+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 14/09/2026

S'inscrire

Formation Microsoft Cloud and AI Security Engineer Associate (SC-500)

Ex AZ-500

4 jours (28 heures)

Présentation

La formation Microsoft Cloud and AI Security Engineer Associate vous prépare à sécuriser les identités, les données, les infrastructures Cloud et les nouveaux workloads IA dans des environnements Azure, hybrides et multicloud.

Vous apprendrez à protéger les accès avec Microsoft Entra ID, à sécuriser les réseaux, les ressources de calcul, le stockage et les bases de données, puis à appliquer des politiques de sécurité et de conformité adaptées aux environnements Cloud.

La formation intègre les nouveaux enjeux de sécurité des applications et agents IA. Vous étudierez la protection des données, des identités agentiques et des workloads utilisant Microsoft Foundry et Copilot Studio, ainsi que les contrôles nécessaires pour limiter leur surface d'attaque.

Vous apprendrez également à évaluer et améliorer votre posture de sécurité avec Microsoft Defender for Cloud et à exploiter les outils Microsoft pour superviser, investiguer et prioriser les risques dans des environnements Cloud et IA.

À l'issue de la formation, vous serez en mesure de mettre en œuvre une stratégie de sécurité de bout en bout et de préparer la certification Microsoft Certified: Cloud and AI Security Engineer Associate.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Sécuriser les identités et les accès avec Microsoft Entra ID
- Protéger les réseaux, données et ressources de calcul Azure
- Mettre en œuvre une démarche de Cloud Security Posture Management
- Sécuriser les applications, workloads et agents IA de l'écosystème Microsoft
- Superviser et prioriser les risques avec les solutions de sécurité Microsoft
- Préparer la certification Microsoft Cloud and AI Security Engineer Associate

Public visé

- Ingénieurs sécurité Cloud
- Ingénieurs sécurité Azure
- Administrateurs sécurité Cloud
- Ingénieurs IAM
- Consultants Cloud Security

Pré-requis

- Disposer d'une expérience pratique de l'administration de Microsoft Azure
- Connaître les fondamentaux des réseaux, du stockage et des ressources de calcul Azure
- Maîtriser les principes de gestion des identités et des accès avec Microsoft Entra ID
- Connaître les fondamentaux de la sécurité Cloud et du modèle de responsabilité partagée
- Une connaissance de Microsoft 365 et des environnements hybrides est recommandée

Pré-requis techniques

- Poste sous Windows 10 ou 11, macOS ou Linux, avec 8 Go de RAM minimum
- Compte Microsoft professionnel associé à un tenant Microsoft Entra ID de formation

Programme de notre formation certification Microsoft Cloud and AI Security Engineer Associate

[Jour 1 - Matin]

Sécuriser les identités et les accès avec Microsoft Entra

- Appliquer les principes du Zero Trust à la gestion des identités et des accès dans Azure
- Configurer l'authentification multifacteur, les méthodes passwordless et les stratégies d'accès conditionnel
- Administrer les rôles Azure RBAC et les rôles Microsoft Entra ID selon le principe du moindre privilège
- Sécuriser les accès privilégiés avec Privileged Identity Management (PIM) et les mécanismes Just-In-Time
- Protéger les identités applicatives, Managed Identities, autorisations OAuth et accès des workloads

- Contrôler les identités utilisées par les applications et agents IA dans l’écosystème Microsoft

[Jour 1 - Après-midi]

Protéger les secrets et appliquer la gouvernance Cloud

- Administrer Azure Key Vault pour protéger les secrets, clés et certificats
- Configurer les autorisations, la rotation des secrets et l’utilisation des identités managées
- Mettre en œuvre Azure Policy pour appliquer les exigences de sécurité et de conformité
- Évaluer les recommandations, standards réglementaires et écarts de configuration avec Microsoft Defender for Cloud
- Appliquer les principes de gouvernance aux ressources Azure, hybrides et multicloud
- Atelier pratique : sécuriser les identités privilégiées, protéger les secrets et appliquer une politique de conformité à l’environnement fil rouge

[Jour 2 - Matin]

Sécuriser les réseaux et les communications Azure

- Segmenter les réseaux avec NSG, ASG et Azure Virtual Network Manager
- Configurer Azure Firewall et les politiques de filtrage des communications
- Protéger les connexions avec VPN, Virtual WAN et les mécanismes d’accès privé
- Utiliser Private Endpoint et Private Link pour limiter l’exposition publique des services Azure
- Sécuriser les accès aux applications et ressources internes avec les mécanismes de connectivité privée
- Analyser les flux et identifier les configurations réseau augmentant la surface d’attaque

[Jour 2 - Après-midi]

Protéger le stockage, les bases de données et les données sensibles

- Sécuriser Azure Storage avec RBAC, SAS, chiffrement et restrictions réseau
- Configurer les clés gérées par le client et les mécanismes de protection des données sensibles
- Protéger Azure SQL avec authentification Microsoft Entra, chiffrement, audit et restrictions réseau
- Utiliser Microsoft Defender pour renforcer la protection des services de stockage et des bases de données
- Mettre en œuvre l’immutabilité et les mécanismes adaptés à la protection contre la modification ou la suppression des données
- Atelier pratique : isoler les services de données de l’environnement fil rouge et sécuriser leurs accès, communications et secrets

[Jour 3 - Matin]

Sécuriser le compute et les plateformes applicatives

- Durcir les machines virtuelles avec Secure Boot, vTPM et les mécanismes de protection des workloads
- Mettre en œuvre la gestion des vulnérabilités, la protection des endpoints et les recommandations de Microsoft Defender for Servers
- Sécuriser les services applicatifs Azure et limiter leur exposition réseau
- Protéger les environnements conteneurisés, les registres d'images et les workloads Cloud Native
- Configurer les identités managées et l'accès sécurisé aux ressources depuis les applications
- Identifier et corriger les mauvaises configurations affectant la sécurité du compute

[Jour 3 - Après-midi]

Sécuriser les workloads, applications et agents IA

- Identifier les risques propres aux applications IA et aux agents : données sensibles, identités, permissions et outils connectés
- Évaluer la posture des données utilisées par les solutions IA avec les capacités de Microsoft Purview
- Sécuriser les identités et autorisations utilisées par les agents et applications intelligentes
- Appliquer les contrôles de sécurité aux solutions développées avec Microsoft Foundry et Microsoft Copilot Studio
- Mettre en œuvre les garde-fous et mécanismes de protection nécessaires aux interactions avec les modèles et outils externes
- Atelier pratique : analyser une application agentique, identifier son exposition aux données et outils puis définir les contrôles de sécurité adaptés

[Jour 4 - Matin]

Gérer la posture de sécurité Cloud, hybride et multicloud

- Configurer Microsoft Defender for Cloud et exploiter le Secure Score pour prioriser les remédiations
- Mettre en œuvre les fonctionnalités de Cloud Security Posture Management (CSPM)
- Évaluer les vulnérabilités, secrets exposés, mauvaises configurations et chemins d'attaque
- Contrôler la conformité des ressources avec les standards et exigences réglementaires
- Étendre la gestion de posture et la protection des workloads aux environnements hybrides, AWS et GCP
- Prioriser les recommandations selon le risque, l'exposition et l'impact sur les workloads

[Jour 4 - Après-midi]

Superviser la sécurité et préparer la certification Cloud and AI Security Engineer Associate

- Centraliser et exploiter les signaux de sécurité issus des ressources Cloud, des identités et des workloads

- Utiliser Microsoft Sentinel et Microsoft Defender XDR pour investiguer les alertes et incidents
- Exploiter Microsoft Security Copilot pour assister l’analyse, l’investigation et la remédiation
- Corréler les informations de posture, vulnérabilités, identités et menaces afin de prioriser les actions de sécurité
- Réviser les domaines de l’examen SC-500 et analyser les scénarios représentatifs de la certification
- Atelier final : auditer l’environnement, identifier les risques Cloud et IA, prioriser les remédiations et résoudre un scénario

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.