LOGbinder EX event collection from Microsoft Exchange Server

The IBM® Security QRadar® DSM for Microsoft Exchange Server can collect LOGbinder V3.5 events.

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

Table 1. LOGbinder for Microsoft Exchange Server

Specification	Value
Manufacturer	Microsoft
DSM name	Exchange Server
RPM file name	DSM-MicrosoftExchange-*QRadar_version-build_number*.noarch.rpm
Supported versions	LOGbinder EX V2.0
Protocol type	Syslog
QRadar recorded event types	Admin Mailbox
Automatically discovered?	Yes
Included identity?	No
More information	Microsoft Exchange website (http://www.office.microsoft.com/en-us/exchange/)

The Microsoft Exchange Server DSM can collect other types of events. For more information on how to configure for other Microsoft Exchange Server event formats, see the *DSM Configuration Guide* that this addendum supplements.

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

1. If automatic updates are not enabled, download the most recent version of the Microsoft Exchange Server DSM RPM.
2. Configure your Microsoft Exchange Server device to send LOGbinder events to QRadar.
3. If the log source is not automatically created, add a Microsoft Exchange Server 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 Exchange Server log source parameters for LOGbinder event collection

Parameter	Value
Log Source type	Microsoft Exchange Server
Protocol Configuration	Syslog

Configuring your LOGbinder EX system to send Microsoft Exchange event logs to QRadar

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

Procedure

1. Open the LOGbinder EX 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.