New

Sécurité cloud et IA sur Azure : Implémenter des contrôles de sécurité de bout en bout

Maîtrisez la sécurité cloud et IA de bout en bout sur Microsoft Azure et Microsoft 365 pour protéger les identités, les données et les charges de travail avec une approche Zero Trust, conforme et directement opérationnelle.

Présentiel ou en classe à distance

4 jours (28 h)
+ certificat optionnel

Prix inter : 2.950,00 € HT
Forfait intra : 8.790,00 € HT

Réf.: MSSC500

Formation officielle Microsoft

Idéal en Distanciel

Cette formation Azure et Microsoft 365 prépare à sécuriser les charges de travail cloud et IA de bout en bout, en couvrant l'identité, les accès, les secrets, les données, la conformité et la détection des menaces. Elle s'appuie sur des technologies clés comme Microsoft Entra ID, PIM, Azure Key Vault, Azure Policy, Microsoft Defender for Cloud, Azure Storage et Azure SQL, pour développer une expertise opérationnelle en sécurité Zero Trust adaptée aux environnements cloud modernes et aux usages d'IA générative
Cette formation prépare à la certification Microsoft certified Cloud and AI Security Engineer Associate.

A qui s'adresse cette formation ?

Pour qui

- Ingénieurs en sécurité Cloud
- Architectes Cloud / Architectes Sécurité
- Administrateurs Systèmes et Cloud
- Ingénieurs infrastructure / Ingénieurs Cloud
- Analystes sécurité / Analystes SOC
- Développeurs applicatif / Développeurs Cloud

Prérequis

- Avoir suivi la formation "Microsoft Azure – Administration" (MSAZ104)
- Bonne connaissance de Microsoft Azure et des concepts de sécurité cloud
- Bases solides en Microsoft Entra ID, RBAC et administration Azure
- Compréhension des principes Zero Trust et du moindre privilège
- Connaissances fondamentales de Microsoft Defender for Cloud
- Notions de réseau Azure, Key Vault, Stockage Azure et Azure SQL
- Expérience pratique recommandée sur des environnements cloud ou hybrides
- Disposez-vous des connaissances nécessaires pour suivre cette formation ? Testez-vous !

Programme

1 - Sécuriser l’accès aux ressources à l’aide de Microsoft Entra

- Concevoir et déployer une authentification sécurisée dans Microsoft Entra ID
- Configurer l’authentification multifacteur MFA avec accès conditionnel Azure
- Mettre en place des options sans mot de passe pour renforcer la sécurité cloud Azure
- Paramétrer la réinitialisation de mot de passe en libre-service pour les environnements hybrides
- Déployer Privileged Identity Management (PIM) pour l’accès just-in-time
- Appliquer les principes de Zero Trust et du moindre privilège
- Sécuriser les applications IA et les agents déclaratifs utilisant des plug-ins d’API
  Ateliers pratiques

  Configurer une stratégie d’authentification multifacteur

  Mettre en place une règle d’accès conditionnel

  Déployer un scénario d’accès privilégié just-in-time avec PIM

  Sécuriser un cas d’usage d’application IA avec identité et accès contrôlés

2 - Sécuriser Azure Key Vault avec la défense en profondeur pour les charges de travail cloud et IA

- Renforcer la sécurité Azure Key Vault pour les environnements d’entreprise
- Appliquer l’accès RBAC et l’activation à la demande pour les opérations sensibles
- Sécuriser l’accès réseau avec des règles de pare-feu et des points de terminaison privés Azure
- Gérer le cycle de vie des clés, secrets et certificats
- Mettre en oeuvre la rotation automatisée des clés et secrets
- Exploiter Microsoft Defender for Cloud pour détecter les menaces ciblant les coffres-forts
- Protéger les secrets exposés dans les charges de travail cloud et IA
  Ateliers pratiques

  Déployer et sécuriser un Azure Key Vault

  Configurer les droits d’accès avec RBAC

  Ajouter des règles réseau et un point de terminaison privé

  Mettre en place la rotation d’un secret et d’une clé de chiffrement

3 - Appliquer la gouvernance de la sécurité et la conformité réglementaire

- Déployer des Azure Policy pour appliquer les règles de gouvernance Azure
- Utiliser les verrous de ressources pour protéger les ressources critiques
- Corriger les recommandations de sécurité dans Microsoft Defender for Cloud
- Évaluer la posture de conformité réglementaire
- Gérer les attributions RBAC à grande échelle selon le principe du moindre privilège
- Protéger les données de sauvegarde contre les ransomwares et suppressions non autorisées
- Intégrer des contrôles de sécurité dans les pipelines Bicep et les pratiques DevSecOps Azure
  Ateliers pratiques

  Créer une Azure Policy pour imposer une configuration de sécurité

  Déployer un verrou de ressource

  Corriger une recommandation dans Defender for Cloud

  Contrôler la conformité d’un environnement Azure à partir d’un scénario métier

4 - Implémenter la sécurité pour Stockage Azure pour l’ingénieur de sécurité cloud et IA

- Comprendre les services et architectures de Stockage Azure
- Sécuriser les comptes de stockage et les accès avec identité managée Azure et RBAC
- Configurer les paramètres de sécurité du compte de stockage
- Mettre en place des stratégies d’accès et désactiver l’accès par clé partagée
- Appliquer des contrôles réseau avec pare-feu, règles IP et points de terminaison privés Azure
- Déployer Microsoft Defender for Storage
- Détecter les fichiers malveillants, données sensibles et menaces liées aux charges de travail IA
  Ateliers pratiques

  Sécuriser un compte de Stockage Azure

  Configurer l’accès via identité managée

  Restreindre l’accès réseau au stockage

Activer Microsoft Defender for Storage et analyser une alerte de sécurité

5 - Implémenter la sécurité pour les bases de données Azure SQL

- Sécuriser Azure SQL Database et SQL Managed Instance
- Configurer l'authentification via Microsoft Entra ID
- Mettre en oeuvre l'isolation réseau avec des points de terminaison privés Azure
- Activer le chiffrement et les contrôles d'accès avancés
- Déployer le masquage dynamique des données et la sécurité au niveau des lignes
- Configurer l'audit pour répondre aux exigences de conformité
- Activer Microsoft Defender for Databases pour détecter les injections SQL et les comportements anormaux

Ateliers pratiques

Sécuriser une base Azure SQL avec Microsoft Entra ID

Mettre en place un point de terminaison privé

Configurer l'audit SQL et le suivi des événements

Activer Defender for Databases et examiner une alerte

Les objectifs de la formation

- Concevoir et déployer des contrôles d'accès sécurisés avec Microsoft Entra ID, MFA, accès conditionnel Azure et Privileged Identity Management (PIM).
- Renforcer la sécurité Azure Key Vault grâce à l'activation à la demande, au RBAC, aux contrôles réseau et à la gestion du cycle de vie des secrets, clés et certificats.
- Appliquer une stratégie de défense en profondeur Azure sur les charges de travail cloud, hybrides et IA.
- Déployer et gouverner des environnements sécurisés avec Azure Policy, verrous de ressources, remédiation et conformité réglementaire.
- Sécuriser le stockage Azure à l'aide de l'identité managée Azure, des stratégies d'accès, des pare-feu et des points de terminaison privés Azure.
- Protéger les bases de données avec des mécanismes de sécurité Azure SQL, d'audit, de chiffrement et de détection des menaces.
- Activer et exploiter Microsoft Defender for Cloud et Microsoft Defender for Storage / Databases / Key Vault pour améliorer la posture de sécurité.
- Intégrer des contrôles de sécurité dans les workflows DevSecOps Azure et les pipelines Bicep.
- Sécuriser les solutions d'IA générative et les agents autonomes, y compris les plug-ins d'API et les usages Microsoft 365 Copilot.
- Mettre en oeuvre une posture Zero Trust pour réduire les privilèges, maîtriser les risques et renforcer la conformité.

Certificat

- Pendant la formation, le formateur évalue la progression pédagogique des participants via des QCM, des mises en situation et des travaux pratiques. Les participants passent un test de positionnement avant et après la formation pour valider leurs compétences acquises.

Les points forts de la formation

- Une pédagogie active et variée : les phases de cours magistral sont complétées par des moments d'échanges et des séances de mise en pratique des acquis
- Les travaux pratiques permettent aux participants de développer une expérience concrète de la mise en place de la sécurité cloud et IA sur Azure
- L'expertise technique et l'expérience de consultants de haut niveau
- Ce stage, à la fois riche et intensif, sera rythmé par des sessions de formation ajustées aux besoins et aux attentes de chaque groupe.

Dates et villes 2026 - Référence MSSC500

Dernières places disponibles Session garantie

A distance

du 26 oct. au 29 oct.	du 14 déc. au 17 déc.

Paris

du 26 oct. au 29 oct.	du 14 déc. au 17 déc.