Primary Actor Use Case Story Enables recording of privileged sessions (servers, cloud, IoT) via CyberArk PSM, preventing fraud (6500,000) and ensuring Zero Trust, AAA, and ISO27001/NIS2/RGPD/DORA compliance. Trigger Access request to critical system (servers, cloud, IoT) from End-User. Clear policy established for session recording, identifying privileged accounts and enforcing separation from standard accounts. Accounts associated with correct platform (AD, multi-cloud: AWS/Azure/GCP, IoT). PSM and SIEM configured for recording and anomaly detection. PAM Administrator verifies recording settings. Post-Condition Session recorded, anomalies detected, logs stored for 1-year RGPD retention. Ensures Zero Trust (universal monitoring, anomaly detection), AAA (Authentication via IDP, Accounting via logs), and compliance with ISO27001/NIS2/RGPD/DORA. Prevents fraud (6500,000). Title: Session Recording Actor Action System Response 1. PAM Admin configures PSM recording 2. System enables encrypted recording 3. End-User requests access via PSM 4. Establishes secure proxy session 5. End-User performs actions 6. PSM records session, SIEM analyzes anomalies 7. Session ends 8. Stores encrypted logs/recordings	UC Name	Privileged Accounts session recording		
Use Case Story Enables recording of privileged sessions (servers, cloud, IoT) via CyberArk PSM, preventing fraud (€500,000) and ensuring Zero Trust, AAA, and ISO27001/NIS2/RGPD/DORA compliance. Trigger Access request to critical system (servers, cloud, IoT) from End-User. Pre-Condition Clear policy established for session recording, identifying privileged accounts and enforcing separation from standard accounts.	UC#	3		
Trigger Access request to critical system (servers, cloud, IoT) from End-User. Pre-Condition Clear policy established for session recording, identifying privileged accounts and enforcing separation from standard accounts. Accounts associated with correct platform (AD, multi-cloud: AWS/Azure/GCP, IoT). PSM and SIEM configured for recording and anomaly detection. PAM Administrator verifies recording settings. Post-Condition Session recorded, anomalies detected, logs stored for 1-year RGPD retention. Ensures Zero Trust (universal monitoring, anomaly detection), AAA (Authentication via IDP, Accounting via logs), and compliance with ISO27001/NIS2/RGPD/DORA. Prevents fraud (€500,000). Primary Flow (PF) Title: Session Recording Actor Action System Response 1. PAM Admin configures PSM recording 2. System enables encrypted recording 3. End-User requests access via PSM 4. Establishes secure proxy session 5. End-User performs actions 6. PSM records session, SIEM analyzes anomalies	Primary Actor	PAM administrator, End-User		
Trigger Access request to critical system (servers, cloud, IoT) from End-User. Pre-Condition Clear policy established for session recording, identifying privileged accounts and enforcing separation from standard accounts. Accounts associated with correct platform (AD, multi-cloud: AWS/Azure/GCP, IoT). PSM and SIEM configured for recording and anomaly detection. PAM Administrator verifies recording settings. Post-Condition Session recorded, anomalies detected, logs stored for 1-year RGPD retention. Ensures Zero Trust (universal monitoring, anomaly detection), AAA (Authentication via IDP, Accounting via logs), and compliance with ISO27001/NIS2/RGPD/DORA. Prevents fraud (£500,000). Primary Flow (PF) Title: Session Recording Actor Action System Response 1. PAM Admin configures PSM recording 2. System enables encrypted recording 3. End-User requests access via PSM 4. Establishes secure proxy session 5. End-User performs actions 6. PSM records session, SIEM analyzes anomalies	Use Case Story			
Pre-Condition Clear policy established for session recording, identifying privileged accounts and enforcing separation from standard accounts. Accounts associated with correct platform (AD, multi-cloud: AWS/Azure/GCP, IoT). PSM and SIEM configured for recording and anomaly detection. PAM Administrator verifies recording settings. Post-Condition Session recorded, anomalies detected, logs stored for 1-year RGPD retention. Ensures Zero Trust (universal monitoring, anomaly detection), AAA (Authentication via IDP, Accounting via logs), and compliance with ISO27001/NIS2/RGPD/DORA. Prevents fraud (€500,000). Primary Flow (PF) Title: Session Recording Actor Action System Response 1. PAM Admin configures PSM recording 2. System enables encrypted recording 3. End-User requests access via PSM 4. Establishes secure proxy session 5. End-User performs actions 6. PSM records session, SIEM analyzes anomalies				
separation from standard accounts. Accounts associated with correct platform (AD, multi-cloud: AWS/Azure/GCP, IoT). PSM and SIEM configured for recording and anomaly detection. PAM Administrator verifies recording settings. Session recorded, anomalies detected, logs stored for 1-year RGPD retention. Ensures Zero Trust (universal monitoring, anomaly detection), AAA (Authentication via IDP, Accounting via logs), and compliance with ISO27001/NIS2/RGPD/DORA. Prevents fraud (€500,000). Primary Flow (PF) Title: Session Recording Actor Action System Response 1. PAM Admin configures PSM recording 2. System enables encrypted recording 3. End-User requests access via PSM 4. Establishes secure proxy session 5. End-User performs actions 6. PSM records session, SIEM analyzes anomalies		· · · · · · · · · · · · · · · · · · ·		
Accounts associated with correct platform (AD, multi-cloud: AWS/Azure/GCP, IoT). PSM and SIEM configured for recording and anomaly detection. PAM Administrator verifies recording settings. Post-Condition Session recorded, anomalies detected, logs stored for 1-year RGPD retention. Ensures Zero Trust (universal monitoring, anomaly detection), AAA (Authentication via IDP, Accounting via logs), and compliance with ISO27001/NIS2/RGPD/DORA. Prevents fraud (€500,000). Primary Flow (PF) Actor Action System Response 1. PAM Admin configures PSM recording 2. System enables encrypted recording 3. End-User requests access via PSM 4. Establishes secure proxy session 5. End-User performs actions 6. PSM records session, SIEM analyzes anomalies	Pre-Condition	. , , , , , , , , , , , , , , , , , , ,		
PSM and SIEM configured for recording and anomaly detection. PAM Administrator verifies recording settings. Session recorded, anomalies detected, logs stored for 1-year RGPD retention. Ensures Zero Trust (universal monitoring, anomaly detection), AAA (Authentication via IDP, Accounting via logs), and compliance with ISO27001/NIS2/RGPD/DORA. Prevents fraud (€500,000). Primary Flow (PF) Actor Action System Response 1. PAM Admin configures PSM recording 2. System enables encrypted recording 3. End-User requests access via PSM 4. Establishes secure proxy session 5. End-User performs actions 6. PSM records session, SIEM analyzes anomalies		·		
PAM Administrator verifies recording settings. Session recorded, anomalies detected, logs stored for 1-year RGPD retention. Ensures Zero Trust (universal monitoring, anomaly detection), AAA (Authentication via IDP, Accounting via logs), and compliance with ISO27001/NIS2/RGPD/DORA. Prevents fraud (€500,000). Primary Flow (PF) Actor Action System Response 1. PAM Admin configures PSM recording 2. System enables encrypted recording 3. End-User requests access via PSM 4. Establishes secure proxy session 5. End-User performs actions 6. PSM records session, SIEM analyzes anomalies		PSM and SIEM configured for recording and anomaly detection. PAM Administrator verifies recording settings.		
Post-ConditionSession recorded, anomalies detected, logs stored for 1-year RGPD retention. Ensures Zero Trust (universal monitoring, anomaly detection), AAA (Authentication via IDP, Accounting via logs), and compliance with ISO27001/NIS2/RGPD/DORA. Prevents fraud (€500,000).Primary Flow (PF)Title: Session RecordingActor ActionSystem Response1. PAM Admin configures PSM recording2. System enables encrypted recording3. End-User requests access via PSM4. Establishes secure proxy session5. End-User performs actions6. PSM records session, SIEM analyzes anomalies				
(universal monitoring, anomaly detection), AAA (Authentication via IDP, Accounting via logs), and compliance with ISO27001/NIS2/RGPD/DORA. Prevents fraud (€500,000). Primary Flow (PF) Title: Session Recording				
compliance with ISO27001/NIS2/RGPD/DORA. Prevents fraud (€500,000). Primary Flow (PF) Title: Session Recording System Response	Post-Condition			
Primary Flow (PF) Actor Action System Response 1. PAM Admin configures PSM recording 3. End-User requests access via PSM 5. End-User performs actions 6. PSM records session, SIEM analyzes anomalies		1,	,	
Actor Action 1. PAM Admin configures PSM recording 2. System enables encrypted recording 3. End-User requests access via PSM 4. Establishes secure proxy session 5. End-User performs actions 6. PSM records session, SIEM analyzes anomalies				
 PAM Admin configures PSM recording System enables encrypted recording End-User requests access via PSM Establishes secure proxy session End-User performs actions PSM records session, SIEM analyzes anomalies 	Primary Flow (PF)			
S. End-User requests access via PSM 4. Establishes secure proxy session 5. End-User performs actions 6. PSM records session, SIEM analyzes anomalies				
5. End-User performs actions 6. PSM records session, SIEM analyzes anomalies			System enables encrypted recording	
anomalies		3. End-User requests access via PSM	4. Establishes secure proxy session	
anomalies		5. End-User performs actions	6. PSM records session, SIEM analyzes	
7 Session ends 8 Stores encrypted logs/recordings		·	- I	
7. Jession ends		7. Session ends	8. Stores encrypted logs/recordings	
Alternate Flow Title: Manual review	Alternate Flow	Title: Manual review		
1(AF1) Trigger: Anomaly detected by SIEM.	1(AF1)			
Post-Condition: Alert sent, session audited.		Post-Condition: Alert sent, session audited.		
Actor Action System Response		Actor Action		
1. SIEM detects anomaly, sends alert. 2. PAM Admin reviews session logs.		 SIEM detects anomaly, sends alert. 	2. PAM Admin reviews session logs.	
Exception Flow (EF1) Title: Recording Failure	Exception Flow (EF1)	Title: Recording Failure Trigger: Technical issue in PSM. Post-Condition: Issue logged, session not recorded, alert sent.		
Trigger: Technical issue in PSM.				
Post-Condition: Issue logged, session not recorded, alert sent.				
Actor Action System Response				
			System fails to record, notifies PAM admin	
2. PAM admin investigates.		2. PAM admin investigates.		