106 Open Source SNORT

The Open Source SNORT DSM for IBM Security QRadar records all relevant SNORT events using syslog.

The SourceFire VRT certified rules for registered SNORT users are supported. Rule sets for Bleeding Edge, Emerging Threat, and other vendor rule sets might not be fully supported by the Open Source SNORT DSM.

Configuring Open Source SNORT

To configure syslog on an Open Source SNORT device:

About this task

The following procedure applies to a system that runs Red Hat Enterprise. The following procedures can vary for other operating systems.

Procedure

1. Configure SNORT on a remote system.
2. Open the `snort.conf` file.
3. Uncomment the following line:

   ```
   output alert_syslog:LOG_AUTH LOG_INFO
   ```
4. Save and exit the file.
5. Open the following file:

   ```
   /etc/init.d/snortd
   ```
6. Add a `-s` to the following lines, as shown in the example:

   ```
   daemon /usr/sbin/snort $ALERTMODE
   $BINARY_LOG $NO PACKET_LOG $DUMP_APP -D
   $PRINT_INTERFACE -i $i -s -u $USER -g
   $GROUP $CONF -i $LOGIR/$i $PASS_FIRST
   ```

   ```
   daemon /usr/sbin/snort $ALERTMODE
   $BINARY_LOG $NO_PACKET_LOG $DUMP_APP -D
   $PRINT_INTERFACE $INTERFACE -s -u $USER -g
   $GROUP $CONF -i $LOGDIR
   ```
7. Save and exit the file.
8. Restart SNORT by typing the following command:

   ```
   /etc/init.d/snortd restart
   ```
9. Open the `syslog.conf` file.
10. Update the file to reflect the following code:

    ```
    auth.info@<IP Address>
    ```

    Where *<IP Address>* is the system to which you want logs sent.
11. Save and exit the file.
12. Restart syslog:

    ```
    /etc/init.d/syslog restart
    ```

What to do next

You can now configure the log source in QRadar.

Configuring a log source

IBM Security QRadar automatically discovers and creates log sources for Open Source SNORT syslog events.

About this task

The following configuration steps are optional.

To create a log source in QRadar:

Procedure

1. Log in to QRadar.
2. Click the **Admin** tab.
3. On the navigation menu, click **Data Sources**.
   The Data Sources pane is displayed.
4. Click the **Log Sources** icon.
   The Log Sources window is displayed.
5. Click **Add**.
   The Add a log source window is displayed.
6. In the **Log Source Name** field, type a name for your log source.
7. In the **Log Source Description** field, type a description for the log source.
8. From the **Log Source Type** list, select **Open Source IDS**.
9. Using the **Protocol Configuration** list, select **Syslog**.
   The syslog protocol configuration is displayed.
10. Configure the following values:

Table 405. Syslog parameters

Parameter	Description
Log Source Identifier	Type the IP address or host name for the log source as an identifier for your Open Source SNORT events.

11. Click **Save**.
12. On the **Admin** tab, click **Deploy Changes**.
    The configuration is complete.
    For more information about SNORT, see the SNORT documentation at http://www.snort.org/docs/.