[sfeir] Institute

AWS | AWSSBP

AWS Security Best Practices

Les bonnes pratiques de sécurité du cloud AWS

1 jour(s) / 7h

Objectifs pédagogiques

- Concevoir et mettre en œuvre une infrastructure réseau sécurisée
- Concevoir et mettre en œuvre la sécurité informatique
- Concevoir et mettre en œuvre une solution de journalisation

Public cible

- Architectes de solutions
- Ingénieurs cloud, y compris ingénieurs de sécurité
- Ingénieurs DevOps
- Services professionnels
- Cloud Center of Excellence (CCOE)

Prérequis

Nous recommandons aux participants de ce cours d'avoir suivi une de ces formations :

- AWS Cloud Practitioner Essentials
- AWS Technical Essentials
- AWS Security Essentials

Programme

Module 1 : Présentation de la sécurité AWS

- Modèle de responsabilité partagée
- Défis clients
- Cadres et normes
- Mise en place des bonnes pratiques
- Conformité dans AWS

Module 2 : Sécuriser le réseau

- Flexible et sécurisé
- Sécurité à l'intérieur d'Amazon Virtual Private Cloud (Amazon VPC)
- Services de sécurité
- Solutions de sécurité tierces

Mise en pratique : Contrôler le réseau

Module 3 : Sécurité Amazon EC2

- Durcissement du calcul
- Cryptage Amazon Elastic Block Store (EBS)
- Gestion et maintenance sécurisées
- Détecter les vulnérabilités
- Utilisation d'AWS Marketplace

Mise en pratique : Sécuriser le point de départ (EC2)

Module 4 : Surveillance et alerte

- Journalisation du trafic réseau
- Journalisation du trafic des utilisateurs et de l'interface de programmation d'applications (API)
- Visibilité avec Amazon CloudWatch
- Amélioration de la surveillance et de l'alerte
- Vérification de votre environnement AWS

Mise en pratique : Surveillance de la sécurité