

Your Cyber INSURANCE



Formation CompTIA Security+ 5 Jours

Jours	Domaines	Contenu de la Journée
Jour 1	Concepts généraux de sécurité (12%)	• Types de contrôles de sécurité (préventif, détectif, correctif...) • Concepts fondamentaux : CIA, Zero Trust, least privilege • Importance de la gestion du changement • Usage approprié des solutions cryptographiques
Jour 2	Menaces, vulnérabilités et atténuation (22%)	• Typologie des acteurs de menace et leurs motivations • Vecteurs de menace et surfaces d'attaque (email, web, IoT...) • Types de vulnérabilités (logiciels, réseaux, humains) • Analyse d'indicateurs d'activités malveillantes (scénarios) • Techniques d'atténuation pour sécuriser l'entreprise
Jour 3	Architecture de sécurité (18%)	• Comparaison des modèles d'architecture et leurs impacts • Application des principes de sécurité à l'infrastructure • Stratégies de protection des données (DLP, chiffrement, classification) • Importance de la résilience et des plans de récupération
Jour 4	Opérations de sécurité (28%)	• Techniques de sécurité à appliquer sur les ressources informatiques • Gestion du matériel, des logiciels et des données • Gestion des vulnérabilités (scans, priorisation, remédiation) • Outils de surveillance et d'alerting • Identity & Access Management (IAM) • Automatisation et orchestration dans les opérations • Activités de réponse aux incidents • Utilisation des sources de données pour enquêtes
Jour 5	Gestion & supervision du programme de sécurité (20%)	• Éléments d'une gouvernance efficace • Processus de gestion des risques • Gestion des risques liés aux tiers • Principes de conformité • Audits et évaluations • Pratiques de sensibilisation à la sécurité