CYBERSECURITE – SECURISATION DE MICROSOFT ACTIVE DIRECTORY

Durée	1/2 jour	Référence Formation	4-SE-MAD

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

Participants
Cette formation d'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
Accueil des stagiaires dans une salle dédiée à la formation équipée d'un vidéo projecteur, tableau blanc et paperboard ainsi qu'un ordinateur par participant pour les formations informatiques.
Positionnement préalable oral ou écrit sous forme de tests d'évaluation, feuille de présence signée en demi-journée, évaluation des acquis tout au long de la formation.
En fin de stage : QCM, exercices pratiques ou mises en situation professionnelle, questionnaire de satisfaction, attestation de stage, support de cours remis à chaque participant.
Formateur expert dans son domaine d'intervention
Apports théoriques et exercices pratiques du formateur
Utilisation de cas concrets issus de l'expérience professionnelle des participants
Réflexion de groupe et travail d'échanges avec les participants

Pour les formations à distance : Classe virtuelle organisée principalement avec l'outil ZOOM. Assistance technique et pédagogique : envoi des coordonnées du formateur par mail avant le début de la formation pour accompagner le bénéficiaire dans le déroulement de son parcours à distance.

PROGRAMME
JOUR 1 – Sécuriser son Active Directory

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 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)

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

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…

Analyse des comptes protégés et sensibles de l'Active Directory
Comptes protégés du système
Groupes protégés du système

Comment surveiller l'AD et être alerte ?
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 ?