CERTIFICATION

CYBERSÉCURITÉ DES DONNÉES, RÉSEAUX ET SYSTÈMES

FFCCERTTERXCS01	PRIX : 10 900 €	DURÉE : 20 JOURS	ÉLIGIBLE CPF

Pauses et déjeuners offerts

Les entreprises doivent ouvrir de plus en plus leur système d'information non seulement entre leurs sites, mais aussi à leurs clients, à leurs fournisseurs, à leurs partenaires et plus généralement, aux utilisateurs d'Internet. La sécurité dans les SI et les réseaux constitue un enjeu stratégique pour tous les responsables de réseaux et SI, de services Web, de paiements sécurisés, etc.

La formation permet de répondre aux exigences de la gouvernance de la sécurité avec une approche globale couvrant les aspects techniques, méthodologiques, organisationnels et réglementaires. Elle permet d'acquérir les compétences nécessaires à l'élaboration et à la mise en place d'un plan de sécurité destiné à la protection des ressources vitales contre les attaques internes et externes.

VOUS ÊTES

- 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 œuvre 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.

OBJECTIFS

- Identifier les principes fondamentaux de la cybersécurité
- Disposer des compétences nécessaires pour concevoir et mettre en œuvre des mécanismes de sécurité
- Utiliser les outils de gestion et analyse de risques
- Présenter l'aspect normatif et réglementaire ainsi que l'audit de sécurité
- Élaborer et mettre en œuvre 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

ÉVALUATION ET CERTIFICATION

- Évaluation des compétences acquises
- Ateliers de mise en œuvre et de simulation de cas pratiques concrets
- Évaluation du mémoire professionnel basé sur un projet individuel soutenu devant un jury

Les participants ayant suivi le parcours avec succès obtiennent la certification du bloc 3 du RNCP38140 délivrée par Télécom Paris.

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
- 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

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 nœuds d'échange
- Sécurité des clés privées et clés publiques
- Cas d'application et TP

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
- 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 œuvre et évaluation de méthodes d'apprentissage dans le cas de problématique de cybersécurité

Synthèse et conclusion

ATELIER

FAISABLE À DISTANCE

EN
RÉALISABLE EN ANGLAIS

RESPONSABLE(S)

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.

MODALITÉS PÉDAGOGIQUES

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.

LABEL

SecNumedu
Formation continue
ANSSI

CERTIFICATION DÉLIVRÉE PAR

TELECOM Paris
IP PARIS