Mettre en œuvre des contrôles de sécurité de bout en bout pour les charges de travail infonuagiques et en IA (SC500T00)

Durée: 4 jours
Public cible: Professionnel TI

À qui s'adresse cette formation ?

En tant que candidat à ce cours, vous êtes un ingénieur en sécurité qui protège les systèmes et les données organisationnelles dans des environnements infonuagiques et hybrides en mettant en place des contrôles de sécurité complets qui préviennent l’accès non autorisé et atténuent les risques de manière proactive.

Ce rôle couvre plusieurs domaines de sécurité, incluant l’identité, le réseau, les applications, les données et le calcul.

Ce rôle veille également à ce que les plateformes, les données, les identités et l’infrastructure utilisées par les charges de travail en IA soient mises en œuvre et surveillées de manière sécurisée.

Vous travaillez en étroite collaboration avec les architectes, administrateurs, ingénieurs, analystes et développeurs responsables d’Azure, Microsoft 365, de l’identité et des accès, de la protection de l’information, des opérations de sécurité, du DevOps, du développement applicatif, des plateformes de bases de données et des réseaux.

Vous devriez avoir une expérience pratique en administration de Microsoft Azure et des environnements hybrides, incluant le calcul, le réseau et le stockage.

Objectifs de la formation

Après avoir terminé ce cours, les participants seront en mesure de/:

- Sécuriser l’identité et l’accès pour les utilisateurs, les applications et les agents.
- Protéger les secrets, les clés, les certificats, le stockage et les bases de données.
-

Appliquer la gouvernance, les stratégies et les contrôles de moindre privilège dans Azure.

- Sécuriser l’accès réseau aux ressources et services Azure.
- Évaluer et protéger les charges de travail en IA, les agents et les chemins d’exposition des données.
- Sécuriser les plateformes de calcul, de conteneurs et d’applications.
- Gérer la posture de sécurité infonuagique dans Azure, les environnements hybrides et multinuages.

Description sommaire

Ce cours vous prépare à concevoir, mettre en œuvre et gérer des contrôles de sécurité de bout en bout dans les environnements Microsoft Azure et Microsoft 365; y compris le paysage émergent des charges de travail en IA et des agents autonomes.

Grâce à une combinaison de séances dirigées par un instructeur et de laboratoires pratiques, vous développez des compétences concrètes en sécurité des identités, protection de l’infrastructure infonuagique, détection des menaces et gestion de la posture de sécurité.

Ce cours s’adresse aux ingénieurs en sécurité responsables de la planification et de la mise en œuvre de contrôles de sécurité dans des environnements infonuagiques, hybrides et multinuages utilisant les technologies de sécurité Microsoft.

Contenu du plan de cours

Parcours d’apprentissage 1 : Sécuriser l’accès aux ressources avec Microsoft Entra ID

- Module 1 : Gérer et mettre en œuvre les méthodes d’authentification dans Microsoft Entra ID
- Module 2 : Mettre en œuvre et configurer Privileged Identity Management (PIM)
- Module 3 : Authentifier votre plugiciel API pour les agents déclaratifs avec des API sécurisées

Parcours d’apprentissage 2 : Sécuriser les secrets et les clés avec Azure Key Vault

- Module 1 : Configurer et sécuriser Azure Key Vault
- Module 2 : Gérer les clés et les secrets dans Azure Key Vault
- Module 3 : Gérer les certificats et surveiller Azure Key Vault
- Module 4 : Protéger Azure Key Vault avec Microsoft Defender for Cloud

Parcours d’apprentissage 3 : Mettre en œuvre la gouvernance pour appliquer la sécurité et la conformité réglementaire

- Module 1 : Appliquer la gouvernance avec Azure Policy et les verrous de ressources
- Module 2 : Configurer les contrôles de sécurité et corriger les recommandations dans Defender for Cloud
- Module 3 : Évaluer la conformité réglementaire dans Defender for Cloud
- Module 4 : Gérer et ajuster les affectations de rôles RBAC pour le moindre privilège
- Module 5 : Protéger les données de sauvegarde avec les fonctionnalités de sécurité d’Azure Backup
- Module 6 : Mettre en œuvre des contrôles de sécurité dans l’infrastructure comme code

Parcours d’apprentissage 4 : Mettre en œuvre la sécurité pour les comptes de stockage

- Module 1 : Décrire les services de stockage Azure
- Module 2 : Mettre en œuvre la sécurité et gérer l’accès pour Azure Storage

- Module 3 : Configurer la sécurité réseau pour Azure Storage
- Module 4 : Mettre en œuvre Microsoft Defender for Storage

Parcours d’apprentissage 5 : Mettre en œuvre la sécurité pour le réseau Azure

- Module 1 : Segmenter et isoler les charges de travail Azure à l’aide des contrôles de sécurité réseau
- Module 2 : Centraliser et appliquer l’inspection du trafic avec Azure Firewall
- Module 3 : Sécuriser la connectivité à distance et hybride avec les passerelles VPN et Microsoft Entra Private Access
- Module 4 : Éliminer l’exposition au réseau public des services Azure PaaS

Parcours d’apprentissage 6 : Mettre en œuvre la sécurité pour l’IA

- Module 1 : Sécuriser l’accès pour l’identité des agents Microsoft Entra
- Module 2 : Analyser les risques liés à l’identité en IA avec Microsoft Defender XDR
- Module 3 : Activer la protection en temps réel pour les agents Copilot Studio
- Module 4 : Configurer la sécurité de l’AI Gateway dans Microsoft Foundry
- Module 5 : Configurer et gérer les garde fous dans Microsoft Foundry
- Module 6 : Protéger les charges de travail en IA avec Microsoft Defender for Cloud
-

Module 7 : Activer la protection des services IA dans Microsoft Defender for Cloud

- Module 8 : Gérer les agents avec Microsoft Agent 365
- Module 9 : Identifier les risques liés aux données en IA avec Microsoft Purview Data Security Posture Management

Parcours d’apprentissage 7 : Mettre en œuvre la sécurité pour les serveurs et les machines virtuelles

- Module 1 : Mettre en œuvre le chiffrement des disques pour les machines virtuelles Azure
- Module 2 : Configurer les fonctionnalités de sécurité Trusted Launch pour les machines virtuelles Azure
- Module 3 : Planifier et mettre en œuvre Azure Bastion
- Module 4 : Gérer la sécurité pour les serveurs hybrides activés par Arc
- Module 5 : Mettre en œuvre Microsoft Defender for Servers
- Module 6 : Activer et appliquer l’accès Just in Time aux machines virtuelles
- Module 7 : Appliquer la configuration de sécurité des VM avec Azure Machine Configuration

Parcours d’apprentissage 8 : Mettre en œuvre la sécurité pour les services de plateforme applicative

- Module 1 : Détecter les risques liés aux conteneurs avec Microsoft Defender for Containers
-

Module 2 : Mettre en œuvre les contrôles de sécurité pour Azure Kubernetes Service

- Module 3 : Mettre en œuvre les contrôles de sécurité pour Azure Container Registry, Container Instances et Container Apps
- Module 4 : Mettre en œuvre les contrôles de sécurité pour Azure Function Apps et Logic Apps
- Module 5 : Mettre en œuvre les contrôles de sécurité pour Azure App Services et Web Application Firewall
- Module 6 : Mettre en œuvre la sécurité du backend API avec Azure API Management

Parcours d’apprentissage 9 : Gérer la posture de sécurité avec Defender for Cloud

- Module 1 : Connecter les environnements hybrides et multinuages à Microsoft Defender for Cloud
- Module 2 : Identifier les risques de sécurité à l’aide de la gestion de la posture de sécurité infonuagique
- Module 3 : Découvrir les actifs non protégés et les vulnérabilités avec Microsoft Defender External Attack Surface Management
- Module 4 : Évaluer la conformité réglementaire dans Defender for Cloud
- Module 5 : Activer et configurer les plans de protection des charges de travail dans Microsoft Defender for Cloud
- Module 6 : Configurer les paramètres de gestion des vulnérabilités Microsoft Defender pour les machines virtuelles Azure

Parcours d’apprentissage 10 : Mettre en œuvre la collecte d’activités et d’événements dans Microsoft Sentinel

- Module 1 : Créer et gérer les espaces de travail Microsoft Sentinel
- Module 2 : Gérer le contenu dans Microsoft Sentinel
- Module 3 : Connecter les services Microsoft à Microsoft Sentinel
- Module 4 : Connecter les sources de données syslog à Microsoft Sentinel
- Module 5 : Connecter les journaux Common Event Format à Microsoft Sentinel
- Module 6 : Connecter les hôtes Windows à Microsoft Sentinel

- Module 7 : Mettre en œuvre les règles d’automatisation et les playbooks dans Microsoft Sentinel
- Module 8 : Gérer le stockage des données et les journaux d’audit des requêtes dans Microsoft Sentinel

Parcours d’apprentissage 11 : Mettre en œuvre Microsoft Security Copilot

- Module 1 : Décrire Microsoft Security Copilot
- Module 2 : Configurer les espaces de travail pour Microsoft Security Copilot
- Module 3 : Gérer les plugiciels et les agents dans Microsoft Security Copilot

Approche et méthode pédagogique

Approche pratique et structurée combinant une théorie ciblée avec des laboratoires pratiques guidés. Les participants mettent progressivement en œuvre des contrôles de sécurité de bout en bout dans Azure, Microsoft 365 et les charges de travail en IA grâce à des exercices réels basés sur des scénarios qui favorisent l’application immédiate des apprentissages.

Ils apprennent à sécuriser les identités, les accès, les données, l’infrastructure infonuagique, les secrets, les applications et les solutions d’IA en utilisant des outils tels que Microsoft Entra ID, Azure Key Vault, Microsoft Defender et Microsoft Security Copilot.

Animé par un formateur certifié Microsoft (MCT), le cours met l’accent sur l’interactivité et le développement de compétences techniques directement transférables pour renforcer la posture de sécurité dans des environnements hybrides et multinuages.

Prérequis

Une connaissance de base est recommandée avant de commencer ce cours/:

-

Connaissances fondamentales d’Azure : abonnements, groupes de ressources, réseaux virtuels, comptes de stockage, machines virtuelles et contrôle d’accès basé sur les rôles Azure (RBAC).

- Connaissances de base en identité et accès : Microsoft Entra ID, utilisateurs, groupes, authentification, autorisation, authentification multifacteur, accès conditionnel, et identités d’applications ou de services.Principes généraux de sécurité : moindre privilège, défense en profondeur, Zero Trust, protection contre les menaces, chiffrement, audit et configuration sécurisée.
- Connaissances de base en réseautique infonuagique : VNets, sous-réseaux, points de terminaison privés, pare-feu, VPN et règles de sécurité réseau.
- Connaissances de base des données et des charges de travail : types courants de charges Azure comme le stockage, les bases de données SQL, les machines virtuelles, les conteneurs, App Services et les API.
- Familiarité avec les outils de sécurité Microsoft : Microsoft Defender for Cloud, Microsoft Sentinel, Microsoft Defender XDR, Microsoft Purview ou Security Copilot.Notions introductives en IA : concepts de base tels que les copilotes, les agents, les invites (prompts), les modèles et l’ancrage des données (data grounding).
- Expérience pratique avec le portail Azure : navigation dans le portail et réalisation de modifications de configuration de base dans un environnement de laboratoire.

Recommandations

Formations complémentaires suggérées: AZ-104, SC-200, SC-300, SC-401

Certifications

Microsoft Certified: Cloud and AI Security Engineer Associate

Notes légales