

## Formation Microsoft Azure Security Technologies (Exam AZ-500)

Formation éligible au CPF, contactez-nous au 22 519 09 66

<b>Durée :</b>	5 jours
<b>Public :</b>	Administrateurs Systèmes Microsoft avec bonnes connaissances d'Azure
<b>Pré-requis :</b>	Formation Microsoft Azure AZ-104 Administration ou les connaissances équivalentes
<b>Objectifs :</b>	Gérer et comprendre les mécanismes de protection des données Azure - Savoir implémenter des méthodes de chiffrement de données Azure - Connaître les protocoles sécurisés et savoir les mettre en place sur Azure.
<b>Sanction :</b>	Attestation de fin de stage mentionnant le résultat des acquis
<b>Taux de retour à l'emploi:</b>	Aucune donnée disponible
<b>Référence:</b>	CLO101550-F
<b>Code CPF:</b>	331066 - contactez-nous au 22 519 09 66
<b>Note de satisfaction des participants:</b>	Pas de données disponibles
<b>Certifications :</b>	MICROSOFT : Microsoft 365 Security Administration (Examen MS-500) Pas de données disponibles au 01/04/2024

### Gérer les identités dans Azure Active Directory (Azure AD)

- Créer et gérer des principaux pour les ressources Azure
- Gérer les groupes Azure AD
- Gérer les utilisateurs Azure AD
- Gérer les comptes externes en utilisant Azure AD
- Gérer les unités d'administration

### Sécuriser les accès avec Azure AD

- Configurer Azure AD Privileged Identity Management (PIM)
- Mettre en place Conditional Access policies, ainsi que le MFA
- Mettre en place Azure AD Identity Protection
- Gérer de l'authentification sans mot de passe
- Examiner les accès

### Gérer les accès des applications

- Intégrer le single sign-on (SSO) et les fournisseurs d'identités pour l'authentification
- Créer une inscription d'application

- Configurer les étendues des autorisations d'application
- Gérer le consentement des autorisations d'application
- Gérer l'accès via API permissions aux abonnements et aux ressources Azure
- Configurer une méthode d'authentification pour le principal de service

### **Gérer le contrôle d'accès**

- Configurer les rôles et permissions Azure pour gérer les accès
- Comprendre les rôles et les permissions des ressources
- Utiliser des rôles standard Azure AD
- Créer et utiliser des rôles personnalisés

### **Sécurité réseau avancée**

- Sécuriser la connectivité des réseaux hybrides networks
- Sécuriser les réseaux virtuels
- Créer et configurer Azure Firewall
- Créer et configurer Azure Firewall Manager
- Créer et utiliser Azure Application Gateway
- Créer et utiliser Azure Front Door
- Utiliser le Web Application Firewall (WAF)
- Configurer le pare-feu sur une ressource, dont les comptes de stockage, Azure SQL, Azure Key Vault ou Azure App Service
- Isoler les réseaux pour les Web Apps et les Azure Functions
- Mettre en oeuvre Azure Service Endpoints
- Implémenter les Azure Private Endpoints, dont l'intégration avec les autres services - Mettre en place Azure Private Links
- Utiliser Azure DDoS Protection

### **Sécurité avancée pour VMs et containers**

- Configurer Azure Endpoint Protection pour les machines virtuelles(VMs)
- Gérer les mises à jour de sécurité pour les VMs
- Configurer la sécurité pour les services de container
- Gérer les accès à Azure Container Registry
- Sécuriser les containers
- Sécuriser les Azure App Services
- Chiffrer les données du tenant
- Chiffrer les données en transit

### **Gestion des stratégies centralisées**

- Configurer une stratégie de sécurité personnalisée
- Créer une stratégie d'initiatives
- Configurer les paramètres de sécurité et d'audit avec Azure Policy

### **Configurer une protection contre les menaces**

- Configurer Azure Defender for Servers
- Évaluer les scans de vulnérabilité d'Azure Defender
- Configurer Azure Defender pour SQL
- Utiliser Microsoft Threat Modeling Tool

## **Gérer les solutions de supervision de sécurité**

- Créer et personnaliser des règles d'alerte avec Azure Monitor
- Configurer les logs de diagnostic et la rétention de log avec Azure Monitor
- Surveiller les logs de sécurité avec Azure Monitor
- Créer et personnaliser des règles d'alerte avec Azure Sentinel
- Configurer des connecteurs avec Azure Sentinel
- Evaluer les alertes et incidents dans Azure Sentinel

## **Sécuriser le stockage**

- Configurer le contrôle d'accès sur les comptes de stockage
- Configurer les clés d'accès des comptes de stockage SAS
- Configurer l'authentification via Azure AD pour Azure Storage et Azure Files
- Configurer les accès délégués

## **Sécuriser les données**

- Activer authentification des base de données avec using Azure AD
- Activer l'audit des bases de données
- Configurer le masquage dynamique de données avec SQL workloads
- Mettre en oeuvre le chiffrement de base de données pour Azure SQL Database
- Implémenter l'isolation réseau pour le stockage des données, dont Azure Synapse Analytics et Azure Cosmos DB

## **Configurer et gérer Azure Key Vault**

- Créer et configurer Key Vault
- Configurer les accès à Key Vault
- Gérer les certificats, les secrets et les clés
- Configurer la rotation de clé
- Gérer les sauvegardes et récupération des certificats, secrets et clés