Ingénierie de sécurité sur AWS

Durée: 3 jours
Public cible: Professionnel TI

À qui s'adresse cette formation ?

- Ingénieurs en sécurité
- Architectes en sécurité
- Opérations de sécurité et informations sur la sécurité

Objectifs de la formation

- Assimiler et tirer parti du modèle de sécurité partagé d'AWS
- Concevoir et intégrer des infrastructures d'application protégées contre les menaces de sécurité les plus courantes
- Protéger les données au repos et en transit par un cryptage
- Appliquer des contrôles et des analyses de sécurité de manière automatisée et reproductible
- Configurer l'authentification de ressources et d'applications dans le cloud AWS
- Recueillir des informations sur les événements en capturant, surveillant, traitant et analysant les journaux
- Identifier et atténuer les menaces entrantes contre les applications et les données
- Effectuer des évaluations de sécurité pour s'assurer que les vulnérabilités courantes sont résolues et que les meilleures pratiques de sécurité sont appliquées

Description sommaire

Ce cours explique comment utiliser efficacement les services de sécurité AWS pour travailler en toute sécurité dans AWS Cloud. Ce cours se concentre sur les pratiques de sécurité recommandées par AWS pour améliorer la sécurité de vos données et systèmes dans le cloud. Ce cours met en lumière les fonctionnalités de sécurité intégrées aux principaux services AWS, notamment les services de calcul, de stockage, de mise en réseau et de base de données. Vous découvrirez également comment tirer parti des services et outils AWS pour automatiser, contrôler et consigner vos activités en continu,

et répondre aux incidents de sécurité. Apprenez à utiliser les pratiques DevOps courantes pour développer, déployer et gérer des applications sur AWS de manière sécurisée.

Contenu du plan de cours

Module 1 : Introduction à la sécurité AWS

- Modèle de responsabilité partagée AWS
- Principes de sécurité dans le cloud • Gouvernance et frameworks de sécurité

Module 2 : Gestion des identités et accès (IAM)

- AWS IAM (utilisateurs, rôles, politiques)
- MFA et meilleures pratiques
- AWS Organizations et contrôle des comptes
- Gestion des accès avec AWS SSO / IAM Identity Center

Module 3 : Protection de l’infrastructure réseau

- Sécurité VPC (subnets, routing)
- Security Groups vs NACL
- AWS Shield et AWS WAF
- AWS Firewall Manager

Module 4 : Protection des données

- Chiffrement au repos et en transit
- AWS KMS et gestion des clés
- AWS CloudHSM
- Gestion des secrets (AWS Secrets, Manager, Parameter Store)

Module 5 : Sécurité des services AWS

- Sécurisation de EC2, S3, RDS, Lambda
- Configuration sécurisée des services
-

Bonnes pratiques d’architecture

Module 6 : Surveillance et journalisation

- AWS CloudTrail (audit)
- Amazon CloudWatch (monitoring)
- AWS Config (conformité)
- Centralisation des logs

Module 7 : Détection des menaces et réponse aux incidents

- Amazon GuardDuty
- AWS Security Hub
- Amazon Inspector
- Playbooks de réponse aux incidents

Module 8 : Automatisation de la sécurité

- Infrastructure-as-Code sécurisée
- Automatisation des contrôles (AWS Config Rules)
- Remédiation automatique

Module 9 : Évaluation et conformité

- Audits de sécurité
- Normes (ISO, PCI-DSS, CIS benchmarks) AWS Artifact

Approche et méthode pédagogique

Cette formation combine des exposés théoriques avec des démonstrations et des laboratoires pratiques permettant d’appliquer immédiatement les concepts de sécurité sur AWS. Les participants travaillent sur des cas réels, analysent des architectures sécurisées et utilisent les services AWS pour configurer, surveiller et automatiser la sécurité. Des échanges interactifs et mises en situation complètent l’apprentissage.

Prérequis

Connaissance de base des services AWS (EC2, S3, VPC, IAM)

Recommandations

- Expérience pratique avec AWS ou formation préalable (ex. AWS Technical Essentials / Architecting on AWS)
- Compréhension des concepts de sécurité TI (réseau, chiffrement, gestion des accès)
- Expérience en administration systèmes ou sécurité peut être un atout