

CERTIFICATION MS AZURE SECURITY ENGINEER ASSOCIATE

Le programme de certification MS Azure Security Engineer Associate est conçu pour les professionnels désirant acquérir des compétences avancées en sécurité informatique dans l'environnement Microsoft Azure.



Ce cours offre une formation complète et approfondie pour maîtriser les outils et technologies nécessaires à la protection des systèmes d'information, à la gestion des menaces et à l'amélioration de la conformité aux réglementations en matière de sécurité. Grâce à une approche pratique et stratégique, ce cours permettra aux participants de se préparer efficacement à l'examen officiel pour devenir Azure Security Engineer Associate.

La certification Microsoft Certified: Azure Security Engineer Associate s'adresse aux professionnels en sécurité des données qui protègent les environnements Azure. Cette certification valide vos compétences en gestion des identités et des accès, en sécurisation des données, des applications et des réseaux, ainsi qu'en gestion des incidents de sécurité.

Idéale pour renforcer les compétences du participant en cybersécurité, cette certification est reconnue mondialement et offre une expertise précieuse pour répondre aux besoins croissants en matière de sécurité dans le cloud.

OBJECTIFS

- Comprendre les principes fondamentaux de la sécurité cloud et les appliquer à l'écosystème Azure.
- Configurer et gérer les stratégies de sécurité sur Azure.
- Implémenter la protection des identités et des données sensibles.
- Gérer les solutions de surveillance, d'analyse des menaces et de réponse aux incidents.
- Assurer la conformité avec les normes de sécurité et réglementations.
- Optimiser les systèmes de défense pour prévenir les cyberattaques.

CONTENU

1. Introduction à la sécurité Azure

- Concepts fondamentaux de la sécurité dans le cloud
- Rôle et responsabilités d'un Azure Security Engineer Associate

2. Gestion des identités et des accès

- Configuration et administration d'Azure Active Directory (AAD)
- Mise en œuvre des politiques d'authentification multi-facteurs (MFA)
- Gestion des rôles et des accès basés sur les identités

3. Protection des données sensibles

- Implémentation de la classification et de l'étiquetage des données
- Chiffrement des données au repos et en transit
- Configuration de la prévention des pertes de données (DLP)

4. Gestion des stratégies de sécurité

- Création et gestion des règles de sécurité
- Configuration des pare-feu et réseaux sécurisés
- Surveillance des points de terminaison avec Microsoft Defender

5. Analyse des menaces et réponse aux incidents

- Surveillance des journaux et gestion des alertes
- Utilisation d'Azure Sentinel pour l'analyse des menaces
- Planification et mise en œuvre de stratégies de réponse aux incidents

6. Conformité et audits

- Utilisation des outils Azure pour la conformité (Azure Policy, Blueprints)
- Audit des systèmes pour garantir l'alignement avec les normes
- *Reporting* et recommandations pour l'amélioration continue

7. Optimisation de la sécurité

- Analyse des points faibles et recommandations
- Planification de la continuité des activités et de la reprise après sinistre
- Outils avancés de protection et d'automatisation de la sécurité