

Sécurisation de Microsoft Active Directory (toutes versions)



OBJECTIFS PEDAGOGIQUES

- Acquérir les connaissances permettant de renforcer la sécurisation d'Active Directory (toutes versions)



PUBLIC CONCERNE

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



PREREQUIS

- Connaissances générales de Windows, et de l'environnement Active Directory Microsoft.



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 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.



MODALITES D'EVALUATION

- 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 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



ACCESSIBILITE

- Les personnes en situation de 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

- Nos formateurs sont des experts dans leurs domaines d'intervention
- Leur expérience de terrain et leurs qualités pédagogiques constituent un gage de qualité.



CERTIFICATION POSSIBLE

- Aucune

Sécurisation de Microsoft Active Directory (toutes versions)

JOUR 1

SECURISER SON ACTIVE DIRECTORY... BIEN SUR, MAIS COMMENT ?

ANALYSE 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 de services
 - Compte d'utilisateurs protégés
 - Compte 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 privilèges 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

JOUR 2 :

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...
 - Être alerté d'un danger potentiel
- Autres outils de centralisation des événements et des logs
- Plan de reprise ou de continuité de services en cas de compromission
 - C'est arrivé ! Il me faut du temps pour réparer... Quelle est ma stratégie pendant cette période ?