

Certified AI Security Professionnal - CAISP (Certification comprise)

Référence : **SECCAISP**

Durée : **5 jours (35 heures)**

Certification : **PECB Certified
Artificial Intelligence Security
Professional**

CONNAISSANCES PRÉALABLE

- Posséder de solides connaissances en cybersécurité et en sécurité de l'information
- Une bonne compréhension des principes généraux de sécurité, notamment la modélisation des menaces, le contrôle d'accès, la gestion des incidents et la surveillance de la sécurité, est requise
- Une connaissance de base du fonctionnement des systèmes d'apprentissage automatique, incluant des concepts tels que l'entraînement des modèles, les pipelines de données et les services basés sur les API, est également nécessaire
- Le matériel pédagogique et la certification ne sont actuellement pas disponibles en français, une bonne compréhension de la langue anglaise est fortement recommandée

PROFIL DES STAGIAIRES

- Ingénieurs en IA et apprentissage automatique chargés du développement, du déploiement ou de la maintenance des systèmes d'IA
- Professionnels de la cybersécurité et de la sécurité de l'information souhaitant approfondir leurs connaissances sur les menaces et les défenses spécifiques à l'IA
- Analystes SOC et spécialistes du renseignement sur les menaces travaillant dans des environnements de sécurité intégrant l'IA
- Architectes et consultants en sécurité informatique concevant ou auditant des architectures de systèmes d'IA
- Professionnels de la gestion des risques et de la conformité travaillant avec des cadres de gouvernance de l'IA et des exigences réglementaires
- Data scientists et développeurs d'IA souhaitant appliquer les bonnes pratiques de sécurité tout au long du cycle de vie du développement de l'IA
- Responsables techniques et chefs de projet en charge de la stratégie et de la gestion des programmes de sécurité de l'IA

OBJECTIFS

- Expliquer l'architecture et le fonctionnement de l'apprentissage automatique, de l'apprentissage profond, des LLM et des agents d'IA, et identifier les risques liés à leur conception, leur entraînement et leur déploiement
- Analyser les menaces pesant sur les systèmes d'IA et de LLM à l'aide de MITRE ATLAS et du Top 10 des LLM de l'OWASP, tout au long du cycle de vie d'une attaque d'IA
- Mettre en œuvre des contrôles de sécurité, des stratégies de surveillance et des processus de veille sur les menaces afin de détecter, contenir et analyser les activités malveillantes
- Concevoir et évaluer un programme de sécurité de l'IA couvrant la réponse aux incidents, la gouvernance de la chaîne d'approvisionnement, la conformité réglementaire, l'architecture sécurisée et les exercices de simulation d'attaques (red teaming)

CERTIFICATION PRÉPARÉE

L'examen « PECB Certified Artificial Intelligence Security Professional » répond pleinement aux exigences du programme d'examen et de certification PECB. Il n'est disponible qu'en Anglais, comporte 80 questions et dure 3 heures.

Pour plus d'informations sur le type d'examen, les langues disponibles et autres détails, veuillez consulter la [liste des examens PECB](#) et le [règlement des examens](#).

MÉTHODES PÉDAGOGIQUES

- Mise à disposition d'un poste de travail par stagiaire
- Remise d'une documentation pédagogique numérique pendant le stage
- La formation est constituée d'apports théoriques, d'exercices pratiques et de réflexions
- Le suivi de cette formation donne lieu à la signature d'une feuille d'emargement

FORMATEUR

- Consultant-formateur expert Cybersécurité

MÉTHODES D'ÉVALUATION DES ACQUIS

- Validation des prérequis envoyée en amont de la formation. En l'absence de réponse d'un ou plusieurs participants, un temps sera consacré en ouverture de session pour prendre connaissance du positionnement de chaque stagiaire sur les objectifs pédagogiques évalués
- Auto-évaluation des acquis par le stagiaire via un questionnaire
- Attestation des compétences acquises envoyée au stagiaire
- Attestation de fin de stage adressée avec la facture

ACCESSIBILITÉ DE LA FORMATION

- Si vous avez besoin d'un aménagement pour suivre votre formation dans de bonnes conditions, nous vous invitons à contacter notre référent handicap au 01 71 19 70 30 ou à l'adresse referent.handicap@edugroupe.com. Un échange en amont nous permettra d'étudier avec vous les adaptations possibles.

CONTENU DU COURS

- 1. JOUR 1 - AI, ML, and deep learning fundamentals**
- 2. JOUR 2 - LLM architecture, training workflows, and attack tactics**
- 3. JOUR 3 - AI security controls and mitigation strategies**
- 4. JOUR 4 - Detection, response, and secure deployment**
- 5. JOUR 5 - Certification exam**