

Microsoft Cybersecurity Architect – Formation intensive («SC100»)

Grâce à cette formation Microsoft officielle, maîtrisez la conception et l'évaluation des stratégies de cybersécurité dans les domaines du Zero Trust, de la GRC, des SecOps, des données et des applications. Préparez-vous à l'examen de certification SC-100

Durée: 4 jours

Prix : 3'400.– excl. 8.1% TVA

Documents : Support numérique officiel Microsoft et Microsoft Learn

Code officiel: SC-100

Contenu

Le contenu de cette formation intensive est basé sur le contenu de l'examen « [SC-100: Microsoft Cybersecurity Architect](#) ». Commencez à vous préparer dès maintenant à votre formation sur Microsoft Learn. Lors des sessions journalières intensives avec nos experts, vous travaillerez avec les supports de formation officiels Microsoft (plus d'informations à la rubrique « méthodologie et didactique »).

Module 1 : Concevoir des solutions qui s'alignent sur les bonnes pratiques et priorités en matière de sécurité

Vous apprendrez à utiliser les bonnes pratiques de sécurité Microsoft critiques telles que le framework CAF (Cloud Adoption Framework), le framework WAF (Well-Architected Framework) et l'architecture de référence de cybersécurité Microsoft (MCRA) pour améliorer la posture de sécurité d'une organisation, appliquer des principes de confiance zéro et réduire les risques d'attaques émergentes.

Chapitres :

- Présentation des frameworks Confiance Zéro (Zéro Trust) et des bonnes pratiques
- Concevoir des solutions qui s'alignent sur le Cloud Adoption Framework (CAF) et le Well-Architected Framework (WAF)
- Concevoir des solutions qui s'alignent sur MCRA (Microsoft Cybersecurity Reference Architecture) et MCSB (Microsoft Cloud Security Benchmark)
- Concevoir une stratégie de résilience pour les cybermenaces courantes comme les rançongiciels
- Étude de cas : Concevoir des solutions qui s'alignent sur les bonnes pratiques et priorités en matière de sécurité

Module 2 : Concevoir des fonctionnalités liées aux opérations de sécurité, aux identités et à la conformité

Découvrez comment concevoir des solutions pour les opérations de sécurité (SecOps), la gestion des identités et des accès, l'accès privilégié et la conformité réglementaire.

Chapitres :

- Concevoir des solutions de conformité réglementaire
- Concevoir des solutions pour gérer les identités et les accès
- Concevoir des solutions pour sécuriser les accès privilégiés
- Concevoir des solutions pour les opérations de sécurité
- Étude de cas : Concevoir des fonctionnalités liées aux opérations de sécurité, aux identités et à la conformité

Module 3 : Concevoir des solutions de sécurité pour les applications et les données

Découvrez comment concevoir des solutions pour sécuriser les données et les applications.

notamment : Microsoft 365, le développement d'applications, les portefeuilles d'applications existants, la découverte et la classification des données avec Microsoft Purview et la sécurité des données pour les charges de travail Azure.

Chapitres :

- Concevoir des solutions pour sécuriser Microsoft 365
- Concevoir des solutions pour sécuriser les applications
- Concevoir des solutions pour sécuriser les données d'une organisation
- Étude de cas : Concevoir des solutions de sécurité pour les applications et les données

Module 4 : Concevoir des solutions de sécurité pour l'infrastructure

Vous apprenez à concevoir pour la sécurité de l'infrastructure, notamment en spécifiant des exigences pour différents modèles cloud, en concevant des solutions pour la gestion de la posture dans des environnements hybrides et multiclouds et en sécurisant des points de terminaison.

Chapitres :

- Spécifier les exigences pour sécuriser les services SaaS, PaaS et IaaS
- Concevoir des solutions pour gérer la posture de sécurité dans les environnements hybrides et multiclouds
- Concevoir des solutions pour sécuriser les points de terminaison serveur et client
- Concevoir des solutions pour la sécurité réseau
- Étude de cas : Concevoir des solutions de sécurité pour l'infrastructure

Objectifs

- Concevoir une stratégie et une architecture Zero Trust
- Évaluer les stratégies techniques de GRC (Gouvernance, Risque et Conformité) et les stratégies d'opérations de sécurité (SecOps)
- Concevoir la sécurité pour l'infrastructure
- Concevoir une stratégie pour les données et les applications
- Maîtriser les bonnes pratiques et priorités en matière de sécurité

Méthodologie & Didactique

Formule d'apprentissage mixte de Digicomp :

- **Pre-study** : dès l'inscription à la formation, vous recevez un accès à Microsoft Learn et vous pouvez dès lors commencer individuellement à vous familiariser avec la matière. Nous vous conseillons de passer en revue toute la matière au moins une fois avant le cours et de vous concentrer plus en détail sur les passages où vous manquez le plus de connaissances.
- **After-study** : après la formation, vous continuez à avoir accès à Microsoft Learn. Vous pouvez ainsi continuer à apprendre et à vous exercer selon vos besoins afin de permettre un apprentissage plus durable et de vous préparer idéalement à l'examen de certification.

Public cible

Ce cours est destiné aux ingénieurs de sécurité cloud expérimentés qui ont effectué une certification précédente dans le portefeuille de sécurité, de conformité et d'identité.

Les participantes et participants doivent au préalable :

- avoir suivi et obtenu l'une des certifications du niveau associé relatives au portefeuille sécurité, conformité et identité (par exemple, AZ-500, SC-200 ou SC-300)
- avoir une expérience et des connaissances avancées en matière d'accès et d'identités, de protection des plateformes, d'opérations de sécurité, de sécurisation des applications

Les participantes et participants qui désirent se préparer et se présenter à l'examen doivent également avoir de l'expérience dans l'implémentation ou l'administration de solutions dans au moins un des domaines suivants :

- Identités et accès
- Protection des plateformes
- Opérations de sécurité
- Sécurité des données
- Sécurité des applications
- Infrastructures hybrides et multiclouds

- [Microsoft Identity and Access Administrator – Formation intensive \(«SC300»\)](#)
- [Microsoft Security Operations Analyst – Formation intensive \(«SC200»\)](#)
- [Microsoft Azure Security Engineer Associate – Formation intensive \(«AZ500»\)](#)

Certification

Cette formation marque la première étape de préparation à l'**examen** :

« [SC-100: Microsoft Cybersecurity Architect](#) »

La réussite de cet examen permet de décrocher la **certification** :

« [Microsoft Certified: Cybersecurity Architect Expert](#) »

ATTENTION : L'examen ne se déroule pas dans le cadre de la formation, vous devrez vous y inscrire séparément. Pratiquer vos nouvelles connaissances en situation réelle augmente considérablement vos chances de réussite à l'examen, c'est pourquoi nous vous conseillons de ne pas passer l'examen tout de suite après votre formation, mais de prendre votre temps et de vous y inscrire lorsque vous serez prêt.

Inscription à l'examen

Vous avez la possibilité de vous inscrire à un examen que vous passerez soit dans un de nos centres de formation Digicomp, agréés centre de test Pearson Vue, à Lausanne ou Genève, soit depuis chez vous.

Chez Digicomp : Inscrivez-vous à l'examen directement sur le site de [Pearson VUE](#) et sélectionnez l'un de nos centres de formation Digicomp (Lausanne ou Genève). Vous pourrez ensuite choisir parmi les créneaux d'examen proposés dans nos centres.

Chez vous : Pour passer un examen depuis chez vous, vous devez vous inscrire en passant par [ce lien](#).

Le prix de l'examen est de CHF 216.- (sous réserve de modification par l'éditeur).

Avez-vous une question ou souhaitez-vous organiser un cours en entreprise ?

Nous vous conseillons volontiers au +41 22 738 80 80 ou romandie@digicomp.ch. Retrouvez toutes les informations détaillées concernant les dates sur www.digicomp.ch/formations-microsoft-technology/microsoft-security-compliance-and-identity/microsoft-certified-cybersecurity-architect-expert/cours-microsoft-cybersecurity-architect-formation-intensive-sc-100

