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

Mis à jour le 17/09/2026

S'inscrire

Formation Certification GIAC GAIPS

5 jours (35 heures)

Présentation

La Formation Certification GIAC GAIPS vous prépare à la certification officielle GIAC AI Platform Security (GAIPS), pour sécuriser les applications GenAI, les LLM, les flux de données et les chaînes de déploiement associées.

Cette formation avancée vous permettra de maîtriser les domaines évalués par l'examen GIAC AI Platform Security (GAIPS), dont la sécurité des architectures d'IA générative, des applications enrichies par la connaissance et des systèmes agentiques.

Vous apprendrez à analyser les surfaces d'attaque propres aux LLM, à prévenir les injections de prompt, les fuites de données, les abus d'outils et les vulnérabilités des intégrations API. Vous saurez également protéger les bases vectorielles, les mécanismes de RAG et les modèles adaptés aux besoins métier.

Le parcours vous accompagne dans la mise en oeuvre de pratiques MLOps et MLSecOps, de la sécurisation des jeux de données jusqu'au déploiement et à la supervision des services d'IA. Les contrôles d'infrastructure, la gestion des identités, les secrets et la gouvernance des risques sont traités dans une approche opérationnelle.

À l'issue de la formation, vous disposerez d'une méthode structurée pour préparer l'examen, résoudre des scénarios techniques de type CyberLive et valider vos compétences de sécurisation des plateformes d'IA en environnement professionnel.

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

Objectifs

- Analyser les risques et les surfaces d'attaque des applications GenAI et LLM
- Sécuriser les architectures RAG, les bases vectorielles et les sources de connaissance externes
- Concevoir des contrôles de sécurité pour les agents, les outils, les API et les intégrations IA
- Appliquer les pratiques MLOps et MLSecOps au cycle de vie des modèles
- Préparer efficacement les scénarios pratiques de la certification GIAC AI Platform Security (GAIPS)

Public visé

- Ingénieur sécurité IA
- Ingénieur Machine Learning
- Ingénieur sécurité applicative
- Ingénieur sécurité cloud
- Consultant cybersécurité

Pré-requis

- Expérience de la sécurité des applications web et des API
- Connaissances opérationnelles de Python et des environnements Linux
- Maîtrise des concepts fondamentaux de cloud computing, conteneurs et réseaux
- Compréhension des principes de Machine Learning, LLM et développement logiciel

Pré-requis techniques

- Poste sous Windows 11, macOS récent ou distribution Linux récente
- Processeur quatre coeurs, 16 Go de RAM et 30 Go d'espace disque disponible
- Navigateur Google Chrome ou Microsoft Edge dans une version récente
- Accès à Docker Desktop ou à une machine virtuelle compatible avec la virtualisation
- Connexion Internet stable, sans filtrage bloquant les services cloud, les WebSockets ou les laboratoires distants

Programme de notre formation GIAC GAIPS

[Jour 1 - Matin]

Fondamentaux de la sécurité des plateformes IA

- Positionnement de la certification GIAC AI Platform Security (GAIPS) et cartographie de ses domaines évalués
- Architecture d'une application GenAI, rôles des modèles fondamentaux, des API, des données et des composants d'orchestration
- Capacités, limites et surfaces d'attaque des LLM
- Panorama des menaces, injection de prompt, exfiltration de données, abus de modèles et détournement de finalité

- Lecture d'un scénario d'examen et méthode de qualification des risques

[Jour 1 - Après-midi]

RAG et protection de la connaissance

- Principes des architectures RAG, ingestion, chunking, embeddings, recherche et génération
- Risques liés aux bases vectorielles, aux documents sources, aux métadonnées et aux connecteurs externes
- Défense contre les injections indirectes, l'empoisonnement documentaire et les fuites interutilisateurs
- Contrôles de cloisonnement, filtrage contextuel, validation des sources et gouvernance des accès
- Atelier pratique : analyser une chaîne RAG vulnérable et mettre en place des contrôles contre l'injection indirecte et la fuite de données.

[Jour 2 - Matin]

Architecture applicative et intégrations sécurisées

- Modèles d'architecture pour applications GenAI orientées production
- Séparation des responsabilités entre interface, orchestrateur, modèles, outils et services de données
- Sécurisation des API, authentification, autorisation, quotas, validation d'entrées et journalisation
- Gestion des secrets, des identités de service et des droits minimaux
- Analyse des vulnérabilités de la chaîne d'approvisionnement logicielle et des dépendances IA

[Jour 2 - Après-midi]

Sécurité des systèmes agentiques

- Fonctionnement des agents, mémoire, planification, appels d'outils et communication interagents
- Risques de confusion d'autorité, escalade de privilèges, exécution d'actions non désirées et boucles autonomes
- Contrôles des outils, politiques d'autorisation, approbation humaine et limitation des capacités
- Sécurisation des protocoles de contexte et des échanges entre composants agentiques
- Atelier pratique : durcir un agent connecté à des outils métier par des politiques d'accès, des garde-fous et une validation d'actions.

[Jour 3 - Matin]

Infrastructure et déploiement des services IA

- Risques de sécurité des modèles et services IA en environnements cloud, hybrides et conteneurisés
- Segmentation réseau, exposition des endpoints d'inférence et protection des flux de données
- Sécurité des conteneurs, des images, des orchestrateurs et des environnements d'exécution
- Gestion des identités, chiffrement, rotation des secrets et configuration sécurisée des services
- Surveillance des usages, traçabilité des requêtes et détection des comportements anormaux

[Jour 3 - Après-midi]

MLSecOps et sécurisation du cycle de vie

- Chaîne de valeur MLOps, données, entraînement, évaluation, publication et exploitation
- Menaces sur les jeux de données, les artefacts de modèles, les registres et les pipelines automatisés
- Contrôles MLSecOps, provenance, intégrité, validation, revue de code et politiques de déploiement
- Gestion des vulnérabilités, des mises à jour de modèles et des incidents de sécurité IA
- Atelier pratique : auditer un pipeline MLOps et définir les contrôles de sécurité nécessaires avant la mise en production.

[Jour 4 - Matin]

Adaptation des modèles et alignement

- Fine tuning, adaptation de modèles, instruction tuning et mécanismes de modération
- Risques de contamination des données, de comportements non alignés et de régression des protections
- Évaluation de la robustesse des modèles face aux requêtes adverses et aux contournements de garde-fous
- Stratégies de filtrage, politiques de contenu, red teaming et tests de sécurité continus
- Critères de choix entre contrôle applicatif, contrôle de modèle et contrôle d'infrastructure

[Jour 4 - Après-midi]

Gestion des risques et gouvernance IA

- Threat modeling appliqué aux applications GenAI et priorisation des scénarios d'attaque
- Responsabilité, traçabilité, protection des données et exigences de conformité
- Conception d'une stratégie de défense adaptée aux enjeux métier, techniques et réglementaires
- Plans de réponse aux incidents, investigation, confinement et amélioration continue
- Atelier pratique : réaliser le threat modeling d'une application IA et produire une feuille de route de remédiation priorisée.

[Jour 5 - Matin]

Stratégie de préparation à l'examen

- Révision structurée des huit domaines de compétences de GIAC AI Platform Security (GAIPS)
- Lecture rapide des scénarios, identification des éléments déterminants et élimination des options non pertinentes
- Préparation aux exercices CyberLive, analyse de l'environnement, collecte d'indices et validation des résultats
- Organisation des supports papier autorisés, indexation personnelle et gestion du temps
- Consolidation des erreurs fréquentes sur RAG, agents, MLOps, API et infrastructure

[Jour 5 - Après-midi]

Simulation de certification et consolidation

- Études de cas transverses couvrant architecture, données, modèles, agents et pipelines de déploiement
- Résolution de scénarios de sécurité dans une logique de décision et de justification technique
- Revue des méthodes de diagnostic, des contrôles compensatoires et des priorités de remédiation
- Plan de révision individuel orienté vers le passage de l'examen officiel
- Atelier pratique : réaliser une simulation de scénario CyberLive combinant analyse d'architecture IA, investigation et mise en oeuvre de mesures de protection.

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.