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

Mis à jour le 31/08/2026

S'inscrire

Formation Certification GIAC GSEC®

Présentation

La formation Certification GIAC GSEC prépare à la certification officielle GIAC Security Essentials et vous apporte les compétences essentielles pour sécuriser des systèmes, réseaux et environnements cloud face aux menaces courantes.

Cette formation vous permet de préparer l'examen GIAC Security Essentials en consolidant les fondamentaux opérationnels de la cybersécurité. Vous apprendrez à appliquer les principes de défense en profondeur, à protéger les identités, à analyser les risques et à mettre en oeuvre des contrôles de sécurité adaptés.

Vous étudierez les domaines couverts par la certification, notamment la sécurité réseau, la cryptographie, le durcissement de Linux et de Windows, la sécurité des applications web, la gestion des vulnérabilités et la réponse aux incidents.

La préparation s'appuie sur des cas d'usage et des exercices pratiques inspirés des situations évaluées lors de l'examen. Vous développerez une méthode de révision efficace, structurerez vos ressources autorisées et vous entraînerez à répondre aux questions techniques dans le temps imparti.

À l'issue de la formation, vous serez en mesure de mobiliser les compétences validées par la certification officielle GIAC Security Essentials, d'interpréter les principaux scénarios de sécurité et de vous présenter à l'examen avec une préparation méthodique.

Objectifs

- Maîtriser les domaines techniques évalués par la certification GIAC Security Essentials
- Appliquer les principes de défense en profondeur aux systèmes, réseaux et services
- Identifier les vulnérabilités, les vecteurs d'attaque et les mesures de remédiation adaptées
- Renforcer la sécurité des environnements Linux, Windows et cloud
- Préparer efficacement l'examen grâce à une stratégie de révision et à des mises en situation

Public visé

- Administrateur systèmes et réseaux
- Analyste SOC
- Ingénieur cybersécurité
- Consultant sécurité
- Technicien sécurité informatique

Pré-requis

- Connaissances fondamentales des réseaux TCP/IP et des protocoles courants
- Pratique courante de l'administration de Linux ou de Windows
- Notions de base en cybersécurité, gestion des identités et contrôle d'accès
- Compréhension des principes de virtualisation et des services cloud

Pré-requis techniques

- Ordinateur équipé de Windows 10 ou 11, macOS 13 ou version ultérieure, ou d'une distribution Linux récente
- Processeur quatre coeurs,16 Go de RAM recommandés et au moins 30 Go d'espace disque disponible
- Installation de VirtualBox 7 ou d'un hyperviseur équivalent permettant d'exécuter des machines virtuelles
- Connexion Internet stable, navigateur Google Chrome ou Mozilla Firefox à jour

Programme de notre formation GIAC GSEC®

[Jour 1 - Matin]

Cadre de certification et fondamentaux de sécurité

- Présentation de la certification officielle GIAC Security Essentials, de ses domaines et de ses compétences validées
- Compréhension du format de l'examen, de la gestion du temps et des principes de préparation
- Fondements de la cybersécurité : confidentialité, intégrité, disponibilité et gestion du risque
- Principes de défense en profondeur, surfaces d'attaque et sélection des contrôles
- Organisation d'une stratégie de révision : objectifs, index de ressources et priorités techniques

[Jour 1 - Après-midi]

Identités, accès et politiques de sécurité

- Modèles de contrôle d'accès : DAC, MAC, RBAC et moindre privilège
- Gestion des identités, authentification multifacteur et cycle de vie des comptes
- Bonnes pratiques de mots de passe, coffres de secrets et protection contre les attaques d'identifiants
- Rôle des politiques, normes, procédures et sensibilisation dans la gouvernance de la sécurité
- Atelier pratique : analyser un scénario de compromission de compte et définir les contrôles d'accès et mesures correctives

[Jour 2 - Matin]

Réseaux, protocoles et architecture défendable

- Révision des protocoles TCP/IP, DNS, DHCP, HTTP et TLS
- Segmentation réseau, zones de confiance, filtrage et principes d'architecture défendable
- Fonctionnement et positionnement des pare-feux, proxys, IDS, IPS et systèmes de journalisation
- Analyse des attaques réseau courantes : écoute, usurpation, déni de service et mouvement latéral
- Protection des réseaux sans fil : chiffrement, authentification et risques de configuration

[Jour 2 - Après-midi]

Sécurité des communications et analyse réseau

- Sécurisation des échanges web, messagerie, accès distant et transferts de fichiers
- Fonctionnement de la cryptographie symétrique, asymétrique, du hachage et des signatures
- Gestion des certificats, autorités de certification et erreurs fréquentes de déploiement TLS
- Lecture de flux et identification d'indicateurs d'activité suspecte dans les communications réseau
- Atelier pratique : examiner une capture réseau avec Wireshark afin d'identifier des faiblesses de protocoles et des anomalies

[Jour 3 - Matin]

Durcissement et sécurité Linux

- Architecture de sécurité Linux, utilisateurs, groupes, permissions et contrôle des privilèges
- Configuration sécurisée des services, accès SSH, journalisation et mises à jour
- Durcissement du système : services inutiles, pare-feu hôte, fichiers sensibles et tâches planifiées
- Surveillance des processus, connexions, journaux et mécanismes de persistance
- Utilitaires de sécurité Linux et méthodes de collecte d'éléments de preuve

[Jour 3 - Après-midi]

Sécurisation des environnements Windows

- Gestion des comptes, groupes, droits utilisateurs et stratégies de sécurité Windows
- Rôle de Active Directory, des stratégies de groupe et de l'authentification centralisée
- Sécurisation des services réseau, du partage de fichiers, de PowerShell et des postes de travail
- Audit des événements, analyse des journaux et détection des activités suspectes
- Atelier pratique : auditer une configuration Windows, prioriser les écarts et proposer un plan de durcissement

[Jour 4 - Matin]

Vulnérabilités, attaques et protection des actifs

- Cycle de gestion des vulnérabilités : découverte, qualification, priorisation et remédiation
- Principes du scan de vulnérabilités, de la validation des résultats et du suivi des correctifs
- Vecteurs d'attaque : ingénierie sociale, exploitation, malwares, élévation de privilèges et exfiltration
- Protection des terminaux, contrôle des applications, sauvegardes et prévention des pertes de données
- Risques des environnements virtualisés et cloud : isolation, configuration et responsabilité partagée

[Jour 4 - Après-midi]

Détection, réponse aux incidents et SIEM

- Phases de la réponse à incident : préparation, détection, confinement, éradication et retour d'expérience
- Qualification des alertes, indicateurs de compromission et critères d'escalade
- Collecte, conservation et corrélation des journaux dans un SIEM
- Construction de scénarios de détection et articulation avec les contrôles de sécurité critiques
- Atelier pratique : traiter un incident simulé à partir de journaux système et réseau, puis formaliser les actions de réponse

[Jour 5 - Matin]

Consolidation des domaines de l'examen

- Révision transversale des objectifs : accès, réseaux, systèmes, cryptographie, cloud et réponse à incident
- Analyse de cas de certification mobilisant plusieurs contrôles de sécurité
- Identification des pièges fréquents : vocabulaire, scénarios techniques, priorisation et choix de mesures
- Préparation des ressources de référence autorisées et optimisation de l'index de recherche
- Méthode de résolution : lecture ciblée, élimination des réponses, gestion des questions différées et vérification

[Jour 5 - Après-midi]

Simulation et préparation finale à la certification

- Rappel des modalités de passage, de la surveillance et des règles applicables à l'examen
- Gestion des quatre heures : allocation du temps, pauses planifiées et traitement des questions complexes
- Approche des exercices CyberLive : analyse de consignes, exécution contrôlée et validation des résultats
- Évaluation des acquis, identification des domaines à renforcer et plan de préparation individuel
- Atelier pratique : réaliser une simulation d'examen avec questions de synthèse et scénario technique chronométré

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.