Fiche du cours

Titre :

SEC410 - Cloud & DevSecOps Security

Description :

Ce cours initie les étudiants aux bonnes pratiques de sécurité dans les environnements cloud et les pipelines DevOps. Il couvre la sécurisation des services cloud, en particulier Amazon Web Services, la gestion des identités et des accès, le chiffrement, la segmentation réseau et la sécurisation des workloads. Les participants apprennent aussi à intégrer des contrôles de sécurité dans les pipelines CI/CD, à scanner des images conteneurisées et à renforcer les clusters Kubernetes. L'approche est concrète et orientée vers des scénarios réels de déploiement et de défense.

Objectifs :

- Comprendre les principes de sécurité dans le cloud et DevSecOps.*
- Sécuriser IAM, VPC et les services critiques AWS.*
- Intégrer des contrôles de sécurité dans les pipelines CI/CD.*
- Scanner et renforcer des images Docker et des clusters Kubernetes.*
- Détecter et corriger les failles dans un environnement cloud moderne.

Chapitres :

1. Introduction à la sécurité Cloud et DevSecOps*
2. IAM, KMS et segmentation réseau sécurisée*
3. Sécurité des workloads (EC2, Lambda, conteneurs)*
4. Sécurisation CI/CD : secrets, policies, scanning automatisé*
5. Sécurité des conteneurs (Docker) et clusters Kubernetes (RBAC, NetworkPolicies)*
6. Surveillance et alertes de sécurité cloud (CloudWatch, Config, GuardDuty)*
7. Intégration des contrôles dans les pipelines et reporting automatisé*
8. Étude de cas pratique : sécurisation d'une application déployée sur AWS

À la fin :

Vous serez capable de sécuriser une infrastructure cloud et un pipeline DevSecOps complet, en intégrant des contrôles de sécurité dans les environnements AWS, Docker et Kubernetes. Vous saurez appliquer les bonnes pratiques de segmentation réseau, de gestion des identités, de chiffrement, de détection et de réponse. Ce cours vous préparera aux rôles orientés Cloud Security et DevSecOps.