

Cloud Computing, sécurité

Séminaire de 2 jours - 14h

Réf : OUD - Prix 2024 : 2 090CHF HT

Comment peut-on assurer la sécurité des informations dans le nuage ? Ce séminaire dresse un panorama complet de ce problème majeur du cloud. Les participants auront une vision concrète des risques de l'utilisation d'un cloud, des différents référentiels existant pour évaluer la sécurité des données et des fournisseurs.

OBJECTIFS PÉDAGOGIQUES

À l'issue de la formation l'apprenant sera en mesure de :

- Identifier les aspects organisationnels de la sécurité du cloud
- Connaitre les fondamentaux de la sécurité des SI et du Cloud
- Appréhender les principales menaces, vulnérabilités et risques du Cloud
- Connaitre les référentiels de normes et de standards pour sécuriser le Cloud
- Évaluer la maturité et le niveau de sécurité des fournisseurs cloud
- Identifier les bonnes pratiques et les solutions de sécurisation des opérateurs de Cloud

LE PROGRAMME

dernière mise à jour : 11/2022

1) Introduction à la sécurité du cloud computing

- Architecture du cloud computing (NIST, ISO 17788/17889).
- Shadow IT : détection et prévention des usages non approuvés du cloud.
- Le principe de responsabilité partagée en IaaS, PaaS et SaaS.
- Les normes ISO 27017 et 27018 pour sécuriser les données dans le cloud.

2) La sécurité des données dans le cloud

- Les données dans le cloud : cycle de vie, classification, anonymisation, pseudonymisation, tokenisation.
- L'approche BYOK (bring your own key) et les solutions HSM dans le cloud.
- Le CASB (cloud access security broker), principes et solutions.

3) Les référentiels de la cloud security alliance (CSA)

- Les 14 domaines du security guidance for critical areas of focus in cloud computing.
- La certification CCSK (certificate of cloud security knowledge).
- La cloud controls matrix (CCM) et le consensus assessments initiative questionnaire (CAIQ).
- Le framework de certification OCF et l'annuaire STAR (security, trust & assurance registry).
- Le code de conduite RGPD (CoC GDPR) pour les fournisseurs.

4) Les risques dans le cloud computing selon l'ENISA

- Évaluation et gestion des risques du cloud par la norme ISO 27005.
- Les spécificités de la gestion des risques dans le cloud.
- Les principaux risques identifiés par l'ENISA.

5) L'évaluation de la sécurité des fournisseurs

- Panorama des certifications/qualifications (SecNumCloud, SSAE18, HDS...).

PARTICIPANTS

DSI, RSI, Chefs de projets, Responsables sécurité, Consultants, Administrateurs, toute personne en charge de la sécurité du Cloud Computing.

PRÉREQUIS

Avoir des connaissances générales des systèmes d'information.

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.

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 stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.
- À l'issue de chaque stage 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 stagiaire 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

Vous avez un besoin spécifique d'accessibilité ? Contactez Mme FOSSE, référente handicap, à l'adresse suivante psh-accueil@orsys.fr pour étudier au mieux votre demande et sa faisabilité.

- La certification de sécurité européenne issue du Cybersecurity Act.
- Intérêts et limites de la certification ISO 27001 pour les services cloud.

6) La sécurité dans les contrats cloud

- Les accords de service (SLA) : pénalités versus indemnités.
- Les clauses de sécurité à insérer dans un contrat de cloud (confidentialité, effacement des données...).
- Clauses de réversibilité amont & aval.

7) Aspects juridiques

- Le cadre juridique des données à caractère personnel (GDPR, CCT, BCR...).
- Comment assurer sa conformité RGPD dans le cloud ?
- Les lois et dispositions américaines (Privacy Shield, Patriot Act., FISA, Cloud Act).
- Comment la loi Godfrain (CP 323) s'applique-elle dans un contexte de cloud international ?
- Les hébergeurs de données de santé (certification HDS, obligations de sécurité, localisation des données, etc.).

LES DATES

CLASSE À DISTANCE
2024 : 18 juin, 03 oct., 07 nov.