AVANTEC
Competence. Security. Trust.



AI Security in der Praxis.

Drei Lösungen, drei Use Cases.



Einführung

Georg Hegyi, Head of Presales, AVANTEC

AI ist längst im Unternehmen.

Ist Ihre Security bereit?

AI verändert nicht nur die Arbeitsweise. Sie verändert auch die Angriffsfläche.

- Mitarbeitende nutzen öffentliche und geschäftliche AI-Anwendungen.
- Unternehmen integrieren AI in bestehende Geschäftsprozesse.
- AI-Agenten erhalten zunehmend Zugriff auf Daten, Systeme und Anwendungen.

Die zentrale Herausforderung:

Wie ermöglichen wir die produktive Nutzung von AI, ohne die Kontrolle über Daten, Zugriffe und Prozesse zu verlieren?

AI schafft neue Angriffsflächen

Ist Ihre Security bereit?

AVANTEC
Competence. Security. Trust.

Bereich	Sicherheitsrisiko
AI-Nutzung	Shadow AI und unkontrollierte Anwendungen
Prompts	Offenlegung vertraulicher Informationen
Modelle & Daten	Prompt Injection und manipulierte Inhalte
AI-Agenten	Übermässige Berechtigungen und unerwünschte Aktionen

Klassische Security reicht allein nicht mehr aus

AVANTEC
Competence. Security. Trust.

Bestehende Security-Disziplinen bleiben wichtig.
AI erfordert zusätzliche Kontrollmechanismen.

Klassische Security

- Network Security
- URL Filtering
- Data Loss Prevention
- Identity & Access Management
- Application Security
- Security Monitoring

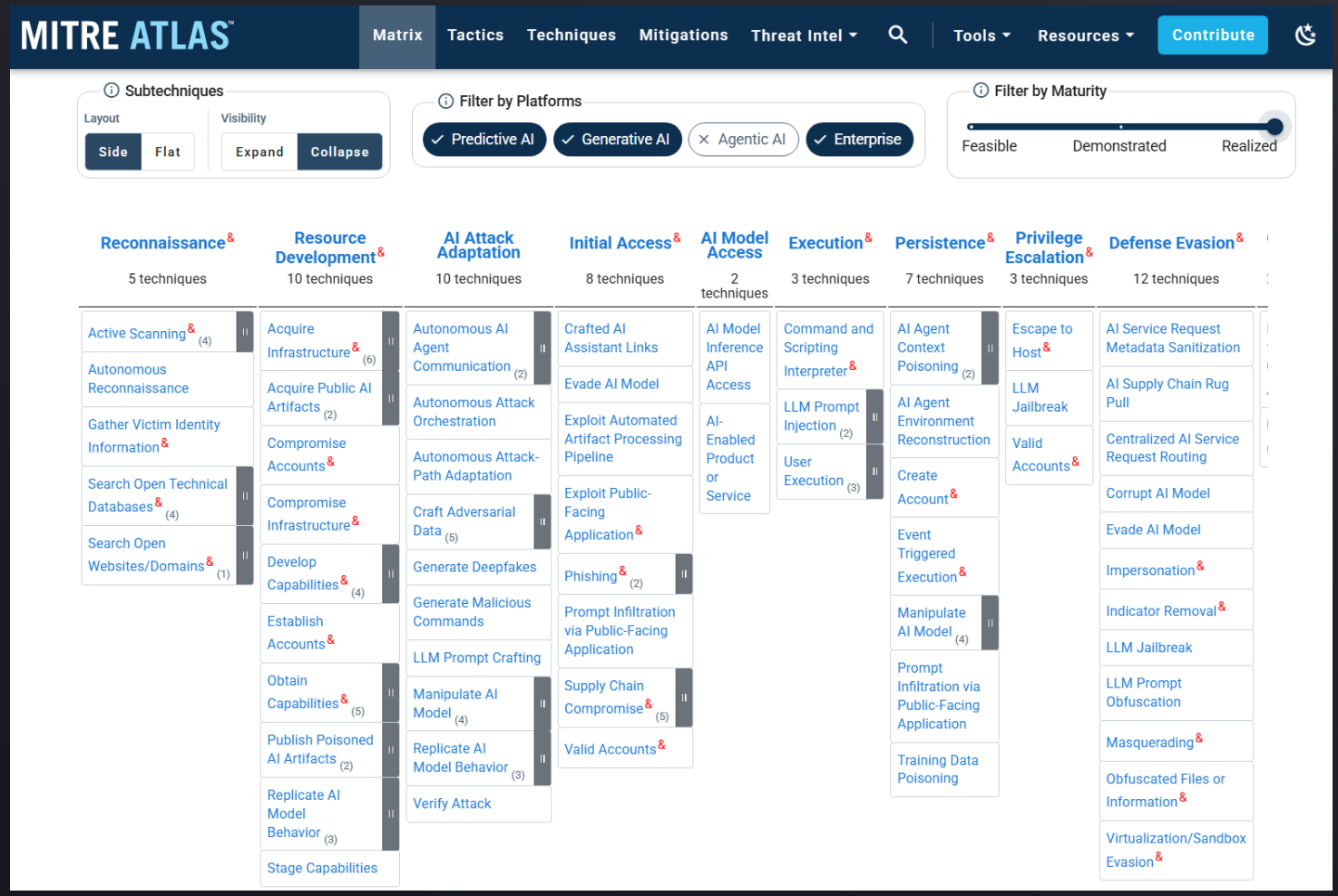
Erweiterte AI-Security

- Kontrolle von AI-Anwendungen und Zugriffen
- Erkennung und Steuerung von AI-Diensten
- Kontrolle von Prompts und Responses
- Kontrolle von AI- und Agent-Berechtigungen
- Schutz von LLMs, RAG und AI-Interaktionen
- Erkennung und Analyse AI-spezifischer Risiken

MITRE ATLAS

Taktiken und Techniken

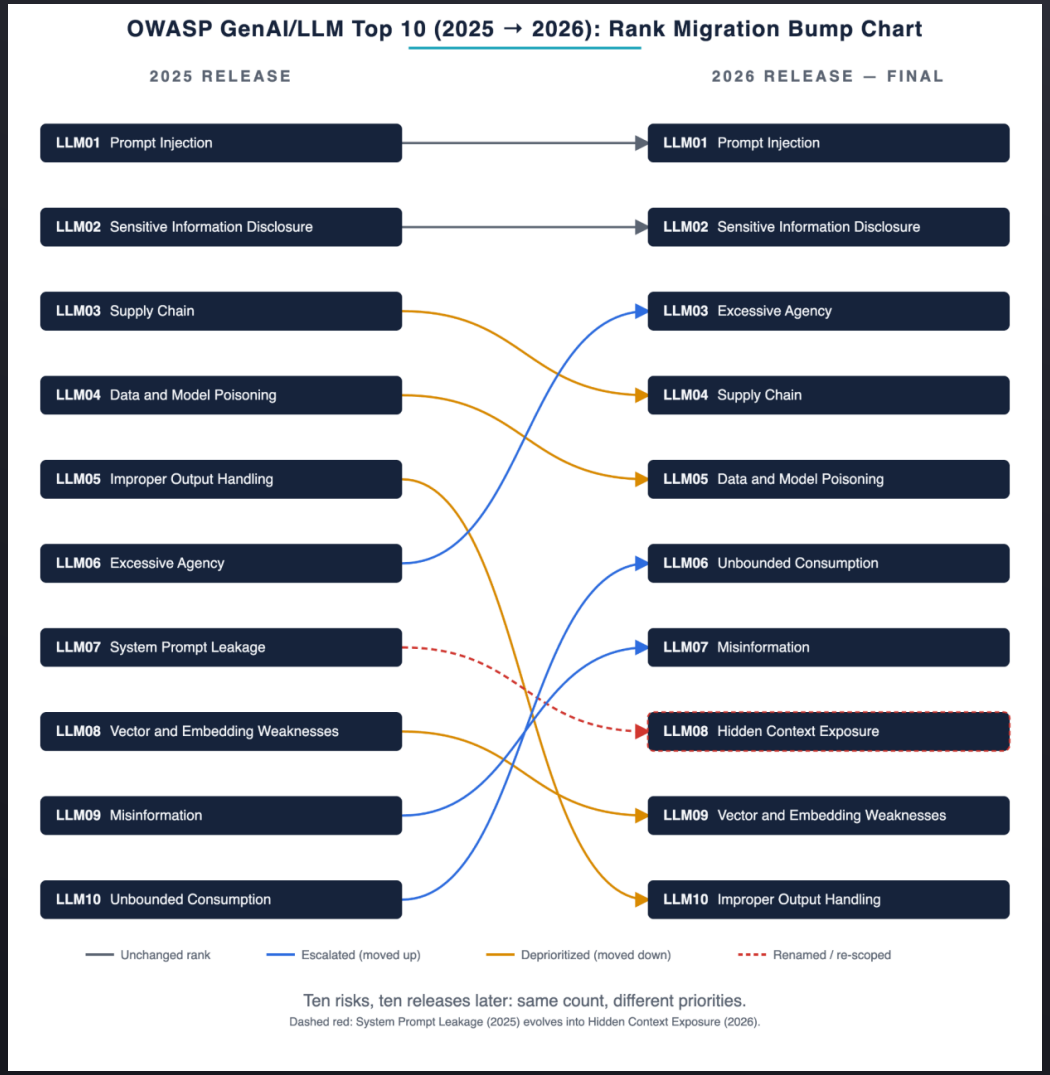
AVANTEC
Competence. Security. Trust.



https://atlas.mitre.org/matrices/ATLAS-matrix

OWASP GenAI/LLM Top 10

Schwachstellen



https://genai.owasp.org/resource/owasp-genai-llm-top-10-2026/

Drei Herausforderungen für Unternehmen

Sichere AI-Nutzung beginnt mit drei Fragen.

AVANTEC
Competence. Security. Trust.

Visibility



Was passiert in unserem Unternehmen?

- Welche AI-Anwendungen werden genutzt?
- Wer nutzt welche Dienste und wie häufig?
- Welche Daten werden verarbeitet?

Control



Was ist erlaubt und was nicht?

- Welche AI-Anwendungen dürfen genutzt werden?
- Welche Daten dürfen übermittelt werden?
- Welche Interaktionen müssen kontrolliert werden?

Protection



Wie schützen wir unsere eigenen AI-Systeme?

- Wie sichern wir AI-Anwendungen und Agenten ab?
- Wie verhindern wir Prompt Injection und Datenabfluss?
- Wie kontrollieren wir Berechtigungen und Aktionen?

Was muss eine moderne AI-Security-Architektur leisten?

Von Transparenz bis zum kontinuierlichen Schutz.

AVANTEC
Competence. Security. Trust.

1. **DISCOVER**
   AI-Anwendungen, Modelle, Agents und Datenflüsse identifizieren.

2. **ASSESS**
   Risiken, Datenklassifizierung und Berechtigungen bewerten.

3. **CONTROL**
   AI-Nutzung steuern und Sicherheitsrichtlinien durchsetzen.

4. **PROTECT**
   Daten, Prompts, Responses, AI-Anwendungen und Agents absichern.

5. **VALIDATE**
   AI-Systeme testen, Angriffe simulieren und Sicherheitsmassnahmen kontinuierlich überprüfen.

AI sicher nutzen. Kontrolle behalten.

Die drei zentralen Handlungsfelder für Security-Verantwortliche:

AVANTEC
Competence. Security. Trust.

KNOW YOUR AI

- Transparenz schaffen und die tatsächliche AI-Nutzung verstehen.

CONTROL YOUR AI

- Anwendungen, Daten und Interaktionen gezielt kontrollieren.

PROTECT YOUR AI

- Eigene AI-Anwendungen, Modelle und Agents absichern.

AI Security: Nicht AI verhindern, sondern AI sicher ermöglichen.

AVANTEC
Competence. Security. Trust.





Demo-Time

Drei Beispiele aus der Praxis

Drei Lösungen im Praxiseinsatz

Alle Hersteller decken sämtliche Themengebiete ab.
Die Auswahl der drei Demos ist exemplarisch und zufällig.

AVANTEC
Competence. Security. Trust.

Check Point
Workforce AI Security

- **DISCOVER**
- **ASSES**
- **CONTROL**
- **PROTECT**


User

Prompts →


KI-Assistenten

- AI Security Posture Management
- Transparenz über AI-Anwendungen
- Zugriffskontrollen und Data Loss Prevention
- Schutz vor Datenabfluss und manipulierten Prompts

Zscaler
AI Guard

- **CONTROL**
- **PROTECT**


User

Prompts →
← Antworten


KI-Anwendung

- Umfassender Schutz für eigene LLMs
- Zugriffskontrollen und Data Loss Prevention
- Kontrolle von Prompts und Responses mit AI Guardrails
- Schutz vor Datenabfluss und manipulierten Prompts

Netskope
AI Red Teaming

- **VALIDATE**


AI Red Teaming

Prompts →
← Antworten


KI-Anwendung

- Sind Chatbots anfällig für Prompt Injection?
- Geben sie vertrauliche Informationen preis?
- Lassen sich LLMs zu unerwünschten Aktionen bewegen?