Sécuriser mes postes de travail Windows 10 et 11

Mise à jour : 15/01/2026

Durée : 3 jours - 21 heures

OBJECTIFS PÉDAGOGIQUES

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

PRÉREQUIS

- Connaissances générales de Windows Clients (Windows 7 ou plus...)

PARTICIPANTS

- Cette formation s'adresse aux administrateurs, aux techniciens et aux responsables de parc informatique en environnement Microsoft

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.
- Alternance entre apports théoriques et exercices pratiques (en moyenne 30 à 50%)
- Remise d'un support de cours.

MODALITÉS D'ÉVALUATION

- Feuille de présence signée en demi-journée
- Évaluation des acquis tout au long de la formation
- Questionnaire de satisfaction
- Attestation de stage à chaque apprenant
- Positionnement préalable oral ou écrit
- Évaluation formative tout au long de la formation
- Évaluation 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 tableau numérique, d'un tableau blanc et de paperboard

MOYENS TECHNIQUES DES CLASSES À DISTANCE

- À 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 recevront une convocation avec 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

- Notre organisme peut vous offrir des possibilités d'adaptation et/ou de compensations spécifiques si elles sont nécessaires à l'amélioration de vos apprentissages sur l'ensemble de nos formations. Aussi, si vous rencontrez une quelconque difficulté, nous vous invitons à nous contacter directement afin d'étudier ensemble les possibilités pour suivre la formation

Programme de formation

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

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 10/11

- 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 récupération / dépannage
- Windows Hello entreprise et PDE (win11 22H2)
- Cryptage de fichiers EFS et déploiement en entreprise

Gestion et déploiement des certificats sur le poste client

- Tour d'horizon de l'autorité de certification Microsoft
- Comment déployer et administrer la gestion des certificats sur les appareils clients (PC, téléphone...)

Sécurisation des applications et du navigateur

- Déploiement de modèle d'administration par GPO
- 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