Architecte de Cybersécurité Microsoft (SC-100T00)

Durée: 4 jours
Public cible: Professionnel TI

À qui s'adresse cette formation ?

Ce cours s’adresse aux ingénieurs en sécurité infonuagique expérimentés ayant déjà obtenu une certification du portefeuille sécurité, conformité et identité .

Les participants doivent posséder une expérience avancée dans plusieurs domaines de l’ingénierie de la sécurité, incluant l’identité et l’accès, la protection des plateformes, les opérations de sécurité, la sécurité des données et des applications. You should also be familiar with hybrid and cloud implementations..

Ils doivent également être familiers avec les environnements hybrides et infonuagiques .

Les débutants devraient plutôt suivre le cours SC 900 : Introduction à la sécurité, la conformité et l’identité Microsoft

Objectifs de la formation

À la fin de ce cours,

les participants seront en mesure de :

- Concevoir une stratégie et une architecture Zero Trust :

  Apprendre à créer des environnements sécurisés basés sur les principes du Zero Trust.
- Sécuriser l’infrastructure :

  Développer des stratégies pour protéger les infrastructures TI contre les menaces.
- Sécuriser les données et les applications :

  Élaborer des plans pour la protection des données et des applications dans divers environnements infonuagiques.
- Recommander les meilleures pratiques et priorités en matière de sécurité :

  Identifier et conseiller les meilleures pratiques pour renforcer la sécurité.
- Évaluer les stratégies de gouvernance, de risques et de conformité (GRC) :

  Analyser et gérer les risques, assurer la conformité réglementaire et gouverner les politiques de sécurité.

- Mettre en place et gérer les opérations de sécurité pour protéger l’infrastructure et les données.

Description sommaire

Il s'agit d'un cours avancé de niveau expert. Bien qu'il ne soit pas nécessaire de participer, vous êtes vivement encouragés à avoir effectué et passé une autre certification de niveau associé dans le portefeuille de sécurité, de conformité et d'identité (par exemple, AZ-500, SC-200 ou SC-300) avant d'assister à cette classe. Ce cours prépare les étudiants avec une expertise en conception et en évaluation des stratégies de cybersécurité dans les domaines suivants : Confiance zéro, Risques conformité en matière de gouvernance (GRC), opérations de sécurité (SecOps) et données et applications. Vous apprendrez également à concevoir l'architecture des solutions à l'aide de principes de confiance zéro et à spécifier des exigences de sécurité pour l'infrastructure cloud dans différents modèles de service (SaaS, PaaS, IaaS).

Contenu du plan de cours

Parcours d’apprentissage 1 : Concevoir des solutions alignées sur les meilleures pratiques de sécurité

- Module 1 : Introduction à Zero Trust et aux cadres de meilleures pratiques
- Module 2 : Concevoir des solutions alignées sur le Cloud Adoption Framework (CAF) et le Well Architected Framework (WAF)
- Module 3 : Concevoir des solutions alignées sur le Microsoft Cybersecurity Reference Architecture (MCRA) et le Microsoft Cloud Security Benchmark (MCSB)
- Module 4 : Concevoir une stratégie de résilience contre les cybermenaces courantes comme les rançongiciels

Parcours d’apprentissage 2 : Concevoir les opérations de sécurité, l’identité et les capacités de conformité

- Module 1 : Concevoir des solutions pour la conformité réglementaire
- Module 2 : Concevoir des solutions pour la gestion des identités et des accès
- Module 3 : Concevoir des solutions pour sécuriser l’accès privilégié

- Module 4 : Concevoir des solutions pour les opérations de sécurité
- Étude de cas 1 : Étude de cas interactive — Concevoir des solutions de sécurité pour l’infrastructure
- Étude de cas 2 : Étude de cas interactive — Moderniser le contrôle d’accès et la résilience face aux menaces

Parcours d’apprentissage 3 : Concevoir des solutions de sécurité pour les applications et les données

- Module 1 : Concevoir des solutions pour sécuriser Microsoft 365
- Module 2 : Concevoir des solutions pour sécuriser les applications
- Module 3 : Concevoir des solutions pour sécuriser les données organisationnelles
- Étude de cas 1 : Étude de cas interactive — Sécuriser les applications et les données

Parcours d’apprentissage 4 : Concevoir des solutions de sécurité pour l’infrastructure

- Module 1 : Définir les exigences pour sécuriser les services SaaS, PaaS et IaaS
- Module 2 : Concevoir des solutions pour la gestion de la posture de sécurité dans les environnements hybrides et multinuages
- Module 3 : Concevoir des solutions pour sécuriser les serveurs et les postes clients
- Module 4 : Évaluer les solutions de sécurité réseau et Security Service Edge (SSE)
- Étude de cas 1 : Étude de cas interactive — Sécuriser les points de terminaison et l’infrastructure

Approche et méthode pédagogique

Approche pratique et structurée combinant théorie ciblée et ateliers guidés .

Les participants développent progressivement une expertise d’architecte en cybersécurité Microsoft grâce à des exercices concrets inspirés de scénarios professionnels .

Ils apprennent à concevoir des stratégies de sécurité globales, intégrer les solutions Microsoft et bâtir des architectures robustes alignées sur les meilleures pratiques et les exigences de conformité .

La formation, animée par un formateur certifié Microsoft (MCT), met l’accent sur l’interactivité et le développement de compétences techniques et stratégiques transférables

Prérequis

Les participants

doivent posséder les connaissances et l’expérience suivantes avant de suivre ce

cours :

- Connaissances conceptuelles des politiques de sécurité, des exigences, de l’architecture Zero Trust et de la gestion des environnements hybrides
- Expérience pratique des stratégies Zero Trust, de l’application des politiques de sécurité et de la définition des exigences de sécurité basées sur les objectifs d’affaires

Recommandations

Prérequis facultatifs:

- Solide connaissance de la cybersécurité (principes, menaces, gestion des risques)
- Expérience avec les solutions Microsoft Security (Defender, Sentinel, Entra ID, Purview)
- Familiarité avec les cadres CAF, WAF, MCRA et MCSB
- Compréhension des concepts infonuagiques (Azure, Microsoft 365)
- Notions d’architecture de sécurité et de gouvernance
- Expérience en administration ou ingénierie de la sécurité (fortement recommandée)
- Connaissance des stratégies de résilience face aux cybermenaces (ex. rançongiciels)
- Recommandation : avoir réussi une certification de niveau associé (SC 200, SC 300, SC 401 ou SC 500)

Certifications

Microsoft certifié : expert en architecture de cybersécurité

Notes légales