

Enjeux actuels, menaces et gestion des risques.....



3

JOURS

21

HEURES

PROGRAMME

Introduction à la cybersécurité

- Concepts de base de la cybersécurité et enjeux actuels.
- Menaces et attaques courantes en cybersécurité.
- Principes de gestion des risques en cybersécurité.
- Cadre réglementaire et normatif en matière de cybersécurité (RGPD, ISO 27001, etc..)

Introduction à la Culture digitale

- Introduction à la Culture digitale : définition et enjeux.
- Évolution des technologies numériques et leur impact sur la société.
- Les compétences numériques essentielles pour les professionnels.
- Transformation digitale des entreprises : concepts clés et modèles de réussite.
- Les nouvelles tendances en matière de technologie (IA, IoT, blockchain, etc.).
- L'impact de la Culture digitale sur les stratégies marketing et la gestion des entreprises.

Culture digitale et cybersécurité en pratique

- L'importance de la culture d'entreprise en matière de cybersécurité.
- Création d'une culture de la sécurité : sensibilisation et engagement des employés.
- Gestion des incidents de sécurité et réponse aux attaques.
- Exercices pratiques de simulation d'attaques et de gestion de crises.
- Études de cas de cyberattaques célèbres et leçons apprises.
- Planification stratégique pour renforcer la Culture digitale et la cybersécurité dans les organisations.

Sécurité des applications

- Principes de base de la sécurité des applications.
- Gestion des vulnérabilités et des correctifs.
- Bonnes pratiques de développement sécurisé (OWASP Top 10).
- Sécurité des bases de données et des applications web.

Gestion des incidents et réponse aux cyberattaques

- Détection et analyse des incidents de sécurité.
- Planification et gestion de la réponse aux incidents.
- Forensics numériques et collecte de preuves.
- Bonnes pratiques pour la gestion post-incident et l'apprentissage.

OBJECTIFS

Acquérir les compétences nécessaires pour explorer les fondamentaux de la cybersécurité, sécuriser les réseaux, les systèmes et les applications, et gérer les incidents liés aux cyberattaques

PUBLIC | PRÉREQUIS

PUBLIC

• Développeur web • Développeur web mobile • Architecte • Concepteur développeur d'applications • Chef de projet technique

PRÉREQUIS

Connaître les bases de l'administration Systèmes et Réseaux

INFOS PRATIQUES

HORAIRES DE LA FORMATION

de 9 h 00 à 12 h 30 et de 13 h 30 à 17 h 00

MÉTHODOLOGIE

PÉDAGOGIQUE

Théorie | Cas pratiques | Synthèse

MODALITÉS D'ÉVALUATION

Évaluation qualitative des acquis tout au long de la formation et appréciation des résultats

DATES ET LIEUX

Aucune session ouverte