Formation Officielle CompTIA SecAI+ certifiante

Maîtriser la Cybersécurité pour l'Intelligence Artificielle – 5 jours

Ce programme est conçu pour transformer des professionnels de la cybersécurité en experts capables de sécuriser les systèmes d'IA et d'utiliser l'IA pour renforcer la posture de sécurité d'une entreprise.

Durée : 35 heures (5 jours)

Profil du stagiaire
Administrateurs réseau, ingénieurs en cybersécurité, analystes SOC, et ingénieurs en IA/ML souhaitant se spécialiser en sécurité

Prérequis

- 3 à 4 ans d'expérience en informatique
- Environ 2 ans d'expérience pratique en cybersécurité

OBJECTIFS PEDAGOGIQUES
À l'issue de cette formation, le candidat sera capable de :

- Comprendre les concepts fondamentaux de l'IA appliqués à la sécurité.
- Sécuriser les systèmes d'IA via des contrôles techniques et des accès rigoureux.
- Utiliser l'IA pour automatiser les tâches de sécurité et améliorer la détection des menaces.
- Gérer les risques, la gouvernance et la conformité (GRC) liés à l'IA à l'échelle mondiale

Répartition du Programme (Domaines de l'Examen)
Le contenu est structuré selon les quatre domaines de compétences de la certification :

Domaine	Thématique	Poids
1.0	Concepts de base de l'IA liés à la cybersécurité [11]	17%
2.0	Sécurisation des systèmes d'IA [12]	40%
3.0	Sécurité assistée par l'IA [13]	24%
4.0	Gouvernance, Risque et Conformité (GRC) de l'IA [14]	19%

CONTENU

Jour 1 : Fondamentaux et Données de l'IA

- **Types d'IA :** Machine Learning, Deep Learning, LLM, SLM et GANs
- **Techniques d'entraînement :** Apprentissage supervisé/non-supervisé, Fine-tuning, élagage (Pruning) et quantification
- **Prompt Engineering :** Zero-shot, One-shot, Multi-shot et rôles système
- **Sécurité des données :** Cycle de vie, lignage des données (lineage), intégrité et provenance
- **Techniques avancées :** RAG (Retrieval-augmented generation) et stockage vectoriel

Jour 2 : Protection et Contrôles Techniques

- **Modélisation des menaces :** Utilisation de l'OWASP Top 10 pour LLM, MIT AI Risk Repository et MITRE ATLAS
- **Contrôles de sécurité :** Mise en œuvre de garde-fous (guardrails), pare-feu de prompt et limites de jetons (tokens)
- **Gestion des accès :** Sécurisation des accès aux modèles, aux données et aux APIs
- **Protection des données :** Chiffrement (au repos, en transit, en cours d'utilisation), anonymisation et masquage

Jour 3 : Audit, Attaques et Défenses

- **Surveillance et Audit :** Détection des hallucinations, analyse des biais et suivi des coûts de l'IA
- **Analyse d'attaques :** Injection de prompts, empoisonnement de modèle (poisoning), jailbreaking et vol de modèle
- **Contrôles compensatoires :** Mise en place de mesures pour contrer le déni de service (DoS) du modèle et la divulgation d'informations sensibles

Jour 4 : L'IA comme Outil de Défense

- **Outils assistés par l'IA :** Utilisation des plug-ins d'IDE, de CLI et du protocole MCP (Model Context Protocol)
- **Cas d'usage sécurité :** Analyse de vulnérabilités, tests de pénétration automatisés et détection d'anomalies

- **Vecteurs d'attaque augmentés :** Deepfakes, ingénierie sociale automatisée et création de malwares via l'IA
- **Automatisation :** Scripts Low-code/No-code, agents d'IA pour l'incident response et intégration CI/CD

Jour 5 : Gouvernance, Éthique et Conformité

- **Structures organisationnelles :** Rôles (IA Architect, IA Security Architect) et politiques internes
- **IA Responsable :** Transparence, explicabilité, équité et protection de la vie privée
- **Cadres réglementaires :** EU AI Act, normes ISO, standards de l'OCDE et NIST AIRMF
- **Risques métiers :** Shadow AI, perte de propriété intellectuelle et risques de réputation.

Tarif : 3500 €HT (hors certification non obligatoire) en pré-order (sortie Fev 26)
Tarif susceptible de changer à tout moment sur 2026