

Comptes dormants & orphelins

Détecter et fermer les accès oubliés qui exposent votre organisation.

Les comptes dormants (inutilisés) et orphelins (sans propriétaire identifié) sont une porte d'entrée idéale pour un attaquant, et un point noir récurrent en audit. Ils s'accumulent silencieusement.

1. Les rendre visibles

- Croisez les comptes avec les données RH (départs, mobilités) et les usages (dernière connexion).
- Repérez les comptes sans propriétaire ou rattachés à des personnes parties.
- Traitez en priorité les comptes à privilèges dormants.

2. Traiter sans casse

- Désactivez avant de supprimer (fenêtre de réversibilité).
- Vérifiez les dépendances (comptes de service utilisés par des traitements).
- Documentez chaque décision pour l'audit.

Cause racine : la plupart des comptes fantômes viennent d'un processus de sortie défaillant. Corrigez la source, pas seulement le symptôme.

3. Empêcher leur retour

- Automatisez le deprovisioning au départ (arrivée/départ fiabilisés).
- Mettez en place une détection récurrente des comptes inactifs.
- Suivez le nombre de comptes fantômes comme indicateur de risque.