

Sessions garanties disponibles

Formation Sécurité et IA Générative : comprendre et maîtriser les risques liés aux LLMs

Réf. SF34349

Explorez les mécanismes des IA modernes et apprenez à identifier et exploiter les vulnérabilités des LLM à travers un challenge pratique et ludique !

1 j Durée	1 000 € HT Inter / participant	2 100 € HT Intra (≤12 pers.)	13 Sessions à venir
--------------	-----------------------------------	---------------------------------	------------------------

Objectifs pédagogiques

- ✓ Comprendre le fonctionnement des IA modernes et des modèles de type LLM
- ✓ Identifier les principales menaces liées à l'utilisation des LLM dans les applications métiers
- ✓ Connaître les 10 risques majeurs selon la taxonomie OWASP LLM 2025
- ✓ Appliquer les bonnes pratiques pour réduire l'exposition aux failles
- ✓ Mettre en pratique les concepts à travers des exercices de sécurité offensifs sur des IA génératives

Public visé & prérequis

Public visé Tous	Prérequis Aucun prérequis pour la partie théorique (présentation des concepts et des risques). Pour la phase challenge, une connaissance de base en Python ou en développement web est recommandée pour au moins un membre du binôme.
-------------------------	--

Programme détaillé

Introduction à l'intelligence artificielle aujourd'hui (30 min)

Notions fondamentales : IA vs Machine Learning, réseaux de neurones, entraînement de modèles
Fonctionnement des applications IA modernes : fine-tuning, déploiement, intégration
Focus sur le RAG (Retrieval-Augmented Generation) : principe et cas d'usage

Nouveaux risques de sécurité liés à l'IA (1h30)

Pourquoi l'IA introduit-elle de nouvelles surfaces d'attaque dans les systèmes d'information ?
Attaques antagonistes : comprendre ce nouveau type de menace ciblant les réseaux neuronaux
Revue des 10 risques majeurs du Top 10 OWASP LLM 2025 :
LLM01 – Injection de prompts
LLM02 – Fuite d'informations sensibles
LLM03 – Vulnérabilités de la chaîne d'approvisionnement
LLM04 – Empoisonnement des données et modèles
LLM05 – Mauvaise gestion des sorties
LLM06 – Capacité d'action excessive
LLM07 – Fuite du prompt système
LLM08 – Faiblesses des vecteurs et embeddings
LLM09 – Dépendance excessive au modèle
LLM10 – Consommation illimitée de ressources
Chaque point est illustré par des scénarios concrets, des exemples d'attaque et des leviers de mitigation.

Challenge pratique (4 à 6h)

Une plateforme interactive avec une douzaine de mini-challenges à réaliser en binôme, accompagnés par le formateur

Chaque défi illustre une ou plusieurs des failles étudiées dans la partie précédente
Classement en temps réel, progression par niveaux de difficulté, accès prolongé après la formation (en option gratuite)

Exemples de challenges :
Prompt injection : forcer le LLM à révéler un mot de passe caché malgré les protections
Injection indirecte : créer un site malveillant pour détourner un service de résumé automatisé
RAG et cloisonnement des données : accéder à des documents censés rester confidentiels

Débriefing final (30 min)

Revue collective des solutions proposées
Explication détaillée des attaques attendues et des mécanismes sous-jacents

Prochaines sessions

DATE	LIEU	STATUT
16/11/2026	à distance	Sur confirmation
12/03/2027	Lyon	Sur confirmation
12/03/2027	Grenoble	Sur confirmation
12/03/2027	Toulouse	Sur confirmation
12/03/2027	à distance	Sur confirmation
25/06/2027	Aix-en-Provence	Sur confirmation

Pourquoi choisir Sparks Formation ?

20 ans d'expertise IT, des formateurs experts et des sessions garanties contre l'annulation.

20 ans
d'expertise

1 068+
formations

11 178
apprenants formés/an

+67
Net Promoter Score

Avis des participants

4,9/5 — 7 avis

William B. — Prévoir l'envoi à chaque participant du livre de CISS au moins un mois avant la formation.

Mickael L. — il est top Romain GARCIA

Votre formateur

Stéphane R. — Formateur

Stéphane intervient notamment sur le développement web et fullstack, ainsi que sur les langages et écosystèmes backend. Son activité de formation remonte à 2015, soit plus de 10 ans d'expérience.

Ils nous font confiance

Cette année notre filière Gouvernance, Risques & Conformité (GRC) a accompagné plus de 30 entreprises dont :

AVEM MÉTROPOLE DE LYON ADISTA ALSTOM ASTEK FRANCE AXA ASSISTANCE FRANCE COMMUNAUTÉ DE COMMUNES DES HAUTS DE FLANDRE CONSORT FRANCE ECONOCOM SERVICES & SOLUTION EGIS +20 autres

Financement & certifications

Cette formation est éligible aux financements OPCO et FNE-Formation. Nos équipes vous accompagnent dans le montage de votre dossier.



Réservez votre place dès maintenant

20 ans d'expertise · 1 000+ formations · NPS +67 · réponse sous 24h ouvrées

0 805 950 800

demande@sparks-formation.com