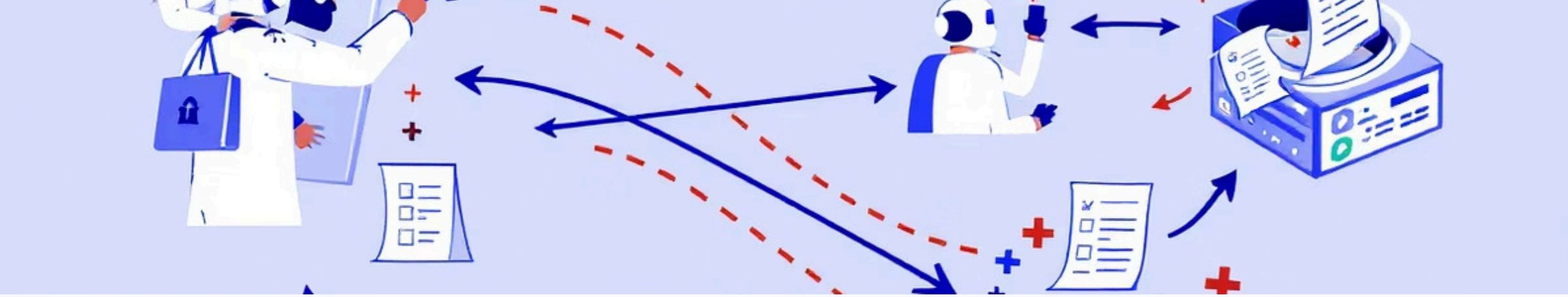
Sécuriser l'IA Générative avec OWASP

OWASP: fondation mondiale dédiée à la sécurité des logiciels

Focus: OWASP GenAI Security Project

Objectif: sensibiliser à l'importance de sécuriser les systèmes IA

par Célia KASSA



Qu'est-ce que l'OWASP GenAI Security Project?

Initiative mondiale

Identifier et atténuer les risques des LLMs

IA générative omniprésente

Chatbots, analyse de données, création de contenu

Projet Flagship depuis 2025

5500+ membres, 110+ entreprises partenaires

Historique du Projet

Mai 2023

Lancement: OWASP Top 10 for LLM Application Security

1

2024

Élargissement: guides CISOs, conformité, deepfakes

2

Mars 2025

Promotion en Flagship Project, adoption mondiale

3

Mission et Objectifs

Identifier

Risques critiques des LLMs

Atténuer

Solutions pratiques pour développeurs

Promouvoir

Adoption éthique et sécurisée de l'IA

OWASP Top 10 pour LLMs

Prompt Injection

Manipulation via instructions malveillantes

Sensitive Information Disclosure

Fuite de données confidentielles

Insecure Output Handling

Utilisation non sécurisée des sorties IA

Ressources Pratiques

Guide Deepfake	Stratégies contre les deepfakes
Checklist Cybersécurité	Pour CISOs et conformité
AI Security Solutions	Catalogue d'outils de sécurité
Agentic Threats Navigator	Menaces des systèmes IA autonomes

Initiatives Clés

AI Red Teaming

Tests via attaques simulées sur LLMs

Secure AI Adoption

Centres d'Excellence pour gouvernance IA

AI Threat Intelligence

Collecte de données sur vulnérabilités réelles

Appel à l'Action

Consultez

Ressources sur genai.owasp.org

Rejoignez

OWASP Cotonou pour des ateliers

Contribuez

Traductions, Red Teaming, événements