+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Mis à jour le 03/03/2026

S'inscrire

Formation Certification Ec-council CCT

2 jours (14 heures)

Présentation

La formation EC-Council CCT™ vous initie aux fondamentaux du pentest avec une approche structurée et immédiatement applicable. Elle permet de reproduire des scénarios d'attaque réalistes pour détecter, exploiter et documenter des failles dans un cadre maîtrisé.

Vous apprendrez à suivre une démarche complète : reconnaissance, énumération, exploitation, post-exploitation et rédaction. L'objectif est de gagner en autonomie pour analyser une surface d'attaque et prioriser les risques, que ce soit en audit interne, en mission de sécurité ou en montée en compétences SOC.

La formation est centrée sur la pratique : ateliers guidés, démonstrations d'outils, exercices sur environnements de lab. Les livrables incluent des checklists opérationnelles, des commandes types, un modèle de rapport et des recommandations de remédiation.

Objectifs

- Identifier une surface d'attaque et collecter des informations utiles.
- Réaliser l'énumération des services et interpréter les résultats.
- Exploiter des vulnérabilités courantes de manière contrôlée.
- Valider l'impact et proposer des mesures de correction.
- Rédiger un rapport d'audit clair et actionnable.

Public visé

- Administrateurs systèmes et réseaux
- Analystes SOC / Blue Team souhaitant comprendre les techniques d'attaque
- Débutants en cybersécurité orientés pentest
- Chefs de projet sécurité

Pré-requis

- Notions de réseaux (TCP/IP, ports, DNS)
- Bases Linux (shell, permissions, services)
- Compréhension des protocoles courants (HTTP, SSH, SMB)
- Culture sécurité : vulnérabilités, correctifs, durcissement

Pré-requis techniques

- PC avec 8 Go RAM minimum (16 Go recommandé)
- Windows (avec WSL2), Linux ou macOS
- Virtualisation : VirtualBox ou VMware + droits d'installation
- Outils : Kali Linux, navigateur récent, éditeur de code, terminal

Programme de formation Ec-council CCT

[Jour 1 - Matin]

Fondamentaux de la cybersécurité et cadre du CCT

- Positionnement du CCT : rôle, périmètre, responsabilités et limites
- Panorama des menaces : malware, phishing, ransomware, attaques web et réseau
- Concepts clés : CIA, surface d'attaque, vulnérabilité vs menace vs risque
- Bonnes pratiques opérationnelles : hygiène numérique, gestion des mots de passe, MFA, sauvegardes
- Atelier pratique : Cartographier une surface d'attaque simple (poste, réseau, services exposés).

[Jour 1 - Après-midi]

Réseaux, protocoles et analyse de trafic

- Rappels réseau : TCP/IP, ports, DNS, DHCP, NAT, routage et segmentation
- Protocoles à risque et points de contrôle : HTTP(S), SMTP, SMB, RDP, SSH
- Notions de journalisation : logs système, logs réseau, horodatage et corrélation
- Lecture d'indicateurs : connexions anormales, scans, exfiltration, C2
- Atelier pratique : Capturer et interpréter un flux réseau (requêtes DNS/HTTP) pour repérer une activité suspecte.

[Jour 2 - Matin]

Sécurité des systèmes : durcissement et gestion des vulnérabilités

- Durcissement poste/serveur : principes least privilege, services inutiles, pare-feu local
- Gestion des correctifs : cycles de patching, priorisation, validation et rollback
- Comptes et identités : politiques de mots de passe, MFA, gestion des droits et revues d'accès
- Vulnérabilités : CVE, criticité (CVSS), exposition et contexte métier
- Atelier pratique : Établir un plan de remédiation à partir d'une liste de vulnérabilités (priorisation et actions).

[Jour 2 - Après-midi]

Réponse à incident et préparation à la certification

- Cycle de réponse à incident : détection, qualification, confinement, éradication, reprise
- Collecte de preuves : préservation, chaîne de custody, artefacts clés (logs, événements, fichiers)
- Communication et escalade : qui alerter, quoi documenter, décisions rapides et traçabilité
- Contrôles essentiels : sauvegardes, EDR/AV, segmentation, sensibilisation, procédures
- Atelier pratique : Simuler un incident (phishing + compromission) et produire une fiche d'intervention (timeline, actions, recommandations).

FAQ – QUESTIONS / RÉPONSES

Dans quelle langue la formation CCT™ vous est enseignée ?

La formation est en français.

L'examen est-il compris dans le prix de la formation ?

Oui, le prix de la certification est inclus au coût de la formation ($499 à titre indicatif). Vous pourrez passer l'examen à la fin de la session.

Comment se déroule l'examen pour la certification CCT™ ?

L'examen consiste en un QCM basé sur la performance composé de 85 epreuves en Lab

Il s'effectue en ligne dans un centre d'examen agréé Pearson Vue.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d’auto-évaluation nous permettant d’apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d’anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l’acquisition correcte des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.