L'ingénierie de sécurité sur AWS

Date et durée

Code formation : AWS16FR
Durée : 3 jours
Nombre d'heures : 21 heures

Description

La sécurité est une source de préoccupation majeure pour les entreprises qui adoptent le cloud, et encore plus avec l'augmentation constante des cyber-attaques et des fuites de données. Cette **formation Security Engineering on AWS** vise à aborder ce sujet en vous donnant une meilleure compréhension de la façon d'interagir et de construire des architectures sécurisées avec Amazon Web Services (AWS).
Le programme se déroule sur 3 jours et intègre des travaux pratiques et des démonstrations pour une approche complète et immersive. Il aborde en profondeur la **protection des données stockées sur AWS**, y compris le chiffrement et les contrôles d'accès. De plus, il vous permettra d'apprendre à générer, collecter et surveiller des logs afin d'identifier rapidement les incidents de sécurité et de **répondre efficacement aux menaces**.
À travers ce cours, vous acquerrez une solide compréhension de **la sécurité dans le cloud AWS**, basée sur la triade CIA (Confidentialité, Intégrité, Disponibilité). Vous saurez créer et analyser des mécanismes d'authentification et d'autorisation avec IAM, gérer les secrets et **protéger vos infrastructures contre les attaques externes**.

Objectifs

À l'issue de cette formation en ingénierie AWS, vous atteindrez les objectifs de compétences suivants :

- expliquer les principes de la sécurité du cloud AWS en se basant sur le triptyque de la CIA (Confidentialité, Intégrité, Disponibilité) ;
- concevoir et analyser les mécanismes d'authentification et d'autorisation avec IAM ;
- gérer et provisionner des comptes de manière sécurisée avec les services AWS appropriés ;
- protéger les données sensibles grâce au chiffrement et à des contrôles d'accès stricts ;
- mettre en place la surveillance, la génération et la collecte de journaux d'événements pour identifier les incidents ;
- détecter, investiguer et répondre efficacement aux incidents de sécurité à l'aide des outils AWS.

Points forts

- **Expertise du formateur** : bénéficiez de l'expertise de formateurs AWS spécialisés en sécurité, qui possèdent une connaissance approfondie des architectures sécurisées, des méthodes de chiffrement avancées et des bonnes pratiques d'ingénierie de la sécurité sur AWS.
- **Mise en pratique interactive** : maîtrisez les concepts complexes de l'ingénierie de la sécurité AWS grâce à des présentations claires et des labs pratiques, vous préparant ainsi à appliquer concrètement les principes de protection de l'infrastructure et de réponse aux incidents.

- **Acquisition de compétences clés** : le contenu de la formation est soigneusement conçu pour vous permettre d'acquérir les compétences essentielles en matière de gestion des identités et des accès, de protection des données sensibles, de surveillance proactive et de réponse efficace aux menaces au sein de l'environnement AWS.

Modalités d'évaluation

Travaux Pratiques

Pré-requis

Suivre cette formation AWS nécessite les prérequis recommandés suivants :

- Avoir des connaissances de base sur les services AWS (formation conseillée : AWS Security Essentials).
- Avoir des connaissances de base en conception et architecture sur AWS (formation conseillée : Architecting on AWS).
- Avoir des connaissances sur les pratiques de sécurité informatique et sur les concepts d'infrastructure.

Public

Cette formation s'adresse aux publics suivants :

- Les **ingénieurs en sécurité** qui souhaitent renforcer leurs compétences dans la mise en œuvre et la gestion des mesures de sécurité spécifiques à l'environnement AWS.
- Les **architectes de sécurité** qui désirent de concevoir des architectures cloud robustes et sécurisées sur AWS.
- Les **architectes cloud** qui cherchent à intégrer les meilleures pratiques de sécurité dès la conception de leurs infrastructures AWS.
- Les **opérateurs cloud** responsables des opérations de maintenance sécurisée des services et des infrastructures AWS.

Programme

Module 1 : comprendre et explorer la sécurité

- Le fonctionnement de la sécurité dans le cloud AWS.
- Le modèle de responsabilité partagée d'AWS.
- Les fondamentaux de l'IAM, de la protection des données, de la détection et de la réponse aux menaces.
- Les différentes manières d'interagir avec AWS (console, CLI et SDK).
- L'utilisation de l'authentification à facteurs multiples (MFA) pour une protection supplémentaire.
- La protection du compte utilisateur racine et des clés d'accès.

Module 2 : sécuriser les points d'entrée sur AWS

- Les politiques IAM, des rôles, des composants de politique et des limites de permissions.
- La manière dont les requêtes API peuvent être journalisées et visualisées avec AWS CloudTrail, et comment consulter et analyser l'historique d'accès.

Travaux pratiques

- Utiliser des politiques basées sur l'identité et les ressources.

Module 3 : gérer et provisionner les comptes sur AWS

- La gestion de plusieurs comptes AWS avec AWS Organizations et AWS Control Tower.
- La capacité à utiliser des fournisseurs et courtiers d'identité pour accéder aux services AWS (*démo*).
- L'utilisation d'AWS IAM Identity Center (successeur d'AWS Single Sign-On) et d'AWS Directory Service.
- La capacité à gérer l'accès des utilisateurs de domaine avec Directory Service et IAM Identity Center (*démo*).

Travaux pratiques

- Gérer des accès utilisateurs de domaine avec AWS Directory Service.

Module 4 : gérer les secrets sur AWS

- Les fonctionnalités d'AWS KMS, CloudHSM, AWS Certificate Manager (ACM) et AWS Secrets Manager.
- La création d'une clé AWS KMS multi-régions (*démo*).
- Le chiffrement d'un secret Secrets Manager avec une clé AWS KMS (*démo*).
- L'utilisation d'un secret chiffré pour se connecter à une base de données Amazon Relational Database Service (Amazon RDS) dans plusieurs régions AWS (*démo*).

Travaux pratiques

- Utiliser AWS KMS pour chiffrer des secrets dans Secrets Manager.

Module 5 : protéger les données

- La surveillance des données pour détecter les informations sensibles avec Amazon Macie.
- La description de la protection des données au repos par le chiffrement et les contrôles d'accès.
- L'identification des services AWS utilisés pour répliquer les données à des fins de protection.
- La détermination de la protection des données après leur archivage.

Travaux pratiques

- Sécurisé des données dans Amazon S3.

Module 6 : protéger l'infrastructure Edge

- Les fonctionnalités AWS utilisées pour construire une infrastructure sécurisée.
- L'identification des services AWS utilisés pour créer de la résilience pendant une attaque.
- L'identification des services AWS utilisés pour protéger les charges de travail contre les menaces externes.
- La comparaison des fonctionnalités d'AWS Shield et d'AWS Shield Advanced.
- La manière dont le déploiement centralisé d'AWS Firewall Manager peut améliorer la sécurité.

Travaux pratiques :

- Utiliser AWS WAF pour atténuer le trafic malveillant.

Module 7 : surveiller et collecter les journaux sur AWS

- L'identification de la valeur de la génération et de la collecte de journaux.
- L'utilisation des journaux de flux Amazon Virtual Private Cloud (Amazon VPC) pour surveiller les événements de sécurité.
- La surveillance des écarts par rapport à la ligne de base.
- La gestion des événements dans Amazon EventBridge.
- La gestion des métriques et des alarmes dans Amazon CloudWatch.

- La liste des options et des techniques d'analyse de journaux disponibles.
- L'identification des cas d'utilisation du trafic VPC Mirroring.

Travaux pratiques

- Surveiller et répondre à des incidents de sécurité.

Module 8 : répondre aux menaces

- La classification des types d'incidents dans la réponse aux incidents.
- Les flux de travail de réponse aux incidents.
- La découverte des sources d'informations pour la réponse aux incidents à l'aide des services AWS.
- Les méthodes pour se préparer aux incidents.
- La détection des menaces à l'aide des services AWS.
- L'analyse et la réponse aux découvertes de sécurité.

Travaux pratiques

- Mener une réponse aux incidents.