CYBERSECURITEAM

Réussir une campagne de recertification

Des revues d'accès qui tiennent en audit, sans épuiser les managers.

La recertification consiste à faire valider régulièrement « qui a accès à quoi » par les bons responsables. Bien menée, elle nettoie les accès et fournit une preuve d'audit fiable. Mal menée, elle devient une corvée que personne ne prend au sérieux.

1. Prioriser plutôt que tout revoir

- Concentrez-vous d'abord sur les accès sensibles et les applications critiques.
- Évitez de solliciter les managers sur des droits sans enjeu.
- Adaptez la fréquence à la criticité (semestrielle pour le sensible).

2. Outiller et responsabiliser

Une campagne manuelle sur tableur ne passe pas à l'échelle et ne prouve rien.

- Automatisez l'extraction des droits et la sollicitation des valideurs.
- Désignez clairement un responsable par périmètre.
- Rendez la décision simple : maintenir / révoquer, avec justification.

> **Preuve d'audit :** conservez la trace horodatée de chaque décision de validation ou de révocation.

3. Boucler la remédiation

- Assurez-vous que les révocations décidées sont réellement appliquées.
- Mesurez le taux de suppression effective (un bon indicateur de sérieux).
- Analysez les droits dormants pour améliorer le processus d'entrée/sortie.

hello@cybersecuriteam.com