CYBERSECURITE – SECURISER MES POSTES DE TRAVAIL WINDOWS 10 ET 11

Durée	3 jours	Référence Formation	4-SE-POSTE

Objectifs
Acquérir les connaissances permettant de sécuriser le fonctionnement et l'utilisation des postes clients Windows 10/11 en entreprise.

Participants
Cette formation s'adresse aux administrateurs, aux techniciens et aux responsables de parc informatique en environnement Microsoft
Quel que soit la taille du réseau sur lequel vous intervenez, pour votre compte ou celui de vos clients, enrichissez vos connaissances et appliquez les meilleurs pratiques pour sécuriser vos postes clients Windows 10 et 11 en entreprise

Pré-requis
Connaissances générales de Windows clients (Windows 7 ou plus…)

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
JOUR 1

Mon poste client est-il sécurisé ?
Comment analyser sa propre situation ?
- Quelques méthodes concrètes d'analyse du risque
- Évaluer les priorités des actions à mener sur le terrain par les IT
- Recommandations de l'Anssi
- Recommandations de Microsoft

Sécurisation du système
Gestion de l'authentification
- Description des protocoles NTLM et Kerberos : forces et faiblesses
- Sécurisation des comptes locaux : Laps / bonnes pratiques
- Sécurisation des comptes de domaine par GPO et bonnes pratiques

Contrôle d'accès
- Authentification multiple sur le poste client
- Utilisation de carte à puce virtuelle

Sécurité du boot et de la virtualisation
- Démarrage sécurisé UEFI
- Device Guard : Configuration
- Sécurisation d'Hyper-V

JOUR 2

Renforcement du système par modèle de sécurité
Tour d'horizon des recommandations
Déploiement des modèles de sécurité proposés par Microsoft
Utilisation des outils Microsoft SCM / SCT / ATA / Secedit…

Gestion de Defender
Administration par GPO et mise à jour
Microsoft Defender pour point de terminaison (Microsoft 365 Defender)

Gestion des mises à jour de Windows 10 et 11
Comment maintenir le poste client à jour ? Internet / WSUS / Azure …

Protection des données et cryptage
Déploiement et gestion de BitLocker en entreprise (GPO / AD / Mdbam…)
Gestion des clés et des agents de récupérations / dépannage
Windows Hello entreprise et PDE (win11 22H2)
Cryptage de fichiers EFS et déploiement en entreprise

JOUR 3

Gestion et déploiement des certificats sur le poste client
Tour d'horizon de l'autorité de certification Microsoft
Gestion des applications Appx et du Store localement et par GPO
Restrictions des applications par Applocker et les restrictions logicielles

Sécurisation du réseau
Gestion du pare-feu : localement / GPO
Gestion de la sécurité du wifi
VPN et accès direct
Sécurisation des protocoles commun du réseau : SMB / Rdp / Rpc …

Synthèse sur la protection du poste de travail