Ingénierie de sécurité sur AWS

Prix : 2 390 €HT

Durée : 3 jours

Code de Référence : AWSECU

Catalogue Architecture AWS

4,58/5 Satisfaction globale - Moyenne des 24 derniers mois

Dans cette formation Ingénierie de Sécurité AWS, vous apprendrez à utiliser les services AWS pour être protégé efficacement et en toute conformité dans le Cloud Amazon. La formation se concentre sur les meilleures pratiques recommandées par AWS pour améliorer la sécurité de vos données et de vos systèmes hébergés dans le Cloud, que cela concerne les services de calcul, de stockage, de réseau ou de base de données. Cette formation AWS porte également sur les objectifs communs en matière de contrôle de la sécurité et des normes de conformité telles que les authentifications, les autorisations ou bien encore le chiffrement.

Elle permet de préparer la **certification AWS Certified Security – Specialty.**

Objectifs de la formation

A l'issue de cette formation AWS, vous serez capable de :

- Expliquer la sécurité du cloud AWS en s'appuyant sur le modèle CIA
- Créer et analyser des authentifications et des autorisations avec IAM
- Gérer et approvisionner des comptes sur AWS avec les services AWS appropriés
- Identifier comment gérer les secrets à l'aide des services AWS
- Surveiller les informations sensibles et protéger les données via le cryptage et les contrôles d'accès
- Identifier les services AWS qui répondent aux attaques provenant de sources externes
- Surveiller, générer et collecter les logs
- Identifier les indicateurs d'incidents de sécurité
- Identifier comment enquêter sur les menaces et les atténuer à l'aide des services AWS

Public

Cette formation Sécurité sur AWS s'adresse aux responsables sécurité, ingénieurs et architectes, auditeurs, personne en charge de la gouvernance, du contrôle et des tests de l'infrastructure informatique de l'organisation, et devant garantir de celle-ci en termes de sécurité, d'évaluation du risque, et de conformité aux normes

Prérequis

Il est recommandé d'avoir suivi la formation Architecture AWS ou de disposer de connaissances et compétences équivalentes. Il est également recommandé de posséder des connaissances des pratiques de sécurité dans le domaine de l'informatique en général et d'avoir de l'expérience en gouvernance, évaluation du risque, en contrôle, et de conformité aux normes. Compréhension de l'anglais et du vocabulaire anglais spécifique IT. Vous souhaitez faire vérifier vos prérequis ? Contactez-nous pour l'organisation d'un entretien téléphonique avec un de nos consultants formateurs.

Certification préparée

La **certification AWS Certified Security Specialty** valide les compétences d'administration sécurité des services cloud Amazon Web Services. Elle atteste que le professionnel peut simplifier le parcours de votre entreprise vers le cloud AWS, protéger les données et les applications et innover en toute confiance.

Programme de la formation

Jour 1

Module 1 : Sécurité sur AWS

- Expliquer la sécurité dans le cloud AWS
- Expliquer AWS Shared Responsibility Model
- Résumer IAM, la protection des données, la détection et réponse aux menaces
- Indiquer les différentes manières d'interagir avec AWS en utilisant la console, le CLI et les SDK
- Décrire comment utiliser l'authentification multi-facteurs (MFA) pour une protection supplémentaire
- Indiquer comment protéger le compte utilisateur root et l'accès

Module 2 : Sécuriser les points d'entrée sur AWS

- Décrire comment utiliser l'authentification multi-facteurs (MFA) pour une protection supplémentaire
- Décrire comment protéger le compte utilisateur root et les clés d'accès
- Décrire les politiques IAM, les rôles, les composants de politiques et les limites de permissions
- Sécuriser les points d'entrée sur AWS : MFA, protection du compte root, clés d'accès et gestion des politiques IAM
- Utiliser AWS CloudTrail pour enregistrer et consulter les demandes API, et analyser l'historique des accès
    - Travaux pratiques : Utilisation des politiques basées sur l'identité et les ressources

Module 3 : Gestion des comptes et provisionnement sur AWS

- Expliquer comment gérer plusieurs comptes AWS en utilisant AWS
- Organizations et AWS Control Tower

- Expliquer comment mettre en place des environnements multi-comptes avec AWS Control Tower
- Démontrer la capacité à utiliser des fournisseurs d'identité et des courtiers pour accéder aux services AWS.
- Expliquer l'utilisation d'AWS IAM Identity Center (successeur d'AWS Single Sign-On) et d'AWS Directory Service
- Démontrer la capacité à gérer l'accès des utilisateurs de domaine avec Directory Service et IAM Identity Center
    - Travaux pratiques : Gestion de l'accès des utilisateurs de domaine avec AWS Directory Service

Jour 2

Module 4 : Gestion des secrets sur AWS

- Décrire et énumérer les fonctionnalités d'AWS KMS, CloudHSM, AWS Certificate Manager (ACM) et AWS Secrets Manager
- Démontrer comment créer une clé AWS KMS multi-régions
- Démontrer comment chiffrer un secret de Secrets Manager avec une clé AWS KMS
- Utiliser un secret chiffré pour se connecter à une base de données Amazon RDS dans plusieurs régions AWS
    - Travaux pratiques : Utilisation d'AWS KMS pour chiffrer les secrets dans Secrets Manager

Module 5 : Sécurité des données

- Surveiller les données pour détecter des informations sensibles avec Amazon Macie
- Expliquer comment protéger les données au repos grâce au chiffrement et aux contrôles d'accès
- Identifier les services AWS utilisés pour répliquer les données à des fins de protection
- Déterminer comment protéger les données une fois archivées
    - Travaux pratiques : Sécurité des données dans Amazon S3.

Module 6 : Protection de l'infrastructure Edge

- Décrire les fonctionnalités AWS utilisées pour construire une infrastructure sécurisée
- Décrire les services AWS utilisés pour créer de la résilience lors d'une attaque
- Identifier les services AWS utilisés pour protéger les charges de travail contre les menaces externes
- Comparer les fonctionnalités d'AWS Shield et d'AWS Shield Advanced
- Expliquer comment le déploiement centralisé via AWS Firewall Manager peut améliorer la sécurité
    - Travaux pratiques : Utilisation d'AWS WAF pour atténuer le trafic malveillant

Jour 3

Module 7 : Surveillance et collecte des logs sur AWS

- Identifier l'importance de générer et de collecter des logs
- Utiliser les logs de flux Amazon Virtual Private Cloud (Amazon VPC) pour surveiller les événements de sécurité
- Expliquer comment surveiller les écarts par rapport à la ligne de base

- Décrire les événements Amazon EventBridge
- Décrire les métriques et les alarmes Amazon CloudWatch
- Lister les options d'analyse des journaux et les techniques disponibles
- Identifier les cas d'utilisation du miroir de trafic dans un cloud privé virtuel (VPC)
    - Travaux pratiques : Surveillance et réponse aux incidents de sécurité

Module 8 : Répondre aux menaces

- Classer les types d'incidents dans la réponse aux incidents
- Comprendre les flux de travail de la réponse aux incidents
- Découvrir les sources d'informations pour la réponse aux incidents en utilisant les services AWS
- Comprendre comment se préparer aux incidents
- Détecter les menaces à l'aide des services AWS
- Analyser et répondre aux résultats de sécurité
    - Travaux pratiques : Réponse aux incidents

Méthodes pédagogiques

Des exercices pratiques et des démonstrations vous permettront de mettre en pratique les notions théoriques présentées. La dernière version du support de cours, en anglais, vous est transmise par voie dématérialisée. Les cours seront disponibles en ligne pendant 730 jours après leur activation et téléchargeables avec Bookshelf application. Pour y accéder, il est nécessaire de créer un compte eVantage sur evantage.gilmoreglobal.com.

Méthodes d'évaluation des acquis

Afin d'évaluer l'acquisition de vos connaissances et compétences, il vous sera envoyé un formulaire d'auto-évaluation, qui sera à compléter en amont et à l'issue de la formation.
Un certificat de réalisation de fin de formation est remis au stagiaire lui permettant de faire valoir le suivi de la formation.

Accompagnement

Vous avez un projet de migration dans le cloud AWS ? Vous souhaitez être accompagné ? Kanopee peut vous aider et vous répondre à toutes vos questions sur toutes les différentes étapes. Contactez-nous !