DAWAN

Plan de la formation

www.dawan.fr

Formation Sécuriser son infrastructure dans Azure

Durée :	3 jours (21 heures)
Tarifs inter-entreprise :	2 475,00 € HT (standard) 1 980,00 € HT (remisé)
Public :	Architectes et administrateurs Azure, ingénieurs systèmes / réseaux, équipes Cloud, RSSI techniques
Pré-requis :	Expérience de base sur Azure (portail, ressources principales, notions de réseau) et en sécurité des SI
Objectifs :	Comprendre l'architecture et les services clés d'Azure sous l'angle de la sécurité - Mettre en œuvre les bonnes pratiques de configuration des identités, réseaux, données et services managés dans Azure - Utiliser les outils natifs de sécurité (Defender for Cloud, Azure Policy, Sentinel…) pour contrôler et superviser l'infrastructure - Construire une architecture Azure durcie adaptée à son organisation
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.
Modalités d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis
Référence :	CYB102774-F

Note de satisfaction des participants:	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Comprendre l'architecture Azure et les principes de sécurité associés

Revoir les concepts clés d'Azure : abonnements, groupes de gestion, ressources, régions
Analyser les modèles de responsabilité partagée spécifiques à Azure
Identifier les services critiques à sécuriser : compute, stockage, bases de données, services PaaS
Découvrir les principaux services de sécurité Azure (Defender, Policy, Sentinel, Key Vault)
Atelier fil rouge : cartographier une infrastructure Azure type et repérer les zones de risque prioritaires

Sécuriser identités et accès dans Azure AD / Entra ID

Configurer les identités et groupes dans Azure AD / Entra ID
Mettre en œuvre les bonnes pratiques d'authentification (MFA, accès conditionnel, SSO)
Appliquer le principe du moindre privilège avec les rôles intégrés et les rôles personnalisés (RBAC)
Surveiller et auditer les connexions et activités d'administration
Atelier fil rouge : définir une stratégie d'accès conditionnel et un modèle RBAC pour un environnement Azure donné

Protéger le réseau et les ressources Azure

Concevoir des architectures réseau sécurisées : VNets, sous-réseaux, NSG, Azure Firewall, Bastion
Utiliser les App Gateway / WAF et Front Door pour protéger les applications exposées

Sécuriser l’accès aux ressources : Private Endpoints, service endpoints, connexions hybrides (VPN, ExpressRoute)
Limiter l’exposition publique des services et mettre en place des contrôles sortants
Atelier fil rouge : proposer un schéma de réseau sécurisé pour une application en production dans Azure

Sécuriser stockage, données et services managés

Protéger les comptes de stockage (chiffrement, accès privés, signatures, configuration niveau container / blob)
Sécuriser les bases de données Azure (SQL, Cosmos DB…) : firewall, authentification, chiffrement, sauvegardes
Utiliser Key Vault pour la gestion des secrets, certificats et clés de chiffrement
Mettre en œuvre les sauvegardes et la résilience (backup, availability sets, zones, scale sets)
Atelier fil rouge : analyser une configuration de stockage / base Azure et proposer des mesures de durcissement

Superviser, auditer et améliorer la posture de sécurité Azure

Utiliser Defender for Cloud pour évaluer la posture de sécurité et corriger les recommandations
Déployer Azure Policy pour appliquer des règles de conformité et bloquer les configurations à risque
Centraliser les logs dans Log Analytics et mettre en place des alertes pertinentes
Découvrir Azure Sentinel pour la corrélation et l’analyse d’incidents
Atelier fil rouge final : construire un mini-plan d’actions Azure Security à partir d’un score de sécurité et d’alertes réelles