Formation AWS – Sécurité & IAM (KMS, conformité)

Informations

Durée : 3 jours (21h.)

Tarif* : Nous consulter

Réf : AWGI

Niveau : Difficile

intra

Mise à jour le 18/12/25

*tarif valable jusqu'au 31/12/2026

Prochaines sessions

Contactez-nous pour connaitre nos futures sessions.

Pré-requis

- Connaissances de base en sécurité informatique
- Notions sur les services AWS fondamentaux (EC2, S3, VPC)
- Avoir suivi la formation AWS Cloud Practitioner Essentials (recommandé)

Objectifs

Objectifs pédagogiques :

- Comprendre le modèle de sécurité AWS et la responsabilité partagée
- Maîtriser la gestion des identités et des accès avec IAM
- Utiliser KMS pour sécuriser et chiffrer les données
- Découvrir les outils de sécurité et conformité AWS (CloudTrail, Config, GuardDuty)
- Appliquer les bonnes pratiques de sécurité dans AWS

Objectifs opérationnels :

- Concevoir, déployer et auditer une infrastructure AWS sécurisée en identifiant les risques liés aux accès, en configurant des politiques IAM robustes, en mettant en œuvre le chiffrement des données avec KMS, et en assurant la surveillance et la conformité via les outils AWS.

Programme

Jour 1 – Fondamentaux de la sécurité AWS

Modèle de responsabilité partagée

Rôle d'AWS vs rôle du client
Impacts sur la gouvernance et la conformité

IAM (Identity & Access Management)

Utilisateurs, groupes et rôles
Politique de moindre privilège (least privilege)
IAM Policies en JSON : structure et bonnes pratiques
MFA (Multi-Factor Authentication)

Sécurisation des accès

Federation (SAML, Active Directory)
Gestion des clés d'accès et rotation
Atelier pratique : créer une organisation IAM avec utilisateurs, rôles et MFA obligatoire

Jour 2 – Chiffrement, gestion des secrets et audit

AWS KMS (Key Management Service)

Concepts : CMK (Customer Master Key), KMS Managed Keys, Customer Managed Keys
Encryption at rest et in transit
Intégration avec S3, EBS, RDS, DynamoDB

AWS Secrets Manager et Parameter Store

Gestion des mots de passe et secrets applicatifs
Rotation automatique des secrets

Audit et traçabilité

AWS CloudTrail : logs d’API et gouvernance
AWS Config : conformité des ressources
Atelier pratique : chiffrer un bucket S3 avec KMS, stocker un mot de passe dans Secrets Manager, auditer les logs CloudTrail

Jour 3 – Sécurité avancée et conformité

Détection et remédiation

Amazon GuardDuty : détection de menaces
AWS Inspector : analyse de vulnérabilités
AWS Security Hub : centralisation de la sécurité

Conformité et certifications

Normes supportées par AWS (ISO, PCI DSS, HIPAA, RGPD)
Outils pour la conformité continue

Cas d’usage

Sécurisation d’une architecture multi-comptes
Mise en conformité RGPD d’un workload AWS
Atelier final : mise en place d’une stratégie complète (IAM + KMS + GuardDuty + CloudTrail) pour une architecture existante