Stratégies de sécurité Cloud

BC04-FM04

Présentation

Compétences associées

C25. Implémenter des stratégies de sécurité robustes dans les environnements cloud en appliquant des politiques de sécurité, utilisant des outils de gestion des identités et des accès, et conduisant des audits de sécurité réguliers pour protéger les infrastructures contre les menaces.

Objectifs

Ce module vise à familiariser les apprenants avec les principaux risques de sécurité associés aux environnements Cloud et les différences avec les infrastructures sur site. Il permet également de maîtriser la gestion des identités, la surveillance des menaces, et les bonnes pratiques pour sécuriser les données et gérer les clés et secrets dans le Cloud. Enfin, ce module aborde les modèles de responsabilité partagée et les normes de sécurité applicables au Cloud.

Prérequis :

Pour suivre ce module, les apprenants devraient avoir :

- des connaissances de base en informatique,
- une compréhension générale des concepts de réseau et de sécurité informatique,
- une familiarité avec les services Cloud.

Liens

Ressources

Introduction

- Sécurité cloud : architecture
- Sécurité On-Premise vs Cloud
- Surface d’attaque en environnement Cloud
- Approche Zero Trust
- Pilier Security du AWS Well-Architected Framework

I- VPC et sécurité réseau

- VPC et architecture

TDs

- TD1 – Conception d’une stratégie IAM sécurisée
- TD2 – Sécurisation réseau AWS (VPC, Security Groups, ALB)
- TD1-b : IAM Central et IAM Projet avec CI/CD
- TD3 – Gestion des secrets, chiffrement et traçabilité AWS
- TD4 – Déploiement d'un backend Spring Boot avec Ansible et GitHub Actions