Les technologies de sécurité en environnement Microsoft Azure

Durée: 4 Jours **Réf de cours: M-AZ500** **Version: A** **Méthodes d'apprentissage: Intra-entreprise & sur-mesure**

Résumé:

Cette formation permet aux participants d'acquérir les compétences et les connaissances nécessaires pour mettre en œuvre des contrôles de sécurité, maintenir la posture de sécurité, identifier et corriger les vulnérabilités en utilisant une variété d'outils de sécurité. La formation couvre les scripts et l'automatisation, la virtualisation et l'architecture N-Tier Cloud.
Cette formation est éligible au Compte Personnel de Formation (CPF) sur moncompteformation.gouv.fr
Mise à jour : 26.11.2022

Public visé:

Cette formation s'adresse aux administrateurs Azure qui veulent comprendre, mettre en place et surveiller la sécurité des ressources Azure

Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Décrire les classifications spécifiques des données sur Azure?
- Identifier les mécanismes de protection des données dans Azure
- Mettre en oeuvre des méthodes de chiffrement de données dans Azure
- Appliquer la sécurité des procoles Internet et les mettre en oeuvre dans Azure
- Décrire les services et fonctionnalités de sécurité Azure

Pré-requis:

Les participants doivent être certifiés Microsoft Azure Administrator Associate ou avoir les connaissances équivalentes.La connaissance les différentes charges de travail Azure ainsi que des notions de sécurité applicables à ces charges est indispensable.

Test et certification

La formation prépare à l'examen AZ-500 – Microsoft Azure Security Technologies, pour obtenir la **certification Microsoft Certified Azure Security Engineer Associate.** (Certification éditeur)

***

Cette formation mène également à la Certification professionnelle inscrite au Répertoire Spécifique de France Compétences RS5308 "Garantir la sécurité de l'infrastructure Cloud Microsoft Azure". Plus de détails sur : https://www.francecompetences.fr/recherche/rs/5308/

Contenu:

Gestion des Identité et accès

- Configurer Azure Active Directory pour les charges de travail Azure workloads et les abonnements
- Configurer Azure AD Privileged Identity Management
- Configurer la securité pour les abonnements Azure

Protection de la plate-forme

- Comprendre la sécurité cloud
- Créer un réseau
- Sécuriser le réseau
- Mettre en place la sécurité des hôtes
- Implémenter la sécurité de la plateforme
- Implémenter la sécurité des abonnements

Opérations de sécurité

- Configurer les services de sécurité
- Configurer des stratégies de sécurité à l'aide d'Azure Security Center
- Gérer les alertes de sécurité
- Répondez aux problèmes de sécurité et les corriger
- Create security baselines

Données et applications

- Configurer des stratégies de sécurité pour gérer les données
- Configurer la sécurité pour l'infrastructure de données
- Configurer le chiffrement pour les données at rest
- Comprendre la sécurité des applications
- Implémenter la sécurité pour le cycle de vie des applications
- Sécuriser les applications
- Configurer et gérer Azure Key Vault

Travaux pratiques

- Contrôle d'accès basé sur les rôles
- Politique Azure
- Verrous du Resource Manager
- MFA, accès conditionnel et protection de l'identité AAD
- Gestion des identités privilégiées d'Azure AD
- Mise en oeuvre de la synchronisation des répertoires
- Groupes de sécurité réseau et groupes de sécurité des applications
- Pare-feu Azure
- Configuration et sécurisation de l'ACR et de l'AKS
- Key Vault (mise en oeuvre de la sécurisation des données par la configuration de Always Encrypted)
- Sécurisation d'Azure SQL Database
- Points d'extrémité des services et sécurisation du stockage
- Azure Monitor
- Centre de sécurité Azure
- Azure Sentinel

Méthodes pédagogiques :

Accès fourni au contenu digital officiel Microsoft
Notez que nous fournissons aux participants un support de cours au format électronique.
Pour profiter pleinement du support électronique dès le 1er jour, nous invitons les participants à se munir d'un PC ou d'une tablette, qu'ils pourront connecter en WiFi dans nos locaux de Rueil, Lyon ou Lille.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

•Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
•Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
•Attention, si vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.