Sécuriser les ressources cloud avec les technologies de sécurité Microsoft (AZ-500)

Description

La sécurité des environnements cloud représente aujourd'hui un enjeu stratégique majeur pour toutes les organisations. Face à l'évolution constante des cybermenaces, les professionnels IT doivent maîtriser les technologies de protection les plus avancées. Cette formation vous permet d'acquérir les compétences essentielles pour sécuriser efficacement vos ressources Azure.

Protégez vos infrastructures cloud avec Microsoft

Conçu pour les ingénieurs et professionnels de la sécurité informatique, ce programme aborde l'ensemble des dimensions critiques. Vous apprendrez à gérer l'identité et les accès, protéger les réseaux virtuels et sécuriser les données sensibles. Chaque module combine théorie et pratique pour une application directe dans vos environnements professionnels.

Contenu du cours
Module 1 : Gérer les contrôles de sécurité pour l'identité et l'accès

- Benchmark de sécurité cloud Microsoft : Gestion des identités et accès privilégié
- Qu'est-ce que l'ID Microsoft Entra ?
- Sécuriser les utilisateurs de Microsoft Entra
- Créer un utilisateur dans l'ID Microsoft Entra
- Sécuriser les groupes Microsoft Entra
- Recommander quand utiliser des identités externes
- Sécuriser les identités externes
- Implémenter Microsoft Entra Identity Protection
- Microsoft Entra Connect
- Microsoft Entra Cloud Sync
- Options d'authentification
- Synchronisation de hachage de mot de passe avec l'ID Microsoft Entra
- Authentification directe Microsoft Entra
- Fédération avec Microsoft Entra ID
- Qu'est-ce que l'authentification Microsoft Entra ?
- Implémenter l'authentification multifacteur (MFA)
- Authentification Kerberos
- Gestionnaire réseau local de la nouvelle technologie (NTLM)
- Options d'authentification sans mot de passe pour l'ID Microsoft Entra
- Implémenter l'authentification sans mot de passe
- Implémenter la protection par mot de passe
- Authentification unique Microsoft Entra ID
- Implémenter l'authentification unique (SSO)
- Intégrer l'authentification unique (SSO) et les fournisseurs d'identité
- Présentation de l'ID vérifié Microsoft Entra
- Configurer l'ID vérifié Microsoft Entra
- Recommander et appliquer des protocoles d'authentification modernes

- Groupes d'administration Azure
- Configurer des autorisations de rôle Azure pour les groupes d'administration, les abonnements, les groupes de ressources et les ressources
- Contrôle d'accès en fonction du rôle Azure
- Rôles intégrés Azure
- Attribuer des autorisations de rôle Azure pour les groupes d'administration, les abonnements, les groupes de ressources et les ressources
- Rôles intégrés Microsoft Entra
- Attribuer des rôles intégrés dans l'ID Microsoft Entra
- Contrôle d'accès en fonction du rôle Microsoft Entra
- Créer et attribuer un rôle personnalisé dans Microsoft Entra ID
- Sécurité confiance zéro
- Microsoft Entra Privileged Identity Management
- Configurer Privileged Identity Management
- Gouvernance des ID Microsoft Entra
- Gestion du cycle de vie des identités
- Flux de travail de cycle de vie
- Gestion des droits d'utilisation
- Délégation et rôles dans la gestion des droits d'utilisation
- Révisions d'accès
- Configurer la gestion des rôles et les révisions d'accès à l'aide de la gouvernance des ID Microsoft Entra
- Implémenter des stratégies d'accès conditionnel pour les ressources cloud dans Azure
- Vue d'ensemble d'Azure Lighthouse

Module 2 : Gérer l'accès aux applications Microsoft Entra

- Gérer l'accès aux applications d'entreprise dans l'ID Microsoft Entra, y compris les octrois d'autorisations OAuth
- Gérer les inscriptions d'applications dans Microsoft Entra ID
- Configurer les étendues des autorisations d'inscription d'une application
- Gérer le consentement de l'autorisation d'inscription d'application
- Gérer et utiliser des entités de service
- Gérer les identités managées pour les ressources Azure
- Recommander quand utiliser et configurer un proxy d'application Microsoft Entra, y compris l'authentification

Module 3 : Planifier et implémenter la sécurité pour les réseaux virtuels

- Benchmark microsoft Cloud Security : Protection des données, journalisation et détection des menaces et sécurité réseau
- Qu'est-ce qu'un réseau virtuel Azure ?
- Azure Virtual Network Manager
- Planifier et implémenter des groupes de sécurité réseau (NSG) et des groupes de sécurité d'application (ASG)
- Planifier et implémenter des itinéraires User-Defined (UDR)
- Planifiez, puis implémentez l'appairage de réseaux virtuels ou une passerelle de réseau virtuel
- Planifier et implémenter un réseau étendu virtuel, y compris un hub virtuel sécurisé
- Connectivité VPN sécurisée, notamment point à site et site à site
- Chiffrement Azure
- Qu'est-ce que le chiffrement de réseau virtuel Azure ?
- Azure ExpressRoute
- Implémenter le chiffrement sur ExpressRoute

- Configurer les paramètres de pare-feu sur des ressources Azure
- Superviser la sécurité réseau en utilisant Network Watcher

Module 4 : Planifier et implémenter la sécurité pour l'accès privé aux ressources Azure

- Planifier et implémenter des points de terminaison de service de réseau virtuel
- Planifier et implémenter des points de terminaison privés
- Planifier et implémenter des services Private Link
- Planifier et implémenter l'intégration réseau pour Azure App Service et Azure Functions
- Planifier et implémenter des configurations de sécurité réseau pour App Service Environment (ASE)
- Planifier et implémenter des configurations de sécurité réseau pour une instance Azure SQL Managed Instance

Module 5 : Planifier et implémenter la sécurité pour l'accès public aux ressources Azure

- Planifier et implémenter le protocole TLS (Transport Layer Security) aux applications, notamment Azure App Service et Gestion des API
- Planifier, implémenter et gérer un pare-feu Azure, Azure Firewall Manager et des stratégies de pare-feu
- Planifier et implémenter une passerelle d'application Azure
- Planifier et implémenter un pare-feu d'applications web
- Planifier et implémenter une porte d'entrée Azure, y compris le réseau de distribution de contenu (CDN)
- Recommander quand utiliser Azure DDoS Protection Standard

Module 6 : Planifier et implémenter une sécurité avancée pour le calcul

- Planifier et implémenter l'accès à distance aux points de terminaison publics, Azure Bastion et l'accès juste-à-temps (JIT) à des machines virtuelles
- Qu'est-ce qu'Azure Kubernetes Service ?
- Configurer l'isolation réseau pour Azure Kubernetes Service (AKS)
- Sécuriser et surveiller Azure Kubernetes Service
- Configurer l'authentification pour Azure Kubernetes Service
- Configurer la sécurité des Azure Container Instances (ACI)
- Configurer la sécurité pour Azure Container Apps (ACA)
- Gérer l'accès à Azure Container Registry (ACR)
- Configurer le chiffrement de disque, Azure Disk Encryption (ADE), le chiffrement en tant qu'hôte et le chiffrement de disque confidentiel
- Recommander des configurations de sécurité pour Gestion des API Azure

Module 7 : Planifier et implémenter la sécurité pour le stockage

- Azure Storage
- Configurer le contrôle d'accès pour les comptes de stockage
- Gérer le cycle de vie pour les clés d'accès du compte de stockage
- Sélectionner et configurer une méthode appropriée pour l'accès à Azure Files
- Sélectionner et configurer une méthode appropriée pour accéder à Azure Blobs
- Sélectionner et configurer une méthode appropriée pour accéder à Tables Azure
- Sélectionner et configurer une méthode appropriée pour l'accès aux files d'attente Azure
- Sélectionner et configurer les méthodes appropriées pour la protection contre les menaces de sécuritédes données, y compris la suppression réversible, les sauvegardes, le contrôle de version et le stockage immuable
- Configurer Apportez votre propre clé (BYOK)
- Activer le double chiffrement au niveau de l'infrastructure stockage Azure

Module 8 : Planifier et implémenter la sécurité pour Azure SQL Database et Azure SQL Managed Instance

- Sécurité pour Azure SQL Database et SQL Managed Instance
- Activer l'authentification de base de données Microsoft Entra
- Activer et superviser l'audit de base de données
- Identifier les cas d'usage pour le portail de gouvernance Microsoft Purview
- Implémenter la classification des données des informations sensibles en utilisant le portail de gouvernance Microsoft Purview
- Planifier et implémenter un masque dynamique
- Implémenter le chiffrement transparent des données
- Recommander quand utiliser Azure SQL Database Always Encrypted
- Implémenter un pare-feu Azure SQL Database

Module 9 : Implémenter et gérer l'application des stratégies de gouvernance cloud

- Benchmark de sécurité du cloud Microsoft : accès, données, identité, réseau, point de terminaison, gouvernance, récupération, incident et gestion des vulnérabilités
- Gouvernance Azure
- Créer, affecter et interpréter des stratégies et des initiatives de sécurité dans Azure Policy
- Déployer des infrastructures sécurisées à l'aide d'une zone d'atterrissage
- Azure Key Vault
- Sécurité d'Azure Key Vault
- Authentification Azure Key Vault
- Créer et configurer un coffre de clés Azure
- Recommander quand utiliser un module de sécurité matériel dédié (HSM)
- Configurer l'accès à Key Vault, y compris les stratégies d'accès au coffre et le contrôle d'accès en fonction du rôle Azure
- Gérer des certificats, des secrets et des clés
- Configurer la rotation des clés
- Configurer la sauvegarde et la récupération des certificats, des secrets et des clés
- Mettre en œuvre des contrôles de sécurité pour protéger les sauvegardes
- Implémenter des contrôles de sécurité pour la gestion des ressources

Module 10 : Gérer la posture de sécurité à l'aide de Microsoft Defender pour cloud

- Implémenter Microsoft Defender pour le cloud
- Identifier et corriger les risques de sécurité en utilisant le niveau de sécurité et l'inventaire de Microsoft Defender pour le cloud

- Évaluer la conformité relativement aux infrastructures de sécurité et à Microsoft Defender pour le cloud
- Ajouter des normes sectorielles et réglementaires à Microsoft Defender pour le cloud
- Ajouter des initiatives personnalisées à Microsoft Defender pour le cloud
- Connecter des environnements cloud hybrides et multiclouds à Microsoft Defender pour cloud
- Implémenter et utiliser Microsoft Defender External Attack Surface Management

Module 11 : Configurer et gérer la protection contre les menaces à l'aide de Microsoft Defender pour cloud

- Activer les services de protection de charge de travail dans Microsoft Defender pour le cloud
- Defender pour serveurs
- Defender pour le stockage
- Analyse des programmes malveillants dans Defender pour le stockage
- Détecter les menaces pour les données sensibles
- Déployer Microsoft Defender pour le stockage
- Activer la configuration d'une stratégie intégrée Azure
- Configurer les plans Microsoft Defender pour les serveurs, les bases de données et le stockage
- Implémenter et gérer microsoft Defender Vulnerability Management
- Espace de travail Log Analytics
- Gérer la conservation des données dans un espace de travail Log Analytics
- Déployer l'agent Azure Monitor
- Collecter des données avec l'agent Azure Monitor
- Règles de collecte de données (DCR) dans Azure Monitor
- Transformations dans les règles de collecte de données (DCR)
- Surveiller les événements de sécurité réseau et les données de performances en configurant des règles de collecte de données (DCR) dans Azure Monitor
- Connectez vos abonnements Azure
- Accès juste-à-temps aux machines
- Activer l'accès juste-à-temps
- Sécurité des conteneurs dans Microsoft Defender pour les conteneurs
- Facteurs de menace Kubernetes managés
- Architecture Defender pour les conteneurs
- Configurez les composants de Microsoft Defender pour les conteneurs
- Microsoft Defender pour la Sécurité DevOps du Cloud
- Support et conditions préalables de la sécurité DevOps
- Posture de sécurité de l'environnement DevOps
- Connecter votre environnement lab GitHub à Microsoft Defender pour le cloud
- Configurer l'action GitHub Microsoft Security DevOps
- Protection contre les menaces par IA de Defender pour Cloud
- Activer la protection contre les menaces pour les charges de travail IA dans Defender for Cloud
- Obtenez le contexte de l'application et de l'utilisateur final pour les alertes d'intelligence artificielle.

Module 12 : Configurer et gérer des solutions de supervision et d'automatisation de la sécurité

- Gérer les alertes de sécurité et y répondre dans Microsoft Defender pour le cloud
- Configurer l'automatisation des workflows en utilisant Microsoft Defender pour le cloud
- Plans de rétention des journaux dans Microsoft Sentinel
- Alertes et incidents émis par Microsoft Sentinel
- Configurer des connecteurs de données dans Microsoft Sentinel
- Activer le règles analytiques dans Microsoft Sentinel
- Configurer l'automatisation dans Microsoft Sentinel
- Automatisation de la réponse aux menaces avec Microsoft Sentinel

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.

Examen

- Ce cours prépare à la certification AZ-500: Associé Ingénieur en Sécurité Azure.

Profils des participants

- Ingénieurs de sécurité Azure
- Ingénieurs qui souhaitent se spécialiser dans la prestation de sécurité pour les plateformes numériques basées sur Azure
- Ingénieurs et administrateurs sécurité
- Responsables infrastructure cloud
- Architectes solutions Azure
- Administrateurs systèmes et réseaux
- Professionnels IT en transition vers le cloud
- Consultants en cybersécurité

Connaissances Préalables

- Avoir suivi la formation suivante Microsoft Azure Administrator (AZ-104) ou expérience équivalente

Objectifs

- Gérer les contrôles de sécurité pour l'identité et l'accès dans Microsoft Entra ID
- Configurer l'accès sécurisé aux applications d'entreprise et gérer les autorisations
- Protéger les accès publics avec Azure Firewall et Application Gateway
- Sécuriser les ressources de calcul et les environnements containerisés
- Configurer le chiffrement et les contrôles d'accès pour le stockage Azure
- Appliquer les stratégies de gouvernance cloud avec Azure Policy et Key Vault
- Gérer la détection des menaces avec Microsoft Defender pour cloud

Description
Formation pour sécuriser les ressources cloud avec les technologies de sécurité Microsoft (AZ-500)
Niveau
Intermédiaire
Prix de l'inscription en Présentiel (CHF)
3200
Prix de l'inscription en Virtuel (CHF)
3000
Durée (Nombre de Jours)
4
Reference
AZ-500T00