FONDAMENTAUX DE LA SÉCURITÉ - ORIENTÉ POSTE DE TRAVAIL

Durée	**3 jours**	**Référence Formation**	**4-WI-98367**

Objectifs

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.

Participants

Pré-requis

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

Moyens pédagogiques

Accueil des stagiaires dans une salle dédiée à la formation équipée d'un vidéo projecteur, tableau blanc et paperboard ainsi qu'un ordinateur par participant pour les formations informatiques.
Positionnement préalable oral ou écrit sous forme de tests d'évaluation, feuille de présence signée en demi-journée, évaluation des acquis tout au long de la formation.
En fin de stage : QCM, exercices pratiques ou mises en situation professionnelle, questionnaire de satisfaction, attestation de stage, support de cours remis à chaque participant.
Formateur expert dans son domaine d'intervention
Apports théoriques et exercices pratiques du formateur
Utilisation de cas concrets issus de l'expérience professionnelle des participants
Réflexion de groupe et travail d'échanges avec les participants
Pour les formations à distance : Classe virtuelle organisée principalement avec l'outil ZOOM. Assistance technique et pédagogique : envoi des coordonnées du formateur par mail avant le début de la formation pour accompagner le bénéficiaire dans le déroulement de son parcours à distance.

PROGRAMME

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.