

Les enjeux stratégiques du risque numérique et les clés pour le gérer

Référence : **SECRISQUE**

Durée : **2 jours**

Certification : **Aucune**

CONNAISSANCES PREALABLES

- Aucun prérequis.

PROFIL DES STAGIAIRES

- Cette formation s'adresse aux « C-Levels » : dirigeants et cadres dirigeants, gestionnaires de risques groupe, directeurs sûreté-sécurité, CISO groupe, Directeurs du numérique, etc.

OBJECTIFS

- Le risque numérique peut mettre en péril de manière imprévisible et fulgurante les organisations, quelle que soit leur taille et leur typologie. Les impacts sur la productivité, la santé financière ou encore la confiance accordée par les clients et les partenaires ne doivent plus être ignorés. C'est pour cette raison que le risque numérique doit être pris en compte au plus haut niveau de l'organisation en adoptant une démarche de maîtrise du risque numérique propre à la structure de celle-ci et à ses missions, de telle sorte que ce risque rejoigne les préoccupations stratégiques, économiques ou juridiques des organisations. Cette formation concrète vous donne l'ensemble des clés et bonnes pratiques pour mettre en place un cadre de gouvernance du risque numérique, valoriser les investissements en matière de cybersécurité, mais également préparer votre organisation à gérer un incident d'origine cyber.

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Sécurité défensive

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Comprendre le risque numérique

- Panorama de la menace cyber
- Comment les attaquants procèdent-ils ?
- Pourquoi les attaques réussissent-elles si souvent ?

S'organiser et bâtir un cadre de gouvernance du risque numérique

- Identifier ses pires scénarios de risque et ses seuils d'acceptation

- Définir une stratégie de sécurité numérique
- Mettre l'humain au centre du jeu
- Maîtriser ses écosystèmes business et IT
- Protéger ses actifs numériques et centres de gravité critiques
- Mettre en place une défense active pour mieux anticiper la survenue d'une attaque

Être réactif et résilient en cas de cyberattaque

- Les spécificités d'une crise d'origine cyber
- Bâtir son organisation de gestion de crise et se préparer
- Gérer une crise cyber et sa communication de crise le jour J

Piloter son risque numérique et valoriser sa cybersécurité

- Surveiller ses indicateurs de « SWOT numérique »
- Piloter sa performance cyber et sa montée en gamme
- Valoriser ses investissements en sécurité numérique

- Utiliser la réglementation comme levier de compétitivité et de confiance numérique

Serious game : le point de vue de l'attaquant pour mieux le déjouer

- Mise en situation : planification d'une cyberattaque et évaluation du retour sur investissement de l'attaquant (espionnage économique, sabotage/rançongiciel)
- Débriefing : échanges, retours d'expérience et enseignements

Informations complémentaires

- Cette formation peut être également réalisée sur une journée