



Durcissement des Systèmes et Réseaux - Hardening

Lien : <https://innov-maroc.com/formation/durcissement-des-systemes-et-reseaux-hardening>

 DURÉE
5 jours (35h)

 RÉFÉRENCE
SEC114

 CATÉGORIE
**Sécurité des Systèmes,
Sécurité des 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
- ✓ Pouvoir optimiser la sécurisation du système

POUR QUI ?

- ✓ Administrateurs
- ✓ Architectes
- ✓ Experts en sécurité
- ✓ Responsables sécurité



Programme détaillé

1 / L'écosystème actuel : Introduction

- L'évolution des systèmes d'information et leurs ouvertures 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
- Mettre 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 / Durcissement des domaines Windows

- 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 des réseaux Wi-Fi
- Sécurisation de l'administration du domaine : WinRM, RPC, WMI, RDP
- Sécurité des services et comptes de services managés (MSA)
- Classification et marquage de l'information pour les systèmes de prévention de pertes de données (DLP)
- Audit et centralisation des journaux d'événements Windows
- Présentation d'une solution d'analyse de menaces avancées (ATA)
- Sécurité des environnements Azure

5 / Durcissement de base Linux

- Mot de passe root et comptes administrateur
- Installation d'éléments supplémentaires : clés et certificats
- Pare-feu Linux : Configuration "iptables", Règles, Netfilter
- Contrôler les accès et l'élévation de privilèges (SELinux)
- Configuration système (systemctl)
- Gestion de comptes d'accès et SSH
- Désactivation des comptes utilisateurs inutilisés
- Délai d'expiration de sessions utilisateurs
- Vérification systèmes de fichiers et droits (Umask)
- Les fichiers à contenu sensible
- Les fichiers exécutables setuid ou setgid
- Fichiers sans utilisateur ou groupe propriétaire
- Les fichiers et répertoires accessibles à tous en écriture
- Les fichiers IPC nommés, sockets ou pipes
- Mails et mails root

6 / Durcir les protocoles

- Les bases de l'authentification Linux (PAM, NSS)
- Analyse des protocoles actifs (Netstat, Wireshark)
- Les services réseau résidents
- Les services exposés à des flux non maîtrisés
- Etude des protocoles et services faillibles
- Maîtrise des flux (TCP Wrapper)

7 / Mécanismes de défense avancée

- Prévention contre le brute-force (Fail2ban)
- Isolation de l'exécution d'un programme (chroot)
- Sécurisation du noyau (grsecurity)
- Détection d'intrusion hôte (OSSEC)
- Configuration d'outils et services de monitoring
- Surveillance du système (auditd)

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

 16 au 20 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>

INNOV MAROC