Professional Cloud Security Manager

Formation Informatique / Bureautique /

OBJECTIFS

- Les différents concepts traités au sein des différents modules de cours :1.
- Le concept de sécurité et de gouvernance dans le cloud computing2.
- Les menaces et les défis de sécurité dans le cloud computing3. la sécurité physique et son impact dans le cloud computing4.
- la gestion et la sécurisation de la virtualisation dans le cloud5. les aspects de sécurité résolus IT grâce au cloud6. les aspects de sécurité introduits et créés par le cloud7.
- les standards et modèles de référence de sécurité existants8. identification de l'écart de votre architecture métier et informatique concernant la sécurité dans le cloud9.
- la gestion des risques cloud10. la gouvernance la sécurité informatique11. monitoring : utilisateurs des systèmes12. gestion des contrats : termes et conditions13.
- contrôle légaux, propriété intellectuelle et protection des données personnelles

PUBLIC

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

PRE-REQUIS

Les stagiaires doivent avoir suivi le module CCC cloud Technology Associate, avec un centre d'examen et un formateur accrédité par l'EXIN.

PROGRAMME

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 informatiques traditionnelles et pour le cloud computing
- Expliquer les différences 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 en termes de défis de sécurité pour le métier que la technique, et leurs effets sur la politique et la gouvernance métier technique
- **Gestion de la sécurité dans le Cloud, application à la virtualisation**
- Expliquer le concept de classification des données et de son importance dans les nuages.
- 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 des services cloud
- Expliquer et mettre en œuvre la gestion des identités et d'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

A retenir

Durée : **3 jours** soit 21h.
Réf. **CYPCS**

01 42 93 52 72

Dates des sessions

Paris
14/05/2018
12/11/2018

Cette formation est également proposée en formule INTRA-ENTREPRISE.

Inclus dans cette formation

Coaching Après-COURS

Pendant 30 jours, votre formateur sera disponible pour vous aider. CERTyou s'engage dans la réalisation de vos objectifs.

100% SATISFACTION GARANTIE

Votre garantie 100% SATISFACTION

Notre engagement 100% satisfaction vous garantit la plus grande qualité de formation.

- 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 ceux liés 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 serré.
- 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.
- Effectuer le durcissement de l'environnement virtuel.
- Balayer les environnements virtuels avec des scanneurs de vulnérabilité régulièrement.

Perspectives

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

Horaires, Planning et Déroulement de cette formation

Horaires

• Formation de 9h00 (9h30 le premier jour) à 17h30.
• Deux pauses de 15 minutes le matin et l'après-midi.
• 1 heure de pause déjeuner

DEROULEMENT

• Les horaires de fin de journée sont adaptés en fonction des horaires des trains ou des avions des différents participants.
• Une attestation de suivi de formation vous sera remise en fin de formation.
• Cette formation est organisée pour un maximum de 14 participants.

PROCHAINES FORMATIONS

PRINCE2 Foundation
PRINCE2 Foundation et PRINCE2 Practitioner

Retrouvez cette formation sur notre site :
Professional Cloud Security Manager