OpenCertif
Centre de formation et de certification professionnelle

SYLLABUS OFFICIEL

Examen SC-100

Architecte en cybersécurité Microsoft

Certification : Microsoft Certified — Cybersecurity Architect Expert

Niveau : Expert | Public : Architectes cybersécurité / CISO

1. Présentation de la certification

L'examen **SC-100 : Microsoft Cybersecurity Architect** valide les compétences des architectes en cybersécurité qui traduisent une stratégie de cybersécurité en capacités protégeant les actifs, l'activité et les opérations d'une organisation. Cette certification atteste de votre capacité à concevoir, guider la mise en œuvre et maintenir des solutions de sécurité alignées sur les principes Zero Trust et les meilleures pratiques pour l'identité, les appareils, les données, l'IA, les applications, le réseau, l'infrastructure et DevOps.

La réussite de cet examen, combinée à une certification Associate préalable (AZ-500, SC-200 ou SC-300), conduit à l'obtention de la certification **Microsoft Certified : Cybersecurity Architect Expert**, l'une des certifications de niveau expert les plus valorisées du portefeuille sécurité Microsoft. Elle est particulièrement pertinente pour les rôles de CISO, d'architecte cybersécurité et de consultant senior en sécurité.

Informations clés

Code de l'examen	SC-100
Intitulé officiel	Microsoft Cybersecurity Architect
Certification obtenue	Microsoft Certified : Cybersecurity Architect Expert
Niveau	Expert
Statut	Actif (mise à jour le 27 avril 2026)
Prérequis pour la certification Expert	Une certification Associate parmi : Azure Security Engineer (AZ-500), Security Operations Analyst (SC-200), Identity and Access Administrator (SC-300)
Durée de l'examen	Environ 100 à 120 minutes (selon planification)
Nombre de questions	40 à 60 questions (QCM, études de cas, glisser-déposer, scénarios pratiques)
Score de réussite	700 / 1000
Langues disponibles	Anglais, français, allemand, japonais, espagnol, chinois (simplifié), coréen (délai d'environ 8 semaines pour les versions localisées)
Validité	1 an, renouvellement gratuit en ligne via Microsoft Learn

Modalité	En centre agréé (OpenCertif — Pearson VUE) ou à distance (OnVUE)

2. Profil du candidat

En tant qu'architecte en cybersécurité Microsoft, vous traduisez une stratégie de cybersécurité en capacités qui protègent les actifs, l'activité et les opérations d'une organisation. Vous concevez, guidez la mise en œuvre et maintenez des solutions de sécurité alignées sur les principes Zero Trust, notamment des stratégies de sécurité pour :

- L'identité et les appareils.
- Les données et l'IA.
- Les applications.
- Le réseau et l'infrastructure.
- Les pipelines DevOps (DevSecOps).
- La gouvernance, le risque et la conformité (GRC).
- Les opérations de sécurité (SecOps).
- La gestion de la posture de sécurité.

En tant qu'architecte cybersécurité, vous collaborez en continu avec les leaders et praticiens de la sécurité, de la vie privée, de l'ingénierie et d'autres rôles de l'organisation pour planifier et implémenter une stratégie de cybersécurité répondant aux besoins métier. Vous avez de l'expérience sur au moins un des domaines suivants à un niveau expert :

- Identité et accès (Microsoft Entra ID, PIM, Conditional Access).
- Protection de la plateforme (Defender for Cloud, baselines, Azure Policy).
- Opérations de sécurité (XDR, SIEM, SOAR, Sentinel, Defender XDR).
- Sécurité des données et de l'IA (Purview, DSPM, Defender for AI).
- Sécurité des applications (WAF, API security, threat modeling).
- Infrastructures hybrides et multicloud (Azure Arc, Azure landing zones).

3. Prérequis et public cible OpenCertif

L'obtention de la certification **Microsoft Certified : Cybersecurity Architect Expert** impose la détention préalable de l'une des certifications Associate suivantes :

- **AZ-500** : Microsoft Certified Azure Security Engineer Associate.
- **SC-200** : Microsoft Certified Security Operations Analyst Associate.
- **SC-300** : Microsoft Certified Identity and Access Administrator Associate.
- Passer le SC-100 seul ne suffit donc pas à obtenir le titre Expert.
- OpenCertif recommande de vérifier la détention d'une certification Associate valide avant de planifier le SC-100.

Public cible OpenCertif

- Architectes cybersécurité et architectes Zero Trust.
- RSSI / CISO et responsables sécurité IT.
- Consultants seniors en sécurité Microsoft (cloud et hybride).
- Ingénieurs sécurité évoluant vers un rôle d'architecte.

- Architectes solutions Azure / Microsoft 365 spécialisés sécurité.
- Responsables conformité et GRC dans des environnements Microsoft.

4. Domaines de compétences mesurées

L'examen est structuré autour de 4 grands domaines de compétences. Le tableau ci-dessous indique le poids relatif de chaque domaine dans l'évaluation finale (version du 27 avril 2026).

Domaine	Intitulé	Pondération
1	Solutions alignées sur les bonnes pratiques de sécurité	20 — 25 %
2	Opérations de sécurité, identité et conformité	25 — 30 %
3	Solutions de sécurité pour l'infrastructure	25 — 30 %
4	Solutions de sécurité pour les applications et les données	20 — 25 %

Remarque : la majorité des questions concernent des fonctionnalités en disponibilité générale (GA). Certaines questions peuvent porter sur des fonctionnalités en préversion couramment utilisées.

5. Détail des compétences mesurées

Cette section détaille de manière exhaustive l'ensemble des compétences couvertes par l'examen SC-100, conformément au guide d'étude officiel Microsoft (version du 27 avril 2026).

1 Solutions alignées sur les bonnes pratiques de sécurité — 20 — 25 %

1.1 Concevoir une stratégie de résilience contre les ransomwares et autres attaques selon les bonnes pratiques Microsoft

- Concevoir une stratégie de sécurité alignée sur les objectifs de résilience métier, y compris l'identification et la priorisation des menaces sur les actifs critiques.
- Concevoir des solutions de continuité d'activité et de reprise après sinistre (BCDR), y compris la sauvegarde et la restauration sécurisées pour les environnements hybrides et multicloud.
- Concevoir des solutions de mitigation des attaques par rançongiciel, y compris la priorisation du BCDR et de l'accès privilégié.
- Évaluer les solutions de mise à jour de sécurité.

1.2 Concevoir des solutions alignées sur les Microsoft Cybersecurity Reference Architectures (MCRA) et le Microsoft Cloud Security Benchmark (MCSB)

- Concevoir des solutions alignées sur les bonnes pratiques de capacités et contrôles de cybersécurité.
- Concevoir des solutions alignées sur les bonnes pratiques de protection contre les attaques internes, externes et de la chaîne d'approvisionnement.
- Concevoir des solutions alignées sur les bonnes pratiques de sécurité Zero Trust, y compris le plan de modernisation rapide pour Zero Trust (RaMP).

1.3 Concevoir des solutions alignées sur le Microsoft Cloud Adoption Framework pour Azure (CAF) et le Microsoft Azure Well-Architected Framework (WAF)

- Concevoir une nouvelle stratégie ou évaluer une stratégie existante de sécurité et de gouvernance basée sur le CAF et le WAF.
- Recommander des solutions de sécurité et de gouvernance basées sur le CAF et le WAF.
- Concevoir des solutions pour implémenter et gouverner la sécurité à l'aide d'Azure landing zones.
- Concevoir un processus DevSecOps aligné sur les bonnes pratiques du Microsoft Cloud Adoption Framework pour Azure (CAF).

2 Opérations de sécurité, identité et conformité — 25 — 30 %

2.1 Concevoir des solutions pour les opérations de sécurité

- Concevoir une solution de détection et réponse incluant XDR (Extended Detection and Response) et SIEM (Security Information and Event Management).
- Concevoir une solution de journalisation et d'audit centralisés, y compris Microsoft Purview Audit.
- Concevoir la supervision pour les environnements hybrides et multicloud.
- Concevoir une solution SOAR (orchestration et réponse automatisée), y compris Microsoft Sentinel et Microsoft Defender XDR.
- Concevoir et évaluer les workflows de sécurité, y compris la réponse aux incidents, la chasse aux menaces (threat hunting) et la gestion des incidents.
- Concevoir et évaluer la couverture de détection des menaces à l'aide des matrices MITRE ATT&CK; (Enterprise, Mobile, et systèmes de contrôle industriels - ICS).

2.2 Concevoir des solutions de gestion de l'identité et des accès

- Concevoir une solution d'accès aux ressources SaaS, PaaS, IaaS, on-premises et multicloud, y compris les contrôles d'identité, réseau et applicatifs.
- Concevoir une solution Microsoft Entra ID pour les environnements hybrides et multicloud.
- Concevoir une solution d'identités externes (B2B, identité décentralisée).
- Concevoir une stratégie moderne d'authentification et d'autorisation : Conditional Access, Continuous Access Evaluation, scoring de risque, actions protégées.
- Valider l'alignement des stratégies de Conditional Access avec la stratégie Zero Trust.
- Spécifier les exigences pour durcir Active Directory Domain Services (AD DS).
- Concevoir une solution de gestion des secrets, clés et certificats.

2.3 Concevoir des solutions de sécurisation des accès privilégiés

- Concevoir une solution d'attribution et de délégation des rôles privilégiés selon l'enterprise access model.
- Évaluer la sécurité et la gouvernance de Microsoft Entra ID, y compris Privileged Identity Management (PIM), entitlement management et access reviews.
- Évaluer la sécurité et la gouvernance d'Active Directory Domain Services (AD DS), y compris la résilience aux attaques courantes.
- Concevoir une solution de sécurisation de l'administration des locataires cloud (SaaS, multicloud).
- Concevoir une solution de Cloud Infrastructure Entitlement Management (CIEM).
- Évaluer une solution de gestion des access reviews.
- Concevoir une solution de postes sécurisés pour l'accès privilégié, y compris l'accès distant.

2.4 Concevoir des solutions pour la conformité réglementaire

- Traduire les exigences de conformité en contrôles de sécurité.
- Concevoir une solution pour répondre aux exigences de conformité via Microsoft Purview.
- Concevoir une solution pour répondre aux exigences de protection de la vie privée, y compris Microsoft Priva.
- Concevoir des solutions Azure Policy pour les exigences de sécurité et de conformité.
- Évaluer et valider l'alignement avec les standards et benchmarks réglementaires à l'aide de Microsoft Defender for Cloud.

3 Solutions de sécurité pour l'infrastructure — 25 — 30 %

3.1 Concevoir des solutions de gestion de posture en environnements hybrides et multicloud

- Évaluer la posture de sécurité via Microsoft Defender for Cloud, y compris le MCSB.
- Évaluer la posture de sécurité via Microsoft Secure Score.
- Concevoir des solutions intégrées de gestion de posture incluant Microsoft Defender for Cloud dans des environnements hybrides et multicloud.
- Sélectionner les solutions de protection des workloads cloud dans Microsoft Defender for Cloud.
- Concevoir une solution d'intégration des environnements hybrides et multicloud via Azure Arc.
- Concevoir une solution Microsoft Defender External Attack Surface Management (Defender EASM).
- Spécifier les exigences et priorités pour un processus de gestion de posture utilisant Microsoft Security Exposure Management : attack paths, attack surface reduction, security insights et initiatives.

3.2 Spécifier les exigences pour sécuriser les endpoints serveurs et clients

- Spécifier les exigences pour les serveurs sur diverses plateformes et systèmes d'exploitation.
- Spécifier les exigences pour les appareils mobiles et les clients : endpoint protection, durcissement, configuration.
- Spécifier les exigences pour les appareils IoT et les systèmes embarqués.
- Évaluer les solutions pour sécuriser l'OT et les ICS via Microsoft Defender for IoT.
- Spécifier les baselines de sécurité pour serveurs et endpoints.
- Évaluer la solution Windows Local Administrator Password Solution (Windows LAPS).

3.3 Spécifier les exigences pour sécuriser SaaS, PaaS et IaaS

- Spécifier les baselines de sécurité pour les services SaaS, PaaS et IaaS.
- Spécifier les exigences de sécurité pour les workloads IoT.
- Spécifier les exigences de sécurité pour les workloads web.
- Spécifier les exigences de sécurité pour les conteneurs.
- Spécifier les exigences de sécurité pour l'orchestration de conteneurs.
- Évaluer les solutions incluant la sécurité des services Azure AI.

3.4 Évaluer les solutions de sécurité réseau et Security Service Edge (SSE)

- Évaluer les designs réseau pour les aligner sur les exigences et bonnes pratiques de sécurité.
- Évaluer les solutions utilisant Microsoft Entra Internet Access comme passerelle web sécurisée.
- Évaluer les solutions utilisant Microsoft Entra Internet Access pour les services Microsoft, y compris les configurations cross-tenant.
- Évaluer les solutions utilisant Microsoft Entra Private Access.

4 Solutions de sécurité pour les applications et les données — 20 — 25 %

4.1 Évaluer les solutions de sécurisation de Microsoft 365

- Évaluer la posture de sécurité pour les workloads de productivité et collaboration via Microsoft Secure Score.
- Évaluer les solutions incluant Microsoft Defender for Office 365 et Microsoft Defender for Cloud Apps.
- Évaluer les solutions de gestion des appareils incluant Microsoft Intune.
- Évaluer les solutions de sécurisation des données dans Microsoft 365 via Microsoft Purview.
- Évaluer les contrôles de sécurité et conformité des données dans Microsoft Copilot for Microsoft 365.

4.2 Concevoir des solutions de sécurisation des applications

- Évaluer la posture de sécurité des portefeuilles d'applications existants.
- Évaluer les menaces sur les applications business-critical via le threat modeling.
- Concevoir et implémenter une stratégie de cycle de vie complet pour la sécurité applicative.
- Concevoir et implémenter des standards et pratiques pour sécuriser le processus de développement applicatif.
- Faire correspondre les technologies aux exigences de sécurité applicatives.
- Concevoir une solution pour les workload identities permettant d'authentifier et accéder aux ressources Azure.
- Concevoir une solution de gestion et sécurité des API.
- Concevoir des solutions sécurisant les applications via Azure Web Application Firewall (WAF).

4.3 Concevoir des solutions de sécurisation des données de l'organisation

- Évaluer les solutions de découverte et classification des données.
- Spécifier les priorités pour la mitigation des menaces sur les données.
- Évaluer les solutions de chiffrement des données au repos et en transit, y compris Azure Key Vault et le chiffrement d'infrastructure.
- Concevoir une solution de sécurité pour les données dans les workloads Azure : Azure SQL, Azure Synapse Analytics, Azure Cosmos DB.
- Concevoir une solution de sécurité pour les données dans Azure Storage.
- Concevoir une solution de sécurité incluant Microsoft Defender for Storage et Microsoft Defender for Databases.

6. Modalités pédagogiques OpenCertif

OpenCertif accompagne les candidats au SC-100 à travers un parcours blended-learning complet, combinant ressources e-learning interactives, sessions tutorées et ateliers techniques pratiques sur les technologies Microsoft Defender XDR, Microsoft Sentinel, Microsoft Entra ID, Microsoft Purview, Microsoft Defender for Cloud et Zero Trust.

Format de la formation

Durée recommandée	60 à 80 heures de formation (selon profil et niveau d'entrée)
Modalité	100 % distanciel asynchrone, ou blended (distanciel + classes virtuelles)
Support pédagogique	Modules interactifs Articulate Rise 360, scénarios immersifs VTS, ateliers techniques
Plateforme LMS	lmsopencertif.fr (Moodle) — accès 24/7 pendant 12 mois
Encadrement	Tutorat asynchrone par expert certifié + classes virtuelles bimensuelles
Évaluations	Quiz formatifs par module, ateliers pratiques, examen blanc final, simulation OnVUE
Certification finale	Passage de l'examen SC-100 en centre OpenCertif (Pearson VUE) ou OnVUE

Parcours d'apprentissage proposé

- **Module 1 :** Stratégie de cybersécurité et rôle de l'architecte.
- **Module 2 :** Résilience et BCDR — stratégie anti-ransomware.
- **Module 3 :** MCRA, MCSB et bonnes pratiques Microsoft.
- **Module 4 :** Zero Trust et RaMP — modernisation rapide.
- **Module 5 :** Cloud Adoption Framework et Well-Architected Framework.
- **Module 6 :** Azure landing zones et DevSecOps.
- **Module 7 :** Opérations de sécurité — XDR, SIEM, SOAR.
- **Module 8 :** Microsoft Sentinel et Microsoft Defender XDR — conception architecturale.
- **Module 9 :** Identité et accès — Microsoft Entra ID, B2B, Conditional Access.
- **Module 10 :** Accès privilégiés — PIM, enterprise access model.
- **Module 11 :** Conformité réglementaire — Microsoft Purview, Priva, Azure Policy.
- **Module 12 :** Gestion de posture — Defender for Cloud, Secure Score, EASM.
- **Module 13 :** Sécurisation des endpoints, IoT, OT et ICS.
- **Module 14 :** Sécurité SaaS / PaaS / IaaS et conteneurs.

- **Module 15 :** Security Service Edge — Entra Internet Access, Entra Private Access.
- **Module 16 :** Sécurisation de Microsoft 365 et Copilot.
- **Module 17 :** Sécurité applicative — WAF, API, threat modeling, workload identities.
- **Module 18 :** Sécurité des données — classification, chiffrement, Defender for Storage / Databases.
- **Module 19 :** Études de cas architecturales et scénarios complexes.
- **Module 20 :** Examen blanc et préparation finale.

7. Ressources d’étude officielles

En complément du parcours OpenCertif, les ressources Microsoft Learn suivantes sont fortement recommandées :

- Documentation sécurité Microsoft (learn.microsoft.com/security).
- Microsoft Cybersecurity Reference Architectures (MCRA).
- Microsoft Cloud Security Benchmark (MCSB).
- Documentation Microsoft Defender for Cloud.
- Zero Trust Guidance Center (learn.microsoft.com/security/zero-trust).
- Microsoft Cloud Adoption Framework pour Azure.
- Microsoft Azure Well-Architected Framework.
- Documentation Microsoft Sentinel et Microsoft Defender XDR.
- Documentation Microsoft Purview et Microsoft Priva.
- Gouvernance, risque et conformité dans Azure.
- Parcours d’apprentissage Microsoft Learn dédiés au SC-100.
- Évaluation pratique gratuite proposée par Microsoft.
- Espace de simulation d’examen (aka.ms/examdemo).
- Security, compliance, and identity community hub.
- Chaînes vidéo : Exam Readiness Zone.

8. Modalités de passage de l’examen

Inscription	Via OpenCertif ou directement sur learn.microsoft.com
Centre d’examen	OpenCertif — Centre agréé Pearson VUE
Examen à distance	Mode OnVUE (surveillance en ligne, conditions strictes)
Pièce d’identité	2 pièces d’identité obligatoires le jour de l’examen
Aménagements	Demande possible (temps additionnel, assistance) sur Microsoft Learn
Résultat	Score communiqué immédiatement à la fin de l’examen
Renouvellement	Annuel, via évaluation gratuite en ligne sur Microsoft Learn
Politique de reprise	Délai d’attente de 24 heures pour la 1re reprise, puis 14 jours entre les tentatives suivantes (maximum 5 tentatives sur 12 mois)

9. Contact et inscription

Pour toute information complémentaire, demande de devis ou inscription à la formation préparatoire au SC-100, l'équipe OpenCertif reste à votre disposition.

OpenCertif
Centre de formation et de certification

app.opencertif.fr
lmsopencertif.fr

Centre agréé Certiport / Pearson VUE
Certifié Qualiopi — Actions de formation

10. Mentions légales et version

Ce syllabus est établi par OpenCertif sur la base du guide d'étude officiel Microsoft SC-100, dans sa version applicable (version du 27 avril 2026). Les compétences mesurées, les pondérations et les objectifs présentés reflètent fidèlement la structure de l'examen telle que publiée par Microsoft.

Version du syllabus : 2026.05 — Édition mai 2026
Source officielle : learn.microsoft.com/credentials/certifications/resources/study-guides/sc-100