

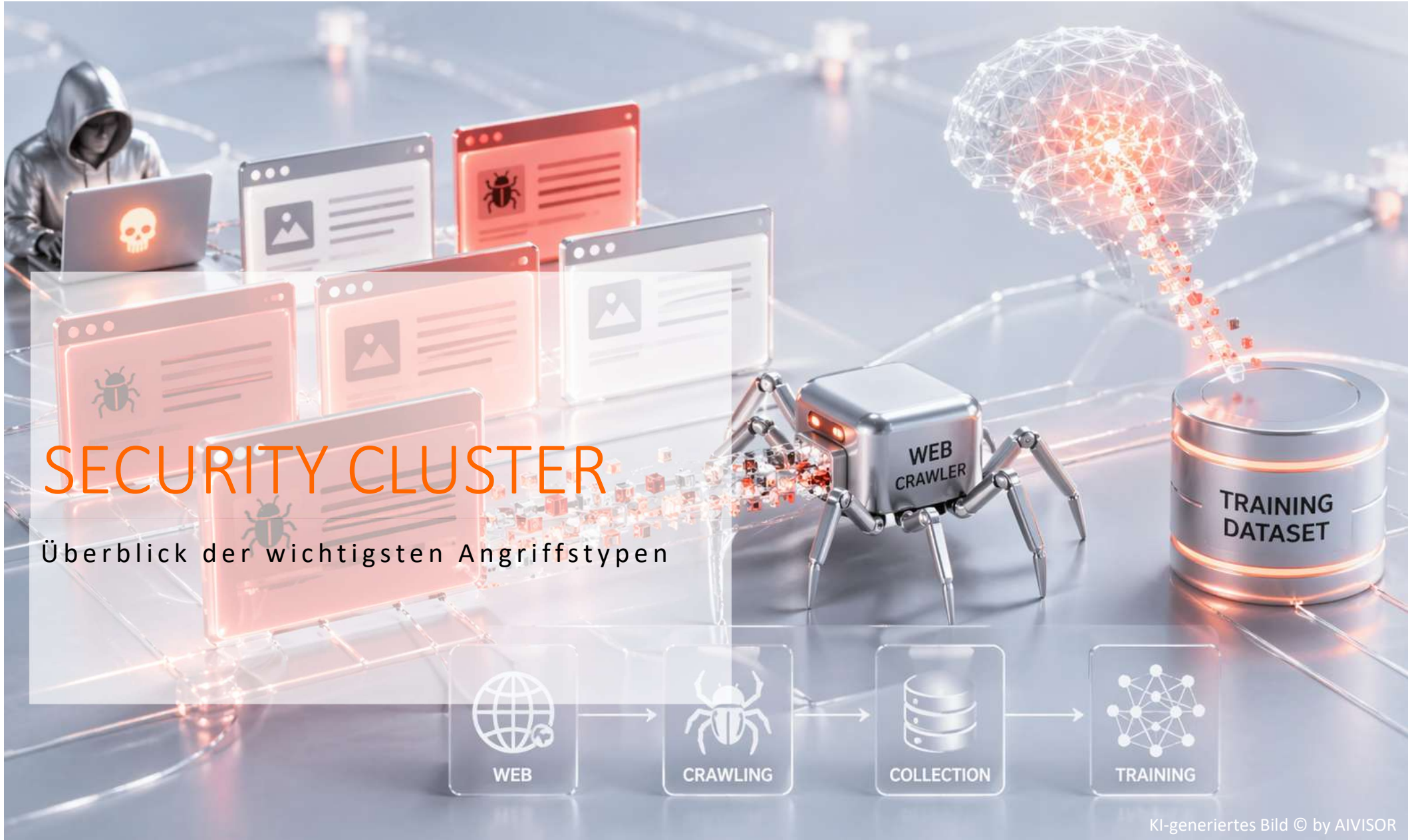


KI-Security für den Mittelstand

RISIKEN ERKENNEN,
KI-SOUVERÄNITÄT SICHERN

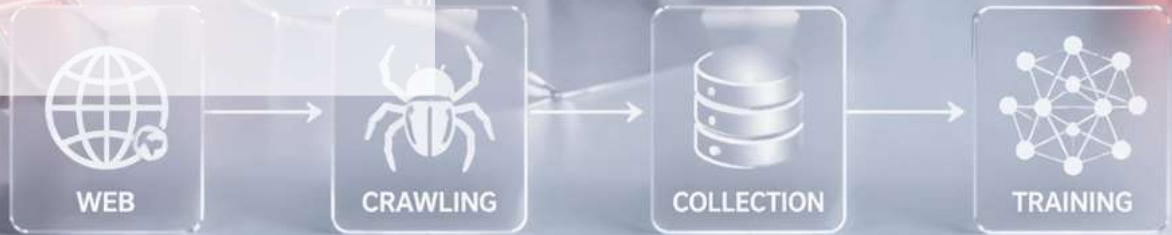
Mai 26

**Folgeevent zur
6. ERFA-Runde
nur für AGAD-
Mitglieder**



SECURITY CLUSTER

Überblick der wichtigsten Angriffstypen



KI-SECURITY REPORT FÜR DEN MITTELSTAND



AI FOCUSED STRATEGY

KI-Use-Case Sicherheitsanalyse

Identifizieren Sie in wenigen Minuten die relevanten Sicherheitsaspekte Ihres KI-Vorhabens – basierend auf den OWASP LLM Top 10 2025.

| | |
|---|--|
|  Unternehmenskontext Diese Angaben helfen, die Analyse auf Ihre Situation zuzuschneiden |  Use-Case Beschreibung Beschreiben Sie Ihr KI-Vorhaben so konkret wie möglich |
|  Technologie & Daten Entscheidend für die Identifikation relevanter Sicherheitsrisiken |  Rahmenbedingungen Technische und organisatorische Rahmenbedingungen |

⚠ Alle Angaben und Analysen erfolgen ohne Gewähr und ersetzen keine professionelle Security-Beratung.

Analyse starten →

Tool-Vorstellung
nur für AGAD-
Mitglieder

FÜR IHRE KI-TASK-
FORCE ENTWICKELT

KMU SECURITY REPORT





KI-SOUVERÄNITÄT

VOM **RISIKO** ZUR **KONTROLLE**

KI-INFRASTRUKTUR IM ÜBERBLICK

Wer kontrolliert Ihre KI

ABHÄNGIGKEIT
DATENRISIKEN
INTRANSPARENZ
KONTROLLVERLUST
SICHERHEITSLÜCKEN

KI-TOOL FÜR IHRE TASK-FORCE



FÜR IHRE KI-TASK-FORCE ENTWICKELT

KI-INFRASTRUKTUR STRATEGIE



KI-INFRASTRUKTUR STRATEGIE

Kontrolle ist zurückholbar.

KI-Security ist kein isoliertes IT-Thema – es ist eine strategische Frage der Kontrolle. Prompt Injection, Datenabfluss, vergiftete Quellen, unkontrollierte Agenten – sie haben eine Gemeinsamkeit:

Sie entstehen nicht trotz der Architektur. Sie entstehen wegen ihr.

Wer seine Daten in fremde Clouds gibt, gibt Kontrolle ab. Wer Agenten ohne Least Privilege betreibt, gibt Kontrolle ab. Wer keine Sichtbarkeit über Shadow AI hat, gibt Kontrolle ab.

Sicherheit entsteht nicht erst durch Schutzmaßnahmen. Sie entsteht durch die Architektur und die strategischen Entscheidungen, die Sie heute treffen.

Was sind Ihre Entscheidungsmöglichkeiten?

Analyse starten →

ca. 15 Minuten · alle Antworten nachjustierbar · anbieter-neutral



GET IN CONTACT

KI-TASK-FORCE



Inkl. Security-
Report &
Infrastruktur-
Strategie in Kürze

KI-KOMPETENZSCHULUNG



KI-SPRECHSTUNDE



KI-Insiderportal explizit für Ihre KI-Task-Force

- Handouts
- Spezielle KI-Agents
- Management Reportingvorlagen
 - Fachartikel
 - 1:1-Calls

Pflichtschulung seit 02.02.2025 gemäß EU AI ACT Art. 4

- Selbstlernereinheit für Ihre Mitarbeiter
 - Online
- Rabatt für AGAD-Mitglieder
Ansprechpartner: Fr. Weiser

INTERESSE?

SPRECHEN SIE UNS FÜR EINE LIVE-DEMO AN

1:1 Gespräch
zu Ihren individuellen KI-Themen
Jeden Freitag
4 Slots à 40 Min.
kostenfrei



KONTAKT

Danke für die Aufmerksamkeit!



Thomas Chmielnik



02303 – 95974-202

0176-632 656 21



tch@aivisor.de

www.aivisor.de



