Cloud - Gouvernance et sécurité

Référence : **CLOUD003** Durée : **3 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• 1-Avoir des connaissances minimales sur le Cloud (caractéristiques, modèles de services, modèles de déploiement). • 2-Avoir des bases en sécurité informatique et réseaux. • 3-Avoir également des notions de management de projet.

PROFIL DES STAGIAIRES

• Cette formation Cloud s'adresse aux architectes, chefs de projets, ingénieurs informatique (réseau, système, développement...).

OBJECTIFS

• Décrire les éléments fondamentaux de la sécurité du Cloud. • Identifier et analyser les risques liés au Cloud. • Interpréter les contrats Cloud. • Mettre en œuvre les bonnes pratiques de sécurité dans le Cloud. • Décrire les techniques de sécurisation réseau du Cloud. • Reconnaître les problématiques de sécurisation des environnements de développeurs dans le Cloud..

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Cloud

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Sécurité du Cloud Computing

Introduction

- Fondamentaux du Cloud Computing
- En quoi la sécurité du Cloud est-elle différente de celle dans l'entreprise ?
- Retour sur les aspects fondamentaux de la sécurité : confidentialité, intégrité, disponibilité, traçabilité
- Principes généraux de sécurité : SMSI, PSSI

La sécurité des infrastructures virtuelles aujourd'hui

- La gestion de la sécurité des environnements virtuels "traditionnels"
- Les menaces et risques actuels et les techniques de sécurisation associées
- L'impact de l'hyperviseur, du stockage et de la virtualisation du réseau

Introduction à la sécurité du Cloud

- Les organismes aux différentes échelles : CNIL, ANSSI, ENISA, Cloud Security Alliance, ISO…
- Les grandes réglementations : HDS, directives européennes...
- Les certifications : ISO 27001, 27002, 27005, 27018

Exemple de travaux pratiques (à titre indicatif)

- Présentation d'une architecture virtuelle dans un contexte client : comment la sécuriser avec les techniques traditionnelles ?

Les risques identifiés

Introduction

- Identification et classification des données externalisables
- Processus de gestion des risques ISO 27005
- Approches qualitatives et quantitatives
- Les principales menaces dans le Cloud

Les principaux risques dans le Cloud

- Les risques stratégiques et organisationnels
- Les risques techniques
- Les risques juridiques
- Autres risques identifiés

Traitement et réduction des risques

- Actions liées aux risques et opportunités ISO 27001
- Actions de réduction organisationnelle des risques
- Actions de réduction techniques des risques

Aspects juridiques : le contrat Cloud

Introduction

- Les différences entre les contrats d'infogérance et les contrats Cloud
- Les matrices de responsabilité
- Gérer et garantir la localisation, le transfert et la sécurité des données, la confidentialité
- La dilution des responsabilités

Les contrats : généralités

- Les clauses clés du contrat : SLA, support, sécurité, facturation, transitions, pénalités, continuité de service...
- Les clauses d'auditabilité
- Les Cloud auditors et les APM
- La réversibilité ou comment changer de provider ?
- L'interopérabilité du Cloud

Les SLA

- Les SLA techniques
- Les SLA opérationnels
- Exemples de SLA de contrats Cloud

La tarification et les licences

- Vers un nouveau modèle de coûts Capex / Opex
- L'impact sur les licences logicielles de l'entreprise
- Comment gérer les licences en environnement hybride ?
- Les outils des providers (Amazon, Azure...) et les outils spécifiques (RightScale...)

Exemples de travaux pratiques (à titre indicatif)

- Etudes de cas : Le contrat de Salesforce ; Le contrat SaaS et son audit pour une société de services financiers ; Référentiel d'exigences de sécurité pour les applications en mode SaaS

Les bonnes pratiques de sécurité dans le Cloud

Sécurisation de l'infrastructure du Cloud

- La sécurité physique et environnementale
- Contrôle d'accès et gestion des identités
- La sécurité des données : chiffrement
- La gestion des mots de passe : cryptologie

Opération et exploitation des SI

- Gestion des changements
- Séparation des environnements
- Sauvegarde des environnements
- Journalisation des évènements

Continuité d'activité

- Les normes de Data Center : Uptime Institut et tier I à IV
- PRA / PCA et/dans le Cloud
- Redondance des ressources et des équipements

Acquisition, développement et maintenance des SI

- Politique de développement
- Développement externalisé

Tiers et ressources humaines

- Procédures d'entrée et de sortie
- La rupture contractuelle

Gestion de la gouvernance dans le(s) Cloud

- Evolution de la DSI et nouvelle organisation
- Les outils pour la DSI
- Les Cloud Management Platforms

Les technologies de sécurité adaptées au Cloud

- Couche applicatives : protection Firewall, NIPS, NIDS, filtrage Web, CASB, SASE...
- Protection des points de terminaison : antivirus, HIDS, HIPS, EDR...

La sécurité du réseau dans le Cloud

Sécurité des flux

- L'impact de la virtualisation du réseau
- La micro-segmentation
- Distributed firewall
- Le cas de VMware NSX

La sécurité entre les Clouds

- Les offres de VPN des providers
- Les possibilités d'interconnecter vos équipements à ceux du Cloud provider
- L'interconnexion des applications SaaS avec des données situées dans l'entreprise

Identity as a Service

- Base de l'IAM
- Sécurité des accès : L'impact de la multiplication des applications SaaS ; La fédération des identités : SAML ; Le cas d'ADFS et de Azure AD ; Les VPN
- Gestion et fédération de l'identité

- L'évolution vers le Identity as a Service : Acteurs : Okta, Ping Identity, Azure AD

Exemples de travaux pratiques (à titre indicatif)

- Etudes de cas : La fédération d'identités avec Office 365 ; La sécurisation des accès à AWS

Sécurité de l'écosystème du développeur dans le Cloud

L'écosystème DevOps

- Les fondamentaux du DevOps
- Les outils clés
- Infrastructure as Code et automatisation : Principes et intérêt (exemple avec Ansible) ; Intégration dans le Cloud, scalabilité et images (exemple avec Packer et Terraform)
- Les conteneurs : Compréhension d'une image de conteneur ; Exemple avec Docker

Stratégies et normes

- Les critères communs
- Security by design
- Les douze règles de développement d'application Cloud Native
- Architecture sécurisée et principes de conception

Sécurisation de l'écosystème - DevSecOps

- Technologies à sécuriser : Sécurisation des conteneurs
- Images et registre
- Isolation et sécurité réseau
- Bonnes pratiques : Sécurisation de l'orchestrateur
- Mise en contexte avec Kubernetes
- Contrôle des accès basé sur les rôles (RBAC)
- Projets complémentaires (CNCF)

*Notre **référent handicap** se tient à votre disposition au 01.71.19.70.30 ou par mail à referent.handicap@edugroupe.com pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.*