CYBERSECURITEAM

PCI-DSS & contrôle d’accès

Ce que le référentiel exige concrètement sur les identités et la journalisation.

Pour les organisations qui traitent des données de cartes, PCI-DSS impose des exigences précises sur le contrôle d'accès. Voici l'essentiel côté identités.

1. Restreindre l'accès aux données

- Limitez l'accès aux données de cartes au strict nécessaire (besoin d'en connaître).
- Cloisonnez : pas d'accès direct entre Internet et les composants stockant ces données.
- Appliquez le moindre privilège sur les systèmes concernés.

2. Identifier et authentifier fortement

- Comptes nominatifs (pas de comptes partagés) pour la traçabilité.
- MFA sur tous les accès administratifs et distants.
- Politique de mots de passe robuste et gestion du cycle de vie.

> **Point clé :** l'accès aux données de cartes doit être justifié, revu périodiquement, et intégralement tracé.

3. Tracer et prouver

- Journalisez tous les accès aux données et aux composants critiques.
- Protégez l'intégrité des journaux et conservez-les conformément aux exigences.
- Menez des revues d'accès régulières et documentées.

hello@cybersecuriteam.com