CYBERSECURITE – DEFENDRE SON SYSTEME INFORMATIQUE DES MENACES EN LIGNE ET SUR SITE

Durée	2 jours	Référence Formation	4-SE-DEF2

Objectifs
Aider les responsables des TPE et PME à protéger leur entreprise des menaces informatiques.

Participants
Responsable de services informatiques et intervenants techniques (service IT)

Pré-requis
Il est nécessaire d'avoir une réelle connaissance informatique.

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
Accueil et introduction
Présentation de l'objectif du cours
Brève introduction à la cybersécurité

Les menaces en ligne pour les TPM et PME
Les principales menaces en ligne : phishing, ransomware, malware, etc.
Les menaces venant de l'intérieur : virus, vol de données, destruction de données…
Exemples de cas réels de cyberattaques contre les petites entreprises
Les conséquences financières et de réputation des cyberattaques

Bonnes pratiques en Cybersécurité
Utilisation de mots de passe forts et uniques
Cryptage de fichiers
Mises à jour régulières des logiciels
Sensibilisation à l'email et aux pièces jointes suspectes
Sensibilisation aux bonnes pratiques : usb, échanges de documents, gestion des comptes…
Travail à distance et prestataires extérieurs
Accès au réseau en inter, Wi-Fi…

Comment sécuriser mon environnement
Le poste de travail
Outils et conseils pour sécuriser le poste utilisateur (Windows 10/11…)

Suite de la sécurisation du poste client
Rappels des technologies disponibles dans Windows : Antivirus, boot sécurisé…
Sécurisation par GPO
Cryptage de postes et des fichiers
Gestion des certificats

Sécuriser le domaine et Active Directory
Comment bien organiser Active Directory et les GPO
Renforcer la gestion des comptes et des groupes pour éviter les failles

Surveiller Active Directory
Comment surveiller son SI à la recherche d'anomalies
Bonnes pratiques et sources d'informations pour aller plus loin…

Sécuriser mon serveur de fichiers
Bonnes pratiques pour gérer le serveur et les permissions sur les fichiers
Outils pour sécuriser le serveur de fichiers
Gestionnaire de ressources, sysinternals…
Comment surveiller les accès aux fichiers ?

Sécuriser les services réseaux du quotidien
Service DHCP et Serveur DNS : quels risques et quelles solutions ?
Gestion des accès depuis l'extérieur : VPN, Web, Rds…
Gestion du Wifi : accès privé / accès public

Gestion des mises à jour serveurs et postes clients
Mise à jour manuelle ou automatisée
Mise à jour des postes clients : obligatoire / facultative
Mise à jour des serveurs : bonnes pratiques ?

Serveurs d'impressions et serveurs applicatifs
Comment augmenter la sécurité de l'impression
Bonnes pratiques pour les serveurs applicatifs

Prévoir un plan de reprise et de continuité en cas d'attaques ou de panne
Evaluer les risques
Définir les priorités
Assurer la continuité