LOGbinder SP event collection from Microsoft SharePoint

The IBM® Security QRadar® DSM for Microsoft SharePoint can collect LOGbinder SP events.

The following table identifies the specifications for the Microsoft SharePoint DSM when the log source is configured to collect LOGbinder SP events:

Table 1. LOGbinder for Microsoft SharePoint specifications

Specification	**Value**
Manufacturer	Microsoft
DSM name	Microsoft SharePoint
RPM file name	DSM-MicrosoftSharePoint-*QRadar_version-build_number*.noarch.rpm
Supported versions	LOGbinder SP V4.0
Protocol type	Syslog
QRadar recorded event types	All events
Automatically discovered?	Yes
Included identity?	No
More information	*http://office.microsoft.com/en-sg/sharepoint/* (http://office.microsoft.com/en-sg/sharepoint/) *http://www.logbinder.com/products/logbindersp/* (http://www.logbinder.com/products/logbindersp/)

The Microsoft SharePoint DSM can collect other types of events. For more information about other Microsoft SharePoint event formats, see the Microsoft SharePoint topic in the *DSM Configuration Guide*.

To collect LOGbinder events from Microsoft SharePoint, use the following steps:

1. If automatic updates are not enabled, download the most recent version of the Microsoft SharePoint DSM RPM.
2. Configure your Microsoft SharePoint device to send LOGbinder events to QRadar.
3. If the log source is not automatically created, add a Microsoft SharePoint DSM log source on the QRadar Console. The following table describes the parameters that require specific values that are required for LOGbinder event collection:

Table 2. Microsoft SharePoint log source parameters for LOGbinder event collection

Parameter	**Value**
Log Source type	Microsoft SharePoint
Protocol Configuration	Syslog

Configuring your LOGbinder SP system to send Microsoft SharePoint event logs to QRadar

To collect Microsoft SharePoint LOGbinder events, you must configure your LOGbinder SP system to send events to IBM Security QRadar.

Procedure

1. Open the LOGbinder SP Control Panel.
2. Double-click **Output** in the Configure pane.
3. Double-click **Syslog-Generic** in the Outputs pane.
4. Select the **Send output to Syslog-Generic** check box, and then enter the IP address and port of your QRadar Console or Event Collector.
5. Click **OK**.
6. To restart the LOGbinder service, click the **Restart** icon.