Contact@cyber-expert.fr
06 04 50 71 06

FORMATION

Formations/Sensibilisations En Cybersécurité

Les cyberattaques évoluent rapidement et les collaborateurs sont la première ligne de défense. Notre programme de formations en cybersécurité vous permet de renforcer la vigilance de vos équipes, de développer leurs compétences techniques et de réduire significativement les risques liés aux erreurs humaines. Que ce soit pour des collaborateurs non techniques, des équipes IT ou des experts en cybersécurité, nos formations s'adaptent à tous les niveaux et besoins spécifiques

PROCÉDURES & AVANTAGES

- **Des modules spécifiques** pour collaborateurs, équipes IT et experts en cybersécurité, couvrant des sujets tels que **l'hygiène numérique, la gestion des incidents, l'analyse forensique ou encore les tests d'intrusion.**
- **Mises en situation réelles**, simulations de cyberattaques et **exercices pratiques** pour assimiler les concepts et **développer des réflexes de sécurité applicables immédiatement.**
- **Flexibilité totale** avec des formats adaptés à vos contraintes organisationnelles : **formations sur site, e-learning ou hybrides avec un suivi personnalisé.**
- Face à l'évolution constante des menaces, nos contenus sont **régulièrement mis à jour** pour **intégrer les dernières tendances et techniques des cybercriminels.**
- **Mesurer le niveau de maturité en cybersécurité** des équipes grâce à des quizz, challenges et simulations d'attaques pour **valider les acquis et identifier les axes d'amélioration.**
- Nos formations et sensibilisations répondent aux **exigences de conformité** (RGPD, NIS2, ISO 27001) et **renforcent les bonnes pratiques en matière de gouvernance et de gestion des risques cyber.**
- Possibilité d'**obtention de certifications reconnues** pour **attester du niveau de cybersécurité de vos équipes et améliorer la posture de sécurité de votre organisation.**

LES BÉNÉFICES CONCRETS POUR VOUS

Nos formations en cybersécurité offrent des retours mesurables à court et long terme.

Réduction du risque humain

Diminution des erreurs et des attaques réussies grâce à des collaborateurs mieux sensibilisés.

Amélioration de la réactivité en cas d'attaque

Meilleure gestion des incidents grâce à des équipes formées aux bonnes pratiques de cybersécurité.

Tests concrets de vulnérabilité

Mesure de l'efficacité des formations avec des campagnes de phishing et des simulations d'attaques ciblées.

Développement d'une culture de sécurité durable

Intégration des bonnes pratiques dans le quotidien des collaborateurs.

Optimisation de la gouvernance et des processus de cybersécurité

Renforcement des politiques internes et mise en conformité avec les réglementations.

Réduction des coûts liés aux cyberattaques

Moins d'incidents, donc moins de pertes financières et de temps d'arrêt.