CYBERSECURITEAM

Le moindre privilège en pratique

N'accorder que les droits strictement nécessaires — sans bloquer les équipes.

Le moindre privilège est le principe le plus rentable de la sécurité des accès : moins de droits inutiles, c'est une surface d'attaque plus faible et des audits plus simples. Encore faut-il l'appliquer sans paralyser l'activité.

1. Partir des rôles, pas des exceptions

Structurez les droits autour d'un modèle de rôles (RBAC) aligné sur les fonctions métier, avec des règles de séparation des tâches (SoD).

- Définissez des rôles métier clairs plutôt que des accès au cas par cas.
- Identifiez les combinaisons interdites (SoD) : qui ne doit jamais cumuler tel et tel droit.
- Faites valider les rôles par les responsables métier.

2. Réduire progressivement, sans big bang

Une réduction brutale casse la production. Avancez par vagues, sur les périmètres les plus sensibles d'abord.

- Ciblez d'abord les droits d'administration et les données sensibles.
- Retirez les droits inutilisés depuis X mois (analyse des usages).
- Prévoyez un processus rapide de ré-attribution en cas de besoin réel.

> **À retenir :** le moindre privilège n'est pas un projet ponctuel mais un état à maintenir — via les revues d'accès et le juste-à-temps.

3. Mesurer et tenir dans la durée

- Suivez le taux de droits « larges » et son évolution.
- Couplez avec des campagnes de recertification régulières.
- Introduisez l'accès juste-à-temps pour les droits les plus puissants.