SÉCURISER MES POSTES DE TRAVAIL WINDOWS 10 ET 11

Public	Aux administrateurs, aux techniciens et aux responsables de parc informatique en environnement Microsoft.
Durée	3 jours - 21 heures
Pré-requis	Connaissances générales de Windows clients (Windows 7 ou plus…).
Objectifs	Acquérir les connaissances permettant de sécuriser le fonctionnement et l'utilisation des postes clients Windows 10/11 en entreprise.
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

JOUR 1 : MON POSTE CLIENT EST-IL SÉCURISÉ ?

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

SÉCURISATION DU SYSTÈME :

- 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 365defender)
- 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 récupérations / Dépannage
  - Windows Hello entreprise et PDE (win11 22H2)
- Cryptage de fichiers EFS et déploiement en entreprise

JOUR 2 : 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

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

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Centre de formation
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

Téléphone
04 76 23 20 50 - 06 81 73 19 35

E-mail
contact@audit-conseil-formation.com

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation