Sécurité Cloud : avancé

Référence : **SECCLOUD2** Durée : **2 jours** Certification : **Aucune**

CONNAISSANCES PREALABLES

• Il est recommandé d'avoir suivi au préalable la formation SECCLOUD1 - Sécurité Cloud : les fondamentaux ou posséder les connaissances et compétences équivalentes.

PROFIL DES STAGIAIRES

• Consultant en sécurité des systèmes d'information. • Responsable Sécurité des Systèmes d'Information.

OBJECTIFS

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

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique papier ou numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques, de réflexions et de retours d'expérience
- Le suivi de cette formation donne lieu à la signature d'une feuille d'émargement

FORMATEUR

Consultant-Formateur expert Techniques Cybersécurité

METHODE D'EVALUATION DES ACQUIS

- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation de fin de stage adressée avec la facture

CONTENU DU COURS

Jour 1

- Introduction module 2 et rappel sur les certifications CSSP et CCSK
- Sécurité des données : Data Loss Prevention - Chiffrement et autres techniques (FHE, pseudo anonymisation, algorithmes de dispersion, Information Right Management)
- Sécurité des plateformes Cloud et des infrastructures : Software Defined Networking - Segmentation des réseaux Cloud et VXLAN.
- Sécurité des applications : Principes de déploiement (SDLC, STRIDE, DREAD, ISO 27034) - Audits et tests - Failles applicatives (OWASP, CSA Top Threats, API, CVSS) - Gestion des identités et des accès (SAML, OAUTH, OpenID).
- Cas concrets : Déploiement CASB (Cloud Access Security Broker) - Gestion des clés avec le protocole KMIP
- Quizz et correction

Jour 2

- Introduction
- Sécurité des opérations : Conception et sécurité du Datacenter - Durcissement systèmes et réseaux (exemple hardening AWS, gestion des logs, gestion des correctifs, IDPS, SecCM, protocole SCAP) - Administration et exploitation - Réaction aux incidents de sécurité (exemples, processus, investigations numériques)
- Aspects juridiques et conformité : Certifications et homologation (SOC, STAR, SO 15408, SecNumCloud) - Gestion des contrats

- Cas concrets : Réaction à un DDoS - Evaluation d'un niveau de sécurité en utilisant le référentiel Cloud Control Matrix