OUTSELL PLAYBOOK

OUTSELL JOURNAL - BESCHLUSSBESCHREIBUNG

Agenten-Skill-Register für GTM: Governance für Lebenszyklus und Sicherheit

FRAGE

Wie werden Agenten-Skills genehmigt, wiederverwendet, aktualisiert und außer Betrieb genommen, ohne versteckte Risiken zu verbreiten?

LEITFAHRZEUGE

Behandeln Sie einen wiederverwendbaren Skill als versionierte Betriebssoftware, nicht als Prompt-Schnipsel. Definieren Sie Zweck, Publisher, Rechte, Scans, Tests, Eigentümer, Rollback und Stilllegung.

HIER FREIST

Zweck, Publisher und Abhängigkeiten registrieren.

DEINE LAGE

Account oder Kohorte

Entscheidung zu treffen

Ausgangszustand und Ausschlüsse

Evidenzquellen, Daten und Grenzen

Unbekannt zur Validierung

ARBEITEN DURCH DEN LEITFAHRT

1. Zweck, Publisher und Abhängigkeiten registrieren

Nachweis oder Eingabe

Output oder Entscheidung

Eigentümer und Überprüfungsstelle

2. Risiko und geringste Rechte zuweisen

Nachweis oder Eingabe

Output oder Entscheidung

Eigentümer und Überprüfungsstelle

3. Jede Revision scannen und prüfen

Nachweis oder Eingabe

Output oder Entscheidung

Eigentümer und Überprüfungsstelle

4. Entscheidungsspezifische Regression testen

Nachweis oder Eingabe

Output oder Entscheidung

Eigentümer und Überprüfungsstelle

5. Pilotieren, überwachen, zurückrollen, stilllegen

Nachweis oder Eingabe

Output oder Entscheidung

Eigentümer und Überprüfungsstelle

VERGLEICH DER OPTIONEN

Prompt-Schnipsel

Hilfreich wenn: Einmalige Schreibhilfe

Einschränkung: Version und Abhängigkeiten unklar

Vorgeschlagene Aktion: Lokal halten und Ausgabe prüfen

Warum das zu unserer Situation passt

Vor dem Handeln erforderliche Beweise

Registrierter Read-only-Skill

Hilfreich wenn: Wiederholbare Aufgabe mit Evidenz

Einschränkung: Fehlerhafte Anweisung verbreitet sich

Vorgeschlagene Aktion: Versionieren, scannen und testen

Warum das zu unserer Situation passt

Vor dem Handeln erforderliche Beweise

Begrenzter Aktions-Skill

Hilfreich wenn: Deterministische Änderung nötig

Einschränkung: Falsche Identität oder Retry schadet

Vorgeschlagene Aktion: Parameter validieren und freigeben

Warum das zu unserer Situation passt

Vor dem Handeln erforderliche Beweise

Breiter autonomer Skill

Hilfreich wenn: Viele Werkzeuge verbunden

Einschränkung: Autorität und Fehler verstärken sich

Vorgeschlagene Aktion: In kleinere kontrollierte Skills teilen

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/agent-skill-registry-governance-gtm/

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