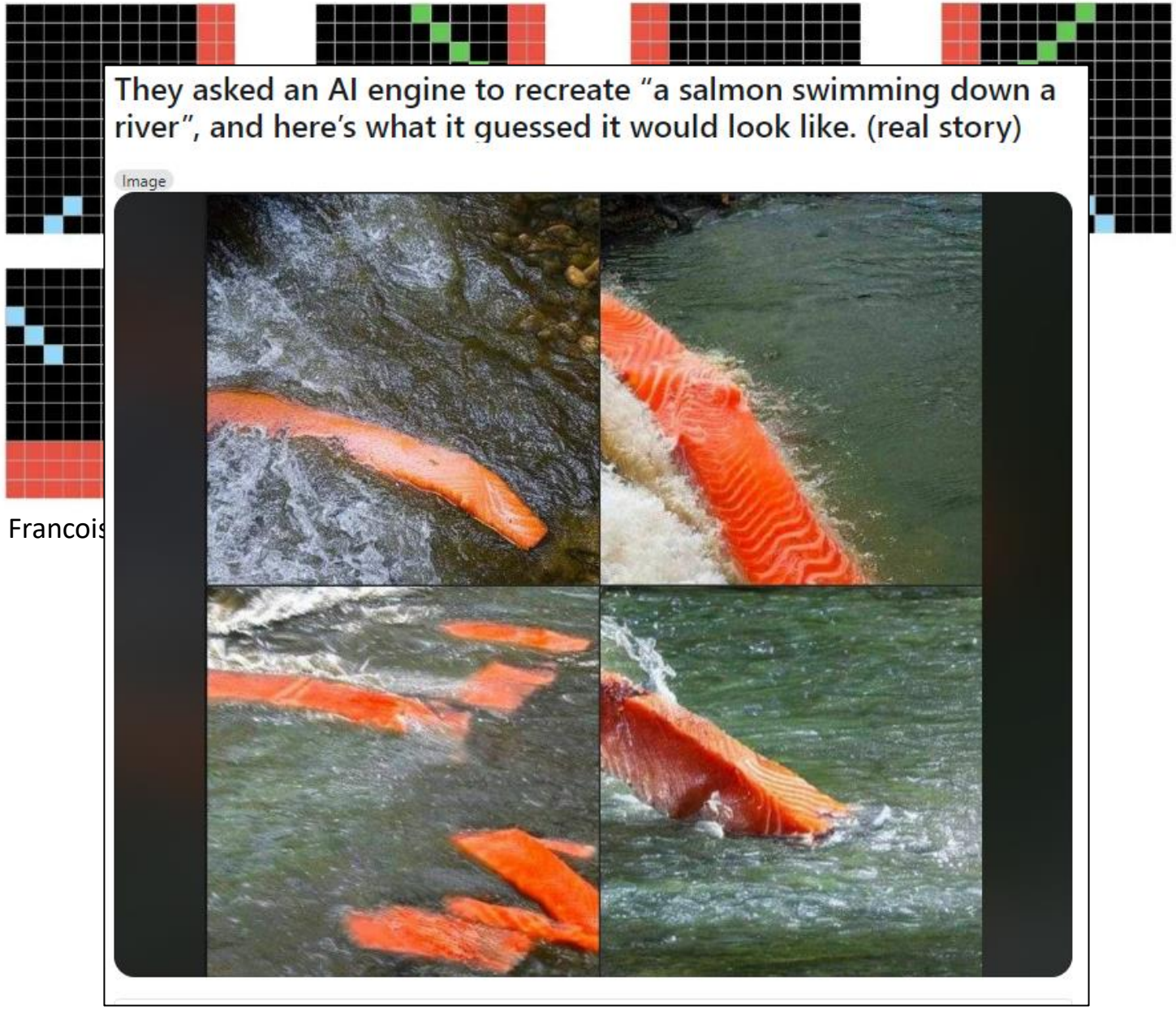
KI und Supply Chain - Cyber-Risiken, Chancen und Erfahrungen aus Sicht des Verwaltungsrats

Prof. em. Dr. Hannes Lubich
Ad Vantis Innovation AG
hannes.lubich@advantis.ch


They asked an AI engine to recreate “a salmon swimming down a river”, and here’s what it guessed it would look like. (real story)
Image

Francois

Anwendung im Unternehmen

3 (schlechte) Alternativen:

- kein Einsatz oder stark überregulierter Einsatz
- Eigenbetrieb
- Einsatz unter Missachtung der gesetzlichen Vorgaben

PS: Kriminelle und fremde Aufklärungsdienste kümmert das nicht

Supply Chain Risiken und deren Relevanz für den Einsatz von KI-gestützten Anwendungen

- Wir sind und bleiben von unseren Versorgern kritisch abhängig
- Wir sind meist Versorgte und Versorger in komplexen und dynamischen Wertschöpfungsketten
- Wir managen Lieferanten und Partner oft nur unzureichend (Vorgaben, Kontrolle der Einhaltung, Massnahmen)
- Verschiedenste Angreifer nutzen diese Schwachstellen systematisch aus
- Neue Gesetze und Regularien (ESG-Reporting, NIS-2/CER usw.) erzwingen erhöhte Aufmerksamkeit für das Thema
- Fremdbetriebene KI-Modelle und deren Anwendung verschärfen das Problem erheblich (Datenschutz, Haftung, Urheberrecht, Arbeitsrecht, Nachvollziehbarkeit)

4 Kernfragen für die Breakout-Session

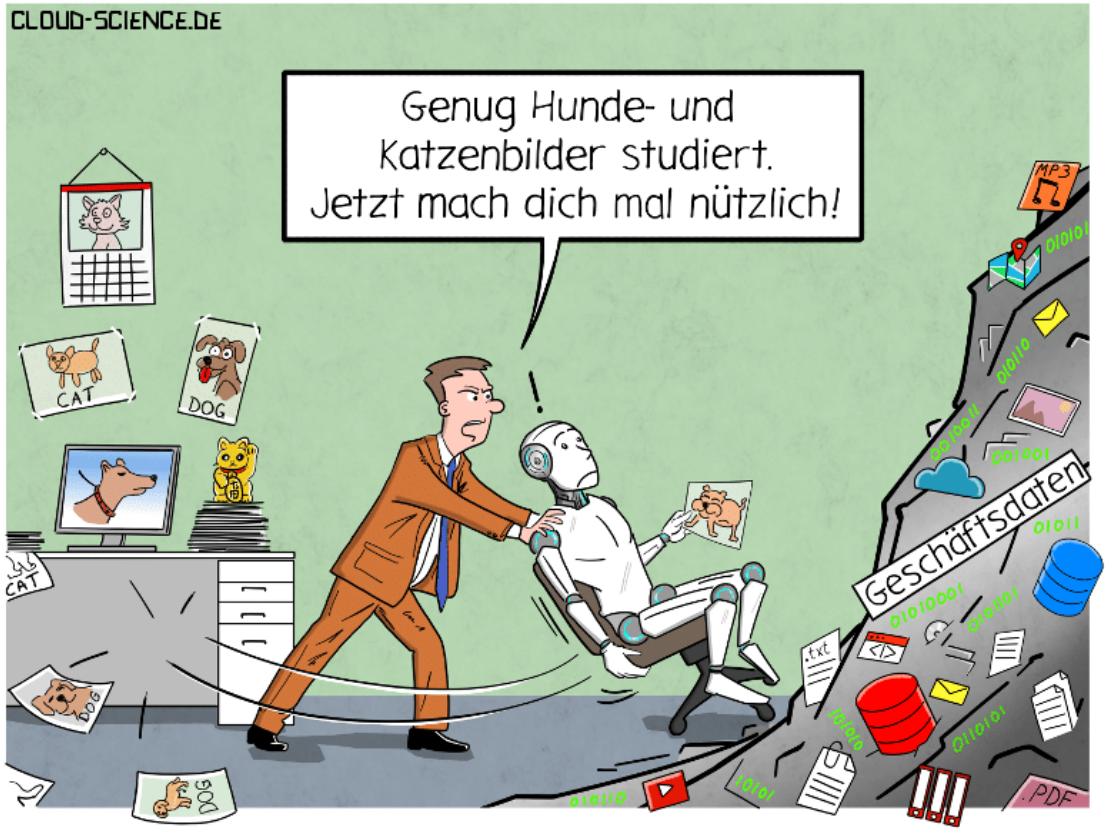
1. Nutzungsmuster von KI im Unternehmensumfeld

2. Einfluss auf die übergeordnete Strategie und Governance

3. Geschäftliche und Cyber-Risiken aus der Nutzung fremdbetriebener KI-Modelle und Anwendungen

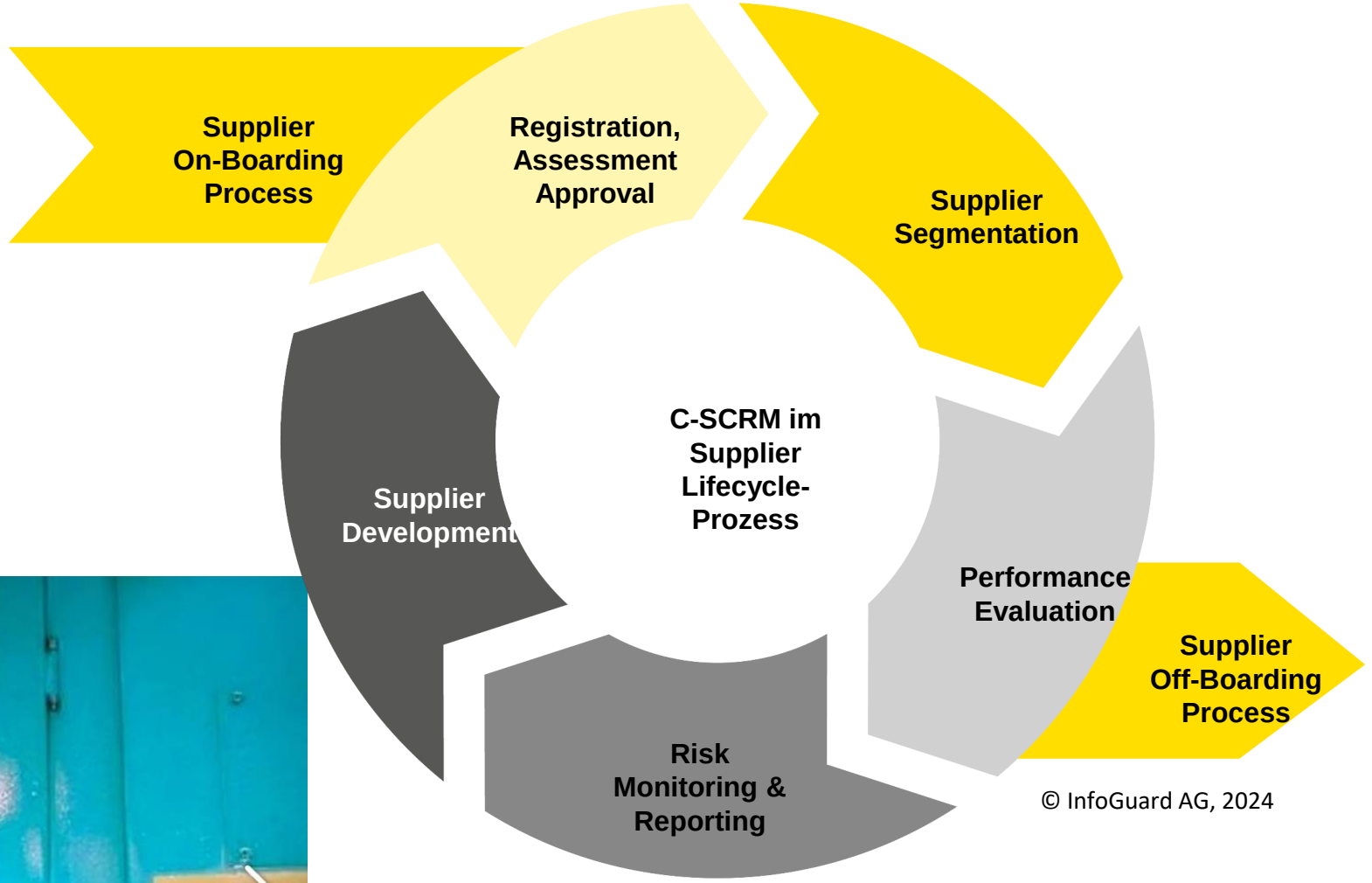
4. Erfahrungen, mögliche Massnahmen und Handlungsoptionen

Stufengerechte Befassung des VR



- Kompetenzaufbau
- Einfluss auf die Strategie
- Vorgaben
- Rahmenbedingungen
- Management von Chancen und Risiken
- Ausreichende Governance

Fazit



© InfoGuard AG, 2024