Cybersécurité

Sécuriser mes postes de travail Windows

3 jours (21 heures)

Délai maximum : 2 mois.

Parcours concourant au développement des compétences. Action de formation réalisée en application des articles L 6313-1 et L 6313-2 du Code du travail.

Si vous êtes en situation de handicap, contactez-nous avant le début de votre formation pour que nous puissions vous orienter efficacement et vous accueillir dans les meilleures conditions.

Objectifs pédagogiques

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

Pré-requis

Connaissances générales de Windows clients (Windows 7 ou plus…)

Modalités pédagogiques

Modalités de formation:

- Formation réalisée en présentiel, à distance ou mixte,
- Toutes nos formations peuvent être organisées dans nos locaux ou sur site
- Feuille de présence signée en demi-journée, questionnaires d'évaluation de la satisfaction en fin de stage et 60 jours après, attestation de stage et certificat de réalisation.
- Horaires de la formation: 9h - 12h30 et 13h30 - 17h.
- Les horaires de la formation sont adaptables sur demande.

Moyens pédagogiques

- Formateur expert dans le domaine,
- Mise à disposition d'un ordinateur, d'un support de cours remis à chaque participant,
- Vidéo projecteur, tableau blanc et paperboard,
- Formation basée sur une alternance d'apports théoriques et de mises en pratique
- Formation à distance à l'aide du logiciel Teams pour assurer les interactions avec le formateur et les autres stagiaires, accès aux supports et aux évaluations. Assistance pédagogique afin de permettre à l'apprenant de s'approprier son parcours. Assistance technique pour la prise en main des équipements et la résolution des problèmes de connexion ou d'accès. Méthodes pédagogiques : méthode expositive 50%, méthode active 50%.

Public visé

- 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

Modalités d'évaluation et de suivi

- Evaluation des acquis tout au long de la formation : QCM, mises en situation, TP, évaluations orales…

Programme de formation

JOUR 1

Mon poste client est-il sécurisé ?

Contacts

Notre centre à **Mérignac**
14 rue Euler
33700 MERIGNAC
05 57 92 22 00
contact@afib.fr

Notre centre à **Périgueux**
371 Boulevard des Saveurs,
24660 COULOUNIEIX CHAMIERS
05 64 31 02 15
contact@afib.fr

Sécuriser mes postes de travail Windows

¨ Comment analyser sa propre situation ?
o Quelques méthodes concrètes d'analyse du risque
o Évaluer les priorités des actions à mener sur le terrain par les IT
o Recommandations de l'Anssi
o Recommandations de Microsoft

Sécurisation du système :
¨ Gestion de l'authentification
o Description des protocoles NTLM et Kerberos : forces et faiblesses
o Sécurisation des comptes locaux : Laps / bonnes pratiques
o Sécurisation des comptes de domaine par GPO et bonnes pratiques
¨ Contrôle d'accès
o Authentification multiple sur le poste client
o Utilisation de carte à puce virtuelle
¨ Sécurité du boot et de la virtualisation
o Démarrage sécurisé UEFI
o Device Guard : Configuration
o 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 Défender
¨ 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…)
o Gestion des clés et des agents de récupérations / dépannage
o 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
¨ 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…

Sécuriser mes postes de travail Windows

Synthèse sur la protection du poste de travail

Mise à jour le 06/10/2023