[sfeir] Institute

AWS | AWSSECESS

AWS Security Essentials

Les concepts fondamentaux de sécurité du cloud AWS

1 jour(s) / 7h

Objectifs pédagogiques

- Identifier les avantages et les responsabilités en matière de sécurité lors de l'utilisation du cloud AWS
- Décrire les fonctionnalités de contrôle et de gestion d'accès d'AWS
- Comprendre les différentes méthodes de chiffrement des données pour sécuriser les données sensibles
- Décrire comment sécuriser l'accès réseau à vos ressources AWS
- Déterminer quels services AWS peuvent être utilisés pour la surveillance et la réponse aux incidents.

Public cible

- Professionnels de l'informatique intéressés par les pratiques de sécurité dans le cloud
- Professionnels de la sécurité avec une connaissance pratique minimale d'AWS

Prérequis

Nous recommandons aux participants de ce cours d'avoir :

- Une connaissance pratique des pratiques de sécurité informatique

- Une connaissance pratique des concepts d'infrastructure ainsi qu'une familiarité avec les concepts et les services cloud AWS

Programme

Module 1 : Explorer le pilier de la sécurité

- Cadre AWS bien architecturé : pilier de la sécurité

Module 2 : Sécurité du Cloud

- Modèle de responsabilité partagée
- Infrastructure mondiale AWS
- Conformité et gouvernance

Module 3 : Gestion des identités et des accès

- Gestion des identités et des accès
- L'essentiel de l'accès et de la protection des données

Mise en pratique : Introduction aux stratégies de sécurité

Module 4 : Protéger l'infrastructure et les données

- Protection de votre infrastructure réseau
- Sécurité Edge
- Atténuation DDoS
- Protéger les ressources de calcul

Mise en pratique : Sécuriser les ressources VPC avec des groupes de sécurité

Module 5 : Détection et réponse

- Contrôles de surveillance et de détection
- L'essentiel de la réponse aux incidents

Module 6 : Synthèse du cours

- Revue du cours