Sécuriser les services et charges de travail Azure avec Microsoft Defender pour le cloud pour les contrôles de conformité réglementaire (SC-5002)

Description

Sécurisez vos services et charges de travail Azure

La sécurité des services cloud est essentielle pour garantir la conformité aux réglementations en vigueur. Avec la formation « Sécuriser les services et charges de travail Azure avec Microsoft Defender pour le cloud pour les contrôles de conformité réglementaire (SC-5002) », vous apprendrez à renforcer la protection de vos infrastructures sur Azure. Ce programme vous guide dans l'implémentation des meilleures pratiques de sécurité grâce à Microsoft Defender pour le cloud.

Maîtrisez les outils clés de la conformité

Dans ce parcours, vous découvrirez comment Microsoft Defender pour le cloud simplifie la conformité réglementaire. Vous apprendrez à analyser et traiter les vulnérabilités en utilisant des outils comme Azure Key Vault, Azure Log Analytics et Azure Private Link. Vous verrez aussi comment configurer des groupes de sécurité réseau et renforcer la surveillance des machines virtuelles Azure.

Contenu du cours
Module 1 : Examiner les normes de conformité réglementaire de Defender pour le cloud

- Normes de conformité réglementaire dans Defender pour le cloud
- Benchmark de sécurité cloud Microsoft dans Defender pour le cloud
- Améliorer votre conformité réglementaire dans Defender pour le cloud

Module 2 : Activer Defender pour le cloud sur votre abonnement Azure

- Connecter vos abonnements Azure
- Configurer Microsoft Defender pour le cloud pour une protection renforcée

Module 3 : Filtrer le trafic réseau avec un groupe de sécurité réseau à l'aide du portail Azure

- Groupe de ressources Azure
- Réseau virtuel Azure
- Façon dont les groupes de sécurité réseau filtrent le trafic
- Groupes de sécurité d'application
- Créer une infrastructure de réseau virtuel

Module 4 : Créer un espace de travail Log Analytics

- Espace de travail Log Analytics
- Créer un espace de travail Log Analytics

Module 5 : Collecter les données de surveillance du système d'exploitation invité des machines virtuelles Azure

- Déployer l’agent Azure Monitor
- Collecter des données avec l’agent Azure Monitor
- Créer une règle de collecte de données et installer l’agent Azure Monitor

Module 6 : Explorer l’accès juste-à-temps à une machine virtuelle

- Comprendre l’accès juste-à-temps aux machines virtuelles
- Activer l’accès juste-à-temps sur des machines virtuelles

Module 7 : Configurer les paramètres de mise en réseau Azure Key Vault

- Concepts de base d’Azure Key Vault
- Bonnes pratiques relatives à Azure Key Vault
- Sécurité réseau Azure Key Vault
- Configurer les pare-feux et réseaux virtuels d’Azure Key Vault
- Configurer les paramètres réseau de Key Vault
- Vue d’ensemble de la suppression réversible dans Azure Key Vault
- Points de terminaison de service de réseau virtuel pour Azure Key Vault
- Activer la suppression réversible dans Azure Key Vault

Module 8 : Se connecter à un serveur Azure SQL avec Azure Private Endpoint

- Azure Private Endpoint
- Azure Private Link
- Se connecter à un serveur Azure SQL à l’aide d’un point de terminaison privé Azure avec le Portail Azure

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.

Profils des participants

- Administrateurs cloud et sécurité
- Ingénieurs en cybersécurité
- Architectes cloud
- Consultants en conformité et sécurité des systèmes d’information
- Responsables IT souhaitant renforcer la sécurité des services Azure

Connaissances Préalables

- Connaissance de base des services et concepts Azure
- Compréhension des principes fondamentaux de la sécurité informatique
- Expérience avec la gestion des ressources cloud et des abonnements Azure

Objectifs

- Utiliser Microsoft Defender pour le cloud pour assurer la conformité réglementaire

- Activer et configurer Defender pour le cloud sur un abonnement Azure
- Mettre en place des groupes de sécurité réseau pour filtrer le trafic
- Créer et gérer un espace de travail Azure Log Analytics
- Déployer et configurer l'agent Azure Monitor pour collecter des données
- Gérer l'accès sécurisé aux machines virtuelles Azure avec l'accès juste-à-temps
- Configurer la mise en réseau d'Azure Key Vault pour protéger les secrets
- Connecter un serveur Azure SQL avec Azure Private Endpoint

Description
Sécuriser les services et charges de travail Azure avec Microsoft Defender pour le cloud pour les contrôles de conformité réglementaire (SC-5002)
Niveau
Intermédiaire
Prix de l'inscription en Présentiel (CHF)
900
Prix de l'inscription en Virtuel (CHF)
850
Durée (Nombre de Jours)
1
Reference
SC-5002