Sécurité des environnements Wi-Fi d'entreprise : WPA3, rogue AP et protocoles avancés

Lien : https://innov-systems.com/formation/securite-des-environnements-wi-fi-dentreprise-wpa3-rogue-ap-et-protocoles-avances

DURÉE
5 jours (35h)

RÉFÉRENCE
SI110

CATÉGORIE
Sécurité Wifi/IOT et Malware

Innov Systems

OBJECTIFS DE LA FORMATION

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

- Comprendre les standards de sécurité Wi-Fi et leurs évolutions
- Identifier les vulnérabilités des réseaux sans fil d’entreprise
- Mettre en œuvre WPA3 et les mécanismes d’authentification sécurisés
- Détecter et neutraliser les rogue access points
- Sécuriser les infrastructures Wi-Fi en environnement professionnel
- Implémenter des solutions WIDS/WIPS
- Améliorer la segmentation et le contrôle d’accès réseau
- Réduire les risques d’attaques sans fil
- Auditer et renforcer la sécurité des réseaux Wi-Fi
- Intégrer les bonnes pratiques de cybersécurité réseau
- Superviser les environnements Wi-Fi à grande échelle
- Étudier des cas concrets d’attaques et de protection Wi-Fi

POUR QUI ?

- Ingénieurs réseaux
- Administrateurs réseau Wi-Fi
- Ingénieurs cybersécurité
- SOC analysts
- Architectes réseau
- Consultants en sécurité informatique
- Administrateurs systèmes et réseaux
- Responsables IT
- Ingénieurs infrastructure
- RSSI / CISO
- Techniciens télécoms
- Toute personne impliquée dans la gestion et la sécurisation des réseaux Wi-Fi d’entreprise

Innov Systems

Programme détaillé

1 / Introduction à la sécurité des réseaux Wi-Fi d’entreprise

- Évolution des standards Wi-Fi (WEP, WPA, WPA2, WPA3)
- Enjeux de sécurité dans les environnements professionnels
- Surface d’attaque des réseaux sans fil

2 / Architecture des réseaux Wi-Fi d’entreprise

- Points d’accès (AP), contrôleurs WLAN et infrastructure réseau
- Segmentation des réseaux (invités, internes, IoT)
- Intégration avec les systèmes d’authentification

3 / WPA3 et nouveaux standards de sécurité

- SAE (Simultaneous Authentication of Equals)
- Chiffrement renforcé et protection contre les attaques offline
- Transition de WPA2 vers WPA3 en entreprise

4 / Authentification et contrôle d’accès

- 802.1X et RADIUS
- Authentification basée sur certificats
- Gestion des identités et politiques d’accès

5 / Menaces sur les réseaux Wi-Fi

- Rogue Access Points (points d’accès malveillants)
- Evil Twin attacks et attaques de type MITM
- Sniffing et interception de trafic sans fil

Innov Systems

6 / Attaques avancées sur Wi-Fi

- Deauthentication attacks
- KRACK et vulnérabilités WPA2
- Exploitation des protocoles faibles

7 / Sécurisation des environnements Wi-Fi

- Segmentation et isolation réseau
- Durcissement des points d’accès
- Politiques de sécurité et configuration sécurisée

8 / Monitoring et détection des intrusions Wi-Fi

- WIDS/WIPS (Wireless Intrusion Detection/Prevention Systems)
- Analyse du spectre radio
- Détection des comportements suspects

9 / Gestion des équipements et gouvernance

- Inventaire des équipements Wi-Fi
- Mise à jour et gestion des firmwares
- Politiques de sécurité réseau

10 / Cas pratiques et audit de sécurité Wi-Fi

- Audit complet d’un réseau Wi-Fi d’entreprise
- Détection et neutralisation d’un rogue AP
- Bonnes pratiques de sécurisation

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

22 au 26 Fév. 2027	Présentiel - Casablanca
19 au 23 Avr. 2027	Présentiel - Casablanca
14 au 18 Juin 2027	Présentiel - Casablanca
09 au 13 Août 2027	Présentiel - Casablanca
04 au 08 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