

Your Cyber INSURANCE



Préparation de la Certification CISSP – 5 Jours

Jours	Domaines couverts	Thèmes clés
Jour 1 : Fondations Stratégiques & Gestion des Actifs	• Domaine 1 : Security and Risk Management (16%) • Domaine 2 : Asset Security (10%)	• Éthique professionnelle & conformité (GDPR, PCI-DSS, etc.) • Gouvernance, politiques, standards, procédures • Gestion des risques (NIST, ISO, COBIT) & modélisation des menaces • Business Continuity & Disaster Recovery (BIA, RTO/RPO) • Classification des actifs & données (publiques, sensibles, critiques) • Rôles : propriétaire, dépositaire, processeur • États des données (au repos, en transit, en usage) • Contrôles : DLP, DRM, CASB, cycle de vie des données
Jour 2 – Security Architecture & Engineering	• Domaine 3 : Security Architecture and Engineering (13%)	• Principes de conception sécurisée : Zero Trust, Defense in Depth, Least Privilege, Fail Securely • Modèles de sécurité : Bell-LaPadula, Biba, Star Model • Architectures : cloud (IaaS/PaaS/SaaS), IoT, microservices, conteneurs, serverless • Sécurité matérielle : TPM, HSM, mémoire protégée • Cryptographie : symétrique/asymétrique, PKI, gestion des clés • Attaques cryptanalytiques : MITM, side-channel, timing, brute force • Sécurité des sites : data centers, HVAC, alimentation, suppression incendie
Jour 3 – Communication & Network Security + IAM	• Domaine 4 : Communication and Network Security (13%) • Domaine 5 : Identity and Access Management (IAM) (13%)	• Modèles OSI & TCP/IP • Protocoles sécurisés : TLS, IPSec, SSH, SSL • Segmentation : VLAN, micro-segmentation, VPC, SDN • Sécurité sans fil : Wi-Fi, 5G, Bluetooth • NAC, endpoint security, CDN • Authentification : MFA, SSO, passwordless • Fédération : SAML, OAuth, OIDC • Modèles d'accès : RBAC, ABAC, MAC, DAC • Gestion du cycle de vie des identités (onboarding → offboarding) • Comptes privilégiés & revues d'accès
Jour 4 – Security Operations + Assessment & Testing	• Domaine 6 : Security Assessment and Testing (12%) • Domaine 7 : Security Operations (13%)	• Surveillance : SIEM, UEBA, IDPS, logging • Gestion des incidents : détection → remédiation → leçons apprises • Forensique numérique et collecte de preuves • Sauvegardes, DRP, BCP, tests de reprise • Sécurité physique & sûreté du personnel • Tests de vulnérabilité & pentests (red/blue team) • Revue de code (SAST, DAST, SCA) • Audits internes/externes & rapport d'écart • Simulations d'attaques & couverture des contrôles
Jour 5 – Software Development Security + Révision Globale	• Domaine 8 : Software Development Security (10%)	• Intégration de la sécurité dans le SDLC (DevSecOps, Agile) • Bonnes pratiques de codage sécurisé • API sécurisées, gestion des dépendances • Tests applicatifs : SAST, DAST, IAST, SCA • Évaluation des logiciels : COTS, open source, SaaS • Maturité logicielle (SAMM, CMM)