CloudWarrior

PLAYBOOK · AGENCI AI DLA FIRM

Agent AI.
Robi tylko to, co ustalono.

Jak wdrażamy agenta AI do jednego procesu w firmie: z zakresem, limitami, logiem i momentem, w którym sprawę przejmuje człowiek.



01 · DLA KOGO

Asystent AI działa „czasem dobrze”.

Zespół korzysta z czatu AI albo ma już asystenta, który odpowiada klientom, sortuje zgłoszenia lub czyta dokumenty. Zwykle działa. Nikt jednak nie wie, co zrobi w nietypowej sytuacji, skąd wziął odpowiedź i do jakich danych ma dostęp.

Agent bez spisanych granic to ryzyko, które rośnie razem z jego uprawnieniami. Ten playbook opisuje, jak te granice ustawić, zanim agent dostanie prawdziwe dane.

To dla Ciebie, jeśli

- zadanie opiera się na tekście: maile, zgłoszenia, dokumenty,
- powtarza się wiele razy w tygodniu,
- wynik łatwo sprawdzić człowiekowi,
- jest osoba, która przejmie wyjątki.

To jeszcze nie ten moment, jeśli

- agent miałby podejmować decyzje bez kontroli,
- nie ma przykładowych spraw do testu,
- zasady procesu nie są nigdzie zapisane,
- chodzi o trenowanie własnego modelu.

Co dostajesz

- Agenta z jasnym zakresem: co robi i czego nigdy nie dotyka.
- Limity: do jakich systemów ma dostęp i co może zrobić bez człowieka.
- Log każdego kroku, żeby było widać, skąd wziął odpowiedź.
- Przekazanie sprawy człowiekowi w ustalonym momencie.

02 · JAK TO PRZEBIEGA

Pięć kroków od rozmowy do przekazania.

01 **Rozmowa**

Bez opłaty. Pokazujesz, gdzie dziś pracuje AI albo gdzie miałoby pracować, i przykłady spraw, w których się myli.

02 **Diagnoza**

Płatna. Spisujemy zakres agenta, jego limity, źródła danych i kryteria odbioru. Koszt zaliczamy na wdrożenie zamówione w ciągu 30 dni.

03 **Budowa**

Na Twoich kontach. Podłączamy agenta do potrzebnych systemów z najmniejszymi możliwymi uprawnieniami. Pierwsze sprawy pokazujemy na żywo.

04 **Sesja odbioru**

Na kopii danych. Sprawdzamy zwykłe sprawy, sprawy spoza zakresu i moment przekazania człowiekowi. Wynik trafia do protokołu.

05 **Przekazanie**

Konfiguracja, log i instrukcja „co robić, gdy agent się myli" trafiają do Ciebie. Opłaty za model płacisz bezpośrednio dostawcy.

Płatność: 50% przed startem, 50% po podpisanym protokole. Termin i cenę ustalamy w diagnozie.

03 · ODBIÓR

Sprawdzamy też to, czego agent ma nie robić.

Przykład dla agenta, który sortuje zgłoszenia od klientów. Dane są przykładowe.

#	KRYTERIUM	JAK SPRAWDZAMY
1	Zgłoszenie trafia do właściwej kategorii i osoby.	Zestaw przykładowych zgłoszeń.
2	Pytanie spoza zakresu trafia do człowieka, bez odpowiedzi agenta.	Celowo nietypowe zgłoszenie.
3	Agent nie ma dostępu do danych, których nie potrzebuje.	Przegląd uprawnień.
4	Każda decyzja ma wpis w logu z jej podstawą.	Odczyt logu po teście.
5	Osoba spoza projektu wyłącza agenta według instrukcji.	Próba z instrukcją w ręku.

Czego potrzebujemy od Ciebie

- Spisanych zasad: co agentowi wolno.
- Przykładowych spraw.
- Osoby, która przejmuje wyjątki.
- Jednej sesji odbioru.

Czego zakres nie obejmuje

- Trenowania własnego modelu.
- Opłat za model.
- Treści, za które odpowiada klient.

Następny krok

Zbierz trzy przykłady, w których obecny asystent się pomylił, albo opisz zadanie w dwóch zdaniach. Wstępna analiza jest bezpłatna.

Opisz zadanie: cloudwarrior.io/pl/ai