

MONTAG, 21. SEPTEMBER: WORKSHOPS

ca. 10:00 - 17:00

Secure Build Pipelines hands-on

Felix Schumacher & Christoph Iserlohn
INNOQ

Security trifft KI: Sichere Softwareentwicklung mit KI-Agenten entlang des SDLC

Sebastian Leuer
Fraunhofer IEM

DIENSTAG, 22. SEPTEMBER: KONFERENZ

09:00 - 09:15

Eröffnung

09:15 - 10:00

Keynote

N. N.

10:00 - 10:30

Kaffeepause

10:30 - 11:15

Nur auf Sand gebaut? Sandboxing-Technologien im Vergleich

Christoph Iserlohn
INNOQ

KI-Systeme absichern – Sicherheitsarchitekturen für Agents und LLMs

Sebastian Leuer
Fraunhofer IEM

5 Jahre Application Security in der Praxis – ein Erfahrungsbericht aus der LBBW

Peter Kruse
LBBW

11:30 - 12:15

Ich kam, ich sah nichts, ich lernte: Hands-On Privacy Enhancing Technologies

Amin Faez
utilacy

The Trust Trap – Security von Coding Assistants

Clemens Hübner
Giesecke+Devrient

TBA

N. N.
INOSOFT [Sponsored Talk]

12:15 - 13:15

Mittagspause

13:15 - 14:00

Post-Quantum-Kryptografie aus Developer-Sicht	TBA	Broken Access Control: Das unterschätzte Risiko, das nie verschwindet
N. N.	N. N. Signpath [Sponsored Talk]	Martina Kraus Kraus IT Consulting

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
Jan-Philipp Steghöfer XITASO	Robert Fritze & Mirko Richter mgm security partners	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
Falko Strenzke MTG	Niklas Mühleis Heidrich Rechtsanwälte	N. N. Cycode [Sponsored Talk]

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	Michael Fuchs inovex	Mehmet Kus OTARIS Interactive Services

10:00 - 10:45

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

Christian Schneider
Freiberufler

TBA

N. N.
[Sponsored
Talk]

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 Ullly
Corporate Trust

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

Christoph Iserlohn
INNOQ

TBA

N. N.
[Sponsored
Talk]

12:00 - 13:00

Mittagspause

13:00 - 13:45

Keynote

N. N.

14:00 - 14:45

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

Klaus Rodewig
Vorwerk
Elektrowerke

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

Thomas Fricke
Freelancer

Cookies 2.0: Fluch oder Segen?

Christian Wenz

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

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

Tim Bastin
L3montree

Angriffe auf die vergessenen Schutzziele

Flora Schäfer
secuvera

16:15 - 17:00

Sicher, resilient, handlungsfähig: Moderne
CI/CD-Pipelines

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

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

Sebastian Bergmann

thePHP.cc

Mario-Leander Reimer

QAware

Philipp Dominik Schubert

SonarSource

Verabschiedung