Sécurisation de Microsoft Active Directory (toutes versions)

Mise à jour nov. 2023

Durée 2 jours (14 heures)

« Délai d'accès maximum 1 mois »

OBJECTIFS PROFESSIONNELS

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

PARTICIPANTS

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

PRE-REQUIS

- 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
- 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.
- 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,
- 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,
- Sanction finale : Certificat de réalisation, certification éligible au RS selon l'obtention du résultat par le stagiaire

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 et de paperboard. Nous préconisons 8 personnes maximum par action de formation en présentiel

MOYENS TECHNIQUES DES CLASSES EN CAS DE FORMATION DISTANCIELLE

- A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation uniquement synchrone en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et comuniquent 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. Nous préconisons 4 personnes maximum par action de formation en classe à distance

ORGANISATION

- Les cours ont lieu de 9h à 12h30 et de 14h à 17h30.

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.

A L'ATTENTION DES PERSONNES EN SITUATION DE HANDICAP

- 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.

Programme de formation

Sécuriser son Active Directory… bien sûr, mais comment ? (00h45)

Analyse des risques et des attaques spécifiques au SI et à l'AD… (01h30)

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

Sécurisation des objets de l'annuaire (02h30)

- Sécurisation des comptes 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)

Sécuriser le contrôleur de domaine (03h15)

- 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 avancée des protocoles NTLM et Kerberos (02h30)

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

Analyse des comptes protégés et sensibles de l'Active Directory (01h30)

- Comptes protégés du système
- Groupes protégés du système

Comment surveiller l'AD et être alerté ? (02h30)

- Les outils disponibles dans Windows : audit / powershell…
- Être alerté d'un danger potentiel
- Autres outils de centralisation des évènements 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 ?