OUTSELL PLAYBOOK

OUTSELL JOURNAL - BESCHLUSSBESCHREIBUNG

Agentenidentität zur Laufzeit: ein Belegplan von Autorität bis Aktion

FRAGE

Wie weisen Enterprise-KI-Anbieter nach, dass Identität, delegierte Autorität und Laufzeitaktionen eines Agenten kontrolliert bleiben?

LEITFAHRZEUGE

Registrierung und Anmeldung sind nur der Anfang. Binden Sie jeden Agenten an Eigentümer und Zweck, begrenzen Sie Delegation, nutzen Sie kurzlebigen Zugriff, beobachten Sie reale Nutzung und testen Sie Widerruf.

HIER FREIST

Agent, Eigentümer, Zweck und Version registrieren.

DEINE LAGE

Account oder Kohorte

Entscheidung zu treffen

Ausgangszustand und Ausschlüsse

Evidenzquellen, Daten und Grenzen

Unbekannt zur Validierung

ARBEITEN DURCH DEN LEITFAHRT

1. Agent, Eigentümer, Zweck und Version registrieren

Nachweis oder Eingabe

Output oder Entscheidung

Eigentümer und Überprüfungsstelle

2. Delegationsgrenze und Laufzeit festlegen

Nachweis oder Eingabe

Output oder Entscheidung

Eigentümer und Überprüfungsstelle

3. Identität, Werkzeug und Ressource korrelieren

Nachweis oder Eingabe

Output oder Entscheidung

Eigentümer und Überprüfungsstelle

4. Ablehnung, Ablauf und Widerruf proben

Nachweis oder Eingabe

Output oder Entscheidung

Eigentümer und Überprüfungsstelle

5. Belege und Lücken je Käuferrolle veröffentlichen

Nachweis oder Eingabe

Output oder Entscheidung

Eigentümer und Überprüfungsstelle

VERGLEICH DER OPTIONEN

Statische Service-Zugangsdaten

Hilfreich wenn: Deterministische Last mit festen Rechten

Einschränkung: Lange Laufzeit erhöht Exposition

Vorgeschlagene Aktion: Rotieren und eng binden

Warum das zu unserer Situation passt

Vor dem Handeln erforderliche Beweise

Registrierte Agentenidentität

Hilfreich wenn: Versionen brauchen Eigentümer und Richtlinie

Einschränkung: Registrierung steuert Verhalten nicht allein

Vorgeschlagene Aktion: Jeden Lauf an Zweck binden

Warum das zu unserer Situation passt

Vor dem Handeln erforderliche Beweise

On-behalf-of-Delegation

Hilfreich wenn: Benutzer erlaubt begrenzte Aufgabe

Einschränkung: Umfang kann über Werkzeuge driften

Vorgeschlagene Aktion: Obergrenzen und kurze Laufzeit erzwingen

Warum das zu unserer Situation passt

Vor dem Handeln erforderliche Beweise

Menschlich freigegebene Ausführung

Hilfreich wenn: Folge erfordert verantwortliches Urteil

Einschränkung: Prüfung kann symbolisch werden

Vorgeschlagene Aktion: Belege zeigen und Stoppmacht behalten

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-runtime-identity-evidence-plan/

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