# Sécuriser mes serveurs Microsoft et mon SI

*Mise à jour : Fév. 2024*

**Durée :** 4 jours - 28 heures

**OBJECTIFS PÉDAGOGIQUES**

- 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

**PRÉREQUIS**

- Une réelle connaissance informatique est nécessaire

**PARTICIPANTS**

- Cette formation s'adresse aux administrateurs, aux techniciens et aux responsables de parc informatique en environnement 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
- Remise d'un support de cours

**MODALITÉS D'ÉVALUATION**

- 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
- Positionnement préalable oral ou écrit
- Evaluation formative tout au long de la formation
- Evaluation sommative faite par le formateur ou à l'aide des certifications disponibles

**MOYENS TECHNIQUES EN PRÉSENTIEL**

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard

**MOYENS TECHNIQUES DES CLASSES À DISTANCE**

- A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et communiquent entre eux et avec le formateur
- Les formations en distanciel sont organisées en Inter-Entreprises comme en Intra-Entreprise
- L'accès à l'environnement d'apprentissage (support de cours, labs) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré
- Les participants reçoivent une invitation avec un lien de connexion
- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition auprès de notre équipe par téléphone au 03 25 80 08 64 ou par mail à secretariat@feep-entreprises.fr

**ORGANISATION**

- Les cours ont lieu de 9h à 12h30 et de 13h30 à 17h

**PROFIL FORMATEUR**

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

**ACCESSIBILITÉ**

- Les personnes atteintes de handicap souhaitant suivre cette formation sont invitées à nous contacter directement, afin d'étudier ensemble les possibilités de suivre la formation. Notre organisme peut vous offrir des possibilités d'adaptation et/ou de compensations spécifiques si elles sont nécessaires à l'amélioration de vos apprentissages

# Programme de formation

**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 :**

**Quel OS Microsoft pour quel usage ?**

- Quel OS Microsoft pour quel usage ?
- Version Core / Nano / Conteneur / Version avec ou sans interface graphique ? Standard ou Datacenter ?

**Et la haute disponibilité dans tout ça ?**

- Rappel des technologies disponibles pour l'environnement Microsoft Serveur
- Virtualisation / Cluster...

**Les outils de sécurisation à ma disposition :**

- 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

**Maintenir son OS à jour :**

- Comment obtenir et déployer les MaJ de l'OS : conseils, bonnes pratiques et outils disponibles...

**Administration "Juste à temps"**

- Comment utiliser l'administration "juste à temps" sur mon parc ?
- Mise en œuvre

**Forêt Bastion**

**PowerShell et la sécurité**

- PowerShell et la sécurité

**Sécuriser son Active Directory... bien sûr, mais comment ?**

- Sécuriser son Active Directory... bien sûr, mais comment ?

**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...

**Sécuriser le contrôleur de domaine**

- Sécuriser le contrôleur de domaine
- Sauvegarde et restauration
- RODC
- AD LDS

**Réduction de la surface d'attaque de l'annuaire**

- 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

**Surveillance de l'AD à la recherche d'attaques**

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

**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 ?

**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

**Sources d'information pour la sécurisation de l'AD : normes et bonnes pratiques**

- Articles Microsoft
- Articles de l'Anssi

**Gestion des certificats dans Windows**

- 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

**Sécurisation d'un serveur applicatif**

- Applocker
- WDAC
- Le cas de messagerie Exchange
- Le cas de l'environnement RDS

**Sécurisation des services réseaux**

- 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

**Sécurisation du serveur de fichiers**

- 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 / ...

**Sécurisation de la virtualisation**

- Machines virtuelles blindées
- Host Guardian Service

**Synthèse sur la protection de notre SI**