AWS Security Essentials

Date et durée

Code formation : AWS09FR
Durée : 1 jour
Nombre d'heures : 8 heures

Description

La **sécurité sur le cloud AWS** constitue un pilier fondamental pour toute organisation y déployant ses infrastructures. Elle englobe des concepts essentiels tels que le contrôle d'accès AWS, les méthodes de chiffrement des données et la sécurisation de l'accès réseau à l'infrastructure. Le **modèle de responsabilité partagée** d'AWS clarifie les rôles en matière d'implémentation de la sécurité, en identifiant les services dédiés à disposition pour répondre aux besoins de votre organisation.
Cette **formation d'une journée de niveau fondamental** s'adresse notamment aux professionnels de la sécurité informatique qui découvrent les services cloud d'AWS. Grâce à des présentations et des travaux pratiques, vous découvrirez le pilier sécurité du framework AWS Well-Architected ainsi que les spécificités de la sécurité dans le cloud. Le programme traite en outre de la gestion des identités et des accès, de la **protection de l'infrastructure et des données**, ainsi que des mécanismes de détection et de réponse aux incidents.
À l'issue de ce cours, vous développerez une **compréhension solide des mesures de sécurité AWS**. Vous serez capable d'identifier les avantages et les responsabilités de la sécurité dans le cloud AWS, et de mettre en œuvre des **bonnes pratiques de sécurisation** pour vos ressources.

Objectifs

À l'issue de cette formation sur la sécurité AWS, vous atteindrez les objectifs de compétences suivants :

- comprendre les responsabilités et les bénéfices inhérents à la sécurité dans l'environnement Cloud AWS ;
- détailler les mécanismes de gestion d'identité et de contrôle d'accès spécifiques à AWS ;
- exposer les différentes approches pour le chiffrement des données, qu'elles soient au repos ou en transit ;
- sécuriser efficacement l'accès réseau vers les ressources déployées sur AWS ;
- sélectionner les services AWS adaptés au monitoring et à la gestion des incidents de sécurité.

Points forts

- **Expertise du formateur** : énéficiez de l'expertise de formateurs AWS qui possèdent une connaissance approfondie des concepts de sécurité, des méthodes de chiffrement et des bonnes pratiques de sécurisation d'infrastructure sur AWS.
- **Mise en pratique interactive** : maîtrisez les concepts fondamentaux de la sécurité AWS grâce à des présentations claires et des ateliers pratiques concrets. Vous serez ainsi préparé à comprendre et appliquer les principes de contrôle d'accès, de protection des données et de sécurisation réseau.
- **Acquisition de compétences clés** : le contenu de la formation est soigneusement conçu pour vous permettre d'acquérir les compétences essentielles en matière d'identification des bénéfices et responsabilités de la sécurité AWS, de description des fonctionnalités de gestion d'accès, et de détermination des services AWS pour la surveillance et la réponse aux incidents.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre cette formation nécessite les prérequis suivants :

- **Pratiques de sécurité IT** : avoir une familiarité avec les méthodes et principes courants de la sécurité informatique.
- **Concepts d'infrastructure IT** : posséder une connaissance des bases de l'infrastructure des technologies de l'information.
- **Notions de cloud computing** : étre familiarisé avec les concepts fondamentaux du cloud computing.

Public

Cette formation s'adresse aux publics suivants :

- Les **professionnels IT de la sécurité** qui souhaitent s'initier aux pratiques de sécurité spécifiques au cloud AWS.
- Les **experts en sécurité** qui possèdent peu ou pas d'expérience pratique avec l'environnement AWS.

Programme

Module 1 : explorer le pilier sécurité

- Présentation générale des principes de sécurité définis dans le framework AWS Well-Architected.

Module 2 : comprendre la sécurité du cloud

- Le fonctionnement du modèle de responsabilité partagée d'AWS.
- L'identification des éléments clés de l'infrastructure globale d'AWS.
- La compréhension des aspects de conformité et de gouvernance dans le cloud.

Module 3 : gérer l'identité et l'accès

- La gestion de l'identité et des accès dans AWS.
- La maîtrise des principes fondamentaux de l'accès et de la protection des données.

Travaux pratiques :

- S'initier à la création et l'application des politiques de sécurité.

Module 4 : protéger l'infrastructure et les données

- Les éléments à mettre en place pour sécuriser son infrastructure réseau.
- Le fonctionnement de la méthode de sécurité en périphérie (Edge Security).
- La mise en place de stratégies d'atténuation des attaques par déni de service distribué (DDoS).
- La mise en place de protection efficace pour les ressources de calcul.

Travaux pratiques :

- Sécuriser des ressources de Virtual Private Cloud (VPC) à l'aide de groupes de sécurité.

Module 5 : détecter et réagir aux Incidents

- La mise en place d'outils de surveillance et de contrôles de détection.
- Les principes essentiels de la réponse aux incidents.

Module 8 : conclure la formation

- Révision sur les points clés du cours.
- Présentation des niveaux de certification AWS.