Formation **Microsoft Azure Sécurité**

A l'issue de la formation, les apprenants maîtrisent les services et fonctionnalités de sécurité Azure. Ils ont acquis les compétences et connaissances nécessaires pour mettre en œuvre les contrôles de sécurité, maintenir la sécurité d'une organisation et identifier et remédier aux incidents.

Durée
4 jours

Objectifs pédagogiques

- S'approprier les meilleures pratiques pour gérer les identités et les accès sur Azure
- Mettre en œuvre la protection de la plateforme
- Sécuriser les données et applications
- Être en mesure de gérer les opérations de sécurité

Public
Administrateurs systèmes et réseaux, ingénieurs sécurité...

Prérequis
Avoir suivi la formation Microsoft Azure Administration ou disposer des connaissances équivalentes.

Programme de formation

Introduction à la formation Azure Sécurité
Présentation générale de la formation Azure Sécurité
Objectifs pédagogiques
Vue d'ensemble de la sécurité dans le Cloud Azure

Gestion des identités et des accès
Configuration et administration de l'instance Azure Active Directory
Gestion des utilisateurs Azure AD
Déploiement et configuration d'Azure AD Connect
La protection des identités : accès conditionnel, authentification multifacteur, révisions d'accès...
Gestion des identités privilégiées
Stratégie de gouvernance d'entreprise : RBAC et Azure Policy

Protection de la plateforme
Implémenter la sécurité du périmètre : défense en profondeur et zero trust
Fonctionnalités pour la sécurité réseau
Sécurité des appareils, machines virtuelles et autres composants qui exécutent les applications dans Azure
Sécurité des conteneurs : Azure Container Instances, Azure Container Registry et Azure Kubernetes Service (AKS)

Sécurité des données et applications
Azure Key Vault : clés, certificats et secrets
Fonctionnalités de sécurité des applications
Sécurité des fichiers et du stockage Azure
Configurer la sécurité de la base de données SQL

Opérations de sécurité
Utiliser Azure Monitor et Log Analytics pour la surveillance

Microsoft Defender pour le Cloud
Azure Sentinel pour le suivi et la réponse aux incidents de sécurité

Moyens et méthodes pédagogiques

- La formation alterne entre présentations des concepts théoriques et mises en application à travers d'ateliers et exercices pratiques.
- Les participants bénéficient des retours d'expérience terrains du formateur ou de la formatrice
- Un support de cours numérique est fourni aux stagiaires

Modalités d'évaluation

- **En amont de la session de formation**, un questionnaire d'auto-positionnement est remis aux participants, afin qu'ils situent leurs connaissances et compétences déjà acquises par rapport au thème de la formation.

- **En cours de formation**, l'évaluation se fait sous forme d'ateliers, exercices et travaux pratiques de validation, de retour d'observation et/ou de partage d'expérience.

- **En fin de session**, le formateur évalue les compétences et connaissances acquises par les apprenants grâce à un questionnaire reprenant les mêmes éléments que l'auto-positionnement, permettant ainsi une analyse détaillée de leur progression.