Sécuriser mes serveurs Microsoft et mon SI

Mise à jour nov. 2023

Durée 4 jours (28 heures)

« Délai d'accès maximum 1 mois »

OBJECTIFS PROFESSIONNELS

- 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.

PRE-REQUIS

- Une réelle connaissance informatique est nécessaire

MOYENS PEDAGOGIQUES

- Réflexion de groupe et apports théoriques du formateur
- Travail d'échange avec les participants sous forme de
- 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.

MODALITES D'EVALUATION

- Feuille de présence signée en demi-journée,
- Evaluation des acquis tout au long de la formation,
- Questionnaire de satisfaction,
- 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,
- Sanction finale : Certificat de réalisation, certification éligible au RS selon l'obtention du résultat par le stagiaire

MOYENS TECHNIQUES EN PRESENTIEL

- Accueil des stagiaires dans une salle dédiée à la formation, équipée d'ordinateurs, d'un vidéo projecteur d'un tableau blanc et de paperboard. Nous préconisons 8 personnes maximum par action de formation en présentiel

MOYENS TECHNIQUES DES CLASSES EN CAS DE FORMATION DISTANCIELLE

- A l'aide d'un logiciel comme Teams, Zoom etc... un micro et éventuellement une caméra pour l'apprenant,
- suivez une formation uniquement synchrone en temps réel et entièrement à distance. Lors de la classe en ligne, les apprenants interagissent et comuniquent entre eux et avec le formateur.
- Les formations en distanciel sont organisées en Inter-Entreprise 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. Nous préconisons 4 personnes maximum par action de formation en classe à distance

ORGANISATION

- Les cours ont lieu de 9h à 12h30 et de 14h à 17h30.

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.

A L'ATTENTION DES PERSONNES EN SITUATION DE HANDICAP

- 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.

Programme de formation

Mon réseau est-il fiable ? (02h30)

- 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 : (00h30)

Quel OS Microsoft pour quel usage ? (00h30)

- Version Core / Nano / Conteneur / Version avec ou sans interface graphique ? Standard ou Datacenter ?

Et la haute disponibilité dans tout ça ? (01h00)

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

Les outils de sécurisation à ma disposition : (03h15)

- 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 : (00h30)

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

Administration "Juste à temps" (01h00)

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

Forêt Bastion (00h30)

PowerShell et la sécurité (00h30)

Sécuriser son Active Directory... bien sûr, mais comment ? (00h30)

Analyse des risques et des attaques spécifiques au SI et à l'AD... (02h30)

Sécuriser le contrôleur de domaine (01h30)

- Sauvegarde et restauration
- RODC
- AD LDS

Réduction de la surface d'attaque de l'annuaire (03h15)

- 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 (01h30)

- 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 (00h30)

- 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 (01h30)

- 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 (01h00)

- Articles Microsoft
- Articles de l'Anssi

Gestion des certificats dans Windows (01h30)

- 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 (02h00)

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

Sécurisation des services réseaux (02h45)

- 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 (03h15)

- 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 (01h00)

- Machines virtuelles blindées
- Host Guardian Service

Synthèse sur la protection de notre SI (00h00)