EduGroupe
Accompagner pour réussir

Mettre en place des contrôles de sécurité Microsoft complets pour les charges de travail dans le cloud et liées à l'IA (SC-500)

Référence : **MSSC500** Durée : **4 jours (28 heures)** Certification : **SC-500**

CONNAISSANCES PRÉALABLE

- Il est recommandé d'avoir des connaissances de base sur les concepts de sécurité dans le cloud, la gestion des identités et des accès, les réseaux et l'administration de Microsoft Azure
- Disposer d'une expérience pratique dans l'administration de Microsoft Azure et d'environnements hybrides, notamment en matière de ressources de calcul, de réseau et de stockage
- Bien maîtriser Microsoft Entra ID et avoir une bonne connaissance de l'administration de Microsoft 365 et des technologies de sécurité Microsoft

PROFIL DES STAGIAIRES

- Ingénieurs en sécurité Cloud et IA
- Ingénieurs en sécurité Azure
- Professionnels IT en charge de la sécurité des environnements Cloud, hybrides et Microsoft 365

OBJECTIFS

- Sécuriser l'accès aux ressources à l'aide de Microsoft Entra
- Sécuriser Azure Key Vault grâce à une défense en profondeur pour le cloud et les charges de travail d'IA
- Appliquer la gouvernance de sécurité et la conformité réglementaire
- Mettre en œuvre la sécurité d'Azure Storage pour les ingénieurs en sécurité du cloud et de l'IA
- Mettre en œuvre la sécurité des bases de données Azure SQL
- Mettre en œuvre des contrôles de sécurité réseau dans Azure
- Mettre en œuvre la sécurité de l'IA
- Mettre en œuvre la sécurité des serveurs et des machines virtuelles
- Sécuriser les services de la plateforme d'applications Azure pour les ingénieurs en sécurité du cloud et de l'IA
- Gérer la posture de sécurité à l'aide de Microsoft Defender for Cloud
- Mettre en œuvre la collecte d'activités et d'événements dans Microsoft Sentinel
- Déployer et exploiter Microsoft Security Copilot

CERTIFICATION PRÉPARÉE

Cette formation officielle Microsoft prépare aux compétences évaluées lors de l'examen SC-500 et à la certification Microsoft Certified: Cloud and AI Security Engineer Associate. Elle couvre notamment la sécurisation des identités, des infrastructures Cloud, des données et des charges de travail IA.

Cet examen est le successeur de l'examen AZ-500 (expirationt le 31 août 2026)

MÉTHODES PÉDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

- Consultant-formateur expert Microsoft

MÉTHODES D'ÉVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

ACCESSIBILITÉ DE LA FORMATION

- EduGroupe met en place un ensemble de dispositifs pour accueillir, accompagner et adapter ses formations aux personnes en situation de handicap (PSH).
- Notre référent(e) handicap se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour tout besoin d'aménagement, afin de vous offrir la meilleure expérience possible.

EduGroupe
Accompagner pour réussir

CONTENU DU COURS

1. Sécuriser l'accès aux ressources à l'aide de Microsoft Entra

- Gérer et mettre en œuvre des méthodes d'authentification dans Microsoft Entra ID
- Mettre en œuvre et configurer la gestion des identités privilégiées (PIM)
- Authentifier votre plugin API pour les agents déclaratifs à l'aide d'API sécurisées

2. Sécuriser Azure Key Vault grâce à une protection renforcée pour le cloud et les workloads IA

- Configurer et sécuriser Azure Key Vault
- Gérer les clés et les secrets dans Azure Key Vault
- Gérer les certificats et surveiller Azure Key Vault
- Protéger Azure Key Vault avec Microsoft Defender for Cloud

3. Assurer la gouvernance en matière de sécurité et la conformité réglementaire

- Appliquer la gouvernance à l'aide d'Azure Policy et des restrictions de ressources
- Configurer des contrôles de sécurité et mettre en œuvre les recommandations dans Defender for Cloud
- Évaluer la conformité réglementaire dans Defender for Cloud
- Gérer et adapter les attributions de rôles RBAC selon le principe du privilège minimal
- Protéger les données de sauvegarde grâce aux fonctionnalités de sécurité d'Azure Backup
- Mettre en œuvre des contrôles de sécurité dans l'infrastructure en tant que code

4. Mettre en œuvre la sécurité d'Azure Storage pour les ingénieurs spécialisés dans la sécurité du cloud et de l'IA

- Décrire les services de stockage Azure
- Mettre en œuvre la sécurité et gérer les accès pour Azure Storage
- Configurer la sécurité réseau pour Azure Storage
- Mettre en œuvre Microsoft Defender for Storage

5. Mettre en place la sécurisation des bases de données SQL Azure

- Configurer la sécurité au niveau de la plateforme pour Azure SQL
- Configurer l'audit pour Azure SQL Database et SQL Managed Instance
- Déployer Microsoft Defender pour les bases de données

6. Appliquer des mesures de sécurité réseau dans Azure

- Segmenter et isoler les Workloads Azure à l'aide de contrôles de sécurité réseau
- Centraliser et appliquer l'inspection du trafic à l'aide d'Azure Firewall
- Sécuriser la connectivité à distance et hybride à l'aide de passerelles VPN et de Microsoft Entra Private Access
- Éliminer l'exposition des services PaaS Azure dans les réseaux publics

7. Mettre en place des mesures de sécurité pour l'IA

- Sécuriser l'accès pour Microsoft Entra Agent Identity
- Analyser les risques liés à l'identité dans le domaine de l'IA à l'aide de Microsoft Defender XDR
- Activer la protection en temps réel pour les agents Copilot Studio
- Configurer la sécurité d'AI Gateway dans Microsoft Foundry
- Configurer et gérer les garde-fous dans Microsoft Foundry
- Protéger les charges de travail d'IA avec Microsoft Defender for Cloud
- Activer la protection des charges de travail Defender for AI Services dans Microsoft Defender for Cloud
- Gérer les agents à l'aide de Microsoft Agent 365
- Identifier les risques liés aux données d'IA à l'aide de Microsoft Purview Data Security Posture Management

8. Mettre en place des mesures de sécurité pour les serveurs et les machines virtuelles

- Mettre en œuvre le chiffrement des disques pour les machines virtuelles Azure
- Configurer les fonctionnalités de sécurité « Trusted Launch » pour les machines virtuelles Azure
- Planifier et mettre en œuvre Azure Bastion
- Gérer la sécurité des serveurs hybrides prenant en charge Arc
- Mettre en œuvre Microsoft Defender pour les serveurs
- Activer et appliquer l'accès « juste à temps » aux machines virtuelles
- Appliquer la configuration de sécurité des machines virtuelles à l'aide d'Azure Machine Configuration

9. Sécuriser les services de la plateforme d'applications Azure pour les ingénieurs sécurité cloud et IA

- Détecter les risques liés aux conteneurs à l'aide de Microsoft Defender for Containers
- Mettre en œuvre des contrôles de sécurité pour Azure Kubernetes Service, Azure Container Registry, Container Instances et Container Apps, les applications Azure Functions et les applications Logic, Azure App Services et le pare-feu d'applications Web
- Mettre en œuvre la sécurité du backend des API à l'aide d'Azure API Management

10. Gérer la stratégie de sécurité à l'aide de Microsoft Defender for Cloud

- Connecter des environnements hybrides et multicloud à Microsoft Defender for Cloud
- Identifier les risques de sécurité à l'aide de la gestion de la stratégie de sécurité dans le cloud (Cloud Security Posture Management)
- Détecter les ressources non protégées et les vulnérabilités à l'aide de Microsoft Defender External Attack Surface Management
- Évaluer la conformité réglementaire dans Defender for Cloud
- Activer et configurer des plans de protection des workloads dans Microsoft Defender for Cloud
- Configurer les paramètres de gestion des vulnérabilités de Microsoft Defender pour les machines virtuelles Azure

11. Mettre en place la collecte des activités et des incidents dans Microsoft Sentinel

- Créer et gérer des espaces de travail Microsoft Sentinel
- Gérer le contenu dans Microsoft Sentinel
- Connecter à Microsoft Sentinel : des services Microsoft, des sources de données syslog, des journaux au format CEF (Common Event Format), des hôtes Windows
- Mettre en œuvre des règles d'automatisation et des playbooks dans Microsoft Sentinel
- Gérer le stockage des données et interroger les journaux d'audit dans Microsoft Sentinel

12. Déployer et utiliser Microsoft Security Copilot

- Décrire Microsoft Security Copilot
- Configurer les espaces de travail pour Microsoft Security Copilot
- Gérer les plug-ins et les agents dans Microsoft Security Copilot