Certification professionnelle de l'ingénieur en sécurité du cloud

Objectifs

- 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

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'avoir suivi la formation "Cloud Technology Associate (CTA)" (CC100) et 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