



CYBER**ARK**[®]

Integration with Rapid7

Implementation Guide



About Rapid7

Rapid7 InsightIDR is your cloud SIEM for modern threat detection & response. It unifies your data with simple, cloud-based data collection, detects common and targeted attacks, and gives your team the context and power to take action.

This guide describes how to configure CyberArk Enterprise Password Vault (EPV) and Privileged Threat Analytics (PTA) to send syslog messages to Rapid7 InsightIDR, and how to configure Rapid7 to be able to receive and process these messages.

The guide is based on CyberArk EPV Version 9.95, CyberArk PTA Version 3.6 and Rapid7 InsightIDR (SaaS delivery).

CyberArk PTA – Rapid7 Integration

PTA is able to send detected incidents as syslog messages to a SIEM tool. This section describes how to configure PTA alerts into Rapid7's cloud SIEM.

When PTA detects an event, it sends a syslog record to InsightIDR in real time, in a CEF/LEEF format. The Syslog integration is controlled by **syslog_outbound** parameter in the PTA **systemparm.properties** file, located in **/opt/tomcat/diamond-resources/local/**.

Configure CyberArk PTA to send incidents to Rapid7 InsightIDR:

1. Log on to PTA as root.
2. Open **/opt/tomcat/diamond-resources/local/systemparm.properties**, and add the following line:

```
syslog_outbound=[{"host": "<ip of Rapid7 server>", "port": <port of your choosing>,  
"format": "CEF", "protocol": "UDP", "siem": "HP ArcSight"}]
```

3. Save the configuration file and close it.
4. Restart PTA.

Configure Rapid7 to receive alerts from CyberArk PTA:

1. From your InsightIDR main dashboard, select **Data Collection** from the left hand menu.
2. When the Data Collection page appears, click the **Setup Event Source** dropdown and choose **Add Event Source**.
3. From the “Raw Data” section, click the **Custom Logs** icon. The “Add Event Source” panel appears.
4. Choose your collector and the “Rapid7 Raw Data” event source. You can also name your event source if you want.
5. Choose the [timezone](#) that matches the location of your event source logs.
6. Under **Collection Method**, choose **Listen for Syslog**
7. Enter the same port that you configured in **/opt/tomcat/diamond-resources/local/systemparm.properties** for CyberArk PTA
8. Select UDP.
9. Click **Save**.

CyberArk EPV – Rapid7 Integration

CyberArk EPV can send audit logs to Rapid7 through the Syslog protocol, giving you a complete, audit-ready view into privileged account activities from within InsightIDR.

These audit logs include privileged users, accounts, and safes activities, which are reported by the Vault to Rapid7.

Benefits of the integration include:

- Multi-layer correlation between log data and alerts from PTA, to allow clients to perform in depth analysis.
- Behavioral analysis identifying suspicious privileged user activity.
- Scores to particular threat – so that customers can decide which incident poses the biggest threat.
- PTA alerts to be included in dashboards and reporting.
- PTA alerts will appear in your broader InsightIDR detections and investigation workflow.

Forward of Syslog is controlled by the following parameters in **DBParm.ini**.

For complete instructions about configuring Syslog servers, **see Integrating with SIEM Applications** in the *Privileged Account Security Implementation Guide*.

Configure the CyberArk Vault to forward events to Rapid7:

1. Navigate to your CyberArk installation folders to grab the standard translator (by default, the location is **C:\Program Files (x86)\PrivateArk\Server\Syslog**). Make a copy of it, name it **“Rapid7.xml”**, and reference it in the **SyslogTranslatorFile** parameter in the **DBPARM.ini** file (see step 2).
2. In the same server installation folder (the default is **C:\Program Files (x86)\PrivateArk\Server**), open **DBPARM.ini**, and add the following lines:

```
[SYSLOG]
SyslogServerIP=<ip of Rapid7 server>
SyslogServerProtocol=UDP
SyslogServerPort=<port of your choosing>
SyslogMessageCodeFilter=295,308,7,24,31,428,361,372,373,359,436,412,411,300,302,294,42
7,57,416,385,386,471,472
SyslogTranslatorFile=Syslog\Rapid7.xml
UseLegacySyslogFormat=no
```

3. Save the file and close it.
4. Restart the Vault, and start the PrivateArk Server Service.

Configure Rapid7 to receive CyberArk Vault events:

1. From your InsightIDR main dashboard, select **Data Collection** from the left hand menu.
2. When the Data Collection page appears, click the **Setup Event Source** dropdown and choose **Add Event Source**.
3. From the “Raw Data” section, click the **Custom Logs** icon. The “Add Event Source” panel appears.
4. Choose your collector and the “Rapid7 Raw Data” event source. You can also name your event source if you want.
5. Choose the [timezone](#) that matches the location of your event source logs.
6. Under **Collection Method**, choose **Listen for Syslog**.
7. Enter the same port that you configured in **dbparm.ini** for **CyberArk Vault**.
8. Select UDP.

9. Click **Save**.

Once CyberArk EPV data starts flowing into InsightIDR, logs will be automatically structured for easy searching, visualizations, and custom alerts.

The screenshot shows the InsightIDR Log Search interface. The search bar contains the query `device.vendor: \"cyberark\"`. The results show two log entries. The first entry is from May 20, 2019, at 13:21:04.758, with a severity of 4. The second entry is from May 20, 2019, at 13:21:29.235, with a severity of 2. Both entries are from the device `18.8.1.38` and are related to the user `\"\"`. The log entries are displayed in a structured format, showing fields like `device.vendor`, `device.product`, `device.version`, `device.event_classification`, `name`, `severity`, `extension`, `host`, `device.customer_label`, `device.customer_label1`, `device.customer_label2`, `device.customer_label3`, `device.customer_label4`, `device.customer_label5`, `device.customer_label6`, `device.customer_label7`, `device.customer_label8`, `device.customer_label9`, `device.customer_label10`, `device.customer_label11`, `device.customer_label12`, `device.customer_label13`, `device.customer_label14`, `device.customer_label15`, `device.customer_label16`, `device.customer_label17`, `device.customer_label18`, `device.customer_label19`, `device.customer_label20`, `device.customer_label21`, `device.customer_label22`, `device.customer_label23`, `device.customer_label24`, `device.customer_label25`, `device.customer_label26`, `device.customer_label27`, `device.customer_label28`, `device.customer_label29`, `device.customer_label30`, `device.customer_label31`, `device.customer_label32`, `device.customer_label33`, `device.customer_label34`, `device.customer_label35`, `device.customer_label36`, `device.customer_label37`, `device.customer_label38`, `device.customer_label39`, `device.customer_label40`, `device.customer_label41`, `device.customer_label42`, `device.customer_label43`, `device.customer_label44`, `device.customer_label45`, `device.customer_label46`, `device.customer_label47`, `device.customer_label48`, `device.customer_label49`, `device.customer_label50`, `device.customer_label51`, `device.customer_label52`, `device.customer_label53`, `device.customer_label54`, `device.customer_label55`, `device.customer_label56`, `device.customer_label57`, `device.customer_label58`, `device.customer_label59`, `device.customer_label60`, `device.customer_label61`, `device.customer_label62`, `device.customer_label63`, `device.customer_label64`, `device.customer_label65`, `device.customer_label66`, `device.customer_label67`, `device.customer_label68`, `device.customer_label69`, `device.customer_label70`, `device.customer_label71`, `device.customer_label72`, `device.customer_label73`, `device.customer_label74`, `device.customer_label75`, `device.customer_label76`, `device.customer_label77`, `device.customer_label78`, `device.customer_label79`, `device.customer_label80`, `device.customer_label81`, `device.customer_label82`, `device.customer_label83`, `device.customer_label84`, `device.customer_label85`, `device.customer_label86`, `device.customer_label87`, `device.customer_label88`, `device.customer_label89`, `device.customer_label90`, `device.customer_label91`, `device.customer_label92`, `device.customer_label93`, `device.customer_label94`, `device.customer_label95`, `device.customer_label96`, `device.customer_label97`, `device.customer_label98`, `device.customer_label99`, `device.customer_label100`.

In InsightIDR Dashboards, you can easily visualize your privileged access security data.

