Sécuriser les Infrastructures Windows et Active Directory en Environnements Hybrides

DURÉE
5 jours (35h)

RÉFÉRENCE
SEC309

CATÉGORIE
Sécurité des Systèmes, Sécurité des Serveurs

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Comprendre les menaces spécifiques aux environnements Windows Server et Active Directory modernes
- Mettre en œuvre les bonnes pratiques de durcissement et de sécurisation des systèmes Windows
- Déployer une administration sécurisée basée sur les principes du moindre privilège et du tiering
- Sécuriser les postes utilisateurs et les comptes à privilèges dans un environnement hybride (local et cloud)
- Réaliser un audit complet et continu de la sécurité de l’infrastructure Active Directory

POUR QUI ?

- Administrateurs systèmes et réseaux
- Responsables et ingénieurs sécurité
- Architectes techniques
- Chefs de projets IT en charge de la sécurité des environnements Windows

Programme détaillé

1/ INTRODUCTION À LA SÉCURITÉ DES INFRASTRUCTURES WINDOWS

- Panorama des menaces et vecteurs d'attaque sur Windows et Active Directory
- Cartographie des rôles et services critiques
- Défense en profondeur et principes Zero Trust
- Bonnes pratiques de conception sécurisée

2/ DURCISSEMENT SYSTÈME WINDOWS

- Désactivation des rôles et services non essentiels
- Gestion des mises à jour et du cycle de vie des systèmes
- Paramétrage des journaux d'événements et surveillance native
- Stratégies de configuration basées sur les GPO de sécurité

3/ DURCISSEMENT RÉSEAU ET COMMUNICATIONS

- Sécurisation des protocoles réseau : SMB, LDAP, RDP, etc.
- Gestion des ports et filtrage réseau (pare-feu, IPsec)
- Protection contre le spoofing et le Man-in-the-Middle
- Configuration avancée du DNS sécurisé (DNSSEC, DNS logging)

4/ CONCEPTION D'UNE ADMINISTRATION SÉCURISÉE

- Modèle de séparation des tâches et comptes d'administration
- Postes et environnements d'administration dédiés
- Architecture tiering et zones d'administration sécurisées
- Notion de bastion et d'accès via serveurs de rebond

5/ GESTION DES COMPTES ET DES MOTS DE PASSE

- Mise en œuvre de Windows LAPS et LAPS v2
- Comptes Protected Users et authentification sécurisée
- Gestion des comptes de service (gMSA)
- Bonnes pratiques de rotation et d’audit des mots de passe

6/ JUST ENOUGH ADMINISTRATION (JEA) ET JUST IN TIME ACCESS (JITa)

- Présentation des modèles JEA et JITa
- Création de rôles d’administration temporaire
- Automatisation et journalisation des élévations de privilèges
- Exemples concrets d’implémentation dans PowerShell et Azure AD

7/ PROTECTION DU POSTE DE TRAVAIL

- Politique de mise à jour et gestion centralisée des correctifs
- Configuration du Secure Boot et intégrité du système
- Activation et gestion de BitLocker à grande échelle
- Déploiement et supervision de Defender for Endpoint

8/ ISOLATION ET CONTRÔLE DES APPLICATIONS

- Application Control et Whitelisting d’applications
- Gestion des pilotes et protection contre le BYOVD
- Virtualization-Based Security (VBS) et Exploit Guard
- Stratégies WDAC et Device Guard : mise en œuvre pratique

9/ PROTECTION DES IDENTITÉS ET DES CREDENTIELS

- Comprendre les attaques Pass-the-Hash et Pass-the-Ticket
- Activation de Credential Guard et des mécanismes anti-latéraux
- Sécurisation des tokens Kerberos et NTLM
- Surveillance des comptes sensibles via Microsoft Defender et SIEM

10/ MÉTHODOLOGIE D’AUDIT DE L’INFRASTRUCTURE

- Types d’audits : configuration, privilèges, conformité
- Mise en place de politiques d’audit Windows avancées
- Collecte et corrélation des logs avec des outils SIEM
- Bonnes pratiques pour documenter et remédier aux écarts

11/ OUTILS D’AUDIT ET DE VISUALISATION DES RISQUES

- Présentation de BloodHound, PingCastle et AD-Control-Path
- Cartographie des relations et chemins d’attaque dans l’AD
- Analyse des graphes d’attaques et priorisation des correctifs
- Utilisation d’outils open source et Microsoft pour la supervision

12/ DÉTECTION DES ATTAQUES ET RÉPONSE AUX INCIDENTS

- Indicateurs de compromission dans un environnement AD
- Simulation d’attaque (Red Team vs Blue Team)
- Réaction et confinement d’un incident sur le domaine
- Mise en place d’un plan de remédiation rapide

13/ RENFORCEMENT CONTINU ET CONFORMITÉ

- Revue de configuration périodique et tests d’intrusion
- Politiques de conformité (ISO 27001, ANSSI, CIS Benchmark)
- Intégration du Cloud (Azure AD) dans la stratégie de sécurité
- Élaboration d’un plan d’amélioration continue de la sécurité

14/ ÉVALUATION FINALE ET PLAN D’ACTION PERSONNALISÉ

- Synthèse des apprentissages et autoévaluation
- Étude de cas : durcissement complet d’une infrastructure fictive
- Construction d’un plan de sécurisation adapté à son contexte

- Conclusion et bonnes pratiques de maintien en condition de sécurité

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

29 Juin au 03 Juil. 2026	Casablanca
24 au 28 Août 2026	
19 au 23 Oct. 2026	

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-systems.com
Web : https//www.innov-systems.com

Scannez pour accéder à la fiche en ligne