

Sécurité et Gouvernance des Infrastructures AWS

Lien : https://innov-maroc.com/formation/securite-et-gouvernance-des-infrastructures-aws

DURÉE
4 jours (28h)

RÉFÉRENCE
VSC317

CATÉGORIE
Amazon Web Services

INNOV MAROC

OBJECTIFS DE LA FORMATION

À l'issue de cette formation, vous serez capable de :

- Maîtriser la conception, la mise en œuvre et la supervision d’une architecture AWS sécurisée à grande échelle
- Intégrer la gouvernance, la conformité et la sécurité dans la stratégie cloud de l’organisation
- Automatiser la gestion des identités, des accès et de la protection des données sensibles
- Mettre en œuvre des stratégies proactives de détection, de prévention et de réponse aux menaces
- Renforcer la résilience de l’infrastructure AWS à travers les outils de sécurité managés et les bonnes pratiques DevSecOps

POUR QUI ?

- Architectes cloud et responsables sécurité cloud
- Ingénieurs sécurité et ingénieurs DevOps
- Responsables d’infrastructures IT en charge de la conformité et de la gouvernance cloud
- Chefs de projets techniques souhaitant approfondir la maîtrise de la sécurité AWS

INNOV MAROC



Programme détaillé

1 / MODÈLE DE RESPONSABILITÉ PARTAGÉE ET GOUVERNANCE CLOUD

- Comprendre le modèle de responsabilité partagée et ses implications organisationnelles
- Identifier les rôles et responsabilités liés à la sécurité sur AWS
- Mettre en place un cadre de gouvernance cloud (politiques, rôles, conformité)
- Intégrer les exigences réglementaires (RGPD, ISO 27001, etc.) dans les environnements AWS

2 / CONTRÔLE DES ACCÈS ET IDENTITÉS

- Structurer la gestion des utilisateurs, groupes et rôles avec IAM
- Élaborer des politiques IAM complexes et sécurisées
- Définir des frontières de permissions et des politiques conditionnelles
- Sécuriser le compte root, les clés d’accès et activer MFA
- Mise en pratique : création et test de politiques IAM avancées

3 / AUTOMATISATION DE LA CONFORMITÉ ET DES BONNES PRATIQUES

- Utiliser AWS Config et AWS Control Tower pour auditer la conformité
- Mettre en œuvre des règles automatisées de conformité et de remédiation
- Intégrer AWS Trusted Advisor et Security Hub dans une démarche de surveillance proactive
- Mise en pratique : automatisation d’un audit de conformité avec AWS Config Rules

4 / PROTECTION ET CHIFFREMENT DES DONNÉES

- Choisir entre AWS KMS, CloudHSM et Secrets Manager selon les cas d’usage

INNOV MAROC

- Gérer le cycle de vie des clés KMS et les accès associés
- Automatiser le chiffrement des données dans S3, RDS et EBS
- Mise en pratique : intégration de la gestion des secrets dans une application multi-régions

5 / CONTRÔLE DE L'ACCÈS AU RÉSEAU ET AUX RESSOURCES

- Configurer des VPC sécurisés : sous-réseaux publics/privés, ACL, Security Groups
- Implémenter la segmentation réseau et le principe du moindre privilège
- Déployer et configurer AWS Network Firewall et AWS PrivateLink
- Mise en pratique : conception d'un VPC sécurisé multi-couches

6 / PROTECTION À LA PÉRIPHÉRIE ET DÉFENSE CONTRE LES ATTAQUES

- Identifier les menaces externes et les stratégies de mitigation
- Configurer AWS Shield, WAF et Firewall Manager
- Intégrer Amazon CloudFront pour la résilience et la sécurité applicative
- Mise en pratique : configuration d'une protection anti-DDoS et d'un WAF adaptatif

7 / COLLECTE ET ANALYSE DES JOURNAUX

- Comprendre les sources de logs AWS : CloudTrail, VPC Flow Logs, CloudWatch Logs
- Centraliser et analyser les journaux via Amazon OpenSearch et S3
- Définir des métriques et alarmes CloudWatch orientées sécurité
- Mise en pratique : création d'un tableau de bord de surveillance de la sécurité AWS

8 / DÉTECTION DES MENACES ET ANALYSE DES COMPORTEMENTS

- Utiliser Amazon GuardDuty, Detective et Security Hub pour la détection avancée
- Corréler les événements de sécurité et identifier les anomalies comportementales
- Automatiser les alertes et réponses avec AWS EventBridge et Lambda
- Mise en pratique : automatisation d'une alerte de menace avec GuardDuty et Lambda

9 / RÉPONSE ET REMÉDIATION AUX INCIDENTS DE SÉCURITÉ

INNOV MAROC

- Élaborer un plan de réponse à incident spécifique à AWS
- Identifier les rôles et outils nécessaires à la gestion d’incident
- Utiliser AWS Systems Manager et Step Functions pour orchestrer les réponses
- Mise en pratique : simulation d’un scénario d’incident et plan de remédiation automatisé

10 / INTÉGRATION DE LA SÉCURITÉ DANS LES PIPELINES CI/CD

- Incorporer les contrôles de sécurité dans CodePipeline, CodeBuild et CodeDeploy
- Scanner les images de conteneurs avec Amazon ECR et AWS Inspector
- Automatiser les audits de sécurité avant le déploiement
- Mise en pratique : pipeline CI/CD sécurisé pour une application Serverless

11 / SUPERVISION CENTRALISÉE ET REPORTING DE CONFORMITÉ

- Construire un tableau de bord global de sécurité et de conformité
- Agréger les données issues de Security Hub, Config et GuardDuty
- Générer des rapports de conformité automatisés pour l’audit interne
- Mise en pratique : création d’un rapport de conformité multi-comptes AWS

12 / STRATÉGIE DE MATURITÉ SÉCURITÉ CLOUD

- Évaluer la maturité sécurité d’une organisation cloud
- Mettre en place un plan d’amélioration continue de la sécurité AWS
- Intégrer la gouvernance, la supervision et la culture sécurité dans la stratégie DevOps
- Étude de cas : élaboration d’une feuille de route sécurité et gouvernance AWS

INNOV MAROC

Approche pédagogique

- Support Ecrit et Projection
- Exposés Interactifs, Podcasts et Vidéos
- Brainstorming et Jeux de Rôle
- Cas Pratiques et Labs inclus pour leur impact opérationnel
- Test de Validation des Acquis des Connaissances

Prochaines dates programmées

10 au 13 Nov. 2026	Distanciel
05 au 08 Jan. 2027	Présentiel - Casablanca
02 au 05 Mars 2027	Présentiel - Casablanca
27 au 30 Avr. 2027	Présentiel - Casablanca
22 au 25 Juin 2027	Présentiel - Casablanca

Autres dates possibles sur demande. Contactez-nous pour organiser une session intra-entreprise.

Réservation & Renseignements

Téléphone : +212 522 247 210
Email : contact@innov-maroc.com
Web : https//www.innov-maroc.com

INNOV MAROC — Tous droits réservés