



CERTIFIED CLOUD SECURITY ENGINEER V2

Évoluez dans un environnement multicloud & maîtrisez les compétences en matière de sécurité du cloud

Code : **CCSEv2**

Le programme Certified Cloud Security Engineer (C|CSE) d'EC-Council répond à la demande croissante des professionnels spécialisés en sécurité cloud.

Cette formation certifiante permet aux professionnels du secteur IT d'acquérir des compétences très demandées et liées au cloud. Le CCSE aidera également les entreprises à mettre en place une solide équipe de sécurité cloud en interne.

Le C|CSE est un mélange de deux concepts liés à la sécurité cloud, à la fois neutres et spécifiques à chaque fournisseur (AWS, Azure, GCP), en faisant un programme unique.

Ce programme met l'accent sur la manière de concevoir et de mettre en œuvre des cadres de gouvernance, de risque et conformité (GRC) dans une architecture de cloud computing.

PROGRAMME

Méthodes mobilisées : Cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : En amont de la formation, une évaluation des compétences de l'apprenant est effectuée. Ensuite, les objectifs sont régulièrement évalués tout au long de la formation (20% d'exercices pratiques) et formalisés sous forme de grille d'évaluation des compétences en fin de module par le formateur, puis par le passage de la certification.

PLAN DE COURS

- **Module 1 :** Introduction to Cloud Security
- **Module 2 :** Platform and Infrastructure in Security Cloud
- **Module 3 :** Application Security in Cloud
- **Module 4 :** Data Security in Cloud
- **Module 5 :** Operation Security in Cloud
- **Module 6 :** Penetration Testing in Cloud
- **Module 7 :** Incident Detection and Response in Cloud
- **Module 8 :** Forensic Investigation in Cloud
- **Module 9 :** Business Continuity and Disaster Recovery in Cloud
- **Module 10 :** Governance, Risk Management and Compliance (GRC) in Cloud
- **Module 11 :** Standards, Policies and Legal Issues in Cloud

PASSAGE DE L'EXAMEN

L'examen CCSE aura lieu à distance.

- **Titre de l'examen :** Certified Cloud Security Engineer
- **Format de l'examen :** QCM
- **Nombre de questions :** 125
- **Durée :** 4 heures
- **Langue :** anglais
- **Score requis :** de 60% à 78%

MAINTIEN DE LA CERTIFICATION

Pour maintenir la certification, il faudra obtenir 120 crédits dans les 3 ans avec un minimum de 20 points chaque année. Pour plus d'informations, vous pouvez consulter le site d'EC-Council.

RÉSULTAT

Directement disponible en fin d'examen.

PROCHAINES DATES  **16 MARS - 8 JUIN - 7 SEPT - 30 NOV**



OBJECTIFS

- Évaluer les techniques de stockage et les menaces pesant sur les données stockées dans le cloud et comprendre comment protéger ces données contre les attaques
- Concevoir et mettre en œuvre un cadre GRC pour l’infrastructure cloud de l’organisation en évaluant divers cadres de conformité et en comprenant les fonctions de conformité fournies par le fournisseur de services
- Concevoir et mettre en œuvre un plan de réponse aux incidents dans le cloud pour l’organisation et détecter les incidents de sécurité à l’aide d’outils d’automatisation de la sécurité
- Concevoir et mettre en œuvre un plan de continuité des activités pour lesservices en cloud en mettant en œuvre des solutions de sauvegarde et derécupération de bout en bout
- Mettre en œuvre et gérer la sécurité du cloud sur diverses plateformes telles que AWS, Azure et Google Cloud Platform
- Utiliser les services et outils de sécurité fournis par Azure, AWS et Google Cloud pour sécuriser l’environnement cloud de l’organisation en comprenant le modèle de responsabilité partagée du fournisseur de services
- Comprendre les implications juridiques associées à l’informatique en cloud afin d’éviter aux organisations des problèmes juridiques
- Évaluer les différentes normes de sécurité de l’informatique en cloud et les organisations responsables de la mise en place de ces normes
- Effectuer des audits de sécurité de l’informatique en cloud et des tests de pénétration pour aider les organisations à respecter les normes, les politiques, les procédures et les réglementations régissant les environnements cloud
- Comprendre et évaluer les différents programmes de conformité et les fonctionnalités offertes par AWS, Azure et Google Cloud
- Mettre en œuvre des contrôles opérationnels et des normes pour construire, exploiter, gérer et maintenir l’infrastructure cloud
- Mettre en œuvre les différents services de détection et de réponse aux menaces proposés par Azure, AWS et Google Cloud afin d’identifier les menaces pesant sur les services cloud de l’organisation
- Comprendre et mettre en œuvre la sécurité pour les environnements cloud privés, multi-locataires et hybrides
- Apprendre à sécuriser les environnements informatiques hybrides et multi-cloud
- Être préparé(e) à l’examen Cloud Security Engineer



INFORMATIONS GÉNÉRALES

Code : CCSEv2
Durée : 5 jours
Prix : 3 890 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92) - ou en distanciel
Examen : inclus. Valable 12 mois pour un passage de l’examen à distance.
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel



PRÉ-REQUIS

- Analystes de la cybersécurité
- Tout autre poste impliquant des administrations de réseau/cloud
- Avoir de bonnes connaissances en cybersécurité
- Avoir des connaissances de bases en Cloud
- Avoir de bonnes connaissances en gestion de la sécurité des réseaux



RESSOURCES

- Support de cours officiel en anglais
- Accès au cours en version numérique pendant un an
- Cours donnés en français
- 20% d’exercices pratiques
- 1 PC par personne



PUBLIC VISÉ

- Ingénieurs Cloud
- Administrateurs de la sécurité des réseaux