Qu'est-ce que la certification CC de l'(ISC)² ?

La certification CC (Certified in Cybersecurity) est délivrée par l'(ISC)² organisme américain bien connue dans le monde de la cybersécurité pour sa certification phare CISSP. Comme le programme de la certification CC est un sous-ensemble de la certification CISSP, c'est donc un excellent moyen d'obtenir une première certification en cybersécurité et de se préparer à l'obtention future du CISSP.

Conscient de l'énorme déficit de main-d'œuvre en Cybersécurité, l'(ISC)² a lancé en septembre 2022 le programme **One Million Certified in Cybersecurity**. Ainsi le 1er passage de l'examen CC est gratuit tant que le seuil d'un million de personnes certifiées dans le monde n'est pas atteint. Attention en cas d'échec au 1er passage, les autres tentatives seront facturées 222 € par l'(ISC)².

Formateur

Boris Motylewski est ingénieur de formation et expert judiciaire en cybercriminalité à la cour d'appel de Montpellier. Il a fondé et dirigé la société ExperLAN, SSII spécialisée dans la sécurité des SI (rachetée par Thalès) puis la société Axiliance, éditeur du pare-feu Web RealSentry (rachetée par Beeware). Il a cofondé la société Securiview, spécialisée dans la détection et remédiation des incidents de sécurité (rachetée par Linkbynet en janvier 2018). Il dirige aujourd'hui la société Verisafe spécialisée dans la Cybersécurité. Conférencier depuis 1995, Boris Motylewski a formé à ce jour plus de 10 000 professionnels de l'IT (RSSI, DSI, experts cybersécurité, chefs de projet, ingénieurs, auditeurs, consultants, enquêteurs de police judiciaire, DPO, etc…).

A qui s'adresse cette formation ?

Cette formation s'adresse à toute personne désireuse d'acquérir de solides connaissances en matière de cybersécurité et de les valoriser par l'obtention d'une certification internationalement reconnue. Elle concerne en particulier les RSSI, auditeurs, experts cybersécurité et consultants. Elle s'adresse également à toute personne du monde de l'IT et du digital souhaitant se reconvertir dans la Cybersécurité (Architectes, chefs de projets, administrateurs IT, DPO, DBA, développeurs, etc…).

Prérequis pour suivre cette formation

Des connaissances générales sur les systèmes, les réseaux informatiques et la sécurité de l'information sont nécessaires pour suivre cette formation avec les meilleures chances de succès. Pour vous en assurer, vous pouvez évaluer vos connaissances sur notre site à l'adresse suivante : https://www.verisafe.fr/qsm_quiz/evaluation-des-prerequis-formation-pcc

Examen CC & prérequis pour la certification CC

L'examen CC est en anglais et se déroule en centre de test Pearson Vue. L'examen est un QCM de 100 questions à réaliser dans un délai maximal de 2 heures. Pour réussir, le candidat doit obtenir un score minimal de 700 points / 1000. Contrairement à la certification CISSP, aucun prérequis n'est demandé par l'(ISC)² pour obtenir la certification CC.

Objectifs pédagogiques

Le principal objectif de cette formation est de disposer de toutes les connaissances nécessaires pour réussir l'examen de certification CC de l'(ISC)^2 dès le 1er essai.

Pour cela, la formation VERISAFE a été spécialement conçue pour atteindre 3 objectifs :

- Adopter la bonne méthode pour faciliter la mémorisation et optimiser sa préparation
- Maîtriser parfaitement les 5 domaines du programme officiel
- Evaluer de manière précise et objective le niveau atteint par rapport au niveau attendu pour réussir l'examen

Méthodes pédagogiques

Présentation magistrale avec analyse technique et déclinaison opérationnelle de tous les points identifiés dans le programme et illustrations concrètes avec de nombreux exemples réels.

En complément des modules vidéos, les participants peuvent consulter en ligne le support de cours (420 slides) comprenant l'ensemble des diapositives utilisées pour l'animation des différentes sessions vidéos.

Nous recommandons fortement aux participants d'utiliser le forum de la plateforme dédié à la certification CC pour échanger sur les différents sujets du programme d'étude.

Afin de **réussir l'examen dès le 1er essai**, nous avons développé une **offre unique** basée sur **10** éléments :

- Formation conçue et animée par Boris Motylewski (Expert en cybersécurité depuis plus de 25 ans)
- QCM de positionnement initial en début de formation pour définir la bonne stratégie d'apprentissage
- Support de cours en français (420 diapositives)
- Dictionnaire de 400 sigles et acronymes Anglais / Français (PDF)
- Glossaire de 500 termes et expressions Anglais / Français (PDF)
- Apprentissage progressif avec contenu pédagogique disponible pendant un an (24h/24 - 7j/7)
- Plus de 60 vidéos HD en français
- Examen blanc en anglais dans des conditions identiques à l'examen officiel
- Forum communautaire entièrement dédié à la préparation de la certification CC

Durée

Cette formation est réalisée en sessions de formation ouverte à distance (FOAD) également appelé e-learning ou distanciel. La durée de la formation (hors travail personnel) est de 13 heures (test de positionnement : 1h, vidéos : 10h, examen blanc : 2h).

Evaluation des acquis & certification

En fin de formation, les participants peuvent vérifier leur niveau de préparation avec un examen blanc qui se déroule dans des conditions identiques à l'examen CC officiel.
L'examen blanc portent sur l'ensemble du programme CC actuellement en vigueur.
Un certificat Verisafe attestant les connaissances acquises est délivré à toute personne ayant obtenu un score supérieur ou égal à 70%.

Préparation à la certification CC

➢ La seule formation en 🇫🇷 pour préparer et réussir la certification **C**ertified in **C**ybersecurity

Cette formation traite en détail les 5 domaines du programme officiel de la certification CC de l'(ISC)^2 actuellement en vigueur.

Introduction : Préparation à l'examen CC

- La certification CC de l'(ISC)^2
- Les différences entre les certifications CC et CISSP
- Inscription et passage de l'examen
- Évaluation des connaissances initiales (QCM 50 questions - 1h)
- Analyse des résultats & stratégie d'apprentissage

Domaine 1 : Principes de sécurité

- La triade CID (Confidentialité, Intégrité et Disponibilité)
- Identification, authentification, autorisation et journalisation (IAAA)
- Les 3 types d'authentification et l'authentification MFA
- Le principe de défense en profondeur
- Vocabulaire et fondamentaux de la gestion du risque
- Le traitement du risque
- Le processus de gestion du risque
- Le code d'éthique de l'(ISC)^2
- La gouvernance de la sécurité
- Politiques, normes, directives et procédures de sécurité
- Les différentes catégories de Lois (pénal, civil, administratif)

Domaine 2 : Continuité / reprise d'activités et réponse aux incidents

- Introduction à la continuité et reprise d'activité
- Terminologie, définitions et principes de BC/DR
- Bilan d'impact sur l'activité (BIA)
- Stratégies BC/DR
- Sauvegarde des données
- Réponse aux incidents

Domaine 3 : Concepts de contrôle d'accès

- Principes généraux pour assurer la sécurité physique
- Prévention, détection et extinction des incendies
- Sécurité des accès physiques
- Séparation des taches, moindre privilège et besoin d'en connaître
- Terminologie et principes fondamentaux du contrôle d'accès
- Les différents types de contrôle d'accès (MAC, RBAC, ABAC,…)

Domaine 4 : Sécurité réseau

- Généralités sur les réseaux et modèle de référence OSI
- L'architecture TCP/IP
- Protocole IP et adressage IP v4 / v6
- Les principaux protocoles applicatifs dans l'architecture TCP/IP
- Les réseaux Wi-Fi et les normes IEEE 802.11
- Attaques DoS et DDoS
- Autres techniques d'attaques
- Attaques par ingénierie sociale
- Firewalls et protection périmétrique
- Isolation des réseaux avec les VLANs
- Contrôle d'accès réseau (NAC)
- Le cloud computing

Domaine 5 : Opérations de sécurité

- Notions fondamentales de cryptographie
- Cryptographie symétrique
- Cryptographie asymétrique
- Fonctions de hachage & signature numérique
- Les infrastructures à clé publique (PKI)
- Cycle de vie des données (classification, destruction, conservation)
- Journalisation des évènements de sécurité
- Les vulnérabilités logicielles et leur exploitation
- Le cycle de vie d'une vulnérabilité et la gestion des correctifs
- Sensibilisation et formation à la sécurité

Examen blanc

- Examen blanc de 100 questions en anglais à réaliser dans des conditions identiques à l'examen officiel (2h).
- Tous nos QCM sont des questions originales développées spécifiquement par VERISAFE pour cette formation.

Le résultat de l'examen blanc comprend un score détaillé domaine par domaine afin de bien identifier vos points forts et surtout vos points faibles !