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

Mis à jour le 30/06/2025

S'inscrire

Formation certification CCSK

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

2 jours (14 heures)

Présentation

Plongez dans l'univers de la sécurité cloud avec notre formation dédiée à la certification CCSK de la cloud security alliance. Ce parcours structuré couvre tout le cycle de de sécurisation d'un environnement multicloud, de la gouvernance stratégique aux réponses aux incidents en passant par l'IAM Zero Trust. À l'issue de la formation, vous serez pleinement préparé à l'examen officiel CCSK et capable de piloter la sécurité de vos infrastructures AWS, Azure et GCP avec confiance

Vous débuterez par la prise en main des référentiels phares de la CSA afin de cartographier vos services cloud et d'établir une matrice de responsabilités claire. Vous apprendrez à évaluer les risques, aligner vos politiques sur les exigences RGPD, ISO 27017/18 et SecNumCloud, puis à déployer des tableaux de bord de gouvernance parlants pour votre comité exécutif.

Vous entrerez ensuite dans le cœur opérationnel de la sécurité cloud : élaboration d'une stratégie IAM "least privilege", configuration de logs centralisés et détection de menaces avec SIEM, segmentation réseau avancée et bastions Zero Trust. Ces notions seront immédiatement appliquées lors d'ateliers pratiques.

La formation se poursuit avec la sécurisation des workloads – VM, conteneurs Kubernetes et fonctions serverless – et l'intégration de DevSecOps : scans SAST/SCA, génération automatique de SBOM et déploiements continus vers un cluster protégé. Vous apprendrez aussi à orchestrer la réponse aux incidents, à automatiser les sauvegardes chiffrées et à tester la résilience via des exercices de chaos engineering.

Comme pour toutes nos formations, celle-ci vous sera présentée avec les toutes dernières actualisations pour le passage de la certification CCSK.

Objectifs

- Valider la certification CCSK v5
- Gouverner la sécurité multicloud
- Déployer Zero Trust et IAM “least-privilege”
- Mettre en œuvre la protection des workloads
- Automatiser DevSecOps & monitoring
- Orchestrer la réponse aux incidents cloud

Public visé

- Responsable cybersécurité
- Architecte cloud
- Consultants GRC
- Chef de projet cloud

PRÉ-REQUIS

- Bases de sécurité informatique : pare-feu, chiffrement, gestion des accès
- Connaissances fondamentales du cloud computing
- Notions réseau (TCP/IP, VPN, proxy) et système (Linux / Windows) utiles pour les labs

Programme de notre formation CCSK

Fondamentaux du Cloud Computing

- Définitions clés et évolution du cloud
- Modèles de service : IaaS, PaaS, SaaS
- Modèles de déploiement : public, privé, hybride, multi-cloud
- Principe de responsabilité partagée fournisseur / client
- Terminologie essentielle : région, zone, tenant, marketplace

Gouvernance & Référentiels CSA

- Rôle du comité de pilotage “Cloud Security”
- Security Guidance v5 : structure et usage
- Cloud Controls Matrix (CCM) : mapping des contrôles
- Gestion des politiques et procédures cloud
- Atelier : Cartographier les services cloud et attribuer les responsabilités (RACI)

Gestion des Risques, Audit & Conformité

- Méthodologies d’analyse de risques adaptées au cloud
- Normes / cadres : ISO 27017/18, SOC 2, SecNumCloud, RGPD
- Due diligence fournisseurs : questionnaires CSA CAIQ, rapports d’audit
- Contrats & SLA sécurité : clauses essentielles

- Atelier : Élaborer une heat-map de risques cloud et plan de traitement

Identity & Access Management et Zero Trust

- Principes Zero Trust et identité comme nouveau périmètre
- Fédérations d'identité, OAuth 2.0, OpenID Connect, SAML
- Gestion du cycle de vie des comptes, rôles et stratégies RBAC/ABAC
- Concepts d'authentification forte (MFA, FIDO2)
- Atelier : Créer une stratégie IAM "least privilege" et vérifier la posture

Monitoring, Journalisation & Audit Continu

- Collecte de logs : CloudTrail, Azure Monitor, GCP Audit Logs
- SIEM, UEBA et corrélation multicloud
- Outils CSPM / CWPP pour l'audit continu
- Principes de détection & réponse aux menaces cloud
- Tableaux de bord et indicateurs clés de performance (KPI)

Sécurité Réseau & Architecture Cloud

- Segmentation logique (VPC/VNet), sous-réseaux privés/publics
- Contrôles réseau natifs : SG, NACL, NSG, firewall WAF
- Conceptions réseau hybrides et transit gateways
- Sécurisation des API & passerelles d'API
- Résilience réseau : haute disponibilité, multirégion, CDN

Protection des Données & Chiffrement

- Classification et cycle de vie des données dans le cloud
- Chiffrement at-rest / in-transit / in-use, gestion des clés (KMS, HSM)
- Stratégies BYOK / HYOK et rotation des clés
- Prévention de perte de données (DLP) et masquage
- Conformité RGPD : localisation, consentement, droit à l'oubli

Sécurité des Workloads & DevSecOps

- Hardening des VM, conteneurs et fonctions serverless
- Benchmarks CIS, contrôles Kubernetes & policy eBPF
- Intégration de la sécurité dans CI/CD (shift-left)
- Gestion des secrets et SBOM : bonnes pratiques
- Atelier : Implémenter un pipeline CI/CD DevSecOps avec scans SAST + SCA

Réponse aux Incidents, Stratégies Émergentes & Préparation Examen

- Plan de réponse aux incidents cloud et exercices table-top
- Sauvegardes, reprise d’activité et chaos engineering
- Tendances 2025 : Zero Trust avancé, IA/GenAI security, FinOps
- Simulation d’examen CCSK (60 QCM, open-book) et débrief ciblé
- Roadmap individuelle de montée en compétence post-certification

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.