SÉCURISER MES SERVEURS MICROSOFT ET MON SI

Durée	**4 jours**	**Référence Formation**	**4-SE-SERV**

Objectifs

Réduire l'exposition aux risques
Gérer et administrer selon les meilleures pratiques
Protéger et défendre son système d'information et ses serveurs concrètement sur le terrain

Participants

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

Pré-requis

Une réelle connaissance informatique est nécessaire

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

Mon réseau est-il fiable ?
- Comment analyser sa propre situation ?
- Quelques méthodes concrètes d'analyse du risque.
- Évaluer les priorités
- Mettre en perspectives les actions à mener sur le terrain par les IT

Sécurisation de l'OS du serveur :
- Version Core / Nano / Conteneur / Version avec ou sans interface graphique ? Standard ou Datacenter ?

Quel OS Microsoft pour quel usage ?
- Rappel des technologies disponibles pour l'environnement Microsoft Serveur
- Virtualisation / Cluster...

Et la haute disponibilité dans tout ça ?
- Modèles d'administration
- Modèles de sécurité : SCM / SCT
- GPO
- Device Guard et Credential Guard
- Bonnes pratiques
- Normes et règles : Microsoft / Anssi
- Sources d'informations sur le Web

Les outils de sécurisation à ma disposition :
- Comment obtenir et déployer les MaJ de l'OS : conseils, bonnes pratiques et outils disponibles...

Maintenir son OS à jour :
- Comment utiliser l'administration "juste à temps" sur mon parc ?
- Mise en oeuvre

Administration "Juste à temps"
- Sauvegarde et restauration
- RODC
- AD LDS

Forêt Bastion
- Normes et bonnes pratiques : Microsoft / Anssi
- Gestion des privilèges
- Délégation et administration avec privilèges minimum
- Authentification robuste et sécurisation d'accès au contrôleur de domaine
- Gestion des "droits d'utilisateurs et des services"
- Gestion des comptes d'ordinateurs et de services
- Gestion des groupes pour une meilleure sécurité

PowerShell et la sécurité
- Les outils disponibles dans Windows : audit / powershell...
- Être alerté d'un danger potentiel
- Des outils tiers possibles

Sécuriser son Active Directory... bien sûr, mais comment ?
- C'est arrivé ! Il me faut du temps pour réparer... Quelle est ma stratégie pendant cette période ?

Analyse des risques et des attaques spécifiques au SI et à l'AD...
- Scénario de synchronisation AD avec Azure
- Gestion des groupes et des comptes utilisateurs
- Approche sécuritaire

Sécuriser le contrôleur de domaine
- Articles Microsoft
- Articles de l'Anssi

Réduction de la surface d'attaque de l'annuaire
- Tour d'horizon des certificats les plus utilisés : authentification / cryptage... / Rds / Exchange...
- Installation et administration de l'autorité de certification Microsoft
- Mise en œuvre concrètes des certificats

Surveillance de l'AD à la recherche d'attaques
- Applocker
- WDAC
- Le cas de messagerie Exchange
- Le cas de l'environnement RDS

Plan de reprise ou de continuité de service en cas de compromission
- Durcissement des protocoles utiles : Smb, Rdp, ...
- Cryptage de trafic réseau : IPSEC / SMB...
- Sécurisation du DHCP
- Sécurisation du DNS
- Pare-feu
- Serveur Radius et NPS / Contrôle d'accès réseau

Microsoft Azure et la synchronisation de l'annuaire avec le nuage
- Filtrage - Quotas - Gestionnaire de rapports
- Classification de données et tâches de gestion de fichiers
- Chiffrement : EFS / BitLocker / Partage de fichiers chiffrés
- Surveillance de l'accès aux fichiers et alertes
- Gestion des permissions
- Bonnes pratiques d'administration
- Haute disponibilité : Cluster / DFS / ...

Sources d'information pour la sécurisation de l'AD : normes et bonnes pratiques
- Machines virtuelles blindées
- Host Guardian Service