EduGroupe
Accompagner pour réussir

Sécurité informatique : vocabulaire, concepts et technologies pour non-initiés

Référence : **SECINIT** Durée : **2 jours (14 heures)** Certification : **Aucune**

Opcommerce

CONNAISSANCES PRÉALABLE

- Aucun prérequis

PROFIL DES STAGIAIRES

- Commerciaux, spécialistes du marketing, futurs consultants, chefs de projets ou responsables de formation amenés à évoluer dans l'univers de la sécurité informatique
- Toute personne souhaitant comprendre la sécurité informatique pour optimiser leur collaboration avec les spécialistes du domaine

OBJECTIFS

- Comprendre les concepts, les technologies et les solutions de sécurité des réseaux informatiques pour travailler avec les spécialistes et piloter les prestataires
- Acquérir la vision globale de la sécurité Connaître les rôles des intervenants du secteur et leurs métiers
- Identifier les nouveaux enjeux associés à la sécurité informatique

CERTIFICATION PRÉPARÉE

- Aucune

MÉTHODES PÉDAGOGIQUES

- La formation repose sur une pédagogie active, progressive et expérientielle, visant à permettre à des non-spécialistes de s'approprier les concepts de la cybersécurité par la compréhension, la manipulation d'outils, la co-construction et la mise en pratique immédiate des notions
- L'animation alterne apports théoriques vulgarisés, cas concrets issus d'entreprises du commerce et du numérique (TPE/PME notamment), et ateliers collaboratifs qui placent le participant dans une logique d'action plutôt que d'écoute passive. Nous mettons à disposition de chaque participant un poste informatique et une connexion Internet pour se connecter à des labs hébergés dans le cloud
- Chaque séquence se conclut par un quiz ou une mise en situation afin de consolider les apprentissages et favoriser la mémorisation à long terme
- Livrables fournis : Support de cours numérique ; Fiches mémo : terminologie et concepts clés ; Modèle de plan de cybersécurité simplifié ; Sitologie : Guide de l'hygiène de l'ANSSI, MOOC gratuits de l'ANSSI, de la CNIL, de BPIFrance Université, de MS Learn, My Mooc, texte du RGPD, vidéos de sensibilisation SensCyber, AutoDiag, etc."
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

- Consultant-formateur expert en Cybersécurité et sécurité offensive

MÉTHODES D'ÉVALUATION DES ACQUIS

- Évaluations formatives tout au long de la session (quiz, mises en situation, jeux de rôle)
- Évaluation sommative finale : test de positionnement et restitution d'un mini-plan d'action cybersécurité
- Évaluation de la satisfaction à chaud et à froid
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

1. Jour 1 – Fondamentaux et concepts clés (7h)

2. Matin (3h30) – Introduction et culture générale en cybersécurité

- Panorama de la cybersécurité : enjeux économiques, juridiques et humains
- Définitions et vocabulaire essentiel : SI, réseau, serveur, pare-feu, phishing, malware, etc.
- Typologie des menaces : malware, ransomware, ingénierie sociale, usurpation d'identité
- Les acteurs de la cybersécurité : RSSI, SOC, CERT, ANSSI, CNIL, prestataires
- 💡 *Atelier 1 : Identifier les menaces dans un cas réel d'entreprise (analyse de scénario)*

3. Après-midi (3h30) – Technologies et solutions de sécurité

- Fonctionnement des solutions de sécurité : antivirus, pare-feu, IDS/IPS, proxy, VPN, chiffrement
- Introduction à la gestion des identités et des accès (IAM)
- Sauvegardes, PRA/PCA, résilience et continuité d'activité
- Les bases de la protection du réseau et du poste de travail
- 💡 *Atelier 2 : Cartographier les solutions de sécurité d'une TPE/PME*

4. Jour 2 – Gouvernance, référentiels et bonnes pratiques (7h)

5. Matin (3h30) – Piloter la sécurité et travailler avec les experts

- Les politiques et chartes de sécurité
- Les référentiels et normes : ISO 27001, RGPD, NIS2, guides ANSSI
- Les responsabilités partagées entre utilisateurs, prestataires et hébergeurs (cloud, SaaS)
- Sécurité des projets numériques : intégration de la sécurité dès la conception
- 💡 *Atelier 3 : Définir un plan d'action cybersécurité simplifié pour un projet digital*

6. Après-midi (3h30) – Tendances, innovations et synthèse

- Les grandes tendances actuelles : IA, IoT, mobilité, télétravail, souveraineté numérique
- Cyber-assurance et obligations réglementaires
- Veille et sensibilisation : comment rester informé et vigilant
- Synthèse collective et évaluation des acquis
- 💡 *Atelier 4 : Simulation : "Réagir à une attaque ransomware dans mon entreprise"*

Notre référent handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible .