Cloud Computing, gouvernance et sécurité

Séminaire de 3 jours - 21h
Réf : CCG - Prix 2024 : 2 890CHF HT

Le Cloud Computing permet aux entreprises de simplifier la gestion du SI et de faire des économies, mais il inquiète au niveau sécurité. Cette formation très riche explique comment évaluer les risques (notamment réglementaires) et quelles solutions mettre en place pour relever le défi en matière de cybersécurité.

OBJECTIFS PÉDAGOGIQUES

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

Apprendre à sécuriser les environnements virtuels et les accès réseau au Cloud

Évaluer et gérer les risques du Cloud Computing selon la norme ISO 27005

Contrôler et superviser la sécurité du Cloud

Apprendre les aspects juridiques et la conformité réglementaire

LE PROGRAMME

dernière mise à jour : 09/2021

1) Introduction à la sécurité du Cloud Computing

- Définition du Cloud Computing (NIST) et norme ISO 17788.
- Les principaux fournisseurs et les principales défaillances déjà constatées.
- Les offres de SecaaS (Security as a Service).
- Les clés d'une architecture sécurisée dans le Cloud.

2) La sécurité des environnements virtuels

- Les risques liés à la virtualisation des serveurs (VM Escape, VM Hopping, VM Theft et VM Sprawl).
- La problématique de la protection anti-malware dans une infrastructure virtualisée.
- Les risques liés aux vulnérabilités, aux API et aux logiciels (Openstack, Docker, VmWare...).

3) La sécurité des accès réseaux au Cloud

- Les accès sécurisés via Ipsec, VPN, https et SSH.
- Les solutions spécifiques d'accès au Cloud (Intercloud, AWS Direct connect...).
- Les solutions CASB (Cloud Access Security Broker).
- Les vulnérabilités des clients du Cloud (PC, tablettes, smartphones) et des navigateurs.

4) Les travaux de la Cloud Security Alliance (CSA)

- Le référentiel Security Guidance for Critical Areas of Focus in Cloud Computing.
- Les douze principales menaces identifiées dans le Cloud.
- Le framework OCF et l'annuaire STAR (Security, Trust & Assurance Registry).
- Comment utiliser la Cloud Controls Matrix (CCM) et le questionnaire CAIQ ?
- La certification des connaissances en sécurité du Cloud : CCSK (Certificate of Cloud Security Knowledge).

5) La sécurité du Cloud Computing selon l'ENISA

- Evaluation et gestion des risques du Cloud par la norme ISO 27005.
- Les trente-cinq risques identifiés par l'ENISA.

PARTICIPANTS

DSI, RSSI, architectes SI, ingénieurs réseaux/stockage/systèmes, responsables sécurité, chefs de projets, consultants.

PRÉREQUIS

Connaissances de base des modèles Cloud SaaS, PaaS, IaaS, et de la sécurité informatique. Notions de management de projet.

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.

- Les recommandations ENISA pour la sécurité des Clouds gouvernementaux.

6) Contrôler la sécurité du Cloud

- Comment contrôler la sécurité dans le Cloud : audit, test d'intrusion, qualification, certification ?
- Que valent les labels de sécurité Secure Cloud, CSA STAR et Cloud confidence ?
- Comment opérer un contrôle continu de la sécurité pendant toute la durée du contrat ?
- Comment sont détectés et notifiés les incidents de sécurité dans le Cloud ?

7) Le contrat Cloud

- Les clauses de sécurité indispensables à insérer dans un contrat de Cloud (comité de suivi, confidentialité...).
- Les clauses de réversibilité (amont & val) pour ne pas se faire piéger par un fournisseur.
- La clause d'audit de sécurité : peut-on toujours la négocier ? Comment faire dans un Cloud public ?
- L'importance de la localisation des données et de la juridiction retenue.
- Les accords de service dans le Cloud (SLA).
- Pénalités et indemnités : bien comprendre les différences.

8) Aspects juridiques et conformité réglementaire

- Quelles sont les responsabilités juridiques du fournisseur ? Quid des sous-traitants du fournisseur ?
- La nationalité du fournisseur et la localisation des Datacenters.
- Le cadre juridique des données à caractère personnel (Directive 95/46 CE, GDPR, CCT, BCR...).
- Après l'annulation du « Safe harbor », quelles sont les nouvelles garanties apportées par le « Privacy Shield » ?
- Le point sur l'USA Patriot Act. Menace-t-il les données dans le Cloud à l'extérieur des USA ?
- Le cadre juridique des données de santé à caractère personnel (loi du 26 janvier 2016).
- Les hébergeurs de données de santé (agrément ASIP, obligations de sécurité, localisation des données, etc.).

9) Les normes de sécurité dans le Cloud

- Que vaut la certification de sécurité ISO 27001 affichée par les fournisseurs ?
- Les normes ISO/IEC 17788:2014 (vocabulaire) et ISO/IEC 17789:2014 (architecture de référence).
- Les nouvelles normes ISO/IEC (27017 & 27018) dédiées à la sécurité dans le Cloud.
- Quel apport de la norme ISO 27018 pour la protection des données personnelles dans le Cloud ?
- La norme ISO 27017 et son complément idéal CSA Cloud Control Matrix.

10) La gestion des licences dans le Cloud

- Comprendre pourquoi la gestion des licences est plus complexe dans le Cloud.
- Comment assurer la conformité ?
- Les limites des outils de gestion des actifs logiciels (Software Asset Management) dans le Cloud.
- Réaliser l'inventaire et faire le rapprochement entre les licences installées, acquises et utilisées dans le Cloud.

LES DATES

CLASSE À DISTANCE
2024 : 18 juin, 08 oct., 17 déc.