AYI NEDJIMI Consultants

PAM : Gestion Complète des Accès P

2 mai 2026 • Mis à jour le 17 mai 2026 • 57 min de lecture • 12208 mots •

La gestion des accès privilégiés (PAM — Privileged Access Management) critiques qu'une organisation peut déployer pour protéger ses actifs numé privilégiés — administrateurs de domaine, root Unix.

La *gestion des accès privilégiés* (PAM — Privileged Access Management) constitu qu'une organisation peut déployer pour protéger ses actifs numériques les plus se de domaine, root Unix, comptes de service avec accès base de données, identités cible numéro un des attaquants avancés. Les rapports Verizon DBIR démontrent d credentials privilégiés est présent dans plus de 80% des violations de données d' négligents exploitent systématiquement l'excès de privilèges pour atteindre des d programme PAM mature répond à cette réalité en éliminant les comptes administra en enregistrant toutes les sessions privilégiées pour l'audit et la forensique, en rot service, en vaultant les mots de passe administrateurs dans un coffre-fort cryptog contrôles PAM dans les processus de conformité NIS2, ISO 27001 et SOC 2. Ce gu solutions du marché, les patterns de déploiement, et r dans la m

Comprendre la surface d'attaque des comptes privilégiés

Avant de concevoir une architecture PAM, il est indispensable d'inventorier et de c
présents dans une organisation moderne. Cette diversité est souvent sous-estimé

Taxonomie des comptes privilégiés

Type de compte	Exemples	Risque princ
Admin domaine Windows	Domain Admins, Enterprise Admins	Accès total à
Admin serveur Unix/ Linux	root, sudo users	Contrôle tota
Comptes de service	SQL Server service account, app-db-user	Credentials s configs
Admin cloud	AWS root, Azure Global Admin	Accès illimité
Admin base de données	sa (SQL Server), sys (Oracle)	Accès à tout
Comptes applicatifs	API keys, OAuth client secrets	Secrets stati
Comptes fournisseurs	MSP, sous-traitants maintenance	Accès tiers n

Réponse sous 24h

Devis gratuit →