Formation de formateur en cybersécurité

Public visé et Pré requis de la formation : Aucun
Conditions d'accès :Etre majeur
Durée : 4 jours
Heures : 28 h
Nombre maximum de places par session : 12
Délai d'accès à la formation : 15 jours avant le début de la formation
Prix : 1100 € / pers.
Taux de satisfaction : 90%
Accessibilité aux personnes à mobilité réduite : Formation et locaux accessibles aux personnes en situations de handicap. Afin de pouvoir vous accueillir dans les meilleures conditions, un contact avec notre centre de formation est impératif

Actions de formation

OBJECTIFS

Comprendre les concepts fondamentaux de la cybersécuritéAcquérir une connaissance approfondie des menaces, des vulnérabilités et des attaques courantes en cybersécurité.Comprendre le cadre réglementaire et les bonnes pratiques de sécurité.Développer des compétences techniques en cybersécuritéMaîtriser les techniques de protection des réseaux et des systèmes d'information.Savoir identifier et réagir efficacement aux incidents de cybersécurité.Adapter les pratiques de cybersécurité aux métiers de la sécurité privéeIntégrer la cybersécurité aux missions de sécurité physique et privée.Utiliser des outils et des méthodes pour sécuriser les systèmes de surveillance, de contrôle d'accès, etc.Acquérir les compétences pédagogiques pour former efficacement en cybersécuritéDévelopper des programmes de formation adaptés aux besoins des professionnels de la sécurité privée.Maîtriser les techniques d'animation et de communication pour adultes.Concevoir et animer des sessions de formation en cybersécuritéÉlaborer des formations adaptées aux différents niveaux de compétence des participants.Utiliser des exercices pratiques et des études de cas pour renforcer l'apprentissage.

SPÉCIALITÉ

Informatique, traitement de l'information, réseaux de transmission des données

VALIDATION

Attestation de fin de formation

MOYENS PÉDAGOGIQUES ET TECHNIQUES

Supports de coursPrésentations PowerPoint et documents PDF.Vidéos explicatives et démonstrations.Outils et MatérielLaboratoires virtuels et simulateurs pour la pratique des compétences techniques.Ordinateurs avec logiciels de cybersécurité (Wireshark, nmap, etc.).Outils de visioconférence et de collaboration en ligne (pour les participants à distance).Études de cas et exercices pratiquesAnalyse d'incidents réels ou fictifs.Simulations d'attaques et exercices de réponse.Ressources additionnellesArticles, livres blancs, et recommandations de lecture.Accès à des forums et communautés en ligne pour échanges entre participants

QUALIFICATION DE L'INTERVENANT

Professionnels expérimentés du secteur de la cybersécurité et de l'informatique pour partager des retours d'expérience concrets.Encadrement individuel : chaque stagiaire peut bénéficier d'un accompagnement personnalisé pour progresser à son rythme

ÉVALUATION

QCM, tests de connaissance à la fin de chaque module théorique.Évaluations pratiques des compétences sur le terrain avec des grilles d'observation précises si le scénario le prévoit

Contenu pédagogique

Jour 1 : Introduction à la Cybersécurité et Contexte de la Sécurité PrivéeMATIN (3H30)

Introduction à la cybersécurité : Concepts clés et définitions

- Qu'est-ce que la cybersécurité ?
- Principales menaces et types d'attaques (malware, phishing, ransomware, etc.)
- Cadre légal et réglementaire (RGPD, CNIL, etc.)

Panorama des acteurs de la cybersécurité

- Acteurs publics et privés : ANSSI, ENISA, etc.
- Rôles des professionnels de la cybersécurité dans la sécurité privée.

APRES MIDI (3H30)Cybersécurité et sécurité privée

- Implications de la cybersécurité pour les métiers de la sécurité privée.
- Cas pratiques : incidents de cybersécurité dans le secteur privé.

Bases des systèmes de gestion de la sécurité de l'information (SMSI)

- Norme ISO 27001 et sa mise en œuvre.
- Introduction aux politiques et procédures de sécurité.

Atelier pratique : Étude de cas sur une attaque cybernétique

- Analyse d'un incident réel ou fictif affectant une organisation de sécurité privée.
- Discussion de groupe et plan d'amélioration.

Jour 2 : Compétences Techniques de Cybersécurité pour les FormateursMATIN (3H30)

Introduction aux réseaux et systèmes d'information

- Concepts de base des réseaux (protocoles, TCP/IP, DNS, etc.)
- Fonctionnement des systèmes d'information et des infrastructures critiques.

Sécurité des réseaux et des systèmes d'information

- Firewall, VPN, IDS/IPS (Systèmes de détection et de prévention d'intrusion).
- Configuration sécurisée des systèmes et des applications.

APRES MIDI (3H30)

Pratiques de cybersécurité dans la sécurité physique

- Points de convergence entre la sécurité physique et numérique.
- Surveillance vidéo, contrôle d'accès et leur sécurisation.

Atelier technique : Simulations de cyberattaques

- Utilisation d'environnements virtuels pour simuler des attaques.
- Détection et réponse aux incidents (techniques de base).

Exercices de groupe : Sécurisation d’un réseau d’entreprise

- Création de scénarios d'entraînement pour former des agents de sécurité.

Jour 3 : Techniques Pédagogiques pour la Formation en CybersécuritéMATIN (3H30)

Fondamentaux de la pédagogie pour adultes

- Techniques d'apprentissage pour les adultes.
- Styles d'apprentissage et adaptation du contenu.

Conception d'un programme de formation en cybersécurité

- Structurer une formation efficace : modules, objectifs d'apprentissage, évaluations.

APRES MIDI (3H30)

Techniques de présentation et d'animation

- Utilisation d'outils interactifs et multimédia.
- Gestion de groupe et communication efficace.

Atelier pratique : Simulation d’une session de formation

- Chaque participant prépare et anime une mini-session sur un sujet de cybersécurité.
- Feedback et conseils d'amélioration.

Jour 4 : Formation Spécialisée et CertificationMATIN (3H30)

Approfondissement des compétences en cybersécurité pour la sécurité privée

- Analyse des menaces spécifiques au secteur (e.g., attaques contre les systèmes de vidéosurveillance).
- Mesures spécifiques de protection et de réponse.

Évaluation des risques et mise en conformité

- Identifier les risques spécifiques à l'organisation.
- Stratégies de gestion des risques et conformité réglementaire.

APRES MIDI (3H30)

Exercice final : Conception d'un programme de formation sur mesure

- Travail en groupes pour développer un programme de formation adapté à une situation réelle.

Certification et clôture de la formation

- Évaluation finale des participants (quiz, cas pratiques).