Formation : Certified Cloud Security Professional (CCSP), certification ISC2

Formation officielle alignée ISC2

Cours pratique - 5j - 35h00 - Réf. CCN

Prix : 4040 CHF H.T.

NEW | Nouvelle édition

La certification CCSP (Certified Cloud Security Professional), délivrée par ISC2, est une certification de référence, vendor-neutral, dédiée à la sécurité du cloud computing. Cette formation vous permettra d'acquérir une vision stratégique et opérationnelle de la sécurité cloud afin de réussir l'examen officiel CCSP, en couvrant l'ensemble des 6 domaines du CCSP Common Body of Knowledge (CBK).

Objectifs pédagogiques

À l'issue de la formation, le participant sera en mesure de :

- Maîtriser les concepts cloud, les modèles de services et les architectures de référence
- Concevoir une architecture cloud sécurisée, cohérente et gouvernée
- Définir et piloter une stratégie de protection des données dans le cloud sur l'ensemble de leur cycle de vie
- Sécuriser les plateformes, infrastructures et services cloud
- Intégrer les exigences de sécurité dans les applications cloud et chaînes CI/CD
- Organiser et piloter les ope rations de sécurité cloud, incluant supervision, gestion des incidents et continuité
- Appliquer les exigences légales, de gestion des risques et de conformité spécifiques aux environnements cloud
- Adopter le raisonnement "cloud security leader" attendu par ISC2 pour réussir l'examen CCSP
- Se préparer efficacement à l'examen officiel CCSP (format et attentes ISC2)

Public concerné

Architectes et ingénieurs IT, responsables des systèmes d'information et de la sécurité, profils DevOps/SecOps, consultants sécurité et professionnels des risques, de la conformité et des contrats IT.

PARTICIPANTS

Architectes et ingénieurs IT, responsables des systèmes d'information et de la sécurité, profils DevOps/SecOps, consultants sécurité et professionnels des risques, de la conformité et des contrats IT.

PRÉREQUIS

La certification CCSP requiert 5 ans d'expérience IT, dont 3 ans en cybersécurité et 1 an en sécurité cloud. Des dispenses sont possibles (diplôme, CCSK). CISSP valide l'ensemble.

COMPÉTENCES DU FORMATEUR

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

MODALITÉS D'ÉVALUATION

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques...

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Prérequis

La certification CCSP requiert 5 ans d'expérience IT, dont 3 ans en cybersécurité et 1 an en sécurité cloud. Des dispenses sont possibles (diplôme, CCSK). CISSP valide l'ensemble.

Vérifiez que vous avez les prérequis nécessaires pour profiter pleinement de cette formation en faisant ce test.

Modalités d'évaluation

Le formateur évalue la progression pédagogique du participant tout au long de la formation au moyen de QCM, mises en situation, travaux pratiques…

Le participant complète également un test de positionnement en amont et en aval pour valider les compétences acquises.

Programme de la formation

1 Domaine 1 - concepts cloud, architecture et design

- Concepts fondamentaux du cloud computing.
- Modèles de services cloud (IaaS, PaaS, SaaS) et modèles de déploiement.
- Principes d'architecture cloud et design sécurisé.
- Modèle de responsabilité partagée.
- Gouvernance et cohérence des contrôles en environnement multicloud.
- Orchestration des services cloud et intégration des composants.

2 Domaine 2 - sécurité des données Cloud

- Gouvernance des données et responsabilités dans le cloud.
- Classification et exigences de protection des données.
- Gestion du cycle de vie des données cloud.
- Contrôles de protection des données (politiques, procédures, mécanismes).
- Gestion de la localisation, de la rétention et de la suppression des données.

3 Domaine 3 - sécurité des plateformes et des infrastructures Cloud

- Architecture et sécurisation des infrastructures cloud.
- Sécurité des plateformes et services cloud.
- Segmentation, isolation et interconnexions cloud.
- Gestion des configurations et des vulnérabilités.
- Contrôles de sécurité des services d'infrastructure.

4 Domaine 4 - sécurité des applications Cloud

- Exigences de sécurité applicative en environnement cloud.
- Intégration de la sécurité dans le cycle de développement et de déploiement.
- Sécurité des API et des services applicatifs.
- Gestion des risques applicatifs spécifiques au cloud.
- Approche "secure-by-design" et alignement avec les politiques de sécurité.

5 Domaine 5 - opérations de sécurité Cloud

- Organisation et gouvernance des opérations de sécurité cloud.
- Supervision, journalisation et surveillance cloud-native.
- Gestion des évènements et incidents de sécurité cloud.
- Gestion des accès et des identités en exploitation.
- Continuité d'activité, résilience et reprise dans les environnements cloud.

MOYENS PÉDAGOGIQUES ET TECHNIQUES

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les formations pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
• À l'issue de chaque formation ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.
• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation ainsi qu'une attestation de fin de formation si le participant a bien assisté à la totalité de la session.

MODALITÉS ET DÉLAIS D'ACCÈS

L'inscription doit être finalisée 24 heures avant le début de la formation.

ACCESSIBILITÉ AUX PERSONNES HANDICAPÉES

Pour toute question ou besoin relatif à l'accessibilité, vous pouvez joindre notre équipe PSH par e-mail à l'adresse psh-accueil@orsys.fr.

6 Domaine 6 - légal, Risque et Conformité

- Cadres légaux et règlementaires applicables aux services cloud.
- Exigences contractuelles et responsabilités client / fournisseur.
- Gestion des risques cloud.
- Conformité, audit et production de preuves.
- Application des politiques et procédures pour répondre aux obligations réglementaires.

7 Préparation à l'examen CCSP

- Présentation de l'examen CCSP.
- Méthodologie de réponse aux questions ISC2.
- Gestion du temps et pièges fréquents.
- Quiz d'évaluation et questions type examen.
- Conseils d'experts certifies CCSP.

Partenariat

Formation officielle dispensée par ACG Cybersecurity, ISC2 Official Training Partner

Options

Certification : 590 € HT

L'examen officiel se déroule en anglais en différé et en distanciel sous forme d'un QCM d'une durée de 3 heures, comprenant 100 à 150 questions, avec un score minimum requis de 700/1000.

Dates et lieux

CLASSE À DISTANCE
2026 : 8 juin, 21 sep., 30 nov.