ADVANCIA TRAINING

Les technologies de sécurité en environnement Microsoft Azure

Réf. AZ-500 · Microsoft · Cybersécurité · **Formation certifiante**

DURÉE	NIVEAU	MODALITÉS	VOUCHER EXAMEN
5 jours	**Avancé**	**Présentiel · Live · Intra**	**Inclus**

Présentation

Cette formation avancée couvre l'ensemble des technologies de sécurité Microsoft Azure : gestion des identités avec Entra ID, sécurisation du réseau et des plateformes, protection des données et supervision via Microsoft Defender for Cloud et Sentinel. Elle s'adresse aux professionnels chargés de concevoir et d'opérer une posture de sécurité robuste sur Azure et prépare directement au passage de l'examen AZ-500.

Objectifs pédagogiques

- Gérer les identités et les accès avec Microsoft Entra ID (RBAC, PIM, accès conditionnel, MFA)
- Sécuriser les réseaux Azure (NSG, Azure Firewall, WAF, Private Link, protection DDoS)
- Durcir et protéger les machines virtuelles, conteneurs et services PaaS
- Chiffrer et gouverner les données (Azure Key Vault, chiffrement, Azure SQL, stockage)
- Superviser la sécurité avec Microsoft Defender for Cloud et Microsoft Sentinel
- Appliquer la gouvernance et la conformité via Azure Policy et le Secure Score

Programme détaillé

1. Module 1 — Gestion des identités et des accès

- Microsoft Entra ID, utilisateurs, groupes et rôles
- RBAC Azure et Privileged Identity Management (PIM)
- Accès conditionnel et authentification multifacteur (MFA)
- Identités managées et Entra ID Protection

2. Module 2 — Sécurité du réseau

- Groupes de sécurité réseau (NSG) et groupes de sécurité applicatifs (ASG)
- Azure Firewall, Firewall Manager et Web Application Firewall
- Private Endpoints et Private Link
- Protection DDoS et Azure Bastion

3. Module 3 — Sécurité des plateformes et du calcul

- Durcissement des machines virtuelles et Endpoint Protection
- Sécurité d'Azure Kubernetes Service (AKS) et des conteneurs
- Gestion des mises à jour et de la posture
- Sécurisation d'App Service et des services PaaS

4. Module 4 — Protection des données et des secrets

- Azure Key Vault : clés, secrets et certificats
- Chiffrement au repos et en transit
- Sécurité d'Azure SQL et du stockage
- Rotation des clés et gestion du cycle de vie

5. Module 5 — Gouvernance et gestion de la posture

- Microsoft Defender for Cloud et Secure Score
- Azure Policy et Blueprints
- Conformité réglementaire et recommandations
- Gestion des vulnérabilités

6. Module 6 — Opérations de sécurité et SIEM

- Microsoft Sentinel : collecte et connecteurs de logs
- Règles analytiques et chasse aux menaces (hunting)
- Playbooks SOAR et automatisation
- Investigation et réponse aux incidents

Prérequis

Bonne connaissance des services Azure fondamentaux (niveau AZ-104 recommandé) ainsi que des concepts de sécurité, de réseau et de virtualisation. Une expérience du scripting (PowerShell ou Azure CLI) est un plus.

Public visé

Ingénieurs et administrateurs sécurité, architectes cloud, administrateurs Azure et professionnels SecOps responsables de la sécurité des environnements Microsoft Azure.

Ce qui est inclus

- Support de cours officiel Microsoft Learning (MOC AZ-500)
- Environnement de labs pratiques sur souscription Azure
- Attestation de réussite Advancia Training
- Voucher d'examen AZ-500 Pearson VUE
- Pauses café, déjeuner et accès à un formateur certifié Microsoft

Certification

Prépare l'examen Microsoft AZ-500 (Azure Security Technologies), menant à la certification Microsoft Certified: Azure Security Engineer Associate. Épreuve d'environ 40 à 60 questions (QCM, scénarios et études de cas) d'une durée approximative de 120 minutes. Advancia Training est centre d'examen agréé Pearson VUE.

1 900 DT HT / participant — tarif inter-entreprise · financement CNFCPP possible