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

Mis à jour le 14/01/2026

S'inscrire

Formation CompTIA SecAI+? : Certification (CY0-001)

ALL-IN-ONE : EXAMEN INCLUS AU TARIF

5 jours (35 heures)

Présentation

Notre formation CompTIA SecAI+ validera votre expertise à la convergence critique entre la cybersécurité et l'intelligence artificielle. Cette certification atteste de votre capacité à sécuriser les systèmes d'IA, tout en tirant parti de ces technologies pour renforcer la défense de votre organisation.

Lors de cette formation, vous bénéficierez d'un programme complet pour vous préparer à cet examen. Nous entamerons cette formation par les concepts essentiels de l'IA (LLM, Machine Learning) et leur cycle de vie, afin de comprendre ce que nous devons protéger.

Vous apprendrez également à maîtriser la modélisation des menaces (OWASP Top 10 LLM, MITRE ATLAS) et à implémenter des barrières de sécurité (Guardrails) pour les modèles et les données. À l'issue de la formation, vous saurez utiliser l'IA comme outil de défense (analyse, automatisation) tout en détectant les attaques spécifiques comme le Prompt Injection ou le Poisoning.

Comme toutes nos formations, celle-ci vous présentera la dernière version des objectifs de l'examen (CY0-001) et privilégie une approche pratique via des labs.

Objectifs

- Comprendre et distinguer les types d'IA (GenAI, LLM, Deep Learning).
- Sécuriser les systèmes IA via le Threat Modeling et les contrôles d'accès.
- Détecter et contrer les attaques spécifiques (Injection, Hallucinations).
- Utiliser l'IA pour automatiser la réponse aux incidents.
- Appliquer la gouvernance et la conformité (EU AI Act, NIST AI RMF).

Public visé

- Analystes Cybersécurité / SOC
- Ingénieurs Sécurité IA
- Data Scientists & Architectes de sécurité
- Ingénieurs Cloud & DevSecOps

Pré-requis

- 3 à 4 ans dans le domaine informatique, dont plus de 2 ans d'expérience pratique en cybersécurité
- Certifications Security+, CySA+, PenTest+ ou équivalentes recommandées
- Maîtrise de l’anglais technique

Note : Ambient IT n’est pas propriétaire de Comptia Certifications© Cette certification appartient à Comptia, Inc.

Programme de notre Formation CompTIA SecAI+ (CY0-001)

[Jour 1 - Matin]

Fondamentaux de l'IA et Techniques d'Apprentissage

- Types d'IA : Generative AI, Machine Learning, Deep Learning
- Architectures : Transformers, LLM vs SLM, GANs
- Techniques d'entraînement : Supervised vs Unsupervised Learning, Reinforcement Learning
- Concepts clés : Fine-tuning, Epoch, Pruning, Quantization
- Prompt Engineering : Zero-shot, Multi-shot, rôles système et templates
- Atelier pratique : Manipulation de prompts et comparaison de modèles (LLM vs SLM).

[Jour 1 - Après-midi]

Sécurité des Données et Cycle de Vie de l'IA

- Traitement des données : Data cleansing, Data lineage et provenance
- Technologies : RAG (Retrieval-Augmented Generation), Vector storage et Embeddings
- Sécurité du cycle de vie : De la collecte au déploiement
- Validation et surveillance : Human-in-the-loop, supervision et feedback
- Principes de conception : Trustworthiness et authenticité
- Atelier pratique : Analyse du cycle de vie des données et identification des risques.

[Jour 2 - Matin]

Modélisation des Menaces pour l'IA

- Référentiels : OWASP Top 10 LLM et ML Security Top 10
- Frameworks : MITRE ATLAS et MIT AI Risk Repository
- Gestion des vulnérabilités : CVE AI Working Group
- Analyse des risques spécifiques aux systèmes IA
- Atelier pratique : Threat modeling sur un cas d'usage avec MITRE ATLAS.

[Jour 2 - Après-midi]

Contrôles de Sécurité et Gestion des Accès

- Contrôles du modèle : Model guardrails, templates de prompts
- Contrôles Gateway : Prompt firewalls, Rate limits, Token limits
- Gestion des accès : Modèles, Données, Agents et API
- Tests et validation des barrières de sécurité (Guardrails)
- Atelier pratique : Configuration de règles de filtrage et de limites d'accès.

[Jour 3 - Matin]

Sécurité des Données et Chiffrement

- Exigences de chiffrement : In transit, At rest, In use
- Protection des données : Anonymisation, Masquage, Rédaction
- Classification et minimisation des données
- Gestion des étiquettes (Data classification labels)
- Atelier pratique : Mise en œuvre de techniques d'anonymisation sur un dataset.

[Jour 3 - Après-midi]

Surveillance et Audit des Systèmes IA

- Monitoring : Prompts (Query/Response) et Logs
- Protection des journaux : Log sanitization
- Surveillance des coûts : Tokens, Stockage, Processing
- Audit de qualité : Détection d'Hallucinations, Biais et Équité
- Atelier pratique : Analyse de logs et détection d'anomalies de coûts.

[Jour 4 - Matin]

Analyse des Attaques et Contre-mesures

- Attaques sur les entrées : Prompt Injection, Jailbreaking
- Attaques sur le modèle : Poisoning, Model Inversion, Model Theft
- Attaques sur la sortie : Insecure output handling, Hallucinations

- Contre-mesures : Least privilege, Validation des entrées, Encryption
- Atelier pratique : Simulation d'une attaque par Prompt Injection et mitigation.

[Jour 4 - Après-midi]

L'IA au service de la Défense (Blue Team)

- Outils : Chatbots sécurité, Plugins IDE, Assistants personnels
- Cas d'usage : Analyse de vulnérabilité, Pattern recognition, Threat modeling
- Automatisation : Scripting (Low-code/No-code), Synthèse documentaire
- Intégration CI/CD : Code scanning, Tests unitaires automatisés
- Atelier pratique : Utilisation d'un assistant IA pour l'analyse de code sécurisé.

[Jour 5 - Matin]

L'IA comme Vecteur d'Attaque et Gouvernance

- Attaques assistées par IA : Deepfakes, Social Engineering avancé
- Automatisation offensive : Génération de malwares, Polymorphisme
- Structures de gouvernance : AI Center of Excellence
- Rôles clés : AI Architect, Data Scientist, AI Risk Analyst
- Atelier pratique : Identification de contenus générés par IA (Deepfake/Phishing).

[Jour 5 - Après-midi]

Risques, Conformité et Réglementations

- Risques IA : Biais, Fuite de données, Shadow AI
- Principes : Fairness, Transparence, Explicabilité
- Réglementations : EU AI Act, Standards OECD, ISO
- Frameworks : NIST AI RMF (Risk Management Framework)
- Conformité : Souveraineté des données et politiques d'entreprise
- Atelier pratique : Évaluation de conformité d'un projet IA selon le NIST AI RMF.

FAQ – QUESTIONS / RÉPONSES

Dans quelle langue la formation Comptia SecAI+ vous est enseignée ?

La formation est en français.

L’examen est-il compris dans le prix de la formation ?

Oui, le prix de la certification est inclus au coût de la formation ($330 à titre indicatif). Vous

pourrez passer l'examen à la fin de la session.

Comment se déroule l'examen pour la certification Comptia SecAI+ ?

L'examen consiste en un QCM basé sur la performance composé de **90 questions** maximum.

Il s'effectue en ligne dans un centre d'examen agréé Pearson Vue.

Cet examen dure **90 minutes**, les langues disponibles sont l'anglais

Pour réussir cet examen, il faut atteindre au minimum 750 points, sur une échelle de 100 à 900 points.

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.