

Microsoft Azure – Gestion de la sécurité

2 jours (14 heures)

Expertise

Présentiel ou classe à distance

à partir de

1 470 € HT par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 04/10/2026.

Objectifs

A l'issue de cette formation, vous serez capable de :

- Définir les normes et standards pour sécuriser le Cloud Microsoft
- Reconnaître les moyens offerts pour la sécurisation du Cloud Microsoft
- Éviter la mise en place d'une sécurité inutilement complexe ou coûteuse
- Réaliser des tests de sécurité et des scénarios d'attaque contrôlés sur un tenant
- Mettre en place des architectures sécurisées
- Utiliser les bonnes pratiques.

Les compétences visées par cette formation font l'objet d'une évaluation.

À qui s'adresse cette formation ?

RSSI, responsables sécurité, chefs de projets et administrateurs.

Prérequis

Avoir des connaissances de base sur l'informatique et Microsoft Azure IaaS.

Programme

1 Pendant votre formation

Microsoft Azure – Gestion de la sécurité

Jour 1

Introduction à la sécurisation du Cloud

- Vue d'ensemble de la sécurité appliquée au Cloud Computing
 - Evolution
 - Besoins
 - Obstacles
- Sécurité dans le Cloud : panorama des services et solutions disponibles
- Définir et mettre en oeuvre une stratégie de sécurité adaptée

Sécurité et menaces

- Vue d'ensemble
 - Menaces propres aux environnements Cloud
 - Outils génériques, natifs et tiers dédiés à la sécurité du Cloud
- Introduction aux méthodes et stratégies de sécurité

La sécurité au sein de Microsoft Azure

- Principales ressources et capacités de sécurité Azure :
 - Gouvernance, conformité et référentiels : Azure Policy, Microsoft Cloud Security Benchmark, Secure Score et tableaux de bord de conformité
 - Posture de sécurité : Microsoft Defender for Cloud, CSPM, recommandations, priorisation des risques et Defender CSPM
 - Protection des workloads : plans Microsoft Defender pour serveurs, stockage, bases de données, conteneurs, App Service, Key Vault, Resource Manager et DNS
 - Sécurité réseau : Azure Firewall, Application Gateway / WAF, NSG, Private Link et Azure DDoS Protection
 - Identité, accès et protection des données : Microsoft Entra ID, RBAC, MFA, accès conditionnel, PIM, Key Vault, chiffrement, sauvegarde et restauration
 - Détection et réponse : vue d'ensemble de Microsoft Sentinel, Microsoft Defender XDR, Azure Monitor et Log Analytics
 - Applications SaaS et usages cloud : Microsoft Defender for Cloud Apps
 - Sécurité hybride et multicloud : Azure Arc, connexions AWS / GCP et supervision des ressources hors Azure
 - DevSecOps et sécurité du cycle de vie applicatif
 - Nouveaux risques liés à l'IA, aux pratiques DevSecOps et aux environnements hybrides ou multicloud
- Analyse des processus de validation et des stratégies associées

- Responsabilité partagée et protection des données
- Bonnes pratiques de gouvernance et de gestion des stratégies Azure

Gérer la sécurité de son tenant

- Introduction à Microsoft Defender for Cloud : posture de sécurité, recommandations, Secure Score et protection des workloads
- Appliquer les principaux contrôles d'identité, d'accès et de protection des données
- Sécurisation du réseau
- Sécuriser les données, les clés, les secrets et les certificats
- Application des stratégies et politiques de sécurité
- Tests et alertes de sécurité
- Prévention des attaques

Jour 2

Mise en oeuvre opérationnelle des contrôles de sécurité

- Mise en oeuvre opérationnelle des contrôles d'identité, de protection des données et de conformité :
 - Configurations avancées, accès externes, tests, alertes et mesures correctives
 - Des stratégies de conformité
- Gestion de la collaboration inter-entreprises
- Gestion des accès externes
- Activation des capacités d'analyse Azure pour renforcer la sécurité du tenant
- Création de campagnes de tests

La sécurité par module

- Vue d'ensemble de la sécurité pour les services Azure
 - Azure App
 - Microsoft Entra ID
 - Azure Compute
 - Azure Database
 - Azure Web
 - Azure Storage
 - Azure Networking

Le suivi de la sécurité

- Outils de suivi de la conformité et de la sécurité
- Journalisations, analyses et audits
- Bonnes pratiques de suivi et d'amélioration continue

Exemples de travaux pratiques (à titre indicatif)

- Mettre en oeuvre l'authentification JIT JEA

- Mettre en oeuvre l'ensemble des capacités de Microsoft Defender
- Analyser les résultats d'attaques simulées et définir les mesures correctives

Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

Nous contacter pour en savoir plus →

Modalités pédagogiques

Formation délivrée en présentiel ou distanciel* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode** démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2I, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

* nous consulter pour la faisabilité en distanciel

** ratio variable selon le cours suivi

Accessibilité aux personnes en situation de handicap

Détails de la session

Du 10 décembre 2026 au 11 décembre 2026 (2 jours / 14 heures)

À distance

Du 10 décembre 2026 au 11 décembre 2026

À distance

- 10 décembre 2026 9h00 – 16h30
- 11 décembre 2026 9h00 – 16h30