



Développer des Applications Windows Sécurisées

Lien : <https://innov-maroc.com/formation/developper-des-applications-windows-securisees>

 DURÉE
3 jours (21h)

 RÉFÉRENCE
SEC124

 CATÉGORIE
**Sécurité des
Applications**

OBJECTIFS DE LA FORMATION

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

- ✓ Apprendre à décomposer son application en composants
- ✓ Savoir modéliser les menaces et apporter des solutions techniques génériques d'atténuation
- ✓ Acquérir les techniques de programmation sécurisée

POUR QUI ?

- ✓ Développeur
- ✓ Responsables technique
- ✓ Chef de projet



Programme détaillé

1 / Introduction

- L'importance de la sécurité
- Contre qui et quoi se défendre ?
- Les failles de sécurité classiques
- Comment une attaque survient ?
- Les challenges de la sécurité

2 / Sécurité dans le framework et du code

- Concepts fondamentaux
- Sécurité d'accès du code et des ressources
- Sécurité basée sur les rôles
- Le principe du W^X
- Services de chiffrement
- Validation et contrôle des entrées / sorties
- Gestion et masquage d'erreurs
- Gestion sécurisée de la mémoire
- Contrôle d'authenticité et d'intégrité d'une application/d'un code
- Offuscation du code
- Reverse engineering sur : bundle C#, application Java, binaire Windows
- Contrôle des droits avant exécution du code
- Sécuriser les données sensibles présentes dans un binaire

3 / Modélisation des menaces

- Décomposer une application
- Déterminer les menaces d'une application
- Noter et classer les menaces
- Répondre aux menaces

4 / Exploitation de « Buffer overrun »

- Initiation à l'exploitation
- Principe général
- Écrasement de l'adresse de retour
- Exploitation des exceptions Win32
- Sécurisation
- Options de compilation (Stack cookies, DEP, ALSR, etc.)
- Différences entre Windows 32 bits et Windows 64 bits

5 / Techniques de programmation sécurisée

- Se méfier des données d'entrée
- S'exécuter avec les droits minimum
- Les pièges du chiffrement
- Déterminer les bons ACLs
- Protéger les données sensibles
- Se protéger des attaques par déni de service
- Éviter d'utiliser des APIs non sécurisées
- Bonnes pratiques la synthèse

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

 11 au 13 Nov. 2026

 Distanciel

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

Réservation & Renseignements

 **Téléphone** : +212 522 247 210

 **Email** : contact@innov-maroc.com

 **Web** : <https://www.innov-maroc.com>

Document généré le 12/10/2026 — Réf : SEC124
INNOV MAROC — Tous droits réservés