0 805 950 800 · appel gratuit
demande@sparks-formation.com

Certifiante

Formation CompTIA SecAI+ (SECAI)

Réf. SF34720

Préparez et obtenez la certification CompTIA SecAI+ pour sécuriser les systèmes d'IA de votre organisation et faire de l'IA un levier opérationnel de votre défense.

5 j	3 500 € HT	0
Durée	Inter / participant	Sessions à venir

Objectifs pédagogiques

✓ Distinguer les principaux types et techniques d'IA (IA générative, apprentissage automatique, transformers, NLP, RAG) et leurs implications sur la sécurité des données

✓ Modéliser les menaces propres aux systèmes d'IA en s'appuyant sur les référentiels du marché (OWASP LLM Top 10, MITRE ATLAS, MIT AI Risk Repository)

✓ Implémenter les contrôles de sécurité d'un système d'IA : guardrails, passerelles de prompts, contrôles d'accès aux modèles, agents et API, chiffrement, supervision et audit

✓ Analyser les preuves d'une attaque visant l'IA (injection de prompt, empoisonnement, inversion, vol de modèle) et recommander les contrôles compensatoires adaptés

✓ Utiliser des outils dotés d'IA pour automatiser les tâches de sécurité (détection, analyse de vulnérabilités, CI/CD) tout en anticipant l'usage offensif de l'IA

✓ Évaluer les risques et la conformité d'un usage de l'IA au regard des cadres de gouvernance (NIST AI RMF, EU AI Act, normes ISO)

✓ Réussir l'examen de certification CompTIA SecAI+ (CY0-001)

Public visé & prérequis

Public visé Tout public

Prérequis- 3 à 4 ans d'expérience en informatique, dont environ 2 ans de pratique opérationnelle en cybersécurité - Certification Security+, CySA+, PenTest+ ou niveau de connaissances équivalent - Anglais technique en lecture — supports de cours officiels en anglais (examen de certification en anglais) - Également recommandé : une aisance avec un environnement Python / Jupyter et la ligne de commande, pour tirer pleinement parti des travaux pratiques

Programme détaillé

Concepts d'IA et sécurité des données

– Types d'IA : IA générative, apprentissage automatique, apprentissage statistique, transformers, apprentissage profond
– Traitement du langage naturel : grands modèles de langage (LLM), petits modèles de langage (SLM), réseaux antagonistes génératifs (GAN)
– Techniques d'entraînement des modèles : apprentissage supervisé, non supervisé, par renforcement, validation de modèle
– Fine-tuning : epoch, pruning, quantization
– Prompt engineering : prompts système et utilisateur, prompting zero-shot, one-shot et multi-shot, rôles système, templates
– Traitement des données : nettoyage, vérification, lignage, intégrité, provenance, augmentation, équilibrage
– Types de données et watermarking : données structurées, semi-structurées, non structurées, marquage des contenus générés
– RAG (génération augmentée par récupération) : stockage vectoriel et embeddings

Activités pratiques :

– Comparaison de réponses d'un LLM selon la structuration du prompt système et le nombre d'exemples fournis
– Mise en place d'une chaîne RAG simple : indexation de documents, embeddings, interrogation
– Analyse d'un jeu de données d'entraînement : détection de déséquilibres et vérification de la provenance

© 2026 Sparks Formation. Tous droits réservés. Fiche générée depuis https://www.sparks-formation.com/formation/comptia-secai-certification/

Modélisation des menaces et contrôles de sécurité des systèmes d'IA

– Ressources de modélisation des menaces IA : OWASP Top 10 pour les LLM et OWASP Machine Learning Security Top 10
– Référentiels complémentaires : MITRE ATLAS, MIT AI Risk Repository, groupe de travail CVE dédié à l'IA
– Cadres de modélisation des menaces : démarche et application aux architectures d'IA
– Contrôles au niveau du modèle : évaluation de modèle, guardrails, templates de prompts
– Contrôles de passerelle : pare-feu de prompts, limitation de débit, limites de tokens, quotas d'entrée (volume et quantité de données)
– Limites de modalité et contrôles d'accès aux endpoints : restriction des formats acceptés et exposition maîtrisée des points d'entrée
– Test et validation des guardrails : vérification de l'efficacité réelle des contrôles mis en place

Activités pratiques :

– Modélisation des menaces d'une application LLM d'entreprise à partir du OWASP Top 10 pour les LLM
– Cartographie de techniques d'attaque observées sur MITRE ATLAS
– Configuration de guardrails et de quotas sur une passerelle d'IA, puis test de contournement

Contrôles d'accès, protection des données et supervision

– Contrôles d'accès aux systèmes d'IA : accès aux modèles, aux données, aux agents, au réseau et aux API
– Exigences de chiffrement : données en transit, au repos et en cours d'utilisation
– Sûreté des données : anonymisation, labels de classification, expurgation, masquage, minimisation
– Supervision des prompts : analyse des requêtes et des réponses, niveau de confiance des réponses
– Journalisation : supervision, assainissement et protection des journaux
– Supervision des débits et des coûts d'IA : prompts, stockage, réponses, traitement
– Audit qualité et conformité : hallucinations, exactitude, biais et équité, accès

Activités pratiques :

– Mise en œuvre de contrôles d'accès différenciés pour un modèle, un agent et une API
– Configuration du masquage et de l'expurgation de données sensibles avant envoi à un modèle
– Construction d'un tableau de bord de supervision des prompts, des coûts et des anomalies de débit

Cycle de vie de l'IA, attaques et contrôles compensatoires

– Sécurité tout au long du cycle de vie de l'IA : cas d'usage métier et alignement avec les objectifs de l'entreprise, collecte des données, préparation, développement et sélection du modèle
– Suite du cycle de vie : évaluation, déploiement, validation, supervision et maintenance, boucle de retour et itération
– Principes de conception centrée sur l'humain : human-in-the-loop, supervision humaine, validation humaine
– Attaques sur les entrées et le comportement du modèle : injection de prompt, jailbreaking, manipulation des entrées, contournement des guardrails, hallucinations, introduction de biais
– Attaques sur le modèle et les données : empoisonnement de données et de modèle, inversion de modèle, vol de modèle, distorsion de modèle (model skewing), attaques par apprentissage par transfert, attaques de la chaîne d'approvisionnement IA
– Attaques sur les sorties et les intégrations : atteinte à l'intégrité des sorties, traitement non sécurisé des sorties, inférence d'appartenance, divulgation d'informations sensibles, manipulation des intégrations applicatives, plug-ins mal conçus, déni de service sur modèle
– Risques d'usage : agentivité excessive (excessive agency) et confiance excessive dans les réponses (overreliance)
– Contrôles compensatoires : pare-feu de prompts, guardrails, contrôles d'accès, contrôles d'intégrité des données, chiffrement, templates de prompts, limitation de débit, moindre privilège
– Analyse post-incident : exploitation des preuves pour caractériser l'attaque et ajuster les contrôles

Activités pratiques :

– Scénario d'injection de prompt et de jailbreak sur un assistant d'entreprise, puis définition des contrôles compensatoires
– Analyse des traces d'un incident d'empoisonnement de données et proposition de contrôles d'intégrité
– Étude de cas sur un vol de modèle : identification des indices et durcissement des accès

L'IA au service et au détriment des opérations de sécurité

– Outils dotés d'IA : plug-ins d'IDE, de navigateur et de ligne de commande, chatbots, assistants personnels, serveurs MCP (Model Context Protocol)
– Cas d'usage défensifs : correspondance de signatures, qualité de code et linting, analyse de vulnérabilités, tests d'intrusion automatisés, détection d'anomalies, reconnaissance de motifs
– Cas d'usage opérationnels : gestion des incidents, modélisation des menaces, détection de fraude, traduction, synthèse
– Vecteurs d'attaque renforcés par l'IA : contenus générés (deepfakes) pour l'usurpation d'identité, la mésinformation et la désinformation, réseaux antagonistes
– Techniques offensives assistées par IA : reconnaissance, ingénierie sociale, obfuscation, corrélation automatisée de données
– Génération automatisée d'attaques : découverte de vecteurs d'attaque, payloads, malwares, honeypots, attaques par déni de service

© 2026 Sparks Formation. Tous droits réservés. Fiche générée depuis https://www.sparks-formation.com/formation/comptia-secai-certification/

distribué
– Automatisation des tâches de sécurité : outils de scripting low-code et no-code, synthèse et résumé documentaires, gestion des tickets de réponse à incident
– Gestion des changements et agents IA : approbations assistées par IA, déploiement et rollback automatisés, recours à des agents
– IA dans les chaînes CI/CD : analyse de code, analyse de composition logicielle, tests unitaires, tests de régression, tests de modèle

Activités pratiques :

– Analyse d'un lot de vulnérabilités assistée par un outil doté d'IA, avec priorisation argumentée
– Automatisation d'une tâche de triage d'incidents à l'aide d'un script généré et revu par l'analyste
– Intégration d'une analyse de code et d'une analyse de composition logicielle assistées par IA dans un pipeline CI/CD
– Étude d'un scénario d'ingénierie sociale amplifié par deepfake et définition des parades

Gouvernance, risques et conformité de l'IA

– Structures de gouvernance : centre d'excellence IA, politiques et procédures relatives à l'IA
– Rôles organisationnels liés à l'IA : data scientist, architecte IA, ingénieur en apprentissage automatique, ingénieur plateforme, ingénieur MLOps, architecte sécurité IA, ingénieur gouvernance IA, analyste risques IA, auditeur IA, ingénieur données
– Principes d'IA responsable : équité, fiabilité et sûreté, transparence, confidentialité et sécurité, explicabilité, inclusivité, redevabilité, cohérence, sensibilisation
– Risques associés à l'IA : introduction de biais, fuite accidentelle de données, atteinte à la réputation, exactitude et performance du modèle, risques liés à la propriété intellectuelle, systèmes autonomes
– Shadow IT et Shadow AI : usages non encadrés de l'IA dans l'organisation
– Cadres réglementaires et normatifs : EU AI Act, standards de l'OCDE, normes ISO relatives à l'IA, NIST AI Risk Management Framework
– Politiques d'entreprise : usages sanctionnés et non sanctionnés, modèles privés et publics, gouvernance des données sensibles
– Évaluations de conformité tierces et souveraineté des données : contrôle des fournisseurs et localisation des traitements

Activités pratiques :

– Classification d'un cas d'usage d'IA au regard des niveaux de risque de l'EU AI Act
– Rédaction d'une politique d'usage de l'IA encadrant modèles publics et données sensibles
– Auto-évaluation d'un système d'IA à l'aide du NIST AI Risk Management Framework

Préparation à la certification

– Modalités de l'examen : QCM et questions basées sur la performance, 60 minutes, 60 questions maximum, seuil de réussite 600 sur 900, examen disponible en anglais et en japonais
– Examen blanc : passage d'un test en conditions réelles
– Stratégies de réponse : gestion du temps, lecture des questions, élimination des distracteurs
– Révision ciblée : synthèse des points clés par domaine de la trame officielle, avec un accent sur la sécurisation des systèmes d'IA (40 % de l'examen)
– Planification : inscription à l'examen et conseils de préparation post-formation

Activités pratiques :

– Examen blanc chronométré avec correction commentée
– Atelier de révision par domaine avec quiz

© 2026 Sparks Formation. Tous droits réservés. Fiche générée depuis https://www.sparks-formation.com/formation/comptia-secai-certification/

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans d'expertise	1 068+ formations	11 178 apprenants formés/an	+67 Net Promoter Score

Avis des participants

Note moyenne des participants de la filière Cybersécurité et Protection des Données : 4,9/5 — 13 avis

William B. — Prévoir l'envoie à chaque particiapnt du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Ils nous font confiance

Cette année notre filière Cybersécurité et Protection des Données a accompagné plus de 69 entreprises dont :

AVEM MÉTROPOLE DE LYON ACTIMAGE CONSULTING SAS ADISTA ADVENTIEL AIGA ALCYOR ALDORIA ALSTOM ALTEN SA +59 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.

Qualiopi processus certifié RÉPUBLIQUE FRANÇAISE

SILVER | Top 15% ecovadis Sustainability Rating JAN 2026

Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com

© 2026 Sparks Formation. Tous droits réservés. Fiche générée depuis https://www.sparks-formation.com/formation/comptia-secai-certification/