Cybersécurité

Sécuriser mes serveurs Microsoft et mon SI

4 jours (28 heures)

Délai maximum : 2 mois.

Parcours concourant au développement des compétences. Action de formation réalisée en application des articles L 6313-1 et L 6313-2 du Code du travail.

Si vous êtes en situation de handicap, contactez-nous avant le début de votre formation pour que nous puissions vous orienter efficacement et vous accueillir dans les meilleures conditions.

Objectifs pédagogiques

- Réduire l'exposition aux risques
- Renforcer la sécurité de son SI et de ses serveurs Windows (toutes versions)
- Gérer et administrer selon les meilleurs pratiques
- Protéger et défendre son système d'information et ses serveurs concrètement sur le terrain
- Cette formation vous propose des méthodes, des outils et des connaissances, pour sécuriser votre environnement et rendre vos serveurs et votre réseau plus robustes et plus sûrs.

Pré-requis

Connaissances générales de Windows Serveur et d'Active Directory

Modalités pédagogiques

Modalités de formation:

- Formation réalisée en présentiel, à distance ou mixte,
- Toutes nos formations peuvent être organisées dans nos locaux ou sur site
- Feuille de présence signée en demi-journée, questionnaires d'évaluation de la satisfaction en fin de stage et 60 jours après, attestation de stage et certificat de réalisation.
- Horaires de la formation: 9h - 12h30 et 13h30 - 17h.
- Les horaires de la formation sont adaptables sur demande.

Moyens pédagogiques

- Formateur expert dans le domaine,
- Mise à disposition d'un ordinateur, d'un support de cours remis à chaque participant,
- Vidéo projecteur, tableau blanc et paperboard,
- Formation basée sur une alternance d'apports théoriques et de mises en pratique
- Formation à distance à l'aide du logiciel Teams pour assurer les interactions avec le formateur et les autres stagiaires, accès aux supports et aux évaluations. Assistance pédagogique afin de permettre à l'apprenant de s'approprier son parcours. Assistance technique pour la prise en main des équipements et la résolution des problèmes de connexion ou d'accès. Méthodes pédagogiques : méthode expositive 50%, méthode active 50%.

Public visé

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

Modalités d'évaluation et de suivi

- Evaluation des acquis tout au long de la formation : QCM, mises en situation, TP, évaluations orales...

Programme de formation

JOUR 1

Contacts

Notre centre à **Mérignac**
14 rue Euler
33700 MERIGNAC
05 57 92 22 00
contact@afib.fr

Notre centre à **Périgueux**
371 Boulevard des Saveurs,
24660 COULOUNIEIX CHAMIERS
05 64 31 02 15
contact@afib.fr

Sécuriser mes serveurs Microsoft et mon SI

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 ?
o Version Core / Nano / Conteneur / Version avec ou sans interface graphique ? Standard ou Datacenter ?
¨ Et la haute disponibilité dans tout ça ?
o Rappel des technologies disponibles pour l'environnement Microsoft Serveur
o 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
o Normes et règles : Microsoft / Anssi…
o 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…

JOUR 2
Sécuriser son Active Directory… bien sûr, mais comment ?

Analyse des risques et des attaques spécifiques au SI et à l'AD…
¨ Tour d'horizon des risques et des attaques spécifiques au SI et à l'AD…
o Sources d'informations
¨ Normes et bonnes pratiques proposées : Microsoft / Anssi

Sécuriser le contrôleur de domaine
¨ Gestion de la sécurité par des contrôleurs multiples
¨ Sauvegarde et restauration
¨ RODC / AD LDS

Sécurisation des objets de l'annuaire
¨ Sécurisation des comptes utilisateurs
o Sécurisation des comptes utilisateurs et de services
o Compte d'utilisateurs protégés
o Comptes de services « managés »
¨ Gestion des comptes d'ordinateurs et délégation
o Gestion des groupes privilégiés et sensibles
o Gestion des droits des utilisateurs et des services
¨ Délégation d'administration pour protéger le SI
o Gestion des privilèges
o Délégation et administration avec privilèges minimum (JEA)

JOUR 3

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…

Sécuriser mes serveurs Microsoft et mon SI

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

Comment surveiller l'AD et être alerté ?
¨ Les outils disponibles dans Windows : audit / powershell…
o Être alerté d'un danger potentiel
¨ Autres outils de centralisation des évènements et des logs
¨ Plan de reprise ou de continuité de service en cas de compromission
o C'est arrivé ! Il me faut du temps pour réparer… Quelle est ma stratégie pendant cette période ?

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 du serveur de fichiers
¨ Filtrage – Quotas – Gestionnaires 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 /…

JOUR 4

Sécurisation d'un serveur applicatif
¨ Applocker
¨ Restriction logicielle
¨ 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

Synthèse sur la protection de notre SI