Les essentiels d'AWS - Sécurité

Durée: 1 jour
Public cible: Professionnel TI

À qui s'adresse cette formation ?

- Professionnels de l'informatique intéressés par les pratiques en matière de sécurité dans le Cloud
- Professionnels de la sécurité ayant peu de connaissances pratiques d'AWS

Objectifs de la formation

- Identifier les avantages et les responsabilités en matière de sécurité liés à l'utilisation du Cloud AWS
- Décrire les fonctionnalités de gestion et de contrôle des accès intégrées d'AWS
- Comprendre les méthodes de chiffrement des données permettant de protéger les données sensibles
- Expliquer comment sécuriser l'accès réseau à vos ressources AWS

Description sommaire

Les essentiels d'AWS - Sécurité aborde les concepts fondamentaux de sécurité du Cloud AWS, notamment le contrôle d'accès AWS, les méthodes de chiffrement des données et la manière dont l'accès réseau à votre infrastructure AWS peut être sécurisé. Basé sur le modèle de sécurité partagée AWS, ce cours aborde la mise en œuvre de la sécurité sur le Cloud AWS. Vous découvrirez également les services de sécurité disponibles et verrez en quoi et pourquoi ils peuvent vous aider à répondre aux besoins de sécurité de votre entreprise. Ce cours vous permet d'approfondir le sujet, de poser des questions, de trouver des solutions et d'avoir le retour de formateurs accrédités par AWS et disposant de connaissances techniques approfondies. Ce cours de niveau fondamental fait partie du parcours d'apprentissage \AWS Training and Certification Security\.

Contenu du plan de cours

La sécurité sur AWS

- Principes de conception de la sécurité dans le cloud AWS
- Modèle de responsabilité partagée AWS
- Module: Sécurité DU Cloud
- Infrastructure mondiale AWS
- Sécurité du centre de données
- Conformité et gouvernance.

La sécurité dans le Cloud - Partie 1

- Gestion des identités et des accès
- Protection des données
- Travaux pratiques - Introduction aux politiques de sécurité.

La sécurité dans le Cloud - Partie 2

- Sécuriser votre infrastructure
- Surveillance et contrôles de détection
- Travaux pratiques - Sécurisation des ressources VPC avec des groupes de sécurité.

La sécurité dans le Cloud - Partie 3

- Atténuation des attaques par DDoS
- Éléments essentiels de la réponse aux incidents
- Travaux pratiques - Automatisation de la réponse aux incidents avec AWS Config et AWS Lambda.

Récapitulatif du cours

- Présentation de l'outil AWS Well-Architected

Approche et méthode pédagogique

La formation repose sur une approche structurée combinant exposés théoriques, démonstrations et travaux pratiques en environnement AWS. Elle permet aux participant.e.s de mettre en application les concepts de sécurité à travers des laboratoires guidés et des exercices concrets. L'animateur.trice accompagne l'apprentissage en apportant des explications techniques et en répondant aux questions issues des cas pratiques.

Prérequis

Maîtriser les concepts du cloud computing

Recommandations

- Bien connaître les pratiques de sécurité informatique et les concepts d'infrastructure
- Avoir un intérêt pour la cybersécurité et la sécurité infonuagique
- Comprendre les enjeux liés à la protection des données et des accès
- Être impliqué dans des projets TI, cloud ou sécurité
- Avoir des notions générales en gestion des identités ou des accès (atout)
- Expérience en administration systèmes, réseaux ou cloud (atout)