41 rue Garibaldi – 69006 LYON

Valérie Thoraval
**04.72.32.50.60**

**contact@cpe-formation.fr**
**cpe-formation.fr**

CYBERSÉCURITÉ

# CYBERSECURITE ET INTELLIGENCE ECONOMIQUE, SE PROTEGER

## OBJECTIFS

Découvrir la cybersécurité et les menaces actuelles. Connaitre les réglementations générales et les réglementations européennes. Déterminer son niveau d'exposition en fonction de son activité, l'impact pour sa société. Détermination de mes points faibles : audit organisationnel, technique, pentest. Surveillances : CERT/SOC, sensibilisation.

## CONTENU PÉDAGOGIQUE

**Jour 1**

**Introduction la sécurité informatique.**

*Risques et menaces*

Présentation des risques et des menaces courantes. Motivation et sociologie des pirates.

Présentation des menaces les plus courantes : exploitation de vulnérabilités, ransomware, phishing, exfiltration de données, attaques d'applications web, codes malveillants... exemples de piratages en entreprises et cas réels.

Introduction aux bonnes pratiques pour limiter les risques, cas d'usages.

Contrôle des accès, authentification et autorisation. Bonnes pratiques des mots de passe, certificats et token, connexions à distances et VPN

La cybersécurité par les réseaux et les failles inhérentes aux objets connectés, aux appareils en mobilité.

Informer le personnel et sécuriser les postes de travail

Comment sensibiliser et informer le personnel, faire prendre conscience qu'une négligence peut provoquer une catastrophe. Souligner les responsabilités de chacun.

Mettre en place les bonnes pratiques de base dans l'entreprise et les faire appliquer. Sécuriser les postes de travail. Agir pour une sécurité au quotidien et maintenir la vigilance dans le temps.

Rédiger et afficher une charte des bonnes pratiques et d'utilisation des ressources informatiques.

Introduction aux aspects sociaux et juridiques, à la cybersurveillance la protection de la vie privée.

*Le cadre juridique*

Découvrir et comprendre les contraintes juridiques et réglementaires, saisir leur intérêt

Connaitre les différents acteurs de la sécurité informatique, leur rôle et les obligations à respecter quant aux pratiques et à la protection des données :

- La CNIL *(Commission Nationale de l'Informatique et des Libertés)* et la législation.
- La RGPD *(Règlement Général sur la Protection des Données)* , objet et objectifs
- L'ANSSI *(Agence Nationale de la Sécurité des Systèmes d'Information),* présentation
- NIS et autres règlementations pouvant impactées les prestataires de service qui souhaitent travailler avec des entreprises aux systèmes d'informations critiques (OIV/SIIV)

Savoir quoi faire en cas d'attaque constatée, dépôt de plainte et assurances spécifiques. Quels recours et protections en cas d'attaque informatique

*Analyse des risques, des vulnérabilités et des menaces*

Les pistes pour entamer une démarche d'analyse et d'évaluation de la maturité cybersécurité de son entreprise. Evaluation des conséquences en cas d'attaque et de perte des données pour son activité, arrêt momentané ou prolongé.

Comment définir et mettre en place une stratégie pour une meilleure protection des pratiques, de l'infrastructure et protection des données.

Décrire le rôle des DSI, DSSI, administrateur système, réseau et autres acteurs de la cybersécurité dans l'entreprise.

**Jour 2**

**Présentation des services essentiels d'un SI & audit**

### DURÉE
2 jours
14 heures

### SESSIONS
- 11 et 12 décembre 2024 en présentiel à Lyon

### FRAIS D'INSCRIPTION (DÉJEUNER INCLUS)
1 275 € HT

### PRÉREQUIS & PUBLIC CONCERNÉ
Ingénieurs, techniciens, chefs de projet ou d'entreprises, directeurs de services, responsables SSI... disposant de connaissance générale de l'informatique

Aider à définir la stratégie d'amélioration de la cybersécurité dans l'entreprise. les norme ISO 2700x

Présentation des différents types d'audit

- Audit de configuration,
- Audit Technique (tests d'intrusion),
- Audit organisationnel,
- Audit d'architecture.

*Objectif* : Etre alerté sur la présence de vulnérabilité et éviter leur exploitation à des fins malveillantes (sabotage, espionnage industriel, compromission de données, indisponibilité de services.)

Définir des plans d'action avec des recommandations à mettre en œuvre par niveau de priorité /criticité.

Détection des tentatives d'intrusion, suivi en temps réel (alerting) : qu'est-ce qu'un SOC en entreprise, une équipe blue team, red team, un SIEM

Gérer son parc informatique et ses vulnérabilités : identification des CVE, programme de patch mangement et hygiène informatique.

## Coordonnées

CPE Lyon Formation Continue

41 rue Garibaldi – 69006 LYON

04.72.32.50.60