Formation Azure – Security Technologies (AZ-500)

Informations

Durée : 4 jours (28h.)

Tarif* : Nous consulter

Réf : AZ-500

Niveau : Difficile

intra

Mise à jour le 18/12/25

*tarif valable jusqu'au 31/12/2025

Prochaines sessions

Contactez-nous pour connaitre nos futures sessions.

Pré-requis

- Connaissances de base en administration Azure (AZ-104 recommandé)
- Notions en sécurité des systèmes et réseaux

Objectifs

Objectifs pédagogiques :

- Mettre en œuvre des contrôles d'accès et d'identité sécurisés
- Protéger les réseaux et les workloads Azure
- Gérer la sécurité des données et applications
- Superviser et répondre aux incidents de sécurité dans Azure
- Se préparer à la certification AZ-500 Microsoft Azure Security Engineer Associate

Objectifs opérationnels :

- Concevoir, déployer et administrer une stratégie de sécurité complète sur Azure : gérer les identités et contrôles d'accès, sécuriser les réseaux et workloads, protéger les données et applications, détecter et répondre aux menaces avec les outils Azure (Defender, Sentinel), et appliquer des politiques de conformité.

Programme

Jour 1 – Gestion des identités et contrôles d'accès

Concepts fondamentaux de sécurité dans Azure

Gestion des identités avec Azure Active Directory (AAD)

Utilisateurs, groupes et rôles
MFA et Conditional Access
Identity Protection et Privileged Identity Management (PIM)

Sécurisation des accès avec RBAC et stratégies avancées

Travaux pratiques

Configurer MFA et Conditional Access
Mettre en place une stratégie PIM pour administrateurs

Jour 2 – Sécurisation des plateformes et des réseaux

Sécurisation des réseaux virtuels

Network Security Groups (NSG)
Azure Firewall et Bastion
DDoS Protection

Conception d'architectures sécurisées pour les workloads

Sécurisation des points de terminaison et des VM

Microsoft Defender for Servers
Just-In-Time VM Access

Travaux pratiques

Déployer et configurer un NSG et un Firewall
Configurer JIT Access sur une VM

Jour 3 – Protection des données et applications

Protection des données dans Azure

Chiffrement des données au repos et en transit
Azure Key Vault (gestion des secrets et clés)
Azure Storage Security

Sécurisation des applications

Application Gateway & WAF
Azure App Service Security
Container Security (AKS, ACR)

Travaux pratiques

Stocker des secrets dans Key Vault et les utiliser dans une application
Configurer un WAF pour sécuriser une application web

Jour 4 – Supervision et réponse aux menaces

Surveillance et détection des menaces

Microsoft Defender for Cloud (anciennement Security Center)
Microsoft Sentinel (SIEM & SOAR)
Alertes et automatisation des réponses

Sécurité opérationnelle et conformité

Azure Policy pour la sécurité
Audits et rapports de conformité (ISO, RGPD, etc.)

Préparation à la certification AZ-500

Domaines d’examen et conseils pratiques
Simulations et QCM

Travaux pratiques

Configurer Defender for Cloud et activer des alertes
Déployer Sentinel et analyser des incidents de sécurité