

Sécurité des systèmes IA et cyberattaques

Financement

Formation professionnelle continue
Non conventionnée / sans dispositif

Organisme responsable et contact

FORMAPACK
SPANNEUT Louis
05.32.58.32.12
contact@formapack.info

Accès à la formation

Publics visés :

Demandeur d'emploi
Jeune de moins de 26 ans
Personne handicapée
Salarié(e)
Actif(ve) non salarié(e)

Sélection :

Entretien

Niveau d'entrée requis :

Sans niveau spécifique

Conditions d'accès :

Entretien

Prérequis pédagogiques :

Non renseigné

Contrat de
professionnalisation
possible ?

Non

Objectif de la formation

Comprendre les enjeux de sécurité liés à l'intelligence artificielle, et apprendre à sécuriser les modèles et les données pour éviter les attaques adversariales et les fuites d'informations.

Contenu et modalités d'organisation

Vulnérabilités des systèmes IA, Attaques adversariales contre les modèles d'IA, Stratégies de défense et techniques de sécurisation, Gestion des données sensibles, Normes et régulations en matière de sécurité IA, Cas d'études et implémentations pratiques.

Durées de la formation

Parcours de formation personnalisable ? **Oui** Type de parcours **Mixte**

Validation(s) Visée(s)

> Attestation de fin de formation

Et après ?

Suite de parcours

Les participants sauront identifier les vulnérabilités spécifiques aux systèmes d'intelligence artificielle et appliquer des stratégies de défense pour protéger ces systèmes contre les cyberattaques.

Calendrier des sessions

Numéro Carif	Dates de formation	Ville	Organisme de formation	Type d'entrée	CPF	Modalités
00521046	du 04/11/2024 au 31/12/2025	(64)	FORMAPACK		Non éligible	