Développez vos talents
Certifiez vos compétences

Sécurité défensive

# Sécurité de l'Active Directory

3 jours (21h00) | ★★★☆☆ 3/5 | SEC-AD | Évaluation qualitative de fin de stage | Formation délivrée en présentiel ou distanciel [1]

Formations Informatique › Cybersécurité › Sécurité défensive

## À l'issue de ce stage vous serez capable de :

- Concevoir des architectures AD sécurisées
- Tester la sécurité de vos infrastructures AD
- Utiliser PowerShell pour la sécurisation AD.

## Niveau requis

Avoir des connaissances de base des environnements Active Directory et des systèmes Windows.

## Public concerné

Responsables de la sécurité SI, administrateurs Windows et Active Directory (AD), gestionnaires de projets axés sur la sécurité, architectes d'infrastructure et de système, intégrateurs système et responsable des superviseurs informatiques et de la protection des données.

## 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 M2i Formation
- Bénéficie d'un suivi de son exécution par une feuille de présence émargée par demi-journée par les stagiaires et le formateur.

**(1) Modalité et moyens pédagogique :**

Formation délivrée en présentiel ou distanciel * (e-learning, classe virtuelle, présentiel à distance). Le formateur alterne entre méthodes ** démonstrative, interrogative et active (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.

Les moyens pédagogiques mis en oeuvre (variables suivant les formations) sont : ordinateurs Mac ou PC (sauf pour les cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel). Environnements de formation installés sur les postes de travail ou en ligne. Supports de cours et exercices.

* Nous consulter pour la faisabilité en distanciel. ** Ratio variable selon le cours suivi.

# Programme

## Jour 1

### Mesures de sécurisation AD complémentaires

- 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 avancé

- 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)
- Enregistrez 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

## Jour 2

### 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

## Jour 3

### 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

## Modalités d'évaluation des acquis

- En cours de formation, par des études de cas ou des travaux pratiques
- Et, en fin de formation, par un questionnaire d'auto-évaluation ou une certification (M2i ou éditeur)