Gérer la sécurité des services Cloud et MS-Azure, synthèse

Cours Synthèse de 2 jours - 14h
Réf : CAZ - Prix 2024 : 1 950CHF HT

Ce cours vous présentera les problématiques et les solutions de sécurité relatives au traitement de données au sein des Clouds publics AWS (Amazon Web Services) et Microsoft Azure. Vous appréhenderez les différents outils et les services disponibles pour évaluer et maîtriser les risques résiduels.

OBJECTIFS PÉDAGOGIQUES

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

Evaluer et maîtriser les risques

Connaître les outils et services disponibles

Comprendre l'organisation nécessaire pour maintenir et améliorer le niveau de sécurité

LE PROGRAMME

dernière mise à jour : 09/2018

1) Les fondamentaux

- Le rapport entre Virtualisation et Cloud Computing.
- Le Cloud (IaaS, PaaS, SaaS), les tendances du marché.
- L'actualité des brèches de sécurité en rapport avec AWS (Amazon Web Services) et Azure.
- Les menaces sur la sécurité du Cloud Computing (Notorious Nine et Dirty Dozen) selon CSA (Cloud Security Alliance).
- Les APTs, les révélations Snowden, les NSL (National Security Letters).
- Le contexte Français et Européen. La position de l'Agence nationale de la sécurité des Systèmes d'Information (ANSSI).

2) Le modèle à responsabilité partagée

- Gestion des Identités et Contrôle d'accès (IAM).
- Authentification Multi-Facteur (MFA).
- Security Token Service (STS).

3) Sécurité des machines virtuelles (VMs)

- Sécurité des images, durcissement des systèmes.
- Sécurité du LAN AWS et Azure.
- Architectures de type Virtual Private Cloud (VPC), Virtual Network et leurs composants.
- Rappel sur la protection périmétrique, le cloisonnement et les types de Firewalls.
- Différence entre Network Access Control Lists (NACLs) et Security Groups (SGs).
- WAF et CDN.
- Lien DirectConnect, Express Route et/ou VPN IPSEC.
- Défense contre les DDoS (Route 53 et DNS, LB, CloudFront).

4) Gestion Cryptographique

- Les concepts de base sur SSL, TLS.
- Autorité de Certification.
- AWS Key Management Service (KMS), HSM Azure KeyVault.

PARTICIPANTS

Direction informatique et fonctionnelle. Tout responsable informatique.

PRÉREQUIS

Connaissances de base des architectures techniques et du management SI.

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.

5) Sauvegardes de données

- Principe et cas d'usages.
- Points d'attention des services AWS et Azure.

6) Contrôler la sécurité

- Amazon Inspector, Azure Security Center.
- AWS : Config Rules, Trusted Advisor, CloudWatch Logs et Events , CloudTrail.
- Azure : Log Analytics, Azure Portal.
- Autres logs (S3 Logs, Bucket Logging , CloudFormation Logs , VPC Flow Logs).
- Intérêt des solutions tierces de renforcement de la sécurité.
- Test d'intrusion : précautions et autorisations préalables.
- Rapporter un abus, une vulnérabilité ou une faille de sécurité.

LES DATES

CLASSE À DISTANCE
2024 : 25 juin, 10 sept., 03 déc.