CompTIA SecAI+ Certification Prep Course

Durée: 5 Jours **Réf de cours: GK021** **Version: CY0-001**

Résumé:

La certification CompTIA SecAI+ atteste des compétences requises pour les professionnels de la cybersécurité chargés de sécuriser les systèmes basés sur l'IA.
La formation de préparation à la certification CompTIA SecAI+ est conçue pour préparer les participants à l'examen CY0-001.
Cette formation permet aux professionnels de la cybersécurité d'acquérir les compétences pratiques nécessaires pour identifier et contrer les menaces liées à l'IA, telles que l'injection de prompts, l'utilisation abusive des modèles, les fuites de données et les attaques adversariales. Ils seront en mesure d'appliquer les principes de « sécurité dès la conception » aux cas d'utilisation, aux politiques et aux flux de travail liés à l'IA.

La certification SecAI+ offre également un moyen vérifiable de démontrer vos compétences aux employeurs, ce qui vous aidera à vous démarquer sur un marché concurrentiel.

Cette formation couvre les domaines clés évalués lors de l'examen SecAI+ : concepts de base de l'IA liés à la cybersécurité, sécurisation des systèmes d'IA, sécurité assistée par l'IA, ainsi que gouvernance, risques et conformité en matière d'IA.
Les participants développent les connaissances et les compétences pratiques nécessaires pour comprendre les concepts clés de l'IA, sécuriser les systèmes d'IA à l'aide de divers contrôles techniques, tirer parti de l'IA pour renforcer la sécurité de l'entreprise tout en automatisant les tâches de sécurité, et comprendre l'impact de la gouvernance, des risques et de la conformité (GRC) sur les technologies d'IA à l'échelle globale.

À l'issue de la formation, les participants seront prêts à contribuer aux activités de gestion des risques, de gouvernance et de réponse aux incidents impliquant l'IA.

Mis à jour 27/10/2026

Public visé:

Cette formation s'adresse aux personnes qui possèdent déjà une certification CompTIA en cybersécurité (telle que Security+, CySA+, PenTest+, etc.) ou une expérience équivalente, et qui souhaitent approfondir leurs compétences pour évoluer vers des postes en pleine mutation dans le domaine des technologies d'IA.

Objectifs pédagogiques:

- À l'issue de cette formation, les participants devraient être capables de :
- Appliquer des concepts fondamentaux et avancés en matière d'IA afin de renforcer la cybersécurité de leur organisation.
- Mettre en œuvre des contrôles de sécurité robustes et les meilleures pratiques pour protéger les systèmes d'IA et les données.
- Tirer parti des outils basés sur l'IA pour améliorer la détection des menaces, la réponse à celles-ci et l'automatisation des opérations de sécurité.
- Maîtriser les enjeux mondiaux en matière de gouvernance, de risques et de conformité

Pré-requis:

Nous recommandons fortement 3 à 4 ans d'expérience dans le domaine de l'informatique, dont environ 2 ans d'expérience pratique en cybersécurité, ainsi que des connaissances de base en environnement Python / Jupyter et en ligne de commande pour les travaux pratiques.

Test et certification

Cette formation prépare à l'examen Comptia SecAI+ .

- Code de l'examen : CY0-001
- Nombre de questions : 60 au maximum, à choix multiples et basées sur les compétences

Une certification préliminaire en cybersécurité (Security+, CySA+, PenTest+, ...) est recommandée mais non obligatoire.

Un bon niveau d'anglais technique (lecture des supports officiels et passage de l'examen en anglais) est nécessaire.

- Nombre de points requis pour réussir : 600 (sur une échelle de 100 à 900)

Le voucher d'examen n'est pas inclus dans le prix de la formation.

Après cette formation, nous vous conseillons le(s) module(s) suivant(s):

Pas de recommandation spécifique.

Contenu:

Module 1 : Concepts liés à l'IA et aux données pour la cybersécurité

Module 2 : Mise en œuvre de la modélisation des menaces et sécurisation des systèmes d'IA

Module 3 : Mise en place de contrôles d'accès pour l'IA

Module 4 : Identification des menaces spécifiques à l'IA et des contrôles complémentaires

Module 5 : Exploitation de l'IA en matière de sécurité et compréhension de ses utilisations abusives

Module 6 : Comprendre la gouvernance, les risques et la conformité propres à l'IA

Méthodes pédagogiques :

Un support de cours officiel est fourni aux participants.

Autres moyens pédagogiques et de suivi:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement