Architecte en cybersécurité Microsoft (SC-100)

Description

Maîtriser l’architecture de la cybersécurité Microsoft

Dans un monde numérique où les menaces évoluent sans cesse, l’architecte en cybersécurité joue un rôle clé. La formation Architecte en cybersécurité Microsoft (SC-100) vous prépare à concevoir des stratégies robustes et adaptées aux environnements modernes. Ce programme de niveau expert est pensé pour vous donner une compréhension avancée des principes de la confiance zéro, de la gouvernance des risques, des opérations de sécurité et de la protection des données et applications.

Ce cours, construit autour des bonnes pratiques Microsoft, est un atout essentiel pour tous les experts désireux d’approfondir leurs compétences. Vous apprendrez à aligner les stratégies de sécurité sur les frameworks de référence, tout en maîtrisant les exigences spécifiques aux infrastructures SaaS, PaaS et IaaS. Grâce à une approche méthodologique et concrète, vous serez capable de concevoir des architectures de sécurité complètes, résilientes et alignées sur les normes réglementaires.

Devenez un expert des architectures de sécurité cloud et hybrides

Concevoir, évaluer et améliorer des architectures de cybersécurité robustes est un enjeu stratégique pour toutes les organisations modernes. Avec la formation Architecte en cybersécurité Microsoft (SC-100), vous serez prêt à relever ce défi et à accompagner les entreprises vers une sécurité optimale. Ce cours complet vous permettra de maîtriser toutes les facettes d’une architecture de sécurité, de la conception initiale à la validation de la conformité, en passant par la protection avancée des données et applications dans des environnements hybrides et multicloud.

Contenu du cours
Module 1 : Présentation des frameworks Confiance Zéro et de meilleures pratiques

- Présentation de la Confiance Zéro
- Initiatives de Confiance Zéro
- Piliers technologiques de la Confiance Zéro Partie 1
- Piliers technologiques de la Confiance Zéro Partie 2

Module 2 : Concevoir des solutions de sécurité conformes au Cloud Adoption Framework (CAF) et au cadre bien structuré (WAF)

- Définir une stratégie de sécurité
- Présentation du Cloud Adoption Framework
- Méthodologie sécurisée du Cloud Adoption Framework
- Présentation des zones d’atterrissage Azure
- Conception de la sécurité avec les zones d’atterrissage Azure
- Présentation de Well-Architected Framework
- Pilier de sécurité Well-Architected Framework

Module 3 : Concevoir des solutions qui s’alignent sur MCRA (Microsoft Cybersecurity Reference Architecture) et MCSB (Microsoft Cloud Security Benchmark)

- Présentation de Microsoft Cybersecurity Reference Architecture et Cloud Security Benchmark
- Concevoir des solutions avec les bonnes pratiques pour les fonctionnalités et les contrôles
- Concevoir des solutions avec les meilleures pratiques de protection contre les attaques internes, externes et de chaîne logistique

Module 4 : Concevoir une stratégie de résilience pour les rançongiciels et d'autres attaques en suivant les bonnes pratiques de sécurité de Microsoft

- Cybermenaces courantes et modèles d'attaque
- Prise en charge de la résilience métier
- Concevoir des solutions pour atténuer les attaques par ransomware, notamment la hiérarchisation de BCDR et l'accès privilégié
- Solutions de conception pour la continuité d'activité et la reprise d'urgence (BCDR), notamment la sauvegarde et la restauration sécurisées
- Concevoir des solutions pour les correctifs de sécurité

Module 5 : Étude de cas : Concevoir des solutions qui s'alignent sur les bonnes pratiques et priorités en matière de sécurité

- Description de l'étude de cas
- Réponses de l'étude de cas
- Procédure pas à pas conceptuelle
- Procédure technique pas à pas

Module 6 : Concevoir des solutions de conformité réglementaire

- Présentation de la conformité réglementaire
- Traduire les exigences de conformité en contrôles de sécurité
- Concevoir une solution pour répondre aux exigences de conformité à l'aide de Microsoft Purview
- Répondre aux exigences de confidentialité avec Microsoft Priva
- Répondre aux exigences de sécurité et de conformité avec Azure Policy
- Évaluer et valider l'alignement sur les normes réglementaires et les benchmarks à l'aide de Microsoft Defender pour le cloud

Module 7 : Concevoir des solutions pour gérer les identités et les accès

- Présentation de la gestion des identités et des accès
- Concevoir des stratégies d'accès aux solutions cloud, hybrides et multicloud (notamment Microsoft Entra ID)
- Concevoir une solution pour les identités externes
- Concevoir des stratégies modernes d'authentification et d'autorisation
- Aligner l'accès conditionnel et Confiance Zéro
- Spécifier les exigences pour sécuriser Active Directory Domain Services (AD DS)
- Concevoir une solution pour gérer les secrets, les clés et les certificats

Module 8 : Concevoir des solutions pour sécuriser les accès privilégiés

- Présentation de l'accès privilégié
- Modèle d'accès d'entreprise
- Évaluer la sécurité et la gouvernance des solutions Microsoft Entra ID
- Concevoir une solution pour sécuriser l'administration des locataires
- Concevoir une solution pour les stations de travail à accès privilégié et les services bastion

- Évaluer une solution de gestion de révision d'accès
- Évaluer la sécurité et la gouvernance des services de domaine Active Directory (AD DS) sur site, y compris la résistance aux attaques courantes

Module 9 : Concevoir des solutions pour les opérations de sécurité

- Présentation des opérations de sécurité (SecOps)
- Concevoir une solution de surveillance pour prendre en charge les environnements hybrides et multicloud
- Concevoir une journalisation et un audit centralisés, notamment Microsoft Purview Audit
- Concevoir une solution de détection et de réponse qui inclut la détection et réponse étendues (XDR) et la gestion des informations et des événements de sécurité (SIEM)
- Concevoir une solution SOAR (Security Orchestration, Automation, and Response)
- Concevoir et évaluer des workflows de sécurité, notamment la réponse aux incidents, le repérage des menaces et la gestion des incidents
- Concevoir et évaluer la couverture de détection des menaces à l'aide de matrices MITRE ATT&CK, notamment au niveau cloud, entreprise, mobile et ICS

Module 10 : Étude de cas : Concevoir des fonctionnalités liées aux opérations de sécurité, aux identités et à la conformité

- Description de l'étude de cas
- Réponses de l'étude de cas
- Procédure pas à pas conceptuelle
- Procédure technique pas à pas

Module 11 : Concevoir des solutions pour sécuriser Microsoft 365

- Présentation de la sécurité pour Exchange, Sharepoint, OneDrive et Teams
- Évaluer la posture de sécurité pour les charges de travail de productivité et de collaboration en utilisant des métriques
- Concevoir une solution Microsoft Defender XDR
- Concevoir des configurations et des pratiques opérationnelles pour Microsoft 365
- Évaluer les contrôles de sécurité et de conformité des données dans Microsoft Copilot pour les services Microsoft 365
- Évaluer les solutions de sécurisation des données dans Microsoft 365 à l'aide de Microsoft Purview

Module 12 : Concevoir des solutions pour sécuriser les applications

- Introduction à la sécurité des applications
- Concevoir et implémenter des standards pour sécuriser le développement d'applications
- Évaluer la posture de sécurité de portefeuilles d'applications existants
- Évaluer les menaces d'application avec la modélisation des menaces
- Concevoir une stratégie de cycle de vie de sécurité pour les applications
- Sécuriser l'accès pour les identités de charge de travail
- Concevoir une solution pour la gestion et la sécurité des API
- Concevoir une solution pour sécuriser l'accès aux applications

Module 13 : Concevoir des solutions pour sécuriser les données d'une organisation

- Introduction à la sécurité des données
- Évaluer les solutions pour la recherche et la classification de données
- Évaluer les solutions pour le chiffrement de données au repos et en transit, notamment Azure KeyVault et le chiffrement d'infrastructure

- Concevoir la sécurité des données pour les charges de travail Azure
- Concevoir la sécurité pour le Stockage Azure
- Concevoir une solution de sécurité avec Microsoft Defender pour SQL et Microsoft Defender pour le stockage

Module 14 : Étude de cas : Concevoir des solutions de sécurité pour les applications et les données

- Description de l'étude de cas
- Réponses de l'étude de cas
- Procédure pas à pas conceptuelle
- Procédure technique pas à pas

Module 15 : Spécifier les exigences pour sécuriser les services SaaS, PaaS et IaaS

- Présentation de la sécurité pour SaaS, PaaS et IaaS
- Spécifier des bases de référence de sécurité pour les services SaaS, PaaS et IaaS
- Spécifier des exigences de sécurité pour les charges de travail IoT
- Spécifier des exigences de sécurité pour les charges de travail web
- Spécifier les exigences de sécurité pour les conteneurs et l'orchestration des conteneurs
- Évaluer la sécurité d'AI Services

Module 16 : Concevoir des solutions pour gérer la posture de sécurité dans des environnements hybrides et multiclouds

- Présentation de la gestion de la posture hybride et multicloud
- Évaluer la posture de sécurité en utilisant Microsoft Cloud Security Benchmark
- Concevoir la gestion intégrée de la posture et la protection des charges de travail
- Évaluer la posture de sécurité en utilisant Microsoft Defender pour le cloud
- Évaluation de la posture avec le degré de sécurisation Microsoft Defender pour le cloud
- Concevoir une protection de charge de travail cloud avec Microsoft Defender pour le cloud
- Intégrer des environnements hybrides et multiclouds à Azure Arc
- Concevoir une solution pour la gestion de la surface d'attaque externe
- Gestion de la posture à l'aide de la gestion de l'exposition des chemins d'attaque

Module 17 : Concevoir des solutions pour sécuriser les points de terminaison serveur et client

- Présentation de la sécurité des points de terminaison
- Spécifier les exigences de sécurité du serveur
- Spécifier des exigences pour les appareils mobiles et les clients
- Spécifier les exigences relatives à l'Internet des objets (IoT) et à la sécurité des appareils incorporés
- Sécuriser la technologie opérationnelle (OT) et les systèmes de contrôle industriels (ICS) avec Microsoft Defender pour IoT
- Spécifier des bases de référence de sécurité pour les points de terminaison serveur et client
- Concevoir une solution pour sécuriser l'accès à distance
- Évaluer les solutions LAPS (solutions de mot de passe d'administrateur local) Windows

Module 18 : Concevoir des solutions pour la sécurité réseau

- Concevoir des solutions pour la segmentation du réseau
- Concevoir des solutions pour le filtrage du trafic avec des groupes de sécurité réseau
- Concevoir des solutions pour la gestion de la posture réseau
- Concevoir des solutions pour le monitoring réseau
- Évaluer les solutions qui utilisent l'accès Internet Microsoft Entra

- Évaluer les solutions qui utilisent l’accès privé Microsoft Entra

Module 19 : Étude de cas : Concevoir des solutions de sécurité pour l’infrastructure

- Description de l’étude de cas
- Réponses à l’étude de cas
- Procédure pas à pas conceptuelle
- Procédure technique pas à pas

Lab / Exercices

- Ce cours vous donne un accès exclusif au laboratoire officiel Microsoft, vous permettant de mettre en pratique vos compétences dans un environnement professionnel.

Documentation

- Accès à Microsoft Learn, la plateforme d'apprentissage en ligne Microsoft, offrant des ressources interactives et des contenus pédagogiques pour approfondir vos connaissances et développer vos compétences techniques.

Examen

- Ce cours prépare à la certification SC-100: Microsoft Cybersecurity Architect.

Profils des participants

- Ingénieurs en sécurité cloud
- Architectes de solutions de sécurité
- Consultants en cybersécurité
- Responsables sécurité IT
- Experts en conformité et gouvernance des données

Connaissances Préalables

- Maîtriser les concepts de base de la cybersécurité et de la conformité
- Connaître les environnements cloud Microsoft et hybrides
- Être certifié sur une certification de niveau associé (AZ-500, SC-200 ou SC-300)

Objectifs

- Concevoir des stratégies de cybersécurité basées sur le modèle de confiance zéro
- Élaborer des solutions conformes aux standards du Cloud Adoption Framework
- Aligner les architectures de sécurité sur Microsoft Cybersecurity Reference Architecture
- Développer des stratégies de résilience face aux attaques par ransomware
- Spécifier des exigences pour sécuriser les infrastructures cloud SaaS, PaaS et IaaS
- Gérer la posture de sécurité dans des environnements hybrides et multiclouds
- Sécuriser les identités, accès privilégiés et opérations de sécurité
- Protéger les applications, données et points de terminaison d'une organisation

Description
Architecte en cybersécurité Microsoft (SC-100)
Niveau
Avancé
Prix de l'inscription en Présentiel (CHF)
3200
Prix de l'inscription en Virtuel (CHF)

3000
Durée (Nombre de Jours)
4
Reference
SC-100T00