Sécuriser mes poste de travail Windows 10 et versions supérieures

Plan de cours N° : 1299

Durée : 3 jours (21h)

PARTICIPANTS / PRE-REQUIS

Administrateurs, techniciens et responsables de parc informatique en environnement Microsoft

Avoir des connaissances générales de Windows clients (Windows 7 ou plus)

OBJECTIFS PEDAGOGIQUES

Analyser et sécuriser son système (authentification, contrôle d'accès...). Renforcer le système par modèle de sécurité. Gérer Defender. Protéger et crypter les données. Gérer et déployer des certificats. Sécuriser le navigateur et les applications. Sécuriser le réseau.

MOYENS PEDAGOGIQUES

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 exercices de synthèse
Alternance entre apports théoriques et exercices pratiques (en moyenne 30 et 70%)
Remise d'un support de cours.
Assistance post-formation d'une durée de 1 an sur le contenu de la formation via notre adresse mail dédiée formateurs@atp-formation.com

MOYENS PERMETTANT LE SUIVI DE L'EXECUTION ET DES RESULTATS

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 PRESENTIEL

Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc

MOYENS TECHNIQUES DES CLASSES A DISTANCE

A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant, suivez une formation en temps réel et entièrement à distance. Lors de la classe 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, labs) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.
Les participants recevront une convocation avec lien de connexion
Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par mail et par téléphone auprès de notre équipe par téléphone au 04.76.41.14.20 ou par mail à contact@atp-formation.com

ORGANISATION

Les cours ont lieu de 9h00-12h30 13h30-17h00

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.

ACCESSIBILITE

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.

MISE A JOUR

10/07/2023

31, av. du Granier
38240 Meylan
Tél. 04 76 41 14 20
Fax 04 76 41 38 45

SARL au capital de 120 000€ - 390 032 050 RCS GRENOBLE
SIRET 390 032 050 00010 - APE 8559A - TVA Intracom. FR03390032050

Sécuriser mes poste de travail Windows 10 et versions supérieures

Plan de cours N° : 1299

Durée : 3 jours (21h)

MON POSTE CLIENT EST-IL SECURISE ?

- 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

SECURISATION DU SYSTEME

- Gestion de l'authentification
  - Description des protocoles NTLM et Kerberos : forces et faiblesses
  - Sécurisation des comptes locaux : Laps / bonnes pratiques
  - Sécurisation des comptes de domaines 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/autres versions
  - Comment maintenir le poste client à jour ? Internet / WSUS / Azure...

PROTECTION DES DONNEES 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 fichers EFS et déploiement en entreprise

GESTION ET DEPLOIEMENT DES CERTIFICATS SUR LE POSTE CLIENT

- Tour d'horizon de l'autorité de certifcation Microsoft
- Comment déployer et administrer la gestion des certificats sur les appareils clients (PC, téléphone...)

SECURISATION 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

SECURISATION DU RESEAU

- 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...

SYNTHESE SUR LA PROTECTION DU POSTE DE TRAVAIL

31, av. du Granier
38240 Meylan
Tél. 04 76 41 14 20
Fax 04 76 41 38 45

SARL au capital de 120 000€ - 390 032 050 RCS GRENOBLE
SIRET 390 032 050 00010 - APE 8559A - TVA Intracom. FR03390032050