Sécuriser mes postes de travail Windows 10 et 11

Informatique

Sécurité logicielle

Référence : 4-SE-POSTE
Durée : 3 jours
Présentiel ou en classe à distance

Tarif Inter : 750 € Prix HT jour / personne
Tarif Intra : 1500 € Prix HT jour / groupe

Mise à jour : 27/11/2023

Durée de validité : du 01/01/2026 au 31/12/2026

Objectifs

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...)

Public concerné

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

Contenu pédagogique

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

Moyens pédagogiques

- Réflexion de groupe et apports théoriques du formateur.
- Travail d'échange avec les apprenants 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 sur 30 à 50% du temps)

Modalités pédagogiques : Présentiel, Distanciel et AFEST

Moyens techniques

En formation présentielle

Accueil des apprenants dans une salle dédiée à la formation et équipée avec :

- Ordinateurs
- Vidéo projecteur ou Écran TV interactif
- Tableau blanc ou Paper-Board

En formation distancielle

A l'aide d'un logiciel comme ® Microsoft Teams ou Zoom, un micro et une caméra pour l'apprenant.

- Suivez une formation en temps réel et entièrement à distance. Lors de la session en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur.
- Les formations en distanciel sont organisées en Inter-Entreprise comme en Intra-Entreprise.
- L'accès à l'environnement d'apprentissage (support de cours, ressources formateur, fichiers d'exercices ...) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.
- Les participants recevront une convocation avec le lien de connexion à la session de formation.
- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 02 35 12 25 55 ou par email à commercial@xxlformation.com

Modalités d'évaluation

- Positionnement préalable oral ou écrit.
- 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
- Evaluation formative tout au long de la formation.
- Evaluation sommative faite par le formateur.

Profil du formateur

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

Adaptation pédagogique et matérielle

Si vous avez besoin d'adaptation matérielle ou pédagogique, merci de prendre contact avec notre référent Handicap par téléphone au 02 35 12 25 55 ou par email à handicap@xxlformation.com

Modalités et délais d'accès à la formation

Les formations sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.

Nos sessions INTER 2026

Sessions de formation à venir :

- Aucune session à venir pour cette formation.

Nos sessions INTRA 2026

Pour organiser cette formation en intra-entreprise, veuillez nous contacter par mail à commercial@xxlformation.com ou par téléphone au 02 35 12 25 55