CYLANCE

QRadar Log Source Extension

install and configuration of LSX file for Cylance

Table of Contents

Table of Figures

No table of figures entries found.

List of Tables

No table of figures entries found.

Overview

This document is intended to provide install directions and use of the QRadar Log Source Extension file designed for Cylance syslog events.

Uploading the LSX File

The following steps provide instruction for uploading the custom LSX file into the QRadar environment.

Uploading the LSX

1. From the **Admin** tab, click the icon labeled **Log Source Extension**, a new window will open
2. Click **Add** in the top-left corner to add a new **LSX**
3. Assign the **LSX** a name, **CylancePROTECT**
4. Select the **Use Condition** as **Parsing Override**
5. Do **NOT** set the **LSX** as the default for a **Log Source Type**
6. Browse to the **LSX** provided by Cylance and click **Upload**, if there are no errors in the LSX file, it will be uploaded to QRadar
7. Click **Save** and close the window

Setting Up Log Source in QRadar

The following steps need to be followed to setup the Log Source for Cylance:

1. From the **Admin** tab, create a new source using the **Log Sources** icon
2. Specify the **Log Source Name**
3. Specify **Log Source Type** as **Universal DSM**
4. Specify the protocol that will be used for **Protocol Configuration**. This should be set to **Syslog**
5. Enter the IP Address or Hostname of the log source as the **Log Source Identifier**, this should be set to 52.88.241.49 or 52.2.154.63
6. Choose your **Target Event Collector** for the Collector which is setup in the Cylance Console to forward events
7. Set **Coalescing Events** to **No**
8. Set the **Log Source Extension** to **CylancePROTECT**
9. Set the **Extension Use Condition** to **Parsing Override**
10. Click **Save** to save the new log source
11. Close the window
12. Click **Deploy Changes** from the **Admin** tab

Cylance Professional Services

Cylance Professional Services complement PROTECT in empowering corporate IT to better protect their organization and reduce the attack surface. Vulnerability and penetration testing establish a baseline security posture. A compromise assessment determines the **who**, **what**, **when** and **how** of a successful attack and provides best practices for remediation. Our incident response and customized services fix problems much faster and in a less intrusive manner than alternative approaches. Alert management and whitelisting services help IT organizations achieve a higher degree of security WITHOUT the hassle of continuous management overhead, productivity impact on users and the mistakes that can be made when pressed to quickly make decisions about the safety of applications.