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

Mis à jour le 26/08/2026

S'inscrire

Formation Certification CREST CPSA

5 jours (35 heures)

Présentation

La certification CREST Practitioner Security Analyst valide les compétences fondamentales attendues pour conduire des évaluations de sécurité sur des infrastructures, des systèmes et des applications web. Elle prépare aux enjeux concrets du pentest, de l'analyse de vulnérabilités et de l'interprétation des résultats techniques.

Notre formation Formation Certification CREST CPSA vous accompagne dans une préparation structurée à l'examen officiel CREST Practitioner Security Analyst. Vous consoliderez les connaissances nécessaires pour comprendre le périmètre d'une mission, identifier les surfaces d'attaque et appliquer une méthodologie de test responsable.

Vous apprendrez à analyser les protocoles réseau, réaliser des phases de reconnaissance, interpréter les résultats de scans et évaluer la sécurité des environnements Windows, Unix et web. Les notions d'authentification, de gestion de session, d'injection, de XSS et de sécurité des bases de données sont également couvertes.

À l'issue de la formation, vous serez en mesure de vous préparer efficacement au format de l'examen, composé de questions à choix multiple, et de mobiliser les compétences validées par la certification dans un contexte de test d'intrusion encadré.

Cette formation combine révisions ciblées, mises en situation et entraînements de type examen afin de renforcer votre maîtrise des domaines du syllabus, votre capacité d'analyse et votre gestion du temps le jour de l'épreuve.

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

Objectifs

- Comprendre les domaines et le format de l'examen CREST Practitioner Security Analyst
- Appliquer une méthodologie de reconnaissance et d'analyse de vulnérabilités
- Interpréter les résultats des outils de scan réseau et applicatif
- Évaluer les risques courants sur les environnements Windows, Unix et web
- Identifier les principales vulnérabilités web et les mesures de remédiation associées
- Se préparer aux questions à choix multiple et gérer son temps d'examen

Public visé

- Pentester junior
- Analyste en cybersécurité
- Consultant en sécurité informatique
- Administrateur systèmes et réseaux
- Analyste SOC

Pré-requis

- Connaissances des réseaux TCP/IP, du routage et des services courants
- Maîtrise des commandes essentielles sous Linux et Windows
- Notions de sécurité des systèmes, des réseaux et des applications web
- Expérience de base avec Nmap et les outils de diagnostic réseau

Pré-requis techniques

- Ordinateur équipé de Windows 10 ou 11, de macOS ou de Linux, avec au moins 16 Go de RAM
- Droits d'installation et d'administration sur le poste de travail
- VirtualBox 7 ou VMware Workstation installé pour exécuter les machines de laboratoire
- Connexion Internet stable, sans filtrage bloquant les téléchargements, les dépôts logiciels et les communications réseau des laboratoires
- Navigateur web récent et éditeur de texte ou terminal disponible

Programme de notre formation CREST CPSA

[Jour 1 - Matin]

Cadre de la certification et méthodologie de test

- Présentation de la certification CREST Practitioner Security Analyst, de ses domaines de compétences et de son positionnement
- Format de l'examen, questions à choix multiple, règles de l'épreuve et stratégie de gestion du temps
- Cycle de vie d'une mission de pentest, autorisation, périmètre, règles d'engagement et traçabilité

- Principes d'éthique, de confidentialité, de gestion des preuves et de communication avec le commanditaire
- Fondamentaux de l'analyse de risques, de la surface d'attaque et de la priorisation des constats

[Jour 1 - Après-midi]

Réseaux et cartographie des cibles

- Révision des protocoles TCP/IP, de l'adressage, du routage, de l'ARP, du DNS et des ports
- Architecture réseau, segmentation, filtrage, pare-feu et mécanismes de contrôle d'accès
- Découverte d'hôtes, identification des services et principes de fingerprinting des systèmes
- Lecture et interprétation des résultats de scan avec Nmap et outils de diagnostic réseau
- Techniques de contournement de filtrage à connaître pour l'examen, dans un cadre autorisé
- Atelier pratique : cartographier un réseau de laboratoire, identifier les hôtes, services et ports exposés, puis interpréter les résultats

[Jour 2 - Matin]

Reconnaissance et collecte d'informations

- Objectifs de la reconnaissance passive et active dans une démarche de test d'intrusion
- Recherche d'informations publiques, noms de domaine, enregistrements DNS et analyse de présence web
- Énumération des sous-domaines, des services, des utilisateurs et des ressources accessibles
- Analyse des métadonnées, des technologies exposées et des fuites d'informations
- Qualification des résultats, réduction des faux positifs et documentation des éléments utiles

[Jour 2 - Après-midi]

Évaluation des services et équipements réseau

- Analyse des services courants, FTP, SMTP, SSH, SNMP, SMB et services RPC
- Notions de capture et d'analyse de trafic, protocoles en clair et détection de configurations faibles
- Sécurité des équipements réseau, interfaces d'administration, services de supervision et configurations
- Principes de sécurité des réseaux sans fil, de la téléphonie IP et des tunnels IPSec
- Lecture de bannières, corrélation des versions et identification des vulnérabilités probables
- Atelier pratique : analyser plusieurs services exposés dans un laboratoire et produire une synthèse des risques observés

[Jour 3 - Matin]

Sécurité des environnements Windows

- Architecture de sécurité Windows, comptes locaux, groupes, droits, services et mécanismes de correctifs
- Fondamentaux de l'Active Directory, domaines, utilisateurs, groupes, stratégies et relations de confiance
- Énumération des utilisateurs, partages, services et informations système sur une cible Windows
- Gestion des mots de passe, politiques de verrouillage, hachage et principes de résistance aux attaques
- Identification des défauts de configuration, des correctifs manquants et des vecteurs d'escalade courants

[Jour 3 - Après-midi]

Sécurité des environnements Unix et Linux

- Architecture des permissions Unix et Linux, utilisateurs, groupes, processus et services
- Énumération des comptes, des partages, des tâches planifiées, des binaires et des configurations sensibles
- Analyse des services NFS, FTP, SMTP, SSH, RPC et X11
- Recherche de vulnérabilités liées aux versions, aux permissions faibles et aux secrets exposés
- Bonnes pratiques de durcissement, de journalisation et de réduction de la surface d'attaque
- Atelier pratique : réaliser une évaluation guidée d'une machine Linux vulnérable et classer les constats par criticité

[Jour 4 - Matin]

Technologies web et méthodologie de test

- Architecture d'une application web, serveurs, proxies, API, composants clients et services de données
- Fonctionnement de HTTP et HTTPS, méthodes, en-têtes, cookies, codes de réponse et redirections
- Reconnaissance applicative, cartographie des contenus, paramètres, répertoires et fonctionnalités
- Modélisation des menaces, vecteurs d'attaque et contrôle des entrées utilisateur
- Authentification, autorisation, gestion de session et divulgation d'informations par les messages d'erreur

[Jour 4 - Après-midi]

Vulnérabilités applicatives et bases de données

- Principes et détection des vulnérabilités XSS, injections SQL et manipulations de paramètres
- Analyse des contrôles de validation, encodage, filtrage et gestion des erreurs
- Risques liés aux sessions, aux cookies, aux jetons et aux mécanismes de contrôle d'accès
- Notions de sécurité des bases MySQL, Microsoft SQL Server et Oracle
- Interprétation des réponses applicatives et formulation de recommandations de remédiation
- Atelier pratique : identifier des vulnérabilités web dans une application de laboratoire et associer chaque constat à une remédiation

[Jour 5 - Matin]

Consolidation et entraînement ciblé

- Révision transversale des domaines du syllabus, réseaux, systèmes, web, bases de données et gestion de mission
- Analyse de scénarios de questions à choix multiple et identification des mots-clés déterminants
- Méthodes d'élimination des réponses incorrectes et arbitrage lorsque plusieurs réponses paraissent plausibles
- Rappel des notions de cryptographie, chiffrement, hachage, intégrité et usages de sécurité
- Préparation logistique de l'examen, compte Pearson VUE, épreuve fermée et règles à respecter
- Atelier pratique : réaliser un examen blanc chronométré, corriger les réponses et établir un plan de révision individualisé

[Jour 5 - Après-midi]

Simulation finale et préparation à l'examen

- Étude de cas complète, de la définition du périmètre à l'analyse des vulnérabilités identifiées
- Corrélation des résultats de reconnaissance, de scan réseau, d'énumération système et de tests web
- Qualification des constats, évaluation de l'impact et priorisation des actions de remédiation
- Synthèse des pièges récurrents de l'examen et des domaines nécessitant une vigilance particulière
- Conseils de gestion du temps, relecture des questions et préparation personnelle avant le passage de l'épreuve
- Atelier pratique : résoudre une simulation finale de questions à choix multiple et débriefer collectivement les choix de réponse

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.

Organisme de formation enregistré sous le numéro 11 75 54743 75. Cet enregistrement ne vaut pas agrément de l’État.
© Ambient IT 2015-2026. Tous droits réservés. Paris, France - Suisse - Belgique - Luxembourg