Auditer et sécuriser l'IA: cybermenaces, éthique et conformité

Durée: 4 jours
Public cible: Professionnel TI

À qui s'adresse cette formation ?

Cadres et équipes responsables des technologies, de la conformité, de la sécurité et des projets IA.

Objectifs de la formation

- Analyser les différences entre les audits classiques en TI et les audits spécifiques à l'intelligence artificielle.
- Classer et distinguer les types d'audits IA (techniques, éthiques, conformité) en fonction de leurs caractéristiques.
- Utiliser les référentiels majeurs (ISO/IEC 42001, NIST AI RMF, MITRE ATT&CK, TRiSM) pour structurer et réaliser un audit IA.
- Planifier et réaliser un audit IA complet en suivant les étapes clés : préparation, collecte d'évidences, analyse, restitution.
- Élaborer une checklist personnalisée et mettre en œuvre des pratiques internes pour assurer la continuité des audits IA.

Description sommaire

Cette formation propose un programme complet pour maîtriser les audits appliqués à l'intelligence artificielle (IA). Elle permet aux participants de comprendre les spécificités des audits IA, d'explorer les principaux cadres de conformité, et de développer une méthodologie pratique pour auditer efficacement les systèmes IA.

Contenu du plan de cours

Semaine 1 : Fondamentaux des audits

Définition et rôle de l'audit en TI et cybersécurité :

-

Copyright © 2026 AFI par Edgenda inc.

Découvrez les spécificités, les étapes et les principaux défis liés aux audits en intelligence artificielle pour assurer la conformité et la sécurité des systèmes numériques.

Semaine 2 : Typologie et cas d'usage des audits IA

Découvrez les différents types d'audits IA :

- Techniques (modèle, données, sécurité), éthiques (biais, transparence, équité) et de gouvernance et conformité. Explorez des cas pratiques : validation réglementaire, réduction des biais et gestion des risques.

Semaine 3 : Référentiels & méthodologie d'audit IA

Panorama des principaux référentiels pour l'IA :

- ISO/IEC 42001 pour le management des systèmes d'IA, NIST AI Risk Management Framework, MITRE ATT&CK appliqué à l'IA, TRiSM (Trust, Risk & Security Management) et principes d'IA responsable.

Semaine 4 : Mise en pratique & simulation d'audit

Découvrez la méthodologie d'audit IA :

- Planification, collecte d'évidences, analyse et restitution. Apprenez à cartographier les risques, définir les contrôles, élaborer une checklist IA, et évaluer la conformité d'un projet IA à travers une étude de cas.

Approche et méthode pédagogique

Ce cours adopte une approche progressive et méthodologique, combinant des exposés conceptuels, des analyses de référentiels et des mises en situation pratiques. L’apprentissage est centré sur la réalisation d’audits d’IA à travers des études de cas, permettant de mobiliser des cadres reconnus et d’appliquer une démarche structurée. La progression vise à développer des compétences concrètes en évaluation des risques, en conformité et en gouvernance des systèmes d’intelligence artificielle.

Prérequis

-

Copyright © 2026 AFI par Edgenda inc.

Connaissances de base en TI et cybersécurité.

- Notions sur l'intelligence artificielle.
- Expérience en conformité, sécurité ou projets technologiques.

Recommandations

Réviser : les bases de la cybersécurité les concepts fondamentaux de l’IA

Se familiariser avec : les enjeux de gouvernance et de conformité

Identifier vos besoins : gestion des risques liés à l’IA audit et contrôle des systèmes IA encadrement éthique et réglementaire

Copyright © 2026 AFI par Edgenda inc.