CLOUD COMPUTING : SECURITE DU CLOUD

Public	À toute personne impliquée dans les domaines ayant trait à la sécurité du cloud computing
Durée	3 jours - 21 heures
Pré-requis	Des connaissances des principes essentiels de la sécurité sont recommandées.
Objectifs	Avec une adoption croissante des technologies cloud computing (informatique en nuage), les problèmes de sécurité sont devenus une réelle préoccupation pour les entreprises. La prise en compte du caractère unique de ces problèmes, dès le début du plan d'implémentation, est le garant d'un investissement pérenne. Cette formation vous apporte une expérience approfondie et pratique de l'identification et de la résolution des problèmes de sécurité des clouds (nuages) publics et privés.
Méthodes pédagogiques	Pour bien préparer la formation, le stagiaire remplit une évaluation de positionnement et fixe ses objectifs à travers un questionnaire. La formation est délivrée en présentiel ou distanciel (e-learning, classe virtuelle, présentiel et à distance). Le formateur alterne entre méthodes démonstratives, interrogatives et actives (via des travaux pratiques et/ou des mises en situation). La validation des acquis peut se faire via des études de cas, des quiz et/ou une certification. Cette formation est animée par un consultant-formateur dont les compétences techniques, professionnelles et pédagogiques ont été validées par des diplômes et/ou testées et approuvées par l'éditeur et/ou par Audit Conseil Formation.
Moyens techniques	1 poste de travail complet par personne De nombreux exercices d'application Mise en place d'ateliers pratiques Remise d'un support de cours Passage de certification(s) dans le cadre du CPF Remise d'une attestation de stage
Modalité d'évaluation des acquis	Evaluation des besoins et objectifs en pré et post formation Evaluation technique des connaissances en pré et post formation Evaluation générale du stage
Délai d'accès	L'inscription à cette formation est possible jusqu'à 5 jours ouvrés avant le début de la session
Accessibilité handicapés	Au centre d'affaires ELITE partenaire d'ACF à 20 m. Guide d'accessibilité à l'accueil.

LES FONDAMENTAUX DU CLOUD COMPUTING

- Les modèles de services du cloud computing :Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS)
- Public
- Privé
- Privé virtuel
- Hybride
- Définir les principes de base de la cybersécurité

GÉRER LES RISQUES DANS LE CLOUD

- Répartir responsabilité et visibilité operationnelles
- Conserver la responsabilité de la sécurité des informations
- Gérer l'authentification et l'autorisation des utilisateurs

VÉRIFIER LES EXIGENCES DE SÉCURITÉ AVEC LES FOURNISSEURS

- Identifier les mesures de sécurité nécessaires
- Définir un accord de niveau de service (SLA)
- Veiller à ce que les SLA répondent aux exigences de sécurité de l'entreprise

SÉCURISER LA PLATE-FORME

- Restreindre l'accès au réseau via des groupes de sécurité
- Configurer un contrôle d'accès utilisateur spécifique à la plate-forme
- Intégrer des systèmes d'authentification/authorisation pour le cloud

COMPARTIMENTER L'ACCÈS POUR PROTÉGERLA CONFIDENTIALITÉ DES DONNÉES

- Securiser les données en mouvement ou au repos
- Identifier le périmètre de sécurité
- Concevoir des architectures cloud résilientes

VERROUILLAGE DE SERVEURS CLOUD

- Scanning for and patching vulnerabilities
- Controlling and verifying configuration management

EXPLOITER LES OPTIONS DE SÉCURITÉ SELON LE FOURNISSEUR

- Définir les groupes de sécurité pour contrôler l'accès
- Filtrer le trafic par numéro de port
- Sélectionner une des options de chiffrement du fournisseur
- Protéger les données archivées

PRENDRE EN CHARGE L'INTÉGRALITÉ DE LA CYBERSÉCURITÉ

- Gérer les risques des clouds publics
- Identifier et attribuer des tâches liées à la sécurité dans chaque modèle de service : SaaS, PaaS, IaaS

CHOIX DU PRODUIT LE MIEUX ADAPTÉ

- Comparer les fonctionnalités de sécurité spécifiquesà chaque produit
- Prendre en compte les exigences d'implémentation

VPC (VIRTUAL PRIVATE CLOUD)

- Simuler un cloud privé dans un environnement public
- Google Secure Data Connector
- Amazon VPC

L'ALTERNATIVE DU CLOUD HYBRIDE

- Connecter les données locales aux applications cloud
- Pontage sécurisé avec VPC
- Augmenter la capacité de manière dynamique afin de répondre à une forte augmentation des besoins

GESTION DE LA GOUVERNANCE DU CLOUD

- Conserver la responsabilité de l'exactitude des données
- Vérifier l'intégrité des données stockées et transmises
- Faire preuve d'attention et de diligence

CONFORMITÉ AUX CERTIFICATIONS ET RÉGLEMENTATIONS

- HIPAA
- Sarbanes-Oxley
- Data Protection Act
- PCI DSS
- Suivre les normes d'audit des systèmes d'information
- Permettre l'audit des données et des processus

METTRE EN OEUVRE UN PLAN POUR MAINTENIR LA DISPONIBLITÉ

- Répartir les données à travers le cloud pour garantir disponibilité et performance
- Addressing data portability and interoperability for a change in cloud providers

OPTIONS EFFICACES DE REPRISE APRÈS SINISTRE DANS LE CLOUD

- Atteindre les objectifs de durée pour la reprise
- Utiliser la redondance pour mieux résister aux attaques DoS

NOUS CONTACTER

Siège social
16, ALLÉE FRANÇOIS VILLON
38130 ÉCHIROLLES

Téléphone
04 76 23 20 50 - 06 81 73 19 35

Suivez-nous sur les réseaux sociaux, rejoignez la communauté !

ACF Audit Conseil Formation

@ACF_Formation

Dernière mise à jour : 03/04/2020