SÉCURISATION DE MICROSOFT ACTIVE DIRECTORY

Public	Cette formation s'adresse aux administrateurs, aux techniciens et aux responsables de parc informatique en environnement Microsoft.
Durée	2 jours - 14 heures
Pré-requis	Connaissances générales de Windows, et de l'environnement Active Directory Microsoft.
Objectifs	Acquérir les connaissances permettant de renforcer la sécurisation d'Active Directory (toutes versions).
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

1. JOUR 1 : ANALYSE DES RISQUES ET DES ATTAQUES SPÉCIFIQUES AU SI ET À L'AD…

- 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

2. SÉCURISATION DES OBJETS DE L'ANNUAIRE

- Sécurisation des comptes d'utilisateurs
  - Sécurisation des comptes d'utilisateurs et de services
  - Compte 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 privilèges minimum (JEA)

3. : 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 lenuage
  - Scénario de synchronisation AD avec Azure
  - Gestion des groupes et des comptes utilisateurs
  - Approche sécuritaire

4. JOUR 2 : 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…

5. : ANALYSE DES COMPTES PROTÉGÉS ET SENSIBLES DE L'ACTIVE DIRECTORY

- Comptes protégés du système
- Groupes protégés du système

6. : 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 service en cas de compromission
  - C'est arrivé ! Il me faut du temps pour réparer… Quelle est ma stratégie pendant cette période ?

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Centre de formation
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

Téléphone
04 76 23 20 50 - 06 81 73 19 35

E-mail
contact@audit-conseil-formation.com

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation