SÉCURISATION DE MICROSOFT ACTIVE DIRECTORY (TOUTES VERSIONS)

Durée	**2 jours**	**Référence Formation**	**4-SE-MAD**

Objectifs
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.

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

Moyens pédagogiques
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

PROGRAMME
Sécuriser son Active Directory… bien sûr, mais comment ?
- Tour d'horizon des risques et des attaques les plus communes
- Sources d'informations
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"
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