Date de publication : 02/03/2026

Formation : Lead Cloud Security Manager, certification PECB

Cours pratique - 5j - 35h00 - Réf. CSX
Prix : 3310 € H.T.

NEW

Cette formation permet d'acquérir les connaissances essentielles pour participer à la mise en place, au pilotage et à l'amélioration d'un programme de sécurité du cloud, en s'appuyant sur les normes ISO/IEC 27017 et ISO/IEC 27018.

Objectifs pédagogiques

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

- Comprendre les concepts, méthodes et techniques pour mettre en œuvre et gérer un programme de sécurité cloud.
- Comprendre la corrélation entre ISO/IEC 27017, ISO/IEC 27018 et d'autres normes et cadres réglementaires
- Savoir interpréter les normes ISO/IEC 27017 et 27018 dans le contexte spécifique d'un organisme
- Développer les compétences pour planifier, déployer, gérer, surveiller et maintenir un programme de sécurité cloud
- Acquérir les compétences pour conseiller un organisme et gérer un programme de sécurité cloud selon les bonnes pratiques

Public concerné

Professionnels, managers, consultants et experts techniques en cybersécurité souhaitant mettre en place, gérer ou améliorer un programme de sécurité cloud et maîtriser les bonnes pratiques associées.

Prérequis

Avoir une compréhension fondamentale des normes ISO/IEC 27017 et ISO/IEC 27018 et une connaissance générale des concepts du cloud computing.

PARTICIPANTS

Professionnels, managers, consultants et experts techniques en cybersécurité souhaitant mettre en place, gérer ou améliorer un programme de sécurité cloud et maîtriser les bonnes pratiques associées.

PRÉREQUIS

Avoir une compréhension fondamentale des normes ISO/IEC 27017 et ISO/IEC 27018 et une connaissance générale des concepts du cloud computing.

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.

Certification

L'examen consiste à répondre à 80 questions, en 3h00 à livre ouvert. À l'issue du cours, une attestation de suivi de la formation de 31 unités de FPC (Formation professionnelle continue) sera délivrée aux participants ayant suivi la formation. Les candidats ayant suivi la formation mais échoué à l'examen peuvent le repasser gratuitement une seule fois dans un délai de 12 mois à compter de la date initiale de l'examen.

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 Introduction aux normes ISO/IEC 27017 et ISO/IEC 27018 et à l'initiation d'un programme de sécurité du cloud

- Objectifs et structure de la formation.
- Normes et cadres réglementaires.
- Concepts et principes fondamentaux du cloud computing.
- Comprendre l'architecture du cloud computing de l'organisme.
- Rôles et responsabilités en matière de sécurité de l'information liés au cloud computing.
- Politique de sécurité de l'information pour le cloud computing.

2 Gestion des risques de sécurité du cloud et mesures spécifiques au cloud

- Gestion des risques de sécurité du cloud computing.
- Sélection et conception de mesures spécifiques au cloud.
- Mise en œuvre de mesures spécifiques au cloud (partie 1).

3 Gestion de l'information documentée et sensibilisation et formation à la sécurité du cloud

- Mise en œuvre de mesures spécifiques au cloud (partie 2).
- Gestion de l'information documentée dans le cloud.
- Sensibilisation et formation à la sécurité du cloud.

4 Gestion des incidents de sécurité du cloud, tests, surveillance et amélioration continue

- Gestion des incidents de sécurité du cloud.
- Tests de sécurité du cloud.
- Surveillance, mesure, analyse et évaluation.
- Amélioration continue.

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.

5 Domaines de compétences couverts par l'examen

- Domaine 1 : principes et concepts fondamentaux du cloud computing.
- Domaine 2 : politique de sécurité de l'information pour le cloud computing et la gestion de l'information documentée.
- Domaine 3 : gestion des risques liés à la sécurité du cloud computing.
- Domaine 4 : contrôles spécifiques au cloud basés sur les normes ISO/IEC 27017 et ISO/IEC 27018.
- Domaine 5 : sensibilisation, formation, rôles et responsabilités en matière de sécurité du cloud.
- Domaine 6 : gestion des incidents de sécurité du cloud.
- Domaine 7 : tests, surveillance et amélioration continue de la sécurité du cloud.