# Hacking éthique et tests d'intrusion sur les objets connectés et systèmes embarqués

*Lien : https://innov-systems.com/formation/hacking-ethique-et-tests-dintrusion-sur-les-objets-connectes-et-systemes-embarques*

DURÉE
**5 jours (35h)**

RÉFÉRENCE
**SI127**

CATÉGORIE
**Cybersécurité IoT, IIoT et Systèmes Robotisés**

Innov Systems

## OBJECTIFS DE LA FORMATION

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

- Comprendre les architectures IoT et embarquées
- Identifier les vulnérabilités des objets connectés
- Réaliser des tests d’intrusion sur systèmes IoT
- Analyser et reverse engineer des firmwares
- Exploiter les failles des protocoles de communication
- Tester la sécurité des interfaces matérielles
- Évaluer les risques des systèmes embarqués critiques
- Rédiger des rapports de pentest professionnels
- Mettre en œuvre des stratégies de sécurisation IoT
- Maîtriser les outils de hacking éthique IoT
- Améliorer la résilience des systèmes connectés
- Étudier des cas concrets de sécurité IoT

## POUR QUI ?

- Ethical hackers
- Pentesters
- Cybersecurity engineers
- IoT security engineers
- Embedded systems engineers
- Firmware developers
- SOC analysts
- DevSecOps engineers
- Consultants cybersécurité
- Ingénieurs systèmes embarqués
- Researchers en sécurité informatique
- Toute personne impliquée dans la sécurité des objets connectés et systèmes embarqués

Innov Systems

## Programme détaillé

### 1 / Introduction au hacking éthique IoT et systèmes embarqués

- Principes du hacking éthique et du pentest IoT
- Surface d’attaque des objets connectés
- Spécificités des systèmes embarqués

### 2 / Architecture des systèmes IoT et embarqués

- Capteurs, microcontrôleurs et firmwares
- Protocoles IoT (MQTT, CoAP, Zigbee, BLE)
- Chaîne complète de communication

### 3 / Reconnaissance et cartographie des systèmes

- Identification des devices connectés
- Analyse des réseaux IoT
- Fingerprinting des équipements embarqués

### 4 / Analyse des firmwares

- Extraction et reverse engineering
- Analyse statique et dynamique
- Détection de vulnérabilités logicielles

### 5 / Sécurité des protocoles de communication

- Failles dans MQTT, BLE, Wi-Fi et Zigbee
- Interception et analyse du trafic
- Attaques man-in-the-middle IoT

Innov Systems

### 6 / Exploitation des vulnérabilités

- Injection de commandes et buffer overflow
- Exploitation des API et interfaces web embarquées
- Escalade de privilèges sur devices IoT

### 7 / Sécurité matérielle et attaques physiques

- JTAG, UART et interfaces de debug
- Attaques par side-channel
- Extraction de firmware et clés cryptographiques

### 8 / Sécurité des systèmes embarqués critiques

- IoT industriel et systèmes SCADA
- Vulnérabilités des systèmes temps réel
- Risques sur infrastructures critiques

### 9 / Tests d’intrusion et méthodologie

- Frameworks de pentest IoT
- Chaîne complète de test d’intrusion
- Reporting et remédiation

### 10 / Défense et durcissement des systèmes IoT

- Secure boot et mise à jour firmware sécurisée
- Chiffrement et authentification forte
- Bonnes pratiques de sécurité IoT

Inov 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