Fondamentaux de la sécurité - Orienté poste de travail

Mise à jour : Fév. 2024

Durée : 3 jours - 21 heures

OBJECTIFS PÉDAGOGIQUES

- A l'issue de la formation, le stagiaire comprendra les enjeux, les outils et les techniques relatifs à la sécurité informatique.
- Préparation à l'examen MTA 98-367.

PRÉREQUIS

- PUBLIC : Informaticien désirant approfondir et valider ses compétences en sécurité informatique.
- PREREQUIS : Connaissances de base en réseaux IP.

PARTICIPANTS

MOYENS PÉDAGOGIQUES

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de réunion-discussion
- Utilisation de cas concrets issus de l'expérience professionnelle
- Validation des acquis par des questionnaires, des tests d'évaluation, des mises en situation et des jeux pédagogiques
- Remise d'un support de cours

MODALITÉS D'ÉVALUATION

- Feuille de présence signée en demi-journée
- Evaluation des acquis tout au long de la formation
- Questionnaire de satisfaction
- Attestation de stage à chaque apprenant
- Positionnement préalable oral ou écrit
- Evaluation formative tout au long de la formation
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles

MOYENS TECHNIQUES EN PRÉSENTIEL

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard

MOYENS TECHNIQUES DES CLASSES À DISTANCE

- A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur
- Les formations en distanciel sont organisées en Inter-Entreprises comme en Intra-Entreprise
- L'accès à l'environnement d'apprentissage (support de cours, labs) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré
- Les participants reçoivent une invitation avec un lien de connexion
- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition auprès de notre équipe par téléphone au 03 25 80 08 64 ou par mail à secretariat@feep-entreprises.fr

ORGANISATION

- Les cours ont lieu de 9h à 12h30 et de 13h30 à 17h

PROFIL FORMATEUR

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité

ACCESSIBILITÉ

- Les personnes atteintes de handicap souhaitant suivre cette formation sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation. Notre organisme peut vous offrir des possibilités d'adaptation et/ou de compensations spécifiques si elles sont nécessaires à l'amélioration de vos apprentissages

Programme de formation

1 Comprendre les niveaux de sécurité

- Connaître les principes de base de la sécurité
- Sécurité physique
- Sécurité des explorateurs Web
- Comprendre la sécurisation d'un réseau WiFi
- Atelier : QCM ; recherche de définitions sur internet

2 Sécurisation d'un système d'exploitation

- Authentification des utilisateurs
- Cryptage et certificats
- Comprendre les permissions
- Comprendre les stratégies de mots de passe
- Connaître les stratégies d'audit et de surveillance
- Définir les catégories de malware
- Ateliers : QCM ; recherche de définitions sur Internet ; détection de virus.

3 Sécurisation des réseaux

- Comprendre le rôle et les types de parefeux
- Connaître le but de la protection d'accès réseau (NAP)
- Comprendre l'isolation réseau (VLAN, IPSec,...)
- Comprendre la sécurisation des protocoles et les types d'attaques courants.
- Ateliers : Paramétrage et tests du parefeu local ; Suivi d'un scenario de sécurisation.

4 Sécurité logicielle

- Comprendre la sécurisation de postes clients
- Comprendre les outils et techniques de protection des mails
- Comprendre les outils et techniques de protection de serveurs Windows
- Ateliers : QCM ; configuration de l'UAC ; vérification du classement SPAM d'un courriel.