FL9CS02 **12 500 €** **29 jour(s)**

NOUVEAU PROGRAMME

[Formation certifiante] Architecture en cybersécurité

OBJECTIFS

- Promouvoir des mesures méthodologiques, techniques et organisationnelles de sécurité
- Définir, déployer et gérer une architecture de sécurité dans différents contextes professionnels
- Intégrer des solutions de sécurité adaptées aux besoins
- Comprendre et réaliser une analyse de risque, un audit de vulnérabilités et de politique de sécurité
- Évaluer une situation de crise, prendre les bonnes décisions et gérer les fonctions de reporting
- Maîtriser les techniques et les outils de gestions d'identité et d'autorisation
- Présenter les risques pour la sécurité du Cloud

PROGRAMME

Introduction

Gestion globale de la sécurité et méthodologie

Conception d'architectures de sécurité

- Conception d'architecture de sécurité et aperçu du marché en solutions de cybersécurité
- Attaques réseaux
- Firewall, routeur, IDS/IPS, VPN
- Cryptographie, fonction de hachage et signature numérique
- Infrastructure de confiance

Normes et règlementations

- Standards 27001 et 27002 pour l'établissement et

DATES ET LIEUX

Du 09/12/2024 au 09/09/2025 à Paris

PUBLIC / PREREQUIS

Techniciens et ingénieurs avec bonne expérience en systèmes d'information et en réseaux informatique.

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.

la gestion du SMSI
- Aspects juridiques
- Protection des données RGPD
- Certification critères communs et CSPN

Analyse et gestion de risques

Audit de sécurité

- Audit de vulnérabilités
- Audit de politique de sécurité
- Gestion de crise et reprise d'activité (PRA) : incidences d'une crise cyber sur l'organisation ou l'entreprise
- Plan de continuité d'activité (PCA) et protection contre la fuite des données sensibles

Outils de supervision, SOC, SIEM

Authentification, Identity & Access Management

- Gestion et fédération des identités : SSO interne et web SSO, OpenID et SAML
- Gestion de rôles : Role Mining, réconciliation de rôles
- Gestion des autorisations : provisioning, gestion des exceptions, reporting
- Aperçu de l'offre commerciale : retour d'expérience et limites de l'offre

L’IA et la cybersécurité

Introduction à l’informatique quantique et la cryptographie post-quantique

Architecture Blockchain

- Fondements et infrastructure de la Blockchain
- Domaines d’exploitation

Sécurité du Cloud

- Typologie des environnements de Cloud, impact pour la sécurité
- Virtualisation et sécurité : menaces et vulnérabilités, solutions de sécurité
- Sécurité des données externalisées
- Référentiels de sécurité Cloud
- Détection et exploitation de vulnérabilités dans le Cloud

DevSecOps

- Outils du DevOps
- Principes et best-practices du Secure Design

- Iintégration de la sécurité dans le cycle de vie du développement logiciel
- Collaboration et communication dans le DevSecOps

Synthèse et conclusion