Salesforce Security Auditing

Contents

Salesforce Security Auditing

The IBM® Security QRadar® DSM for Salesforce Security Auditing can collect Salesforce Security Auditing audit trail logs that you copy from the cloud to a location that QRadar can access.

The following table identifies the specifications for the Salesforce Security Auditing DSM:

Table 1-1. Salesforce Security Auditing DSM specifications

Specification	Value
Manufacturer	Salesforce
DSM	Salesforce Security Auditing
RPM file name	DSM-SalesforceSecurityAuditing-*QRadar_Version-Build_Number*.noarch.rpm
Protocol	Log File
QRadar recorded events	Setup Audit Records
Automatically discovered	No
Includes identity	No
More information	Salesforce web site (http://www.salesforce.com/)

Salesforce Security Auditing DSM integration process

To integrate Salesforce Security Auditing DSM with QRadar, use the following procedures:

1. If automatic updates are not enabled, download and install the most recent versions of the following RPMs on your QRadar Console:
   - Log File Protocol RPM
   - Salesforce Security Auditing RPM
2. Download the Salesforce audit trail file to a remote host that QRadar can access.
3. For each instance of Salesforce Security Auditing, create a log source on the QRadar Console.

Downloading the Salesforce audit trail file

To collect Salesforce Security Auditing events, you must download the Salesforce audit trail file to a remote host that QRadar can access.

About this task

You must use this procedure each time that you want to import an updated set of audit data into QRadar. When you download the audit trail file, you can overwrite the previous audit trail CSV file. When QRadar retrieves data from the audit trail file, QRadar processes only audit records that were not imported before.

Procedure

1. Log in to your Salesforce Security Auditing server.
2. Go to the **Setup** section.
3. Click **Security Controls**.
4. Click **View Setup Audit Trail**.
5. Click **Download setup audit trail for last six months (Excel.csv file)**.
6. Copy the downloaded file to a location that QRadar can reach by using Log File Protocol.

Configuring a Salesforce Security Auditing log source in QRadar

To collect Salesforce Security Auditing events, configure a log source in QRadar.

Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. In the navigation menu, click **Data Sources**.
4. Click the **Log Sources** icon.
5. Click **Add**.
6. From the **Log Source Type** list, select **Salesforce Security Auditing**.
7. From the **Protocol Configuration** list, select **Log File**.
8. Configure the following Salesforce Security Auditing parameters:

Parameter	Description
Event Generator	RegEx Based Multiline
Start Pattern	(\d{1,2}/\d{1,2}/\d{4} \d{1,2}:\d{2}:\d{2} [APM]{2} \w+),
End Pattern	Ensure that this parameter remains empty.
Date Time RegEx	(\d{1,2}/\d{1,2}/\d{4} \d{1,2}:\d{2}:\d{2} \w{2} \w+),
Date Time Format	MM/dd/yyyy hh:mm:ss aa z

9. Configure the remaining parameters.
10. Click **Save**.
11. On the Admin tab, click **Deploy Changes**.