Certified Cybersecurity Technician

- **Public visé** : Techniciens et experts sécurité, Techniciens et experts support, Ingénieurs réseau, Analystes en Sécurité, Analystes SOC, Managers IT, Avant-ventes techniques.
- **Méthodes pédagogiques :** Phase d'auto-apprentissage à l'aide des supports officiels d'EC Council (Supports numériques, Labs (exercices pratiques). Théorie, demonstrations, retour d'experience.
- **Accessibilité** : Formation accessible à tout public.
  N'hésitez pas à nous faire part de toutes demandes spécifiques afin que l'on adapte au mieux nos modalités de formation (aménagement des horaires, des lieux, des supports…)
- **Prérequis** : Connaissances informatiques de bases. Maitrise de l'anglais technique pour supports de formation.
- **Evaluation** : Les candidats pourront passer l'examen sur la plateforme ECCexam pour obtenir la certification, le dernier jour de la formation ou ultérieurement. Durée de l'examen: 3h. Nombres de questions : 60 (dont 50 qcm et 10 pratiques). Attestation de formation envoyé aux apprenants à l'issu de la formation. *Le passage de la certification est optionnel.*

Programme détaillé

Jour 1
Module 1: Information Security Threats and Vulnerabilities
Module 2 : Information Security Attacks
Module 3 : Network Security Fundamentals
Module 4 :Identification, Authentication, and Authorization

Jour 2
Module 5 : Network Security Controls Administrative Controls
Module 6 : Piratage de systèmeNetwork Security Controls Physical Controls
Module 7 : Network Security Controls Technical Controls
Module 8 : Network Security Assessment Techniques and Tools

Jour 3
Module 9 : Ingénierie sociale
Module 10 : Denial of Service
Module 11 : Détournement de session
Module 12 : Evading IDS, Firewalls and honeypots

Jour 4
Module 13 : Piratage de serveurs Web
Module 14 : Piratage d'application Web
Module 15 : SQL Injection
Module 16 : Piratage réseaux sans fil
Module 17 : Piratage des plateformes mobiles

Jour 5
Module 18 : IoT hacking et OT hacking
Module 19 : Cloud Computing
Module 20 : Computer Forensics
Module 21 : Business Continuity and Disaster Recovery
Module 22 : Risk Management

Objectifs pédagogique

- Analyser les concepts clés de la cybersécurité, y compris la sécurité de l'information et la sécurité des réseaux, afin de déterminer leur impact sur la protection des données
- Évaluer les menaces, vulnérabilités et attaques en matière de sécurité de l'information pour identifier les risques potentiels dans un environnement donné
- Classer les différents types de logiciels malveillants selon leur fonctionnement et leur impact sur les systèmes informatiques
- Démontrer les processus d'identification, d'authentification et d'autorisation pour sécuriser l'accès aux informations sensibles
- Mettre en œuvre des contrôles de sécurité des réseaux en utilisant des techniques et des outils d'évaluation appropriés pour assurer la protection des infrastructures
- Décrire les protocoles de communication et leur rôle dans la sécurité des réseaux informatiques
- Décrire les principes fondamentaux de la cryptographie et de l'infrastructure à clé publique pour comprendre leur rôle dans la sécurisation des communications

Prix H.T.	Stagiaires	Conditions	Durée	Langue
2 990€ par personne	Groupe de 3 à 10 pers.	Présentiel / Distanciel	35h sur 5 jours	Formateur Francophone