Programme de cours
Sécuriser les services et charges de travail Azure avec Microsoft Defender for Cloud pour les vérifications de conformité réglementaire

Durée :	1 jour soit 7 heures	Référence :	SC-5002

Public visé :

Cette formation est destinée aux professionnels de l'informatique et de la sécurité qui travaillent avec des services cloud, notamment Azure. Plus spécifiquement, voici les profils susceptibles de bénéficier de cette formation :

- **Administrateurs cloud** : Ceux qui gèrent et sécurisent des environnements Azure et doivent garantir la conformité avec des normes et réglementations de sécurité.
- **Professionnels de la sécurité informatique** : Experts en cybersécurité responsables de la mise en place de contrôles et de stratégies pour protéger les données et les infrastructures cloud.
- **Architectes cloud** : Ceux qui conçoivent des architectures sécurisées sur Azure et souhaitent intégrer les meilleures pratiques de sécurité et de conformité dans leurs solutions.
- **Consultants en conformité et sécurité** : Consultants externes ou internes qui accompagnent les entreprises dans l'adoption et la mise en œuvre de solutions cloud conformes aux normes de sécurité et de réglementation.
- **Responsables de la gouvernance et de la conformité** : Professionnels en charge de la gestion de la conformité réglementaire et de la supervision de la mise en œuvre des politiques de sécurité dans les environnements cloud.

Pré-requis :

- **Connaissances de base sur Azure** : Comprendre l'architecture d'Azure, la gestion des abonnements et des ressources (groupes de ressources, machines virtuelles, réseaux virtuels).
- **Notions de base en cybersécurité** : Connaître les principes fondamentaux de la sécurité des réseaux et la gestion des accès (IAM) dans un environnement cloud.
- **Pratique avec le portail Azure** : Être capable de naviguer et de configurer des services de base via le portail Azure.

Objectifs pédagogiques :

- **Maîtriser** les normes de conformité réglementaire et les contrôles du Microsoft Cloud Security Benchmark dans Microsoft Defender pour Cloud pour garantir la conformité des services Azure.
- **Acquérir** les compétences nécessaires pour activer et configurer Microsoft Defender pour Cloud sur un abonnement Azure, renforçant ainsi la gestion de la sécurité et la protection des charges de travail cloud.
- **Appliquer** les meilleures pratiques de sécurité réseau en configurant et filtrant le trafic à l'aide des groupes de sécurité réseau (NSG) et en créant une infrastructure de réseau virtuel dans Azure.
- **Mettre en œuvre** une collecte efficace des données de sécurité en déployant l'agent Azure Monitor et en configurant les règles de collecte de données pour assurer une surveillance renforcée des machines virtuelles et autres ressources Azure.
- **Configurer** des connexions sécurisées aux services Azure, y compris l'accès Just-in-Time aux machines virtuelles et l'utilisation de points de terminaison privés pour les bases de données SQL, afin de garantir la sécurité des communications et des données sensibles.

Compétences acquises à l'issue de la formation :

- Maîtriser les normes de conformité réglementaire et les contrôles du Microsoft Cloud Security Benchmark dans Microsoft Defender pour Cloud pour garantir la conformité des services Azure.
- Acquérir les compétences nécessaires pour activer et configurer Microsoft Defender pour Cloud sur un abonnement Azure, renforçant ainsi la gestion de la sécurité et la protection des charges de travail cloud.
- Appliquer les meilleures pratiques de sécurité réseau en configurant et filtrant le trafic à l'aide des groupes de sécurité réseau (NSG) et en créant une infrastructure de réseau virtuel dans Azure.
- Mettre en œuvre une collecte efficace des données de sécurité en déployant l'agent Azure Monitor et en configurant les règles de collecte de données pour assurer une surveillance renforcée des machines virtuelles et autres ressources Azure.
- Configurer des connexions sécurisées aux services Azure, y compris l'accès Just-in-Time aux machines virtuelles et l'utilisation de points de terminaison privés pour les bases de données SQL, afin de garantir la sécurité des communications et des données sensibles.

Modalités pédagogiques :

Session dispensée en présentiel ou téléprésentiel, selon la modalité inter-entreprises ou intra-entreprises sur mesure.
La formation est animée par un(e) formateur(trice) durant toute la durée de la session et présentant une suite de modules théoriques clôturés par des ateliers pratiques validant l'acquisition des connaissances. Les ateliers peuvent être accompagnés de Quizz.
L'animateur(trice) présente la partie théorique à l'aide de support de présentation, d'animation réalisée sur un environnement de démonstration.
En présentiel comme en téléprésentiel, l'animateur(trice) accompagne les participants durant la réalisation des ateliers.

Moyens et supports pédagogiques :

Cadre présentiel
Salles de formation équipées et accessibles aux personnes à mobilité réduite.
- Un poste de travail par participant
- Un support de cours numérique ou papier (au choix)
- Un bloc-notes + stylo
- Vidéoprojection sur tableau blanc
- Connexion Internet
- Accès extranet pour partage de documents et émargement électronique

Cadre téléprésentiel
Session dispensée via notre solution iClassroom s'appuyant sur Microsoft Teams.
- Un compte Office 365 par participant
- Un poste virtuel par participant

- Un support numérique (PDF ou Web)
- Accès extranet pour partage de documents et émargement électronique

Informations sur l'accessibilité :

Programme de cours
Sécuriser les services et charges de travail Azure avec Microsoft Defender for Cloud pour les vérifications de conformité réglementaire

Description / Contenu

Ce parcours de formation vous guide pour sécuriser les services et les charges de travail Azure en appliquant les contrôles du Microsoft Cloud Security Benchmark dans Microsoft Defender pour Cloud via le portail Azure.

Module 1 : Examinez les normes de conformité réglementaire de Defender pour Cloud.
Dans ce module, nous nous concentrerons sur l'utilisation de Microsoft Defender pour Cloud afin de simplifier la conformité réglementaire en identifiant et en résolvant les problèmes qui entravent le respect des normes et certifications de conformité.

- Normes de conformité réglementaire dans Defender pour Cloud
- Microsoft Cloud Security Benchmark dans Defender pour Cloud
- Améliorez votre conformité réglementaire dans Defender pour Cloud

Module 2 : Activez Defender pour Cloud sur votre abonnement Azure.
Dans ce module, nous nous concentrerons sur l'activation de Microsoft Defender pour Cloud sur votre abonnement Azure afin d'améliorer la surveillance de la sécurité, la gestion de la conformité et la protection contre les menaces pour vos applications cloud.

- Connectez vos abonnements Azure
- Exercice : Configurer Microsoft Defender pour Cloud pour une protection renforcée

Module 3 : Filtrez le trafic réseau à l'aide d'un groupe de sécurité réseau via le portail Azure.
Dans ce module, nous nous concentrerons sur le filtrage du trafic à l'aide des groupes de sécurité réseau (NSG) dans le portail Azure. Apprenez à créer, configurer et appliquer des groupes de sécurité réseau pour renforcer la sécurité de votre réseau.

- Groupe de ressources Azure
- Réseau virtuel Azure
- Comment les groupes de sécurité réseau filtrent le trafic
- Groupes de sécurité des applications
- Exercice : Créer une infrastructure de réseau virtuel

Module 4 : Créez un espace de travail Log Analytics.
Dans ce module, vous apprendrez à créer un espace de travail Log Analytics dans le portail Azure pour Microsoft Defender pour Cloud, ce qui améliore la collecte de données et l'analyse de sécurité.

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

Module 5 : Collectez les données de surveillance du système d'exploitation invité à partir des machines virtuelles Azure et hybrides en utilisant l'agent Azure Monitor.
Ce module vous montre comment déployer et gérer l'agent Azure Monitor, configurer les règles de collecte de données et l'intégrer à Microsoft Defender pour Cloud afin de renforcer la sécurité.

- Déployer l'agent Azure Monitor
- Collecter des données avec l'agent Azure Monitor
- Collecter des données à partir de vos charges de travail avec l'agent Log Analytics
- Configurer l'agent Log Analytics et l'espace de travail
- Exercice – Créer et modifier les règles de collecte de données et les associations dans Azure Monitor
- Exercice – Créer une règle de collecte de données et installer l'agent Azure Monitor

Module 6 : Explorer l'accès Just-in-Time à une machine virtuelle.
Dans ce module, nous nous concentrerons sur le risque des ports de gestion ouverts sur les machines virtuelles et sur la manière dont l'accès Just-in-Time (JIT) aux machines virtuelles dans Microsoft Defender pour Cloud permet d'atténuer cette menace.

- Comprendre l'accès Just-in-Time aux machines virtuelles
- Activer l'accès Just-in-Time aux machines virtuelles
- Exercice : Activer l'accès Just-in-Time sur les machines virtuelles

Module 7 : Configurer les paramètres de réseau d'Azure Key Vault.
Dans ce module, vous apprendrez à configurer les paramètres de réseau d'Azure Key Vault via le portail Azure afin d'assurer un accès sécurisé et contrôlé à vos secrets stockés.

- Concepts de base d'Azure Key Vault
- Meilleures pratiques d'Azure Key Vault
- Sécurité réseau d'Azure Key Vault
- Configurer les pare-feu et réseaux virtuels d'Azure Key Vault
- Exercice : Configurer les paramètres réseau de Key Vault
- Vue d'ensemble de la suppression souple dans Azure Key Vault
- Points de terminaison de service réseau pour Azure Key Vault
- Exercice – Activer la suppression souple dans Azure Key Vault

Module 8 : Se connecter à un serveur SQL Azure avec un point de terminaison privé Azure via le portail Azure.
Ce module vous guide sur la manière de connecter de manière sécurisée un serveur SQL Azure via le point de terminaison privé Azure dans le portail Azure, ce qui améliore la sécurité de la communication des données.

- Point de terminaison privé Azure
- Azure Private Link
- Exercice – Se connecter à un serveur SQL Azure en utilisant un point de terminaison privé Azure via le portail Azure