SARL ONEO
1025 rue Henri Becquerel
Parc Club du Millénaire, Bât. 27
34000 MONTPELLIER
N° organisme : 91 34 0570434

Nous contacter :
04 67 13 45 45
www.ait.fr
contact@ait.fr

Référence	**4-SE-POSTE**
Durée	**3 jours (21 heures)**
Éligible CPF	**NON**
Mise à jour	**27/11/2023**

Sécuriser mes postes de travail Windows 10 et 11

Objectifs pédagogiques

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

Public concerné

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

Prérequis

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

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,Evaluation des acquis tout au long de la formation,
- Questionnaire de satisfaction,
- Attestation de stage à chaque apprenant,
- 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

Moyens techniques en présentiel

Accueil des stagiaires dans une salle dédiée à la formation équipée à minima d'un vidéo projecteur et d'un tableau blanc et/ou paperboard.

Pour les formations nécessitant un ordinateur, un PC est mis à disposition de chaque participant.

Moyens techniques en distanciel

A l'aide d'un logiciel (Teams, Zoom...), d'un micro et éventuellement d'une caméra les apprenants interagissent et communiquent entre eux et avec le formateur.

Sessions organisées en inter comme en intra entreprise.

L'accès à l'environnement d'apprentissage ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.

Pour toute question avant et pendant le parcours, assistance technique à disposition au 04 67 13 45 45.

Organisation

Délai d'accès : 5 jours ouvrés
(délai variable en fonction du financeur)

Les cours ont lieu de 9h à 12h30 et de 13h30 à 17h

Accessibilité

Les personnes en situation d'handicap sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation.

Pour tout renseignement, notre référent handicap reste à votre disposition : mteyssedou@ait.fr

Profil formateur

Formateur expert du domaine.

Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité.

Certification possible

Aucune

Sécuriser mes postes de travail Windows 10 et 11

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