OpenSSF
OPEN SOURCE SECURITY FOUNDATION

openssf.org
github.com/ossf
openssf.slack.com
linkedin.com/company/openssf

Advancing Trust and Transparency in Artificial Intelligence

The **OpenSSF AI/ML Security Working Group** focuses on securing the machine learning supply chain from data to deployment, building trust, transparency, and integrity throughout the AI lifecycle.

Key Highlights

Model Signing v1.0
The OpenSSF AI/ML Security Working Group released Model Signing v1.0, a new specification that helps developers cryptographically sign and verify machine learning models.

Learn More
openssf.org/projects/model-signing

MLSecOps Whitepaper
The MLSecOps Whitepaper provides practical guidance for securing AI and machine learning pipelines. It helps teams apply security and DevSecOps principles to machine learning systems at every stage.

Read Whitepaper
openssf.org/blog/mlsecops-whitepaper

Supporting Education

Course: Secure AI/ML-Driven Software Development (LFEL1012)
This free Express Learning course from The Linux Foundation teaches how to apply security best practices throughout the AI/ML development lifecycle. It is ideal for developers, decision-makers, and security professionals.

ENROLL

OpenSSF Guidance on AI Code Assistant Instructions
To help developers use these tools safely, OpenSSF created the Security-Focused Guide for AI Code Assistant Instructions, developed by the Best Practices and AI/ML Security Working Groups with contributors from Microsoft, Google, and Red Hat.

Tech Talk: Securing the AI Lifecycle – Trust, Transparency & Tooling in Open Source
Watch OpenSSF experts for a deep dive into open source tools and practices for securing AI systems.

WATCH

AI/ML Security Working Group
Addressing security challenges within AI/ML development, systems, and processes.
openssf.org/groups/ai-ml-security/

Cyber Reasoning Systems SIG - securing critical OSS projects
aicyberchallenge.com

SAFE-MCP SIG - securing LLM-based agents
github.com/SAFE-MCP/safe-mcp