CCSP® : spécialiste certifié en sécurité du cloud computing

Date et durée

Code formation : CCSP-ISC2-FR
Durée : 5 jours
Nombre d'heures : 35 heures

Formation avec certification

CCSP® : Certified Cloud Security Professional

Description

La certification CCSP (Certified Cloud Security Professional) est **un titre de haut niveau dans le domaine de la cybersécurité**. Délivrée par l'ISC2, elle atteste de votre niveau d'expertise dans la conception, la mise en œuvre et la gestion de la sécurité des environnements cloud. Très recherchée par les entreprises, la qualification CCSP est un atout de taille pour tout professionnel de la sécurité informatique.
À travers cette **formation CCSP,** vous aborderez tous les domaines de la sécurité du cloud, tels que la gouvernance, l'architecture, les opérations, la protection des données et la conformité. Elle vous permettra d'acquérir les connaissances et les compétences nécessaires pour **concevoir des architectures cloud sécurisées**, mettre en œuvre des contrôles de sécurité efficaces et gérer les risques liés au cloud computing.
Une fois ce programme de 5 jours terminé, vous serez également prêt pour le **passage de l'examen officiel CCSP** inclus dans notre offre. La réussite de celui-ci vous permettra d'obtenir le certificat de Certified Cloud Security Professional (plus d'informations dans l'onglet certification).

Oo2 est un partenaire de formation (ATP), agréée par l'ISC2. Ce qui vous garantit des formations conformes aux normes de qualité rigoureuses de l'ISC2. Une enquête récente démontre que plus de 80 % des organisations préfèrent travailler avec un organisme agréé.

Objectifs

A l'issue de la formation CCSP, vous atteindrez les objectifs suivants :

- comprendre en profondeur les concepts de sécurité dans le cloud

- maitriser les meilleures pratiques pour sécuriser des données, des applications et des infrastructures dans le cloud.
- mettre en œuvre des contrôles de sécurité techniques, notamment des pare-feu, des systèmes de détection d'intrusion, des systèmes de cryptographie et des systèmes de gestion des vulnérabilités.
- gérer les risques liés à la sécurité des données dans le cloud qui prend en compte les aspects techniques, organisationnels et humains ;
- assurer le respect des normes et des réglementations en vigueur pour les services cloud ;
- répondre aux défis de la sécurité dans un environnement cloud en constante évolution.
- se préparer et réussir l'examen CCSP pour obtenir le titre de Certified Cloud Security Professional.

Points forts

• Un formateur agréé par l'ISC2.
• Des supports de cours officiels.
• Un apprentissage actif et interactif grâce à des cas pratiques et des quiz.
• Un taux de réussite élevé grâce notre expérience pour maximiser vos chances de succès.
• Le passage de l'examen officiel CCSP inclus dans le prix de la formation.

Certification

Cette formation vous permet de passer la certification professionnelle Certified Cloud Security Professional de l'ISC2. Un code coupon vous sera fourni à la fin du cours afin que vous puissiez programmer votre examen dans un centre de test Pearson VUE.

Informations sur l'examen de certification CCSP®

Prérequis :

- justifier d'une expérience professionnelle de 5 ans minimum dans les technologies de l'information, dont au moins 3 ans en sécurité de l'information et 1 an dans la sécurité des infrastructures cloud.
- une bonne compréhension des concepts de base de la sécurité informatique (cryptographie, réseaux, systèmes d'exploitation, etc.).
- une connaissance des différents types de cloud (public, privé, hybride) et des modèles de service (IaaS, PaaS, SaaS).

Note : *il est possible de compenser une partie de l'expérience requise si vous avez obtenu les certifications CCSK (Certified Cloud Security Knowledge) ou CISSP (Certified Information Systems Security Professional).Si vous ne possédez pas suffisamment d'expérience, vous pouvez tout de même passer l'examen, mais vous serez certifié en tant que « Associate » et disposerez de 6 ans pour acquérir les 5 années requises.*
En savoir plus sur les exigences du CCSP
Format de l'examen :

- Type d'examen : QCM de 125 questions couvrant les 6 domaines de cette formation.
- Durée : 3 heures
- Lieu : centres de test Pearson VUE
- Livre ouvert : non
- Langues : anglais, chinois, japonais et allemand
- Note de passage : 700 points sur 1000

Une fois l'examen réussi, vous recevrez le titre professionnel de *Certified Cloud Security Professional délivrée par l'ISC2*. Celui-ci est soumis à un **renouvellement de 3 ans** à compter de sa date de délivrance.

Modalités d'évaluation

Quiz / QCM
Etude de cas

Pré-requis

Suivre cette formation nécessite les prérequis suivants :

- une solide expérience professionnelle dans le domaine des technologies de l'information et principalement en sécurité de l'information et en infrastructure cloud ;
- une compréhension des concepts de base de la sécurité informatique (cryptographie, réseaux, systèmes d'exploitation, etc.) ;
- une bonne connaissance des différents types de cloud (public, privé et hybride) et des modèles de service (IaaS, PaaS et SaaS) ;
- savoir lire et comprendre l'anglais pour le passage de l'examen CCSP.

Public

Cette formation s'adresse aux publics suivants :

- les architectes cloud ;
- les ingénieurs en sécurité informatique et réseau ;
- les responsables de la sécurité des systèmes d'information (RSSI) ;
- les consultants en sécurité informatique ;
- les auditeurs en sécurité des systèmes d'information ;
- les administrateurs systèmes et réseaux ;
- les chefs de projet IT ;
- tous professionnels de l'informatique qui souhaitent approfondir leurs connaissances en sécurité du cloud et obtenir une certification reconnue dans ce domaine.

Programme

1. Comprendre les concepts, l'architecture et la conception du cloud

- Les concepts du cloud computing.
- L'architecture de référence du cloud.
- Les concepts de sécurité clé pour le cloud computing.
- Les principes de conception du cloud computing sécurisé.
- L'évaluation des fournisseurs de services cloud.

2. Sécuriser des données dans le cloud

- Les concepts de données cloud.
- La conception et la mise en œuvre d'architectures de stockage de données cloud.
- La conception et la mise en œuvre des technologies et des stratégies de sécurité des données.
- La mise en œuvre de la découverte de données.
- La mise en œuvre de la classification des données.
- La conception et la mise en œuvre de la gestion des droits de l'information (IRM).
- La planification et la mise en œuvre des politiques de conservation, de suppression et d'archivage des données.
- La conception et la mise en œuvre de l'auditabilité, de la traçabilité et de l'imputabilité des événements liés aux données.

3. Sécuriser des plateformes et des infrastructures cloud

- Les composants de l'infrastructure cloud.
- La conception d'un centre de données sécurisé.

- L'analyse des risques associés à l'infrastructure cloud.
- La conception et la planification des contrôles de sécurité.
- La planification de la reprise après sinistre et la continuité des activités.

4. Sécuriser des applications dans le cloud

- La promotion et la sensibilisation à la sécurité des applications.
- Le processus et l'application du cycle de vie du développement logiciel sécurisé (SDLC).
- L'application de l'assurance et de la validation des logiciels cloud.
- L'utilisation de logiciels sécurisés vérifiés.
- Les particularités d'une architecture cloud.
- La création de solutions de gestion des identités et des accès (IAM) adaptées.

5. Effectuer des opérations de sécurité dans le cloud

- La création et la mise en œuvre d'une infrastructure physique et logique.
- La gestion et le maintien de l'infrastructure physique et logique.
- La mise en œuvre de contrôles opérationnels et des normes (ITIL, ISO/CEI 20000, etc.).
- Le support pour le service de criminalistique numérique.
- La gestion de la communication avec les parties concernées.
- La gestion des opérations de sécurité.

6. Gérer les aspects légaux, les risques et la conformité

- L'adaptation des exigences juridiques et des risques propres au cloud.
- Les questions relatives à la protection des données à caractère personnel
- Les processus d'audit, les méthodologies et leurs adaptations pour un environnement cloud.
- Les enjeux de l'informatique dématérialisée pour la gestion des risques de l'entreprise.
- L'externalisation et la définition des contrats relatifs à l'informatique dématérialisée.