Sécuriser mes serveurs Microsoft et mon SI

Hard Skills : Bureautique - Informatique -Comptabilité - Gestion

Informatique

Référence : 4-SE-SERV
Durée : 4 jours
Présentiel ou en classe à distance

Tarif Inter : 750 € Prix HT jour / personne
Tarif Intra : 1500 € Prix HT jour / groupe

Mise à jour : 27/11/2023

Durée de validité : du 01/01/2025 au 31/12/2025

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

Prérequis

Une réelle connaissance informatique est nécessaire

Public concerné

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

Contenu pédagogique

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 oeuvre

Forêt Bastion

Sécurité

- PowerShell et la sécurité
- Sécuriser son Active Directory… bien sûr, mais comment ?
- 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

Moyens pédagogiques

- Réflexion de groupe et apports théoriques du formateur.
- Travail d'échange avec les apprenants 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 sur 30 à 50% du temps)

Modalités pédagogiques : Présentiel, Distanciel et AFEST

Moyens techniques

En formation présentielle

Accueil des apprenants dans une salle dédiée à la formation et équipée avec :

- Ordinateurs
- Vidéo projecteur ou Écran TV interactif
- Tableau blanc ou Paper-Board

En formation distancielle

A l'aide d'un logiciel comme ® Microsoft Teams ou Zoom, un micro et une caméra pour l'apprenant.

- Suivez une formation en temps réel et entièrement à distance. Lors de la session en ligne, les apprenants interagissent et communiquent 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, ressources formateur, fichiers d'exercices …) ainsi qu'aux preuves de suivi et d'assiduité (émargement, évaluation) est assuré.
- Les participants recevront une convocation avec le lien de connexion à la session de formation.
- Pour toute question avant et pendant le parcours, une assistance technique et pédagogique est à disposition par téléphone au 02 35 12 25 55 ou par email à commercial@xxlformation.com

Modalités d'évaluation

- Positionnement préalable oral ou écrit.
- 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
- Evaluation formative tout au long de la formation.
- Evaluation sommative faite par le formateur.

Profil du formateur

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

Adaptation pédagogique et matérielle

Si vous avez besoin d'adaptation matérielle ou pédagogique, merci de prendre contact avec notre référent Handicap par téléphone au 02 35 12 25 55 ou par email à handicap@xxlformation.com

Modalités et délais d'accès à la formation

Les formations sont disponibles selon les modalités proposées sur la page programme. Les inscriptions sont possibles jusqu'à 48 heures ouvrées avant le début de la formation. Dans le cas d'une formation financée par le CPF, ce délai est porté à 11 jours ouvrés.

Sessions de formation à venir :

- Aucune session à venir pour cette formation.

Pour organiser cette formation en intra-entreprise, veuillez nous contacter par mail à commercial@xxlformation.com ou par téléphone au 02 35 12 25 55