FC9CS01 2 470 € 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
- Identifier une vision globale des enjeux et des problèmes de sécurité liés à l'interconnexion des réseaux et du monde Internet et à la protection des données personnelles
- Lister les éléments clés pour une sécurisation optimale, démontrer comment sécuriser et gérer les applications sensibles, les services et les réseaux
- Mettre en œuvre 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 électronique
- Gestion de clés, certificats et infrastructure à clé publique (PKI), contraintes de déploiement

COMPRENDRE

## DATES ET LIEUX

Du 13/05/2024 au 15/05/2024 à Paris
Du 12/11/2024 au 14/11/2024 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 générales en réseaux et en systèmes d'information (SI) sont souhaitables afin de tirer pleinement profit de la 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

## 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

## Menaces et systèmes de protection des systèmes d'information

- Problèmes de sécurité sur Internet
- Évolution des attaques et des failles
- Concepts de la sécurité des réseaux
- Protocoles SSL et IPSec
- Architecture sécurisée : Firewall / Proxy, DMZ
- Réseaux privés virtuels (VPN)
- Détection d'intrusion (outils IDS, IPS)
- Gestion de l'authentification : IAM, PKI
- Plan de reprise et continuité d'activité (PRA, PCA)
- Sécurité des réseaux sans fil

## Nouveaux challenges de sécurité

- Cloud Computing
- Gestion des événements de sécurité (SIEM, SOC) : retours d'expérience
- Internet des objets : IoT, NFC, BLE
- Perspectives

## Synthèse et conclusion

théoriques.