

# Application & AI Security

Die digitale Transformation und der Einsatz von künstlicher Intelligenz beschleunigen die Innovation, schaffen aber gleichzeitig neue und komplexe Angriffsvektoren in Anwendungen und KI-Modellen.

Kontrollen am Ende des Lebenszyklus kommen zu spät. Wir verankern Sicherheit dort, wo sie wirkt: in Architekturentscheidungen, im SDLC und in MLOps. Ziel ist, die Angriffsfläche klein zu halten, Änderungen zuverlässig auszuliefern und regulatorische Vorgaben nachweisbar zu erfüllen.

Wahre digitale Resilienz entsteht, wenn Sicherheit von Anfang an in den gesamten Entwicklungszyklus integriert wird („Shift Left“). Ein robuster Ansatz für Application und AI Security stellt sicher, dass Ihre Innovationen nicht nur schnell, sondern auch sicher auf den Markt kommen, das Vertrauen Ihrer Kunden stärken und Ihr Unternehmen vor neuartigen Bedrohungen nachhaltig schützen.

## Typische Ausgangslage:

- Nachgelagerte Sicherheitsprüfungen **verlangsamen die Entwicklungs- und Release-Zyklen** und werden als Engpass wahrgenommen.
- **Schwachstellen in Anwendungen werden erst spät** in der Test- oder Produktionsphase entdeckt, was hohe Kosten für die Behebung verursacht.
- Es fehlt an spezifischem Know-how zur **Absicherung von KI-Systemen** gegen Angriffe wie Data Poisoning, Model Evasion oder den Diebstahl von Modellen.
- Die Einhaltung neuer **regulatorischer Anforderungen** (z. B. EU AI Act oder Cyber Resilience Act) für (KI-)Anwendungen stellt eine komplexe und unübersichtliche Herausforderung dar.

Ohne einen integrierten Ansatz für die **Sicherheit von Anwendungen und KI** bleibt Innovation ein unkalkulierbares Risiko und Sicherheit wird zu einer Bremse statt zu einem strategischen Wegbereiter für Agilität und Qualität.

## Unser Vorgehen:

Wir verstehen, dass jede Anwendungslandschaft und jeder KI-Anwendungsfall **einzigartig** ist. Daher entwickeln wir maßgeschneiderte Sicherheitsstrategien und -lösungen, die sich nahtlos in Ihre bestehenden **Entwicklungs- und MLOps-Prozesse** einfügen.

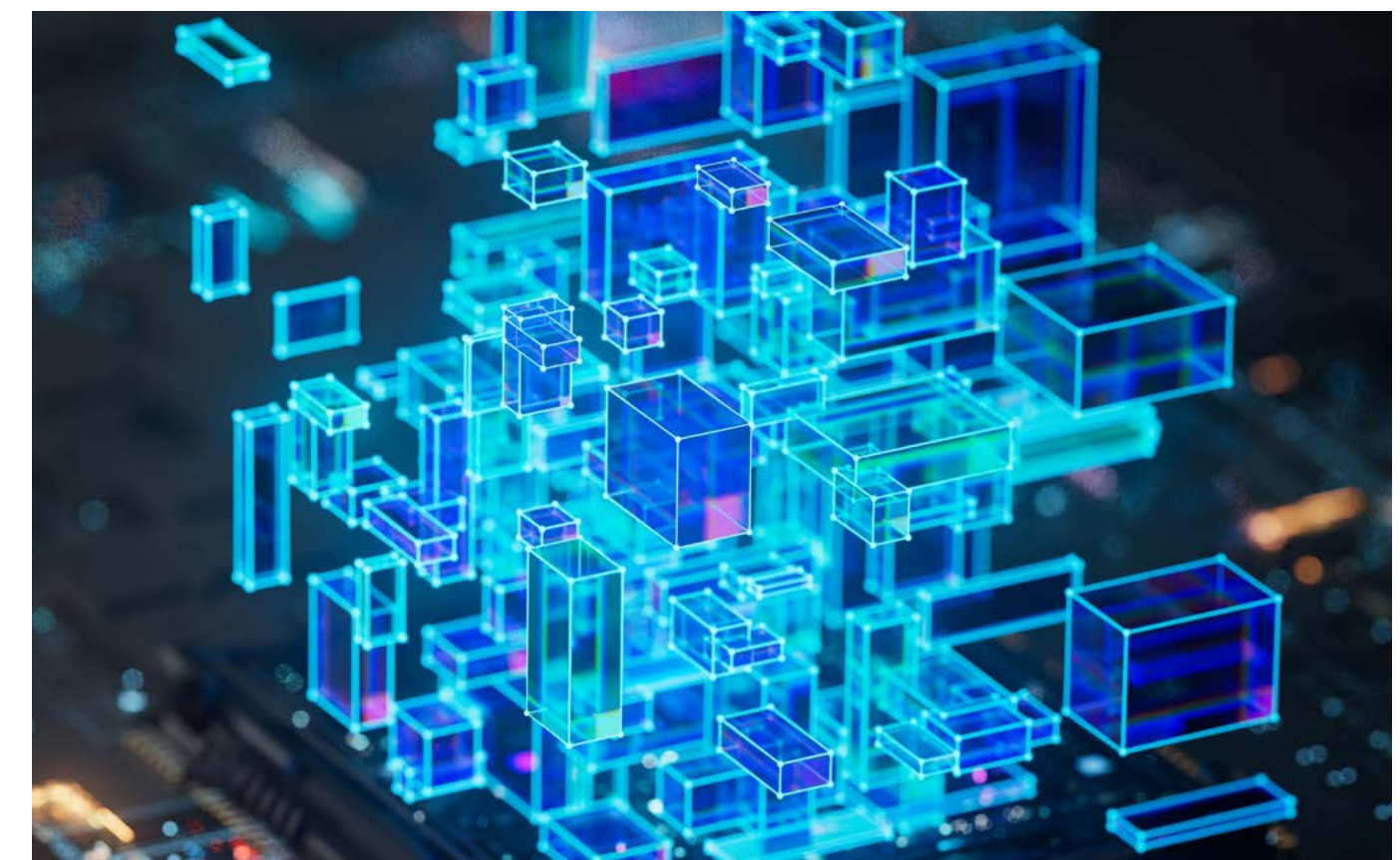
In DevSecOps setzen wir auf **Automatisierung**: Policies als Code, signierte Artefakte, SBOM und Herkunftsnachweise schaffen eine überprüfbare Lieferkette; Zugriffe auf Build- und Deploy-Pipelines sind streng gesteuert, Freigaben folgen einem Risiko- und Vier-Augen-Prinzip.

Das Ergebnis sind stabilere Releases mit weniger Nacharbeiten, nachvollziehbare Sicherheitsentscheidungen und **auditfähige Artefakte** im Tagesgeschäft. Die Angriffsfläche in Code, Daten und Modellen sinkt messbar.

Wir helfen Ihnen, Sicherheitsrisiken in Ihrem Software- und KI-Lebenszyklus frühzeitig

durch **Threat Modeling** zu identifizieren, die richtigen Werkzeuge in Ihre **CI/CD-Pipeline** zu integrieren und das Sicherheitsbewusstsein Ihrer Teams zu schärfen.

Mit unserer umfassenden Expertise in DevSecOps und AI Security sind wir Ihr Partner beim Aufbau einer sicheren Innovationskultur. So können Sie die Chancen der Digitalisierung und KI voll ausschöpfen und sind gleichzeitig für die Bedrohungen von morgen gewappnet.



**KPMG.**  
**Make the**  
**Difference.**

## Kontakt

Für weitere Informationen wenden Sie sich bitte an unsere Expert:innen oder besuchen Sie uns unter [kpmg.at](https://www.kpmg.at).

**Bernhard Knasmüller**  
Senior Manager

M +43 664 888 29180  
[bknasmueller@kpmg.at](mailto:bknasmueller@kpmg.at)

**Victoria Edelsbacher**  
Assistant Managerin

M +43 664 883 08779  
[vedelsbacher@kpmg.at](mailto:vedelsbacher@kpmg.at)

[kpmg.at](https://www.kpmg.at)



© 2025 KPMG Austria GmbH Wirtschaftsprüfungs- und Steuerberatungsgesellschaft, eine österreichische Gesellschaft mit beschränkter Haftung und ein Mitglied der globalen KPMG Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer private English company limited by guarantee, angeschlossen sind. Alle Rechte vorbehalten.