FL9CS01 **10 500 €** **20 jour(s)**

[Formation certifiante] Cybersécurité des données, réseaux et systèmes

OBJECTIFS

- Définir la gouvernance de la sécurité des systèmes d'information de l'entreprise
- Mettre en place des mécanismes de sécurité
- Élaborer et mettre en œuvre un plan de sécurité destiné à la protection des ressources vitales de l'entreprise
- Concevoir et mettre en œuvre une architecture de sécurité

PROGRAMME

Introduction : Cybersécurité et Cybercriminalité

Mécanismes et algorithmes de sécurité

- Cryptographie : Principes et Vocabulaire
- Cryptographie symétrique et asymétrique
- Fonctions de Hachage
- Infrastructure de Confiance
- Certificats numériques
- Infrastructure de gestion de clés publiques (PKI)
- Signature digitale

Travaux pratiques : Techniques cryptographiques

Introduction à la cryptographie post quantique

Authentification

- Identité numérique et sécurité
- Identification et authentification
- Gestion d'identités et des accès (CIAM)
- Contrôle d'accès (RBAC, ABAC, LBAC)
- Référentiels d'identités

Travaux pratiques : Authentification et contrôle d'accès

NOUVEAU PROGRAMME ATELIER

DATES ET LIEUX

Du 09/09/2024 au 10/04/2025 à Paris

PUBLIC / PREREQUIS

- Techniciens ou ingénieurs réseaux sans expérience en sécurité
- Chefs de projets ou responsables de solutions intégrant des contraintes de sécurité
- Consultants, architectes de systèmes
- Administrateurs systèmes et réseaux
- Équipes sécurité des réseaux
- Responsables informatiques, responsables des systèmes d'information
- Intégrateurs de systèmes
- Managers impliqués dans la sélection, la mise en œuvre ou le support d'un accès sécurisé à l'entreprise

Des connaissances de base sur les réseaux (TCP/IP) et les systèmes d'information, sont vivement recommandé afin de tirer pleinement profit 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

Sécurité des réseaux

- Attaques réseaux
- Protocoles IPv4, IPv6 et IPsec
- VPN, Pare-feu, Proxy applicatif
- Détection et prévention d'intrusion

Normes et Législations

- Standards ISO 27001 et 27002
- Protection des données RGPD
- Gestion de crise et reprise d'activité
- Critères communs

Gestion et Analyse de risques

- Principales méthodes : ISO 27005, EBIOS RM

Audit de Sécurité

- Audit de vulnérabilités : les principes et différentes étapes
- Audit de la politique de sécurité

Sécurité par la gestion opérationnelle SOC & SIEM

- Méthodologies d'implémentation et d'exploitation
- Traitement opérationnel des évènements de sécurité

Étude de cas concret de gestion d'un SOC

Sécurité des applications et du développement

- Historique SSL/TLS, Architecture et services de TLS
- Solutions pour le contrôle d'accès aux applications (password, OTP, SSO)
- Méthodes et outils pour l'audit du code
- Principe du développement sécurisé et bonnes pratiques

Sécurité des réseaux sans fil

- Fonctionnement du WEP et du WPA (TKIP)
- WPA2 et WPA3
- Déploiement d'une infrastructure WIFI et/ou attaque sur une structure WEP, WPA ou WPA2

La Blockchain

IA et cybersécurité

Synthèse et conclusion

communications numériques de Télécom Paris.

ORGANISATION PEDAGOGIQUE

Cette formation est organisée à temps partiel à raison de quelques jours par mois pour permettre la poursuite d'une activité professionnelle.

International : +33 (0)1 75 31 95 90