

SŁOWNICZEK



SŁOWNIK AI

Proszę dopasować wyrażenie do definicji.

A -sztuczna inteligencja (AI)	B -model językowy	C - duży model językowy (LLM)
D -agent – agenty AI	E -AI agentowe	F -Uprząż (Harness)
G -Halucynacja	H -Piaskownica (Sandbox)	I -Prompt / Polecenie
J -Ucieczka z piaskownicy	K -Token	L -Pętla agenta
M -Metoda „red teaming”	N -API (Application Programming Interface)	O -Człowiek w pętli
P -Człowiek nad pętlą		

- ____ Oznacza sytuację, w której AI może działać autonomicznie, ale człowiek monitoruje jej działania i może w razie potrzeby interweniować.
- ____ Dziedzina informatyki zajmująca się tworzeniem systemów, które wykonują zadania wymagające zwykle ludzkiej inteligencji, takie jak rozumienie języka, rozpoznawanie obrazów, podejmowanie decyzji czy uczenie się.
- ____ Model działania, w którym człowiek uczestniczy w procesie decyzyjnym AI, na przykład zatwierdzając ważne działania agenta przed ich wykonaniem.
- ____ System AI wyszkolony na dużych ilościach tekstu, który potrafi analizować i generować język. Modele językowe przewidują, jakie słowa lub fragmenty tekstu powinny pojawić się w danym kontekście.
- ____ Kontrolowane testowanie systemu AI poprzez celowe próby znalezienia jego słabości, błędów lub sposobów obejścia zabezpieczeń.
- ____ Zaawansowany model językowy wytrenowany na ogromnych zbiorach danych. Może między innymi odpowiadać na pytania, streszczać teksty, tłumaczyć, pisać kod i prowadzić rozmowę.
- ____ Interfejs pozwalający jednemu programowi komunikować się z innym systemem lub usługą. Agent AI może na przykład korzystać z API banku, kalendarza albo wyszukiwarki.
- ____ System wykorzystujący model AI do samodzielnego wykonywania określonych zadań. W przeciwieństwie do zwykłego chatbota agent może planować działania, korzystać z narzędzi, wykonywać kolejne kroki i reagować na wyniki swoich działań.
- ____ Sytuacja, w której model generuje informację, która brzmi wiarygodnie, ale jest nieprawdziwa, nieprecyzyjna lub nie ma odpowiedniego oparcia w danych.
- ____ Zestaw zasad przekazywanych modelowi w celu określenia jego roli, zachowania i ograniczeń. Zwykle znajduje się na wyższym poziomie niż instrukcje użytkownika.
- ____ Podejście, w którym system AI może samodzielnie realizować zadania poprzez planowanie, podejmowanie decyzji i korzystanie z dostępnych narzędzi.
- ____ Sytuacja, w której program lub agent zdoła ominąć ograniczenia środowiska izolowanego i uzyskać dostęp do zasobów, które powinny być dla niego niedostępne.
- ____ Jednostka tekstu przetwarzana przez model językowy. Token może odpowiadać całemu słowu, części słowa, znakowi lub grupie znaków.
- ____ Odizolowane środowisko, w którym można bezpiecznie uruchamiać kod lub agenta AI. Ogranicza dostęp systemu do rzeczywistych zasobów, dzięki czemu potencjalnie niebezpieczne działanie nie powinno wpłynąć na główny system.
- ____ Powtarzający się proces, w którym agent analizuje sytuację, podejmuje decyzję, wykonuje działanie, sprawdza wynik i na tej podstawie decyduje o kolejnym kroku.
- ____ Warstwa infrastruktury i logiki zbudowana wokół modelu AI. Dostarcza modelowi narzędzia, zarządza jego działaniem, kontroluje przepływ informacji i może nakładać ograniczenia bezpieczeństwa.