



**CYBERARK<sup>®</sup>**  
The Identity Security Company<sup>™</sup>

# PAM Administration

Privileged Session Management

Part 2



# Agenda

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

1. Monitor and manage privileged session **recordings**
2. Monitor and manage privileged session **audits**
3. 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

## Monitoring

Last sign in: 8/26/2021 | cindy

Filter

Filters

Sessions properties ?

Sessions activities ?

From

To

☒ 08/24/2021 12:00 AM

☐ Today

08/26/2021 11:59 PM

Apply


Recordings

Active sessions

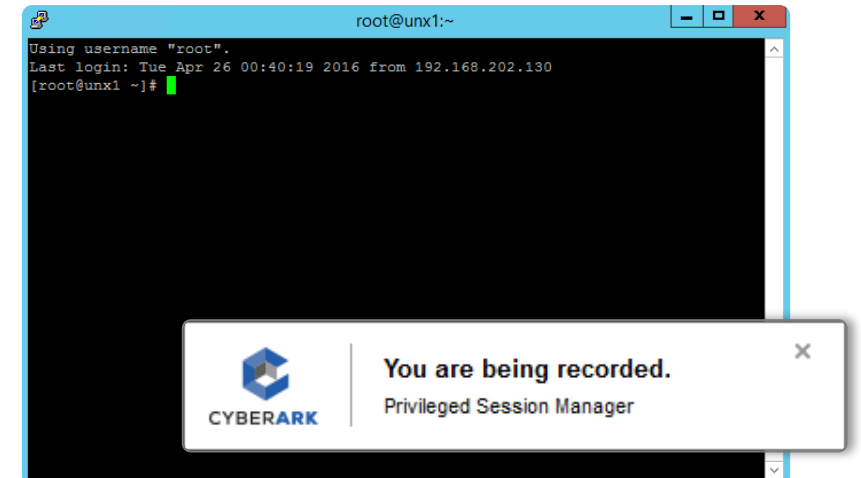
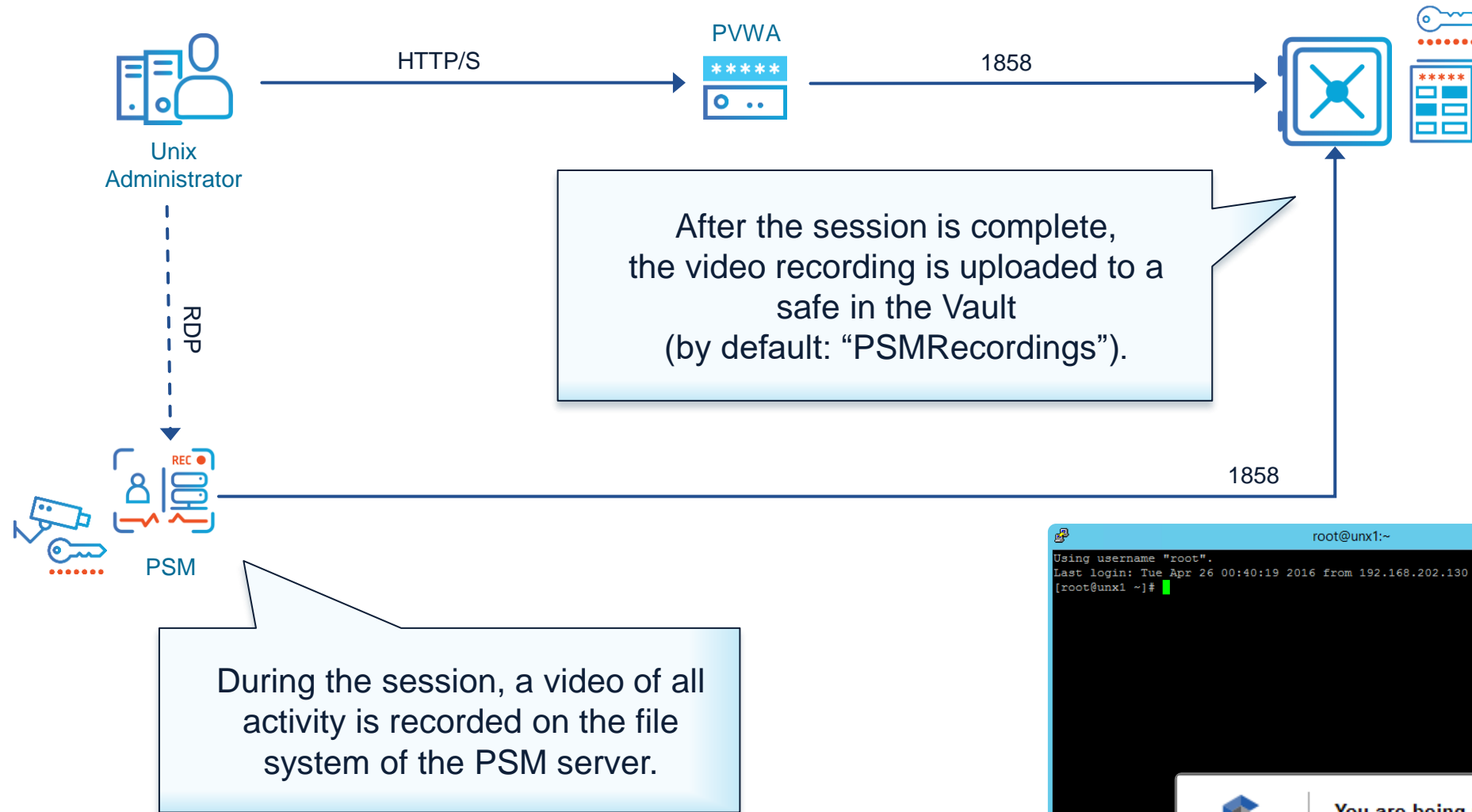
27 results for: From: 8/24/2021 12:00 AM , To: 8/26/2021 11:59 PM [Clear all filters](#) [Additional details & actions in classic interface](#)

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	<a href="#">Play</a>
80	john	RDP	localadmin01	target-win.acme.corp	WINSRVCLADM45	8/24/2021 07:54 AM	<a href="#">Play</a>

© 2023 CyberArk Software Ltd. All rights reserved

 CYBERARK®

# Recordings



# Enable Recordings: Master Policy

The screenshot shows the CyberArk console interface for the Master Policy. A callout box points to the 'Session Management' section, which is highlighted with a pink border. The 'Session Management' section contains two policy rules: 'Require privileged session monitoring and isolation' and 'Record and save session activity', both set to 'Active'.

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

**Session Management**

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

**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')	-	-
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	-

**Audit**

Policy Rule	Value	Exceptions
Activities audit retention period	90	-

**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.

# View Recordings in the PSM

The screenshot displays the CyberArk Monitoring interface. At the top, the 'Monitoring' header is visible on the left, and the user 'cindy' is logged in on the right, with a 'Last sign in: 8/26/2021' timestamp. A callout box points to the user name, stating 'Member of the Auditors group'. The main content area shows a session recording for 'paul as root02 on target-lin' from 8.24.2021 07:34 AM to 8.24.2021 07:42 AM. On the left, a timeline for 'Aug 24 Tuesday' shows a single event at 7:34:27 AM labeled 'passwd'. The right pane shows a terminal window titled 'root@target-lin:~' with the following text: 'Using username "root02".', 'Last login: Tue Aug 24 07:25:35 2021 from components.acme.corp', and two prompts '[root@target-lin ~]#' with a green cursor. At the bottom right, there is a 'Activate Windows' watermark.

Monitoring

Last sign in: 8/26/2021 | cindy

paul as root02 on target-lin

8.24.2021 07:34 AM - 8.24.2021 07:42 AM

Member of the Auditors group

Aug 24 Tuesday

7:34:27 AM passwd

```
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 ~]#
```

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 Classic Interface for monitoring SSH session recordings. The top navigation bar includes a sidebar with icons for Home, Monitor, Audit, and Settings. The main content area is titled "Recording details: carlos-LINSSH30-logon01-10.0.0.20-2021/08/24 06:35:40 AM-2021/08/24 06:36:21 AM".

**Recording 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:

**Account Details:**

- Platform ID: LINSSH30
- Username: logon01
- Address: 10.0.0.20

**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

**Session Transcript:**

```
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 interface also shows a "Play" button and a "Customize" link. The bottom status bar indicates "Displaying events 1 - 3 of 3".



# 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

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

# 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

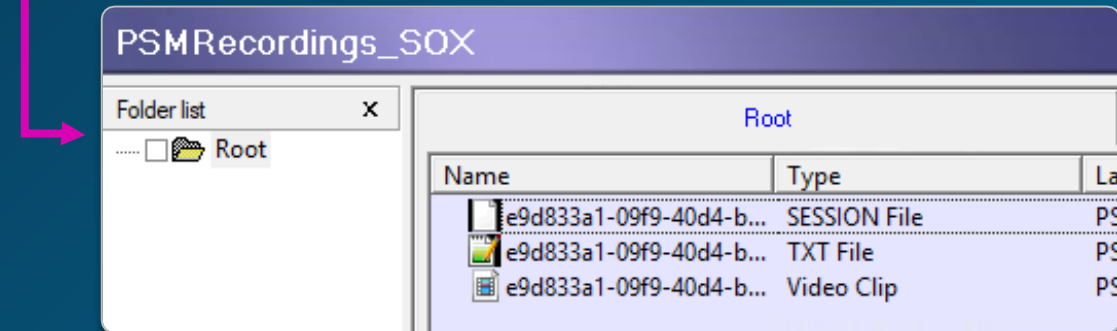
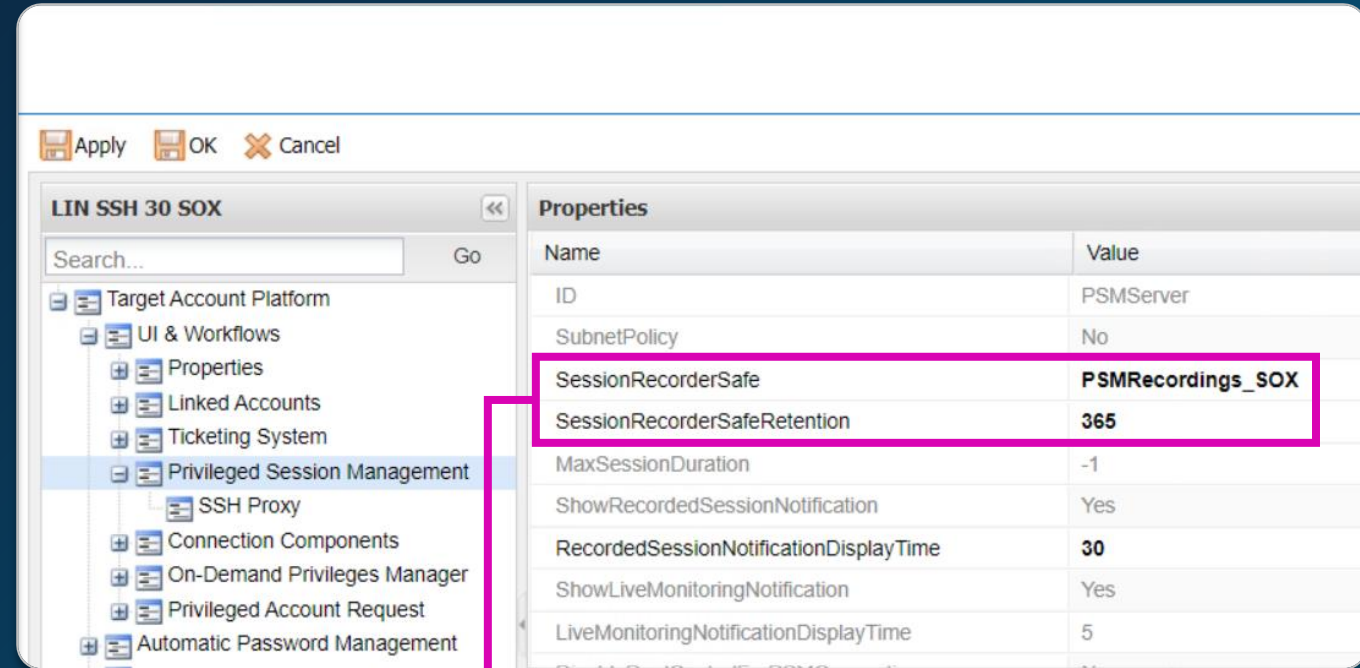
- 100 KB/min – average SSH session
- 200 KB/min – average low activity RDP session
- 300 KB/min – average high activity RDP session with rich wallpaper

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

# 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 CyberArk Monitoring interface. On the left, a table lists session recordings with columns for Risk, User, and a Play button. The 'john' session is highlighted with a red risk score of 80. On the right, the details for the 'john' session are shown, including the connection path 'john connected as localadmin01 on target-win.acme.corp', start time '8/24/2021 07:54 AM', and duration '00:07:05'. A red box highlights the 'Session risk score' of 80 (HIGH) and the 'Strongest impact activity/event' of '[8/24/2021 07:59 AM] New User'. Below this, a timeline shows activities like 'explorer.exe, Program Manager' and 'mmc.exe, Computer Management'.

Risk ↓	User	
80	paul	Play
80	john	Play
-	Carlos	Play
-	mike	Play
-	carlos	Play video (V9 UI)
-	mike	Play
-	john	Play
-	mike	Play
-	robert	Play
-	john	Play
-	paul	Play

john connected as localadmin01 on target-win.acme.corp  
Start: 8/24/2021 07:54 AM Duration: 00:07:05

**80 HIGH Session risk score**  
Strongest impact activity/event [8/24/2021 07:59 AM] New User

8 Activities in the session

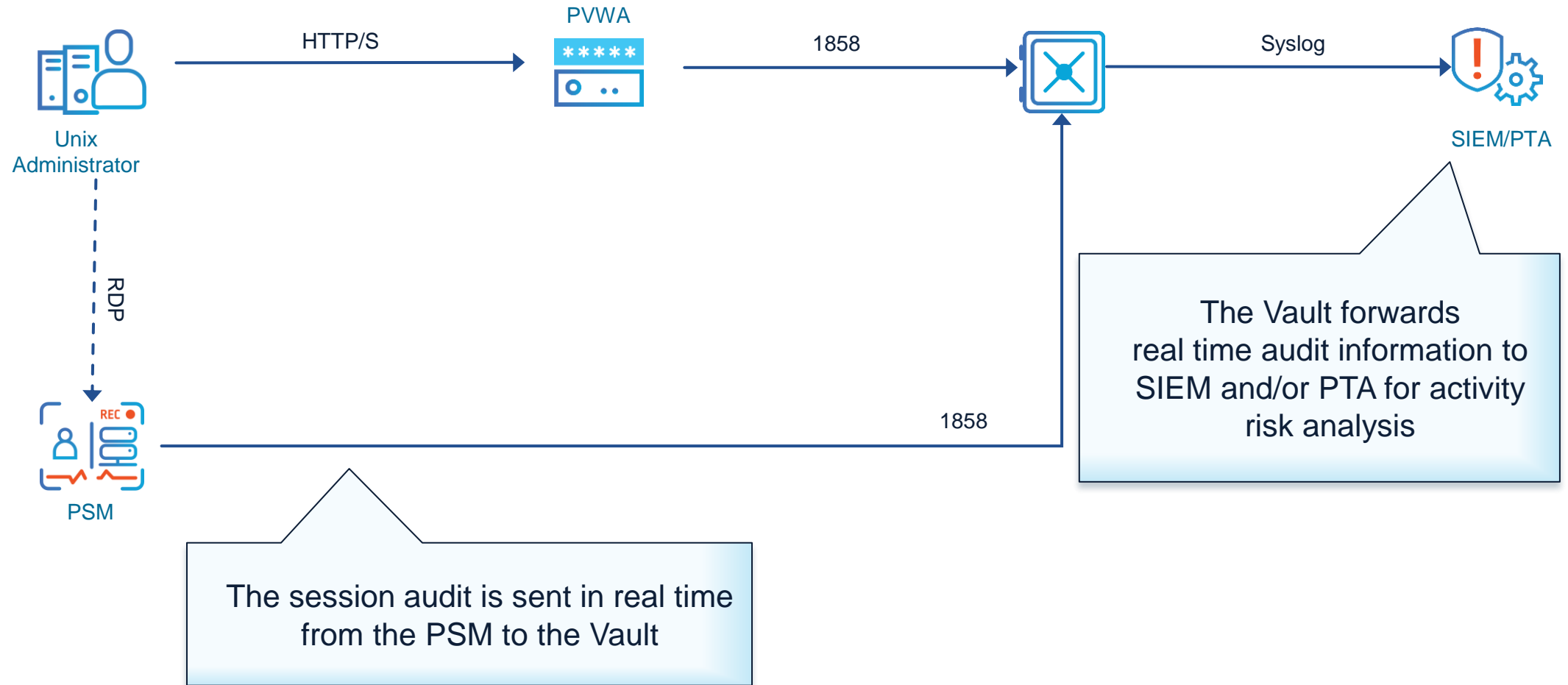
Aug 24 Tuesday

7:54:09 AM explorer.exe, Program Manager

7:54:27 AM 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 screenshot displays the 'Monitoring' dashboard with the 'Active sessions' tab selected. On the left, a table lists active sessions with columns for Risk, User, and actions. The session for user 'john' has a risk score of 80 and a 'Monitor' button. The main panel shows session details for 'john connected as localadmin01 on target-win.acme.corp', including start time (8/26/2021 07:08 AM) and duration (00:00:54). A red box highlights the 'Session risk score' of 80 (HIGH) and the event 'New User'. Below this, a timeline shows activities: 'explorer.exe, Program Manager' at 7:08:16 AM and 'mmc.exe, Computer Management' at 7:08:46 AM. A pink box highlights the 'Terminate', 'Suspend', 'Resume', and 'Monitor' buttons. A callout box points to these buttons with the text: 'The **PSM** can also automatically suspend or terminate sessions when notified by **PTA** or a third-party threat analytics tool'.

Risk	User	Actions
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

80 HIGH Session risk score  
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

The **PSM** can also automatically suspend or terminate sessions when notified by **PTA** or a third-party threat analytics tool

# 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

## Monitoring

Last sign in: 2/7/2022 | cindy

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

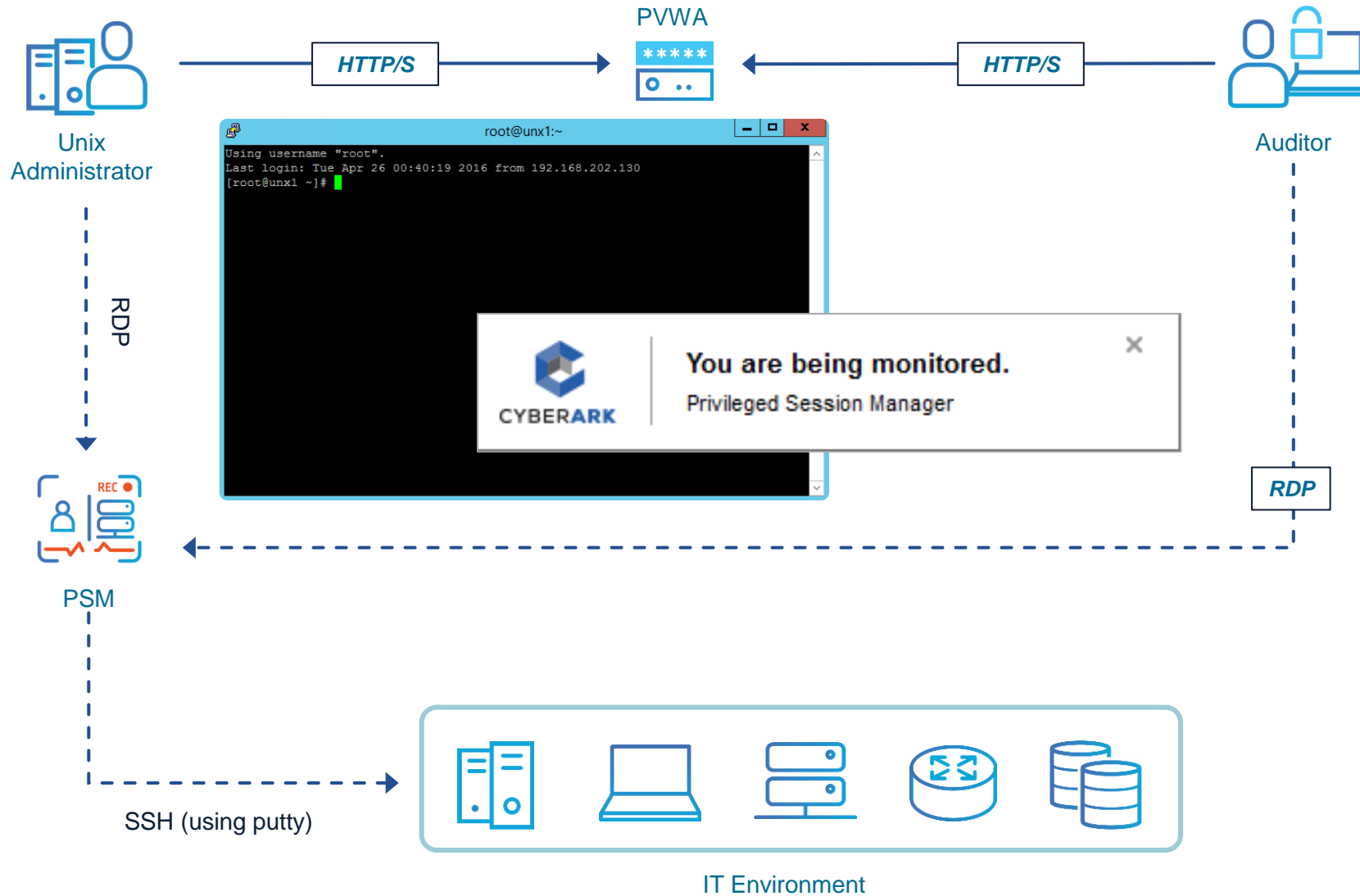
Feb 07

Today

4:27:05 PM useradd mike

4:27:12 PM passwd mike

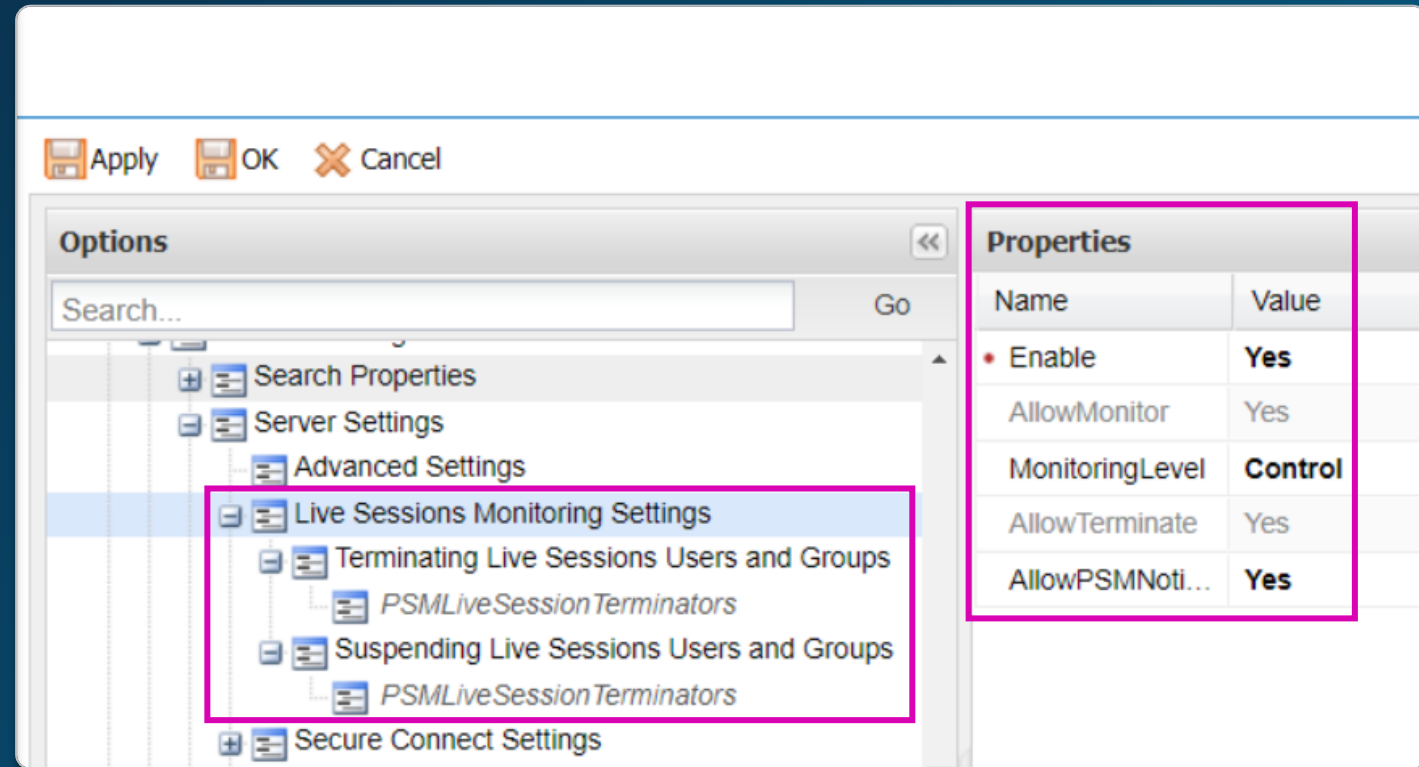
# Monitor Active Sessions





# 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 session

1 results for: From: 2/6/2022 12:00 AM

Risk	User	F
-	carlos	1

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

minate

Suspend

Resume

Monitor

© 2023 CyberArk Software Ltd. All rights reserved

CYBERARK®

# 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