



PAM Administration

Privileged Session Management Part 2



Agenda

Upon completion of this session, the participant will be able to:

- Monitor and manage privileged session **recordings**
- Monitor and manage privileged session **audits**
- Monitor and manage **active privileged sessions**



Recordings

In this section we will discuss how to enable, monitor and manage privileged session recordings



Recordings

- The **PSM** and **PSM for SSH** create video and text recordings for privileged sessions and store them in the **Vault** where they can be viewed at any time by authorized users
- You can store **PSM** video and text recordings in an external storage device

The screenshot displays the CyberArk Monitoring dashboard. On the left is a vertical sidebar with icons for various functions. The main area is titled 'Monitoring' and includes a 'Filter' button and a user profile 'cindy' with the last sign-in date '8/26/2021'. Below this is a 'Filters' section with tabs for 'Sessions properties' and 'Sessions activities'. It features date and time pickers for 'From' and 'To' ranges, with an 'Apply' button. The 'Recordings' tab is active, showing 'Active sessions' with 27 results. A table lists session details, and each row has a 'Play' button for viewing the recording.

Monitoring Last sign in: 8/26/2021 | cindy

Filter

Filters

Sessions properties Sessions activities

From To

08/24/2021 12:00 AM 08/26/2021 11:59 PM

Today

Apply

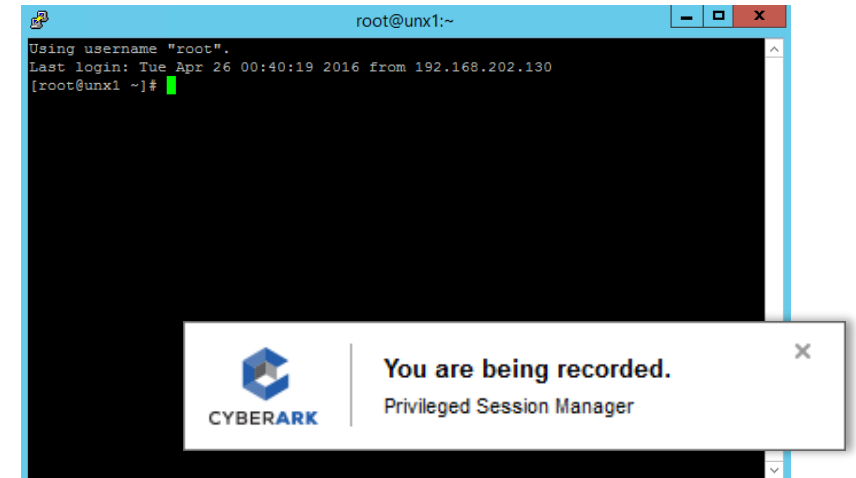
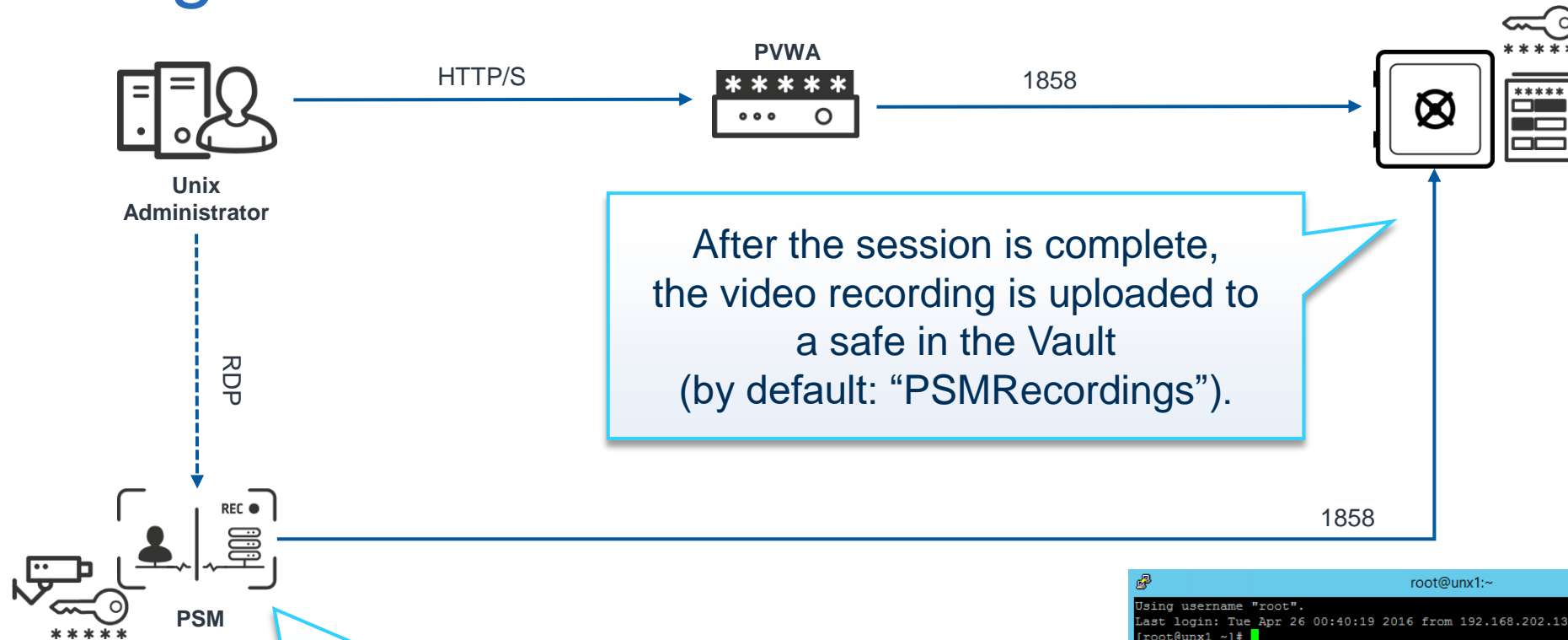
Recordings » Active sessions

27 results for: From: 8/24/2021 12:00 AM , To: 8/26/2021 11:59 PM [Clear all filters](#) [Additional details & actions in classic interface](#)


Risk ↓	User	Client	Account User Name	Account Address	Account Policy ID	Start	
80	paul	SSH	root02	target-lin	LINSSH30	8/24/2021 07:34 AM	Play
80	john	RDP	localadmin01	target-win.acme.corp	WINSRVCLCLADM45	8/24/2021 07:54 AM	Play



Recordings



Enable Recordings: Master Policy





POLICIES


Master Policy


Policy by Platform


Access Control (Safes)























CYBERARK

Policies > Master Policy

Master Policy ?

▼ Privileged Access Workflows

Policy Rule	Value	Exceptions
Require dual control password access approval	-	-
Enforce check-in/check-out exclusive access	-	-
Enforce one-time password access	-	-
Allow EPV transparent connections ('Click to connect')	Active	-
Require users to specify reason for access	-	-

▼ Password Management


Policy Rule	Value	Exceptions
Require password change every X days	60	5
Require password verification every X days	7	-

▼ Session Management

Policy Rule	Value	Exceptions
Require privileged session monitoring and isolation	Active	-
Record and save session activity	Active	-

▼ Audit

Policy Rule	Value	Exceptions
Activities audit retention period	90	-

Last sign in: 8/26/2021 |  mike ▾

Overview

Introduction to Policy Management

The Master Policy allows you to easily define a corporate level policy that reflects the business goals and guidelines for managing privileged accounts and sessions across your entire organization.

Using policy exceptions, you can define different policy behavior for specific platforms that require different workflows or policies to those defined in the Master Policy. The Master Policy also allows you to measure how well the corporate policy is adhered to and easily view the gaps.

To view or define the Master Policy behavior, select a policy rule to view its current related settings.

Activate Windows
Go to Settings to activate Windows.

Enable session recording in the Master Policy for all platforms or for specific platforms by use of exceptions



View Recordings in the PSM

Member of the Auditors group

The screenshot displays the CyberArk PSM Monitoring interface. The top header bar is grey and contains the 'Monitoring' title, a user icon, and the text 'Last sign in: 8/26/2021 | cindy'. Below the header, a session title 'paul as root02 on target-lin' is shown with a timestamp '8.24.2021 07:34 AM - 8.24.2021 07:42 AM'. A left sidebar contains various icons for navigation. The main area shows a timeline for 'Aug 24 Tuesday' with a single event at '7:34:27 AM' labeled 'passwd'. To the right, a terminal window titled 'root@target-lin:~' displays the following text:

```
root@target-lin:~  
Using username "root02".  
Last login: Tue Aug 24 07:25:35 2021 from components.acme.corp  
[root@target-lin ~]#  
[root@target-lin ~]#
```

At the bottom right of the interface, there is a message: 'Activate Windows Go to Settings to activate Windows.'



Monitor Recordings (PSM for SSH)

- Recordings created by **PSM for SSH** are currently displayed in the classic interface

The screenshot displays the CyberArk PSM for SSH interface. The top navigation bar includes icons for Back, Search, Save Text, Play, Protect, and Refresh. The user 'cindy' is logged in, with the last sign-in on 8/26/2021. The main heading is 'Recording details: carlos-LINSSH30-logon01-10.0.0.20-2021/08/24 06:35:40 AM-2021/08/24 06:36:21 AM'.

Account Details:

- User: carlos
- From IP: 10.0.20.1
- Remote machine: 10.0.0.20
- Interface: PSM
- Client: PSMP-SSH
- Protocol: SSH
- Start: 8/24/2021 6:35:40 AM
- End: 8/24/2021 6:36:21 AM
- Duration: 00:00:41
- Safe: PSMRecordings
- Locked By:

Text Recording:

- Size: 3KB
- Last Reviewed By:
- Last Review Date:

Security Incidents:

The Session has not triggered security incidents in Privileged Threat Analytics (PTA)

Risk Score:

Highest Risk Activity:

Activity Offset:

Events:

Offset	Action
00:00:32	pwd
00:00:37	ls -al
00:00:40	exit

A terminal window titled 'carlos-LINSSH30-logon01-10.0.0.20-2021/08/24 06:35:40 AM-2021/08/24 06:36:21 AM' is overlaid on the interface, showing the following output:

```
total 44
drwx----- 4 logon01 logon01 4096 Aug 24 01:40 .
drwxr-xr-x. 441 root root 16384 Oct 29 2020 ..
-rw----- 1 logon01 logon01 94 Aug 24 06:11 .bash_history
-rw-r--r-- 1 logon01 logon01 18 Jul 18 2013 .bash_logout
-rw-r--r-- 1 logon01 logon01 176 Jul 18 2013 .bash_profile
-rw-r--r-- 1 logon01 logon01 124 Jul 18 2013 .bashrc
drwxr-xr-x. 3 logon01 logon01 4096 Aug 24 01:40 .gnome2
drwxr-xr-x. 4 logon01 logon01 4096 Jul 23 2014 .mozilla
[logon01@target-lin ~]$ ex
```

The bottom of the interface shows a 'Page' indicator and a 'Displaying events 1 - 3 of 3' message.



Manage Recordings



Sizing Calculations for the PSM Server

$$(S_{PSM}) = (C_{session})(t_{session})(R_{session\ recording}) + 20GB$$

SPSM = Required storage on PSM Server

Csession = Maximum Number of Concurrent Sessions

tsession = Average length of recorded session

Rsession recording = Average bit rate of recorded video

- 100 KB/min – average SSH session
- 200 KB/min – average low activity RDP session
- 300 KB/min – average high activity RDP session with rich wallpaper

$$(25\text{ sessions}) \times (180\text{ minutes/session}) \times (300\text{ KB/minute}) + 20GB = 21.35GB$$



Sizing Calculations for the Vault Server

$$(S_{Vault}) = (t_{retention})(N_{session})(t_{session})(R_{session\ recording}) + 20GB$$

SVault = Required storage on Vault Server

tretention = Retention history requirement

Nsession = Average number of recorded sessions per day

tsession = Average length of recorded session

Rsession recording = Average bit rate of recorded video

- 100 KB/min – average SSH session
- 200 KB/min – average low activity RDP session
- 300 KB/min – average high activity RDP session with rich wallpaper

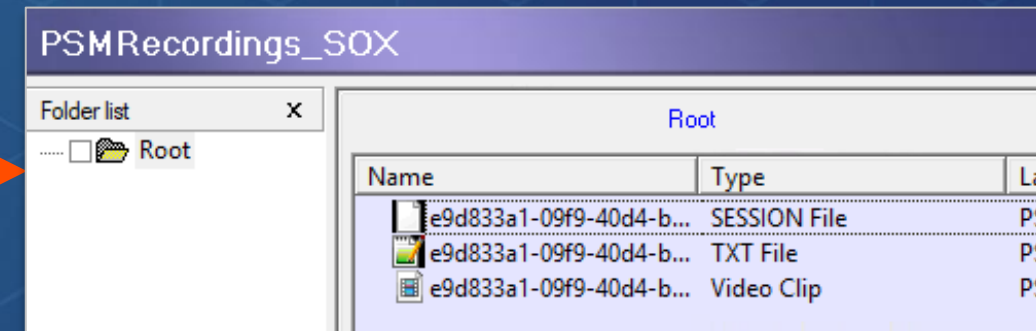
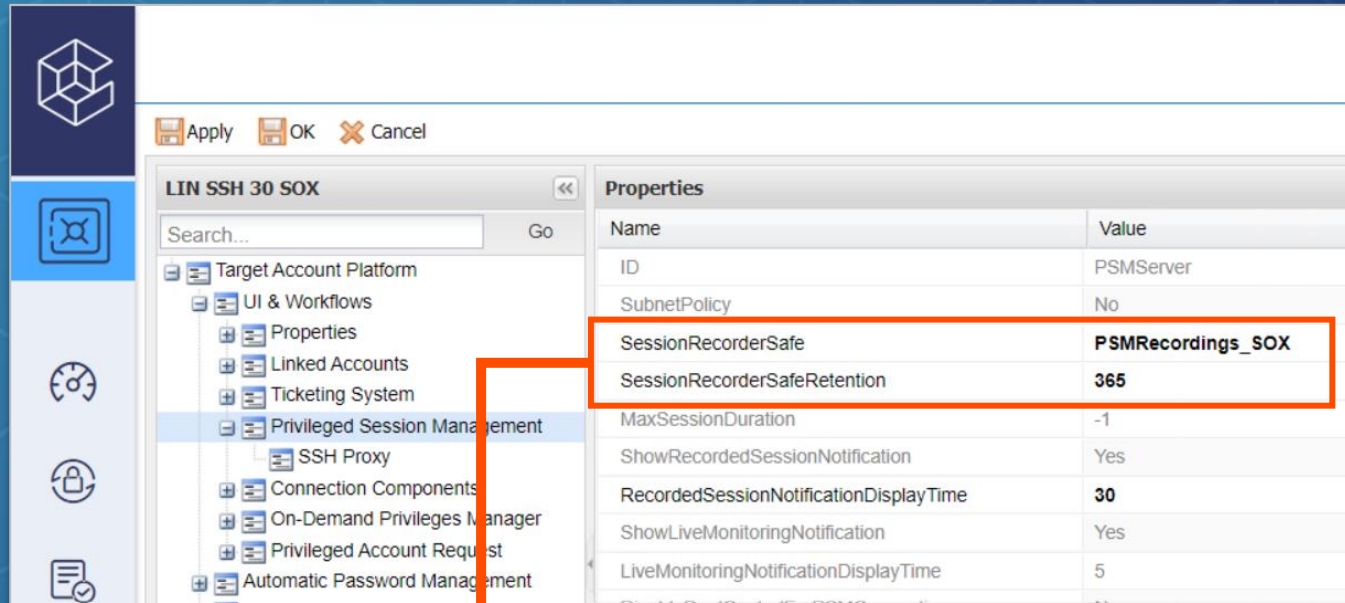
$$(90\text{ days}) \times (400\text{ sessions/day}) \times (180\text{ minutes/session}) \times (300\text{ KB/minute}) + 20GB = 1.96\text{ TB}$$



PSM Recording Safes

Recordings are stored by default in a safe called:
PSMRecordings

- Custom recording safes can be defined at the platform level
- The safes are created automatically by the **PSM** when it uploads the first recording to the **Vault**
- For example, a separate recordings safe for SOX-compliant Linux accounts (365 days retention period)



PSM Recording Safes

- Members of the **Auditors** group are automatically granted permissions on all Recording Safes
- You can also manually set different auditors for each Recording Safe according to their access control policy

Safe Details: PSMRecordings_SOX

Back Refresh

Name: PSMRecordings_SOX
Description: Object level access is enabled
Auto-purge is enabled
Saved accounts: Account versions from the last 365 days

Members											
Add Member											
User Name	Use	Retri...	List	Add	Upd...	Upd...	CPM	Ren...	Delete	Unlock	Man...
Auditors	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Backup Users	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Batch	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
DR Users	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Master	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Notification ...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Operators	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PSMApp_CO...	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PSMAppUsers	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
PSMMaster	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

☐ Hide predefined users and groups



Session Audits

In this section we will discuss how to monitor privileged session audits



Session Audit

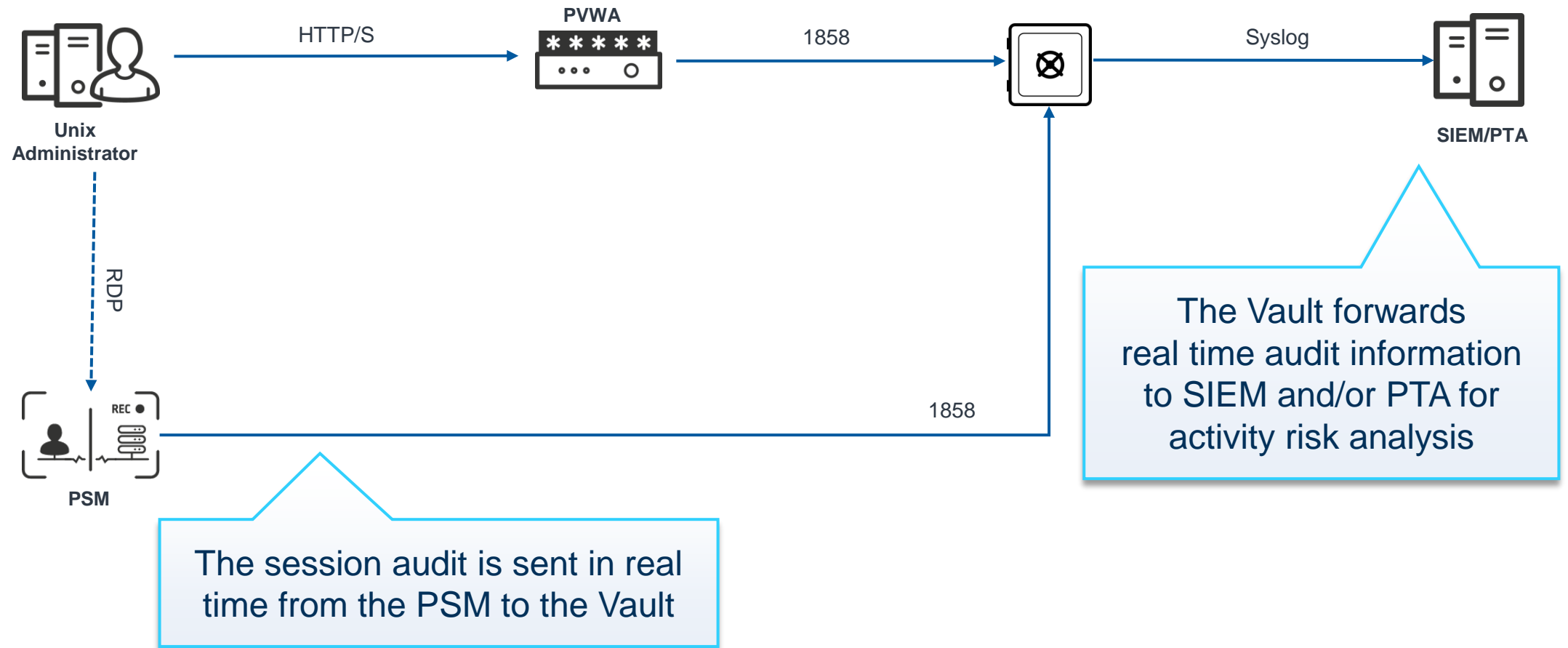
- By default, the **PSM** records all the activities that take place during privileged sessions and provides audit data for the following events:
 - SQL commands
 - SSH keystrokes
 - Window titles
 - Universal keystrokes
- **PSM for SSH** can create audit records for activities that are performed during SSH, SCP, and Telnet connections

The screenshot displays the 'Monitoring' dashboard. On the left, a sidebar contains navigation icons. The main area is divided into 'Recordings' and 'Active sessions' tabs. Under 'Recordings', a table lists 27 results for a specific time range. Two rows are highlighted with a red box, showing a risk score of 80 for users 'paul' and 'john'. The 'john' row is selected, leading to a detailed view on the right. This view shows session information for 'john' connecting to '101 on target-win.acme.corp'. A red box highlights a 'Session risk score' of 80, labeled 'HIGH', with the description 'Strongest impact activity/event [8/24/2021 07:59 AM] New User'. Below this, a timeline shows activities like 'explorer.exe, Program Manager' and 'mmc.exe, Computer Management'.

When integrated with the PTA, the suspicious activity risk score is also available in the Monitoring pane, allowing the auditing team to prioritize session auditing based on risk



Audit



Active Session Monitoring

In this section we will discuss how to monitor and manage active privileged sessions



Active Session Monitoring (PSM)

- The **PSM** enables authorized users to monitor active sessions, take part in controlling these sessions, and suspend or terminate them
- The **PSM** can also automatically suspend or terminate sessions when notified by **PTA** or a third-party threat analytics tool

The screenshot displays the 'Monitoring' interface. On the left is a sidebar with icons for various functions. The main area is divided into two sections. The top section shows a table of active sessions with one result for user 'john' and a risk score of 80. The bottom section provides details for this session, including the connection information 'john connected as localadmin01 on target-win.acme.corp', start time '8/26/2021 07:08 AM', and duration '00:00:54'. A red box highlights the 'Terminate', 'Suspend', 'Resume', and 'Monitor' buttons. Below this, a 'Session risk score' of 80 (HIGH) is shown, along with the activity 'New User'. A timeline of activities is also visible, showing 'explorer.exe, Program Manager' and 'mmc.exe, Computer Management'.

Risk	User	Monitor
80	john	Monitor

john connected as localadmin01 on target-win.acme.corp
Start: 8/26/2021 07:08 AM Duration: 00:00:54

Additional details & actions in classic interface

Terminate Suspend Resume Monitor

Session risk score
80 HIGH
Strongest impact activity/event [8/26/2021 07:08 AM] New User

3 Activities in the session

Aug 26 Today

7:08:16 AM explorer.exe, Program Manager

7:08:46 AM mmc.exe, Computer Management



Active Session Monitoring (PSM for SSH)

While it is not possible to monitor or control live **PSM for SSH** sessions, it is possible to view the live session audit

The screenshot displays the CyberArk Monitoring interface. On the left is a navigation sidebar with icons for various security functions. The main content area is titled "Monitoring" and includes a "Filter" button. Below this, there are tabs for "Recordings" and "Active sessions", with the latter being selected and highlighted by a red box. A table shows one result for the active sessions, with a risk score of 90 and the user "mike". To the right of the table, a summary box indicates "mike connected as root03 on target-lin" with a start time of 2/7/2022 04:26 PM and a duration of 00:00:55. Below this, there are tabs for "Activities" and "Details", with "Activities" selected and highlighted by a red box. A red box highlights a "Session risk score" of 90 (HIGH) with the text "Strongest impact activity/event [2/7/2022 04:27 PM] passwd mike". Below the risk score, a timeline shows two activities in the session: "useradd mike" at 4:27:05 PM and "passwd mike" at 4:27:12 PM. The interface also shows the user "cindy" in the top right corner and a "Last sign in: 2/7/2022" timestamp.

Monitoring

Filter

Recordings **Active sessions**

1 results for: From: 2/5/2022 12:00 AM... × Clear all filters

Risk	User
90	mike

mike connected as root03 on target-lin

Start: 2/7/2022 04:26 PM Duration: 00:00:55

Activities Details

● 90 HIGH Session risk score
Strongest impact activity/event [2/7/2022 04:27 PM] passwd mike

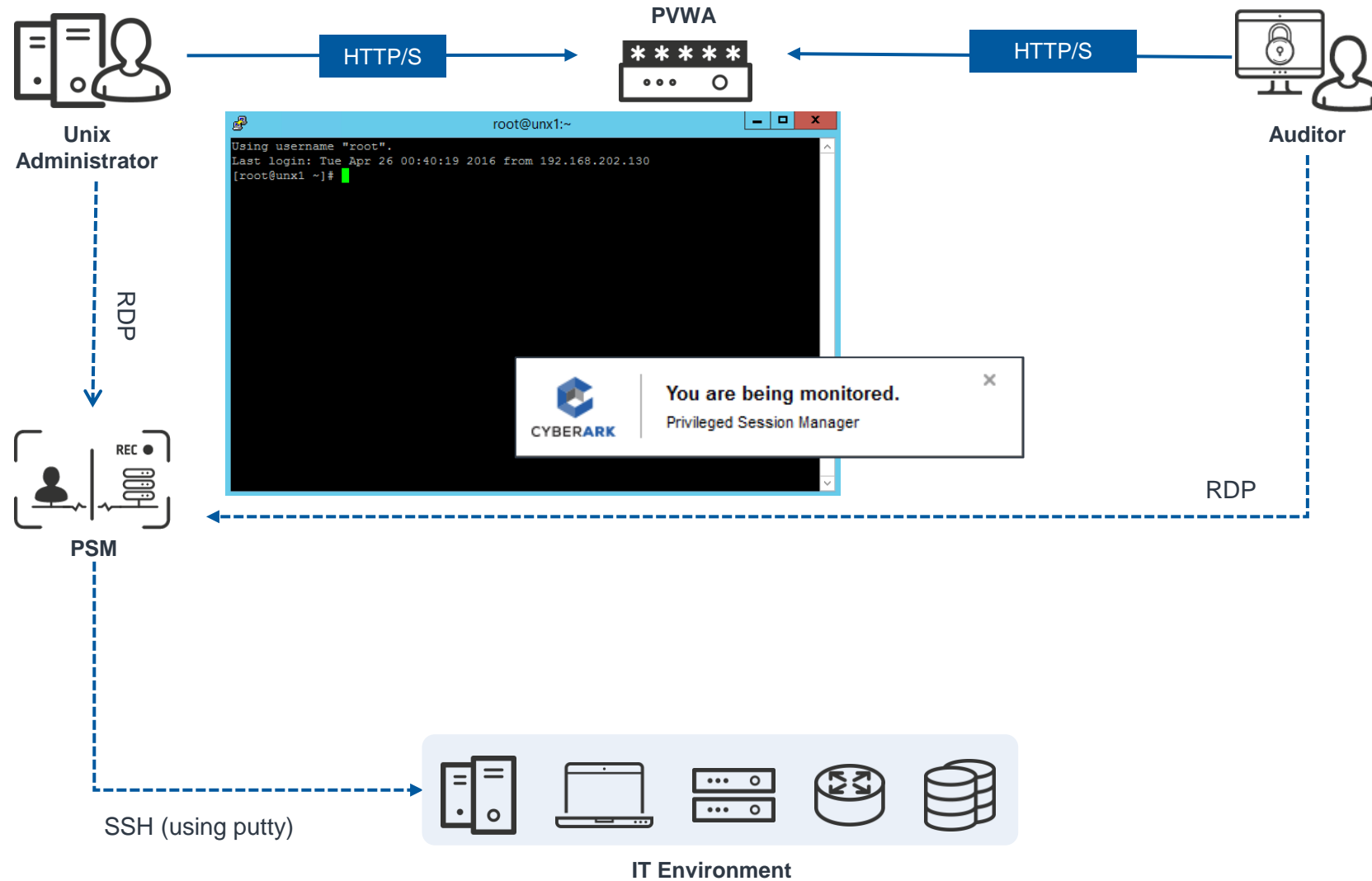
2 Activities in the session

Feb 07 Today

- 4:27:05 PM useradd mike
- 4:27:12 PM passwd mike

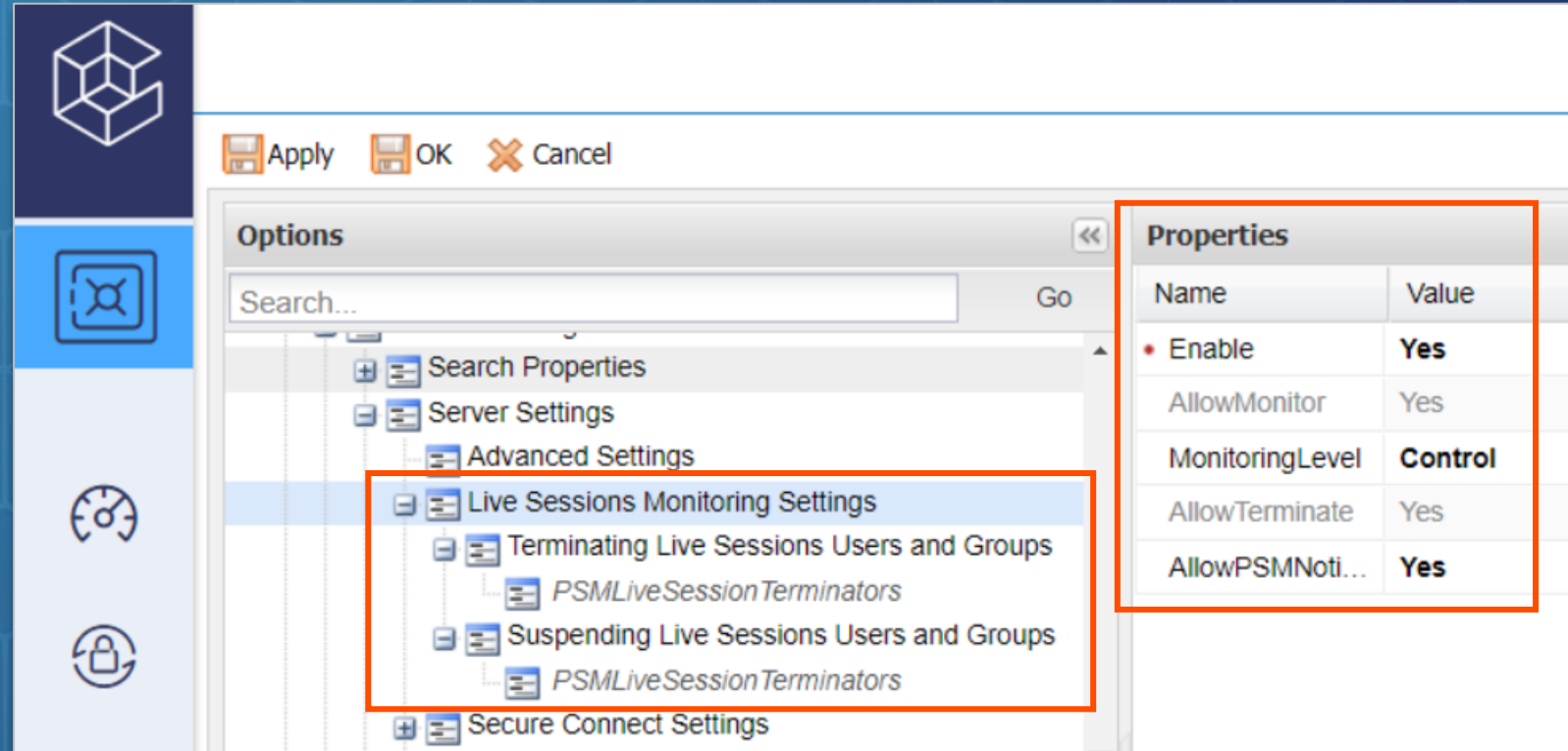


Monitor Active Sessions




Enable and Configure Live Session Monitoring


- Live session monitoring settings determine how users can monitor live privileged sessions and the types of activities that they can perform
- By default, all members of the **Vault** group **PSMLiveSessionTerminators** are authorized to suspend and terminate active sessions



Monitor Active Sessions



Monitoring






 Filter

Recordings

» Active

1 results for: From: 2/6/2022

Risk	User
-	carlos



PSM - 10.0.20.1 - Remote Desktop Connection

Controlling COMPONENTS\PSMConnect (sessionID 6) on COMPONENTS

```
root@target-lin:~  
Using username "root02".  
Last login: Tue Feb  8 09:43:21 2022 from pvwa.acme.corp  
[root@target-lin ~]#  
[root@target-lin ~]#  
[root@target-lin ~]# useradd carlos  
[root@target-lin ~]# passwd carlos  
Changing password for user carlos.  
New password:  
Retype new password:  
passwd: all authentication tokens updated successfully.  
[root@target-lin ~]#  
[root@target-lin ~]#  
[root@target-lin ~]#
```

Last sign in: 2/7/2022 | cindy

Additional details & actions in classic interface

Terminate Suspend Resume **Monitor**



Summary



Summary

In this session we covered:

-  Privileged session monitoring capabilities for PSM and PSM for SSH
-  How to monitor and manage privileged session recordings
-  How to monitor and manage privileged session audits
-  How to monitor and manage active privileged sessions



Additional Resources



External Storage of PSM Recordings

<https://training.cyberark.com/elearning/external-storage-of-psm-recordings>

You may now complete the following exercises:

Privileged Session Management – Part 2

- Privileged Session Terminators
- Monitor, Suspend and Terminate Active Sessions
- Monitor Recordings

