+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 GCED®

5 jours (35 heures)

Présentation

La certification GIAC Certified Enterprise Defender valide votre capacité à défendre un environnement d'entreprise grâce à la surveillance réseau, l'analyse de paquets, la réponse aux incidents et l'analyse des malwares.

La Formation Certification GIAC GCED vous prépare à la certification officielle GIAC Certified Enterprise Defender et à son examen surveillé. Vous consolidez les compétences attendues pour concevoir, exploiter et améliorer une défense technique adaptée aux environnements d'entreprise.

Vous apprendrez à mettre en oeuvre une infrastructure défensive, à exploiter les journaux et les flux réseau, à analyser des captures de paquets et à qualifier les alertes de sécurité. La formation couvre également les fondamentaux du test d'intrusion, de la collecte de preuves et du traitement des incidents.

À l'issue de la formation, vous serez en mesure de reconnaître les techniques d'intrusion, de conduire une analyse initiale de malware et de coordonner les actions de confinement, d'éradication et de remédiation. Vous disposerez aussi d'une méthode de préparation structurée pour l'examen GCED officiel.

Cette formation aborde enfin la stratégie d'examen, l'organisation des supports autorisés, les exercices de mise en situation et l'entraînement sur des cas représentatifs. Vous pourrez ainsi valoriser des compétences opérationnelles en détection des menaces et en défense de l'entreprise.

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

Objectifs

- Maîtriser les domaines de compétences évalués par la certification GIAC Certified Enterprise Defender.
- Analyser des paquets, des journaux et des alertes afin de détecter une intrusion.
- Mettre en oeuvre des contrôles de défense réseau et de supervision adaptés.
- Appliquer une démarche de réponse à incident, de la qualification à la remédiation.
- Identifier les comportements suspects et réaliser une analyse initiale de malware.
- Préparer efficacement l'examen GCED avec une méthode de révision et d'indexation.

Public visé

- Analyste SOC
- Ingénieur sécurité réseau
- Répondeur à incident
- Consultant cybersécurité
- Testeur d'intrusion

Pré-requis

- Maîtrise des fondamentaux des réseaux TCP/IP et des principaux protocoles.
- Connaissances pratiques des systèmes Windows et Linux.
- Expérience initiale de l'analyse de journaux et des outils de sécurité.
- Connaissances de base en réponse à incident et en architecture de sécurité.

Pré-requis techniques

- PC équipé de Windows 11, macOS 13 ou d'une distribution Linux récente.
- Processeur quatre coeurs, 16 Go de RAM recommandés et 30 Go d'espace disque disponible.
- Possibilité d'exécuter une machine virtuelle avec VirtualBox 7 ou un hyperviseur équivalent.
- Installation de Wireshark et de Nmap, avec les droits nécessaires à leur utilisation.
- Connexion Internet stable, sans filtrage bloquant les plateformes de visioconférence et de formation.

Programme de notre formation GIAC GCED®

[Jour 1 - Matin]

Cadre de la certification et défense d entreprise

- Présentation de la certification GIAC Certified Enterprise Defender et des compétences validées.
- Lecture des domaines évalués, du format d examen et des critères de préparation.
- Principes de défense en profondeur et modèle de sécurité d entreprise.
- Cartographie des actifs, des surfaces d attaque et des priorités de protection.
- Rôles du SOC , de l équipe réseau, de la réponse à incident et de la gestion des vulnérabilités.

[Jour 1 - Après-midi]

Protocoles et contrôles réseau

- Révision des protocoles TCP/IP , DNS, HTTP, TLS, SMTP et SMB sous l angle défensif.
- Identification des attaques courantes sur les protocoles et des mesures de durcissement.
- Segmentation, filtrage, pare-feu, proxy, VPN et contrôle des accès réseau.
- Référentiels de configuration sécurisée et contrôles de sécurité essentiels.
- Lecture des indicateurs réseau utiles à la détection d activité anormale.
- Atelier pratique : analyser une capture réseau avec Wireshark afin d identifier un comportement suspect et de proposer les contrôles défensifs adaptés.

[Jour 2 - Matin]

Supervision et détection des intrusions

- Architecture de network security monitoring et positionnement des sondes.
- Fonctionnement et réglage des systèmes de détection et de prévention d intrusion.
- Types de paquets, sessions, flux, métadonnées et captures complètes.
- Construction d une stratégie de détection fondée sur les actifs et les scénarios de menace.
- Qualification des alertes, réduction des faux positifs et priorisation des investigations.

[Jour 2 - Après-midi]

Journaux, flux et investigation réseau

- Sources de logs réseau, système, sécurité et applicatives.
- Centralisation, normalisation et conservation des événements dans un SIEM.
- Exploitation des données de flux pour repérer les communications anormales.
- Corrélation entre alertes, journaux et éléments de contexte de l entreprise.
- Constitution d une chronologie d incident à partir de traces techniques.
- Atelier pratique : mener une investigation sur un jeu de journaux et de flux, qualifier l incident et produire une chronologie argumentée.

[Jour 3 - Matin]

Réponse à incident et renseignement sur les menaces

- Cycle de vie de la réponse à incident , préparation, détection, confinement, éradication et retour d expérience.
- Qualification, criticité, périmètre et collecte des informations nécessaires à la décision.
- Articulation entre renseignement sur les menaces, indicateurs et Cyber Kill Chain.
- Communication technique, conservation des preuves et coordination des parties prenantes.
- Choix des actions de confinement selon les impacts métier et opérationnels.

[Jour 3 - Après-midi]

Investigation numérique et analyse de malwares

- Principes de forensique numérique et identification des artefacts utiles.
- Signes d infection, mécanismes de persistance et comportements malveillants courants.
- Analyse statique, analyse dynamique et précautions de sécurité en environnement isolé.
- Interprétation des résultats des outils automatisés et limites de leurs conclusions.
- Notions de désassemblage, décompilation et techniques d obfuscation.
- Atelier pratique : analyser les artefacts d un poste compromis dans un environnement isolé, identifier les indicateurs et définir les actions de remédiation.

[Jour 4 - Matin]

Tests d intrusion au service de la défense

- Objectifs, périmètre, règles d engagement et éthique du test d intrusion.
- Reconnaissance, énumération, identification des vulnérabilités et validation des risques.
- Compréhension des techniques d attaque afin d améliorer les capacités de détection.
- Outils de diagnostic et de test, interprétation des résultats et limites d usage.
- Rédaction de constats techniques et recommandations de correction priorisées.

[Jour 4 - Après-midi]

Architecture défensive et amélioration continue

- Conception de contrôles préventifs, détectifs et correctifs dans une architecture hybride.
- Protection des services réseau et cloud, gestion des identités et journalisation.
- Durcissement, gestion des correctifs et validation des configurations de sécurité.
- Mesure de l efficacité de la détection par les cas d usage et les indicateurs de performance.
- Élaboration d une feuille de route de renforcement de la posture de sécurité.
- Atelier pratique : concevoir une architecture défensive pour une entreprise fictive et justifier les contrôles, sources de logs et priorités de déploiement.

[Jour 5 - Matin]

Méthodologie de préparation à l examen

- Organisation des révisions selon les objectifs de la certification GCED.
- Création d un index de références papier exploitable pendant un examen autorisant les supports imprimés.
- Gestion du temps, lecture des énoncés et élimination des réponses non pertinentes.
- Révision transversale des protocoles, de la détection, de la réponse à incident et de l analyse de malwares.
- Analyse des erreurs récurrentes et définition d un plan de progression individuel.

[Jour 5 - Après-midi]

Simulation et consolidation des acquis

- Révision des notions clés couvrant les domaines de l examen GIAC Certified Enterprise Defender.
- Analyse de scénarios intégrés associant intrusion réseau, journaux, malware et remédiation.
- Justification des décisions techniques à partir d éléments de preuve et de contraintes métier.
- Conseils de préparation finale, planification du passage et gestion des conditions d examen surveillé.
- Synthèse des compétences opérationnelles validées par la certification.
- Atelier pratique : réaliser une simulation de préparation à l examen sur un cas de défense d entreprise, puis corriger collectivement les choix d investigation et de remédiation.

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.