# Microsoft Cybersecurity Architect

**Durée: 4 Jours** **Réf de cours: M-SC100** **Méthodes d'apprentissage: Classe à distance**

## Résumé:

**Cette formation est délivrée en synchrone à distance tout en garantissant l'accès à un environnement d'apprentissage complet**
Elle permet aux participants d'acquérir les compétences et connaissances nécessaires pour concevoir et à évaluer des stratégies de cybersécurité dans les domaines suivants : Confiance zéro, gouvernance, risque et conformité (GRC), opérations de sécurité (SecOps), et données et applications. Les participants apprendront également à concevoir et à architecturer des solutions en utilisant les principes de confiance zéro et à spécifier les exigences de sécurité pour l'infrastructure du cloud dans différents modèles de services (SaaS, PaaS, IaaS).
*Mise à jour : 14.12.2022*

## Public visé:

Cette formation s'adresse aux professionnels de l'informatique ayant une expérience et des connaissances avancées dans un large éventail de domaines d'ingénierie de la sécurité, notamment l'identité et l'accès, la protection des plateformes, les opérations de sécurité, la sécurisation des données et la sécurisation des applications. Ils doivent également avoir une expérience des mises en œuvre hybrides et en nuage.

## Objectifs pédagogiques:

- A l'issue de la formation, les participants seront capables de :
- Concevoir une stratégie et une architecture de confiance zéro
- Évaluer les stratégies techniques de gouvernance, de risque et de conformité (GRC) et les stratégies de sécurité opérationnelle
- Concevoir la sécurité de l'infrastructure
- Concevoir une stratégie pour les données et les applications

## Pré-requis:

Expérience et connaissances avancées en matière d'identité et d'accès, de protection des plateformes, d'opérations de sécurité, de sécurisation des données et de sécurisation des applications.

Expérience des mises en œuvre hybrides et dans le Cloud.

- M-SC300 - Administration des accès et de l'identité Microsoft
- M-SC400 - Administration de la Protection de l'information Microsoft

## Test et certification

Cette formation prépare à la certification **Microsoft Certified : Cybersecurity Architect Expert Certification** après réussite de l'examen SC-100 .

Pour valider votre titre de certification Cybersecurity Architect Expert, vous devez obtenir également au moins l'un des titres suivants :

- Microsoft Certified : Security Operations Analyst Associate SC-200
- Microsoft Certified : Identity and Access Administrator Associate SC-300
- Microsoft Certified : Azure Security Engineer Associate AZ-500
- Microsoft 365 Certified : Security Administrator Associate certification MS-500

## Contenu:

Construire une stratégie et une architecture de sécurité globale

- Introduction
- Aperçu de la confiance zéro
- Développer des points d'intégration dans une architecture
- Développer des exigences de sécurité basées sur des objectifs commerciaux
- Traduire les exigences de sécurité en capacités techniques
- Concevoir la sécurité pour une stratégie de résilience
- Concevoir une stratégie de sécurité pour les environnements hybrides et multi-tenant
- Concevoir des stratégies techniques et de gouvernance pour le filtrage et la segmentation du trafic
- Comprendre la sécurité des protocoles
- Exercice : Construire une stratégie et une architecture de sécurité globale
- Contrôle des connaissances
- Résumé

Concevoir une stratégie d'opérations de sécurité

- Introduction
- Comprendre les cadres, processus et procédures des opérations de sécurité
- Concevoir une stratégie de sécurité en matière de journalisation et d'audit
- Développer des opérations de sécurité pour les environnements hybrides et multi-clouds
- Concevoir une stratégie pour la gestion des informations et des événements de sécurité (SIEM) et l'orchestration de la sécurité
- Évaluer les flux de travail de sécurité
- Examiner les stratégies de sécurité pour la gestion des incidents
- Évaluer la stratégie des opérations de sécurité pour le partage des renseignements techniques sur les menaces
- Surveiller les sources de renseignements sur les menaces et les mesures d'atténuation.

Concevoir une stratégie de sécurité des identités

- Introduction
- Sécuriser l'accès aux ressources du cloud
- Recommandation d'un magasin d'identité pour la sécurité
- Recommandation de stratégies d'authentification et d'autorisation sécurisées
- Accès conditionnel sécurisé
- Conception d'une stratégie d'attribution et de délégation de rôles
- Définir la gouvernance des identités pour les contrôles d'accès et la gestion des droits
- Conception d'une stratégie de sécurité pour

Évaluer la posture de sécurité et recommander des stratégies techniques pour gérer les risques

- Introduction
- Évaluer la posture de sécurité à l'aide de repères
- Évaluer la posture de sécurité à l'aide de Microsoft Defender for Cloud
- Évaluer les postures de sécurité à l'aide de Secure Scores
- Évaluer l'hygiène de sécurité des charges de travail dans le Cloud
- Concevoir la sécurité d'une Azure Landing Zone
- Interpréter les renseignements sur les menaces techniques et recommander des mesures d'atténuation des risques
- Recommander des capacités ou des contrôles de sécurité pour atténuer les risques identifiés.

Comprendre les meilleures pratiques d'architecture et la façon dont elles évoluent avec le cloud

- Introduction
- Planifier et mettre en œuvre une stratégie de sécurité au sein des équipes
- Établir une stratégie et un processus pour une évolution proactive et continue de la stratégie de sécurité
- Comprendre les protocoles réseau et les meilleures pratiques de segmentation du réseau et de filtrage du trafic

Concevoir une stratégie pour sécuriser les points d'extrémité des serveurs et des clients

- Introduction
- Définir les lignes de base de la sécurité pour les points d'extrémité des serveurs et des clients
- Définir les exigences de sécurité pour les serveurs
- Spécifier les exigences de sécurité pour les appareils mobiles et les clients
- Préciser les exigences en matière de sécurisation des services de domaine Active Directory
- Conception d'une stratégie de gestion des secrets, des clés et des certificats
- Concevoir une stratégie d'accès à distance sécurisé
- Comprendre les cadres, processus et procédures des opérations de sécurité
- Comprendre les procédures d'investigation approfondie par type de ressources

Concevoir une stratégie pour sécuriser les services PaaS, IaaS et SaaS

Spécifier les exigences de sécurité pour les applications

- Introduction
- Comprendre la modélisation des menaces pour les applications
- Définir les priorités pour atténuer les menaces pesant sur les applications
- Définir une norme de sécurité pour l'intégration d'une nouvelle application
- Définir une stratégie de sécurité pour les applications et les API

Concevoir une stratégie de sécurisation des données

- Introduction
- Établir des priorités pour atténuer les menaces pesant sur les données
- Concevoir une stratégie pour identifier et protéger les données sensibles
- Définir une norme de chiffrement pour les données au repos et en mouvement

l'accès des rôles privilégiés à l'infrastructure
- Concevoir une stratégie de sécurité pour les activités privilégiées
- Comprendre la sécurité des protocoles

Évaluer une stratégie de conformité réglementaire

- Introduction
- Interpréter les exigences de conformité et leurs capacités techniques
- Évaluer la conformité de l'infrastructure en utilisant Microsoft Defender for Cloud
- Interpréter les scores de conformité et recommander des actions pour résoudre les problèmes ou améliorer la sécurité
- Concevoir et valider la mise en œuvre de la politique Azure
- Conception pour les exigences de résidence des données
- Traduire les exigences de confidentialité en exigences pour les solutions de sécurité

- Introduction
- Définir des lignes de base de sécurité pour les services PaaS
- Spécifier les lignes de base de sécurité pour les services IaaS
- Spécifier les lignes de base de sécurité pour les services SaaS
- Spécifier les exigences de sécurité pour les charges de travail IoT
- Spécifier les exigences de sécurité pour les charges de travail de données
- Spécifier les exigences de sécurité pour les charges de travail Web
- Spécifier les exigences de sécurité pour les charges de travail de stockage
- Spécifier les exigences de sécurité pour les conteneurs
- Spécifier les exigences de sécurité pour l'orchestration des conteneurs

## Méthodes pédagogiques :

Pour le suivi de cette formation à distance depuis un site client équipé, il suffit d'avoir une bonne connexion internet, un casque avec micro et d'être dans un endroit au calme pour en profiter pleinement. Une fiche explicative est adressée en amont aux participants pour leur permettre de vérifier leur installation technique et de se familiariser avec la solution technologique utilisée.
L'accès à l'environnement d'apprentissage (support de cours officiel, labs), ainsi qu'aux feuilles d'émargement et d'évaluation est assuré.
En savoir plus : https://www.globalknowledge.com/fr-fr/solutions/methodes-d'apprentissage/classe-a-distance

## Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

•Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
•Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
•Attention, si vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.