Trend Micro Deep Discovery Analyzer

The Trend Micro Deep Discovery Analyzer DSM for IBM® Security QRadar® can collect event logs from your Trend Micro Deep Discovery Analyzer console.

The following table identifies the specifications for the Trend Micro Deep Discovery Analyzer DSM:

Table 1. Trend Micro Deep Discovery Analyzer DSM specifications

Specification	**Value**
Manufacturer	Trend Micro
DSM name	Deep Discovery Analyzer
RPM file name	DSM-TrendMicroDeepDiscoveryAnalyzer-*build_number*.noarch.rpm
Supported versions	1.0
Event format	LEEF
QRadar recorded event types	All events
Automatically discovered?	Yes
Included identity?	No
More information	Trend Micro website (www.trendmicro.com/DeepDiscovery⌂)

To integrate Trend Micro Deep Discovery with QRadar, use the following steps:

1. If automatic updates are not enabled, download the most recent versions of the following RPMs.
   - DSMCommon
   - Trend Micro Deep Discovery DSM
2. Configure your Trend Micro Deep Discovery device to enable communication with QRadar.
3. If QRadar does not automatically detect Trend Micro Deep Discovery as a log source, create a Trend Micro Deep Discovery log source on the QRadar Console.

Configuring your Trend Micro Deep Discovery Analyzer instance for communication with QRadar

To collect Trend Micro Deep Discovery Analyzer events, configure your third-party instance to enable logging.

Procedure

1. Log in to the Deep Discovery Analyzer web console.
2. Click **Administrator** > **Log Settings**.
3. Select **Forward logs to a syslog server**.
4. Select **LEEF** as the log format.
5. In the **Syslog server** field, type the IP address of your QRadar Console or Event Collector.

6. In the **Port** field, type 514.

Adding a Trend Micro Deep Discovery Analyzer log source on your QRadar Console

Use this procedure if your QRadar Console did not automatically discover the Trend Micro Deep Discovery Analyzer log source.

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. In the **Log Source Identifier** field, type the IP address or host name of the Trend Micro Deep Discovery Analyzer device.
7. From the **Log Source Type** list, select **Trend Micro Deep Discovery Analyzer**.
8. From the **Protocol Configuration** list, select **Syslog**.
9. Configure the remaining parameters.
10. Click **Save**.