DAWAN

Plan de la formation

www.dawan.fr

Formation Préparation à la Certification CISSP (Information Systems Security Professional)

Durée :	5 jours (35 heures)
Tarifs inter-entreprise :	3 775,00 € HT (standard) 3 020,00 € HT (remisé)
Public :	RSSI, DSI, consultants, auditeurs, administrateurs systèmes et réseaux
Pré-requis :	Expérience significative en sécurité des systèmes d'information recommandée (conformément aux prérequis CISSP)
Objectifs :	Connaître les domaines et rubriques du CISSP Common Body of Knowledge (CBK®) - Maîtriser les fondamentaux de la sécurité des systèmes d'information dans les 8 domaines du CBK - Se préparer efficacement à l'examen de certification CISSP
Modalités pédagogiques, techniques et d'encadrement :	• Formation synchrone en présentiel et distanciel. • Méthodologie basée sur l'Active Learning : 75 % de pratique minimum. • Un PC par participant en présentiel, possibilité de mettre à disposition en bureau à distance un PC et l'environnement adéquat. • Un formateur expert.
Modalités d'évaluation :	• Définition des besoins et attentes des apprenants en amont de la formation. • Auto-positionnement à l'entrée et la sortie de la formation. • Suivi continu par les formateurs durant les ateliers pratiques. • Évaluation à chaud de l'adéquation au besoin professionnel des apprenants le dernier jour de formation.
Sanction :	Attestation de fin de formation mentionnant le résultat des acquis

Référence :	CYB102768-F
Note de satisfaction des participants:	Pas de données disponibles
Contacts :	commercial@dawan.fr - 09 72 37 73 73
Modalités d'accès :	Possibilité de faire un devis en ligne (www.dawan.fr, moncompteformation.gouv.fr, maformation.fr, etc.) ou en appelant au standard.
Délais d'accès :	Variable selon le type de financement.
Accessibilité :	Si vous êtes en situation de handicap, nous sommes en mesure de vous accueillir, n'hésitez pas à nous contacter à referenthandicap@dawan.fr, nous étudierons ensemble vos besoins

Comprendre la structure du CISSP et le domaine Sécurité et gestion des risques

Découvrir le CBK CISSP et les 8 domaines de la certification
Comprendre les principes de gouvernance, de politique de sécurité et de conformité
Aborder les notions de gestion des risques, d'appétence au risque et de responsabilité
Relier les cadres de référence (ISO 27001, NIST, RGPD, etc.) au domaine CISSP
Atelier fil rouge : cartographier les principaux cadres de sécurité utilisés dans son organisation avec le domaine 1 du CISSP

Approfondir la sécurité des assets, l'ingénierie de la sécurité et la sécurité des réseaux

Analyser la classification, la gestion et la protection des actifs (physiques et logiques)
Découvrir les concepts d'architecture et d'ingénierie de la sécurité (modèles, sécurité matérielle, fiabilité)
Étudier la sécurité des télécommunications et des réseaux : protocoles, architectures, zones, technologies de sécurité
Relier ces connaissances aux choix d'architectures sécurisées pour l'entreprise
Atelier fil rouge : analyser une architecture réseau simple et identifier les forces et faiblesses au regard du CBK

Maîtriser la gestion des identités, l'évaluation de la sécurité et la continuité

Comprendre les concepts de gestion des identités et des accès (IAM, authentification, autorisation, fédération)
Explorer les méthodes d'évaluation de la sécurité et de tests (audits, pentests, revues, analyses de vulnérabilités)

Étudier la continuité des opérations et les plans de reprise d’activité
Relier ces notions aux exigences de résilience et de conformité
Atelier fil rouge : construire une mini-carte mentale reliant IAM, tests de sécurité et continuité pour un système critique

Explorer la sécurité du développement logiciel et les autres domaines transverses

Découvrir les principes de sécurité dans le cycle de développement logiciel (SDLC sécurisé, DevSecOps, tests applicatifs)
Aborder les aspects de sécurité physique, de sensibilisation et de formation
Relier les différents domaines CISSP à des cas concrets d’organisation
Identifier les domaines dans lesquels un approfondissement personnel est nécessaire
Atelier fil rouge : analyser un cas d’incident applicatif et relier les failles au domaine “sécurité du développement logiciel”

Construire sa stratégie de préparation à l’examen CISSP

Comprendre le format de l’examen CISSP et les types de questions
Élaborer une stratégie de préparation : planning, ressources, supports, banques de questions
S’entraîner sur un ensemble de questions types couvrant les 8 domaines
Identifier ses points forts et axes de progrès pour optimiser sa préparation
Atelier fil rouge final : simulation d’une mini-session d’examen et plan de révision personnalisé