Smartfuture
Business | Education | Training solutions

Microsoft Azure

Formation & Certification

Architecte en cybersécurité Microsoft

SC-100

4 jours

Inscription

Visitez notre site web
smartfuture.tn

Architecte en cybersécurité Microsoft

Objectifs de la formation :

La formation "Expert Microsoft en architecture de cybersécurité" vise à doter les participants des compétences nécessaires pour concevoir et mettre en œuvre des solutions de sécurité robustes sur les plateformes Microsoft. Les participants apprendront à évaluer les risques de sécurité, à élaborer des stratégies de protection, à configurer des solutions de sécurité Microsoft (telles que Microsoft Defender, Azure Security Center, et Microsoft Sentinel), et à intégrer les principes de sécurité dans les architectures cloud et hybrides. À l'issue de la formation, les participants seront capables de protéger efficacement les infrastructures et les données tout en garantissant la conformité aux normes et réglementations en matière de sécurité.

Population ciblée :

- Architectes IT et de sécurité
- Administrateurs systèmes et réseaux
- Ingénieurs en cybersécurité
- Responsables de la sécurité des informations

Prérequis :

- Solide compréhension des concepts de cybersécurité
- Expérience avec les services Microsoft, notamment Azure et Microsoft 365
- Connaissances en administration des systèmes et des réseaux
- Familiarité avec les réglementations et normes de sécurité (comme ISO 27001, NIST, etc.)

Le programme de la formation

Architecte en cybersécurité Microsoft

Microsoft Azure

Durée : 28 heures

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

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

- Concevoir une stratégie de sécurité pour prendre en charge les objectifs de résilience de l'entreprise, notamment l'identification et la hiérarchisation des menaces sur les ressources vitales pour l'entreprise
- Concevoir des solutions pour la continuité d'activité et reprise d'activité (BCDR), y compris la sauvegarde et la restauration sécurisées pour les environnements hybrides et multicloud.
- Concevoir des solutions pour atténuer les attaques par ransomware, notamment la hiérarchisation de BCDR et l'accès privilégié
- Concevoir des solutions pour les correctifs de sécurité

Concevoir des solutions qui s'alignent sur MCRA (Microsoft Cybersecurity Reference Architectures) et MCSB (Microsoft Cloud Security Benchmark)

- Concevoir des solutions qui s'alignent sur les bonnes pratiques relatives aux fonctionnalités et aux contrôles de cybersécurité
- Créer des solutions qui s'alignent avec les meilleures pratiques de protection contre les attaques internes, externes et liées à la chaîne d'approvisionnement
- Concevoir des solutions qui s'alignent sur les bonnes pratiques relatives à la sécurité Confiance Zéro, notamment le plan de modernisation rapide pour la Confiance Zéro (RaMP)

Concevoir des solutions qui s'alignent sur le Microsoft Cloud Adoption Framework pour Azure et le Microsoft Azure Well-Architected Framework

- Concevoir une nouvelle stratégie ou évaluer une stratégie existante de sécurité et de gouvernance basée sur le Microsoft Cloud Adoption Framework (CAF) pour Azure et le Microsoft Azure Well-Architected Framework
- Recommander des solutions de sécurité et de gouvernance selon le Microsoft Cloud Adoption Framework pour Azure et le Microsoft Azure Well-Architected Framework
- Concevoir des solutions pour implémenter et gouverner la sécurité à l'aide de zones d'atterrissage Azure
- Concevoir un processus DevSecOps qui s'aligne sur les meilleures pratiques dans Microsoft Cloud Adoption Framework (CAF)

Inscription

Smartfuture
Business | Education | Training solutions

Le programme de la formation

Architecte en cybersécurité Microsoft

Microsoft Azure

Module 2: Concevoir des capacités en matière d'opérations de sécurité, d'identité et de conformité

Concevoir des solutions pour les opérations de sécurité

- 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 pour la journalisation et un audit centralisés, notamment Microsoft Purview Audit
- Concevoir une solution de surveillance pour prendre en charge les environnements hybrides et multicloud
- Concevoir une solution d'orchestration, d'automatisation et de réponse dans le domaine de la sécurité (SOAR), notamment Microsoft Sentinel et Microsoft Defender XDR
- 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

Concevoir des solutions pour gérer les identités et les accès

- Concevoir une solution pour accéder aux ressources SaaS (software as a service), PaaS (platform as a service), IaaS (infrastructure as a service), hybrides/locales et multiclouds, notamment des contrôles d'identité, de réseau et d'application
- Concevoir une solution pour Microsoft Entra ID, y compris pour les environnements hybrides et multiclouds
- Concevoir une solution pour les identités externes, y compris les identités B2B, B2C et décentralisées
- Concevoir une stratégie moderne d'authentification et d'autorisation, y compris l'accès conditionnel, l'évaluation continue de l'accès, l'évaluation des risques et les actions protégées.
- Valider l'alignement des stratégies d'accès conditionnel sur une stratégie 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

Concevoir des solutions pour sécuriser les accès privilégiés

- Concevoir une solution pour attribuer et déléguer des rôles privilégiés à l'aide du modèle d'accès d'entreprise
- Évaluer la sécurité et la gouvernance de Microsoft Entra ID, y compris Microsoft Entra Privileged Identity Management (PIM), la gestion des droits d'utilisation et l'examen des accès
- Évaluer la sécurité et la gouvernance des services de domaine Active Directory (AD DS) locaux, y compris la résistance aux attaques courantes
- Concevoir une solution pour sécuriser l'administration des locataires cloud, notamment l'infrastructure et les plateformes SaaS et multiclouds

Smartfuture
Business | Education | Training solutions

Inscription

Le programme de la formation

Architecte en cybersécurité Microsoft

Microsoft Azure

- Concevoir une solution de gestion des droits d'utilisation de l'infrastructure cloud qui inclut Gestion des autorisations Microsoft Entra
- Évaluer une solution de gestion des révisions d'accès qui inclut Microsoft Entra Permissions Management
- Concevoir une solution pour la station de travail à accès privilégié (PAW), y compris l'accès à distance

Concevoir des solutions de 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
- Concevoir une solution pour répondre aux exigences de confidentialité, notamment Microsoft Priva
- Concevoir des solutions Azure Policy pour répondre aux exigences de sécurité et de conformité
- Évaluer et valider l'alignement sur les normes réglementaires et les benchmarks à l'aide de Microsoft Defender pour le cloud

Module 3 : Concevoir des solutions de sécurité pour l'infrastructure

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

- Évaluer l'état de la sécurité en utilisant Microsoft Defender pour le cloud, y compris le Microsoft cloud security benchmark (MCSB)
- Évaluer la posture de sécurité en utilisant le niveau de sécurité Microsoft
- Concevoir des solutions intégrées de gestion de l'état de la sécurité qui incluent Microsoft Defender pour le cloud dans des environnements hybrides et multi-cloud
- Sélectionner les solutions de protection des charges de travail dans Microsoft Defender pour le cloud
- Concevoir une solution pour intégrer des environnements hybrides et multiclouds avec Azure Arc
- Concevoir une solution pour Microsoft Defender External Attack Surface Management (Defender EASM)
- Spécifiez les exigences et les priorités d'un processus de gestion de l'état qui utilise les voies d'attaque de la gestion de l'exposition, la réduction de la surface d'attaque, les connaissances en matière de sécurité et les initiatives

Smartfuture
Business | Education | Training solutions

Inscription

Le programme de la formation

Architecte en cybersécurité Microsoft

Microsoft Azure

Spécifier les exigences en matière de sécurisation des points de terminaison du serveur et du client

- Spécifier les exigences de sécurité pour les serveurs, y compris plusieurs plateformes et systèmes d'exploitation
- Spécifier les exigences de sécurité pour les appareils mobiles et les clients, y compris la protection, la sécurisation renforcée et la configuration des points de terminaison
- Spécifier les exigences de sécurité pour les appareils IoT et les systèmes incorporés
- Évaluer des solutions pour sécuriser les technologies opérationnelles (OT) et les systèmes de contrôle industriels (ICS) avec Microsoft Defender pour IoT
- Spécifier des lignes de base de sécurité pour les points de terminaison serveur et client
- Évaluer les solutions LAPS (solutions de mot de passe d'administrateur local) Windows

Spécifier les exigences pour sécuriser les services 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 les exigences de sécurité pour les charges de travail web
- Spécifier des exigences de sécurité pour les conteneurs
- Spécifier les exigences de sécurité pour l'orchestration des conteneurs
- Évaluer les solutions qui incluent Azure AI Services Security

Évaluer les solutions pour la sécurité réseau et Security Service Edge (SSE)

- Évaluer les conceptions réseau pour s'aligner sur les exigences de sécurité et les meilleures pratiques
- Évaluer les solutions qui utilisent Microsoft Entra Internet Access comme passerelle web sécurisée
- Évaluer les solutions qui utilisent Microsoft Entra Internet Access pour accéder à Microsoft 365, y compris les configurations interlocataires
- Évaluer les solutions qui utilisent l'accès privé Microsoft Entra

Module 4: Concevoir des solutions de sécurité pour les applications et les données

Évaluer des solutions pour sécuriser Microsoft 365

- Évaluer la posture de sécurité pour les charges de travail de productivité et de collaboration en utilisant des métriques, y compris le Niveau de sécurité Microsoft
- Évaluer les solutions qui incluent Microsoft Defender pour Office et les applications Microsoft Defender pour le cloud

Smartfuture
Business | Education | Training solutions

Inscription

Le programme de la formation

Architecte en cybersécurité Microsoft

Microsoft Azure

- Évaluer les solutions de gestion des appareils qui incluent Microsoft Intune
- Évaluer les solutions de sécurisation des données dans Microsoft 365 à l'aide de Microsoft Purview
- Évaluer la sécurité des données et les contrôles de conformité dans Microsoft Copilot pour les services Microsoft 365

Concevoir des solutions pour sécuriser les applications

- Évaluer la posture de sécurité de portefeuilles d'applications existants
- Évaluer les menaces pesant sur les applications vitales pour l'entreprise en utilisant la modélisation des menaces
- Concevoir et implémenter une stratégie de cycle de vie complet pour la sécurité des applications
- Concevoir et implémenter des normes et des pratiques pour sécuriser le processus de développement d'applications
- Mapper les technologies aux exigences de sécurité des applications
- Concevoir une solution d'identité de charge de travail pour authentifier les ressources cloud Azure et y accéder
- Concevoir une solution pour la gestion et la sécurité des API
- Concevoir des solutions qui sécurisent les applications à l'aide d'Azure Web Application Firewall (WAF)

Concevoir des solutions pour sécuriser les données d'une organisation

- Évaluer les solutions pour la recherche et la classification de données
- Spécifier des priorités pour atténuer les menaces sur les données
- Évaluer les solutions pour le chiffrement de données au repos et en transit, notamment Azure KeyVault et le chiffrement d'infrastructure
- Concevoir une solution de sécurité pour les données dans les charges de travail Azure, notamment Azure SQL, Azure Synapse Analytics et Azure Cosmos DB
- Concevoir une solution de sécurité pour les données dans Stockage Azure
- Concevoir une solution de sécurité qui inclut Microsoft Defender pour le stockage et Microsoft Defender for Databases

Smartfuture
Business | Education | Training solutions

Inscription

Smartfuture
Business | Education | Training solutions

Notre équipe de formateurs

Nos formateurs certifiés sur les technologies Microsoft possèdent une expertise pédagogique et pratique de haut niveau, combinant une maîtrise approfondie des outils avec une expérience terrain solide. Leur double compétence leur permet de transmettre des connaissances actualisées et concrètes, adaptées aux besoins réels des entreprises. Grâce à leur certification, ils sont en mesure d'offrir des formations interactives, axées sur la résolution de problématiques techniques et l'optimisation des infrastructures Microsoft, garantissant ainsi des résultats tangibles et une montée en compétences rapide des équipes.

Investissez dans la formation avec des formateurs qualifiés : validez vos compétences et propulsez la performance de votre entreprise !

Smartfuture
Business | Education | Training solutions

Pour obtenir plus d'informations, n'hésitez pas à nous contacter.

Thank You

47, Av Mouaouia Ibn Abi Sofiane EL Menzah 6 Ariana Tunisie
+216 70 100 500
www.smartfuture.tn