FFCCERTT ERXCS06 7 900 € 12 jour(s)

[Formation certifiante] Cybersécurité : Stratégie, Gouvernance et Résilience

OBJECTIFS

- Expliquer les fondamentaux de la cybersécurité et les principales menaces émergentes
- Identifier les risques, les actifs critiques et les exigences réglementaires applicables afin de prioriser les actions de protection
- Élaborer une stratégie de cybersécurité intégrant les dimensions de gouvernance, de gestion des risques et de conformité
- Appliquer les principaux référentiels et exigences réglementaires (NIS2, DORA, RGPD, ISO 27001, etc.) afin de mettre en œuvre une démarche de conformité adaptée à l'organisation
- Dialoguer efficacement afin de faciliter la prise de décision et le pilotage des projets de cybersécurité

PROGRAMME

Introduction

Cybersécurité et cybercriminalité

- Objectifs de sécurité
- Domaines d'application
- Différents besoins en sécurité
- Le cyberspace et ses menaces
- Éléments de vulnérabilités
- Les cyberrisques
- Les principales cyberattaques et leurs caractéristiques

Tendances récentes et menaces émergentes

Mécanismes et algorithmes de cryptographie

- La cryptographie : Principes et Vocabulaire
- Cryptographie symétrique et asymétrique

NOUVEAU ATELIER RÉALISABLE À DISTANCE

DATES ET LIEUX

Du 26/04/2027 au 02/11/2027

PUBLIC / PREREQUIS

Cette formation s'adresse aux managers, commerciaux, chefs de projet, responsables risques et conformité, auditeurs, consultants et futurs RSSI souhaitant acquérir une vision globale de la gouvernance, de la gestion des risques et de la conformité en cybersécurité.

Aucun prérequis technique.

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.

- Fonctions de Hachage et certificats numériques
- Signature Digitale

IA et cybersécurité

- Principes de l'intelligence artificielle et du Machine Learning
- Mise en œuvre et évaluation de méthodes d'apprentissage dans le cas de problématique de cybersécurité
- Explicabilité de l'IA

Gestion et analyse de risques

- Les principales méthodes : ISO 27005, EBIOS RM

Normes et Législations

- Les standards ISO 27001 et 27002 pour l'établissement et la gestion du SMSI
- La directive NIS2
- Protection des données RGPD
- Gestion de crise et reprise d'activité

Audit de sécurité

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

Zero Trust : posture de sécurité renforcée

- Origine du modèle Zero Trust
- Principes et conception : Architecture à 5 piliers
- Gouvernance, risques et conformité dans un modèle Zero Trust
- Transition vers le Zero Trust : Mise en place progressive

Synthèse et conclusion