Conseils Tech

Nos astuces techniques et technologiques

En mode Hardening* Windows

*Durcissement des environnements

#1 - Tes environnements Windows tu renforceras

Windows est une porte d’entrée privilégiée pour les attaquants. Pour **bien verrouiller et renforcer vos environnements**, de nombreux paramètres sont à activer, à condition de bien les utiliser et de **les adapter à vos usages.**

#2 - Le niveau de sécurité de Windows tu évalueras

Que ce soit pour les contrôleurs de domaine, les postes de travail et les serveurs, qu'ils soient ou non dans un domaine, il est primordial d’évaluer leur niveau de sécurité.
L'intégralité des composants Windows (système, réseau, authentification, Windows defender, ...)
doit être pris en compte.

#3 - Ton niveau cible tu détermineras

Pour protéger vos données/votre environnement,
il est nécessaire de mettre en place une stratégie de renforcement en fonction de vos contraintes et de vos risques.
Cela permet d'identifier et de corriger les éventuelles faiblesses de sécurité pouvant compromettre vos systèmes.

#4 - Ton niveau de sécurité tu maintiendras

Maintenir son niveau de sécurité est tout aussi important que de le renforcer et d'évaluer son environnement.
Surveillez régulièrement votre environnement ainsi que les différents accès afin de remédier rapidement à toute intrusion en cas d'attaque.

#5 - Ton esprit à la sécurité tu conformeras

La sécurité d'un système dépend de nombreux paramètres.
Développez votre esprit critique face aux enjeux de sécurité et formez-vous ainsi que vos équipes sur ce sujet.
Pensez à **garder une vision exhaustive de la sécurité et soyez attentifs afin de rester agiles** face aux menaces !

#6 - Des référentiels tu utiliseras

L’ANSSI (Agence nationale de la sécurité des systèmes d’information) ainsi que d'autres organismes internationaux (CIS, DISA) fournissent des référentiels de sécurité reconnus. **Suivez leurs recommandations pour protéger vos systèmes d’information.**

koesio
Corporate Technologies

EXPERT CYBER
LABEL SÉCURITÉ NUMÉRIQUE
Cybermalveillance.gouv.fr
RÉPUBLIQUE FRANÇAISE

Nos équipes vous accompagnent sur ces sujets.

Contactez-nous :

aviti@aviti.fr