REQUIREMENTS, AGILITÄT, SECURITY & AI

Wie Requirements-Management und agile Methoden Security in der Software-Entwicklung stärken – und wie AI dabei als Enabler wirkt.

JOACHIM METTENLEITER

REQUIREMENTS, AGILITÄT, SECURITY & AI

Imagine…

Dampf

Grenzen der Kraft von Menschen (oder Tieren) hinter sich lassen

Strom

Fast überall, jederzeit und für jeden Zweck verfügbar

Internet

Vernetzt & virtuell, ultra-schnelle Evolution

Das alles zusammen - nur schneller und größer

generated with FLUX.2 max

SECURITY ALS ANFORDERUNG

Warum Requirements-Management entscheidend ist

"SECURITY IS NOT A PRODUCT – BUT A PROCESS.“

Bruce Schneier

…und vergessene Security-Anforderungen fallen meist nicht zuerst dem Kunden auf

"SECURITY IST KEIN FEATURE –
ES IST EINE EIGENSCHAFT."

Security-Anforderungen sind oft implizit – und werden deshalb vergessen

Frei nach Bruce Schneier

REGULATORIK ALS TREIBER – EU CYBER RESILIENCE ACT

CRA verlangt:

- Security by Design
- Vulnerability Disclosure Policy
- SBOM (Software Bill of Materials)
- Lifecycle-Management
- Nachweisbarkeit der Konformität

Was das bedeutet:

- Anforderungen müssen dokumentiert und rückverfolgbar sein
- SBOM erfordert sauberes Konfigurationsmanagement
- Agile Prozesse müssen Security-Gates integrieren
- AI kann bei Analyse und Compliance-Check helfen

AGILE METHODEN & SECURITY

Kein Widerspruch – sondern eine Chance

„Agile is not chaotic.
Chaotic is not agile.“

LinkedIn -Spruch

„Man darf nie an die ganze Straße auf einmal denken, verstehst Du? Man muss nur

an den nächsten Schritt denken,

den nächsten Atemzug, den nächsten Besenstrich.

Und immer wieder nur den nächsten.“

„Dann macht es Freude; das ist wichtig,

dann macht man seine Sache gut.

Und so soll es sein.“

Beppo Strassenkehrer (Michael Ende)

KLASSISCH VS. AGIL – SECURITY IM ENTWICKLUNGSPROZESS

KLASSISCH

- Security einmalig zu Beginn erfasst
- Kaum Reaktion auf neue Bedrohungslagen
- Security-Review am Ende – zu spät
- Lange Zyklen = grosses Zeitfenster für Schwachstellen
- Rückwirkende Korrekturen sind teuer

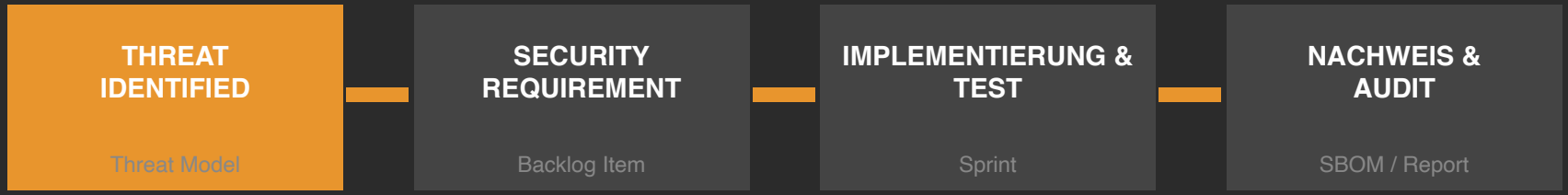
AGIL

- Security als Epic im Product Backlog
- Security User Stories im Sprint Planning
- Threat Modeling iterativ verfeinert
- Security Reviews Teil jedes Sprint Reviews
- Schnelle Reaktion auf CVEs und neue Bedrohungen

"SECURITY FIRST IST KEIN GEGENSATZ ZU AGILITY FIRST. ES IST DIE VORAUSSETZUNG."

Praxiserfahrung

TRACEABILITY – HERZSTÜCK DES SECURITY REQUIREMENTS MANAGEMENT



Vollständige Rückverfolgbarkeit: Von der Bedrohung über die Anforderung bis zum Test und Nachweis.

Security-Gates in der CI/CD-Pipeline: SAST, DAST, Dependency Scanning, Container Scanning.

SBOM als Compliance-Artefakt: Automatisch generiert – Basis für CRA-Konformität.

AI ALS ENABLER

Konkrete Anwendungsfelder in der sicheren Softwareentwicklung

"YOU CAN´T ALWAYS GET WHAT YOU WANT.“

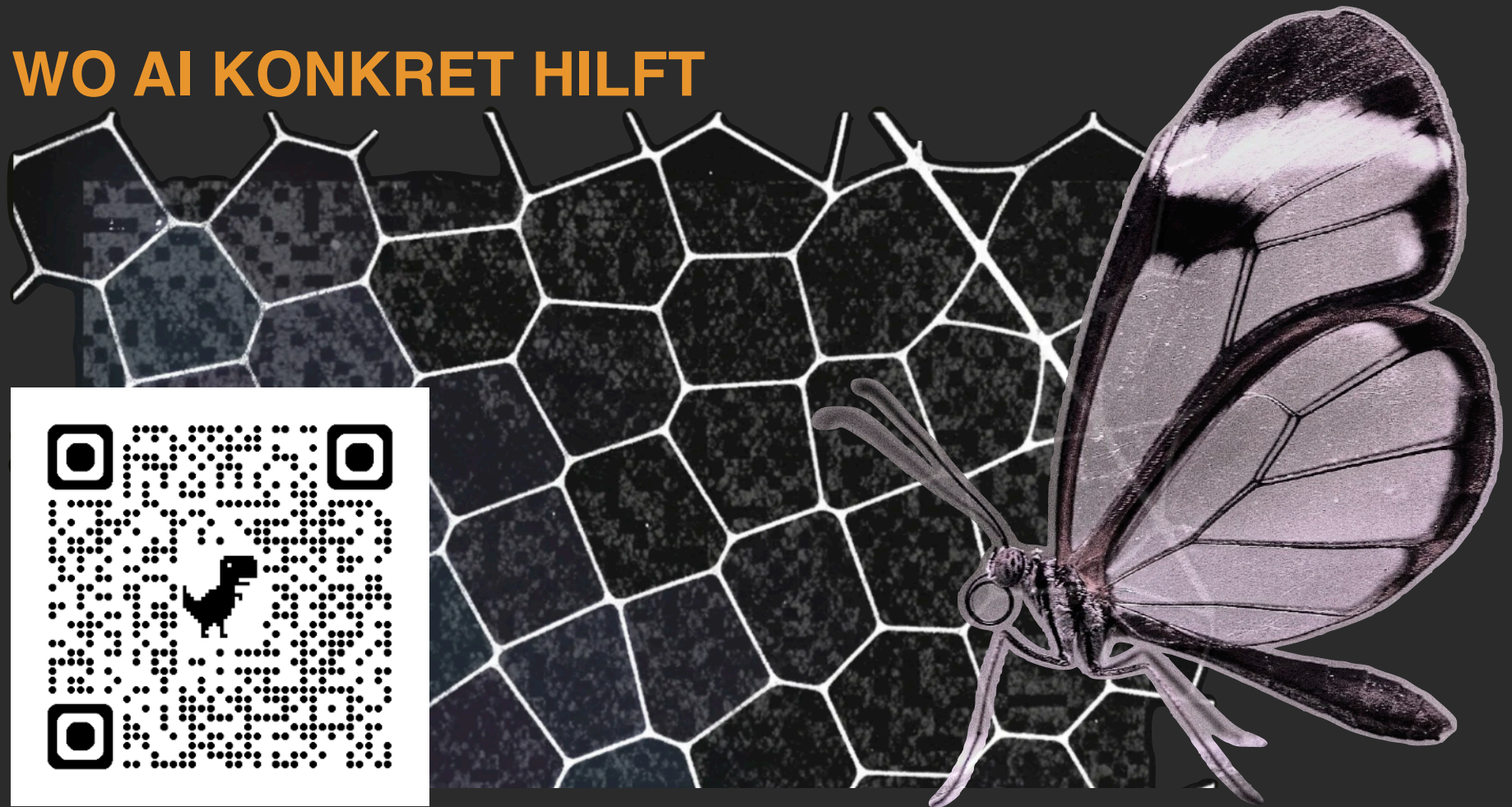
"WHAT YOU GET IS WHAT YOU ASK FOR.“

Praxiserfahrung

IMAGINE...

DER GUTE KUMPEL, DER IMMER ZEIT HAT

WO AI KONKRET HILFT



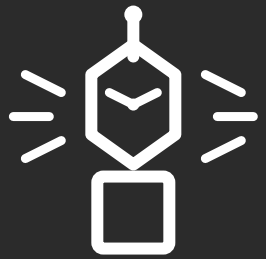
WO AI KONKRET HILFT

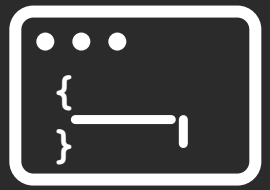
- REQUIREMENTS
- BACKLOG
- CODING
- TESTING
- COMPLIANCE

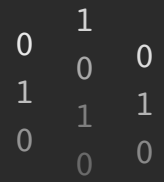
WO AI KONKRET HILFT

REQUIREMENTS	AI analysiert Stakeholder-Aussagen, schlägt Security-Anforderungen vor – inklusive Bedrohungsszenarien
BACKLOG	Automatisches Erstellen von Security User Stories aus Threat Models; Priorisierungsvorschläge nach Risikogewichtung
CODING	Coding-Assistenten erkennen unsichere Code-Patterns in Echtzeit und schlagen sichere Alternativen vor
TESTING	AI-generierte Testfälle für Security; Fuzzing-Unterstützung; Anomalie-Erkennung in Testergebnissen
COMPLIANCE	Automatische Analyse auf CRA-/ISO-Konformität; SBOM-Erstellung und CVE-Monitoring mit AI

Der Elefant im Raum…







generated with Deepseek

Entwickler

AI Agent

Programmiersprache

Binärdaten

WRAP UP

DER GESAMTRAHMEN – ALLES GREIFT INEINANDER

REQUIREMENTS MANAGEMENT

- Security-Anforderungen explizit erfassen
- Traceability sicherstellen
- Acceptance Criteria für Security
- Compliance-Nachweise ermöglichen

AGILE METHODEN

- Security in jeden Sprint integrieren
- Threat Modeling iterativ
- Definition of Done mit Security-Gates
- Schnelle Reaktion auf Bedrohungen

AI ALS ENABLER

- Requirements-Analyse & -generierung
- Vulnerability Detection im Code
- SBOM-Analyse & CVE-Monitoring
- Compliance-Prüfung automatisiert

REQUIREMENTS, AGILITÄT & SECURITY

Wie Requirements-Management und agile Methoden Security in der Software-Entwicklung stärken – und wie AI dabei als Enabler wirkt.

Vielen Dank!

Fragen? :-)