Architecture et Sécurité des Infrastructures AWS

Lien : https://innov-systems.com/formation/architecture-et-securite-des-infrastructures-aws

DURÉE	RÉFÉRENCE	CATÉGORIE
4 jours (28h)	**SEC325**	**Sécurité du Cloud**

OBJECTIFS DE LA FORMATION

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

- Comprendre et appliquer les principes d’architecture sécurisée sur AWS selon le modèle de responsabilité partagée
- Concevoir des environnements AWS résilients, chiffrés et conformes aux bonnes pratiques de sécurité
- Mettre en œuvre des contrôles d’accès, de surveillance et de réponse aux incidents automatisés
- Intégrer la sécurité dès la conception dans les pipelines DevOps et les environnements hybrides
- Exploiter les outils AWS pour la détection des menaces, la gestion des identités et la gouvernance des données

POUR QUI ?

- Ingénieurs cloud
- Architectes systèmes ou solutions
- Responsables sécurité des systèmes d’information (RSSI)
- Administrateurs AWS souhaitant renforcer la sécurité de leurs environnements

Innov Systems

Programme détaillé

1 / COMPRENDRE LA SÉCURITÉ AWS

- Modèle de responsabilité partagée AWS
- Cadres de conformité et certifications AWS (ISO, SOC, RGPD, etc.)
- Gestion des risques et approche Zero Trust
- Atelier : Cartographie des responsabilités de sécurité dans un environnement AWS

2 / GESTION DES IDENTITÉS ET DES ACCÈS (IAM)

- Bonnes pratiques IAM et stratégies de moindre privilège
- Politiques, rôles et permissions conditionnelles
- Authentification multi-facteurs et fédération d'identités (SSO, ADFS, Azure AD)
- Atelier : Conception d'une politique IAM sécurisée et audit des permissions

3 / GOUVERNANCE ET CONTRÔLE CENTRALISÉ

- AWS Organizations et contrôle multi-comptes
- AWS Control Tower et Service Catalog
- Application des guardrails et conformité automatique
- Atelier : Mise en place d'une architecture multi-comptes sécurisée

4 / SÉCURISATION DES DONNÉES AU REPOS ET EN TRANSIT

- Chiffrement et gestion des clés avec AWS KMS et CloudHSM
- Protection des données dans Amazon S3, RDS et DynamoDB
- Sauvegarde, archivage et restauration sécurisée (AWS Backup, Glacier)
- Atelier : Mise en œuvre du chiffrement des données et rotation automatique des clés

5 / SÉCURITÉ DES APPLICATIONS ET DES CHARGES DE TRAVAIL

Innov Systems

- Sécurisation des AMI et durcissement des systèmes EC2
- Analyse de vulnérabilités avec AWS Inspector et AWS Systems Manager
- Gestion des configurations et des secrets avec AWS Secrets Manager et Parameter Store
- Atelier : Intégration de la sécurité dans le pipeline CI/CD avec AWS CodePipeline

6 / SÉCURITÉ DES ENVIRONNEMENTS WEB ET SERVEURS D'APPLICATION

- Sécurisation des API avec Amazon API Gateway et AWS Cognito
- Protection contre les attaques OWASP Top 10 avec AWS WAF
- Intégration du CDN sécurisé avec Amazon CloudFront
- Atelier : Configuration d'un pare-feu applicatif et d'une authentification d'API

7 / SÉCURISATION DU RÉSEAU AWS

- Conception sécurisée d'un Amazon VPC (sous-réseaux, ACL, NAT, pare-feux)
- Gestion des accès via VPN, Direct Connect et Transit Gateway
- Protection DDoS avec AWS Shield et AWS Firewall Manager
- Atelier : Création d'une topologie réseau sécurisée avec segmentation et contrôle du trafic

8 / SURVEILLANCE ET DÉTECTION DES MENACES

- Surveillance proactive avec Amazon CloudWatch, Config et Macie
- Analyse des journaux via CloudTrail, Kinesis et Athena
- Détection des anomalies et menaces avec AWS GuardDuty et Detective
- Atelier : Analyse d'un incident de sécurité et réponse automatisée via AWS Lambda

9 / GESTION DES INCIDENTS ET TRAÇABILITÉ

- Architecture de détection et d'alerte
- Processus d'investigation et confinement d'incident
- Conservation des preuves et intégration avec SIEM externes
- Atelier : Simulation d'un incident et mise en place d'un plan de réponse AWS

Inov Systems

10 / AUTOMATISATION DE LA SÉCURITÉ DÈS LA CONCEPTION

- Intégration de la sécurité dans le cycle DevSecOps
- Utilisation d’AWS CloudFormation et CDK pour la conformité automatisée
- Catalogue de services sécurisés et réutilisables
- Atelier : Automatisation du déploiement sécurisé d’une architecture complète AWS

11 / SÉCURITÉ DANS LES ENVIRONNEMENTS HYBRIDES ET SANS SERVEUR

- Sécurité des workloads hybrides (On-Premises / AWS)
- Protection des environnements Lambda et Fargate
- Gestion des accès et journaux dans les architectures hybrides
- Atelier : Déploiement d’un environnement hybride sécurisé avec Direct Connect et VPN

12 / OPTIMISATION ET AUDIT DE LA SÉCURITÉ AWS

- Évaluation continue des bonnes pratiques (AWS Well-Architected Framework – Pilier Sécurité)
- Audit des comptes et revue de conformité automatique
- Plans d’amélioration et documentation de la posture de sécurité
- Atelier : Audit complet d’une infrastructure AWS existante et plan d’optimisation

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

Innov Systems

Prochaines dates programmées

12 au 15 Jan. 2027	Présentiel - Casablanca
09 au 12 Mars 2027	Présentiel - Casablanca
04 au 07 Mai 2027	Présentiel - Casablanca
29 Juin au 02 Juil. 2027	Présentiel - Casablanca
31 Août au 03 Sep. 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-systems.com
Web : https//www.innov-systems.com

Innov Systems — Tous droits réservés

Innov Systems