UC Name	**Privileged Accounts session recording**	
UC #	3	
Primary Actor	PAM administrator, End-User	
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.	
	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
	7. Session ends	8. Stores encrypted logs/recordings
Alternate Flow 1(AF1)	**Title: Manual review**	
	Trigger: Anomaly detected by SIEM.	
	Post-Condition: Alert sent, session audited.	
	Actor Action	**System Response**
	1. SIEM detects anomaly, sends alert.	2. PAM Admin reviews session logs.
Exception Flow (EF1)	**Title: Recording Failure**	
	Trigger: Technical issue in PSM.	
	Post-Condition : Issue logged, session not recorded, alert sent.	
	Actor Action	**System Response**
		1. System fails to record, notifies PAM admin
	2. PAM admin investigates.	