OUTSELL PLAYBOOK

OUTSELL JOURNAL - BESCHLUSSBESCHREIBUNG

Migration zu gehosteten KI-Agenten: ein Evidenzkontinuitätsplan

FRAGE

Wie erklärt man den Wechsel von eigener Agenteninfrastruktur zu einem gehosteten Runtime, ohne ihn als automatischen Qualitäts-, Sicherheits- oder Skalierungsbeleg darzustellen?

LEITFAHRZEUGE

Bewahren Sie Produktgrenze, Eval-Set, Trace-IDs, Sicherheitsentscheidungen und Rollback-Kriterien. Managed Infrastructure verändert Verantwortung, nicht die Evidenzpflicht.

HIER FREIST

Aufgabe, Konsequenz und Owner definieren.

DEINE LAGE

Account oder Kohorte

Entscheidung zu treffen

Ausgangszustand und Ausschlüsse

Evidenzquellen, Daten und Grenzen

Unbekannt zur Validierung

ARBEITEN DURCH DEN LEITFAHRT

1. Aufgabe, Konsequenz und Owner definieren

Nachweis oder Eingabe

Output oder Entscheidung

Eigentümer und Überprüfungsstelle

2. Schnittstellen, Daten und Schwellen einfrieren

Nachweis oder Eingabe

Output oder Entscheidung

Eigentümer und Überprüfungsstelle

3. Sessions, Netzwerk, Telemetrie und Lifecycle abbilden

Nachweis oder Eingabe

Output oder Entscheidung

Eigentümer und Überprüfungsstelle

4. Migration und Rollback proben

Nachweis oder Eingabe

Output oder Entscheidung

Eigentümer und Überprüfungsstelle

5. Nur mit Evidenz und datierten Grenzen releasen

Nachweis oder Eingabe

Output oder Entscheidung

Eigentümer und Überprüfungsstelle

VERGLEICH DER OPTIONEN

Self-managed Runtime

Hilfreich wenn: Infrastrukturkontrolle ist wesentlich

Einschränkung: Team besitzt Scaling und Isolation

Vorgeschlagene Aktion: Kapazität und Recovery dokumentieren

Warum das zu unserer Situation passt

Vor dem Handeln erforderliche Beweise

Hosted Agent Runtime

Hilfreich wenn: Custom Code braucht verwaltete Sessions

Einschränkung: Kontrollen bleiben konfigurationspflichtig

Vorgeschlagene Aktion: Versionen, Netzwerk, Sessions und Traces testen

Warum das zu unserer Situation passt

Vor dem Handeln erforderliche Beweise

Prompt-Agent

Hilfreich wenn: Task passt zu unterstützten Tools

Einschränkung: Weniger Runtime-Kontrolle

Vorgeschlagene Aktion: Tool- und Governance-Grenzen prüfen

Warum das zu unserer Situation passt

Vor dem Handeln erforderliche Beweise

Deterministischer Service

Hilfreich wenn: Workflow und Regeln stabil

Einschränkung: Weniger flexibel

Vorgeschlagene Aktion: Vorhersehbare Ausführung bevorzugen

Warum das zu unserer Situation passt

Vor dem Handeln erforderliche Beweise

ZUSAMMENFASSUNG ZU EINEM ABGEBOTENEN NÄCHSTEN SCHRITT

Ausgewählte Maßnahme

Verantwortlicher Eigentümer

Erforderliche Genehmigung

Erfolgsmessung und -definition

Datum der Überprüfung

Kriterien fortsetzen, überarbeiten oder stoppen

Leitfaden: https://outselll.com/de/blogs/hosted-agent-migration-evidence-continuity/

Veröffentlicher und Evidenzpolitik: https://outselll.com/de/editorial-policy/