VON KI-CHAOS ZU KI-KONTROLLE: KI IM IT-GRUNDSCHUTZ ABBILDEN

ISO 9001
ISO 27001

neam
part of connexta

IHRE REFERENTIN

Julia Dreier

Security Consultant

Informationssicherheitsbeauftragte(r) mit TÜV Rheinland geprüfter Qualifikation

IT-Grundschutz-Praktiker

BCM-Praktiker

Julia.Dreier@neam.de

VON KI-CHAOS ZU KI-KONTROLLE: KI IM IT-GRUNDSCHUTZ ABBILDEN

ISO 9001
ISO 27001

neam
part of connexta

DIE AUSGANGSLAGE:
WENN INNOVATION AUF BÜROKRATIE TRIFFT

Geschwindigkeit

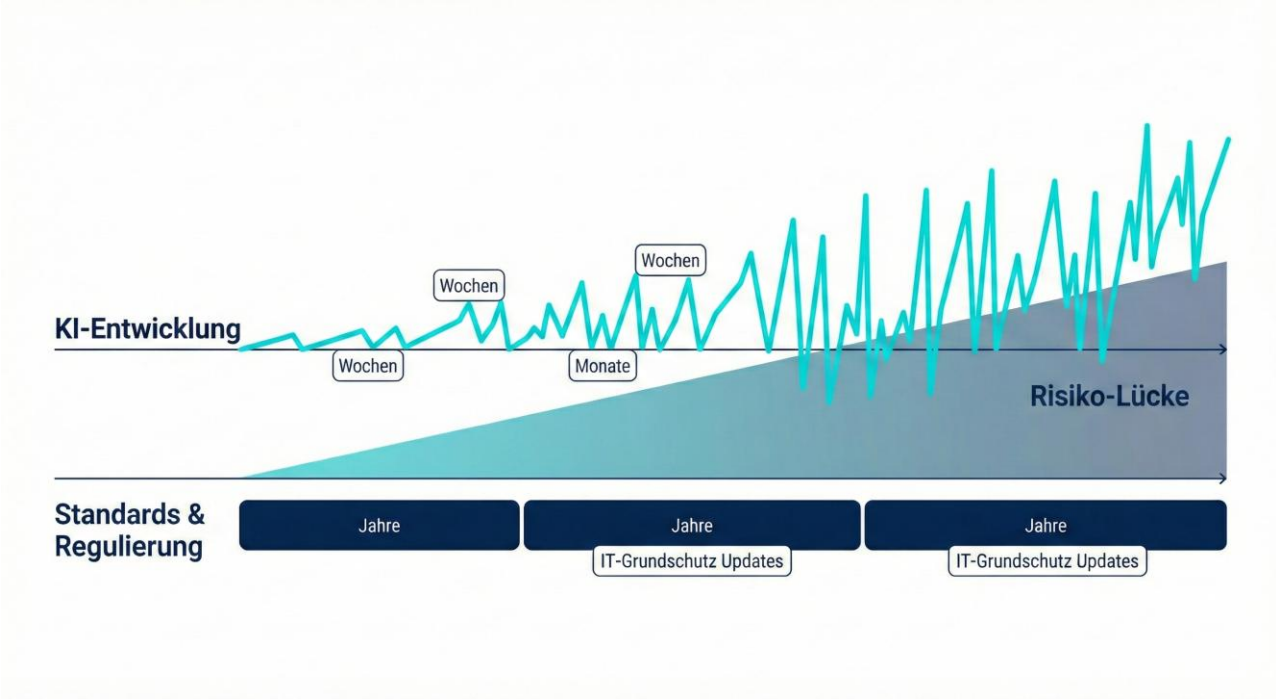
KI-Entwicklungszyklen sind extrem kurz.

Der Druck

Verschieden Regulatorien müssen eingehalten werden

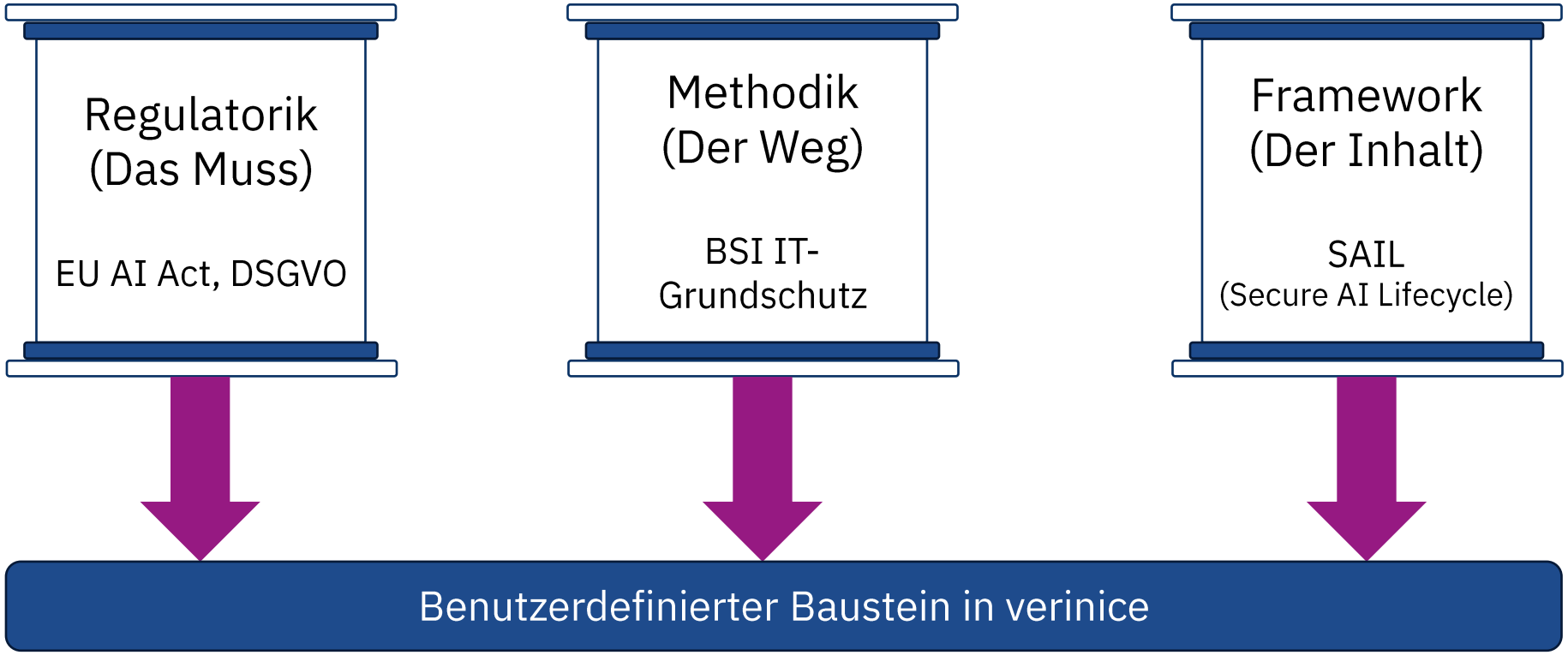
Die Lücke

Aktuell kein „KI-Baustein“ im Kompendium



Wir können nicht warten. Wir müssen die Brücken jetzt bauen.

DIE STRATEGIE:
DIE BRÜCKE – SAIL, BSI UND DER AI ACT



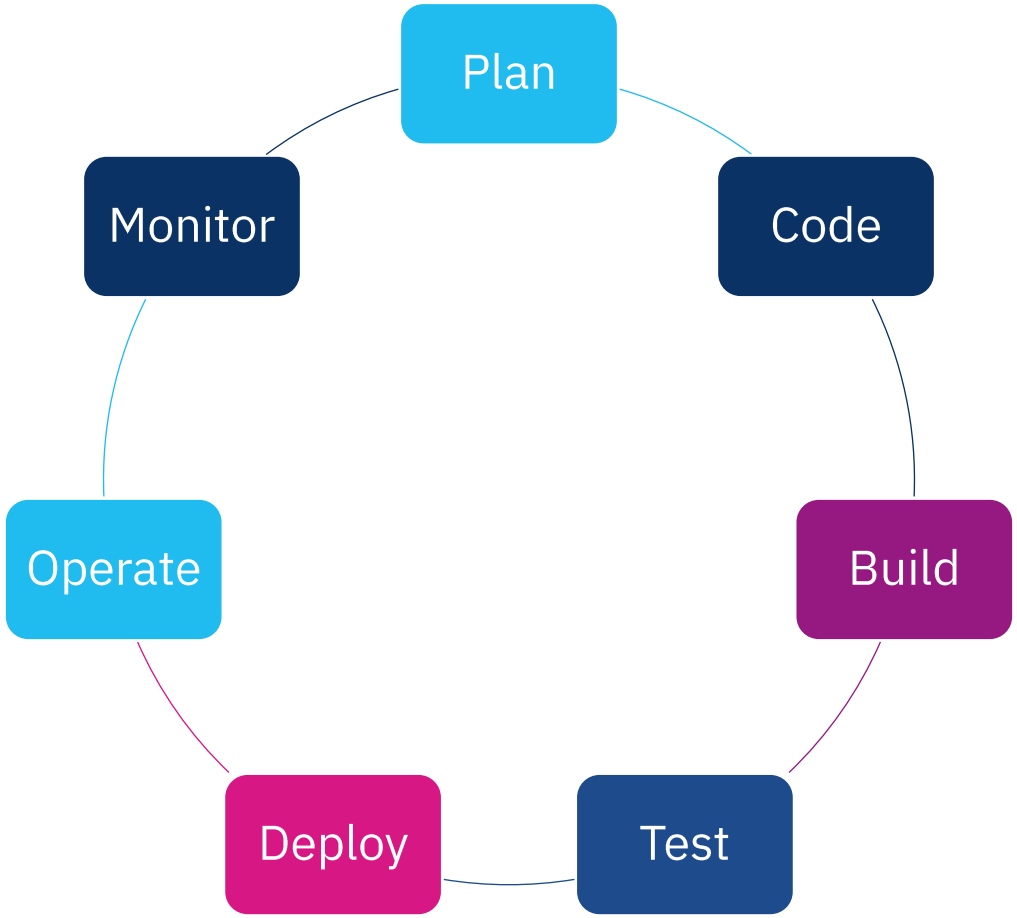
SAIL liefert die spezifischen Gefährdungen und Maßnahmen, die im aktuellen BSI-Prozess fehlen.

EU AI ACT

- Weltweit erstes umfassendes KI-Gesetz
- Risikobasierter Ansatz
- Strenge Anforderungen für „Hochrisiko-KI“

- Horrende Bußgelder bei Nicht-Compliance
- Basis für eine sichere KI-Kultur in Institutionen
- Schulungspflicht

SAIL FRAMEWORK



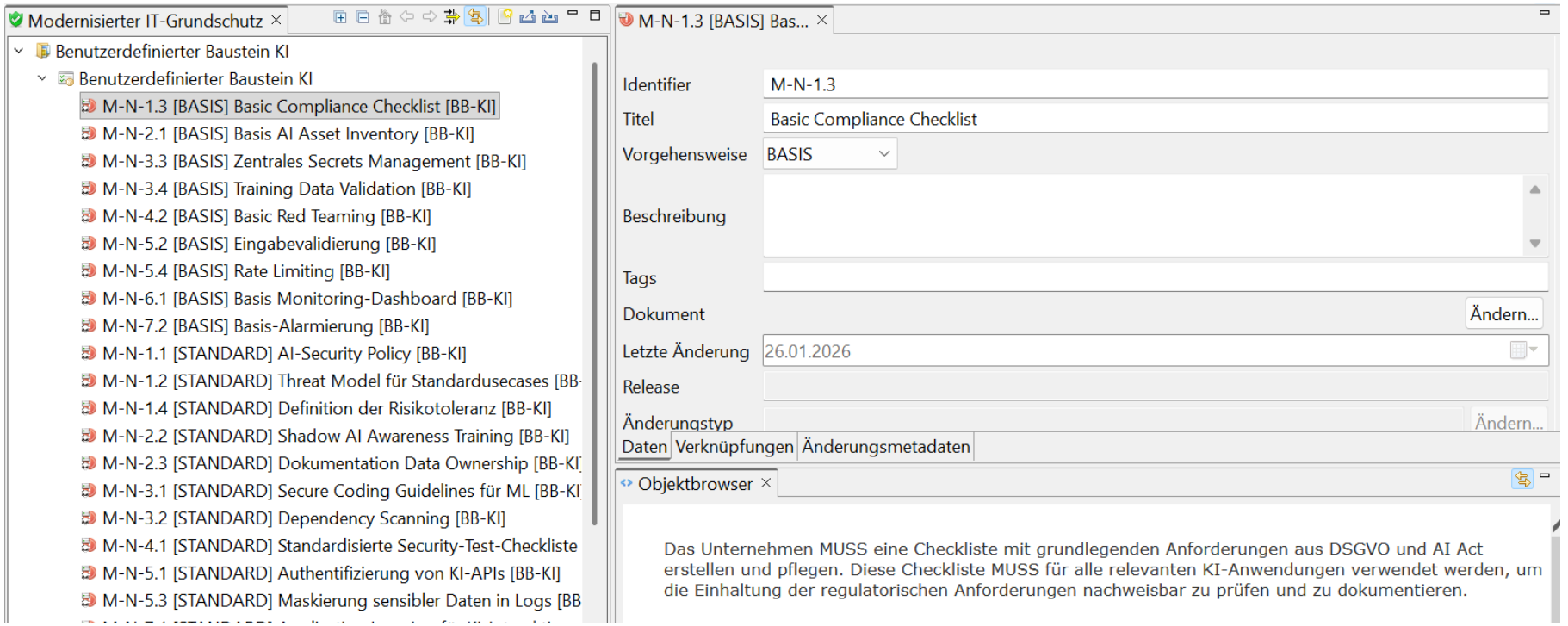
- Brücke zwischen AI-Development, MLOps und Informationssicherheit
- Begleitet den gesamten Lebenszyklus
- Ergänzt bestehende Standards wie NIST, ISO 42001
- Fokus auf pragmatische Umsetzung in Institutionen

SAIL FRAMEWORK

- Phase 1: Kickoff & Governance (Strategie & Verantwortlichkeiten)
- Phase 2: Use Case Identifikation (Bewertung & Auswahl)
- Phase 3: Data Assessment (Datenquellen & Qualität)
- Phase 4: Risikoanalyse & Leitlinie (Gefährdungen & Regeln)
- Phase 5: Technologieauswahl (Plattform & Architektur)
- Phase 6: Pilotprojekt & Testphase (Validierung & Red Teaming)
- Phase 7: Implementierung, Monitoring & Optimierung (Dauerbetrieb)

DER BENUTZERDEFINIERTE BAUSTEIN

- Gefährdungskatalog (basierend auf SAIL Risiken).
- Maßnahmenkatalog (basierend auf Best Practices & AI Act).
- Schutzbedarfsfeststellung (angepasst an KI-Szenarien).



SCHUTZBEDARFSFESTSTELLUNG

SCHADENSSZENARIEN

Verstoß gegen Gesetze/Vorschriften/Verträge

Beeinträchtigung des informationellen Selbstbestimmungsrechts

Beeinträchtigung der persönlichen Unversehrtheit

Beeinträchtigung der Aufgabenerfüllung

Negative Innen-/Außenwirkung

Finanzielle Auswirkungen

SCHUTZBEDARFSFESTSTELLUNG

SCHADENSSZENARIEN

Bias und Diskriminierung

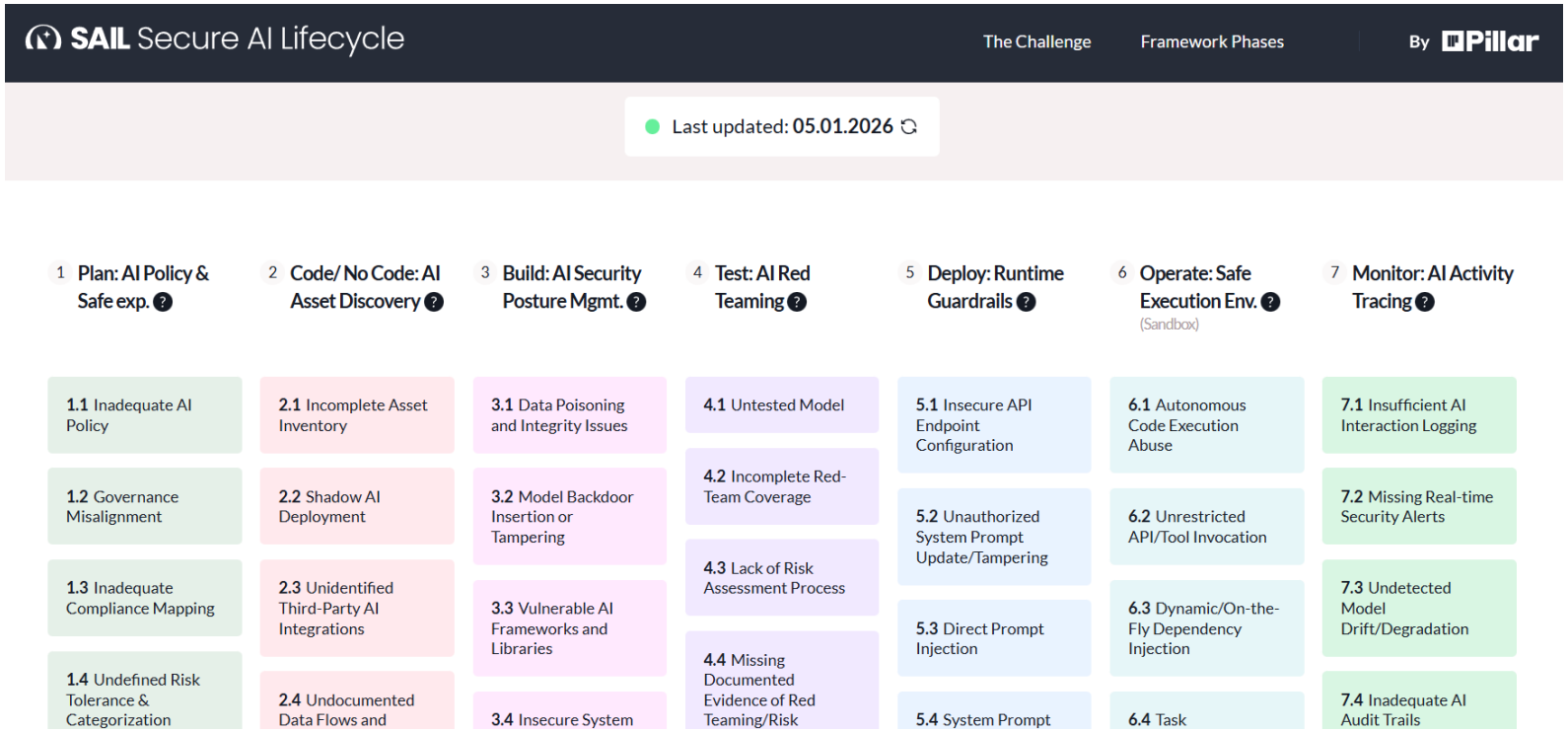
Prompt Injection/ Adversarial Attacks

Model Poisoning/ Data Poisoning

Model Extraction/ IP-Verlust

RISIKOANALYSE

- Gefährdungskatalog = SAIL Framework
- 73 Risiken aufgeteilt in 7 Phasen



DER BENUTZERDEFINIERTE BAUSTEIN
BEISPIEL

Problem: Der AI Act fordert Transparenz (Art. 13) und fehlerfreie Trainingsdaten (Art. 10).

Die Lösung im Baustein:

- Maßnahme "M-N-3.4 Training Data Validation" (erfüllt Datenqualität).
- Maßnahme "M-H-3.6 Model Versioning & Audit Trail" (erfüllt Dokumentationspflichten).

FAZIT

- KI-Sicherheit ist komplex, der AI Act macht sie verbindlich.
- Unser Baustein übersetzt den Gesetzestext (AI Act) und technische Frameworks (SAIL) in BSI-Maßnahmen.
- Mit verinice wird Compliance nachweisbar – audit-sicher und integriert.

FRAGEN

neam
part of connexta

VIELEN DANK
FÜR IHRE AUFMERKSAMKEIT!