Sécurité et Gouvernance des Environnements Microsoft Azure

Lien : https://innov-maroc.com/formation/securite-et-gouvernance-des-environnements-microsoft-azure

DURÉE	RÉFÉRENCE	CATÉGORIE
5 jours (35h)	**VSC334**	**Microsoft Azure**

OBJECTIFS DE LA FORMATION

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

- Comprendre et maîtriser les principes fondamentaux de la sécurité cloud appliqués à Microsoft Azure
- Déployer des stratégies d’identité et d’accès sécurisées avec Microsoft Entra ID
- Implémenter des contrôles de sécurité réseau, applicatifs et de données dans Azure
- Utiliser Microsoft Defender et Sentinel pour la détection, la prévention et la remédiation des menaces
- Mettre en œuvre une gouvernance et une conformité de la sécurité alignées sur les meilleures pratiques Azure

POUR QUI ?

- Administrateurs systèmes et cloud
- Responsables infrastructure et sécurité
- Ingénieurs et architectes cloud
- Chefs de projet techniques orientés sécurité

Programme détaillé

1 / INTRODUCTION À LA SÉCURITÉ CLOUD ET À LA GOUVERNANCE AZURE

- Comprendre les responsabilités partagées entre Microsoft et le client
- Identifier les outils et services clés de sécurité Azure
- Définir les politiques de gouvernance et les bonnes pratiques de conformité
- Explorer le centre de sécurité Microsoft Defender pour le Cloud

2 / STRUCTURER LA GOUVERNANCE ET LA CONFORMITÉ DANS AZURE

- Implémenter Azure Policy pour le contrôle de la conformité
- Utiliser Azure Blueprint pour normaliser les déploiements sécurisés
- Gérer les abonnements, groupes de gestion et ressources
- Créer des zones d’atterrissage sécurisées pour les environnements de production

3 / GESTION DES CLÉS ET DES SECRETS AVEC AZURE KEY VAULT

- Créer et gérer des coffres-forts de clés pour la protection des secrets
- Définir les politiques d’accès et de rotation des clés
- Configurer l’intégration Key Vault avec des services Azure (VM, App Service, SQL)
- Mettre en œuvre le chiffrement de bout en bout à l’aide de HSM

4 / GESTION DES IDENTITÉS ET DES RÔLES

- Créer et administrer des utilisateurs, groupes et rôles
- Comprendre le modèle RBAC (Role-Based Access Control)

- Définir des rôles personnalisés selon les besoins organisationnels
- Sécuriser les identités externes et invitées dans Entra ID

5 / AUTHENTIFICATION ET ACCÈS CONDITIONNEL

- Configurer l’authentification multifacteur (MFA) et sans mot de passe
- Mettre en œuvre des stratégies d’accès conditionnel basées sur le risque
- Intégrer l’authentification unique (SSO) pour les applications internes et SaaS
- Superviser les connexions et les alertes liées à la compromission d’identité

6 / PRIVILEGED IDENTITY MANAGEMENT (PIM) ET SÉCURITÉ DES ACCÈS ÉLEVÉS

- Comprendre le principe du moindre privilège
- Configurer la gestion des identités à privilèges dans Entra ID
- Auditer et approuver les demandes d’accès temporaire
- Utiliser des alertes et journaux d’audit pour le suivi des activités privilégiées

7 / SÉCURISER LES RÉSEAUX VIRTUELS ET LES FLUX DE DONNÉES

- Configurer des groupes de sécurité réseau (NSG) et d’application (ASG)
- Mettre en place des routes personnalisées et filtrage du trafic
- Sécuriser les connexions hybrides avec VPN, ExpressRoute et Virtual WAN
- Monitorer et diagnostiquer les incidents réseau avec Azure Network Watcher

8 / PROTÉGER L’ACCÈS PUBLIC ET PRIVÉ AUX RESSOURCES

- Restreindre l’accès public aux ressources critiques
- Mettre en œuvre Private Link, Private Endpoints et App Service Environment
- Configurer des services de sécurité périphériques (Azure Firewall, WAF, DDoS)
- Intégrer Application Gateway et Front Door pour la sécurité applicative

9 / SÉCURISER LES RESSOURCES DE STOCKAGE ET LES BASES DE DONNÉES

- Appliquer le chiffrement au repos et en transit
- Gérer les accès et les clés dans le stockage Azure (Blob, Files, Tables)
- Implémenter le masquage dynamique et Always Encrypted pour Azure SQL
- Utiliser Microsoft Purview pour la classification et la protection des données sensibles

10 / RENFORCER LA SÉCURITÉ DES MACHINES VIRTUELLES ET DES CONTENEURS

- Sécuriser l’accès distant avec Azure Bastion et Just-In-Time VM Access
- Configurer Azure Disk Encryption et la gestion des certificats
- Mettre en œuvre la sécurité des clusters AKS et des registres ACR
- Appliquer les principes de sécurité Zero Trust pour les environnements de calcul

11 / SURVEILLANCE DE LA POSTURE DE SÉCURITÉ AVEC MICROSOFT DEFENDER

- Utiliser Defender pour le Cloud pour évaluer la posture de sécurité
- Identifier les vulnérabilités et appliquer les recommandations
- Connecter des environnements hybrides et multiclouds
- Configurer des alertes et rapports de conformité automatisés

12 / DÉTECTION ET RÉPONSE AUX MENACES AVEC MICROSOFT SENTINEL

- Intégrer des sources de données multiples dans Microsoft Sentinel
- Créer des règles d’analyse et des playbooks automatisés
- Configurer des alertes de détection en temps réel
- Mettre en œuvre la réponse automatique aux incidents via Logic Apps

13 / MISE EN ŒUVRE D’UNE STRATÉGIE GLOBALE DE SÉCURITÉ AZURE

- Élaborer un plan d’amélioration continue de la posture de sécurité
- Évaluer la conformité par rapport aux normes ISO, NIST et RGPD
- Automatiser les processus de remédiation et de reporting
- Finaliser une feuille de route opérationnelle pour la sécurité Azure

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

17 au 21 Août 2026	Distanciel
12 au 16 Oct. 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