Formation AWS – Sécurité et Gestion des Identités (IAM, KMS, Compliance)

Informations

Durée : 3 jours (21h.)

Tarif* : Nous consulter

Réf : AWSS

Niveau : Difficile

intra

Mise à jour le 16/09/25

*tarif valable jusqu'au 31/12/2025

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 AWS
Introduction à IAM : utilisateurs, groupes, rôles et politiques
Politiques IAM : inline vs managed, JSON policy structure
Atelier : création d’utilisateurs et rôles IAM sécurisés

Jour 2 – Chiffrement et sécurité avancée

Introduction au chiffrement dans AWS
AWS KMS : concepts, clés gérées par AWS vs gérées par le client
Secrets Manager et Parameter Store
Atelier : chiffrer des données avec KMS et gérer des secrets

Jour 3 – Conformité et outils de sécurité

CloudTrail : journalisation et audit des actions utilisateurs
AWS Config : suivi de conformité des ressources
Services de sécurité : GuardDuty, Inspector, Security Hub
Étude de cas : mise en place d’une architecture AWS conforme et sécurisée
Préparation certification Security Specialty (QCM et exemples)