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

Mis à jour le 20/08/2026

S'inscrire

Formation Certification CREST CCT APP

4 jours (28 heures)

Présentation

La Formation Certification CREST CCT APP vous prépare à l'examen officiel CREST Certified Tester Application, une certification avancée qui valide votre capacité à conduire des tests d'intrusion applicatifs, systèmes et cloud dans des environnements exigeants.

Cette formation de préparation vous permet de consolider les compétences attendues pour réussir la certification CREST Certified Tester Application. Vous approfondirez les méthodologies de pentest, l'analyse des surfaces d'attaque, l'exploitation de vulnérabilités et la restitution des résultats dans un contexte professionnel.

Vous apprendrez à maîtriser les domaines techniques couverts par l'examen, notamment la sécurité des applications web, les API, les injections, l'authentification, les environnements Windows et Linux, les bases de données, le cloud et la conteneurisation.

Le parcours vous prépare aux deux volets de l'examen officiel : l'épreuve écrite, composée de questions à choix multiple et d'un scénario rédactionnel, ainsi que l'épreuve pratique menée dans un environnement contrôlé. Vous développerez une approche structurée pour qualifier les risques, rédiger des constats exploitables et optimiser votre gestion du temps.

À l'issue de la formation, vous serez en mesure d'aborder la certification avec une méthodologie solide, de démontrer vos compétences de pentester senior et de conduire des évaluations de sécurité applicative conformes aux attentes d'une mission réelle.

Comme toutes nos formations, celle-ci vous présentera **la dernière version stable** de la technologie et ses nouveautés.

Objectifs

- Maîtriser le périmètre et les attentes de l'examen CREST Certified Tester Application
- Identifier et exploiter des vulnérabilités avancées dans des applications web, des API et des infrastructures associées
- Mettre en oeuvre une méthodologie de test d'intrusion adaptée aux scénarios de certification
- Analyser les impacts, qualifier les risques et produire des constats de sécurité structurés
- Préparer efficacement les épreuves écrite et pratique dans les contraintes de temps de l'examen

Public visé

- Pentester
- Consultant en cybersécurité
- Auditeur de sécurité applicative
- Red Teamer

Pré-requis

- Expérience confirmée en tests d'intrusion applicatifs et systèmes
- Maîtrise des protocoles HTTP, TCP/IP, DNS et TLS
- Connaissances avancées des environnements Linux et Windows
- Pratique des vulnérabilités web, des API, des bases de données SQL et des mécanismes d'authentification

Pré-requis techniques

- Ordinateur équipé de Windows 10 ou 11, de macOS ou d'une distribution Linux récente
- Processeur 64 bits, 16 Go de RAM recommandés et 50 Go d'espace disque disponible
- Solution de virtualisation VMware Workstation, VMware Fusion ou VirtualBox installée et opérationnelle
- Connexion Internet stable, autorisant les téléchargements de machines virtuelles et les accès aux plateformes de laboratoire

Programme de notre formation CREST CCT APP

[Jour 1 - Matin]

Cadre de certification et méthodologie d'évaluation

- Positionnement de la certification CREST Certified Tester Application et niveau de compétence attendu
- Décomposition des épreuves : questions à choix multiple, scénario rédactionnel et examen pratique
- Analyse du syllabus : applications web, infrastructures, systèmes, cloud, conteneurs et macOS
- Cycle d'une mission de pentest : autorisation, périmètre, règles d'engagement, collecte de preuves et restitution

- Gestion du temps, lecture des consignes, stratégie de réponse et critères de réussite

[Jour 1 - Après-midi]

Reconnaissance et cartographie de la surface d'attaque

- Approche structurée de la reconnaissance passive et active dans un périmètre autorisé
- Énumération des services, empreintes technologiques, analyse DNS, HTTP, TLS et métadonnées
- Cartographie des applications, des API, des environnements d'administration et des sources de fuite d'information
- Hiérarchisation des vecteurs d'attaque selon l'exposition, la criticité et les chemins de compromission
- Atelier pratique : cartographier une cible de laboratoire, identifier les technologies exposées et produire un plan de test priorisé

[Jour 2 - Matin]

Sécurité applicative et attaques sur les entrées

- Modélisation des menaces applicatives et analyse des vecteurs d'attaque web modernes
- Recherche et validation des vulnérabilités SQL Injection, NoSQL Injection, XPath Injection et injection de commandes
- Analyse des faiblesses de validation : XSS, XXE, SSRF, CRLF Injection et traversée de répertoires
- Fuzzing raisonné, contournement de filtres, encodages, chaînes de requêtes et contrôle de l'exploitabilité
- Construction de preuves fiables et distinction entre vulnérabilité théorique, impact démontré et faux positif

[Jour 2 - Après-midi]

Authentification, autorisation et logique métier

- Évaluation des mécanismes d'authentification, de gestion des mots de passe, de MFA et de récupération de compte
- Tests d'autorisation : escalade horizontale et verticale, IDOR, mass assignment et contrôle d'accès aux API
- Analyse des sessions, cookies, jetons, fixation de session, rejeu et faiblesses de JWT
- Identification des vulnérabilités de logique métier, de concurrence et de contournement de parcours
- Atelier pratique : compromettre un parcours applicatif de laboratoire par abus d'autorisation, puis documenter l'impact et la remédiation

[Jour 3 - Matin]

Pivoting, systèmes et environnements d'infrastructure

- Techniques de pivoting, transfert de ports, proxification et maintien d'une chaîne de preuves
- Énumération et exploitation des environnements Windows, Active Directory, services distants et permissions locales
- Reconnaissance des systèmes Linux et Unix, processus, services, secrets et permissions de fichiers
- Élévation de privilèges locale, post exploitation, accès aux données et analyse des mécanismes de persistance
- Tests des services réseau, protocoles d'administration, partages, annuaires et configurations de chiffrement

[Jour 3 - Après-midi]

Cloud, conteneurs et chaînes de compromission

- Reconnaissance et risques des environnements cloud : IAM, journalisation, stockage, métadonnées et réseaux virtuels
- Évaluation des erreurs de configuration dans les conteneurs Docker, les clusters Kubernetes et les plateformes virtualisées
- Analyse des secrets, identités de service, registres, volumes, rôles et mouvements entre hôte et cloud
- Identification des scénarios de compromission combinant application, infrastructure, base de données et services cloud
- Atelier pratique : exploiter une chaîne de compromission en laboratoire depuis une application web vers un environnement conteneurisé

[Jour 4 - Matin]

Épreuve écrite et production de livrables

- Révision ciblée des domaines techniques à forte densité pour les questions à choix multiple
- Lecture et décomposition d'un scénario : périmètre, contraintes, risques, obligations et livrables attendus
- Qualification des vulnérabilités : vraisemblance, impact métier, criticité, conditions d'exploitation et priorisation
- Rédaction de constats : preuve, description technique, conséquence, recommandation et communication au client
- Simulation de l'épreuve scénario : allocation du temps, réponses longues structurées et contrôle qualité final

[Jour 4 - Après-midi]

Simulation intégrée de certification

- Préparation de l'environnement pratique : outils disponibles, contraintes de poste, fichiers autorisés et stratégie de notes

- Exploitation méthodique d'un environnement cible mêlant application, système, base de données et services réseau
- Arbitrage entre profondeur technique, couverture du périmètre, collecte des réponses et gestion du chronomètre
- Débriefing des erreurs fréquentes : fausse piste, preuve insuffisante, réponse imprécise et perte de temps
- Atelier pratique : réaliser une simulation chronométrée de l'épreuve pratique, répondre aux questions et restituer une stratégie de correction personnalisée

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.