# Architecte en cybersécurité Microsoft (SC-100)

## Date et durée

Code formation : SC-100T00-A
Durée : 4 jours
Nombre d'heures : 21 heures

## Formation avec certification

Microsoft Certified : Cybersecurity Architect Expert

## Description

Un architecte en cybersécurité Microsoft conçoit et met en œuvre des **solutions de sécurité robustes sur la plateforme Azure**. Son rôle est d'analyser les risques, de concevoir des architectures sécurisées, de mettre en œuvre des contrôles de sécurité et de garantir la conformité aux normes réglementaires. Il est également responsable de la gestion des incidents de sécurité et de la mise en place de plans de continuité d'activité.
Cette formation Microsoft de 4 jours vous prépare à **devenir un architecte en cybersécurité Microsoft certifié**. Vous apprendrez à analyser les risques, à concevoir des architectures de sécurité, à mettre en œuvre des solutions de sécurité avancées, à gérer les incidents et à garantir la conformité. Vous découvrirez les dernières technologies de sécurité Microsoft, telles que **Azure Security Center, Microsoft Defender**, et les meilleures pratiques pour sécuriser les environnements cloud. Des exercices pratiques et des études de cas concrets vous permettront d'appliquer vos connaissances à des scénarios réels.
Au terme de ces cours, vous serez également préparé à l'examen Microsoft SC-100, qui vous permet d'obtenir la certification de **Microsoft Certified : Cybersecurity Architect Expert** (*en savoir plus dans l'onglet Certification)*. Cette certification prestigieuse atteste de votre expertise en matière de conception et d'implémentation de solutions de sécurité robustes sur la plateforme Azure.

## Objectifs

*À la fin de cette formation Microsoft SC-100, vous validerez les objectifs de compétences suivants :*

- concevoir des architectures de sécurité robustes et alignées sur les meilleures pratiques Microsoft, en particulier le modèle Zero Trust ;
- implémenter des solutions de sécurité complètes couvrant l'ensemble du cycle de vie des applications et des données ;
- gérer les risques de manière proactive en mettant en place des mécanismes de détection, de réponse et de récupération efficaces ;
- assurer la conformité réglementaire en traduisant les exigences légales en contrôles techniques concrets ;
- optimiser la posture de sécurité de leur organisation en utilisant les outils et les services Microsoft les plus récents ;
- se préparer efficacement à l'examen Microsoft SC-100 : Architecte en cybersécurité Microsoft.

## Points forts

- **Un formateur expert et certifié Microsoft :** apprenez auprès d'un formateur architecte certifié, spécialisé dans la conception de solutions de sécurité avancées.
- **Une approche pratique et centrée sur les scénarios réels :** mettez en pratique vos connaissances grâce à des exercices et des études de cas conçus pour vous préparer aux défis du monde réel.
- **Une préparation complète à l'examen SC-100 :** préparez-vous efficacement à l'examen de certification SC-100 (voucher inclus). Des sessions de révision et des exemples de questions optimiseront vos chances de réussite.
- **Garantie de certification :** cette formation inclut le "Microsoft Exam Replay", ce qui vous permet de repasser l'examen gratuitement en cas d'échec à la première tentative.
- **Développez une vision stratégique de la sécurité :** apprenez à concevoir des architectures de sécurité robustes et à évaluer les risques de manière proactive.

Certification

*Cette formation est une préparation à l'examen SC-100, qui mène à la certification* ***Microsoft Certified : Cybersecurity Architect Expert.*** *Un voucher (code coupon) vous sera fourni à la fin du cours, vous permettant de programmer votre examen.*

## Modalités pratique de l'examen SC-100

Pour vous inscrire à l'examen, vous devez créer un compte sur le site web de Microsoft Learn (si vous n'en avez pas déjà un) et lier votre profil à un compte Pearson VUE. Sur le site de Pearson VUE, recherchez l'examen SC-100 : Microsoft Cybersecurity Architect Expert. Choisissez votre mode d'examen (centre de test ou en ligne sous surveillance à distance), sélectionnez une date et une heure, puis entrez le code du voucher. Cette formation inclut le "Microsoft Exam Replay", ce qui vous permet de repasser l'examen gratuitement en cas d'échec à la première tentative.

- **Type d’examen :** l'examen comprend différents types de questions, notamment des QCM, des réponses courtes, des études de cas et d'autres formats interactifs.
- **Durée :** jusqu'à 2 heures, incluant le temps pour les instructions.
- **Lieu :** En ligne sous surveillance à distance (proctoring) ou dans des centres de test agréés Pearson VUE.
- **Livre ouvert :** non autorisé
- **Langue :** Anglais, Chinois (simplifié), Français, Allemand, Japonais, Coréen, Portugais (Brésil) et Espagnol
- **Note de passage :** 700 ou plus sur une échelle allant de 0 à 1000
- **Résultats :** les résultats sont généralement disponibles quelques minutes après la fin de l'examen en centre de test et jusqu'à 24 heures après un examen en ligne.

**À savoir :** *pour* devenir Microsoft Certified Cybersecurity Architect Expert, vous devez obtenir l'une des 3 certifications suivantes :

- Microsoft Certified: Azure Security Engineer Associate
- Microsoft Certified: Identity and Access Administrator Associate
- Microsoft Certified: Security Operations Analyst Associate.

*Pour maintenir votre certification active, vous devrez passer une évaluation de renouvellement gratuite sur Microsoft Learn chaque année.*
En savoir plus sur le renouvellement

Modalités d'évaluation

Travaux Pratiques
Etude de cas

Pré-requis

*Suivre cette formation nécessite les prérequis suivants :*

### Prérequis obligatoires

- Être familier avec les concepts de sécurité informatique, tels que les menaces, les vulnérabilités, les risques et les meilleures pratiques.
- Avoir une expérience avec des outils de sécurité tels que les SIEM, les SOAR, les WAF et les antivirus.
- Avoir une connaissance des principaux cadres de référence en sécurité (NIST, CIS, ISO 27001).

### Prérequis recommandés

- Avoir une expérience préalable avec les composants de la plateforme Power Platform (Power Apps, Power Automate, Power BI, Power Virtual Agents).
- Être familier avec les services Azure, en particulier ceux liés à l'intégration, à l'automatisation et à la sécurité (Azure Logic Apps, Azure Functions, Azure API Management, Azure Active Directory).
- Avoir une expérience en développement d'API et en intégration de systèmes.
- Avoir des connaissances en gestion du cycle de vie des applications (ALM).
- Connaître les concepts de gouvernance informatique et de conformité (RGPD, etc.).

Public

*Cette formation s'adresse aux publics suivants :*

- **les architectes solutions et les architectes d'entreprise** qui souhaitent acquérir une expertise approfondie en matière de conception et d'implémentation de solutions de sécurité dans un environnement Microsoft ;
- **les consultants en sécurité** qui désirent élargir leur champ de compétences aux architectures cloud et aux solutions de sécurité Microsoft spécifiques ;
- **les ingénieurs systèmes** qui ont une expérience en infrastructure et qui souhaitent se spécialiser dans la sécurité des systèmes d'information ;
- **les développeurs** qui ont une bonne connaissance des technologies Microsoft et qui souhaitent s'orienter vers des rôles plus stratégiques en matière de sécurité ;
- **les professionnels de la sécurité** qui ont une expérience dans d'autres environnements cloud (AWS, GCP) et qui souhaitent se spécialiser sur Azure ;
- **les responsables de la sécurité des informations** souhaitant acquérir une vision plus technique des solutions de sécurité.

Programme

### Module 1 : maîtriser les fondamentaux de la cybersécurité et architecturer des solutions Microsoft

- L'identification des menaces et des vulnérabilités les plus courantes dans les environnements Microsoft.
- L'évaluation des risques et la définition d'une posture de sécurité adaptée aux besoins de l'entreprise.
- La création d'architectures de solutions alignées sur les référentiels Microsoft (MCRA, MCSB, CAF, Well-Architected Framework), en tenant compte des contraintes de sécurité.

### Module 2 : sécuriser les identités et les accès

- La gestion centralisée des identités dans Microsoft Entra ID, en intégrant les concepts d'IAM et de PIM.
- Le contrôle granulaire des accès aux ressources, en s'appuyant sur les principes du Zero Trust.
- La mise en œuvre d'une authentification multifactorielle forte pour renforcer la sécurité des comptes.

### Module 3 : protéger les données

- La classification et la protection des données sensibles en utilisant des outils comme Microsoft Purview.
- Le chiffrement des données au repos et en transit, en s'appuyant sur les fonctionnalités de chiffrement de Azure.
- La prévention des pertes de données (DLP) pour limiter les fuites d'informations sensibles.

### Module 4 : sécuriser le développement

- L'intégration de la sécurité dès les premières phases du développement (DevSecOps), en utilisant des outils comme Azure DevOps.
- La sécurisation des API et des applications web, en mettant en œuvre des mécanismes de protection contre les attaques OWASP.
- La protection des applications cloud natives, en tenant compte des spécificités des conteneurs et des fonctions serverless.

### Module 5 : renforcer l'infrastructure

- La protection des ressources Azure à l'aide de Microsoft Defender, en incluant la gestion des vulnérabilités et la détection des menaces.
- Le déploiement de solutions de sécurité réseau (VPN, pare-feu, segmentation), en s'appuyant sur Azure Network Watcher.
- La sécurisation des environnements hybrides, en intégrant les composants on-premises.

### Module 6 : assurer la résilience

- La planification de la continuité d'activité et de la reprise après sinistre, en utilisant des outils comme Azure Site Recovery.
- La réponse efficace aux incidents de sécurité, en s'appuyant sur Microsoft Sentinel.
- La prévention et la gestion des attaques par ransomware, en mettant en place des stratégies de sauvegarde et de restauration régulières.

### Module 7 : garantir la conformité

- L'évaluation de la conformité aux réglementations (RGPD, HIPAA, etc.), en utilisant des outils comme Microsoft Compliance Manager.
- La mise en œuvre de contrôles de conformité personnalisés pour répondre aux exigences spécifiques de l'entreprise.
- La gestion des risques de non-conformité, en intégrant les concepts de GRC (Governance, Risk and Compliance).

### Module 8 : optimiser les opérations de sécurité

- La surveillance continue des menaces en temps réel, en utilisant des outils comme Microsoft Defender for Cloud.
- L'automatisation des tâches de sécurité récurrentes, en utilisant des outils comme Azure Automation.
- L'amélioration continue de la posture de sécurité de l'organisation, en utilisant des métriques et des indicateurs clés de performance (KPI).

### Module 9 : mettre en pratique et appliquer les connaissances

- Mise en pratique des concepts à travers des exercices et des études de cas concrets :
    - conception de solutions de sécurité sur mesure, en s'appuyant sur les connaissances acquises tout au long de la formation ;
    - résolution de cas pratiques et d'études de cas, en simulant des scénarios réels de cyberattaques.

### Module 10 : préparer l'examen SC-100

- Révision des concepts clés du cours.
- Séance de conseils et d'astuces pour l'examen.
- Analyse d'exemples de questions d'examen.
- Découverte des ressources complémentaires pour la préparation.