UC Name	**Just-in-time approval workflow**	
UC #	2	
Primary Actor	PAM administrator, End-user	
Use Case Story	Enables JIT access to critical systems (servers, cloud, IoT) via CyberArk PVWA/PSM, reducing leaks (25%) and outages (10 in 2024), 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 JIT access, identifying privileged accounts and enforcing separation from standard accounts (IGA-managed).	
	Accounts associated with correct platform (AD, multi-cloud: AWS/Azure/GCP, IoT).	
	List of approvers predefined (Safe, Members, permissions).	
	Master Policy configured for dual control.	
	PAM Administrator verifies workflow settings.	
Post-Condition	Session validated and audited, End-User accesses system via PSM. Ensures Zero Trust (continuous verification, least privilege), AAA (Authentication via IDP, Authorization via workflow, Accounting via logs), and compliance with ISO27001/NIS2/RGPD/DORA. Reduces leaks (25%) and outages (10 in 2024).	
Primary Flow (PF)	**Title: Justin-time approval workflow**	
	Actor Action	**System Response**
	1) PAM Admin configures dual control in Master Policy	2) System logs approver settings
	3) End-User submits request via PVWA	4) Sends notification to Approver
	5) Approver approves request	6) PVWA provisions JIT access, PSM opens session
	7) End-user connects via PSM	8) Session recorded, logs stored
Alternate Flow 1(AF1)	**Title: Request rejection**	
	Trigger: Approver rejects request	
	Post-Condition: Access denied, compliant with Zero Trust/AAA.	
	Actor Action	**System Response**
	1) Approver rejects request via PVWA	2) System notifies End-User of denial.
Exception Flow (EF1)	**Title: Request Expiry**	
	Trigger: Approver does not respond within 30 minutes	
	Post-Condition: Request expires, End-User resubmits.	
	Actor Action	**System Response**
		1) System expires request, notifies End-User to resubmits.