Technologies de sécurité Microsoft Azure (AZ-500T00)

Durée: 4 jours
Public cible: Professionnel TI

À qui s'adresse cette formation ?

Les étudiants doivent avoir au moins un an d''expérience pratique de la sécurisation des charges de travail Azure et une expérience des contrôles de sécurité pour les charges de travail sur Azure.

Objectifs de la formation

- Décrire les classifications de données spécialisées sur Azure
- Identifier les mécanismes de protection des données Azure
- Utiliser des méthodes de chiffrement de données Azure
- Protocoles Internet sécurisés et comment les intégrer sur Azure
- Décrire les services et les fonctionnalités de sécurité Azure

Description sommaire

Dans ce cours, les étudiants acquerront les connaissances et les compétences nécessaires pour mettre en œuvre des contrôles de sécurité, maintenir la posture de sécurité et identifier et corriger les vulnérabilités à l''aide de divers outils de sécurité. Le cours couvre les scripts et l''automatisation, la virtualisation et l''architecture cloud N-tier.

Contenu du plan de cours

Parcours d''apprentissage 1 : Sécuriser l''identité et l''accès

- Gérer les contrôles de sécurité pour l''identité et l''accès
- Gérer l''accès aux applications Microsoft Entra

Parcours d''apprentissage 2 : Sécuriser les réseaux

- Planifier et implémenter la sécurité pour les réseaux virtuels
- Planifier et implémenter la sécurité pour l''accès privé aux ressources Azure
-

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

Parcours d''apprentissage 3 : Sécuriser le calcul, le stockage et les bases de données

- Planifier et implémenter une sécurité avancée pour le calcul
- Planifier et implémenter la sécurité pour le stockage
- Planifier et implémenter la sécurité pour Azure SQL Database et Azure SQL Managed Instance

Parcours d''apprentissage 4 : Gérer la sécurité d''Azure avec Microsoft Defender for Cloud et Microsoft Sentinel

- Implémenter et gérer l''application des politiques de gouvernance Cloud
- Gérer la posture de sécurité avec Microsoft Defender for Cloud
- Configurer et gérer la protection contre les menaces avec Microsoft Defender for Cloud
- Configurer et gérer les solutions de surveillance et d''automatisation de la sécurité

Approche et méthode pédagogique

Approche pratique et structurée combinant théorie ciblée et ateliers guidés. Les participants sécurisent progressivement les environnements Azure à l’aide des technologies de sécurité Microsoft Azure à travers des exercices concrets inspirés de scénarios professionnels, favorisant une mise en application immédiate des apprentissages. Ils apprennent à protéger les identités, les données et les ressources, ainsi qu’à mettre en œuvre des contrôles de sécurité et de gouvernance adaptés. Animée par un formateur certifié Microsoft, la formation privilégie l’interactivité et le développement de compétences techniques directement transférables pour renforcer la posture de sécurité des environnements Azure en contexte professionnel.

Prérequis

Avant de suivre ce cours, les étudiants doivent avoir une connaissance de : Administrateur associé Microsoft Azure ou contenu équivalent

Recommandations

-

Bases en administration Azure Connaissance des concepts de cybersécurité (menaces, contrôle d’accès, chiffrement)

- Compréhension des réseaux (IP, pare-feu, segmentation)
- Notions de gestion des identités (Microsoft Entra ID)
- Familiarité avec les ressources Azure (VM, stockage, applications)