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

Mis à jour le 24/08/2026

S'inscrire

Formation Certification CREST CCP INF

Présentation

La formation Certification CREST CCP INF prépare à la certification officielle CREST Certified Tester - Infrastructure (CCT INF), référence avancée pour valider vos compétences en tests d'intrusion d'infrastructure, analyse des risques et restitution professionnelle.

Cette formation vous permet de préparer méthodiquement l'examen CREST Certified Tester - Infrastructure (CCT INF), destiné aux professionnels capables d'évaluer la sécurité des systèmes, réseaux, services exposés et environnements d'entreprise. Vous consoliderez les compétences attendues sur les infrastructures Windows, Linux, les réseaux, le cloud, la virtualisation et les technologies web.

Vous apprendrez à organiser une mission de pentest, de la phase de cadrage à la rédaction du rapport, en appliquant une méthodologie rigoureuse de reconnaissance, d'énumération, d'exploitation et de validation. La préparation couvre également l'analyse des protocoles, l'identification des vulnérabilités, le pivoting, les services d'annuaire et les mécanismes de sécurité réseau.

À l'issue de la formation, vous serez en mesure de mobiliser les techniques évaluées lors de l'examen écrit et pratique, de prioriser les constats selon leur risque et de produire des livrables exploitables par les équipes techniques et décisionnaires. Vous disposerez d'une stratégie de préparation adaptée au format Pearson VUE et aux attendus de la certification.

La formation aborde également les scénarios de certification, la gestion du temps, les exercices pratiques en environnement contrôlé et les bonnes pratiques de restitution. Elle vous aide à renforcer votre autonomie pour conduire des évaluations d'infrastructure complexes dans un cadre légal, éthique et professionnel.

Objectifs

- Maîtriser les domaines techniques évalués par la certification CREST Certified Tester - Infrastructure (CCT INF).
- Structurer une mission de pentest d'infrastructure, du cadrage à la restitution.
- Identifier, exploiter et qualifier des vulnérabilités sur des environnements Windows, Linux, réseau et cloud.
- Analyser les résultats d'outils de sécurité et conduire des actions de pivoting contrôlées.
- Préparer les épreuves écrite, scénario et pratique de la certification.
- Rédiger des constats de sécurité précis, priorisés et orientés risque.

Public visé

- Pentester
- Consultant cybersécurité
- Auditeur sécurité
- Red Teamer
- Ingénieur sécurité réseau

Pré-requis

- Expérience confirmée en tests d'intrusion et en évaluation de sécurité d'infrastructures.
- Maîtrise opérationnelle des systèmes Windows et Linux.
- Connaissances avancées des réseaux TCP/IP, des services DNS, SMB, LDAP et Active Directory.
- Pratique des outils Nmap, Wireshark, Burp Suite et Metasploit.
- Capacité à rédiger des rapports techniques de sécurité en anglais.

Pré-requis techniques

- Poste sous Windows 11, macOS ou Linux, avec processeur 64 bits, 16 Go de RAM minimum et 80 Go d'espace disque disponible.
- Logiciel de virtualisation VMware Workstation 17, VMware Fusion 13 ou VirtualBox 7.
- Machine virtuelle Kali Linux récente et environnement de laboratoire isolé compatible avec les exercices de pentest.
- Connexion Internet stable, sans filtrage bloquant les téléchargements, les dépôts logiciels et les accès aux laboratoires autorisés.
- Navigateur Google Chrome, Mozilla Firefox ou Microsoft Edge à jour.

Programme de notre formation CREST CCP INF

[Jour 1 - Matin]

Cadre de certification et méthodologie d'évaluation

- Positionnement de la certification officielle CREST Certified Tester - Infrastructure (CCT INF) et compétences attendues.

- Structure des épreuves, critères de réussite, répartition des compétences et stratégie de préparation.
- Cycle de vie d'une mission de pentest : autorisation, cadrage, règles d'engagement, collecte de preuves et gestion des risques.
- Construction d'une méthodologie reproductible de reconnaissance, d'énumération, de validation et de restitution.
- Atelier pratique : analyser un énoncé de mission, définir le périmètre, les hypothèses, les règles d'engagement et le plan de test.

[Jour 1 - Après-midi]

Réseaux, protocoles et cartographie d'attaque

- Révision avancée des couches TCP/IP , du routage, des VLAN, d'IPv4 , d'IPv6 et des mécanismes de filtrage.
- Analyse des protocoles DNS , ARP , DHCP , SMB , SNMP , SSH et des services de messagerie.
- Découverte d'hôtes, fingerprinting système, énumération de services et interprétation des réponses réseau.
- Analyse de trafic, manipulation de paquets, détection des contrôles NAC et identification des surfaces d'exposition.
- Atelier pratique : cartographier un réseau cible autorisé avec Nmap et Wireshark , puis produire une matrice de services exploitables.

[Jour 2 - Matin]

Évaluation des environnements Windows et Active Directory

- Architecture de sécurité Windows : comptes, jetons, privilèges, services, registre, stratégies locales et mécanismes de durcissement.
- Reconnaissance Active Directory : domaines, forêts, trusts, objets, groupes, GPO, délégations et chemins d'attaque.
- Énumération authentifiée et non authentifiée des services LDAP , Kerberos , SMB et RPC .
- Analyse des erreurs de configuration : permissions excessives, secrets exposés, partages, politiques de mots de passe et mouvements latéraux.
- Atelier pratique : conduire une phase d'énumération Active Directory et documenter les chemins de compromission potentiels.

[Jour 2 - Après-midi]

Systèmes Linux, services Unix et élévation de privilèges

- Modèle de sécurité Linux et Unix : comptes, permissions, sudo, capabilities, services, processus et journaux.
- Énumération des services FTP , NFS , SMTP , RPC , SSH , X11 et bases de données.
- Recherche de vulnérabilités locales : binaires SUID, tâches planifiées, droits d'écriture, secrets, configurations faibles et kernels vulnérables.

- Principes d'exploitation contrôlée, stabilisation d'accès, collecte de preuves et conservation de la traçabilité.
- Atelier pratique : auditer un serveur Linux vulnérable, démontrer une élévation de privilèges contrôlée et consigner les preuves.

[Jour 3 - Matin]

Technologies web, bases de données et cloud

- Reconnaissance des serveurs web, API, frameworks, mécanismes d'authentification, sessions et contrôles d'autorisation.
- Analyse des vulnérabilités SQL , NoSQL , LDAP , XML , injection de commandes, XSS, téléversement de fichiers et traversée de répertoires.
- Évaluation de la sécurité des bases de données, des secrets applicatifs et des chaînes de connexion.
- Fondamentaux de l'évaluation cloud : identités, rôles, stockage, métadonnées, configurations exposées et conteneurisation.
- Atelier pratique : identifier et qualifier des vulnérabilités sur une application d'administration exposant une API et une base de données.

[Jour 3 - Après-midi]

Exploitation, pivoting et chaînes d'attaque

- Sélection raisonnée des vecteurs d'exploitation selon le contexte, l'impact métier et les contraintes d'engagement.
- Techniques de pivoting , proxying, tunneling, relais et accès aux segments internes autorisés.
- Gestion des identifiants, réutilisation de sessions, mouvement latéral et limitations imposées par les contrôles de sécurité.
- Évaluation des environnements virtualisés, des snapshots, des mécanismes d'isolation et des risques d'échappement de machine virtuelle.
- Atelier pratique : construire une chaîne d'attaque de laboratoire depuis un service exposé jusqu'à un actif interne, avec justification de chaque étape.

[Jour 4 - Matin]

Scénario écrit, analyse de risque et reporting

- Préparation à l'épreuve écrite : questions à choix multiple, scénario de mission, gestion du temps et lecture des consignes.
- Qualification des vulnérabilités : vraisemblance, impact, criticité, priorisation et formulation d'un risque compréhensible.
- Rédaction des constats : preuve, description technique, scénario d'exploitation, conséquence, recommandation et contrôle compensatoire.
- Communication avec le client : restitution, limites de l'évaluation, qualité rédactionnelle, conformité et obligations légales.

- Atelier pratique : traiter un scénario de certification, rédiger des constats priorisés et présenter une synthèse de risque.

[Jour 4 - Après-midi]

Simulation finale et préparation opérationnelle

- Rappel des domaines du syllabus : réseau, systèmes, services, virtualisation, web, cloud, macOS et compétences transverses.
- Stratégie pour l'épreuve pratique : reconnaissance rapide, priorisation, validation des réponses et gestion des impasses.
- Prise en main de l'environnement de type Kali Linux , des outils autorisés et des ressources préchargées.
- Analyse des erreurs fréquentes : collecte de preuves insuffisante, confusion entre vulnérabilité et risque, mauvaise priorisation et restitution incomplète.
- Atelier pratique : réaliser une simulation chronométrée de certification combinant reconnaissance, exploitation contrôlée, analyse de risque et restitution.

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.