Tél : +352 27 39 351
Fax : +352 27 39 52 68
Email : formation@oxiane.lu

Certified Cloud Security Professional

Les services de Cloud Computing sont de plus en plus prisés par les entreprises de toutes tailles. Réactivité, service à la demande, connectivité, disponibilité, souplesse, mobilité sont des bénéfices auxquels adhèrent les décideurs et les utilisateurs. La gamme des offres disponibles est étoffée (fonctions commerciales, ressources humaines, finance, gestion de projet, opérations, infrastructures et développements informatiques, gestion documentaire, outils collaboratifs). Les aspects sécurité doivent être intégrés à différentes étapes : rédaction des cahiers des charges, choix des solutions, conception des architectures, examen des clauses contractuelles, conformité légale, mise en œuvre et exploitation du service, interface entre les équipes informatiques internes, gestion des incidents.

Cette formation prépare à la Certification CCSP – Certified Cloud Security Professional.
Pour être titulaire de la certification CCSP, les candidats doivent d'une part réussir l'examen CCSP, d'autre part, disposer de cinq années d'expérience professionnelle en technologies de l'information, dont trois ans en sécurité de l'information, ainsi qu'au moins une année dans un ou plus des six domaines du CCSP Common Body of Knowledge (CBK®) de (ISC).

Détails

- Code : CCSP
- Durée : 4 jours (28 heures)

Public
- Consultants en Sécurité
- Responsable Sécurité

Pré-requis
- Aucune

Objectifs
- Obtenir une vision pointue des offres de Cloud Computing
- Appréhender précisément tous les risques induits par ces services en termes de sécurité de l'information
- Connaître l'ensemble des aspects légaux et de conformité (juridique, niveaux de service, audit, standards…)
- Comprendre la sécurité des plateformes et infrastructures de Cloud Computing
- Comprendre la sécurité des applications

Programme

Exigences et concepts en termes de conception en architecture Cloud computing

- Les concept du Cloud computing
- Les architectures de référence du Cloud computing
- Les concepts de sécurité associés au cloud computing
- Les principes de conception de sécurité du Cloud de Computing
- L'identification des services de cloud computing de confiance

La sécurité des données dans le cloud computing

- Le cycle de vie des données du cloud computing
- Conception et déploiement des architectures de stockage en cloud computing
- Conception et application des stratégies de sécurité des données
- Connaissances et déploiement des technologies de classification et de découverte des données
- Conception et mise en oeuvre des exigences légales de sécurité des données concernant l'identification des informations personnelles (PII)
- Conception et déploiement du Data Rights Management
- Planification et mise en oeuvre des politiques de rétention, de suppression et d'archivage des données
- Conception et déploiement des démarches d'audit, de détection et de démontrabilité

La sécurité des infrastructures et des plates-formes de cloud computing

- Les composants de l'infrastructure du cloud computing
- Evaluation des risques de l'infrastructure du cloud computing
- Conception et planification des contrôles de sécurité
- Conception et déploiement de plan de reprise et de continuité des services et des métiers

La sécurité des applications de cloud computing

- Formation et sensibilisation de la sécurité autour des services du Cloud computing
- Validation et assurance des solutions logicielles du Cloud computing
- Utilisation des logiciels vérifiés, approbation des API
- SDLS : cycle de vie du développement de la sécurité logicielle
- Les architectures applicatives du Cloud computing
- Conception et déploiement d'une solution d'IAM(Identity & Access Management)

Gestion des opérations

- Planification des processus de conception du data Center
- Développement et mise en oeuvre d'une infrastructure physique du Cloud
- Gestion opérationnelle et maintenance d'une infrastructure physique de Cloud computing

- Conception, maintenance et gestion d'une infrastructure logique de Cloud computing
- Conformité avec les normes de type ISO 20000-1 ou des référentiels comme ITIL
- Evaluation des risques d'une infrastructure logique et physique du Cloud Computing
- Collecte et conservation des preuves numériques (forensic)
- Communication avec les parties prenantes

Les exigences légales et la conformité

- Risques et exigences légales d'un environnement de Cloud Computing
- La gestion de la vie privée, diversité des exigences légales en fonction des pays
- Méthodes et processus d'audit d'un environnement de cloud computing
- La gestion des risques au niveau de l'entreprise d'un écosystème cloud computing
- Conception et gestion des contrats, notamment dans le cadre d'une démarche d'externalisation
- Gestion des fournisseurs du Cloud Computing

Modalités

- Type d'action :Acquisition des connaissances
- Moyens de la formation :Formation présentielle – 1 poste par stagiaire – 1 vidéo projecteur – Support de cours fourni à chaque stagiaire
- Modalités pédagogiques :Exposés – Cas pratiques – Synthèse
- Validation :Exercices de validation – Attestation de stages