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

Mis à jour le 03/10/2025

S'inscrire

# Formation CC - Certified in Cybersecurity

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

3 jours (21 heures)

## Présentation

Certified in Cybersecurity (CC) est une certification d'entrée de gamme délivrée par ISC². Conçue pour valider les fondamentaux de la cybersécurité, elle couvre les principes de sécurité, la sécurité réseau, les contrôles d'accès, les opérations et la gestion d'incidents.

Notre formation CC vous permettra de maîtriser les bases opérationnelles : analyse des menaces et vulnérabilités, mise en œuvre de contrôles efficaces, surveillance et réponse aux incidents, ainsi que les notions clés de gouvernance et de conformité.

Vous apprendrez à appliquer les bonnes pratiques sur les réseaux, les systèmes et les applications, à interpréter les journaux et à prioriser les actions correctives. La formation alterne apports théoriques et ateliers pratiques et se conclut par un examen blanc complet corrigé.

À l'issue de la formation, vous serez en mesure d'aborder l'examen officiel avec méthode, de consolider vos acquis sur chaque domaine du CC et de bâtir un plan de progression.

Comme toutes nos formations, celle-ci s'appuie sur la dernière version stable du référentiel ISC² et une approche résolument pratique et opérationnelle.

## Objectifs

- Comprendre les fondamentaux de la cybersécurité et leurs usages.
- Identifier et analyser menaces et vulnérabilités.
- Appliquer les contrôles sur réseaux, systèmes et applications.
- Mettre en place surveillance et réponse aux incidents.
- Se préparer efficacement à la certification ISC² CC.
- Réaliser un examen blanc avec correction détaillée.

## Public visé

- Administrateurs systèmes / réseaux
- Analystes SOC juniors
- Consultants IT
- Profils en reconversion vers la cybersécurité

## Pré-requis

- Bases en systèmes et réseaux
- Connaissances générales IT

## Programme de formation CC – Certified in Cybersecurity

### [Jour 1 - Matin]

### Introduction à la cybersécurité et à la certification CC

- Positionnement de la certification ISC² CC et attentes du marché
- Panorama des menaces, vulnérabilités et risques
- Rôles et responsabilités des équipes sécurité
- Lexique essentiel : actifs, contrôles, exposition, probabilité
- Méthodologie pédagogique et ressources de préparation
- Atelier pratique : Auto diagnostic initial et débrief.

### [Jour 1 - Après-midi]

### Principes de sécurité et concepts fondamentaux

- Triade CIA : Confidentialité, Intégrité, Disponibilité
- Notions de gouvernance, politiques et lignes directrices
- Gestion du risque : identification, analyse, traitement
- Modèles d’authentification et d’autorisation
- Contrôles préventifs/détectifs/correctifs
- Atelier pratique : Cartographier risques et contrôles d’un SI type.

### Gestion des menaces, attaques et vulnérabilités

- Typologie d’attaques : phishing, malware, ransomware, ingénierie sociale
- Vulnérabilités applicatives et erreurs de configuration
- Cycle de vie de l’incident et priorisation
- Indicateurs d’attaque/compromission (IoA/IoC)
- Outils de détection et de réponse
- Atelier pratique : Triage d’un incident et premières actions.

### [Jour 2 - Matin]

## Sécurité des réseaux et des systèmes

- Architectures, segmentation et durcissement
- Contrôles périmétriques : firewalls, IDS/IPS, WAF
- Protocoles et services sécurisés : TLS, VPN, SSH
- Durcissement Windows et Linux (patching, comptes, services)
- Journalisation et corrélation d'événements
- Atelier pratique : Configuration d'un pare-feu logiciel + lecture de logs.

[Jour 2 - Après-midi]

## Sécurité opérationnelle et surveillance

- Surveillance : SIEM, journaux, alertes et tableaux de bord
- Gestion du changement et du patch (vulnérabilités)
- BCP/DRP : sauvegardes, restauration et tests
- Résilience et continuité d'activité
- Processus de réponse aux incidents et communication
- Atelier pratique : Chasse aux anomalies dans des journaux fournis.

## Sécurité des applications et du cloud

- Principes de développement sécurisé et erreurs courantes
- Vulnérabilités OWASP (XSS, injection, CSRF…)
- Modèle de responsabilité partagée en cloud
- IAM : gestion des identités, MFA, rôles
- Conformité et journalisation côté cloud
- Atelier pratique : Corriger une faille XSS dans un snippet.

[Jour 3 - Matin]

## Gouvernance, risques et conformité

- Cadres et normes : ISO 27001, NIST, RGPD
- Politiques, chartes et sensibilisation
- Registre des risques : suivi et revues
- Audits, preuves et amélioration continue
- Alignement sécu – métier
- Atelier pratique : Mini-plan de gestion des risques d'une BU.

## Préparation à l'examen Certified in Cybersecurity

- Domaines du CC et pondérations
- Stratégies de révision et plan d'étude

- Méthodes pour les QCM : élimination, mots-pièges, timing
- Parcours officiels et ressources ISC²
- Conseils logistiques (Pearson VUE / CAT)
- Atelier pratique : Mini-examen thématique + correction argumentée.

### [Jour 3 - Après-midi]

### Consolidation des acquis

- Récapitulatif des concepts clés par domaine
- Fiches mémo et checklists « jour J »
- Erreurs fréquentes et parades
- Plan d’action personnalisé jusqu’à l’examen
- Q&R avancées avec l’instructeur
- Atelier pratique : Construction d’un plan de révision sur 2 semaines.

### Passage de l’examen blanc et correction

- Mise en situation examen blanc complet (conditions réelles)
- Correction détaillée et explications par domaine
- Analyse des résultats et axes de progrès
- Conseils de gestion du temps et du stress
- Checklist finale « pré-examen »
- Atelier pratique : Passage de l'examen blanc + correction.

## 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.