Cybersécurité

Sécurisation de Microsoft Active Directory

2 jours (14 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

Acquérir les connaissances permettant de renforcer la sécurisation d'Active Directory (toutes versions)

Pré-requis

Connaissances générales de Windows, et de l'environnement Active Directory Microsoft.

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

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 les plus communes

o Sources d'informations

¨ Normes et bonnes pratiques proposées : Microsoft / Anssi

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

Sécurisation de Microsoft Active Directory

Sécurisation des objets de l'annuaire
¨ Sécurisation des comptes d'utilisateurs
o Sécurisation des comptes d'utilisateurs et de services
o Compte d'utilisateurs protégés
o Compte 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)

Sécuriser le contrôleur de domaine
¨ Gestion de la sécurité par des contrôleurs multiples
¨ Sauvegarde et restauration
¨ RODC / AD LDS
¨ Microsoft Azure et la synchronisation de l'annuaire avec le nuage
o Scénario de synchronisation AD avec Azure
o Gestion des groupes et des comptes utilisateurs
o Approche sécuritaire

JOUR 2 :

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…

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 services en cas de compromission
o C'est arrivé ! Il me faut du temps pour réparer… Quelle est ma stratégie pendant cette période ?