



Windows Server 2016 : sécurisation de l'infrastructure

Lien : <https://innov-maroc.com/formation/windows-server-2016-securisation-de-linfrastructure>

 DURÉE
5 jours (35h)

 RÉFÉRENCE
SEC107

 CATÉGORIE
**Sécurité des Systèmes,
Sécurité des Serveurs**

OBJECTIFS DE LA FORMATION

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

- ✓ Pouvoir assurer la sécurité des systèmes Windows Server
- ✓ Etre capable de sécuriser le développement d'applications
- ✓ Savoir configurer et gérer une administration JEA et JIT
- ✓ Savoir configurer le pare-feu Windows et les pare-feux distribués
- ✓ Etre en mesure de sécuriser l'infrastructure de virtualisation

POUR QUI ?

- ✓ Ingénieurs système et réseau



Programme détaillé

1 / Détection des intrusions et utilisation des outils Sysinternals

- Présentation des attaques
- Vue d'ensemble de la détection des violations
- Les outils Sysinternals

2 / Protection des « credentials » et des accès privilégiés

- Présentation des droits d'utilisateur
- Comptes d'ordinateurs et de service
- Protection des informations d'identification
- Les stations de travail avec accès privilégiés et les serveurs Jump
- Solution locale de mot de passe administrateur (LAPs)

3 / Restriction des droits administrateur avec JEA (Just Enough Administration)

- Présentation d'une administration JEA
- Configuration et déploiement JEA

4 / Gestion des accès privilégiés et des forêts administratives

- Vue d'ensemble des forêts ESAE (Enhanced Security Administrative Environment)
- Présentation de MIM (Microsoft Identity Manager)
- Mise en œuvre de JIT (Just In Time) et la gestion des accès privilégiés via MIM (Microsoft Identity Manager)

5 / Atténuation des malware et des menaces sous Windows Server 2016

- Configurer et gérer Windows Defender
- Restreindre les logiciels (SRPs) et AppLocker
- Configurer et utiliser la fonctionnalité Device Guard
- Utiliser et déployer kit EMET (Enhanced Mitigation Experience)

6 / Analyser les activités via l'audit avancé

- Vue d'ensemble de l'audit
- Stratégies d'audit avancées
- Configuration de l'audit et de la connexion Windows PowerShell

7 / Déploiement et configuration d'Advanced Threat Analytics et de Microsoft Operations Management Suite (OMS)

- Vue d'ensemble de Advanced Threat Analytics (ATA)
- Déployer et configurer OMS

8 / Sécurisation de l'infrastructure de virtualisation

- Infrastructures protégées (Guarded Fabric)
- Machines virtuelles chiffrées (encryption-supported) et blindées (shielded)

9 / Sécurisation du développement d'applications et de l'infrastructure serveur

- Utilisation de SCM (Security Compliance Manager)
- Introduction aux Nano servers
- Les conteneurs

10 / Protéger les données avec le cryptage

- Planifier et implémenter le chiffrement
- Planifier et implémenter le BitLocker

11 / Limitation de l'accès aux fichiers et aux dossiers

- Introduction à FSRM
- Outils de gestion de ressources pour serveur de fichiers
- Implémenter la gestion de la classification et les tâches liées à la gestion de fichiers
- Contrôle d'accès dynamique (Dynamic Access Control)

12 / Utilisation des firewalls pour contrôler le trafic

- Présentation des menaces de sécurité associées au réseau
- Présentation du Pare-feu Windows avec fonctions avancées de sécurité
- Configuration d'IPsec
- Pare-feu de centre de données

13 / Sécurisation du trafic réseau

- Menaces contre la sécurité du réseau et règles de sécurité pour la connexion
- Configuration des paramètres DNS avancés
- Examiner le trafic réseau avec Microsoft Message Analyzer
- Sécuriser et analyser le trafic SMB

14 / Mise à jour de Windows Server

- Vue d'ensemble de WSUS
- Déployer des mises à jour via WSUS

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>

Document généré le 12/10/2026 — Réf : SEC107
INNOV MAROC — Tous droits réservés