PARVENIR
Email : parvenir9@gmail.com
Tel : 06 78 38 04 95

Sensibilisation à la Sécurité

Cette formation vous permettra d'acquérir un niveau d'expertise élevé dans le domaine de la sécurité
Modalité d'accès: 3 semaines après la signature de la convention

Durée: 14.00 heures (2.00 jours)

Profils des apprenants

- Administrateurs de systèmes ainsi que les techniciens chargés du support mais également toute personne impliquée dans la sécurité du système d'information.

Prérequis

- Aucun

Accessibilité et délais d'accès

Si vous êtes porteur d'un handicap merci de bien vouloir contacter isabelle Maleplate référente handicap au 0678380495 afin de pouvoir échanger sur l'adaptation de votre parcours de formation
3 semaines

Qualité et indicateurs de résultats

Pour la période 2023:
Taux de satisfaction des apprenants 0%
Nombre d'apprenants 0%
Taux et causes des abandons 0%
Taux de retour des enquêtes 0%

Objectifs pédagogiques

- A l'issue de la formation, le stagiaire sera capable de :
- Acquérir un niveau d'expertise élevé dans le domaine de la sécurité en réalisant différents scénarios complexes d'attaques
- Définir des solutions de sécurité avancées

Contenu de la formation

- La sécurité informatique : comprendre les menaces et les risques
  - Introduction : cadre général, qu'entend-on par sécurité informatique (menaces, risques, protection) ?
  - Comment une négligence peut-elle créer une catastrophe ? Quelques exemples.
  - La responsabilité.
  - Les composantes d'un SI et leurs vulnérabilités. Systèmes d'exploitation client et serveur. Réseaux d'entreprise (locaux, site à site, accès par Internet). Réseaux sans fil et mobilité.
  - Les applications à risques : Web, messagerie... Base de données et système de fichiers. Menaces et risques.
  - Sociologie des pirates. Réseaux souterrains. Motivations. Typologie des risques. La cybercriminalité en France. Vocabulaire (sniffing, spoofing, smurfing, hijacking...).
- La protection de l'information et la sécurité du poste de travail
  - Vocabulaire. Confidentialité, signature et intégrité. Comprendre les contraintes liées au chiffrement.

PARVENIR
Email : parvenir9@gmail.com
Tel : 06 78 38 04 95

- Schéma général des éléments cryptographiques. Windows, Linux ou MAC OS : quel est le plus sûr ?
- Gestion des données sensibles. La problématique des ordinateurs portables.
- Quelle menace sur le poste client ? Comprendre ce qu'est un code malveillant.
- Comment gérer les failles de sécurité ? Le port USB. Le rôle du firewall client.

- L'authentification de l'utilisateur et les accès de- puis l'extérieur
  - Contrôles d'accès : authentification et autorisation. Pourquoi l'authentification est-elle primordiale ?
  - Le mot de passe traditionnel. Authentification par certificats et token.
  - Accès distant via Internet. Comprendre les VPN. De l'intérêt de l'authentification renforcée.
  - Analyse des risques, des vulnérabilités et des menaces. Les contraintes réglementaires et juridiques.
  - Pourquoi mon entreprise doit respecter ces exigences de sécurité ?
  - Les hommes clés de la sécurité : comprendre le rôle du RSSI et du Risk manager.
  - Agir pour une meilleure sécurité : les aspects sociaux et juridiques. La CNIL, la législation.
  - La cybersurveillance et la protection de la vie privée. La charte d'utilisation des ressources informatiques. La sécurité au quotidien. Les bons réflexes.

Organisation de la formation

Équipe pédagogique
La formation sera assurée par un expert en cyber sécurité

Moyens pédagogiques et techniques

- Questions orales ou écrites (QCM…) Des mises en situation Le formateur évaluera les acquis en utilisant des exercices pratiques à la fin de chaque séquence pédagogique

Dispositif de suivi de l'exécution de l'évaluation des résultats de la formation

- Evaluation des acquis par des exercices de mise en situation

Tarif inter-entreprise par personne HT : 1200.00 €
Tarif intra : nous consulter

Date de création 19 juin 2023

Date de mise à jour 19/06/2023