FC9CS04 3 600 € 5 jour(s)

[Formation] Sécurité des systèmes d'information

OBJECTIFS

- Identifier les risques, les enjeux de sécurité et les éléments clés pour la sécurisation d'un système d'information, d'un point de vue technique et managérial
- Concevoir, déployer, gérer ou évaluer des solutions de sécurisation

PROGRAMME

Introduction

Sécurité des systèmes d'information (SI) et protection des données

- Introduction à la sécurité des SI
- Problématiques de sécurité dans les SI et réseaux
- Sécurité des accès distants
- Protection des données dans un SI

Protection des données personnelles

- Données à caractère personnel
- Identification, biométrie et techniques d'authentification
- Gestion des identités
- Aspects juridiques et réglementaires
- Anonymat, privacy, Privacy by Design, techniques d'anonymisation

Cryptographie pour la sécurité des systèmes d'information

- Techniques cryptographiques
- Systèmes à clé secrète, systèmes à clé publique
- Mise en œuvre au sein de services d'authentification, de chiffrement et de signature électronique

Applications sécurisées

- Infrastructures à clé publique (PKI), certificat

PANORAMA

DATES ET LIEUX

Nous contacter pour les sessions à venir

PUBLIC / PREREQUIS

Toute personne intéressée par la sécurité des systèmes d'information, RSSI, ingénieurs informatique, DSI, administrateurs, etc.

Une bonne connaissance des principes de base de la sécurité permet de tirer un meilleur parti de cette formation.

COORDINATEURS

Maya BADR

Enseignante et responsable pédagogique en cybersécurité et technologies du numérique à Télécom Paris Executive Education. Elle a obtenu son diplôme de doctorat en communications numériques de Télécom Paris.

MODALITES PEDAGOGIQUES

Des exemples et des démonstrations illustrent les concepts théoriques.

électronique et contraintes de déploiement en entreprise
- Exemples d'applications sécurisées
- Contraintes de sécurité en environnement cloud et big data

Management de la sécurité

- Organisation de la sécurité, approche managériale et rôle d'un RSSI
- Normes ISO/CEI 27001 et 27002, PSSI
- Gestion du risque
- ISO/CEI 27005, ISO 31000, méthodes d'analyse et EBIOS
- Référentiels tiers : ANSSI, ENISA, etc.

Audit de sécurité

Architectures de sécurité

- Principes de construction d'architectures de sécurité réseau
- Segmentation logique et physique par technologies de pare-feu
- Exemple d'architectures

Sécurité des systèmes d'exploitation

- Introduction à la sécurité des systèmes d'exploitation
- Sécurité des antivirus

Supervision et gestion des événements de sécurité

- Logiciels de détection et de prévention d'intrusion (IDS/IPS)
- Security Event Information Management (SIEM)

Protection des sites et infrastructures Web

- Sécurité des navigateurs Internet
- Sécurité Web

Synthèse et conclusion