FFCCERTT **10 600 €** **20 jour(s)**
ERXCS01

[Formation certifiante] Cybersécurité des données, réseaux et systèmes

OBJECTIFS

Identifier les principes fondamentaux de la cybersécurité
Disposer des compétences nécessaires pour concevoir et mettre en oeuvre des mécanismes de sécurité
Maitriser les outils de gestion et analyse de risques
Présenter l'aspect normatif et règlementaire ainsi que l'audit de sécurité
Élaborer et mettre en oeuvre un plan de sécurité destiné à la protection des ressources vitales de l'entreprise
Recueillir les incidents de sécurité en s'appuyant sur des analyses de risques, un SOC ou un CERT

PROGRAMME

Introduction : Cybersécurité et Cybercriminalité

- Objectifs de sécurité
- Cyberspace et menaces
- Principales cyberattaques et caractéristiques

Gestion et analyse de risques

- Principales méthodes : ISO 27005, EBIOS RM

Normes et législations

- Standards ISO 27001 et 27002
- Protection des données RGPD
- UNECE WP.29
- Gestion de crise et reprise d'activité
- Critères communs

Audit de sécurité

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

NOUVEAU PROGRAMME ATELIER RÉALISABLE À DISTANCE

DATES ET LIEUX

Du 07/10/2024 au 19/05/2025 à Paris

PUBLIC / PREREQUIS

Chefs de projets ou responsables de solutions intégrant des contraintes de sécurité
Techniciens ou ingénieurs réseaux
Consultants, administrateurs systèmes et réseaux
Responsables informatiques, responsables des systèmes d'information
Managers impliqués dans la sélection, la mise en oeuvre ou le support d'un accès sécurisé à l'entreprise

Des connaissances de base sur les réseaux et les systèmes d'information sont vivement recommandées 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 communications numériques de Télécom Paris.

ORGANISATION PEDAGOGIQUE

Mécanismes de sécurité et infrastructure de confiance

- Cryptographie : principes et vocabulaire
- Cryptographie symétrique et asymétrique
- Fonctions de Hachage, certificats numériques, signature digitale
- Infrastructure de gestion de clés publiques (PKI)

Introduction à l'informatique quantique et cryptographie post-quantique

Authentification

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

Sécurité des réseaux

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

Blockchain

- Origine et différents standards
- Fonctionnalités des passerelles et des noeuds d'échange
- Sécurité des clés privées et clés publiques
- Cas d'application et TP

Sécurité des applications et du développement

- Introduction à l'OWASP
- Historique SSL/TLS, Architecture et services de TLS
- Solutions pour le contrôle d'accès aux applications (password, OTP, SSO)
- 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

IA et Cybersécurité

- Les principes de l'intelligence artificielle et de l'apprentissage statistique

Mise en oeuvre et évaluation de méthodes

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

Les promotions sont constituées de 10 à 15 personnes.

Synthèse et conclusion