

Your Cyber INSURANCE



Plan de formation – AZ500 Les technologies de sécurité en environnement Microsoft Azure : 5 jours

Jours	Module	Contenu
Jour 1	Gestion des Identité et accès	Partie théorique (2 heures) • Concepts de base d'Azure Active Directory (AAD) • Gestion des identités avec Privileged Identity Management (PIM) • Contrôle des accès avec RBAC (Role-Based Access Control) • Sécurisation des abonnements Azure • Introduction à l'identité hybride et synchronisation des répertoires Partie pratique (4 heures) • Mise en œuvre du RBAC et gestion des rôles • Configuration de politiques Azure et verrous Resource Manager • Activation de la MFA et mise en place de l'accès conditionnel • Gestion des identités privilégiées avec PIM • Synchronisation des identités locales avec Azure AD
Jour 2	Protection de la plate-forme Azure	Partie théorique (2 heures) • Principes fondamentaux de la sécurité cloud • Sécurisation des réseaux virtuels • Protection des hôtes et ressources Azure • Sécurisation des abonnements et des services de la plateforme Partie pratique (4 heures) • Configuration de Network Security Groups (NSG) et Application Security Groups (ASG) • Déploiement et configuration du pare-feu Azure • Sécurisation des Azure Container Registry (ACR) et des clusters AKS
Jour 3	Sécurité des données et des applications	Partie théorique (2 heures) • Gestion de la sécurité des données et des infrastructures • Configuration du chiffrement des données au repos • Concepts de sécurité pour le cycle de vie des applications • Sécurisation des secrets et clés via Azure Key Vault Partie pratique (4 heures) • Mise en œuvre de Azure Key Vault pour la gestion des secrets • Sécurisation des Azure SQL Databases et du stockage • Implémentation du chiffrement Always Encrypted • Sécurisation des applications et des endpoints

Your Cyber INSURANCE



Plan de formation – AZ500 Les technologies de sécurité en environnement Microsoft Azure: 5 jours

Jours	Module	Contenu
Jour 4	Opérations de sécurité Azure	Partie théorique (2 heures) • Configuration des services de sécurité Azure • Mise en place de politiques de sécurité avec Azure Security Center • Gestion des alertes de sécurité et remédiation des incidents • Définition des standards de sécurité (security baselines) Partie pratique (4 heures) • Analyse et traitement des alertes de sécurité • Configuration de Azure Monitor pour la supervision des ressources • Introduction à Azure Sentinel pour la détection avancée • Simulation de scénarios de sécurité et remédiation
Jour 5	Cas pratiques et consolidation	Partie théorique (2 heures) • Révision des concepts clés : identité, protection, supervision, données et applications • Bonnes pratiques pour sécuriser une infrastructure Azure complète Partie pratique (4 heures) • Scénarios combinés : RBAC, MFA, PIM, NSG/ASG, ACR/AKS, Key Vault • Mise en œuvre complète d'un environnement sécurisé Azure • Utilisation de Azure Monitor et Azure Sentinel pour la détection et la remédiation • Évaluation pratique des compétences acquises