

Plan de cours N° : 1300

Durée : 2 jours (14h)

PARTICIPANTS / PRE-REQUIS

Administrateurs, techniciens et responsables de parc informatique en environnement Microsoft
Connaissances générales de Windows et de l'environnement Active Directory Microsoft

OBJECTIFS PEDAGOGIQUES

Sécuriser des comptes utilisateurs. Gérer des comptes utilisateurs. Sécuriser le contrôleur de domaine. Synchroniser l'annuaire avec le nuage. Surveiller l'AD et gérer les alertes.

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

Plan de cours N° : 1300

Durée : 2 jours (14h)

ANALYSER DES RISQUES ET DES ATTAQUES SPECIFIQUES AU SI ET A L'AD

- Tour d'horizon des risques et des attaques les plus communes
 - Sources d'informations
- Normes et bonnes pratiques proposées : Microsoft / ANSSI

SECURISATION DES OBJETS DE L'ANNUAIRE

- Sécurisation des comptes d'utilisateurs
 - Sécurisation des comptes d'utilisateurs et des services
 - Comptes d'utilisateurs protégés
 - Comptes de services "managés"
- Gestion des comptes d'ordinateurs et délégation
 - Gestion des groupes privilégiés et sensibles
 - Gestion des droits des utilisateurs et des services
- Délégation d'administration pour protéger le SI
 - Gestion des privilèges
 - Délégation et administration avec privilège minimum (JEA)

SECURISER LE CONTROLEUR DE DOMAINE

- Gestion de la sécurité par des contrôleurs multiples
- Sauvegarde et Restauration
- RODC / AD LDS
- Microsoft Azure et la synchronisation de l'annuaire avec le nuage
 - Scénario de synchronisation AD avec Azure
 - Gestion des groupes et des comptes utilisateurs
 - Approche sécuritaire

DESCRIPTION AVANCEE DES PROTOCOLES NTLM ET KERBEROS

- NTLM 1 et 2 : quelles failles possibles ?
- Kerberos : forces et délégation de contraintes
- Description des méthodes et outils d'attaques possibles

ANALYSE DES COMPTES PROTEGES ET SENSIBLES DE L'ACTIVE DIRECTORY

- Comptes protégés du système
- Groupes protégés du système

COMMENT SURVEILLER L'AD ET ETRE ALERTE ?

- Les outils disponibles dans Windows : audit / powershell...
 - Etre alerté d'un danger potentiel
- Autres outils de centralisation des évènements et des logs
- Plan de reprise ou de continuité de service en cas de compromission