FFCNCERC ERXCS01 2 520 € 3 jour(s)

[Formation] Comprendre la cybersécurité pour dialoguer avec les experts

OBJECTIFS

- Décrire les notions fondamentales en cybersécurité
- Expliquer le monde de la cybersécurité et sa gouvernance, les risques et menaces, le cadre technique, normatif, légal et réglementaire
- Donner une vision globale des enjeux et des problèmes de sécurité liés à l'interconnexion des réseaux et du monde Internet
- Expliquer l'importance de la protection des données personnelles
- Démontrer comment sécuriser et gérer les applications sensibles, les services et les réseaux
- Mettre en oeuvre les démarches de sécurité inhérentes aux besoins fonctionnels

PROGRAMME

Introduction

Enjeux et problématiques de sécurité dans les systèmes d'information (SI) et les réseaux

- Exemples réels d'attaques et fraudes
- Problématique de confiance à distance
- Risques, menaces, vulnérabilités
- Contraintes et challenges de la sécurité en entreprise
- Enjeux de sécurité en nomadisme et accès distants

Sécurité des données et de l'information

- Protection des données
- Introduction à la cryptographie : techniques, choix de solutions, tailles de clés
- Fonction de hachage, certificats et signature numérique
- Gestion de clés et infrastructure à clé publique (PKI)

Gestion des événements de sécurité (SIEM,

NOUVEAU PROGRAMME | RÉALISABLE À DISTANCE | COMPRENDRE

DATES ET LIEUX

Du 09/04/2025 au 11/04/2025 à Paris
Du 08/10/2025 au 10/10/2025 à Paris

PUBLIC / PREREQUIS

Responsables d'entreprise, DSI, ingénieurs techniques ou commerciaux, toute personne impliquée dans les systèmes d'information ou souhaitant acquérir les connaissances de base en cybersécurité.

Des connaissances de base en réseaux et en SI sont souhaitables afin de tirer pleinement profit de cette formation.

COORDINATEURS

Xavier AGHINA

Responsable de la Sécurité des Systèmes d'Information (RSSI) chez W-HA, avec l'objectif de garantir la sécurité, la disponibilité et l'intégrité du système d'information et des données. Il a développé une expertise en cybersécurité, par la conduite des projets techniques et un programme de recherche sur le paiement mobile et la protection des objets connectés.

MODALITES PEDAGOGIQUES

Des exemples illustrent les concepts théoriques.

SOC)

Contexte normatif, réglementaire et juridique

- Politique de sécurité en entreprise
- Métiers de la sécurité, gouvernance
- Gestion des identités, anonymat, privacy
- Protection des données personnelles : enjeux, techniques et risques juridiques
- Réglementation (CNIL, RGPD, etc.)
- Recommandations ANSSI

Audits et incidents de sécurité

- Techniques et outils d'audit de sécurité
- CERTs et FIRST
- Traitement des incidents de sécurité

Sécurité des réseaux

- Concepts de la sécurité des réseaux
- Protocoles SSL et IPSec
- Architecture sécurisée : Firewall / Proxy, DMZ
- Réseaux privés virtuels (VPN)
- Détection et prévention d'intrusion (outils IDS, IPS)
- Authentification
- Plan de reprise et continuité d'activité (PRA, PCA)
- Sécurité des réseaux sans fil

Synthèse et conclusion