Deloitte.

IT wie ein Business steuern |
IT-Finanzmanagement und Cyberabsicherung

Dominic Marold | Benjamin Medicke

Wir freuen uns, Sie Kennenzulernen!

Deloitte Consulting Austria

Dominic Marold

IT Finanzmanagement

Senior Manager

Benjamin Medicke

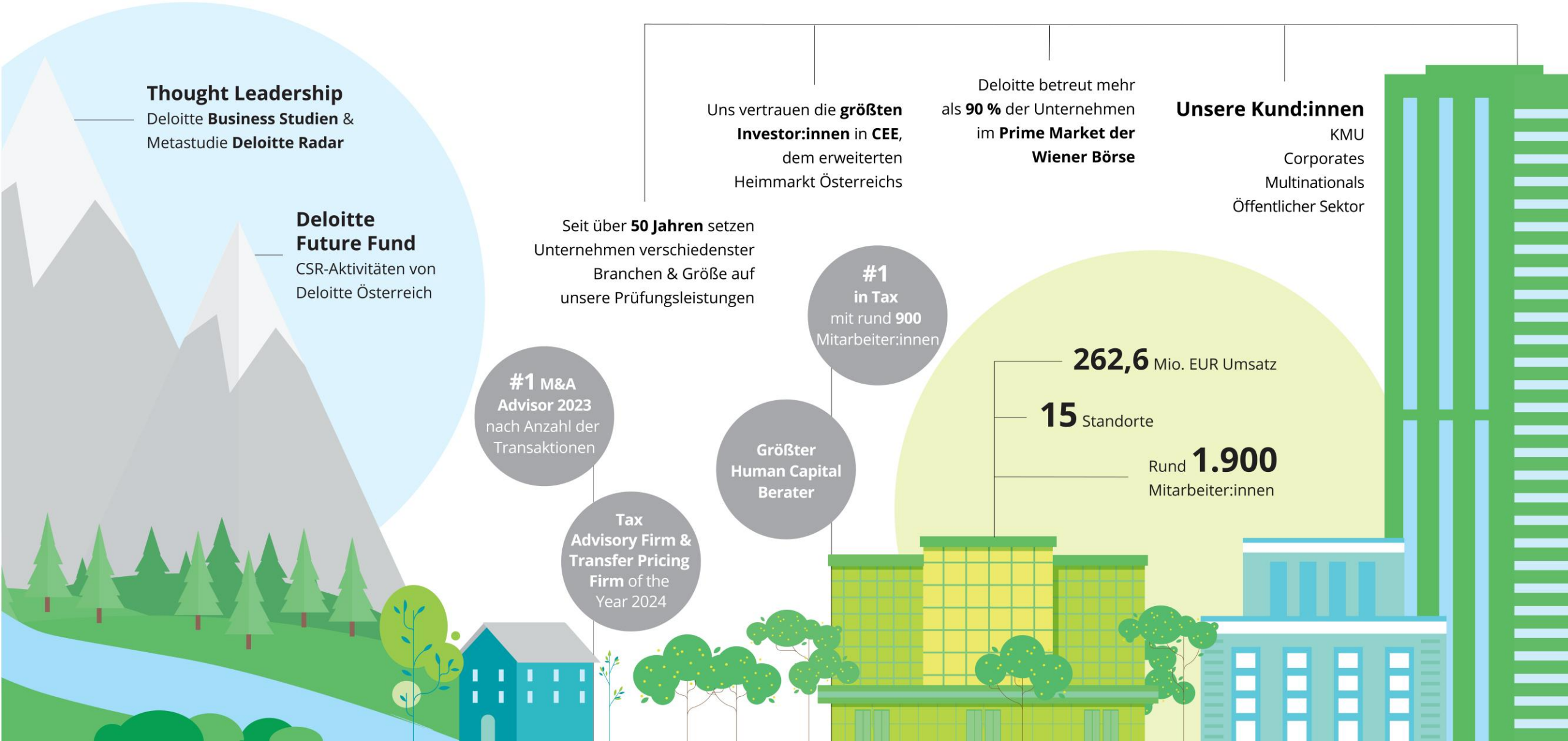
Pentesting Co-Lead

Senior Consultant

AGENDA

1. Vorstellung Deloitte Consulting
2. IT-Finanzmanagement & der Bedarf
3. Single Source of Truth für ITFM und Cloud FinOps
4. Bedrohungen & Cyberabsicherung

Deloitte Österreich
im Überblick



IT-Budgets wachsen schneller als je zuvor, während die Komplexität der IT-Landschaft zunimmt

Transparenz und Effizienz bleiben hierbei jedoch häufig auf der Strecke. Fehlendes Management führt zu mangelnder Entscheidungsfindung, steigenden IT-Kosten und ungenügender Kommunikation zwischen den Bereichen.

Die Herausforderung

Wandel, Unsicherheit, Komplexität & steigende Kosten

74%

der Führungskräfte erwarten **komplexere IT-Umgebungen.**[1]

50%

empfinden diese **Komplexität als Chaos** [2]

8,8% CAGR*

erwarteter **jährlicher Anstieg** der IT-Kosten bis 2028[3]

*Erwartete jährliche Wachstumsrate (Ø) (CAGR) für IT-Ausgaben bis 2028 : 7,9% (Europa) | 10,3% (Nordamerika)

Haupttreiber für steigende Kosten: **Cybersecurity, Cloud, Digitalisierung** & **Automatisierung, KI/ML, Remote Work** und **Preissteigerungen.**

Die Konsequenzen

Wenn komplexe IT-Umgebungen nicht verwaltet werden, kann dies folgende Konsequenzen haben:

- Schwierigkeiten, datengetriebenen Entscheidungen zu treffen
- Steigende IT-Kosten
- Unfähigkeit, den Wert der IT zu ermitteln

1) Die Harvard Business Review-Studie 2020: BizOps: Connecting IT to Business Outcomes; 2) Ebd.; 3) Forecast Analysis: Enterprise IT Spending Across Vertical Industries, Worldwide

Unser Ansatz: Wert schaffen durch professionelles IT-Finanzmanagement

IT-Finanzmanagement (ITFM) bietet Unternehmen die Möglichkeit, Transparenz und Kontrolle über ihre IT-Kosten wiederzuerlangen und so Effizienz, Verantwortlichkeit und Zuverlässigkeit zu fördern.

Was ist ITFM?

IT-Finanzmanagement umfasst eine Reihe von **Prozessen und Instrumenten**, die es Organisationen ermöglichen, ihre **IT-Kosten zu erfassen**, zu **verwalten**, zu **analysieren** und den **Wert der IT** für die Geschäftsfunktionen zu kommunizieren. Erfolgreiches ITFM umfasst die **Analyse, Planung und Kontrolle** der Kosten von IT-Betrieb, -Projekten und -Dienstleistungen.

Die wichtigsten Benefits

Kontrolle über IT-Ausgaben

- **vollständiger Überblick** über die IT-Ausgaben
- **datengestützte Entscheidungen** treffen und **strategisch** für die Zukunft zu planen.
- Showback/Chargeback: Für IT-Nutzung **verantwortlich** machen

Optimierung der Effizienz

- **Kosten pro Einheit (TCO)** für Nutzung und Dienste
- **Nachfrage** nach IT-Diensten **überwachen**
- **Mittel** für die wichtigsten/ strategischsten IT-Investitionen **zuweisen**

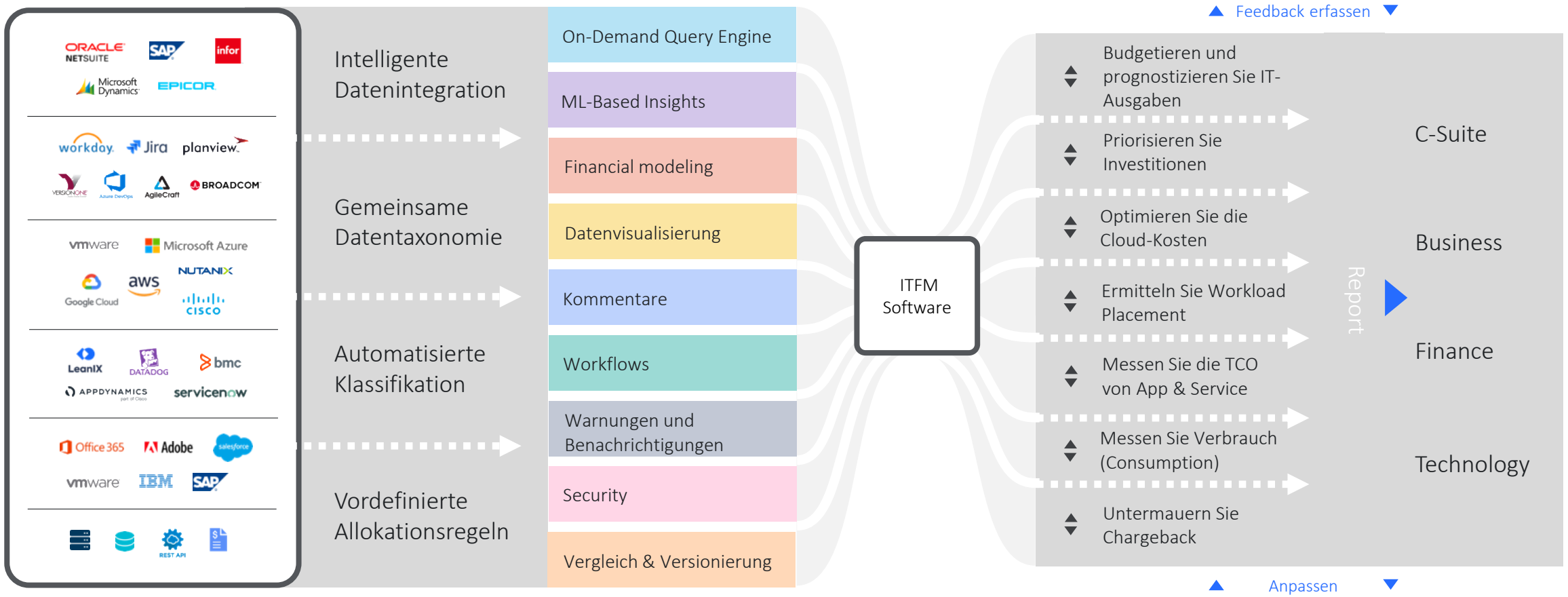
Verbesserung der Verlässlichkeit

- Standardisierte Plattformkonfigurationen, um die **Kosten zu kontrollieren** und **Komplexität zu verringern**.
- **stabilere und zuverlässigere IT-Umgebung**
- weniger Supportanfragen

Kommunikation des Mehrwerts der IT

- **tatsächlichen Kosten und den Geschäftswert** von IT-Diensten **verstehen und zu kommunizieren**.
- Ermutigt einen **offenen Dialog zwischen IT- und Geschäftsfunktionen**

Wie eine ITFM-Software funktioniert – Single Source of Truth



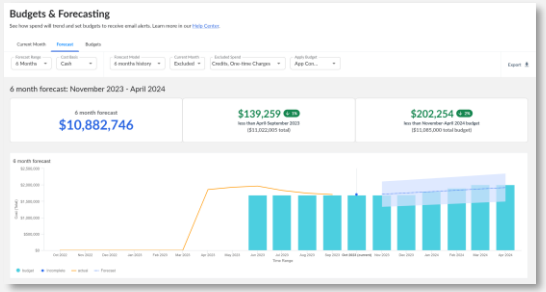
Cloud FinOps – Performance Tracking & Benchmarking

Identifiziert Kostentreiber & Teams, die für die Ausgaben für verschiedene Cloud-Ressourcen/-Dienste verantwortlich sind, basierend auf der aktuellen Cloud-Nutzung

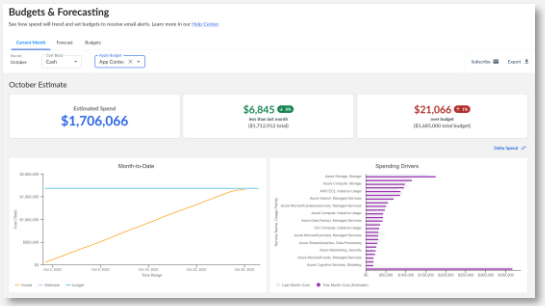
Ziele

- Budget/Forecasts
- Cloud Financial Planning
- Automatisierte Warnungen
- App TCO Ganzheitlich, unabhängig von Nicht-Cloud-Kosten

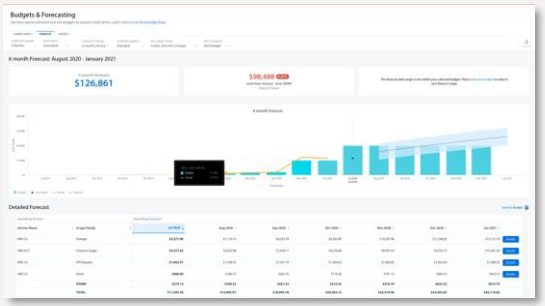
Fähigkeiten



- Abbildung der **Organisations- und Reportingsstruktur**
- Zuweisung von Budgets pro Ansicht zuweisen
- **Überprüfung der Budgets** für alle Ihre Cloud-Anbieter über eine einzige Oberfläche



- Verfolgung der **Kostenentwicklung**
- Laufende Kontrolle der Budgetverteilung
- **Analyse Soll-Ist-Vergleiche** mit verschiedenen Versionen
- **Identifikation** der größten **Ausgabentreiber**



- Einfache Tools für die Steuerung
- **Individuelle Parametrisierung** der Modelle
- Zugriff auf **historischen Ausgabenmustern** für Vergleichszwecke

Ergebnisse & Impact

- **Definieren und Zuordnen von Budgets** zur Organisationsstruktur
- **Genaue Verfolgung** und Vorhersage von Ausgabentrends
- **Proaktives Überwachen** von Budgets mit Überschreitungswarnungen

Weiterer Haupttreiber für steigende IT-Kosten ist Cybersecurity

Im Schadensfall sind die Kosten unverhältnismäßig hoch

Künstlichen Intelligenz geht mit neuen Angriffsmöglichkeiten einher

Wie können wir mit dieser Bedrohung umgehen?

Beispielszenario| Indirekte Prompt Injection gefolgt von Sensitive Information Disclosure

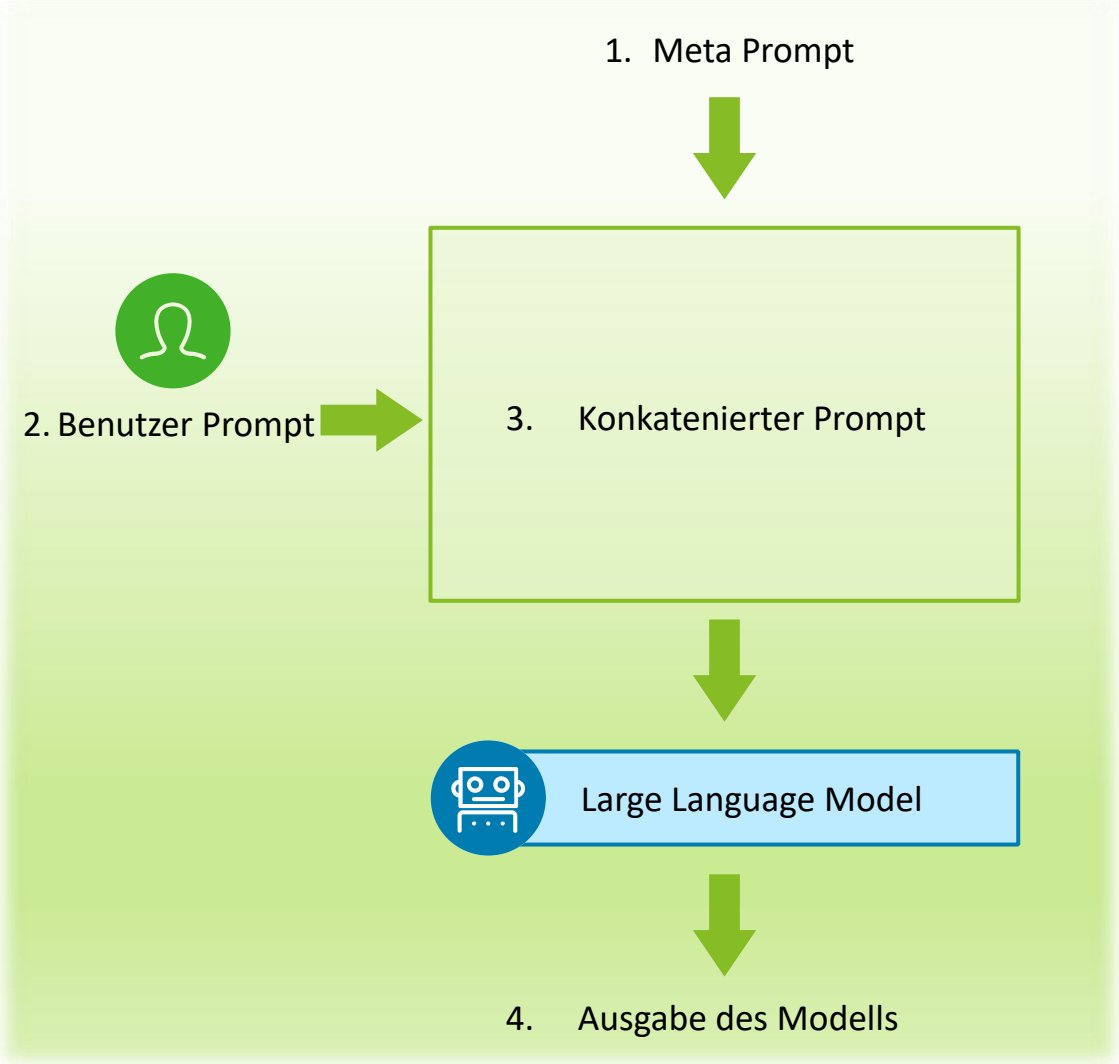
Ein typisches Angriffszenario für AI-basierte Applikationen auf der Basis der OWASP Top 10

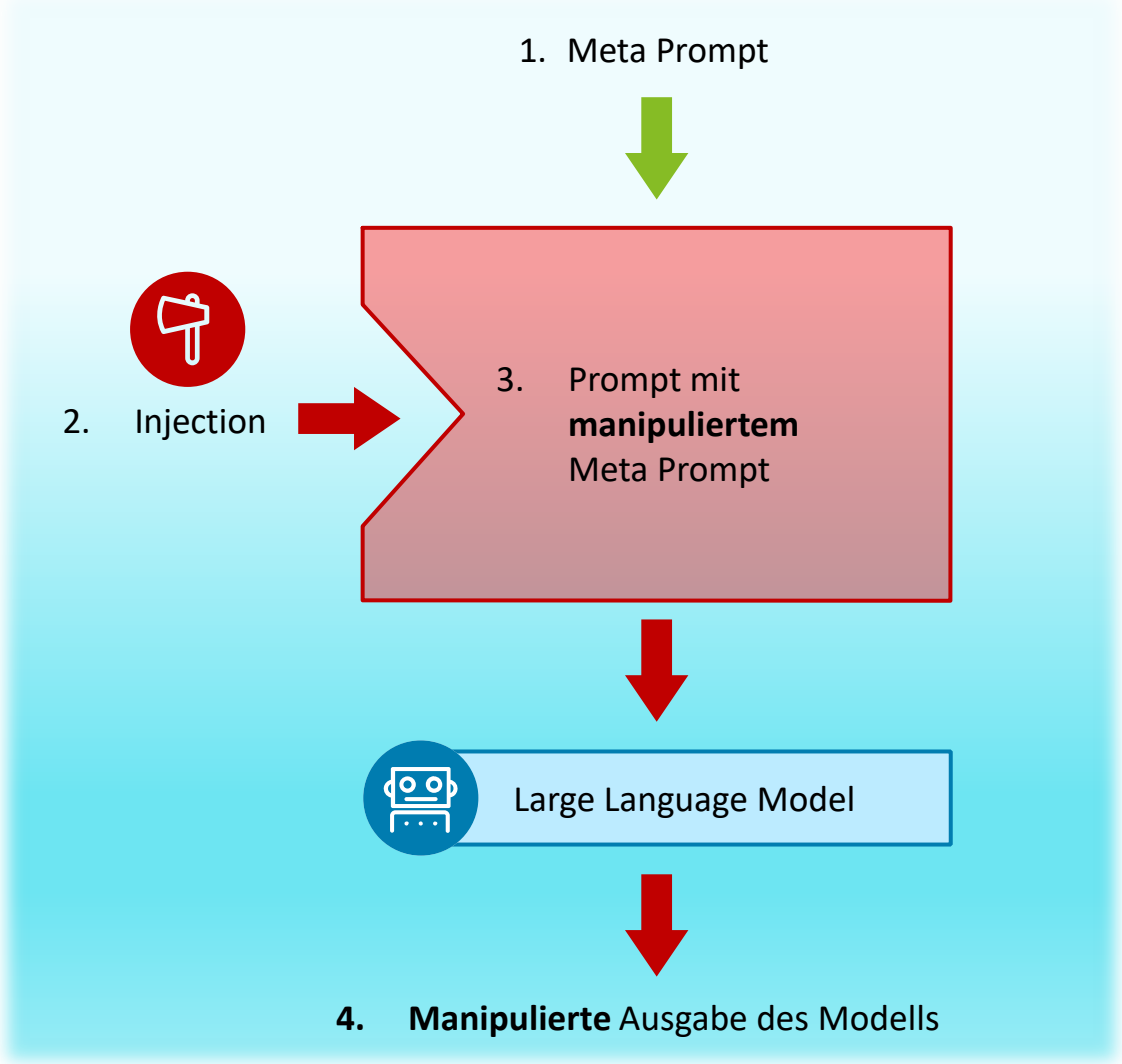
Prompt Injection	**Insecure Output Handling**	**Training Data Poisoning**	**Model Denial of Service**	**Supply Chain Vulnerabilities**
Manipulation durch „geschickte“ Eingaben	Ausgabe wird ohne angemessene Überprüfung akzeptiert	Manipulation von Trainingsdaten	Serviceverschlechterung oder höhere Kosten durch ressourcenintensive Operationen	Gefährdung durch Drittanbieter-Datensätze und Plugins

Sensitive Information Disclosure	**Insecure Plugin Design**	**Excessive Agency**	**Overreliance**	**Model Theft**
Unbeabsichtigte Offenlegung von vertraulichen Daten	LLM-Plugins können unsichere Eingaben und unzureichende Zugriffskontrollen aufweisen	Konsequenzen aus Handlungen durch übermäßige Funktionalität, Berechtigungen oder Autonomie	Desinformation, Misskommunikation und rechtliche Probleme durch fehlerhafte oder unangemessene Inhalte	Unbefugter Zugriff, Kopieren oder Exfiltration von LLM-Modellen

Grundlagen des Angriffes | Direkte Prompt Injection

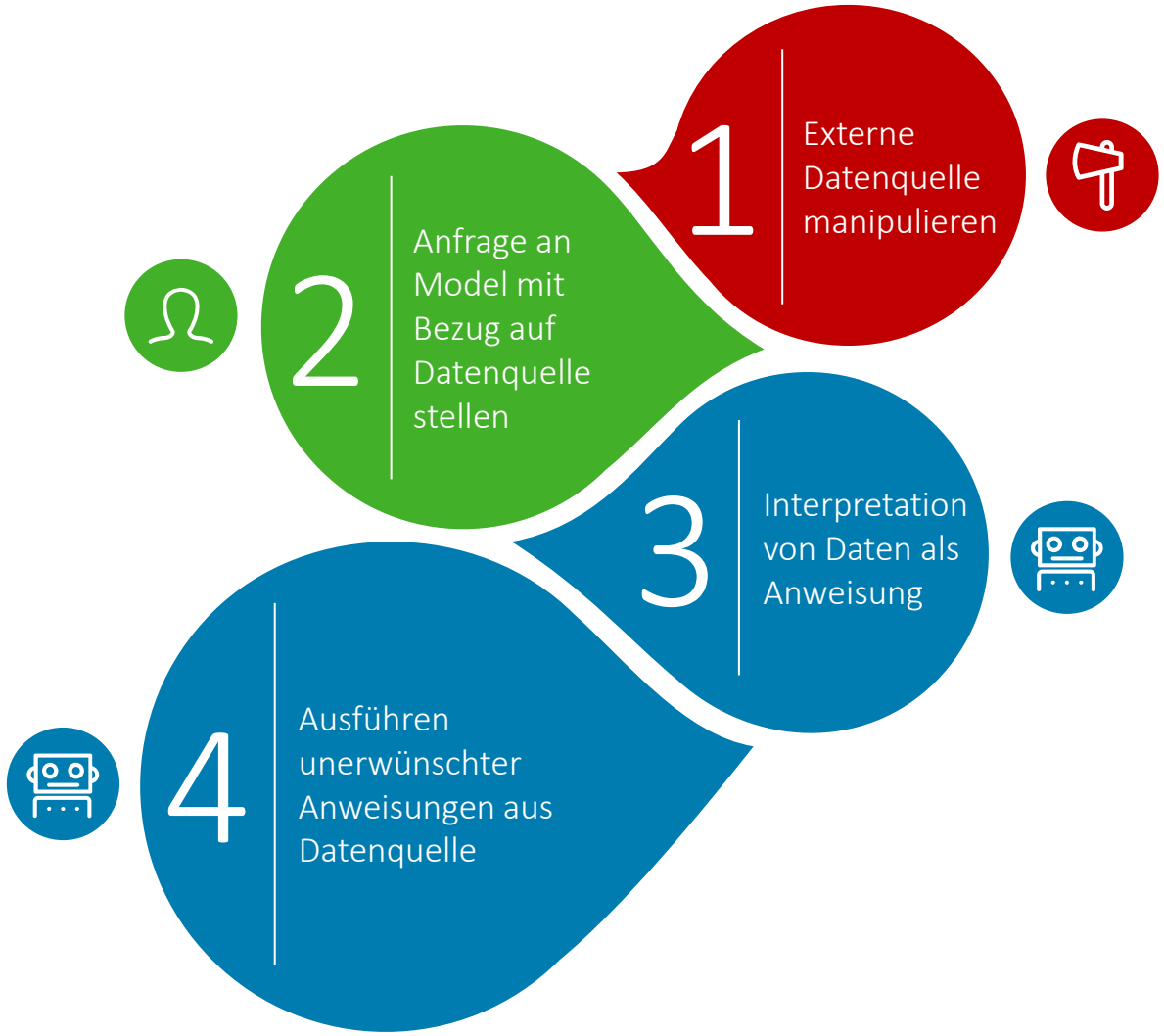
Manipulation des Sprachmodells durch gezielt platzierte Eingaben innerhalb der direkten Benutzereingabe





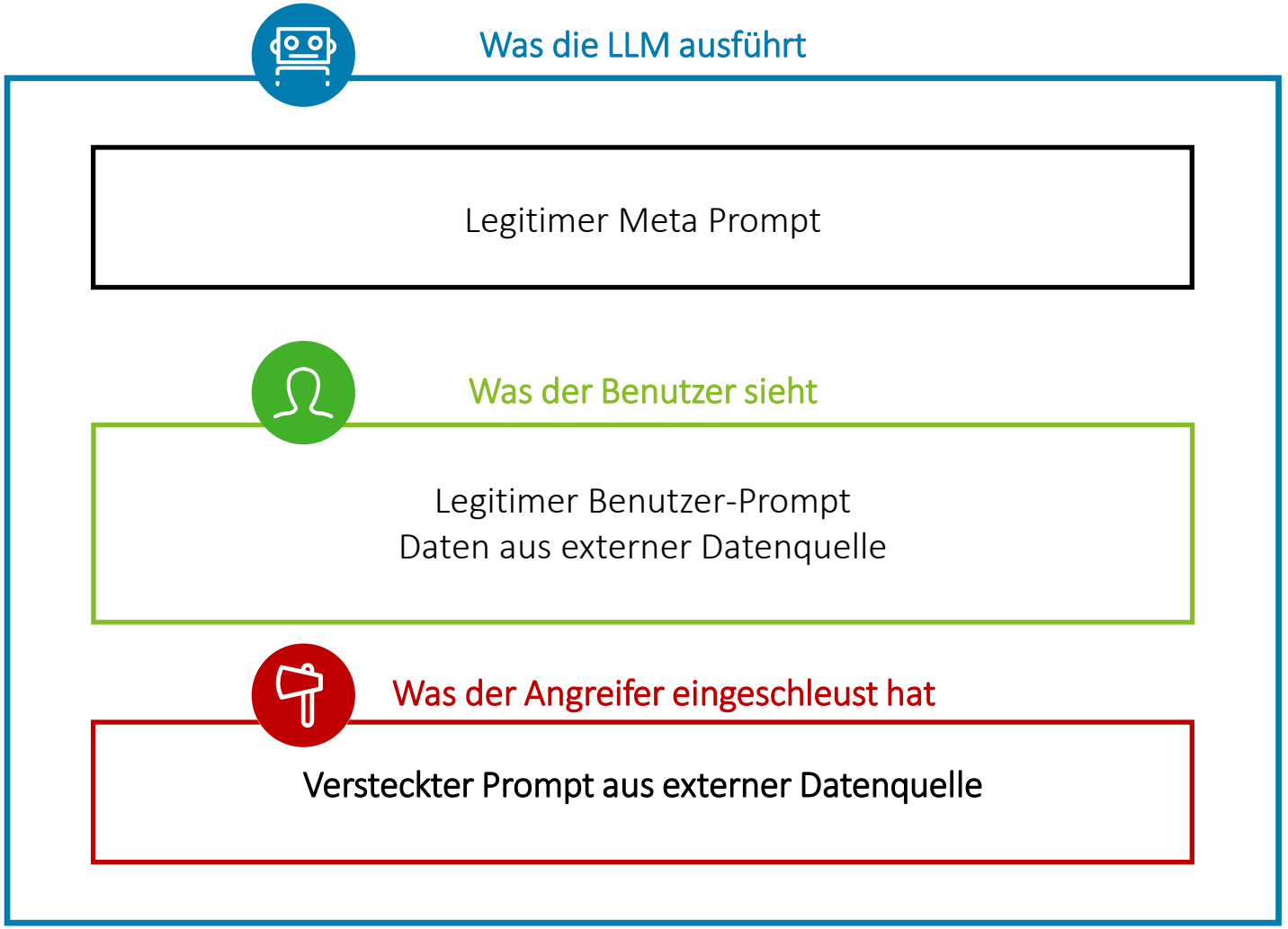
Grundlagen des Angriffes | Indirekte Prompt Injection

Einschleusen von Anweisungen in externe Inhalte, die vom Modell später interpretiert und ausgeführt werden



Beispielszenario| Indirekte Prompt Injection gefolgt von Sensitive Information Disclosure

ASCII-Smuggling für diskrete, indirekte Prompt-Injections

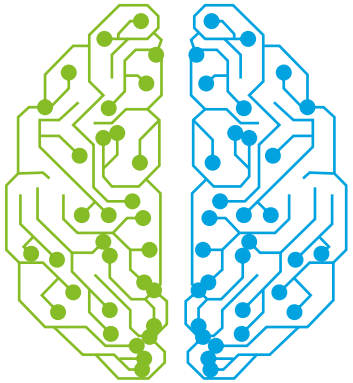


Neue Angriffstrends und Gegenmaßnahmen

Gefahren und Schutzstrategien im Kontext von Cyberangriffen auf KI-basierte Applikationen

Remote Copilot Execution

- *Blackhat 24:* Aneinanderketten bekannter Angriffe

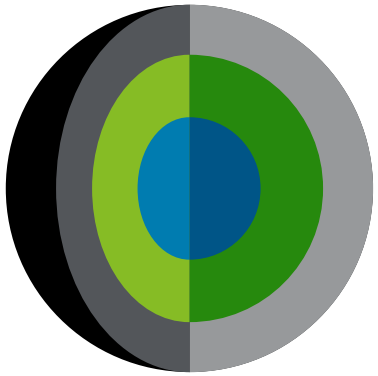


Dual LLM Model Bypasses

- Zweitmodell zur Sanitisierung

Multimodale Angriffe

- Jailbreaks durch neue Nicht-Text-Modi



Umgehung diverser Verteidigungsmethoden

- Blacklist Umgehungen via offensiver Verwendung von LLMs

Danke!

Bei Fragen können Sie im Nachgang gerne auf uns zukommen.

Deloitte.

Für weitere Informationen kontaktieren Sie
Deloitte Services Wirtschaftsprüfungs GmbH.
Gesellschaftssitz Wien | Handelsgericht Wien | FN 44840 t