// 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

Felix Schumacher & Christoph Iserlohn
INNOQ
Villa Kennwood

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

Sebastian Leuer
Fraunhofer IEM
Villa Sonoma

DIENSTAG, 22. SEPTEMBER: KONFERENZ

09:00 - 09:15

Eröffnung

09:15 - 10:00

Predictability Is Vulnerability: What four years of cyber war teach about software security

Volodymyr Styran
SSSCIP
Track 1

10:00 – 10:30

Kaffeepause

10:30 - 11:15

KI-Systeme absichern – Sicherheitsarchitekturen für Agents und LLMs

Sebastian Leuer
Fraunhofer IEM
Track 1

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

Peter Kruse
LBBW
Track 2

Nur auf Sand gebaut? Sandboxing-Technologien im Vergleich

Christoph Iserlohn
INNOQ
Track 3

11:30 - 12:15

The Trust Trap – Security von Coding Assistants

Clemens Hübner
Giesecke+Devrient
Track 1

Die Warnlampe leuchtet: Live-Angriff auf einen KI-gesteuerten Leitstand

Patrick Kempf & Timo Becker
INOSOFT [Sponsored Talk]
Track 2

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

Amin Faez
utilacy
Track 3

12:15 – 13:15

Mittagspause

13:15 - 14:00

Broken Access Control: Das unterschätzte Risiko, das nie verschwindet

Martina Kraus
Kraus IT Consulting
Track 1

Integrität und Authentizität von SBOMs: Anforderungen, Standards und ein Reality-Check

Stefan Wenig
SignPath [Sponsored Talk]
Track 2

Post-Quanten-Kryptografie: BSI-Vorgaben und der Weg in die Praxis

Stephan Ehlen & René Meusel
BSI, Rohde & Schwarz Networks and Cybersecurity
Track 3

14:15 - 15:00

Wie „hackt“ man eine API? Vom Angriff zur effektiven Verteidigung

Thomas Bayer
predic8
Track 1

Sichere MCP-Server entwickeln: OAuth, Token Exchange und Hardening in der Praxis

Robert Fritze
mgm security partners
Track 2

Kryptografische Inventarisierung in der Praxis: Transparenz und Governance schaffen

Jan-Philipp Steghöfer
XITASO
Track 3

15:00 – 15:30

Kaffeepause

15:30 - 16:15

Wer haftet, wenn der Vibe kippt? – Zur rechtlichen Verantwortung beim Vibe Coding

Niklas Mühleis
Heidrich Rechtsanwälte
Track 1

Passkeys in der Praxis: Sichere Implementierung mit Keycloak

Martina Kraus
Kraus IT Consulting
Track 2

Technische Herausforderungen der PQC Migration

Falko Strenzke
MTG
Track 3

16:30 - 17:15

Security Compliance Quiz – Teste dein Wissen zu Regulatorik und Standards

Julia Wasserer & Sebastian Leuer
Bundesverwaltungsamt, Fraunhofer IEM
Track 1

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

Johannes Bär
condignum
Track 1

Von XZ bis Trivy: Was Supply-Chain-Angriffe über unsere Pipelines verraten

Michael Fuchs
inovex
Track 2

Cyber Resilience Act & Legacy Code – Warum technische Schulden zum Haftungsrisiko werden

Mehmet Kus
OTARIS Interactive Services
Track 3

10:00 - 10:45

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

Christian Schneider
Freiberufler
Track 1

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

Sven Rieger
M&M Software
Track 2

Sicherheitsrisiken in Multi-Tenant-Architekturen finden und beheben

Lorin Lehawany & Sven Nobis
ERNW Enno Rey Netzwerke
Track 3

10:45 – 11:15

Kaffeepause

11:15 - 12:00

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

Christoph Iserlohn
INNOQ
Track 1

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

Philipp Dominik Schubert
SonarSource
Track 2

Wenn Rule Files und Skills Entwickler und Agenten manipulieren

Steffen Hellwig
Cycode [Sponsored Talk]
Track 3

12:00 – 13:00

Mittagspause

13:00 - 13:45

Panel: Sichere Softwareentwicklung in Zeiten von Agentic AI

Christoph Iserlohn & Clemens Hübner & Sebastian Leuer
INNOQ, Giesecke+Devrient, fraunhofer IEM
Track 1

14:00 - 14:45

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

Sebastian Bergmann
thePHP.cc
Track 1

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

Thomas Fricke & Tobias Weiss
Freelancer
Track 2

Cookies 2.0: Fluch oder Segen?

Christian Wenz
Track 3

14:45 – 15:15

Kaffeepause

15:15 - 16:00

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

Mario-Leander Reimer
QAware

Track 1

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

Tim Bastin
L3montree

Track 2

Verabschiedung