CYBERSECURITEAM

Reprendre le contrôle des comptes à privilèges

Inventaire, coffre-fort, rotation et sessions : par où commencer un dispositif PAM.

Les comptes à privilèges (administrateurs, comptes de service, comptes techniques) sont les plus puissants — donc les plus exposés en cas de compromission ou d'audit. Voici une trajectoire pragmatique.

1. Savoir ce que l'on a

On ne protège pas ce qu'on ne connaît pas. La première étape est l'inventaire.

- Recensez les comptes admin, de service et partagés, application par application.
- Identifiez les comptes « orphelins » ou dont personne ne connaît l'usage.
- Classez par criticité (accès aux données sensibles, aux environnements de production…).

2. Mettre sous coffre-fort les accès critiques

- Centralisez les secrets dans un coffre-fort (vault) plutôt que dans des fichiers ou des têtes.
- Activez la rotation automatique des mots de passe des comptes les plus sensibles.
- Supprimez les mots de passe partagés au profit d'accès nominatifs.

> **Priorité :** commencez par les comptes qui exposent le plus (production, données réglementées), pas par la couverture exhaustive.

3. Tracer et limiter dans le temps

- Enregistrez les sessions d'administration sensibles.
- Passez à un accès « juste-à-temps » : le droit n'est ouvert que le temps nécessaire.
- Corrélez les événements avec votre SIEM pour la détection.