[sfeir] Institute

SFEIR Institute | CLOUDSECFND

Sécurité Cloud les fondamentaux

Comprendre les enjeux, moyens, techniques et outils pour assurer une protection optimale sur le cloud

7h

Présentation du cours

La formation Cloud Security Fundamentals est une introduction à la sécurité sur le cloud, elle permet aux participants de comprendre et évaluer les nouveaux risques apportés par le cloud afin de les orienter vers une mise en œuvre d'un programme de sécurité cloud adaptée et basée sur les bonnes pratiques.

Objectifs pédagogiques

- Connaître les nouveaux risques apportés par le cloud.
- Connaître les moyens mis en œuvre par les cloud providers pour la sécurité.
- Connaître les premiers chantiers de sécurité à attaquer lors de la migration sur le cloud
- Connaître les pratiques, les techniques et outils pour assurer une protection optimale sur le cloud.

Public cible

Tous publics et métiers intéressés par la sécurité dans le cloud, dont les équipes techniques (développeurs, ingénieurs, architectes, devops,...), les décideurs (CTO, CISO, CxO).

Prérequis

- Des connaissances de base sur le cloud computing sont nécessaires. Avoir des connaissances équivalentes ou avoir suivi la formation Cloud 360°.
- Pas de prérequis techniques.

Programme

Module 1 : Introduction à la sécurité du cloud computing

- Les principes fondamentaux de la sécurité sur le cloud
- Les modèles de déploiement cloud (IaaS, PaaS et SaaS) et le principe de responsabilité partagée.
- Les principales menaces sur le cloud avec des exemples d'incidents réels.

Module 2 : Gestion des identités et contrôle d'accès

- Le rôle de l'IAM dans la protection des environnements cloud.
- Principales attaques contres l'IAM
- Bonnes pratiques pour se protéger contre le vol d'identités cloud et contre les abus de contrôle d'accès.

Module 3 : Sécurité des services IaaS et PaaS

- Les risques liés au IaaS et au PaaS.
- Limitation de la surface d'attaque sur les machines virtuelles et automatisation du hardening et du patching.
- Confidential Computing
- Segmentations et Isolation : les différents mécanismes.

Module 4 : Sécurité de la donnée

- Les risques liés au « Cloud Storage ».
- Chiffrement des données en transit et au repos.
- Prévention de la fuite de données.
- Stratégies de protection contre les ransomwares
- Identification des données sensibles grâce aux outils DLP (Data Loss Protection).

Module 5 : Sécurité des applications

- Emploi des outils de sécurité pour les applications déployées sur le cloud.

- Protéger les applications sur les cloud à l'aide d'outils fournis par les cloud providers : Firewall applicatifs (WAF), solutions anti-DDoS, etc.
- Bonnes pratiques sur la sécurité des applications sur le cloud.

Module 6 : Le SecOps sur le cloud

- Détection des événements de sécurité à l'aide des fonctions de logging et intégration avec les outils SIEM.
- Les solutions de sécurité mises à disposition par les cloud providers.
- Les solutions tierce-partie de maintien de la posture de sécurité cloud (CSPM).