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

Security Engineering on AWS est une formation de trois jours, en présentiel et animée par un formateur, qui apprend aux professionnels de la sécurité à sécuriser les workloads Amazon Web Services (AWS) dans les six domaines de sécurité AWS : identity and access management, sécurité de l'infrastructure, protection des données, threat detection, incident response et gouvernance. Les participants alternent hands-on labs, démonstrations du formateur et knowledge checks. La progression part des contrôles fondamentaux d'identité et de réseau pour aller jusqu'à la détection, la réponse et la gouvernance à l'échelle de l'organisation. La formation aborde également la protection des applications de generative AI et l'usage sécurisé des outils de productivité GenAI.

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 :

- Concevoir et dépanner des stratégies d'authentification et d'autorisation fondées sur le principe du least privilege, l'attribute-based et le role-based access control, ainsi qu'une gestion centralisée des identités
- Concevoir l'architecture des contrôles de sécurité de l'infrastructure, et les dépanner, pour les services de network edge, les workloads de compute et la segmentation réseau
- Mettre en œuvre des contrôles de protection des données in transit et at rest, notamment le key management, la rotation des secrets et le data masking
- Concevoir des solutions de monitoring, d'alerting et de logging pour détecter les activités anormales au sein d'un compte AWS ou d'une organisation
- Élaborer et exécuter un incident response plan, incluant la capture d'artefacts forensiques, le containment, l'eradication, le recovery et la root-cause analysis
- Gouverner un environnement AWS à grande échelle avec AWS Organizations, AWS Control Tower et les services de conformité
- Mettre en place des protections pour les applications de generative AI et sécuriser l'usage des outils de productivité GenAI

Public

Cette formation Sécurité sur AWS s'adresse aux security engineers, cloud security architects, security operations engineers, DevSecOps engineers, solutions architects spécialisés en sécurité, professionnels IT chargés de sécuriser des workloads AWS.

Prérequis

Il est recommandé d'avoir suivi la formation Architecture AWS ou de disposer de connaissances et compétences équivalentes. Il est également recommandé de de maîtriser les concepts réseau (TCP/IP, DNS et firewalls), d'être familiarisés avec l'AWS Management Console et l'AWS Command Line Interface (AWS CLI). 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 : Vue d'ensemble de la sécurité et Shared Responsibility

- Décrire l'AWS Shared Responsibility Model et son évolution selon le type de service
- Expliquer la superposition des couches de defense-in-depth : identité, edge, réseau, compute et données
- Présenter les six domaines de sécurité AWS et la logique du build, operate et govern flow

Module 2 : Identity and Access Management – Authentification

- Concevoir des solutions d'identité pour l'authentification des humains, des applications et des systèmes avec AWS IAM Identity Center, Amazon Cognito et la fédération
- Configurer des identifiants temporaires avec AWS STS et IAM Roles Anywhere
- Appliquer des stratégies de multi-factor authentication (MFA), notamment le MFA obligatoire pour le compte root et les facteurs phishing-resistant
- Dépanner les échecs d'authentification fédérée à l'aide d'AWS CloudTrail

Hands-on lab 1 : Accès fédéré avec IAM et multi-factor authentication

Module 3 : Identity and Access Management – Autorisation

- Concevoir une autorisation selon le principe du least privilege avec les IAM policies, les permission boundaries et Amazon Verified Permissions
- Analyser les échecs d'autorisation avec IAM Policy Simulator et IAM Access Analyzer
- Corriger les permissions non souhaitées et le problème du confused deputy

Hands-on lab 2 : Least privilege avec ABAC et IAM Access Analyzer

Module 4 : Sécurité de l'infrastructure – Network edge

- Choisir des stratégies de sécurité edge en fonction des menaces anticipées
- Mettre en œuvre une protection edge multicouche avec AWS WAF, AWS Shield et Amazon CloudFront
- Configurer les web ACLs AWS WAF, les managed rule groups et les rate-based rules
- Filtrer le DNS sortant avec Amazon Route 53 Resolver DNS Firewall

Jour 2

Module 5 : Sécurité de l'infrastructure – Compute Workloads

- Durcir les workloads de compute avec des rôles adaptés, EC2 Image Builder et AWS Systems Manager
- Mettre en œuvre la gestion des vulnérabilités avec Amazon Inspector (y compris la code security) et Amazon GuardDuty
- Configurer un accès d'administration sécurisé, sans bastion ni clés SSH, avec AWS Systems Manager Session Manager
- Appliquer des protections pour les applications de generative AI (OWASP Top 10 for LLM Applications) et sécuriser les outils de productivité GenAI

Module 6 : Sécurité de l'infrastructure – Contrôles de sécurité réseau

- Concevoir la segmentation réseau avec les security groups, les network ACLs et AWS Network Firewall
- Mettre en œuvre un accès applicatif zero-trust avec AWS Verified Access et Amazon VPC Lattice
- Identifier les accès réseau non souhaités avec Network Access Analyzer
- Sécuriser la connectivité hybride avec AWS Site-to-Site VPN et AWS Direct Connect (MACsec)

Hands-on lab 3 : Contrôles de sécurité réseau avec AWS WAF et segmentation AWS Network Firewall.

Module 7 : Protection des données – Data in transit

- Imposer le chiffrement des connexions aux ressources avec les ELB security policies et le mutual TLS
- Gérer les certificats TLS avec AWS Certificate Manager (ACM)
- Configurer un accès privé avec AWS PrivateLink et les VPC endpoints
- Configurer le chiffrement in transit entre ressources

Module 8 : Protection des données – Data at rest

- Concevoir le chiffrement at rest avec AWS KMS et AWS CloudHSM, y compris le modèle d'autorisation KMS à trois couches
- Appliquer une architecture de référence de bout en bout pour l'envelope encryption cross-account sur Amazon S3
- Configurer les contrôles d'intégrité et de cycle de vie des données avec Amazon S3 Object Lock et S3 Glacier Vault Lock

- Configurer des sauvegardes résilientes face aux ransomwares avec AWS Backup et le multi-party approval
- Détecter les données sensibles at rest avec Amazon Macie

Hands-on lab 4 : Sécurité des données S3 avec SSE-KMS, application via bucket policy, réplication et Macie

Module 9 : Protection des données – Secrets, identifiants et key material

- Gérer la rotation des secrets avec AWS Secrets Manager, y compris les identifiants gérés par RDS
- Gérer le key material importé vs généré par AWS, ainsi que les external key stores
- Mettre en œuvre le data masking avec la data protection d'Amazon CloudWatch Logs et d'Amazon SNS
- Mettre en œuvre une gestion multi-Region des clés et des certificats avec AWS Private CA

Hands-on lab 5 : Rotation AWS KMS multi-Region, Secrets Manager et data masking

Jour 3

Module 10 : Détection – Solutions de logging

- Identifier les sources de logs selon les besoins, notamment AWS CloudTrail, VPC Flow Logs et les logs réseau
- Configurer l'ingestion centralisée des logs dans un compte de logging dédié et dans Amazon Security Lake
- Analyser et corréler les logs avec CloudWatch Logs Insights, Amazon Athena et Amazon OpenSearch Service

Module 11 : Détection – Monitoring et alerting

- Configurer le monitoring des workloads et l'agrégation des événements dans une organisation multi-comptes
- Agréger les findings avec AWS Security Hub, Security Hub CSPM, Amazon GuardDuty et Amazon Macie
- Créer des métriques, des alertes et des dashboards avec Amazon CloudWatch et AWS Config pour détecter les activités anormales

Hands-on lab 6 : Detection pipeline routing findings to alerts with Amazon EventBridge and Amazon SNS

Module 12 : Détection – Troubleshooting Monitoring and Logging

- Diagnostiquer les problèmes de fonctionnement, de permissions et de configuration dans les pipelines de logging
- Corriger les erreurs de configuration courantes à l'origine de logs manquants

Hands-on lab 7 : Centralized logging pipeline and fixing broken logging.

Module 13 : Incident response

- Concevoir des incident response plans, des runbooks et un accès break-glass

- Configurer les services pour la préparation aux incidents, notamment AWS Security Incident Response et AWS Shield Advanced
- Tester l'efficacité de l'incident response avec des simulations de sécurité (game days) et la simulation d'événements GuardDuty
- Capturer des artefacts forensiques sur une ressource compromise
- Valider les findings pour évaluer le périmètre et l'impact
- Appliquer les procédures de containment, d'eradication et de recovery
- Perform root-cause analysis with Amazon Detective
- Automatiser la réponse initiale à un incident avec Amazon EventBridge et AWS Lambda

Démonstration : Réponse à une compromission avec Amazon Detective

Hands-on lab 8 : Incident response – capturer, isoler, corriger et automatiser

Module 14 : Gouvernance à grande échelle

- Concevoir une gouvernance multi-comptes avec AWS Organizations et AWS Control Tower
- Appliquer les politiques à grande échelle avec les service control policies (SCPs) et les resource control policies (RCPs)
- Évaluer la conformité à grande échelle avec AWS Config, AWS Firewall Manager et l'AWS Well-Architected Tool

Conclusion de la formation

- Synthèse de la formation
- Prochaines étapes et ressources complémentaires

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 ? Kanopée peut vous aider et vous répondre à toutes vos questions sur toutes les différentes étapes. Contactez-nous !