Sécuriser mes postes de travail Windows 10 et 11

Mise à jour nov. 2023

Durée 3 jours (21 heures)

« Délai d'accès maximum 1 mois »

Prévention / Sécurité

OBJECTIFS PROFESSIONNELS

- 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

PRE-REQUIS

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

MOYENS PEDAGOGIQUES

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de
- 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.
- Remise d'un support de cours.

MODALITES D'EVALUATION

- Feuille de présence signée en demi-journée,
- Evaluation des acquis tout au long de la formation,
- Questionnaire de satisfaction,
- Positionnement préalable oral ou écrit,
- Evaluation formative tout au long de la formation,
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles,
- Sanction finale : Certificat de réalisation, certification éligible au RS selon l'obtention du résultat par le stagiaire

MOYENS TECHNIQUES EN PRESENTIEL

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard. Nous préconisons 8 personnes maximum par action de formation en présentiel

MOYENS TECHNIQUES DES CLASSES EN CAS DE FORMATION DISTANCIELLE

- A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation uniquement synchrone en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et comuniquent 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, labs) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré. Nous préconisons 4 personnes maximum par action de formation en classe à distance

ORGANISATION

- Les cours ont lieu de 9h à 12h30 et de 14h à 17h30.

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.

A L'ATTENTION DES PERSONNES EN SITUATION DE HANDICAP

- Les personnes atteintes de handicap souhaitant suivre cette formation sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation.

Programme de formation

Mon poste client est-il sécurisé ? (01h00)

- 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 (03h00)

- 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 (03h00)

- Tour d'horizon des recommandations
- Déploiement des modèles de sécurité proposés par Microsoft
- Utilisation des outils Microsoft SCM / SCT / ATA / Secedit...

Gestion de Defender (02h00)

- 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 (01h00)

- Comment maintenir le poste client à jour ? Internet / WSUS / Azure...

Protection des données et cryptage (02h00)

- 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 (02h00)

- 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 (03h00)

- 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 (04h00)

- 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 (00h00)