Cybersécurité

Référent Cybersécurité en TPE/PME

Devenir le pilier cybersécurité de son entreprise et piloter la sécurité opérationnelle de manière efficace

Public visé

- Référents cybersécurité / SSI
- DSI, RSI, RSSI en environnement PME
- Responsables informatiques
- Responsables conformité ou RGPD
- Dirigeants techniques ou chefs d'entreprise

Les objectifs de la formation

- Comprendre les enjeux et menaces liés à la cybersécurité dans le contexte TPE/PME.
- Savoir identifier les risques spécifiques et y répondre avec des mesures pragmatiques.
- Être capable de structurer une politique de sécurité (PSSI) adaptée à la taille de l'organisation.
- Développer des réflexes opérationnels en cas d'incident de sécurité.
- Intégrer la cybersécurité dans les processus métier, la gouvernance et la culture d'entreprise.
- Être autonome dans la mise en œuvre de la conformité réglementaire (RGPD, NIS2, etc.).
- Constituer une boîte à outils de veille et de réponse aux menaces.

Méthodes pédagogiques

- Approche actionnelle : cas concrets, simulations, co-construction
- Retours d'expérience terrain issus de nos missions d'audit PASSI, avec exemples de vulnérabilités récurrentes dans les SI de PME ; nos accompagnements cybersécurité en région dans le cadre des dispositifs « Diag Cyber » ou « Plan France Relance » ; nos interventions SOC & CSIRT sur incidents réels (ransomware, fuite de données, usurpation de prestataire IT) ; les enseignements tirés de notre veille active au sein du Campus Cyber et de l'écosystème ANSSI/CERT-FR.
- Contributeurs à des groupes de travail nationaux (Campus Cyber, France Num, etc.)
- Pédagogie inversée avec ressources en ligne à explorer avant/après
- Accès à la plateforme ACG Cyber Academy pour les ateliers et exercices interactifs

Les prérequis de la formation

- Maîtrise de l'environnement numérique d'entreprise
- Connaissances de base en réseaux et systèmes (niveau utilisateur averti)
- Appétence pour les enjeux technico-réglementaires

Programme de la formation

Jour 1 : Fondamentaux, enjeux, cadre juridique

- Définition cybersécurité / cyberdéfense / cybercriminalité
- Typologies : ransomware, phishing, APT, supply chain
- Vulnérabilités humaines (exploits sociaux)
- Acteurs : ANSSI, CNIL, DGSI, gendarmerie
- Cadre juridique : RGPD, CNIL, responsabilités, preuve

Jour 2 : Hygiène numérique & sécurité de base

- Politique mot de passe, MFA
- Veille et mises à jour (patching, obsolescence)
- BYOD, réseaux ouverts, périphériques non maîtrisés
- Cartographie et valeur des données
- Règles d'hygiène ANSSI PME

Jour 3 : Analyse de risque et PSSI PME

- Introduction EBIOS / MEHARI version simplifiée
- Identification des actifs, menaces, scénarios
- Matrice de criticité
- Constitution d'une PSSI : périmètre, objectifs, charte

Jour 4 : Externalisation, innovation, crise

- Cloud : SaaS, IaaS, clauses essentielles, SecNumCloud
- Innovation : protection de la propriété (brevets, recettes)
- Plan de gestion de crise
- Signalement ANSSI, CNIL, contrats, preuves

Jour 5 : Sécurité web, boîte à outils du référent cybersécurité& Projet de synthèse

- WordPress, Prestashop : configuration, failles courantes
- Bases de données : droits, logs, sessions
- Sécurité des paiements : PCI-DSS
- Outils de scan & OSINT : Shodan, WPScan, TheHive

5 Jours
35 Heures

Sur demande

+33 1 89 62 34 30

formation@acgcybersecurity.fr

Campus Cyber, Tour Eria, 5 Rue Bellini 92800 Puteaux, FRANCE

Toutes nos formations sont accessibles aux personnes en situation de handicap.

ACG CyberAcademy 2025