

Your Cyber INSURANCE



Préparation de la Certification CCSP – 5 Jours Intensifs

Jours	Domaines couverts	Thèmes clés
Jour 1	Cloud Concepts, Architecture & Design (17%)	- Définitions et caractéristiques du cloud (NIST) : on-demand, multi-tenancy, élasticité, etc. - Rôles : CSP, client, partenaire, broker - Modèles de déploiement : public, privé, hybride, communautaire, multi-cloud - Catégories de services : IaaS, PaaS, SaaS - Référentiels d'architecture : CSA, NIST, Well-Architected Framework - Principes de sécurité : Zero Trust, Privacy by Design, Shared Responsibility - Évaluation des fournisseurs : ISO/IEC 27017, PCI DSS, Common Criteria, FIPS 140-2 - Impact des technologies émergentes : AI, IoT, edge, quantum, containers, serverless
Jour 2	Cloud Data Security (20% – domaine le plus pondéré)	- Cycle de vie des données cloud (création → destruction) - Types de données : structurées, non structurées, semi-structurées - Localisation et dispersion des données - Classification, étiquetage et cartographie des données - Technologies de protection : - Chiffrement (au repos, en transit) + gestion des clés - DLP, IRM, Tokenization, Masquage, Hachage - Stratégies de rétention, archivage, suppression sécurisée, Legal Hold - Auditabilité et traçabilité : logs, non-répudiation, chaîne de preuve
Jour 3	Cloud Platform & Infrastructure Security (17%)	- Composants : compute, stockage, réseau, plan de gestion, virtualisation - Conception d'un data center cloud sécurisé : Physique (localisation, HVAC, alimentation) - Logique (partitionnement, accès) - Environnemental (résilience, redondance) - Menaces spécifiques : hyperviseur compromise, attaques sur containers, fuite de mémoire - Contrôles de sécurité : - Sécurité physique/environnementale - Segmentation réseau, micro-segmentation - Authentification/autorisation pour les accès admin - Continuité d'activité : BIA, RTO/RPO, plans DR/BC, tests - Outils : HSM, TPM, NSG, bastion hosts
Jour 4	Cloud Application Security (17%)	- Vulnérabilités courantes : OWASP Top 10, SANS Top 25 - SDLC sécurisé (Waterfall, Agile, DevSecOps) - Méthodologies de test : SAST, DAST, IAST, SCA, Tests fonctionnels & non-fonctionnels, cas d'abus - Composants de sécurité applicative : WAF, API Gateway, DAM, XML Firewall - Gestion des API : authentification, quotas, monitoring - Sécurité de la chaîne d'approvisionnement : - Modèles d'identité : SSO, MFA, Federation, IdP, CASB, gestion des secrets
Jour 5	Cloud Security Operations + Legal, Risk & Compliance (16% + 13% = 29%)	- Déploiement sécurisé de l'infrastructure : IaC (Terraform, CloudFormation) - Durcissement des OS (baselines, patch management) - Surveillance intelligente : SIEM, IDS/IPS, honeypots, UEBA - Opérations : gestion des incidents, forensic cloud, sauvegardes/restauration – Legal, Risk & Compliance - Cadre juridique : GDPR, HIPAA, PCI, SOX, législation par pays - Données privées : PII, PHI, différences contractuelles vs réglementaires - Évaluation des risques cloud : verrouillage fournisseur, juridiction, disponibilité - Audit cloud : SOC 1/2/3, SSAE, ISAE, ISO 27050 (eDiscovery)