// heise devSec()

HEISE DEVSEC KI UND SECURITY
8. APRIL 2025

09:00 - 09:15		Begrüßung
09:15 - 10:00		Produktivitätswunder oder Büchse der Pandora? Software Security in Zeiten von AI Clemens Hübner
10:15 - 11:00		/Security when using AI/ Prompt & Pray - wenn KI Code schreibt und der CRA mitliest Klaus Rodewig — Vorwerk
11:15 - 12:00		/Security when using AI/ Sicherheitsnetze für den sicheren Einsatz von Coding-Agenten Jana Prechelt & Ludwig Richter — andrena objects
12:15 - 13:15		Mittagspause
13:15 - 14:00		/Security for AI/ Breaking the Bot: Live-Hacking von LLMs, Agenten und MCP Florian Teutsch — inovex
14:15 - 15:00		/Security for AI / LLM-Security: Die OWASP-Liste der Angriffsvektoren Johann-Peter Hartmann — Mayflower
15:15 - 15:30		Kaffeepause
15:30 - 16:15		/Security against AI/ Vibe Hacking & Security-Agenten: Angreifer rüsten auf, Verteidiger ziehen nach Frank Ully — Corporate Trust
16:30		Verabschiedung