+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 06/02/2026

S'inscrire

Formation Certification AWS Security Specialty

3 jours (21 heures)

Présentation

AWS Certified Security – Specialty est une certification avancée centrée sur la sécurité des environnements AWS.

Elle valide la capacité à concevoir, déployer et exploiter des architectures sécurisées, en maîtrisant la gestion des identités, le chiffrement, la sécurité réseau, la détection des menaces et la réponse aux incidents.

Notre formation vous permettra de maîtriser les bonnes pratiques de sécurité cloud et les services AWS associés : gouvernance multi-comptes, contrôle d'accès avec IAM, gestion des clés via AWS KMS, durcissement réseau VPC, protection applicative avec AWS WAF, ainsi que détection et investigation avec GuardDuty, CloudTrail et AWS Config.

Vous apprendrez à réduire la surface d'attaque, protéger les données sensibles et industrialiser la sécurité sur AWS grâce à des garde-fous organisationnels, des stratégies d'isolation, et des mécanismes d'observabilité et d'audit adaptés aux environnements d'entreprise.

À l'issue de la formation, vous serez en mesure de sécuriser des comptes AWS à grande échelle, de mettre en place une stratégie de chiffrement robuste, d'implémenter une défense en profondeur, et de préparer efficacement l'examen SCS-C02.

Comme toutes nos formations, celle-ci s'appuie sur la dernier référentiel de la certification SCS-C02 d' AWS et privilégie une approche résolument pratique et opérationnelle.

Objectifs

- Comprendre le modèle de responsabilité partagée AWS et les exigences de gouvernance.
- Mettre en œuvre un contrôle d'accès robuste avec IAM et les principes de least privilege.
- Protéger les données par le chiffrement et la gestion des clés avec AWS KMS.
- Sécuriser le réseau AWS avec VPC, Security Groups, NACL et accès privés.

- Détecter, investiguer et auditer avec CloudTrail, AWS Config et GuardDuty.
- Se préparer efficacement à la certification SCS-C02.

Public visé

- Ingénieurs Cloud / DevOps opérant des environnements AWS
- Ingénieurs sécurité / DevSecOps en charge de la sécurisation cloud
- Architectes Cloud / Architectes sécurité
- Administrateurs AWS responsables de la conformité, de l’audit et des accès

Pré-requis

- Bonne connaissance des fondamentaux AWS
- Notions de base en sécurité
- Expérience pratique de l’exploitation d’un environnement cloud recommandée

Programme de formation Certification AWS Certified Security – Specialty (SCS-C02)

[Jour 1 - Matin]

Responsabilité partagée et gouvernance

- Comprendre le modèle de responsabilité partagée AWS et ses impacts opérationnels
- Appliquer les principes de sécurité cloud et les piliers de référence
- Panorama des exigences de conformité : ISO, SOC, PCI-DSS
- Mettre en place une organisation sécurisée : gouvernance, séparation des environnements
- Référentiel AWS Well-Architected : focus Security Pillar
- Atelier pratique : Analyser une architecture AWS.

[Jour 1 - Après-midi]

Gestion des identités et des accès

- Fondations IAM : users, groups, roles, policies et evaluation logic
- Appliquer le least privilege et la séparation des responsabilités
- Utiliser IAM Access Analyzer pour détecter les accès externes
- Mettre en œuvre la fédération : SSO, identity providers, sessions
- Gérer les credentials : rotation, MFA, bonnes pratiques du compte root
- Atelier pratique : Créer des rôles IAM sécurisés.

Sécurité des comptes et des organisations

- Structurer un environnement multi-comptes avec AWS Organizations
- Appliquer des garde-fous avec les SCP (Service Control Policies)
- Sécuriser le compte root : MFA, restrictions, procédures de récupération
- Centraliser la gouvernance : délégation d'administration, séparation des logs
- Mettre en place une stratégie d'audit multi-comptes et de conformité
- Atelier pratique : Déployer une organisation et appliquer des SCP de sécurité.

[Jour 2 - Matin]

Chiffrement et gestion des clés

- Comprendre le chiffrement au repos et en transit dans AWS
- Maîtriser AWS KMS : clés, policies, grants et intégrations
- Distinguer AWS Managed Keys vs Customer Managed Keys
- Mettre en œuvre la rotation, la séparation des usages et la gouvernance des clés
- Appliquer les bonnes pratiques de chiffrement sur S3, EBS, RDS
- Atelier pratique : Chiffrer S3 et RDS avec KMS.

[Jour 2 - Après-midi]

Sécurité réseau AWS

- Isoler avec VPC : subnets publics/privés, routage, NAT et bastion
- Contrôler les flux avec Security Groups et NACL
- Accès privé aux services : VPC Endpoints et PrivateLink
- Bonnes pratiques d'architecture : segmentation, micro-segmentation, "deny by default"
- Approche Zero Trust et principes de durcissement réseau
- Atelier pratique : Sécuriser une application AWS via segmentation réseau et endpoints privés.

Protection contre les menaces

- Protection applicative : AWS WAF (règles, managed rules, rate limiting)
- Protection DDoS : AWS Shield et stratégies de résilience
- Détection : GuardDuty (signaux, findings, sévérité, bonnes pratiques)
- Réagir : intégration alerting, workflows de triage, notifications
- Intégration SOC : centralisation, corrélation et priorisation des alertes
- Atelier pratique : Déclencher/observer un finding GuardDuty et définir une réponse.

[Jour 3 - Matin]

Logs, audit et observabilité

- Journaliser avec CloudTrail : events, data events, organisation trails
- Conformité et drift : AWS Config (rules, aggregators, remediation)

- Centraliser les logs : comptes dédiés, collecte multi-comptes, rétention
- Mettre en place alertes et enquêtes : recherche, filtres, corrélation
- Forensique : collecte de preuves, traçabilité, préparation à l’investigation
- Atelier pratique : Construire une base d’audit multi-comptes.

[Jour 3 - Après-midi]

Réponse aux incidents et remédiation

- Structurer la réponse aux incidents : détection, containment, éradication, recovery
- Automatiser des actions : Lambda, événements, intégrations et approbations
- Définir des playbooks : rôles, responsabilités, procédures et escalade
- Remédiation : isolation, rotation des clés, blocage d’accès, durcissement
- Post-mortem : lessons learned, amélioration continue, prévention
- Atelier pratique : Automatiser une réponse sur un incident simulé.

Préparation à la certification SCS-C02

- Comprendre la structure et les attentes de l’examen SCS-C02
- Revoir les scénarios types : IAM, chiffrement, réseau, détection, réponse
- Identifier les pièges fréquents : “best answer”, coûts, sécurité par défaut
- Stratégie de résolution : lecture, élimination, gestion du temps
- Checklist de révision : points critiques et priorités
- Atelier pratique : Passage de l'examen blanc + correction.

Sociétés concernées

Cette formation s’adresse à la fois aux particuliers ainsi qu’aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.