AVANCÉ

FORMATION CERTIFIANTE

CERTIFIED CYBERSECURITY TECHNICIAN

Apprenez les compétences de base essentielles dans 4 disciplines : la défense des réseaux, le piratage éthique, l'investigation numérique et les opérations de sécurité

Code : CCT

Le C|CT est un programme de cybersécurité pour les nouveaux professionnels de la cybersécurité, conçu par EC-Council, pour répondre aux besoins et à la demande mondiale de techniciens en cybersécurité possédant de solides compétences de base. Le C|CT est axé sur la pratique, avec plus de 50 % du temps de formation consacré aux laboratoires. La certification C|CT d'EC-Council plonge les étudiants dans un transfert de connaissances bien structuré.

Cette formation s'accompagne de tâches de réflexion critique et d'exercices de laboratoire immersifs qui permettent aux candidats d'appliquer leurs connaissances et de passer à la phase de développement des compétences. Le programme propose une approche multidimensionnelle qui intègre la défense des réseaux, le hacking éthique et les opérations de sécurité afin de garantir que les titulaires de la certification disposent d'une formation solide et complète leur permettant de configurer, d'analyser et d'identifier les problèmes au sein d'une organisation.
À l'issue du programme, les professionnels certifiés C|CT disposeront d'une base solide dans les principes et techniques de cybersécurité, ainsi que d'une exposition pratique aux tâches requises dans des postes de travail réels.

PROGRAMME

Méthodes mobilisées : cette formation est construite avec une alternance de cours théoriques et de cas pratiques afin de favoriser l'acquisition des savoirs du programme (cf. Ressources).

Modalités d'évaluation : les objectifs sont régulièrement évalués tout au long de la formation (50% exercices pratiques : labs) et formalisés par le passage de la certification.

PLAN DE COURS

- **Module 1 :** Information Security threats and vulnerabilities
- **Module 2 :** Information Security attacks
- **Module 3 :** Network Security fundamentals
- **Module 4 :** Identification, authentification and authorization
- **Module 5 :** Network Security controls: administrative controls
- **Module 6 :** Network Security controls: physical controls
- **Module 7 :** Network Security controls: technical controls
- **Module 8 :** Network Security assessment techniques and tools
- **Module 9 :** Application Security
- **Module 10 :** Virtualization and cloud computing
- **Module 11 :** Wireless Network Security
- **Module 12 :** Mobile Device Security
- **Module 13 :** Internet of Things (IoT) and Operationnal Technology (OT) Security
- **Module 14 :** Cryptography
- **Module 15 :** Data Security
- **Module 16 :** Network Troubleshooting
- **Module 17 :** Network Traffic Monitoring
- **Module 18 :** Network Log Monitoring and Analysis
- **Module 19 :** Incidence Response
- **Module 20 :** Computer Forensics
- **Module 21 :** Business Continuity and Disaster Recovery
- **Module 22 :** Risk Management

PASSAGE DE L'EXAMEN

L'examen CCT 212-82 aura lieu à distance.

- **Titre de l'examen :** Certified Cybersecurity Technician
- **Format de l'examen :** QCM
- **Nombre de questions :** 60
- **Durée :** 3 heures
- **Langue :** anglais
- **Score requis :** 70% minimum de bonnes réponses.

RÉSULTAT

Directement disponible en fin d'examen.

MAINTIEN DE LA CERTIFICATION

Pour maintenir la certification, il faudra obtenir 120 crédits dans les 3 ans avec un minimum de 20 points chaque année. Pour plus d'informations, vous pouvez consulter le site d'EC-Council.

PROCHAINES DATES

24 mars 2025
23 juin 2025
25 août 2025
27 octobre 2025

INFORMATIONS GÉNÉRALES

Code : CCT
Durée : 5 jours
Prix : 2 990 € HT
Horaires : 9h30 - 17h30
Lieu : Levallois (92)
ou en distanciel
Examen : inclus.
Valable 12 mois pour un passage de l'examen à distance.
Les + : petits-déjeuners, pause-café et déjeuners offerts pour les stagiaires en présentiel

OBJECTIFS

- Comprendre les concepts clés de la cybersécurité, y compris la sécurité de l'information et la sécurité des réseaux
- Comprendre les menaces, les vulnérabilités et les attaques en matière de sécurité de l'information, ainsi que les différents types de logiciels malveillants.
- Contrôler la sécurité des réseaux :
  - Contrôles administratifs (cadres, lois, actes, programmes de gouvernance et de conformité, politiques de sécurité)
  - Contrôles physiques (politiques de sécurité physique et sur le lieu de travail, contrôles environnementaux)
  - Contrôles techniques (protocoles de sécurité du réseau, segmentation du réseau, pare-feu, systèmes de détection et de prévention des intrusions…), ainsi que serveurs proxy, VPN, analyse du comportement des utilisateurs, contrôle de l'accès au réseau…
- Connaître :
  - les techniques et outils d'évaluation de la sécurité des réseaux (chasse aux menaces, renseignements sur les menaces, évaluation des vulnérabilités, piratage éthique, tests de pénétration, gestion des configurations et des actifs)
  - Les techniques de conception et de test de la sécurité des applications
  - Les principes fondamentaux de la virtualisation, de l'informatique en nuage et de la sécurité en nuage
  - Les principes fondamentaux des réseaux sans fil, cryptage sans fil et mesures de sécurité connexes
  - Les principes fondamentaux des dispositifs mobiles, IoT et OT et mesures de sécurité connexes
  - La cryptographie et infrastructure à clé publique
  - Les contrôles de la sécurité des données, méthodes de sauvegarde et de conservation des données et techniques de prévention des pertes de données
  - Le dépannage du réseau, la surveillance du trafic et des journaux, et l'analyse du trafic suspect.
  - Le processus de traitement et de réponse aux incidents
  - Les principes fondamentaux de la criminalistique informatique et des preuves numériques
  - Les concepts de continuité des activités et de reprise après sinistre
  - Les concepts, phases et cadres de gestion des risques
- Être préparé(e) à l'examen Certified Cybersecurity Technician

PUBLIC VISÉ

- Professionnels de l'informatique en début de carrière
- Responsables informatique
- Toute personne souhaitant démarrer sa carrière dans la cybersécurité ou ajouter une solide compréhension des techniques et concepts fondamentaux.

PRÉ-REQUIS

Les stagiaires doivent avoir des connaissances de base en cybersécurité, en cloud et en gestion de la sécurité des réseaux

RESSOURCES

- Support de cours officiel en anglais
- Accès au cours en version numérique pendant un an
- Cours donnés en français
- 50% d'exercices pratiques
- 1 PC par personne