Professional Cloud Security Manager

Durée: 3 Jours **Réf de cours: GKPCS** **Version: 1.0**

Résumé:

Le Cloud Computing connaît une adoption croissante chez les grands comptes, mais aussi chez les PME et TPE, qui n'hésitent plus, parfois, à y déverser des données sensibles. Or, la prudence reste pourtant de mise.

En effet, quels que soient tous les avantages qu'une entreprise tire du cloud computing, l'actualité montre que les organisations sont souvent victimes de failles de sécurité interne ou externe, dont les dommages vont jusqu'à sa fermeture. Pour cette raison, toute démarche de Cloud doit faire appel aux concepts de la Gouvernance et mettre l'accent sur la sécurité.

Ainsi, cette formation propose une démarche de la gestion de la sécurité et des risques qui englobe aussi bien une approche technique, métier, que légale. L'accent est mis sur la gouvernance pour une vision globale de la sécurité de la gestion des risques.
De nombreuses études de cas alimentent la formation et permet la mise en pratique des concepts étudiés.
Financement : Cette formation est éligible à l'action collective Fafiec CLOUD

Public visé:

Cette formation s'adresse aux Professionnels de la Gouvernance, de la gestion des risques et de la conformité, aux Spécialistes de l'audit et de la conformité informatique, aux Professionnels de la sécurité informatique et du cloud computing.

Objectifs pédagogiques:

- Les différents concepts traités au sein des différents modules de cours :
- 1. Le concept de sécurité et de gouvernance dans le cloud computing
- 2. Les menaces et les défis de sécurité dans le cloud computing
- 3. la sécurité physique et son impact dans le cloud computing
- 4. la gestion et la sécurisation de la virtualisation dans le cloud
- 5. les aspects de sécurité résolus IT grâce au cloud
- 6. les aspects de sécurité introduits et créés par le cloud
- 7. les standards et modèles de référence de sécurité existants
- 8. identification de l'écart de votre architecture métier et informatique concernant la sécurité dans le cloud
- 9. la gestion des risques cloud
- 10. la gouvernance la sécurité informatique
- 11. monitoring : utilisateurs des systèmes
- 12. gestion des contrats : termes et conditions
- 13. contrôle légaux, propriété intellectuelle et protection des données personnelles

Pré-requis:

Posséder le niveau de connaissances contenu dans le cours GKCVE.

Test et certification

Contenu:

Introduction

- Introduction : rappel des définitions et des caractéristiques du Cloud Computing
- Comment sécuriser les différents modèles de service et de déploiement du cloud computing
- Expliquer comment concevoir une infrastructure, des configurations et des applications sécurisées dans un environnement de cloud computing
- Expliquer, appliquer et analyser comment gérer l'accès du cloud computing en utilisant des comptes, des utilisateurs et des groupes
- Expliquer, appliquer et analyser les différentes manières de sécuriser les données, le système d'exploitation et les applications dans une infrastructure globale de cloud computing

Gouvernance, sécurité et risques

- Expliquer le concept de gouvernance, de risque et de conformité
- Décrire et expliquer le concept sous-jacent de CIA
- Expliquer et mettre en œuvre des plans de traitement des risques et de mitigation dans le cloud
- Expliquer les risques et les impacts du cloud en termes de défis de sécurité à relever aussi bien pour le métier que la technique, et leur effet sur la politique et la gouvernance métier et technique
- Identifier les terminologies utilisées pour décrire les menaces et les questions de sécurité en ce qui concerne le cloud computing

Menaces et défis de sécurité pour le cloud computing

- Comprendre et expliquer les différences entre gouvernance, la gestion des risques et la conformité dans une informatique traditionnelle et pour le cloud computing
- Expliquer les différences entre la sécurité et la conformité pour le cloud computing
- Expliquer et mettre en œuvre un modèle de sécurité et de conformité partagé
- Expliquer les risques et les impacts du cloud computing aussi bien en termes de défis de sécurité pour le métier que pour la technique, et leurs effets sur la politique et la gouvernance métier

Gestion de la sécurité dans le Cloud, application à la virtualisation

- Expliquer le concept de classification des données et de son importance dans le Cloud.
- Expliquer l'importance d'utiliser un framework d'entreprise de gestion des identités et des accès
- Expliquer la gestion d'accès sous-jacente
- Expliquer les avantages de la gestion des identités et des accès (IAM), y compris l'automatisation des processus et rationalisation des interactions entre des utilisateurs et les services cloud
- Expliquer et mettre en œuvre la gestion des identités et des accès dans le cloud
- Expliquer les risques et les impacts des protections de données à l'utilisation, au repos et en transit
- Expliquer les types d'implémentations de sécurité réutilisés pour sécuriser les données dans le cloud

Les aspect légaux, contractuels et de monitoring opérationnel

- Expliquer les concepts de paysage légal et réglementaire dans le Cloud.
- Expliquer les défis juridiques dans le Cloud.
- Expliquer et mettre en œuvre les mesures d'atténuation liées aux éléments juridiques clés dans le cloud.
- Expliquer les risques et les opportunités de surveillance des services dans le cloud.
- Identifier les terminologies utilisées pour décrire les menaces et les problèmes de sécurité, en particulier celles liées au cloud computing.

La sécurité du réseau dans le Cloud

- Les concepts de base de la sécurité du réseau
- La gestion des vulnérabilités et la conception d'architecture sécurisée des services de cloud computing
- Prise de conscience de la gestion de la vulnérabilité et la conception d'architecture sécurisée des différents acteurs du cloud computing

Business Continuity

- Expliquer le concept de continuité métier (la business continuity, BC), et de recouvrement après désastre (disaster recovery, DR)
- Expliquer les défis de la BC et DR
- Expliquer comment mettre en œuvre dans le cloud une BC et un DR
- Expliquer les risques et les opportunités en utilisant des solutions de BC et DR dans le cloud
- Expliquer le concept de planification de la capacité et de la performance dans le cloud

La sécurité dans la virtualisation, Les containers

- Gestion des accès (rôles) et de l'authentification.
- Définir des serveurs ESX pour des tâches différentes et des niveaux de sécurité différents.
- Sécurité de la persistance « Storage ».
- Sécuriser la console.
- Séparation des tâches entre les administrateurs.
- Mettre à jour les composants.
- Sécuriser les réseaux physiques et virtuels.
- Mettre place une infrastructure de journalisation et de surveillance adéquate.
- Implanter une solution de sécurité qui tire profit de VMSafe ou l'équivalent.
- Durcir et protéger les VM elles-mêmes.
- Balayer les environnements virtuels avec des scanners de vulnérabilité.

Perspectives

- Panorama des dernières études en sécurité, perspectives, avancées, émergence de standards de sécurité pour le Cloud

Méthodes pédagogiques :

Support de cours en français remis aux participants.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
• Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

•Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
•Votre place sera confirmée à la réception d'un devis ou ""booking form"" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
•Attention, si vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.