SÉCURISER MES SERVEURS MICROSOFT ET MON SI NIVEAU 2

Public	Cette formation s'adresse aux administrateurs, aux techniciens et aux responsables de parc informatique en environnement Microsoft.
Durée	5 jours - 35 heures
Pré-requis	Connaissances générales de Windows Serveur et d'active directory.
Objectifs	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
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

JOUR 1 : MON RÉSEAU EST-IL FIABLE ?

- Comment analyser sa propre situation ?
- Quelques méthodes concrètes d'analyse du risque.
- Evaluer 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 ?

- 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…

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 les plus communes
  - 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 d'utilisateurs
  - Sécurisation des comptes d'utilisateurs et de services
  - Compte d'utilisateurs protégés
  - Comptes de services « managés »
- Gestion des comptes d'ordinateurs et délégation
  - Gestion des groupes privilégiés et sensibles
  - Gestion des droits des utilisateurs et des services
- Délégation d'administration pour protéger le SI
  - Gestion des privilèges
  - 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…

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…
  - 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
  - C'est arrivé ! Il me faut du temps pour réparer… Quelle est ma stratégie pendant Sources d'information pour la sécurisation del'AD : normes et bonnes pratiques

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 / …

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

JOUR 4 : MISE EN œUVRE D'UNE PKI MICROSOFT : (ATELIER)

- Installation et administration de l'autorité de certification
- Utilisation et gestion de la vie des certificats :
  - Serveurs Web sécurisés
  - Bitlocker, Efs
  - Authentication
  - Ouverture de session par carte à puce virtuelle
- Administration avancée de la PKI
  - Demande de certificat pour d'autres utilisateurs
  - Récupération des clés privées des certificats perdus

JOUR 5 : SÉCURISATION DU POSTE CLIENT WINDOWS 10/11

- Gestion des mises à jour de Windows 10/11
- Comment maintenir le poste client à jour ? Internet / WSUS / Azure…
- Sécurité du boot et de la virtualisation
  - Démarrage sécurisé UEFI
  - Device guard : configuration
  - Sécurisation d'Hyper-V
- Renforcement du système par modèle de sécurité
  - Tour d'horizon des recommandations
  - Déploiement des modèles de sécurité proposés par Microsoft
  - Utilisation des lignes de base pour le client windows 10/11
- Gestion de Defender
  - Administration par GPO et mise à jour
  - Microsoft Defender pour point de terminaison (Microsoft 365defender)

GESTION DU CENTRE DE SÉCURITÉ

- Isolement du noyau
- SmartScreen
- Dossiers protégés…

SÉCURISATION DU RÉSEAU

- Gestion du pare-feu pour la sécurité
- Gestion de la sécurité du wifi

SÉCURISATION DES APPLICATIONS ET DU NAVIGATEUR

- Déploiement de modèle d'administration par gpo
- Gestion des applications Appx et du Store localement et par GPO
- Restrictions des applications par Applocker et les restrictions logicielles
- Déploiement du contrôle d'application : WDAC

SYNTHÈSE SUR LA PROTECTION DE NOTRE SI

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Centre de formation
87, RUE GÉNÉRAL MANGIN
38000 GRENOBLE

Téléphone
04 76 23 20 50 - 06 81 73 19 35

E-mail
contact@audit-conseil-formation.com

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation @ACF_Formation ACFauditconseilformation