

// heise devSec()

HEISE DEVSEC KI UND SECURITY
8. APRIL 2025

09:00 - 09:15	Begrüßung		
09:15 - 10:00	 The Good, the Bad and the Ugly – Security im Spannungsfeld von KI und Entwicklung	Clemens Hübner	inovex
10:15 - 11:00	 Sicherheitsnetze für den sicheren Einsatz von Coding-Agenten	Jana Prechelt & Ludwig Richter	andrena objects
11:15 - 12:00	 Vibe Hacking & Security-Agenten: Angreifer rüsten auf – Verteidiger ziehen nach	Frank Ullig	Corporate Trust
12:15 - 13:15	Mittagspause		
13:15 - 14:00	 LLM-Security: Die OWASP-Liste der Angriffsvektoren	Johann-Peter Hartmann	Mayflower
14:15 - 15:00	 MCP Security: Model Context Protocol sicher im Unternehmen einsetzen	Kai Kreuzer	Deutsche Telekom
15:15 - 15:30	Kaffeepause		
15:30 - 16:15	 Hands-on LLM Security – Schwachstellen und Gegenmaßnahmen	Clemens Hübner & Florian Teutsch	inovex
16:30	Verabschiedung		