Professional Cloud Security Manager (PCS)

Évaluer les risques liés à l'utilisation d'une solution Cloud

Présentiel ou en classe à distance

Durée : 3 jours (21 h)

Réf. : CC102

Prix inter : 2.490,00 € HT

La formation Professional Cloud Security Manager (PCS) de CCC (Cloud Credential Council) permet d'explorer les concepts liés à la sécurité, au risque et à la mise en conformité dans un environnement Cloud. A l'occasion de ces 3 journées, les participants identifieront les risques liés au Cloud Computing, notamment sur l'activité de l'entreprise ou de l'organisation, et mesureront l'impact éventuel d'une sécurité mal assurée. Ils acquerront ensuite les connaissances nécessaires à la mise en sécurité d'une solution de Cloud Computing.

Les objectifs de la formation

- Être capable d'appliquer les meilleures pratiques de règles de gouvernance et de sécurité
- Comprendre comment sécuriser les différents services Cloud et les modèles de déploiement
- Pouvoir expliquer le design sécurité au regard de l'infrastructure, des configurations et des applications
- Savoir gérer l'accès aux ressources Cloud
- Être en mesure de sécuriser les data, les OS, les applications et l'infrastructure Cloud

A qui s'adresse cette formation ?

Pour qui

- CDO (Chief Digital Office), professionnel sécurité IT, professionnel du risque et de la conformité, auditeur des services Cloud Computing, administrateur/ingénieur réseau, consultant et opérationnel IT

Prérequis

- Connaissances en langue anglaise
- Il est souhaitable d'avoir 5 ans d'expérience dans la sécurité des entreprises et une bonne compréhension des services du Cloud Computing et des modèles de déploiement
- Il est également conseillé d'être certifié Cloud Technology Associate

Programme

1 - Sécurité, risques et gouvernance

- Les concepts
- La gestion de la sécurité IT
- La gouvernance IT
- La sécurité du Cloud Computing
- Implémentation des traitements et mitigations de risque Cloud
- Les impacts business et techniques sur la politique de gouvernance

2 - Les menaces de sécurité et les défis

- Différence de gouvernance traditionnelle et Cloud
- Les différences entre la sécurité partagée et le modèle de conformité dans le Cloud
- Les risques et les impacts en termes business et technique et leurs conséquences sur la politique de gouvernance technique : protection/classification des data, modèles de menaces, ISA – SLA - Asset partagés

3 - Gestion de sécurité dans le Cloud

- La classification des données et son importance
- Les risques et les mesures pour réduire les menaces de sécurité
- La confidentialité et la gestion/implémentation des identités (IAM)
- Les problématiques d'accès, de confidentialité, de risque et de conformité
- Les modèles de services et de déploiement qui impactent la valeur business

4 - Légal, contractuel et monitoring opérationnel dans le Cloud

- Concepts
- Les défis
- Implémentation des mitigations liées aux éléments clés légaux
- Risques et opportunités des services monitorés Cloud

5 - Gestion du réseau de sécurité dans le Cloud

- La gestion de la vulnérabilité et l'architecture sécurité au regard du Cloud et de son rôle
- SDN
- NVS
- Les avantages de la virtualisation, la gestion Patch et les tests de pénétration

6 - Continuité du business, restauration de désastre et planning de performance et de capacité

- Concepts de la continuité business (BC) et de la restauration du désastre (DR)
- Les défis
- L'implémentation de la capacité dans le BC et DR
- Les risques et opportunités
- Le concept de la planification de la Capacité et de la Performance

7 - Pratiques de gestion de sécurité Cloud avancée

- Spécificité sur les enjeux de la gouvernance et de la sécurité sur un modèle PaaS
- Prise de conscience des enjeux de sécurité et de gouvernance pour concevoir et gérer les systèmes PaaS
- Développement standard
- Sécurité API

8 - Planning de sécurité, standards et évolution du Cloud

- Process de sécurité et enjeux des softwares
- Application et services opérés dans le Cloud
- Planning
- Contrôle, audit et évolution de la sécurité du Cloud

Evaluation

- Cette formation fait l'objet d'une évaluation formative.

Les points forts de la formation

- Une pédagogie active et variée : 40% du temps de la formation est dédié à la pratique avec des discussions, partages d'expériences et études de cas sur une plate-forme dédiée sur internet (Work-Labs).
- La formation est en langue française, le support est en langue anglaise.
- La qualité d'une formation officielle de Cloud Credential Council.

Dates et villes 2024 - Référence CC102

A distance

du 3 juin au 5 juin	du 18 sept. au 20 sept.	du 4 déc. au 6 déc.