

Microsoft Azure – Implémenter des contrôles de sécurité de bout en bout pour le Cloud et les charges de travail IA

4 jours (28 heures)

Expertise

Présentiel ou classe à distance

à partir de

2 940 € HT par personne (TVA en vigueur)

Contenu mis à jour le 30/09/2026. Document téléchargé le 07/10/2026.

Objectifs

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

- Gérer les identités, les accès et la gouvernance avec Microsoft Entra ID, Azure Key Vault et Azure Policy
- Sécuriser le stockage, les bases de données et les services réseau Azure
- Sécuriser les charges de travail de calcul, y compris les solutions IA, les serveurs, les conteneurs et les services applicatifs
- Gérer et surveiller la posture de sécurité avec Microsoft Defender for Cloud, Microsoft Sentinel et Microsoft Security Copilot.

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

À qui s'adresse cette formation ?

Ingénieurs de sécurité chargés de la protection des systèmes et des données dans des environnements Cloud et hybrides.

Prérequis

Avoir une expérience pratique dans l'administration d'Azure et d'environnements hybrides, notamment le calcul, le réseau et le stockage ainsi qu'une solide connaissance de Microsoft Entra ID et une familiarité avec l'administration Microsoft 365.

Programme

1 Pendant votre formation

Microsoft Azure – Implémenter des contrôles de sécurité de bout en bout pour le Cloud et les charges de travail IA

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

- Gérer et implémenter des méthodes d'authentification dans Microsoft Entra ID
- Implémenter et configurer Privileged Identity Management (PIM)
- Authentifier votre plug-in d'API pour les agents déclaratifs avec des API sécurisées

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

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

Appliquer la gouvernance de la sécurité et la conformité réglementaire

- Appliquer la gouvernance avec des Azure Policy et des verrous de ressources
- Configurer les contrôles de sécurité et corriger les recommandations dans Defender for Cloud
- Evaluer la conformité réglementaire dans Defender for Cloud
- Gérer et dimensionner correctement les attributions de rôles RBAC selon le principe du moindre privilège
- Protéger les données de sauvegarde avec des fonctionnalités de sécurité Sauvegarde Azure
- Implémenter des contrôles de sécurité dans l'infrastructure en tant que code

Implémenter la sécurité pour le stockage Azure

- Décrire les services de stockage Azure
- Implémenter la sécurité et gérer l'accès pour le stockage Azure
- Configurer la sécurité réseau pour le stockage Azure
- Implémenter Microsoft Defender pour le stockage

Implémenter la sécurité pour les bases de données Azure SQL

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

Implémenter des contrôles de sécurité réseau dans Azure

- Segmenter et isoler les charges de travail Azure à l'aide de contrôles de sécurité réseau
- Centraliser et appliquer l'inspection du trafic à l'aide de Pare-feu Azure
- Sécuriser la connectivité distante et hybride à l'aide de passerelles VPN et de Accès privé Microsoft Entra

- Eliminer l'exposition du réseau public aux services PaaS Azure

Implémenter la sécurité pour l'IA

- Accès sécurisé pour l'identité de l'agent Microsoft Entra
- Analyser les risques liés aux identités IA à l'aide de Microsoft Defender XDR
- Activer la protection en temps réel pour les agents Copilot Studio
- Configurer la sécurité de la passerelle AI dans Microsoft Foundry
- Configurer et gérer des garde-fous dans Microsoft Foundry
- Protéger les charges de travail IA avec Microsoft Defender for Cloud
- Activer Defender pour les services d'IA protection des charges de travail dans Microsoft Defender for Cloud
- Gérer les agents à l'aide de Microsoft Agent 365
- Identifier les risques liés aux données IA à l'aide de Gestion de la posture de sécurité des données Microsoft Purview

Implémenter la sécurité pour les serveurs et les machines virtuelles

- Implémenter le chiffrement de disque pour les machines virtuelles Azure
- Configurer les fonctionnalités de sécurité de lancement approuvées pour les machines virtuelles Azure
- Planifier et implémenter Azure Bastion
- Gérer la sécurité des serveurs hybrides avec Arc
- Implémenter Microsoft Defender pour les serveurs
- Activer et appliquer l'accès juste-à-temps aux machines virtuelles
- Appliquer la configuration de sécurité des machines virtuelles avec Azure Machine Configuration

Sécuriser les services de plateforme d'applications Azure

- Détecter les risques liés aux conteneurs à l'aide de Microsoft Defender pour les conteneurs
- Implémenter des contrôles de sécurité pour Azure Kubernetes Service
- Implémenter des contrôles de sécurité pour Azure Container Registry, Container Instances et Container Apps
- Implémenter des contrôles de sécurité pour les applications de fonction Azure et les applications logiques
- Implémenter des contrôles de sécurité pour Azure App Services et Web Application Firewall
- Implémenter la sécurité du back-end d'API à l'aide de Gestion des API Azure

Gérer la posture de sécurité en utilisant Microsoft Defender pour le Cloud

- Connecter des environnements hybrides et multiclouds à Microsoft Defender for Cloud
- Identifier les risques de sécurité à l'aide de la gestion de la posture de sécurité cloud
- Découvrir des ressources et des vulnérabilités non protégées à l'aide de Microsoft Defender External Attack Surface Management
- Evaluer la conformité réglementaire dans Defender for Cloud
- Activer et configurer des plans de protection des charges de travail dans Microsoft Defender for Cloud
- Configurer les paramètres de Microsoft Defender Vulnerability Management pour les machines virtuelles Azure

Implémenter l'activité et la collecte d'événements dans Microsoft Sentinel

- Créer et gérer des espaces de travail Microsoft Sentinel
- Gérer le contenu dans Microsoft Sentinel
- Connecter services Microsoft à Microsoft Sentinel
- Connecter des sources de données Syslog à Microsoft Sentinel
- Connecter des journaux Common Event Format à Microsoft Sentinel
- Connecter des hôtes Windows à Microsoft Sentinel
- Implémenter des règles d'automatisation et des playbooks dans Microsoft Sentinel
- Gérer le stockage des données et interroger les journaux d'audit dans Microsoft Sentinel

Déployer et exploiter Microsoft Security Copilot

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

Certification (en option)

- Prévoir l'achat d'un voucher en supplément
- Le passage de l'examen se fera (ultérieurement) dans un centre agréé Pearson Vue
- L'examen (en anglais) s'effectuera en ligne

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 2 novembre 2027 au 5 novembre 2027 (4 jours / 28 heures)

Paris La Défense

Du 2 novembre 2027 au 5 novembre 2027 Paris La Défense

- 2 novembre 2027 9h00 – 15h30
- 3 novembre 2027 9h00 – 15h30
- 4 novembre 2027 9h00 – 15h30
- 5 novembre 2027 9h00 – 15h30