

CompTIA SecAI+ (SECAI)

ID SECAI Prix CHF 2 089,- (Hors Taxe) Durée 3 jours

A qui s'adresse cette formation

- Analyste sécurité
- Analyste SOC
- Administrateur systèmes senior
- Ingénieur DevSecOps / CI/CD
- Spécialiste des opérations cyber militaires
- Ingénieur Cloud
- Testeur d'intrusion / Consultant sécurité
- Data Scientist / Ingénieur ML
- Responsable risques et conformité

Pré-requis

Il est recommandé d'avoir :

- 3 à 4 ans d'expérience en IT, avec environ 2 ans d'expérience pratique en cybersécurité.
- Security+, CySA+, PenTest+ ou équivalent

Objectifs

À l'issue de ce cours, vous devrez être capable de :

- Maîtriser les concepts fondamentaux de l'IA (types d'IA, IA générative, transformers, machine learning/deep learning, NLP, RAG) ainsi que les principes de sécurité des données et des modèles qui en découlent
- Appliquer une démarche de threat modeling adaptée aux systèmes IA et déployer les contrôles de sécurité correspondants (guardrails, gateways, quotas d'usage, tests de contrôles)
- Concevoir et gérer les contrôles d'accès aux modèles, agents et API IA (chiffrement, monitoring, audit, suivi de performance et de coûts)
- Identifier les principales techniques d'attaque visant les systèmes IA (backdoors, empoisonnement et inversion de modèle, vol de modèle) et définir des contrôles compensatoires ainsi qu'une analyse post-incident
- Exploiter l'IA comme levier opérationnel pour la sécurité (détection, analyse de vulnérabilités, automatisation, DevSecOps) tout en anticipant son usage offensif (ingénierie sociale, reconnaissance)
- Structurer une gouvernance IA responsable, intégrant

gestion des risques, conformité réglementaire et reporting

Contenu

Module 1 — Concepts d'IA et de données pour la cybersécurité

- Concepts d'IA et principaux types d'IA
- IA générative et transformers
- Machine learning et deep learning
- Traitement du langage naturel (NLP)
- Approches d'entraînement des modèles d'IA
- Fondamentaux du prompt engineering
- Considérations de sécurité des modèles
- Types de données IA et techniques de sécurisation des données
- Concepts de RAG (génération augmentée par récupération)
- Intégrité des données et contrôles de traitement

Module 2 — Modélisation des menaces et sécurisation des systèmes d'IA

- Fondamentaux de la modélisation des menaces IA
- Processus et prérequis de la modélisation des menaces
- Cadres de modélisation des menaces IA
- Types de contrôles de sécurité IA
- Guardrails de modèles et templates de prompts
- Contrôles de passerelle et d'interface
- Quotas d'utilisation et contrôles de limitation
- Tests des contrôles de sécurité

Module 3 — Contrôles d'accès pour l'IA

- Principes et modèles de contrôle d'accès pour l'IA
- Contrôles d'accès aux modèles et agents
- Sécurité des accès API et réseau
- Contrôles de sécurité des données IA
- Mesures de chiffrement et de protection des données
- Surveillance et journalisation des systèmes IA
- Suivi des performances et des coûts
- Audit IA et suivi de conformité

Module 4 — Menaces IA et contrôles compensatoires

- Sécurité du cycle de vie de l'IA
- Considérations éthiques de conception de l'IA

- Types et techniques d'attaques sur l'IA
- Attaques de type backdoor et cheval de Troie sur les modèles
- Empoisonnement et inversion de modèle
- Risques de vol de modèle
- Stratégies de contrôles compensatoires
- Analyse post-incident IA

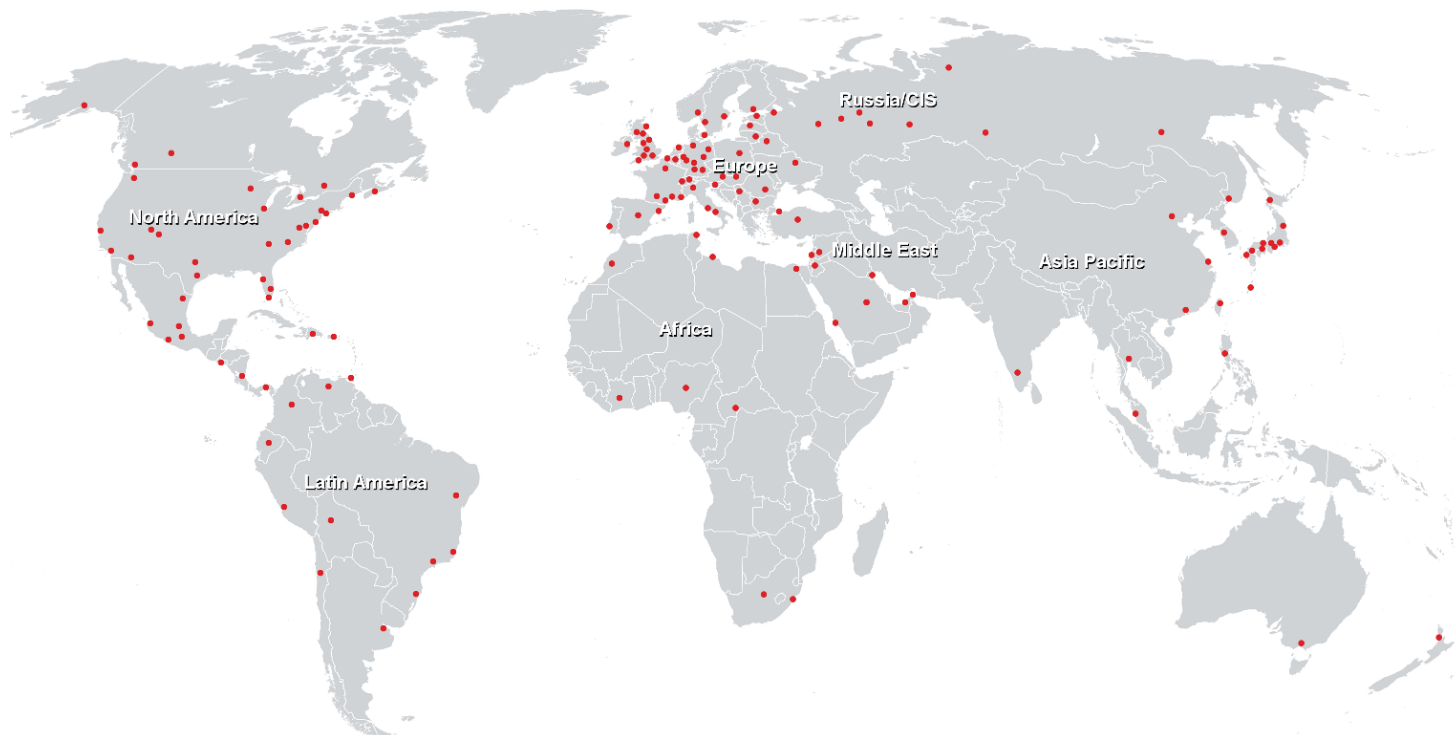
Module 5 — Exploiter l'IA dans les opérations de sécurité

- Outils de sécurité dotés d'IA
- Cas d'usage de l'IA en détection et analyse
- IA pour l'évaluation des vulnérabilités
- Vecteurs d'attaque renforcés par l'IA
- IA pour l'ingénierie sociale et la tromperie
- Techniques de reconnaissance par IA
- Automatisation pilotée par IA
- IA dans les workflows DevSecOps
- Scripting et synthèse assistés par IA

Module 6 — Gouvernance, risques et conformité de l'IA

- Structures de gouvernance IA
- Rôles organisationnels liés à l'IA
- Principes d'IA responsable
- Identification et évaluation des risques IA
- Thématiques réglementaires liées à l'IA
- Cadres de conformité pour l'IA
- Conception de politiques IA organisationnelles
- Reporting de conformité

Centres de formation dans le monde entier



Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3
CH-8304 Wallisellen
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>