Sécurisation de Microsoft Active Directory (toutes versions)

Informatique

Sécurité logicielle

Référence : 4-SE-MAD
Durée : 2 jours
Présentiel ou en classe à distance

Tarif Inter : 750 € Prix HT jour / personne
Tarif Intra : 1500 € Prix HT jour / groupe

Mise à jour : 27/11/2023

Durée de validité : du 01/01/2026 au 31/12/2026

Objectifs

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

Prérequis

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

Public concerné

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

Contenu pédagogique

Sécuriser son Active Directory… bien sûr, mais comment ?

Analyse des risques et des attaques spécifiques au SI et à l'AD…

- 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

- 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

- 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

- 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

- Comptes protégés du système
- Groupes protégés du système

Comment surveiller l'AD et être alerté ?

- 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 ?

Moyens pédagogiques

- Réflexion de groupe et apports théoriques du formateur.
- Travail d'échange avec les apprenants 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 sur 30 à 50% du temps)

Modalités pédagogiques : Présentiel, Distanciel et AFEST

Moyens techniques

En formation présentielle

Accueil des apprenants dans une salle dédiée à la formation et équipée avec :

- Ordinateurs
- Vidéo projecteur ou Écran TV interactif
- Tableau blanc ou Paper-Board

En formation distancielle

A l'aide d'un logiciel comme ® Microsoft Teams ou Zoom, un micro et une caméra pour l'apprenant.

- Suivez une formation en temps réel et entièrement à distance. Lors de la session 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, ressources formateur, fichiers d'exercices ...) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.
- Les participants recevront une convocation avec le lien de connexion à la session de formation.
- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 02 35 12 25 55 ou par email à commercial@xxlformation.com

Modalités d'évaluation

- Positionnement préalable oral ou écrit.
- 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
- Evaluation formative tout au long de la formation.
- Evaluation sommative faite par le formateur.

Profil du formateur

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

Adaptation pédagogique et matérielle

Si vous avez besoin d'adaptation matérielle ou pédagogique, merci de prendre contact avec notre référent Handicap par téléphone au 02 35 12 25 55 ou par email à handicap@xxlformation.com

Modalités et délais d'accès à la formation

Les formations sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.

Nos sessions INTER 2026

Sessions de formation à venir :

- Aucune session à venir pour cette formation.

Nos sessions INTRA 2026

Pour organiser cette formation en intra-entreprise, veuillez nous contacter par mail à commercial@xxlformation.com ou par téléphone au 02 35 12 25 55