Sécurité des environnements Active Directory & Azure AD (Entra ID) : durcissement et détection

Lien : https://innov-systems.com/formation/securite-des-environnements-active-directory-azure-ad-entra-id-durcissement-et-detection

DURÉE
5 jours (35h)

RÉFÉRENCE
SI125

CATÉGORIE
Identité, Gestion des Accès (IAM) et Zero Trust

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre l’architecture Active Directory et Entra ID
- Identifier les vulnérabilités des environnements d’identité
- Mettre en œuvre des stratégies de durcissement AD et cloud
- Sécuriser les authentifications et accès utilisateurs
- Détecter les attaques sur les infrastructures d’identité
- Utiliser les outils Microsoft de sécurité des identités
- Réduire les risques liés aux comptes privilégiés
- Implémenter des politiques d’accès conditionnel
- Superviser et auditer les environnements hybrides
- Réagir efficacement aux incidents de sécurité AD
- Améliorer la posture globale de sécurité des identités
- Étudier des cas concrets d’attaques et de défenses AD

POUR QUI ?

- Administrateurs systèmes et Active Directory
- Ingénieurs sécurité Microsoft
- Architectes IAM
- RSSI / CISO
- SOC analysts
- Cloud security engineers
- Consultants cybersécurité
- Ingénieurs systèmes et réseaux
- DevSecOps engineers
- Ingénieurs Microsoft 365 / Azure
- Responsables infrastructure IT
- Toute personne impliquée dans la gestion et la sécurisation des identités d’entreprise

Innov Systems

Programme détaillé

1 / Introduction aux annuaires Active Directory et Entra ID

- Rôle d'Active Directory dans les systèmes d'information
- Evolution vers Azure AD (Microsoft Entra ID)
- Enjeux de sécurité des identités hybrides

2 / Architecture des environnements d'identité hybrides

- Domaines, forêts et trusts AD
- Synchronisation AD Connect / Entra Connect
- Modèle hybride on-premise et cloud

3 / Gestion des identités et des accès (IAM)

- Cycle de vie des identités utilisateurs
- Groupes, rôles et privilèges
- Principe du moindre privilège

4 / Authentification et mécanismes de sécurité

- Kerberos, NTLM et authentification moderne
- MFA et accès conditionnel
- Protection des comptes sensibles

5 / Durcissement d'Active Directory

- Sécurisation des contrôleurs de domaine
- GPO de sécurité et configuration avancée
- Réduction de la surface d'attaque AD

Innov Systems

6 / Sécurisation de Microsoft Entra ID

- Politiques de sécurité cloud identity
- Conditional Access policies
- Protection des identités et Identity Protection

7 / Détection des attaques sur les identités

- Attaques Pass-the-Hash, Pass-the-Ticket, Golden Ticket
- Détection des mouvements latéraux
- Surveillance des comportements suspects

8 / Outils de monitoring et de détection

- Microsoft Defender for Identity
- Azure Sentinel (Microsoft Sentinel)
- Audit logs et SIEM

9 / Réponse aux incidents liés aux identités

- Procédures de remédiation AD compromise
- Isolation et rotation des credentials
- Playbooks de réponse automatisée

10 / Cas pratiques et stratégies de sécurisation

- Audit d’un environnement AD/Entra ID
- Mise en place d’une architecture sécurisée
- Bonnes pratiques de durcissement et monitoring

Innov Systems

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

15 au 19 Fév. 2027	Présentiel - Casablanca
12 au 16 Avr. 2027	Présentiel - Casablanca
07 au 11 Juin 2027	Présentiel - Casablanca
02 au 06 Août 2027	Présentiel - Casablanca
27 Sep. au 01 Oct. 2027	Présentiel - Casablanca

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

Innov Systems — Tous droits réservés