Active Directory : maîtrisez la compromission et la sécurisation des environnements Windows

Lien : https://innov-systems.com/formation/active-directory-maitrisez-la-compromission-et-la-securisation-des-environnements-windows

DURÉE
5 jours (35h)

RÉFÉRENCE
SI02

CATÉGORIE
Sécurité des Systèmes et Serveurs

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre le fonctionnement de l’Active Directory
- Identifier les principales techniques de compromission AD
- Détecter les signes d’attaques et d’intrusions
- Maîtriser les bonnes pratiques de sécurisation AD
- Renforcer la gestion des identités et des accès
- Mettre en place des stratégies de défense efficaces
- Réagir efficacement en cas d’incident de sécurité
- Améliorer la résilience des infrastructures Windows
- Réaliser des audits de sécurité Active Directory
- Développer une expertise en cybersécurité des environnements Microsoft

POUR QUI ?

- Administrateurs systèmes et réseaux
- Ingénieurs cybersécurité
- Responsables IT et infrastructure
- Analystes SOC
- Architectes systèmes Microsoft
- Techniciens support informatique avancé
- Toute personne impliquée dans la sécurité des environnements Windows et Active Directory

Innov Systems

Programme détaillé

1 / Introduction à l'Active Directory

- Rôle de l'Active Directory dans les systèmes d'information
- Architecture et composants essentiels
- Importance dans la gestion des identités

2 / Modèle de sécurité de l'Active Directory

- Gestion des comptes utilisateurs et groupes
- Contrôleurs de domaine et politiques de sécurité
- Principes de contrôle d'accès

3 / Techniques de compromission de l'Active Directory

- Attaques par vol d'identifiants (credential dumping)
- Pass-the-Hash et Pass-the-Ticket
- Élévation de privilèges

4 / Failles courantes et mauvaises configurations

- Permissions excessives
- Mots de passe faibles et politiques inadéquates
- Erreurs de configuration des GPO

5 / Outils d'attaque utilisés par les cybercriminels

- Frameworks d'attaque Active Directory
- Outils de reconnaissance et d'exploitation
- Techniques de mouvement latéral

Innov Systems

6 / Détection des compromissions

- Indicateurs de compromission (IOC)
- Surveillance des logs et événements Windows
- Outils de détection d’anomalies

7 / Durcissement de l’Active Directory

- Bonnes pratiques de configuration sécurisée
- Gestion des privilèges minimum (Least Privilege)
- Sécurisation des comptes administrateurs

8 / Protection des identités et des accès

- Authentification multifactorielle (MFA)
- Gestion des comptes à privilèges
- Séparation des rôles administratifs

9 / Stratégies de réponse à incident

- Plan de réponse en cas de compromission
- Isolation des systèmes infectés
- Restauration sécurisée de l’Active Directory

10 / Audit et amélioration continue de la sécurité

- Audits réguliers de sécurité AD
- Tests de pénétration (pentest)
- Mise à jour et durcissement continu

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