Vertrauen ist gut, Zero Trust ist besser

REPLY
SPIKE

Ulrich Sickelmann
Vodafone Client Director

Mobil: +49 171 627 7771
Mail: u.sickelmann@reply.de

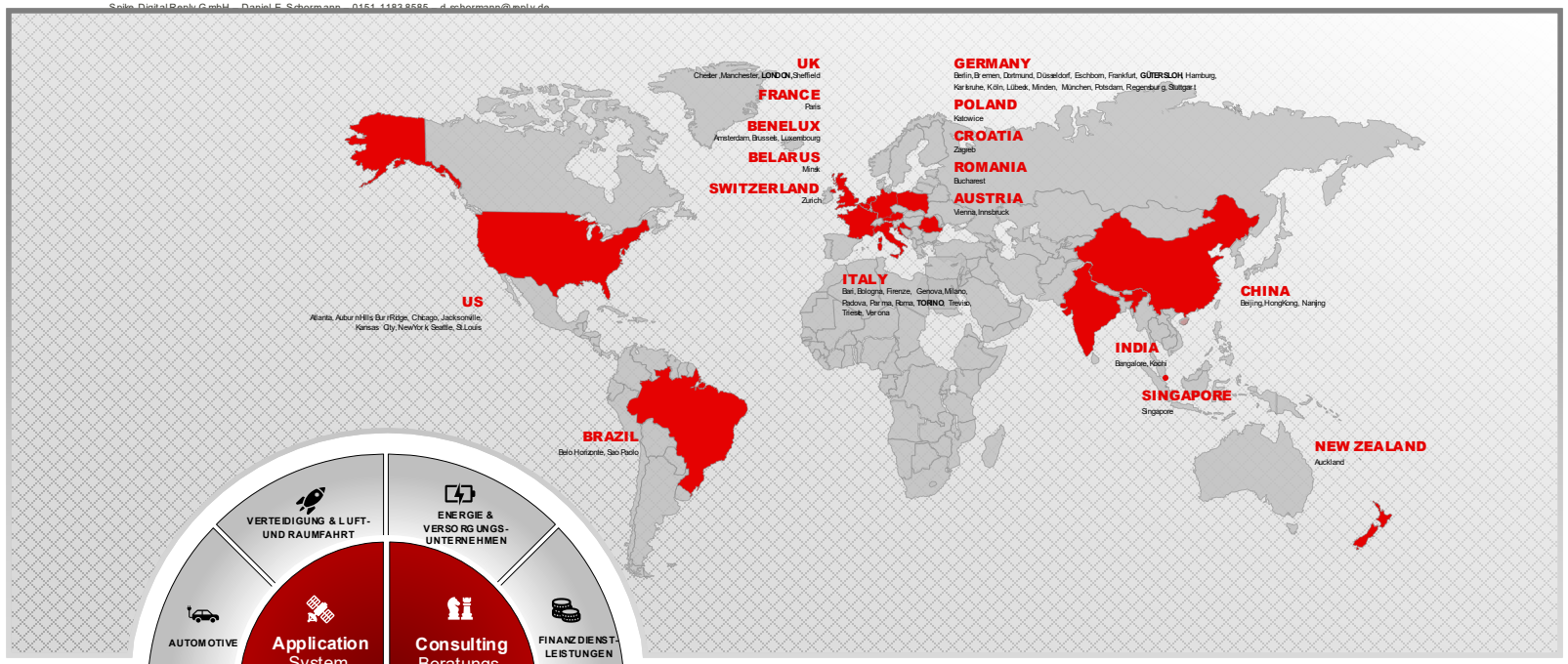
Lukas Hügle
Senior security Consultant
Mobil: +49 15119557668
Mail: l.huegle@reply.de

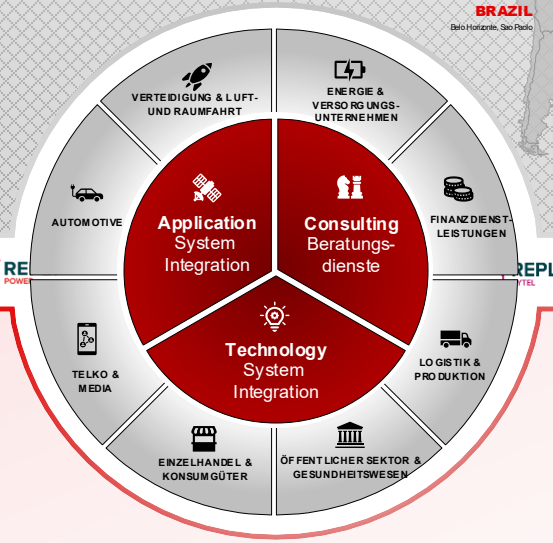
REPLY

Die Reply versteht sich als **Netzwerk** aus hochspezialisierten Unternehmen um bestmögliche **IT- und Digitalisierungs-Dienstleistungen** weltweit anzubieten.

TISAX ISO 27001 ISO 9001:2015 COMPANY

CYBER SECURITY MADE IN GERMANY





REPLY GO REPLY POWER REPLY STORM REPLY MACROS REPLY OPEN REPLY DATA REPLY TECHNOLOGY REPLY INFINITY REPLY 4BRANDS REPLY RIVERLAND REPLY AIRWALK REPLY SPRINT

15
LÄNDER

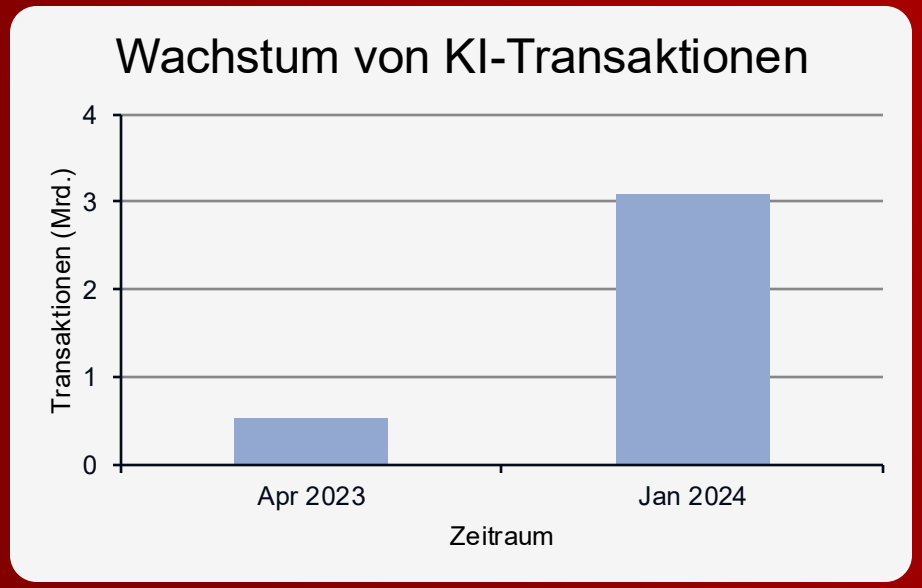
13.000+
MITARBEITER

40+
BÜROS

600+
SECURITY EXPERTS

Reply besteht **aus einem Netzwerk** von **hochspezialisierten Unternehmen**, die Kunden bei der Definition und Entwicklung von Geschäftsmodellen zur Optimierung und Integration von Prozessen, Anwendungen und Geräten unter Verwendung neuer Technologie- und Kommunikations-paradigmen unterstützen, wie z. B. Big Data, Cloud Computing, Sicherheit, digitale Kommunikation, Internet der Dinge, Mobile und Social Networking

Einführung & Adaptionslage



- AI-Transaktionen stiegen von 521 Mio. (Apr 2023) auf 3,1 Mrd. (Jan 2024) – fast 600 % Wachstum
- 18,5 % aller AI-Anfragen werden blockiert – Sicherheitsbedenken nehmen zu
- Top-Branchen: Fertigung, Finanz & Versicherungen, Services

Spike Digital Reply GmbH – Daniel E. Schormann– 0151 1183 8585 – d.schormann@reply.de

Einführung & Adaptionslage

Most businesses lack a clear AI adoption roadmap: McKinsey
Usage has doubled among businesses in the last year, but CIOs still have a laundry list of to-do’s to prepare the tech foundation and governance structure.

➡ Ohne Security keine KI-Strategie

Spike Digital Reply GmbH – Daniel E. Schormann– 0151 1183 8585 – d.schormann@reply.de

Bedrohungslandschaft

Prompt Injection
Manipulierte Eingaben entlocken Geheimnisse

Sensitive Info
Ausgaben verraten vertrauliche Daten

Daten & Modelle
Vergiftete Trainingsdaten & Backdoors

Output Handling
Unvalidierte Ausgabe → Codeausführung

Excessive Agency
Agenten mit zu viel Autonomie

Prompt Leakage
System-Prompts geben Geheimnisse preis

Vektoren & Embeddings
Schwache Vektoren ermöglichen Angriffe

Halluzination & Ressourcen
Falsche Infos & unkontrollierter Verbrauch

Spike Digital Reply GmbH – Daniel E. Schormann– 0151 1183 8585 – d.schormann@reply.de

Absicherung von AI mit Zero-Trust-Prinzipien

Annahme eines Angriffs & Transparenz über die Nutzung von KI

Least Privilege & Schutz der durch KI genutzten und erzeugten Daten

Explizite Verifizierung & Governance der KI-Nutzung

Spike Digital Reply GmbH – Daniel E. Schormann– 0151 1183 8585 – d.schormann@reply.de

Umsetzung und Best Practices

Technische Maßnahmen

- Eingabe- & Ausgabehärtung: Filter, Gateways, Validierung
- Isolation & Sandboxing: Speicherkapselung, Containerisierung
- Monitoring & Telemetrie: Logging, Anomalieerkennung, Token-Limits
- Least Privilege & Segmentation: RBAC
- Fallback & Human-in-the-loop: Notfallpläne, manuelle Freigaben

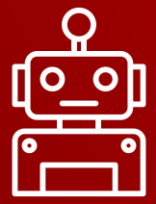
Governance & Organisation

- KI-Governance & Richtlinien: Freigabeprozesse, Datenklassifizierung
- Schulungen & Sensibilisierung: Case Studies, Red Teaming, Security-Kommunikation
- Dynamische Threat Intelligence: Red Teams & Community-Sharing
- Compliance & Datenschutz: DSFA, EU AI Act, ISO 42001

Spike Digital Reply GmbH – Daniel E. Schormann– 0151 1183 8585 – d.schormann@reply.de

Use Case – AI Terraform Converter

Cloudformation übergeben



LLM-Agent erzeugt Terraform

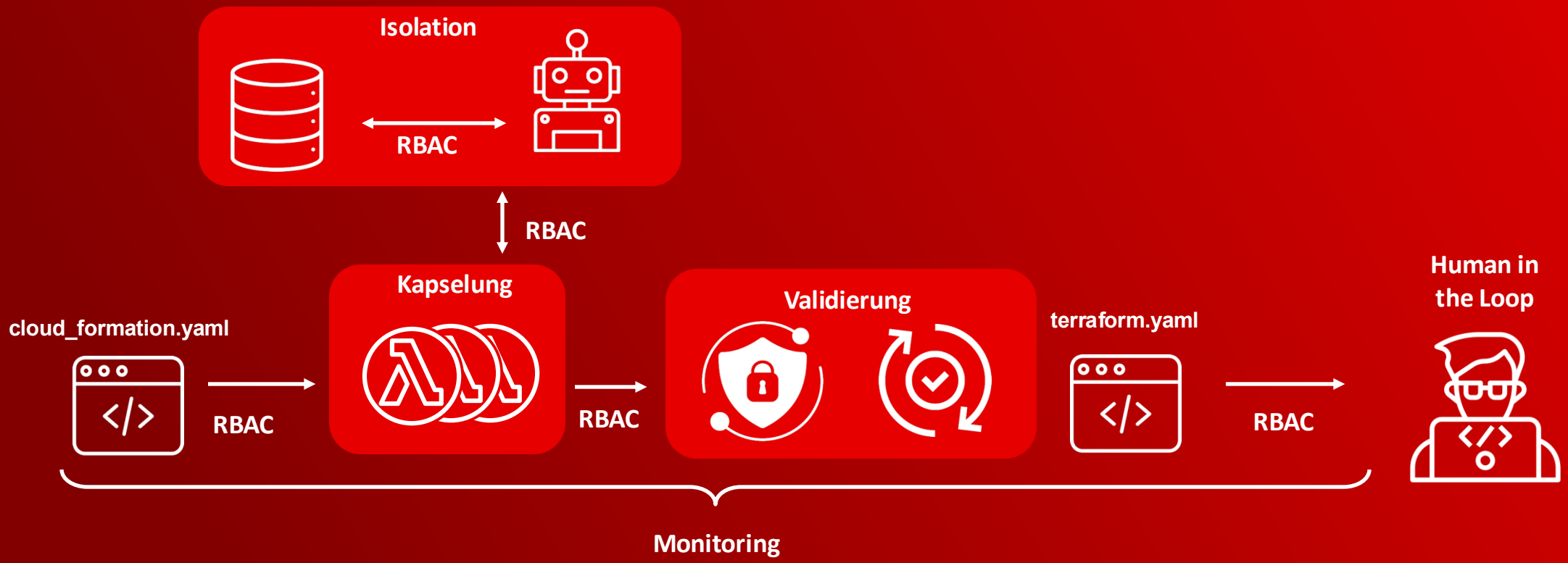
Security Validation

Deployment

- Übersetzung der Infrastruktur nach Terraform
- Die Sicherheit Verbessern
- Integration von Compliant Policies

Spike Digital Reply GmbH – Daniel E. Schormann– 0151 1183 8585 – d.schormann@reply.de

Anwendung Zero Trust



Spike Digital Reply GmbH – Daniel E. Schormann– 0151 1183 8585 – d.schormann@reply.de

Empfehlungen

1. Identifizieren Sie, wo generative Ki in ihrer Organisation eingesetzt wird
2. Klassifizieren und schützen Sie sensible Daten
3. Überwachen und kontrollieren Sie KI-bezogenes Verhalten
4. Arbeiten Sie über Sicherheits-, Daten- und Compliance-Teams hinweg zusammen.

Spike Digital Reply GmbH – Daniel E. Schormann– 0151 1183 8585 – d.schormann@reply.de

Q&A

Spike Digital Reply GmbH – Daniel E. Schormann– 0151 1183 8585 – d.schormann@reply.de