// heise devSec()

HEISE DEVSEC KI UND SECURITY
11. MAI 2026 ONLINE

MONTAG, 21. SEPTEMBER: WORKSHOPS

ca. 10:00 - 17:00

Secure Build Pipelines hands-on	Security trifft KI: Sichere Softwareentwicklung mit KI-Agenten entlang des SDLC
Felix Schumacher & Christoph Iserlohn INNOQ	**Sebastian Leuer** Fraunhofer IEM

DIENSTAG, 22. SEPTEMBER: KONFERENZ

09:00 - 09:15

Eröffnung

09:15 - 10:00

Keynote [TBA]

N. N.

10:00 – 10:30

Kaffeepause

10:30 - 11:15

Nur auf Sand gebaut? Sandboxing-Technologien im Vergleich	KI-Systeme absichern – Sicherheitsarchitekturen für Agents und LLMs	5 Jahre Application Security in der Praxis – ein Erfahrungsbericht aus der LBBW
Christoph Iserlohn INNOQ	**Sebastian Leuer** Fraunhofer IEM	**Peter Kruse** LBBW

11:30 - 12:15

Ich kam, ich sah nichts, ich lernte: Hands-On Privacy Enhancing Technologies	The Trust Trap - Security von Coding Assistants	TBA [Sponsored Talk]
Amin Faez utilacy GmbH	**Clemens Hübner** Giesecke+Devrient	**N. N.**

12:15 – 13:15

Mittagspause

13:15 - 14:00

Post-Quantum-Kryptografie aus Developer-Sicht	TBA [Sponsored Talk]	Angriffe auf die vergessenen Schutzziele
N. N.	**N. N.**	**Flora Schäfer** secuvera

14:15 - 15:00

Kryptografische Inventarisierung in der Praxis: Transparenz und Governance schaffen	Sichere MCP-Server entwickeln: OAuth, Token Exchange und Hardening in der Praxis	Wie „hackt“ man eine API? Vom Angriff zur effektiven Verteidigung
Christian Näther & Jan-Philipp Steghöfer XITASO GmbH	**Robert Fritze & Mirko Richter** mgm security partners GmbH	**Thomas Bayer** predic8

15:00 – 15:30

Kaffeepause

15:30 - 16:15

Technische Herausforderungen der PQC Migration	Wer haftet, wenn der Vibe kippt? – Zur rechtlichen Verantwortung beim Vibe Coding	TBA [Sponsored Talk]
Falko Strenzke MTG AG	**Niklas Mühleis** Heidrich Rechtsanwälte	**N. N.**

16:30 - 17:15

Security Compliance Quiz – Teste dein Wissen zu Regulatorik und Standards

Julia Wasserer & Sebastian Leuer
Bundesverwaltungsamt, Fraunhofer IEM

17:30 - 18:30

Thementische

18:30 - 21:30

Get-together

MITTWOCH, 23. SEPTEMBER: KONFERENZ

09:00 - 9:45

LLM-gestützte Code Reviews und Schwachstellensuche: Wirksamkeit und Grenzen	Von XZ bis Trivy: Was Supply-Chain-Angriffe über unsere Pipelines verraten	Cyber Resilience Act & Legacy Code - Warum technische Schulden zum Haftungsrisiko werden
Johannes Bär condignum GmbH	**Michael Fuchs** inovex GmbH	**Mehmet Kus** OTARIS Interactive Services GmbH

10:00 - 10:45

Vier grüne Häkchen, trotzdem gehackt: Threat Modeling für agentenbasierte KI

Christian Schneider
Freiberufler

TBA [Sponsored Talk]

N. N.

CRA und IEC 62443-4-1 in der Praxis: Mehr als Threat Modeling und Penetration Testing

Sven Rieger
M&M Software

10:45 – 11:15

Kaffeepause

11:15 - 12:00

MCP und RAG absichern: Wenn KI-Agenten auf Firmendaten zugreifen

Frank Ully
Corporate Trust GmbH

Super sichere Software oder ultra unsicheres Slopaggedon? KI und die Software-Supply-Chain

Christoph Iserlohn
INNOQ

TBA [Sponsored Talk]

N. N.

12:00 – 13:00

Mittagspause

13:00 - 13:45

Keynote [TBA]

N. N.

14:00 - 14:45

Smart & Safe: Wie KI-Agenten den Thermomix CRA-ready machen

Klaus Rodewig & Mascha Lampert
Vorwerk Elektrowerke GmbH & Co. KG

Broken Access Control: Das unterschätzte Risiko, das nie verschwindet

Martina Kraus
Kraus IT Consulting

Cloud Native und Secure By Design mit Open Source - Wie kann das zusammengehen?

Thomas Fricke
Freelancer

14:45 – 15:15

Kaffeepause

15:15 - 16:00

Sicherheitsrisiken in Multi-Tenant-Architekturen finden und beheben

Lorin Lehawany & Sven Nobis
ERNW Enno Rey Netzwerke GmbH

Bit-for-Bit: Unser Weg zur sicheren Container-Lieferkette

Tim Bastin
L3montree GmbH

C++26 Hardening: Die “Stop the Bleed”-Strategie für sicheren Legacy-Code

Philipp Dominik Schubert
SonarSource Sàrl

16:15 - 17:00

Test-Driven Security

Zero Trust Agents: Sichere KI-Workloads mit OPA und Kubernetes

Sebastian Bergmann
thePHP.cc

Mario-Leander Reimer
QAware GmbH

Verabschiedung