

# Durcissement Sécurité Windows

*Lien : https://innov-maroc.com/formation/durcissement-securite-windows*

DURÉE
**5 jours (35h)**

RÉFÉRENCE
**SEC112**

CATÉGORIE
**Sécurité des Systèmes et Serveurs**

## OBJECTIFS DE LA FORMATION

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

- Comprendre l’intérêt des techniques de durcissement systèmes et réseau
- Maîtriser les différentes techniques de durcissement des systèmes Windows

## POUR QUI ?

- Administrateurs
- Architectes
- Experts en sécurité
- Responsables sécurité

INNOV MAROC



## Programme détaillé

### 1 / L'écosystème actuel : Introduction

- L'évolution des systèmes d'information et leur ouverture sur le monde
- Les menaces courantes pesant sur les systèmes d'information
- Les menaces récentes
- Chronologie et évolutions majeures des systèmes d'exploitation Windows

### 2 / Redéfinir la sécurité informatique

- Mise en place d’un atelier de machines Linux/Windows vulnérables et à durcir
- Cartographie d’un système d’information
- Faire une veille sur les vulnérabilités connues
- Restreindre l’accès à un réseau filaire ou sans-fil
- Cloisonnement réseau
- M une machine et ses services avec un pare-feu

### 3 / Une défense alignée aux attaques

- Compréhension de la défense par rapport à un scénario d'attaque
- Segmentation des phases d'un attaquant
- Etudier les outils et méthodes d'attaque par phases avec la Cyber Kill Chain (ATT&CK)
- Les attaques courantes dans un domaine Windows

### 4 / Durcir les domaines Windows

INNOV MAROC

- Limiter l'installation d'applications non conformes grâce à AppLocker
- Gérer les droits (ACL) des comptes utilisateurs
- Sécurisation de l'Active Directory
- Architecture PKI
- Sécurisation de l'administration du domaine : WinRM, RPC, WMI, RDP
- Sécurisation des services et comptes de services managés (MSA)
- Classification et marquage de l'information pour les systèmes de prévention de pertes de données (DLP)
- Journalisation
- Présentation d'une solution d'analyse de menaces avancées (ATA)
- Sécurité des environnements Azure

## 5 / Durcir les serveurs et postes clients

- Sécurisation du démarrage (Secure Boot - UEFI : Unified Extensible Firmware Interface)
- Chiffrement de disque
- Firewall Windows (configuration et règles)
- Le contrôle des comptes utilisateur (UAC)
- Sécurisation des contenus Web (Smartscreen)
- Windows Defender
- Fonctionnalités antivirales : Device Guard, Credential Guard, AMSI (Anti-Malwares Scan Interface)
- Augmentation de la maîtrise de PowerShell

## 6 / Durcir les protocoles

- Les bases de l'authentification Microsoft
- Authentification de domaine
- NTLM (NT LAN Manager)
- Processus de "Défi-Réponse"
- NTLMv2
- Kerberos
- Analyse des protocoles actifs sur le domaine (Netstat et Wireshark)

INNOV MAROC

- Etude des protocoles et services faillibles

### 7 / Mécanismes de défense avancée

- Les éditeurs de sécurité (Cyberark et Hexatrust)
- Défenses spécifiques à l'attaque Kerberoasting
- Mesures de détection pour l'attaque DCShadow

## 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

| | |
|---|---|
| 01 au 05 Fév. 2027 | Présentiel - Casablanca |
| 29 Mars au 02 Avr. 2027 | Présentiel - Casablanca |
| 24 au 28 Mai 2027 | Présentiel - Casablanca |
| 19 au 23 Juil. 2027 | Présentiel - Casablanca |
| 13 au 17 Sep. 2027 | Présentiel - Casablanca |

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

INNOV MAROC

## Réservation & Renseignements

**Téléphone :** +212 522 247 210
**Email :** contact@innov-maroc.com
**Web :** https//www.innov-maroc.com


INNOV MAROC — Tous droits réservés