

Mis à jour le 15/03/2024

S'inscrire

Formation Préparation à la Certification CCSP®

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

Prouvez votre expertise en sécurité cloud. La certification CCSP® est le titre reconnu mondialement à destination des professionnels en charge de la sécurité d'un environnement cloud.

Durant notre formation CCSP®, vous réviserez tous les chapitres présents à l'examen. En effet, nous couvrons les 6 domaines du CCSP® Common Body of Knowledge de l'ISC2 :

- Concepts, architecture et conception de l'informatique cloud
- Sécurité des données dans le cloud
- Sécurité de la plateforme et de l'infrastructure cloud
- Sécurité des applications cloud
- Opérations de sécurité dans l'informatique dématérialisée
- Juridique, risque et conformité

Avec l'aide d'un formateur certifié, nous vous accompagnerons dans votre préparation. Suite à l'apprentissage des différents modules, nous vous donnerons les stratégies essentielles pour terminer l'épreuve à temps en engendrant le maximum de points.

Cette [certification](#) renforcera grandement votre attractivité auprès des employeurs si vous désirez un emploi dans le domaine du cloud computing.

Objectifs

- Acquérir les connaissances nécessaires à la réussite de l'examen CCSP®
- Maîtriser les connaissances en sécurité de l'information dans les six domaines du CBK
- Comprendre les besoins en sécurité dans un environnement cloud
- Acquérir les connaissances nécessaires pour conseiller une organisation sur les meilleures pratiques en sécurité cloud

Public visé

- DSI
- RSSI
- Informaticien
- Administrateur réseau
- Ingénieur cloud
- Consultant en cybersécurité

Pré-requis

- Prouver 5 ans d'expérience professionnelle en informatique dont 3 ans en sécurité informatique
- Connaissances en cloud computing
- Compréhension de l'anglais technique

Note : Ambient IT n'est pas propriétaire de CCSP®, cette certification appartient à ISC2®, INC.

Programme de la Préparation à la Certification CCSP®

Concepts, architecture et conception de l'informatique cloud

- Comprendre les concepts du cloud computing
- Décrire l'architecture de référence du cloud
- Comprendre les concepts de sécurité relatifs à l'informatique cloud
- Comprendre les principes de conception de l'informatique cloud sécurisée
- Évaluer les fournisseurs de services d'informatique cloud

Sécurité des données dans le cloud

- Décrire les concepts de données cloud
- Concevoir et mettre en œuvre des architectures de stockage de données dans le cloud
- Concevoir et appliquer des technologies et des stratégies de sécurité des données
- Mettre en œuvre la découverte de données
- Mettre en œuvre la classification des données
- Concevoir et mettre en œuvre la gestion des droits de l'information (IRM)
- Planifier et mettre en œuvre des politiques de conservation, de suppression et d'archivage des données
- Concevoir et mettre en œuvre l'auditabilité, la traçabilité et la responsabilité des événements liés aux données.

Sécurité de la plateforme et de l'infrastructure cloud

- Comprendre les composants de l'infrastructure cloud

- Concevoir un centre de données sécurisé
- Analyser les risques associés à l'infrastructure cloud
- Concevoir et planifier des contrôles de sécurité
- Planifier la reprise après sinistre (DR) et la continuité des activités (BC)

Sécurité des applications cloud

- Préconiser la formation et la sensibilisation à la sécurité des applications
- Décrire le processus du cycle de vie du développement logiciel sécurisé (SDLC)
- Appliquer le cycle de développement sécurisé des logiciels (SDLC)
- Appliquer l'assurance et la validation des logiciels cloud
- Utiliser des logiciels sécurisés vérifiés
- Comprendre les spécificités de l'architecture des applications cloud
- Concevoir des solutions appropriées de gestion des identités et des accès (IAM)

Opérations de sécurité dans l'informatique dématérialisée

- Construire et mettre en œuvre l'infrastructure physique et logique de l'environnement cloud
- Exploiter et maintenir l'infrastructure physique et logique de l'environnement cloud
- Mettre en œuvre des contrôles et des normes opérationnels
- Soutenir la criminalistique numérique
- Gérer la communication avec les parties concernées
- Gérer les opérations de sécurité

Juridique, risques et conformité

- Articuler les exigences juridiques et les risques uniques dans l'environnement "cloud".
- Comprendre les questions relatives à la protection de la vie privée
- Comprendre le processus d'audit, les méthodologies et les adaptations nécessaires pour un environnement cloud
- Comprendre les implications de l'informatique dématérialisée pour la gestion des risques de l'entreprise
- Comprendre la conception des contrats d'externalisation et d'informatique dématérialisée

Stratégies et astuces pour réussir l'examen

Examen blanc

FAQ – QUESTIONS / RÉPONSES

En quelle langue la formation CCSP® vous est enseignée ?

La formation est en français.

En quelle langue se déroule l'examen ?

L'examen se déroule en anglais.

L'examen est-il compris dans le prix de la formation ?

Oui, le prix de la certification est inclus au coût de la formation (555€ HT à titre indicatif). Vous pourrez passer l'examen à la fin de la session.

Comment se déroule l'examen pour la certification CCSP® ?

L'examen consiste en un QCM composé de 150 questions sur les domaines suivants :

- Concepts, architecture et conception de l'informatique cloud
- Sécurité des données dans le cloud
- Sécurité de la plateforme et de l'infrastructure cloud
- Sécurité des applications cloud
- Opérations de sécurité dans l'informatique dématérialisée
- Juridique, risque et conformité

Il s'effectue en ligne dans un centre d'examen agréé Pearson Vue à Paris.

Cet examen dure 4 heures et est en anglais.

Pour réussir cet examen, il faut au minimum obtenir 700 points sur 1000 points.

Peut-on passer l'examen à distance ?

Non, l'examen doit être réalisé dans un centre officiel Pearson Vue à Paris.

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.