

# Utiliser l'Intelligence Artificielle (IA) dans le cadre du pentesting

3 jours (21 heures)

Expertise

Présentiel ou classe à distance

à partir de

**2 925 € HT** par personne (TVA en vigueur) Repas inclus en présentiel

Contenu mis à jour le 25/09/2026. Document téléchargé le 07/10/2026.

## Objectifs

A l'issue de cette formation, vous serez capable de :

- Identifier les apports, les limites et les enjeux de l'Intelligence Artificielle (IA) appliquée au pentesting
- Utiliser les outils et frameworks d'IA modernes (LLM, agents autonomes, copilotes offensifs) pour automatiser ou enrichir les tests d'intrusion
- Concevoir et exécuter un scénario complet de pentest hybride (manuel et IA-assisté)
- Identifier les faux positifs, documenter et rapporter efficacement les résultats produits par une IA
- Appliquer les bonnes pratiques éthiques, réglementaires et de gouvernance liées à l'usage de l'IA en Cybersécurité offensive.

Les compétences visées par cette formation font l'objet d'une évaluation.

## À qui s'adresse cette formation ?

Pentesters, red-teamers, consultants en Cybersécurité, auditeurs techniques, RSSI, formateurs et chercheurs en Cybersécurité offensive.

## Prérequis

Maîtriser les étapes classiques du pentest (reconnaissance, scan, exploitation, post-exploitation). Avoir des connaissances de base en Intelligence Artificielle (LLM, prompts, agents). Savoir utiliser les outils standards : Nmap, Metasploit, Burp Suite...

# Programme

## 1 Pendant votre formation

### Utiliser l'Intelligence Artificielle (IA) dans le cadre du pentesting

Jour 1 – Matin

#### Introduction et exploration des outils IA-Pentest

- Introduction au rôle de l'IA dans le pentest moderne
- Etat de l'art : IA Générative, agents multi-outils, copilotes offensifs, frameworks émergents (AutoGPT, LangChain, PentestGPT, GPT-Recon...)
- Présentation des cas d'usage réels par la communauté offensive (OWASP, Black Hat 2025, DefCon AI Village)

*Exemple de travaux pratiques (à titre indicatif)*

- *Installation des environnements de test et premiers prompts pour la reconnaissance automatisée*

Jour 1 – Après-midi

#### Introduction et exploration des outils IA-Pentest – Suite

- OSINT et reconnaissance augmentée par IA : génération automatisée de stratégies d'énumération et analyse des résultats
- Automatisation des scans de vulnérabilités avec IA (reconnaissance intelligente des services, priorisation)

*Exemple de travaux pratiques (à titre indicatif)*

- *Création d'un pipeline IA pour la reconnaissance (Nmap, LLM et Data Parsing)*

Jour 2 – Matin

#### Exploitation, automatisation et Adversaire AI

- Modélisation du pentest hybride : intégration IA dans la phase exploitation / post-exploitation
- Présentation des modules IA-assistés : génération de payloads, fuzzing intelligent, exploitation adaptative
- Introduction à l'Adversaire AI : détournement, contournement et évocation de modèles ML

*Exemple de travaux pratiques (à titre indicatif)*

- *Génération automatisée d'exploits et analyse des faux positifs IA*

Jour 2 – Après-midi

### Exploitation, automatisation et Adversaire AI – Suite

- Pentesting sur environnement vulnérable avec support IA
  - Identification de vulnérabilités
  - Génération de code d'exploitation par IA
  - Interprétation des logs et détection assistée

*Exemple de travaux pratiques (à titre indicatif)*

- *Réalisation d'un scénario complet d'exploitation IA-assistée sur un lab*

Jour 3 – Matin

### Rapport, gouvernance et limites éthiques

- Analyse critique : biais, hallucinations, sécurité des prompts, confidentialité des données
- Cadre légal et éthique : réglementation IA (AI Act, RGPD, responsabilité du pentester IA)

*Exemple de travaux pratiques (à titre indicatif)*

- *Rédaction automatisée d'un rapport de pentest IA avec exportation format pro (Markdown / PDF)*

Jour 3 – Après-midi

*Exemple de travaux pratiques (à titre indicatif)*

- *Simulation d'un pentest complet IA-assisté : du scan à la restitution client*

## Financement

Plusieurs dispositifs de financement sont accessibles via les OPCO (Opérateurs de Compétences), organismes agréés par le ministère du Travail dont le rôle est d'accompagner, collecter et gérer les contributions des entreprises au titre du financement de la formation professionnelle.

Pour plus d'information, une équipe de gestionnaires SKOLAE Formation spécialisée vous accompagne dans le choix de vos formations et la gestion administrative.

[Nous contacter pour en savoir plus →](#)

## Modalités pédagogiques

Formation délivrée en présentiel ou distanciel\* (blended-learning, e-learning, classe virtuelle, présentiel à distance).

Le formateur alterne entre méthode\*\* démonstrative, interrogative et active (via des travaux pratiques et/ou des mises en situation).

Variables suivant les formations, les moyens pédagogiques mis en oeuvre sont :

- Ordinateurs Mac ou PC (sauf pour certains cours de l'offre Management), connexion internet fibre, tableau blanc ou paperboard, vidéoprojecteur ou écran tactile interactif (pour le distanciel)
- Environnements de formation installés sur les postes de travail ou en ligne
- Supports de cours et exercices

En cas de formation intra sur site externe à M2i, le client s'assure et s'engage également à avoir toutes les ressources matérielles pédagogiques nécessaires (équipements informatiques...) au bon déroulement de l'action de formation visée conformément aux prérequis indiqués dans le programme de formation communiqué.

\* nous consulter pour la faisabilité en distanciel

\*\* ratio variable selon le cours suivi

### Accessibilité aux personnes en situation de handicap

## Détails de la session

Du 4 novembre 2026 au 6 novembre 2026 (3 jours / 21 heures)

Metz

Du 4 novembre 2026 au 6 novembre 2026 Metz

- 4 novembre 2026 ..... 9h00 – 16h00
- 5 novembre 2026 ..... 9h00 – 16h00
- 6 novembre 2026 ..... 9h00 – 16h00