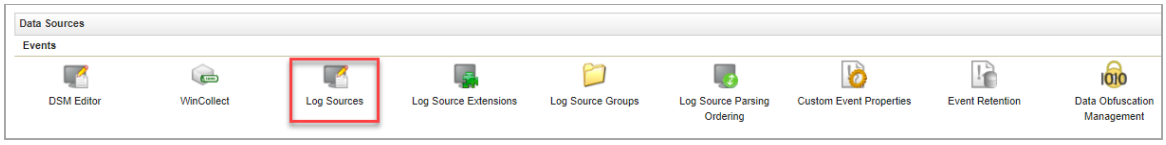
9. Configure a second log source, using either the **Syslog** or **Forwarded** protocol. For instructions, see To add SentinelOne as a log source for QRadar using the Syslog or Forwarded protocol [11].

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

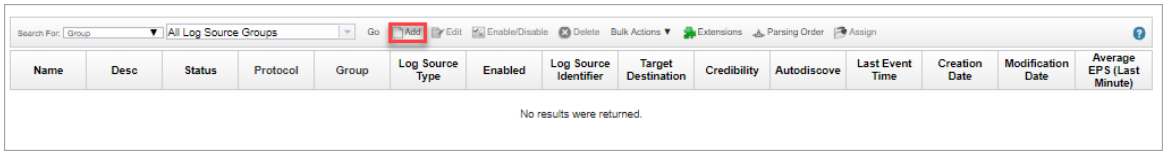
Use the Syslog or Forwarded protocol for QRadar to receive unencrypted syslog events from SentinelOne.

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

3. Click **Log Sources**.



4. Click **Add**.

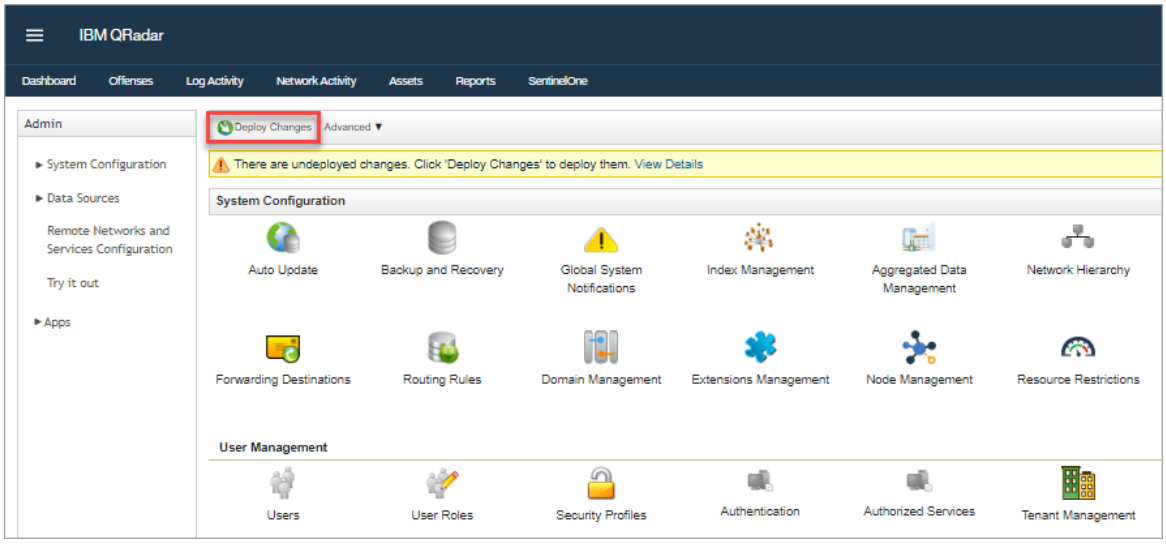


5. In the form that opens:

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

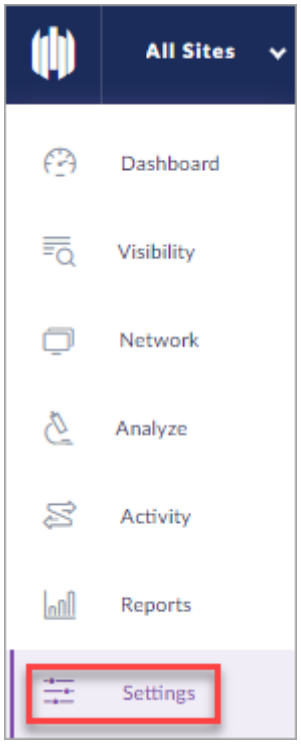
2. In the browser address bar, enter the management console URL provided by the SentinelOne support team (for example, *https://yourcompany.sentinelone.net/*).

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.

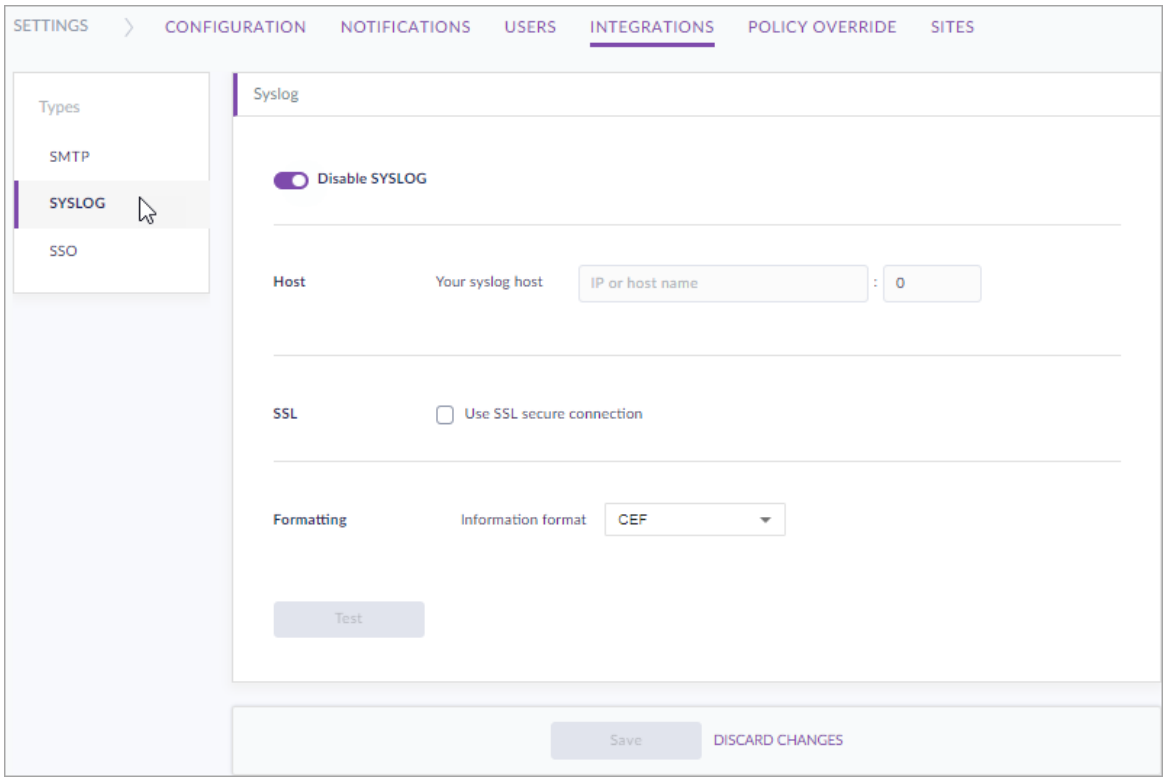
4. In the SentinelOne Management Console, click **Settings**.



5. If you are a Site or Account Admin, you must select one Site to open Settings.

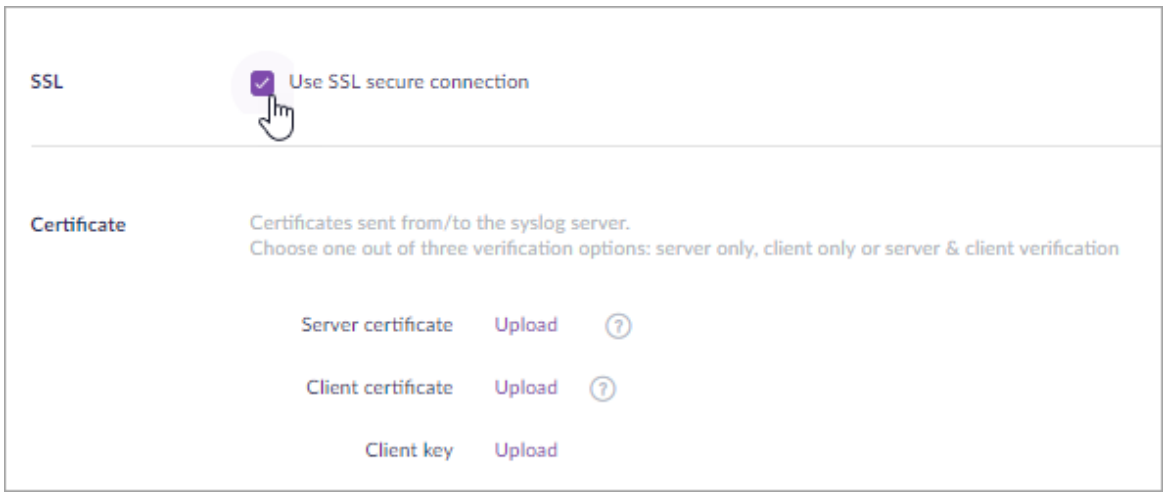
6.

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.



- **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`.

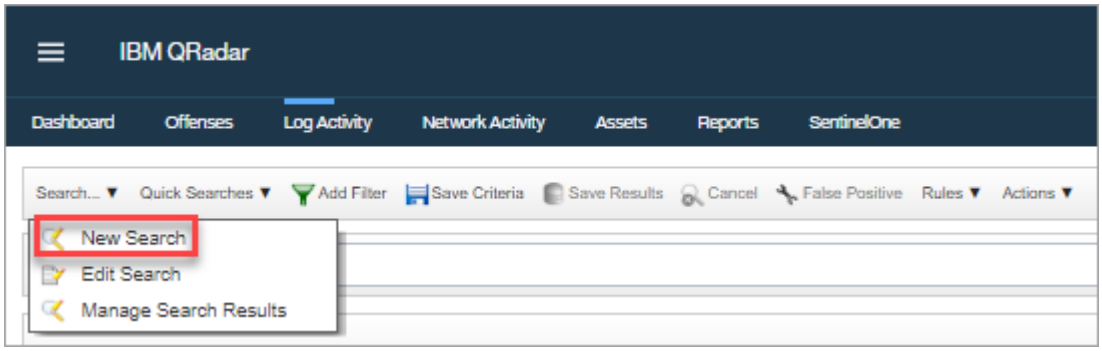
12. In Formatting, select **CEF2**. This format is required to enable integration with the SentinelOne DSM.
13. To verify connectivity with your QRadar server, click **TEST** to send a test trap.
14. If the test passed, click **SAVE**.

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:

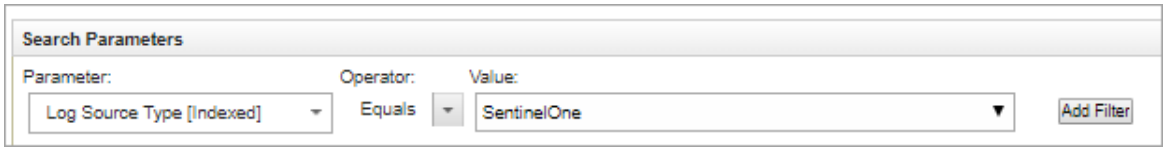
1. In the QRadar Console, click **Log Activity**.
2. Click **Search** and select **New Search**.



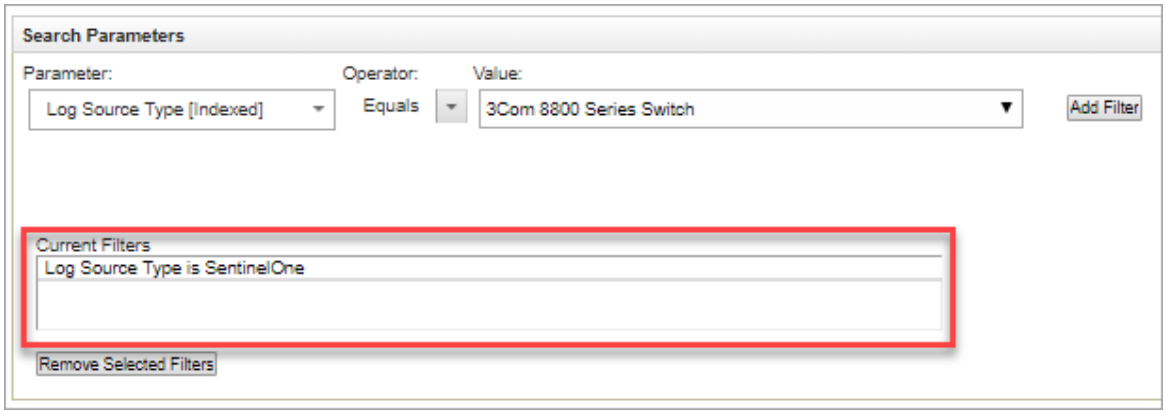
3. In **Search Parameters > Parameter** , select **Log Source Type [Indexed]**.

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

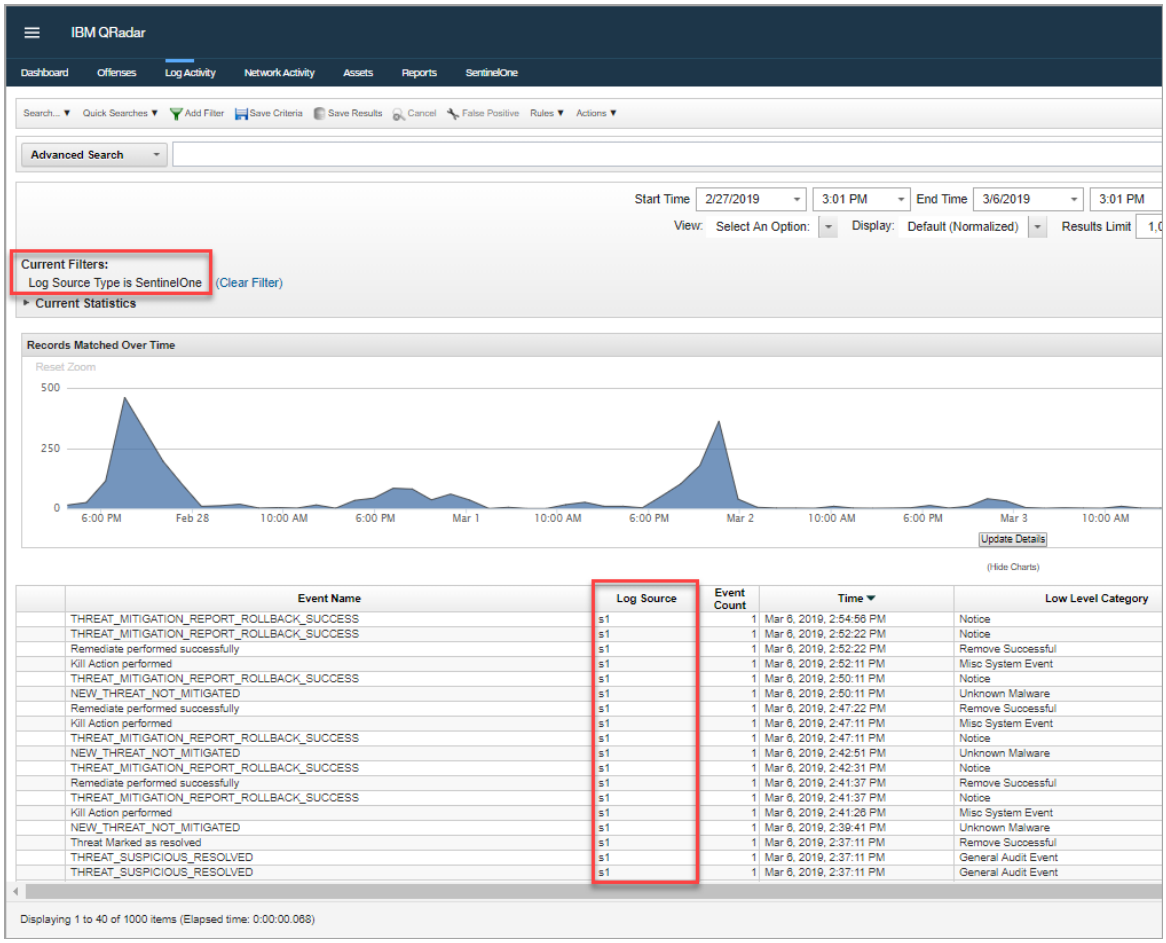
   Select **SentinelOne** as the **Value**.



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

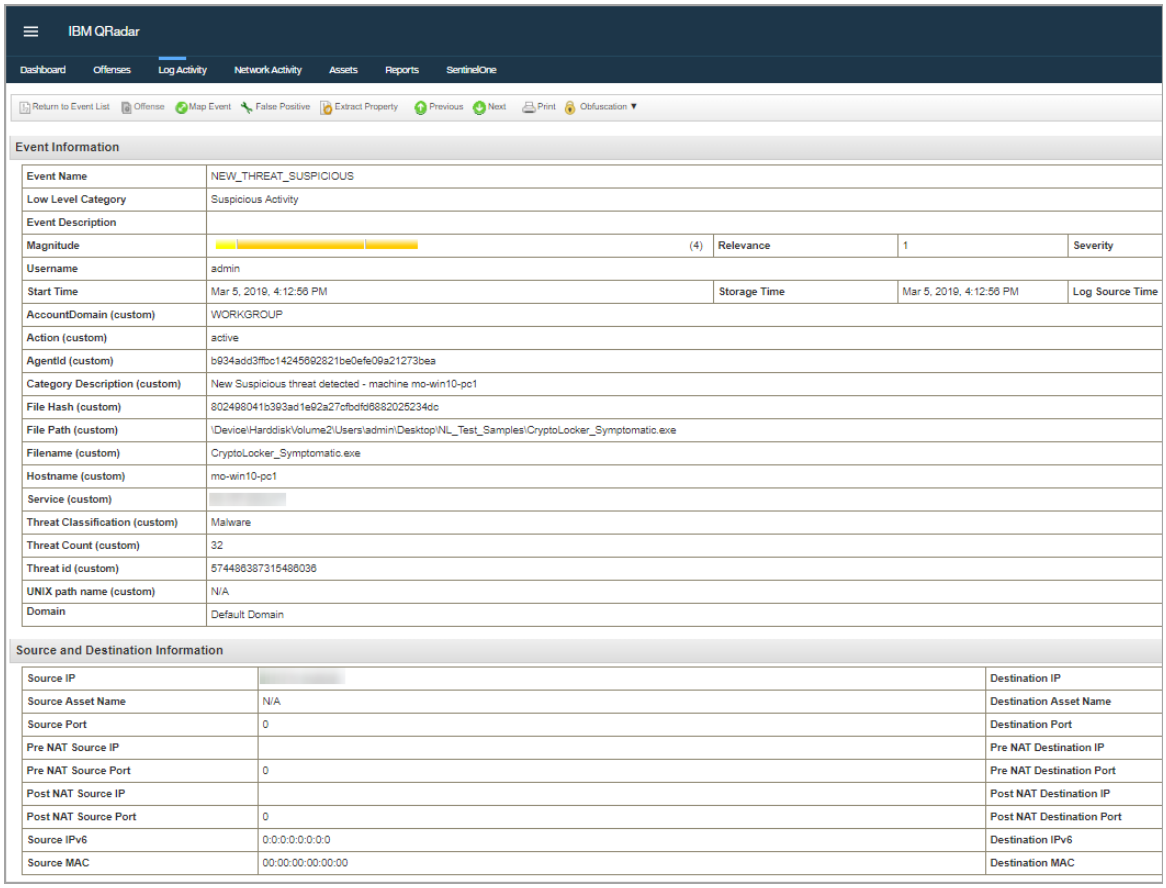


5. Click **Search**. The QRadar Log Activity shows all log activity sent from SentinelOne to QRadar.



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

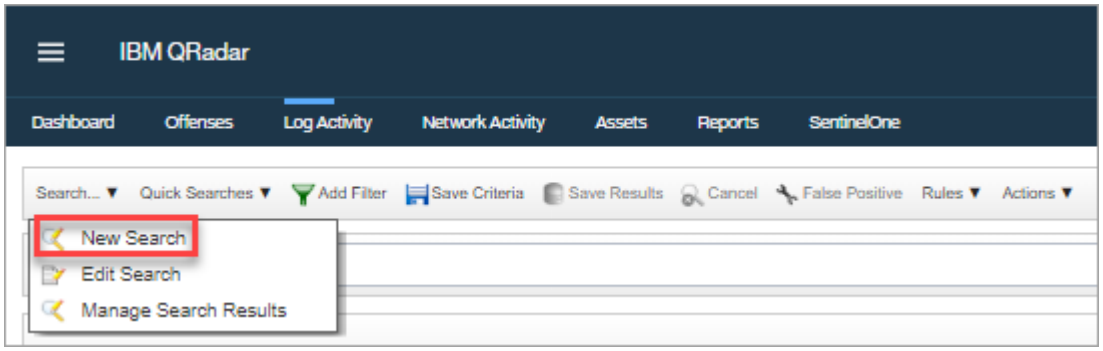
6. Double-click an event row for more details.



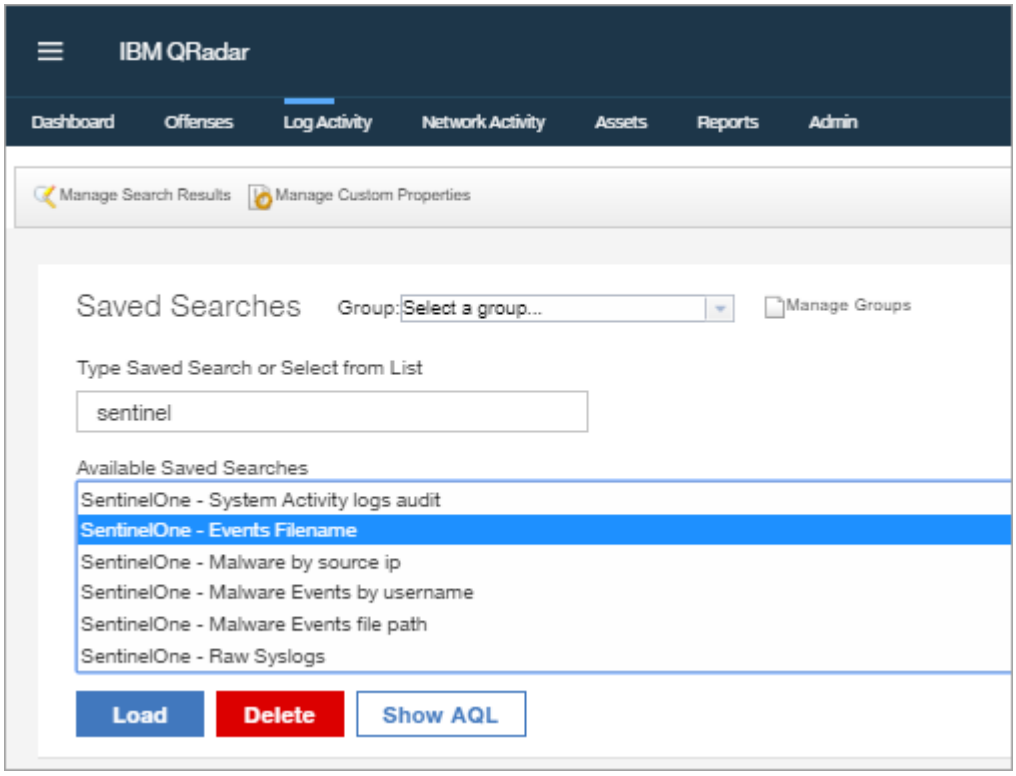
To use predefined SentinelOne filters:

The SentinelOne DSM comes with SentinelOne predefined saved filters.

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

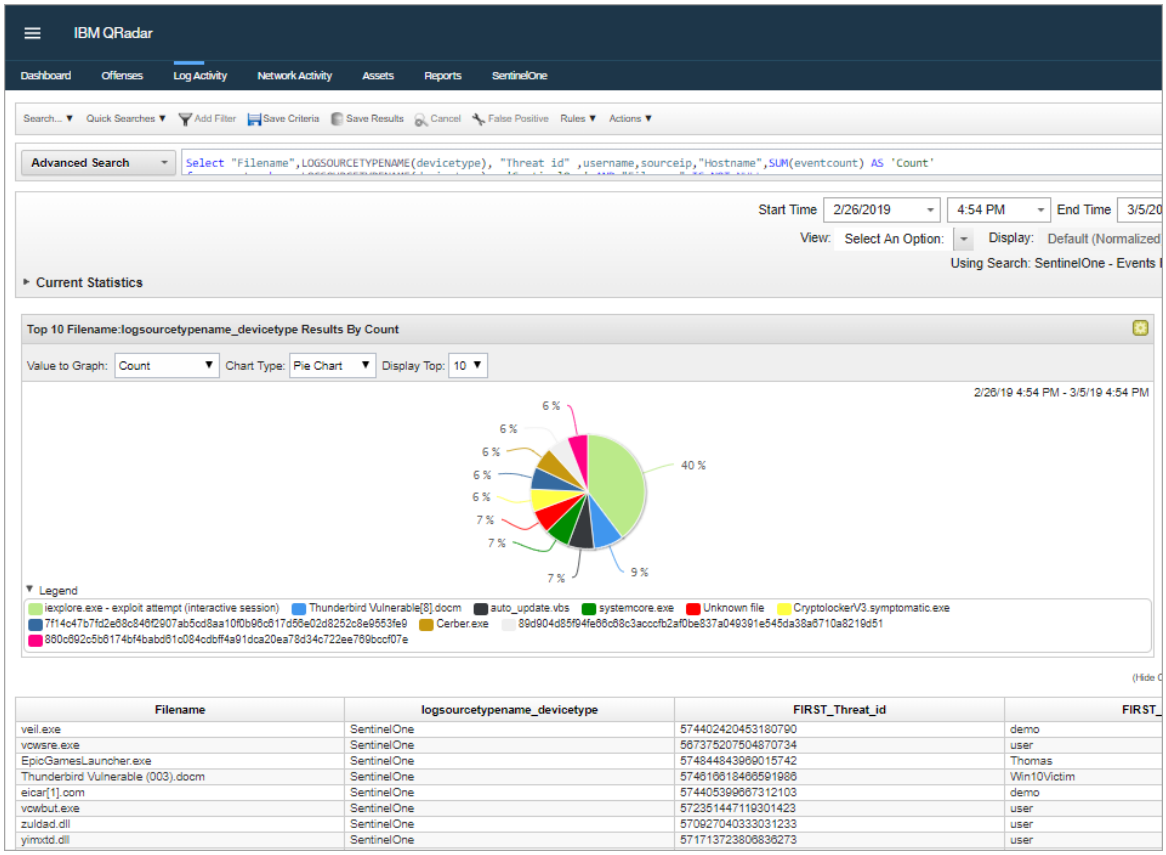


3. In **Type Saved Search or Select from List**, enter `SentinelOne`.



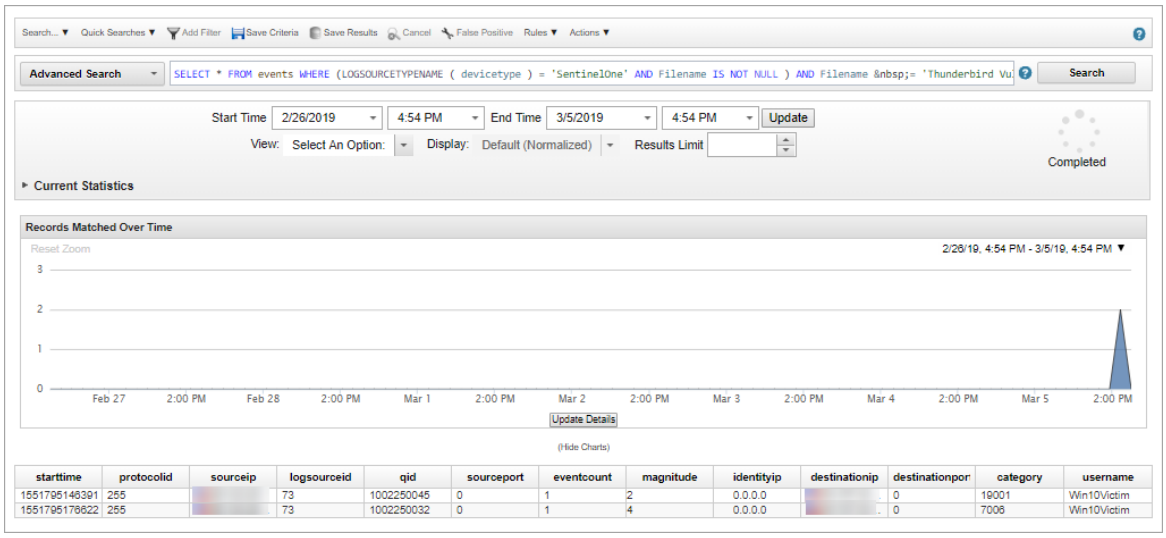
4. Select one of the predefined saved filters.

5. Click **Load**.

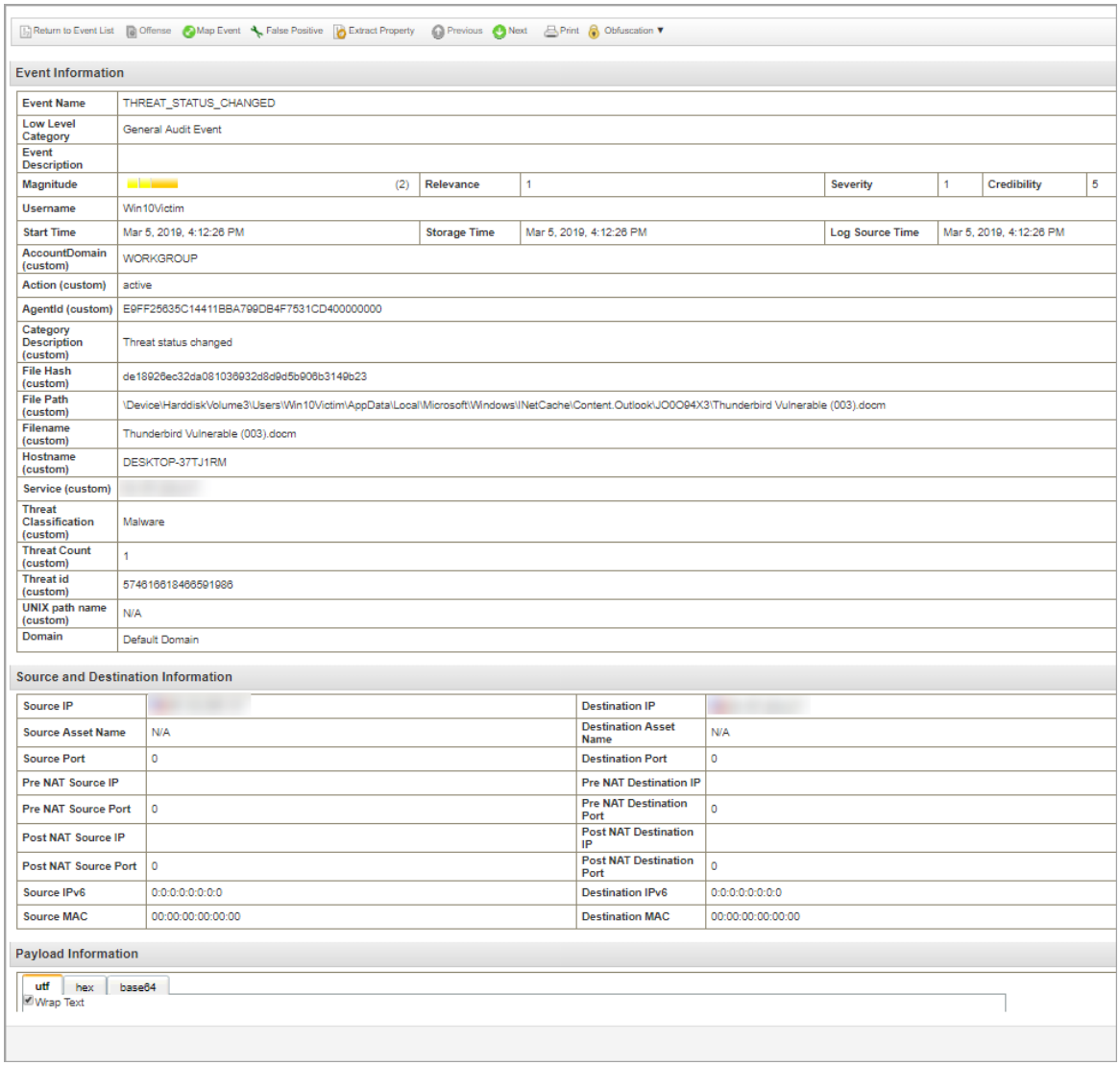


6. Click an event for more details.

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



7. 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
Win10\Victim
Start Time
Mar 5, 2019, 4:12:26 PM
Storage Time
Mar 5, 2019, 4:12:26 PM
Log Source Time
Mar 5, 2019, 4:12:26 PM
AccountDomain (custom)
WORKGROUP
Action (custom)
active
AgentId (custom)
E9FF25635C14411BBA799DB4F7531CD400000000
Category Description (custom)
Threat status changed
File Hash (custom)
de18926ec32da081036932d8d9d5b906b3149b23
File Path (custom)
\Device\HarddiskVolume3\Users\Win10\Victim\AppData\Local\Microsoft\Windows\INetCache\Content.Outlook\JO0O94X3\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)
574616618466591986
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.

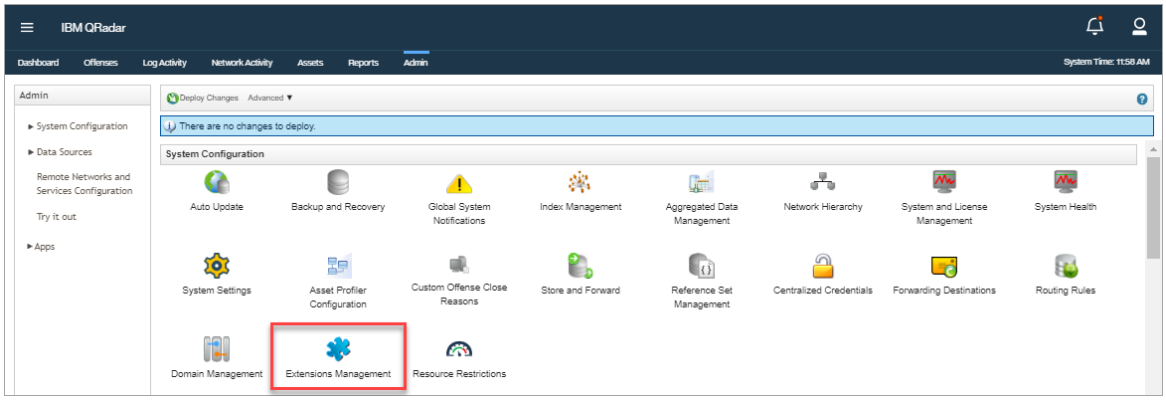
Note: The SentinelOne App is not supported on Internet Explorer.

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.

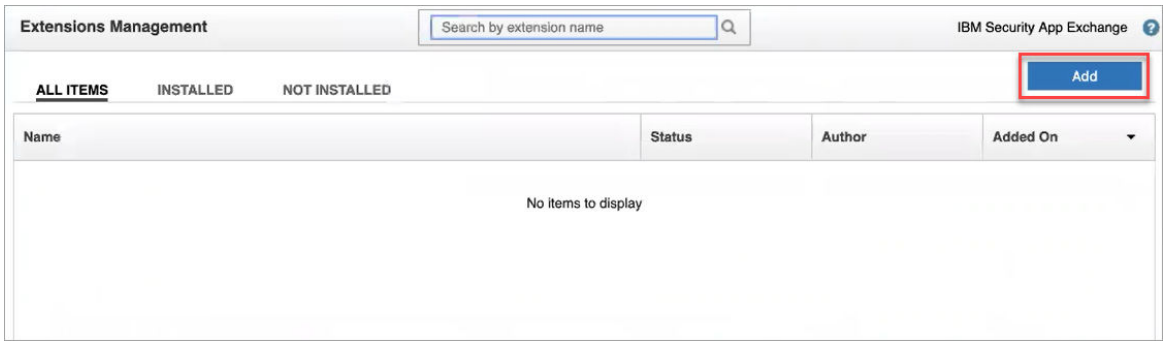
To install the SentinelOne App:

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**.

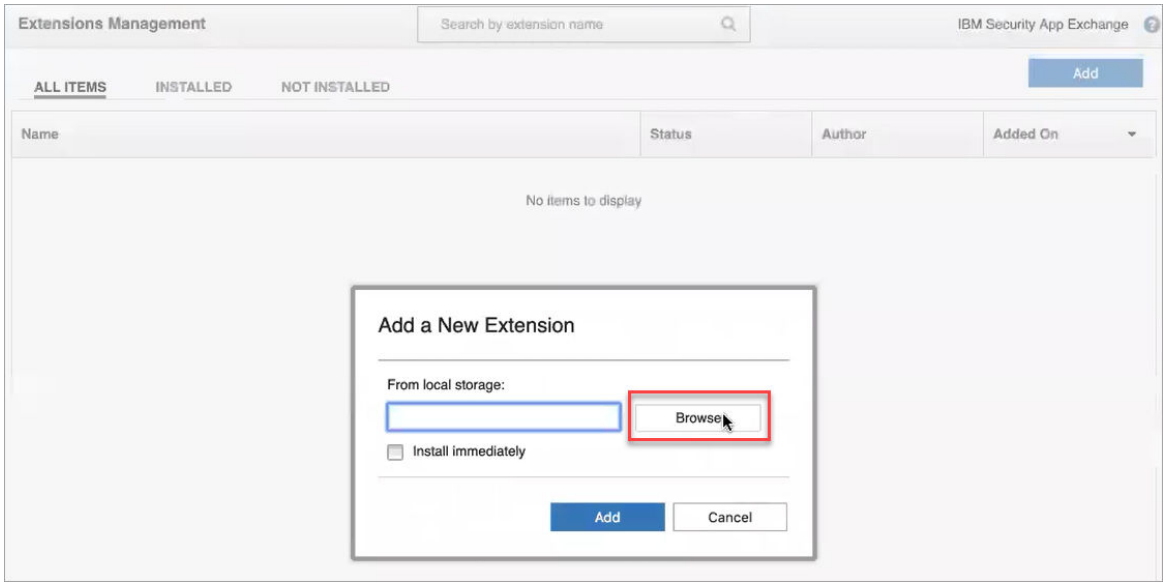


5. In the window that opens, click **Add**.



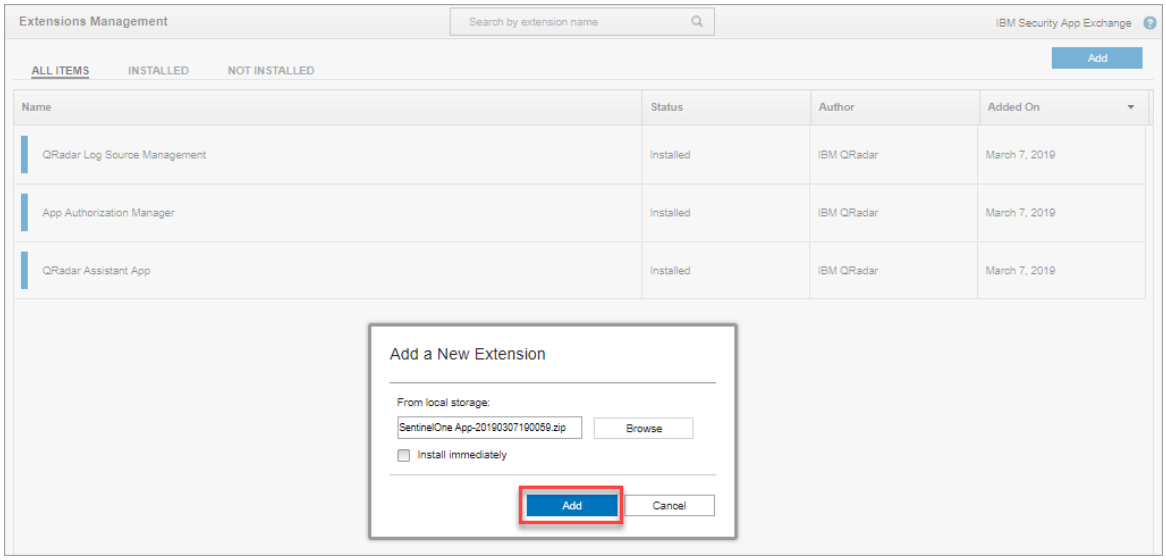
6. In the window that opens, click **Browse**. Browse to the location of the downloaded SentinelOne App file.

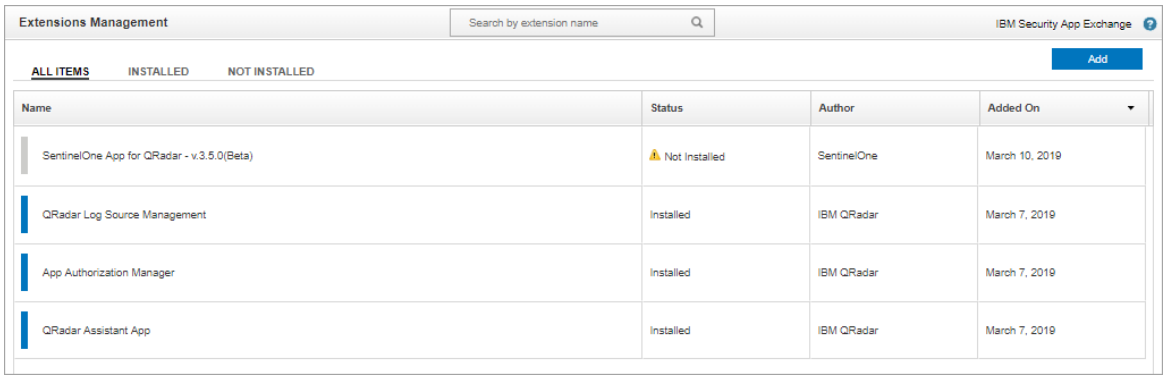
   If you do not see this option, make sure you have the required Admin permissions.



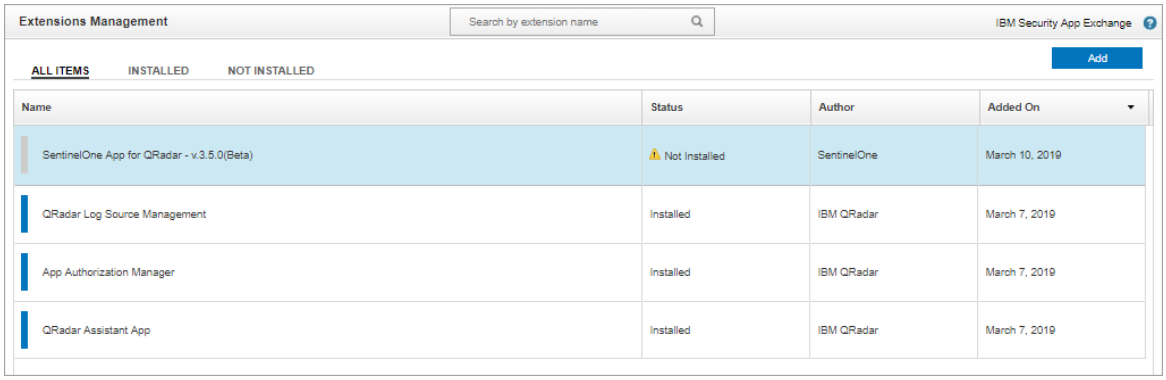
7. If you want to immediately install the app, skip to Step 10.

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

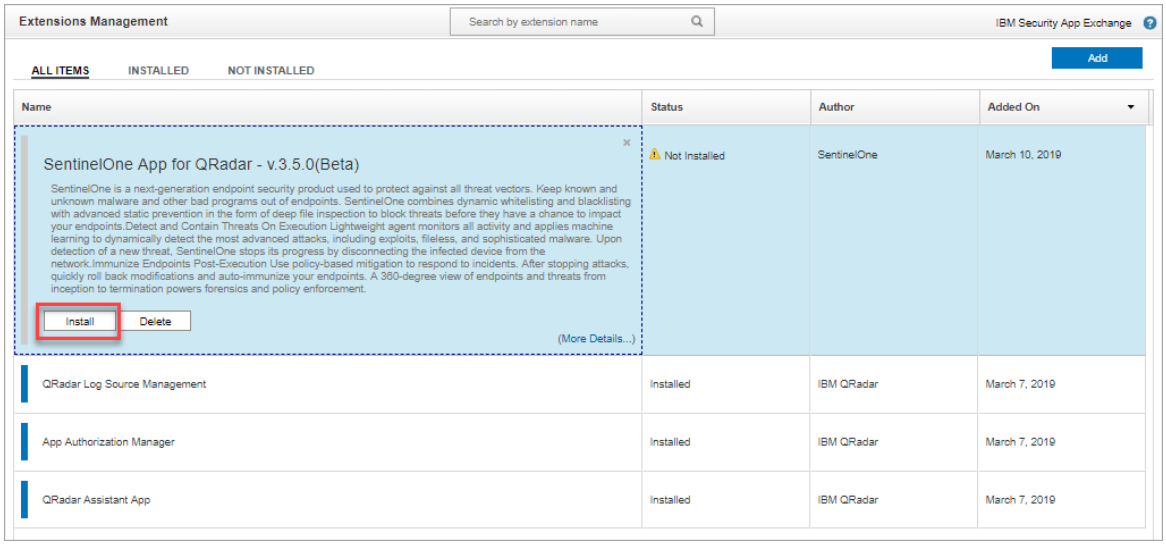




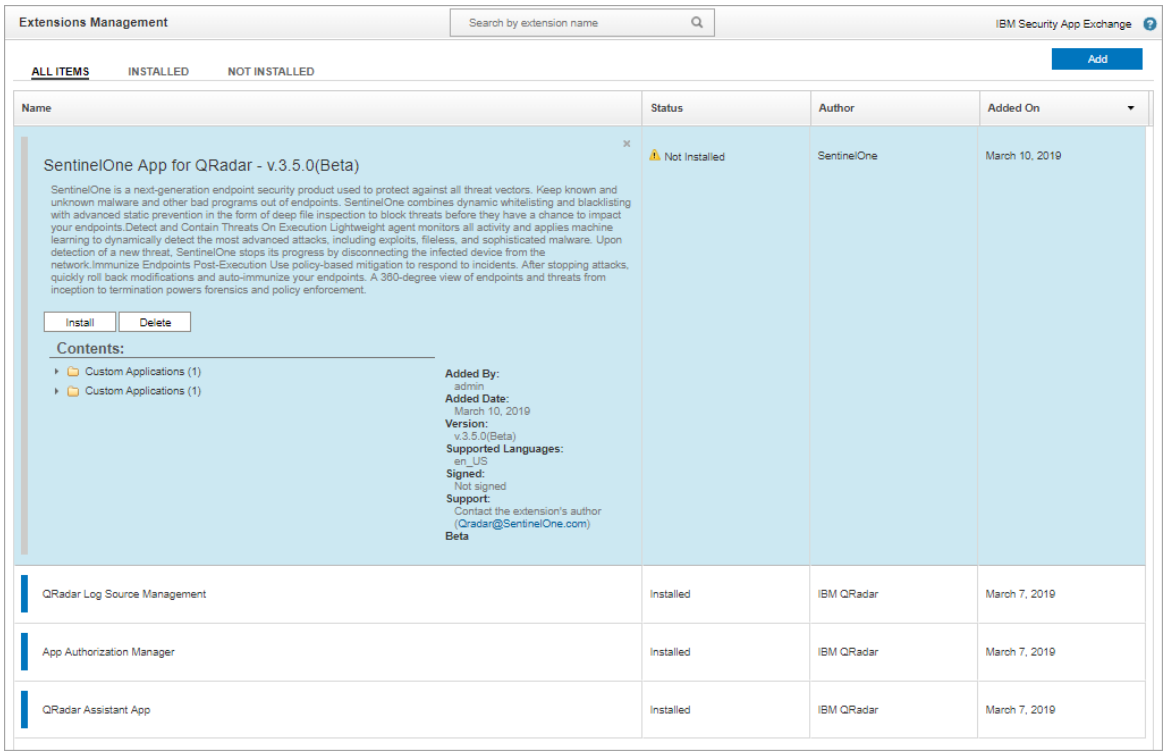
8. Select **SentinelOne App for QRadar**.



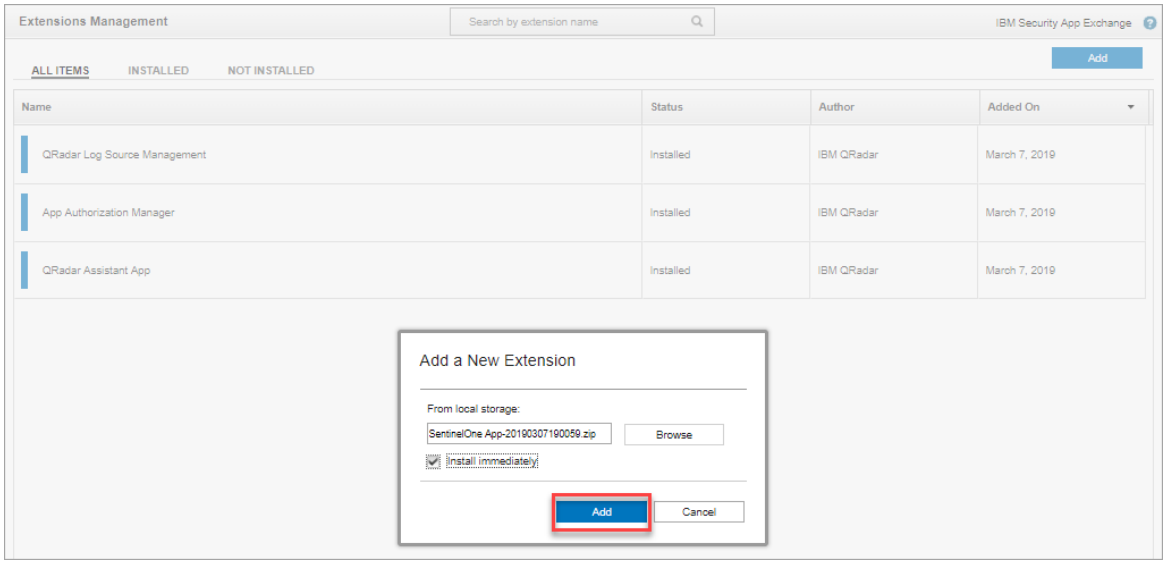
9. In the box that opens, click **Install**.



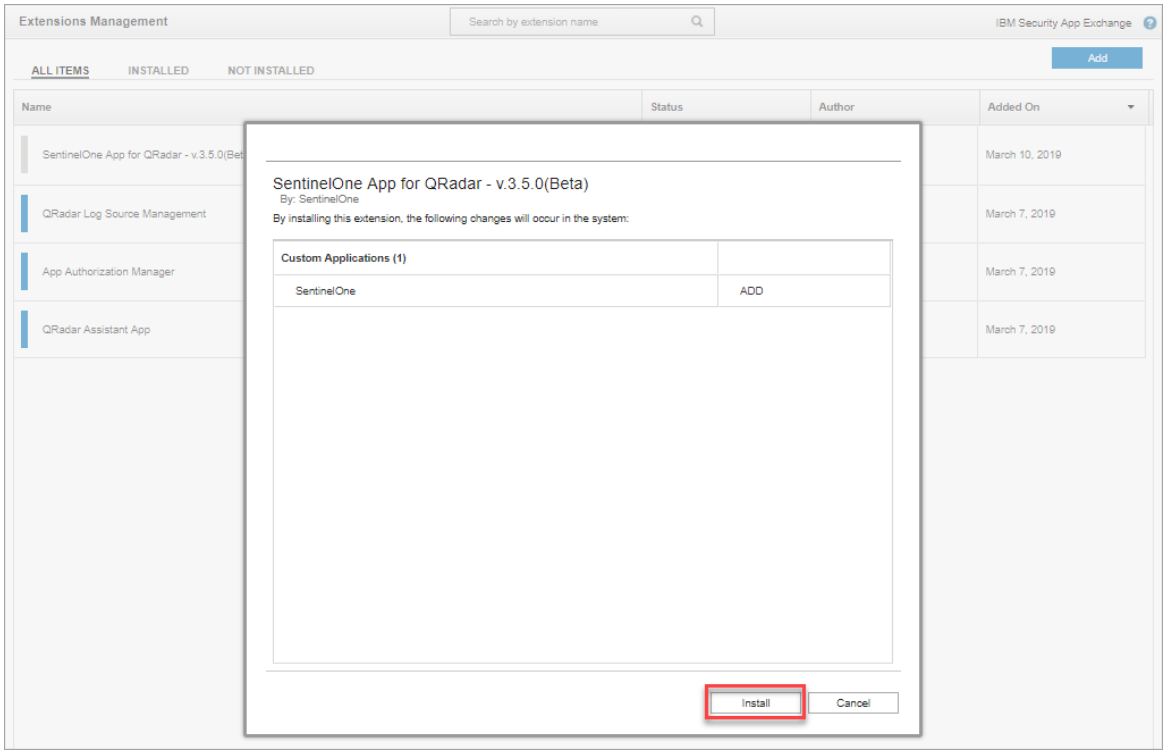
You can click **More Details** to see more information and the installation files.



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

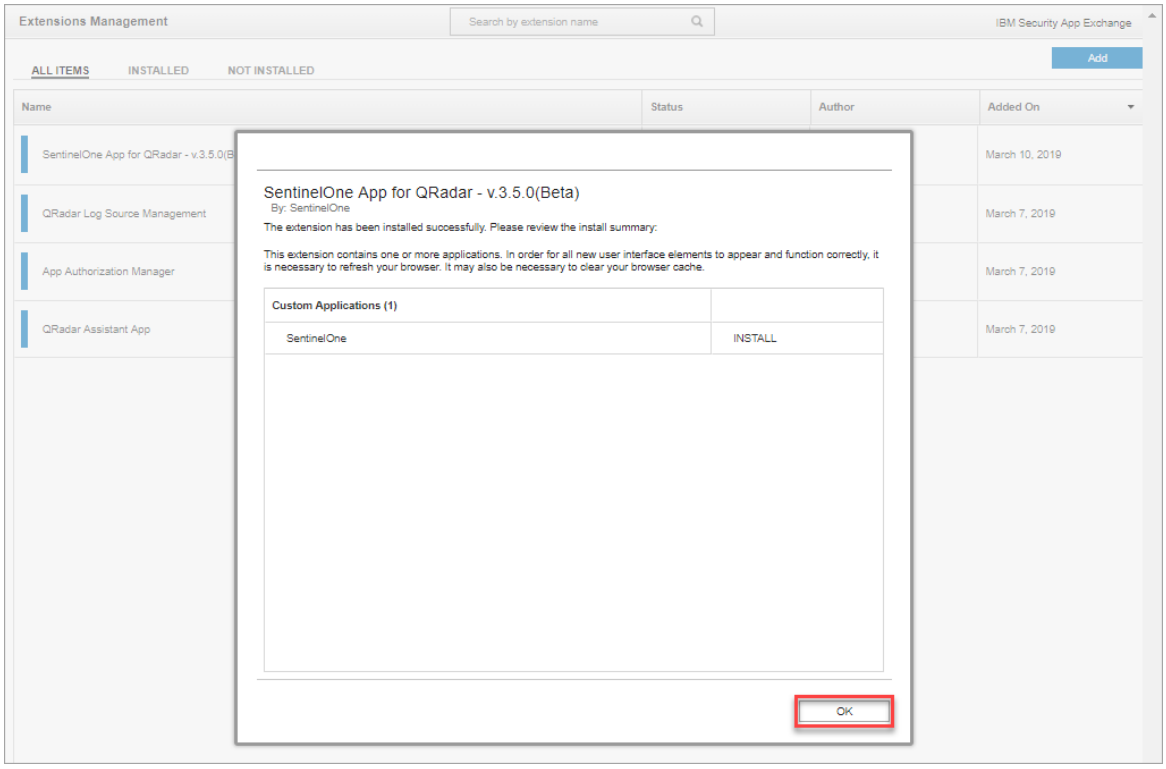


11. In the window that opens, click **Install**.

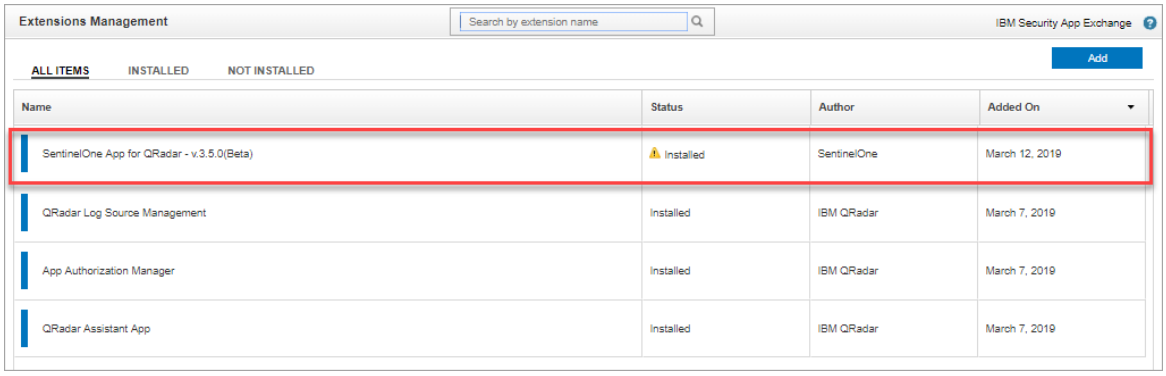


The installation might take a couple of minutes.

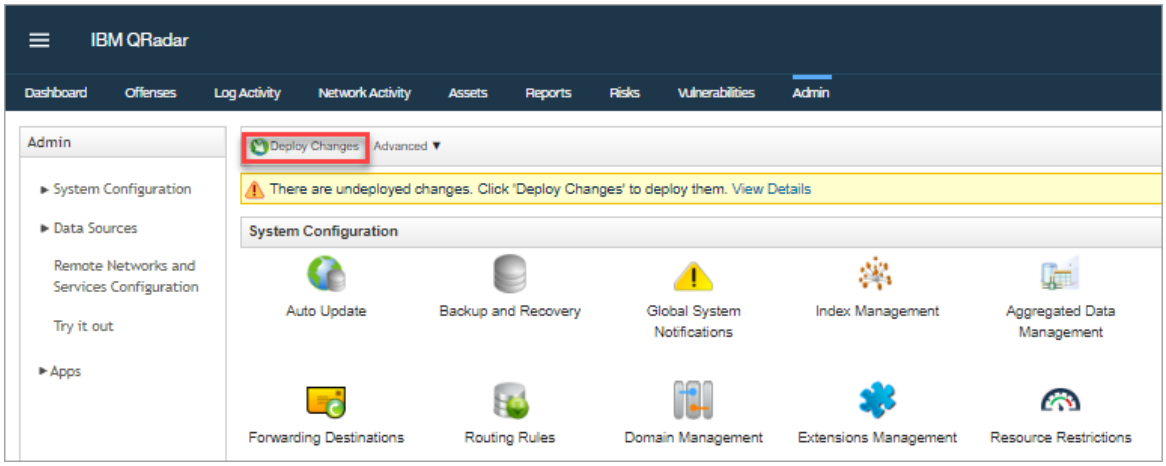
12. When you see the message that the extension installed successfully, click **OK**.



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:

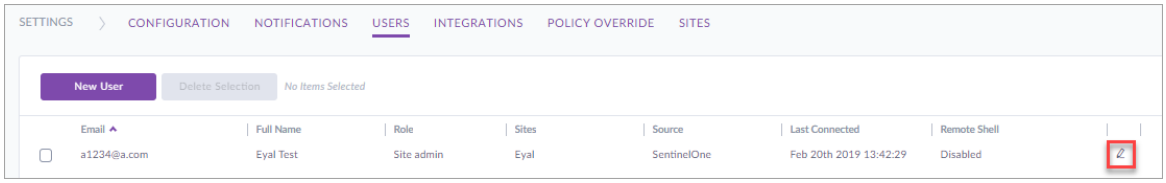
1. In your Management Console, click **Settings** > **USERS**.

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.

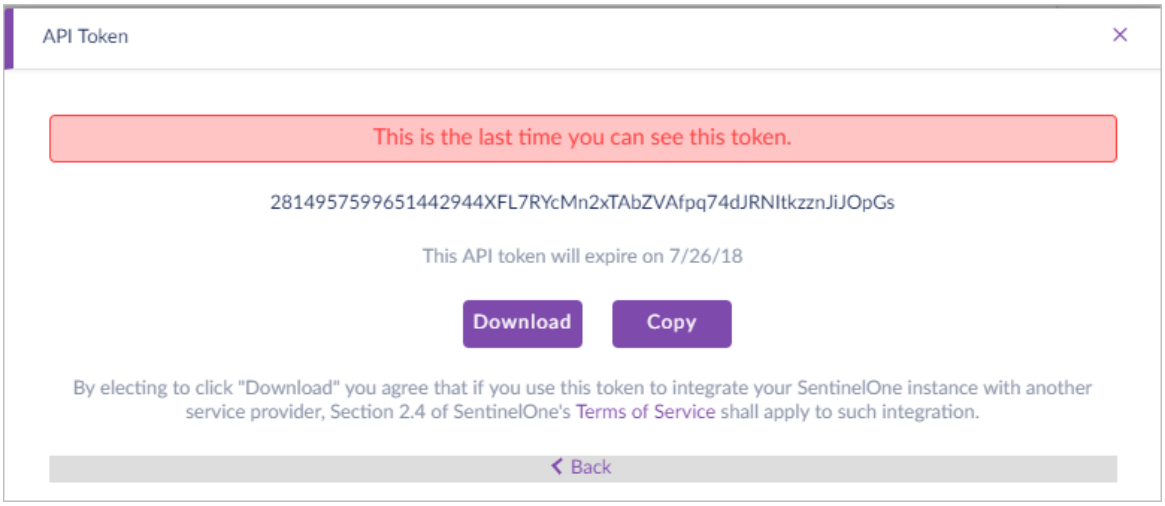


The **Edit User** window opens.

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

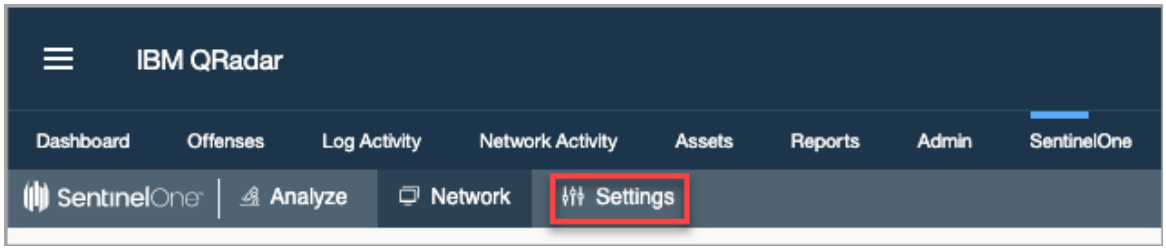
To use the SentinelOne App, you must add each SentinelOne Management Console as input for the SentinelOne App.

To add a SentinelOne Management Console in the SentinelOne App:

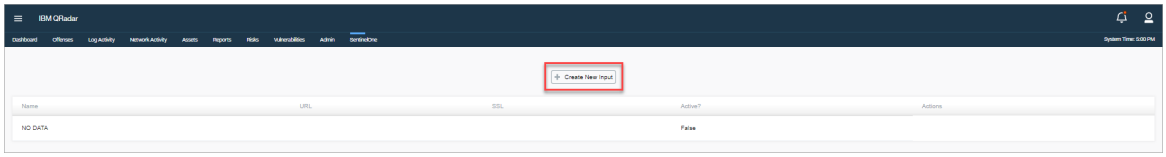
Note: If you have more than one SentinelOne Management Console, repeat this procedure for each one.

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**.

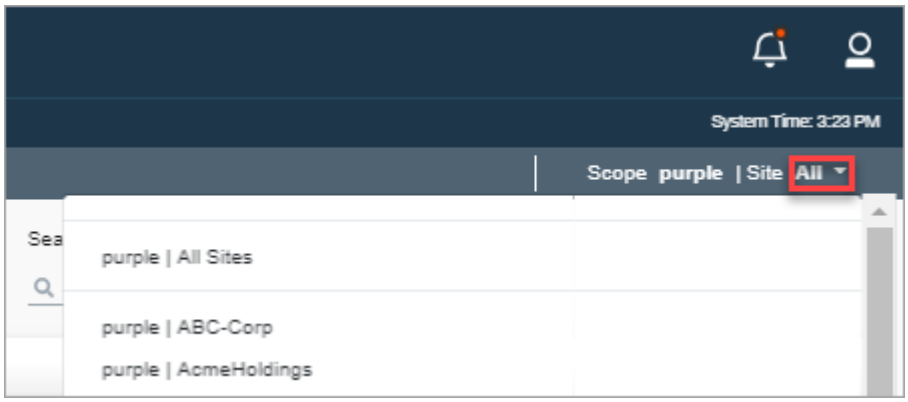
4.4. Using the SentinelOne App

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

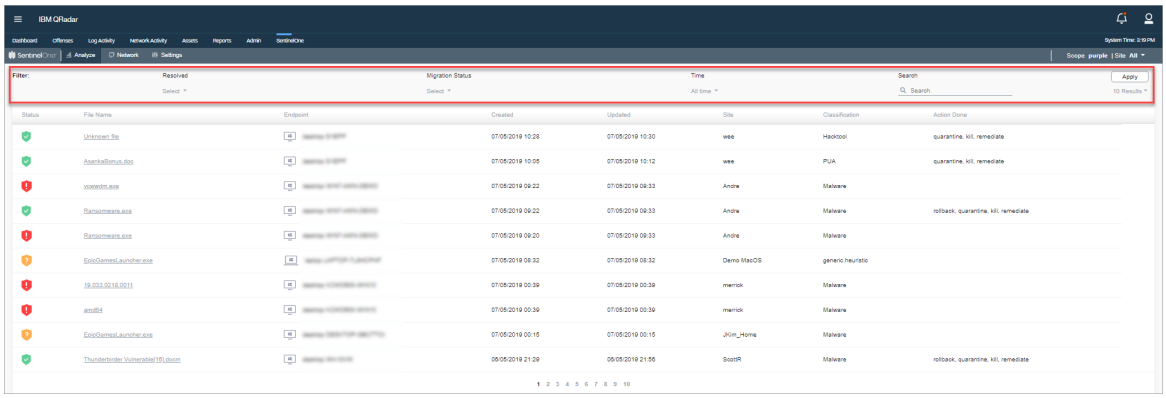
To see and filter threats:

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.



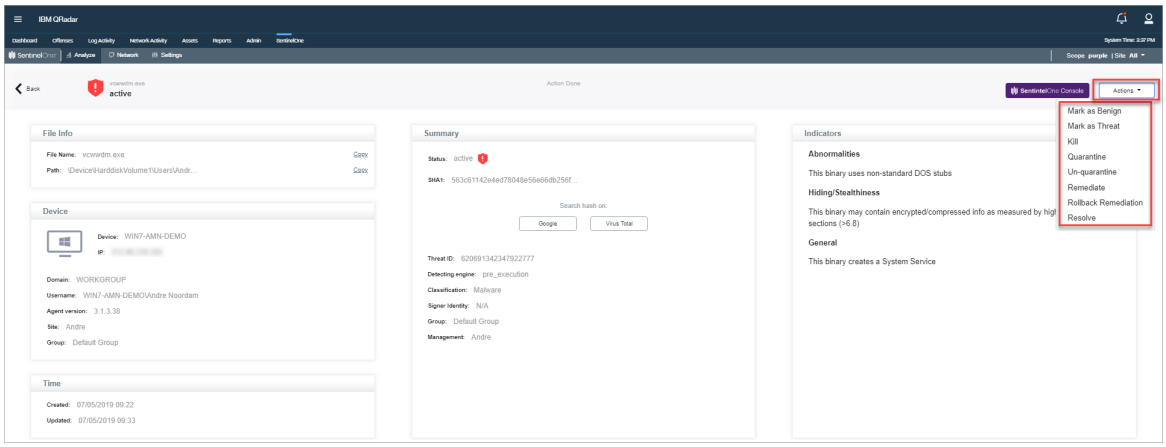
3. To find specific threats, use the **Filter** and **Search** options, and click **Apply**.



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

To mitigate a threat:

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



5. 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**.

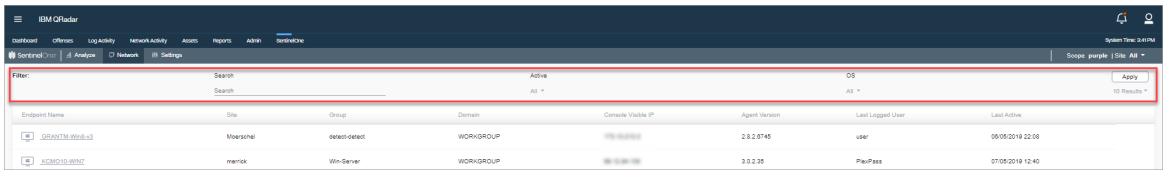
- **Un-quarantine** - Removes a file from quarantine.
- **Remediate** - (Windows and macOS) Stops processes, quarantines binaries, removes linked libraries, deletes seed files, and restores configuration of the OS, application, and user settings to the state before the attack began.
- **Rollback** -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

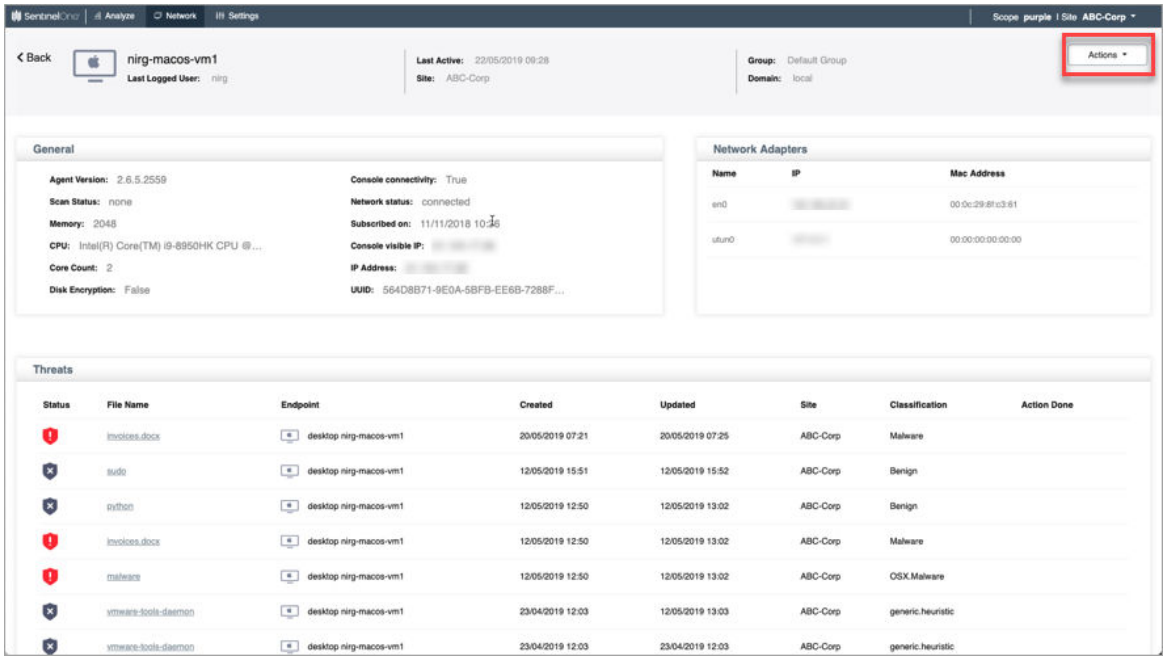
1. Click **SentinelOne > Network**.
2. Use the **Filter** and **Search** options to find specific endpoints, for example, of a specific OS.



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**.



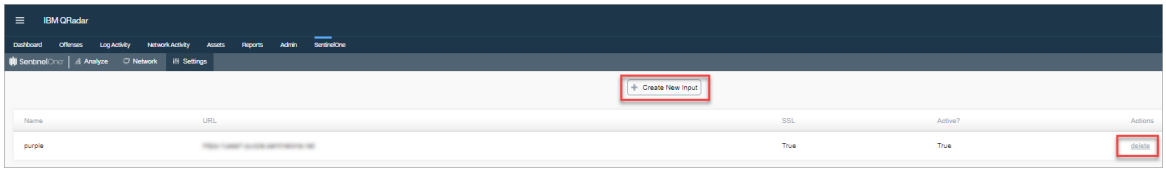
5. Select an action.

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**.



To view threats in the SentinelOne Management Console:

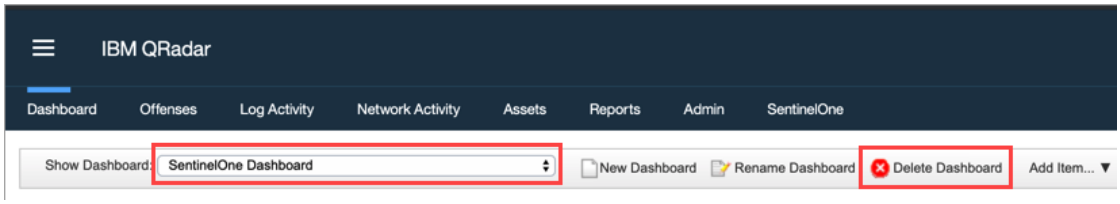
Open the SentinelOne Management Console for more features. For example: Perform more actions on endpoints, view threat attack story lines, and run administrative actions. For a video tour of the Management Console, click here.

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

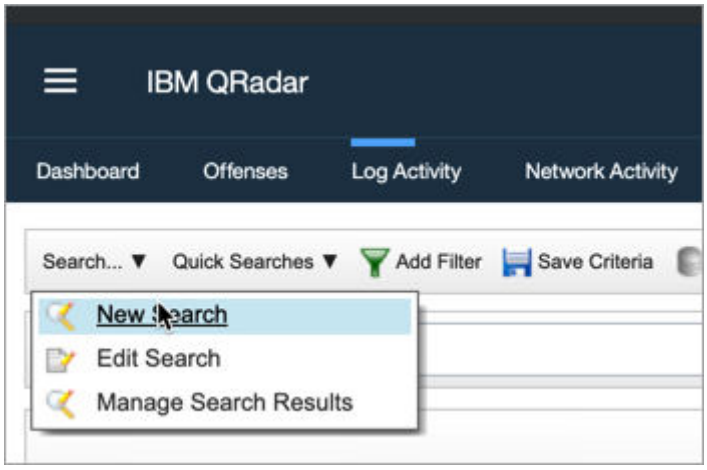
5. Upgrading From the Beta Version

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

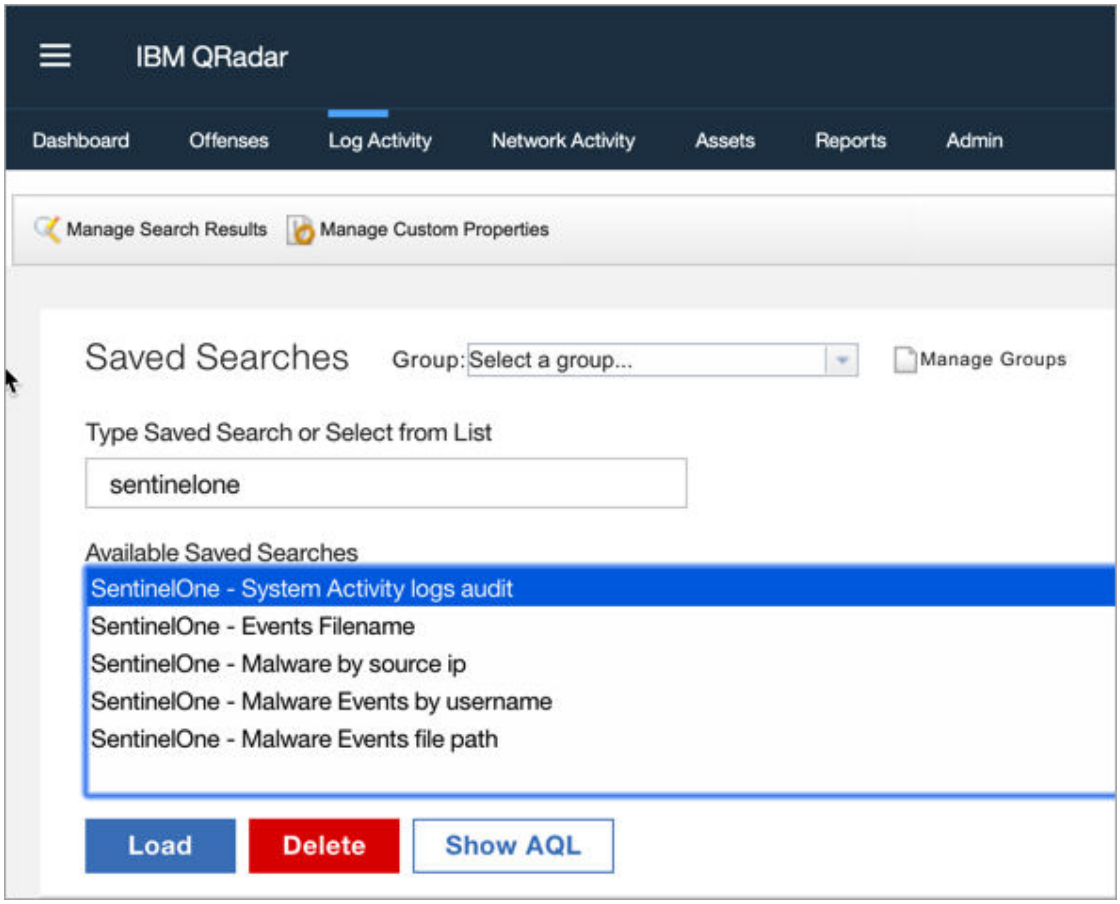
1. Uninstall the existing SentinelOne DSM.
    1. Select **Admin** from the Main menu, and click **Extensions Management**.
    2. Select the SentinelOne DSM from the list, and click **Uninstall**.
2. Uninstall the existing SentinelOne App.
    1. Select **Admin** from the Main menu, and click **Extensions 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`	**`Event Category`**
SentinelOne	The Company field is hard-coded to SentinelOne.	SentinelOne	**`SentinelOne`**
Mgmt	SentinelOne component and version.	`Mgmt`	**`S1environment`**

OS	Short name of the operating system of the endpoint.	`Windows`
		`Linux`
		`OS X`
			`S1osName`

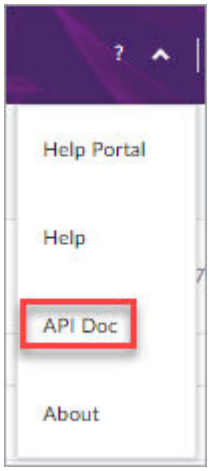
eventID	Unique ID Of the event. This is matched to the QRadar Event IDs.	*integer*	**`Event ID`**
eventName	Readable text to complement the ID and to headline the event in text.	*string*	**`EventDesc`**
eventSeverity	Threat level, according to SentinelOne intelligence, mapped to the RFC 3164 severity values.	*string*	
Details	Available on certain alerts, in standard and custom QRadar variables, for correlation when possible.	See next table	

6.2. Finding SentinelOne Events

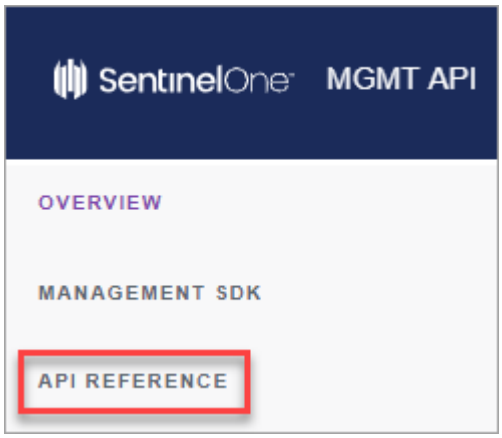
To add SentinelOne events to the QRadar logs, you need a list of the SentinelOne event names and ID numbers.

To see a complete list of SentinelOne events:

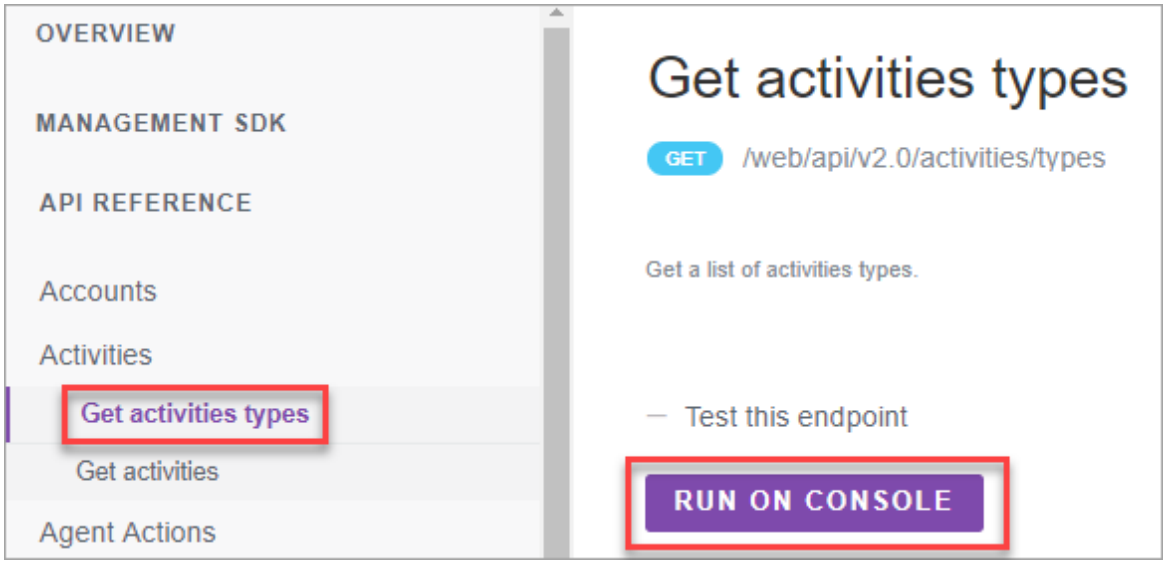
1. Open the SentinelOne Management Console.
2. Click the **Help menu > API Doc**.



3. Click **API REFERENCE**.

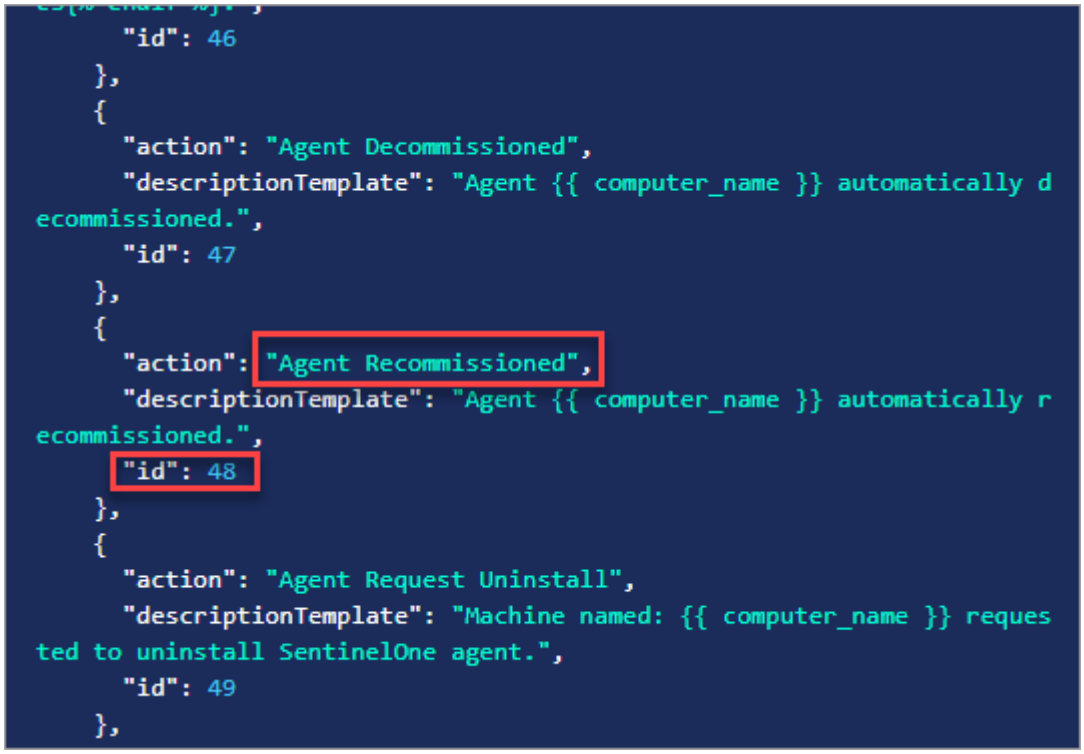


4. Click **Activities > Get activities types**.



5. Click RUN ON CONSOLE.

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



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

Email: Support@sentinelone.com