

EXEMPLE DE RAPPORT

43

/ 100

**Exposition importante**

Plusieurs portes d'entrée restent ouvertes. Quelques actions simples réduiraient nettement votre exposition.

Votre score par catégorie

Gouvernance

35/100

Accès & protection

75/100

Facteur humain

18/100

Données & sauvegardes

75/100

Exposition sur Internet

20/100

Réaction aux incidents

40/100

Votre plan d'action prioritaire

1

FACTEUR HUMAIN · 18/100

Faire de vos équipes une ligne de défense

Premier geste : Partagez une consigne simple : en cas de doute sur un e-mail, on ne clique pas et on prévient. Puis mesurez le risque réel par une simulation.

[Spectorly : sensibilisation & simulation de phishing \(essai gratuit 2 jours\) →](#)

2

EXPOSITION SUR INTERNET · 20/100

Savoir ce qu'un attaquant voit de vous

Premier geste : Listez vos sites, noms de domaine et accès à distance, et vérifiez qui en détient les identifiants.

[Diagnostic Applicatif gratuit, puis audit ou test d'intrusion →](#)

Donner un pilote à votre cybersécurité

Premier geste : Désignez un responsable (interne ou externe) et inscrivez un point cyber à l'ordre du jour de la direction chaque trimestre.

Gouvernance Cyber Déléguée (RSSI à temps partagé) →

Aller plus loin

Passez à un audit complet de votre cybersécurité

Ce score mesure ce que vous savez de votre sécurité. Un attaquant, lui, regarde ce qui est **réellement exposé**. Notre audit approfondi, mené par un expert CyberSpector :

- analyse en détail vos réponses et vos pratiques ;
- vérifie techniquement votre exposition (site, messagerie, nom de domaine, accès distants) ;
- vous remet un rapport complet et une feuille de route chiffrée et priorisée.

Prestation sur devis. Prenez rendez-vous pour cadrer votre besoin et recevoir une proposition adaptée.

Prendre rendez-vous : calendly.com/demo-spectorly/rendez-vous-cyberspector

Ou directement : 🇫🇷 +33 1 60 20 05 94 · 🇨🇩 +229 01 66 06 86 97 · contact@cyberspector.com