COMPRENDRE LA CYBERSÉCURITÉ POUR DIALOGUER AVEC LES EXPERTS

FFCNCERCERXCS01	PRIX : 2 580 €	DURÉE : 3 JOURS

Pauses et déjeuners offerts

NOUVEAU PROGRAMME

COMPRENDRE

RÉALISABLE EN ANGLAIS

FAISABLE À DISTANCE

CYBERSÉCURITÉ

FORMATIONS INTER-ENTREPRISES

PRÉSENTATION

La cybersécurité est souvent perçue comme complexe, ce qui peut rendre le dialogue avec les experts difficile. Cette formation rend accessibles à tous les concepts essentiels et les principaux mécanismes de protection.

Dans un contexte où les menaces cyber évoluent en permanence et où l'intelligence artificielle fait émerger de nouveaux usages comme de nouveaux risques, la formation propose un large tour d'horizon des techniques de cybersécurité et de leurs applications. Elle définit le vocabulaire et explique les notions fondamentales nécessaires pour comprendre les enjeux et adopter les bonnes pratiques.

OBJECTIFS

- Décrire les notions fondamentales en cybersécurité
- Identifier les concepts clés et les enjeux essentiels de la cybersécurité dans un contexte professionnel
- Expliquer l'écosystème de la cybersécurité y compris la gouvernance, les risques et menaces courants ainsi que le cadre technique simplifié
- Maîtriser les aspects normatif, légaux et réglementaires liés à la cybersécurité

PROGRAMME

Introduction
- Les principales cyberattaques et leurs caractéristiques
- Risques, menaces et vulnérabilités
- Objectifs de sécurité
- Domaines d'application en entreprise

Cybersécurité : un levier de performance pour l'entreprise

Sécurité des systèmes d'information
- Protection des données
- La cryptographie et ses applications
- Fonction de hachage, certificats et signature numérique
- Gestion de clés et infrastructure à clé publique (PKI)
- Gestion des événements de sécurité (SIEM, SOC)

IA et Cybersécurité

Sécurité des réseaux
- Concepts de la sécurité des réseaux
- Architecture sécurisée : Firewall / Proxy, DMZ
- Réseaux privés virtuels (VPN)

Gestion et Analyse de risques
- Définitions et notions élémentaires sur le risque cyber
- Les normes sur la gestion et l'analyse de risques
- La norme ISO/IEC 27005
- Présentation de EBIOS-RM
- Étude de cas

Contexte normatif, réglementaire et juridique
- Définitions et notions élémentaires
- ISO/IEC 27001 et 27002
- Complémentarité de la directive NIS2 et du Cyber Resilience Act (CRA)
- Recommandations ANSSI

Audits et incidents de sécurité
- Outils normatifs de référence pour l'audit
- Audit de politique de sécurité

Synthèse et conclusion

PUBLIC/PRÉREQUIS

Responsables d'entreprise, DSI, ingénieurs techniques, commerciaux ou juristes, toute personne impliquée dans les systèmes d'information ou souhaitant acquérir les connaissances de base en cybersécurité.

Des connaissances de base sur le numérique en entreprise sont souhaitables afin de tirer pleinement profit de cette formation.

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

Des démonstrations et des mises en situation illustrent les concepts théoriques.