SÉCURITÉ DE L'ACTIVE DIRECTORY

Public	Ce cours Sécurité Active Directory s'adresse aux responsables de la sécurité SI, administrateurs Windows et Active Directory (AD), gestionnaires de projet axés sur la sécurité, architectes d'infrastructure et de système, intégrateurs système et responsable des superviseurs informatiques et de la protection des données.
Durée	3 jours - 21 heures
Pré-requis	Pour suivre cette formation Sécurité Active Directory, il est nécessaire d'avoir des connaissances de base des environnements Active Directory et des systèmes Windows.
Objectifs	Concevoir des architectures AD sécurisées Tester la sécurité de vos infrastructures AD Utiliser PowerShell pour la sécurisation AD
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
Planning	Du 08/09/2025 au 10/09/2025
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.

MESURES DE SÉCURISATION DE L'ACTIVE DIRECTORY

- Authentification par certificat et chiffrement TLS pour PowerShell
- Certificats pour :
- - L'authentification par carte à puce de PowerShell Remoting
- - Le chiffrement TLS de la communication à distance PowerShell
- - Signer des scripts PowerShell pour AppLocker
- - Le chiffrement TLS des requêtes WMI avec PowerShell
- - Crypter les mots de passe administrateur (au lieu de LAPS)
- - Les serveurs Web, les contrôleurs de domaine et tout le reste
- Installer un serveur de certificats Windows avec PowerShell

SÉCURITÉ AD AVANCÉE

- Script d'installation PowerShell pour l'infrastructure à clé publique (PKI)
- Gérer les certificats numériques avec PowerShell
- Modèles de certificats personnalisés dans Active Directory
- Contrôle de l'inscription automatique des certificats
- Configuration d'une batterie de serveurs Web de répondeur OCSP (Online Certificate Status Protocol)
- Configuration de la publication de la liste de révocation des certificats
- Déploiement de cartes à puce, de jetons intelligents et de cartes à puce virtuelles TPM
- La référence en matière d'authentification multifacteur est une carte à puce / un jeton
- Jetons intelligents YubiKey pour la connexion, la communication à distance PowerShell et bien plus
- Cartes à puce virtuelles Trusted Platform Module (TPM)
- Enregistrer en toute sécurité des jetons et des cartes au nom d'autres utilisateurs
- Comment révoquer les certificats compromis
- Script PowerShell pour :
- - Auditer les autorités de certification racines de confiance
- - Supprimer les certificats de pirate

AUTOMATISATION DU RENFORCEMENT DES SERVEURS POUR DEVOPS

- Remplacement du gestionnaire de serveur par PowerShell
- Ajout et suppression de rôles et de fonctionnalités
- Collecte à distance d'un inventaire des rôles et des fonctionnalités
- Pourquoi utiliser Server Nano ou Server Core ?
- Exécution automatique de PowerShell après une panne de service
- Identités, mots de passe et risques des comptes de service
- Outils pour réinitialiser les mots de passe des comptes de service en toute sécurité

SCRIPT DU PARE-FEU WINDOWS

- Gestion PowerShell des règles du pare-feu Windows
- Bloquer les connexions sortantes des logiciels malveillants
- Contrôle d'accès basé sur les rôles pour les ports d'écoute
- Intégration IPsec approfondie pour l'authentification des utilisateurs
- Journalisation du pare-feu dans les journaux d'événements, pas dans les journaux texte

PARTAGER LES AUTORISATIONS POUR LES PORTS D'ÉCOUTE TCP / UDP AVEC IPSEC

- Gestion PowerShell des règles IPsec
- IPsec pour bloquer les mouvements latéraux post-exploitation
- Limitation de l'accès aux ports en fonction de l'appartenance à un groupe global
- VLAN chiffrés basés sur IPsec
- IPsec n'est pas seulement pour les VPN !

PROTOCOLES ET SERVICES EXPLOITABLES

- Billets Kerberos
- Attaques RDP (Remote Desktop Protocol)
- Chiffrement natif SMBv3 vs Wireshark
- NTLM, NTLMv2 et Kerberos
- Gouffres DNS pour la détection des logiciels malveillants et des menaces
- Attaques DNS DoS et limitation du taux de réponse

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

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

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

ACF Audit Conseil Formation

@ACF_Formation

Dernière mise à jour : 27/09/2023