Bit9 Security Platform

Use the IBM® Security QRadar® SIEM DSM for Bit9 Security Platform to collect events from Bit9 Parity devices.

The following table identifies the specifications for the Bit9 Security Platform DSM:

Table 1. DSM specifications for Bit9 Security Platform

Specification	Value
Manufacturer	Bit9
DSM name	Bit9 Security Platform
RPM file name	`DSM-Bit9Parity-`*`build_number`*`.noarch.rpm`
Supported versions	V6.0.2 and up
Event format	Syslog
Supported event types	All events
Automatically discovered?	Yes
Included identity?	Yes
Technical risk?	Yes
More information	Bit9 website (http://www.bit9.com)

To integrate Bit9 Security Platform with QRadar, complete the following steps:

1. If automatic updates are not enabled, download the most recent version of the Bit9 Security Platform DSM RPM.
2. Configure your Bit9 Security Platform device to enable communication with QRadar. You must create a syslog destination and forwarding policy on the Bit9 Security Platform device.
3. If QRadar does not automatically detect Bit9 Security Platform as a log source, create a Bit9 Security Platform log source on the QRadar Console. Use the following Bit9 Security Platform values to configure the log source parameters:

Log Source Identifier	The IP address or host name of the Bit9 Security Platform device
Log Source Type	Bit9 Security Platform
Protocol Configuration	Syslog

Configuring Bit9 Security Platform to communicate with QRadar

Configure your Bit9 Security Platform device to forward events to IBM Security QRadar in LEEF format.

Procedure

1. Log in to the Bit9 Security Platform console with Administrator or PowerUser privileges.
2. From the navigation menu, select **Administration** > **System Configuration**.
3. Click **Server Status** and click **Edit**.

4. In the **Syslog address** field, type the IP address of your QRadar Console or Event Collector.
5. From the **Syslog format** list, select **LEEF (Q1Labs)**.
6. Select the **Syslog enabled** check box and click **Update**.