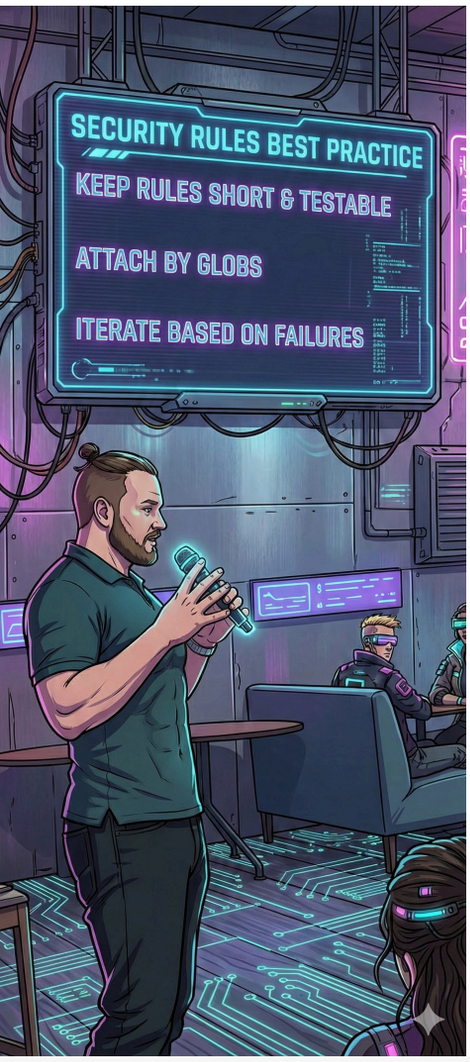
Penchuk CYBER

INNOVATIVE THINKING | TEAM OF TOP CYBER EXPERTS | AI ENHANCED CYBER SERVICES | QUICK, AGILE AND HIGH QUALITY



Penchuk Cyber

Secure Development in the Age of AI

One-Day Intensive Training for Developers Using AI Coding Assistants

AI coding assistants like Cursor, Claude Code, and Copilot are transforming software development, while introducing new attack surfaces, trust boundaries, and security failures.
This hands-on training equips developers to use AI tools securely, critically, and responsibly, without sacrificing productivity.

PENCHUKCYBER.COM | CONTACT@PENCHUKCYBER.COM | +972 55-504-8270

Delivered by Sergei Penchuk

Sergei Penchuk (Founder & CEO) leads Penchuk Cyber, drawing on his experience as former CTO, CISO and a seasoned tech founder.
He is a recognized leader in cybersecurity and artificial intelligence, with decades of commercial and military experience protecting organizations worldwide. Sergei architected AI-driven defense solutions, and understands the unique challenges fast-growing companies face.

Agenda and Syllabus

Morning Session – Frontal Lecture

Security-Driven AI Development

- The New Developer Role: Architect, verifier, and security gatekeeper
- Why AI-Generated Code Is Not Secure by Default (secure vs correct gap)
- OWASP LLM Top 10 & AI-Era Attack Patterns (prompt injection, RAG risks, MCP threats)
- Secure Prompt Engineering & AI Personas for Production Code
- Integrating AI into the Secure SDLC with Human-in-the-Loop Controls

Afternoon Hands-On Lab

Realistic Adversarial Scenario

- Take ownership of a vulnerable, AI-generated code repository
- Detect OWASP Top 10 and LLM Top 10 vulnerabilities using AI IDEs
- Identify hidden malicious instructions and prompt injection vectors
- Build a new AI-powered feature in a polluted repository environment
- Implement secure input validation, output handling, and least-privilege controls
- Deploy safely under real-world constraints

Key Outcomes

Train your developers to use AI — securely

- Confident, secure use of AI coding assistants
- Ability to detect prompt injection and AI-era supply chain risks
- Practical application of OWASP LLM Top 10
- Creation of enforceable security rule packs for AI IDEs
- Integration of AI into existing SSDLC without increasing risk

Trusted by Industry Leaders:

upwind · PAGAYA · CHECK POINT · PENTERA · nuvei · Bank of Israel · ICICI Bank · HDFC BANK · flo. LIVE · Island · שלמה sixt · Israel Electric