

Agentic Enterprise: gdy AI przestaje czekać na polecenie



Michał Smereczyński
Cloud Lead

Firma agentowa zaczyna od zdarzenia

Klasyczny model

Człowiek zauważa
Człowiek interpretuje
Człowiek uruchamia
proces

Model agentowy

- 1** **ZDARZENIE**
Nowy sygnał w danych lub systemie
- 2** **DECYZJA**
Agent ocenia kontekst i planuje
- 3** **DZIAŁANIE**
Narzędzie wykonuje dozwolony krok

Człowiek nie znika. Przesuwa się z wykonywania każdego kroku do definiowania celu, granic i odpowiedzialności.

Od asystenta do cyfrowego wykonawcy

1

ASYSTENT

Odpowiada i pomaga
człowiekowi

2

CYFROWY KOLEGA

Realizuje zadania
i przekazuje wynik

3

OPERATOR PROCESU

Prowadzi przebieg,
eskaluje wyjątki

81%

liderów oczekuje, że w ciągu 12–18 miesięcy agenci będą umiarkowanie lub szeroko włączeni w strategię AI ich firmy.

Największa zmiana dzieje się między krokami

WCZEŚNIEJ

Kolejka zadań

Proces czeka, aż ktoś go uruchomi.
Wiedza jest w głowach i instrukcjach.
Wyjątki wracają do skrzynki odbiorczej.

PO ZMIANIE

Przepływ zdarzeń

Zdarzenie uruchamia ocenę sytuacji.
Kontekst jest pobierany w chwili decyzji.
Człowiek dostaje tylko sprawy wymagające osądu.

Projektujemy nie odpowiedź modelu, lecz zamknięty cykl: sygnał, decyzja, działanie, obserwacja, korekta.

Autonomia jest parametrem procesu, nie przełącznikiem

Większa autonomia

1 **CZYTA** zbiera kontekst

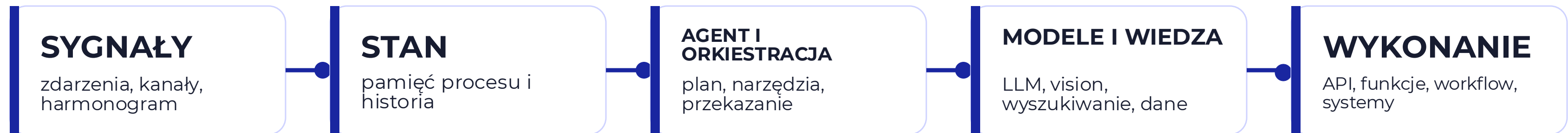
2 **REKOMENDUJE** proponuje decyzję

3 **DZIAŁA ODWRACALNIE** zapisuje szkic lub obserwację

4 **PROSI O ZGODĘ** czeka przed skutkiem biznesowym

5 **DZIAŁA W GRANICACH** wykonuje dozwolone kroki

System agentowy to więcej niż model

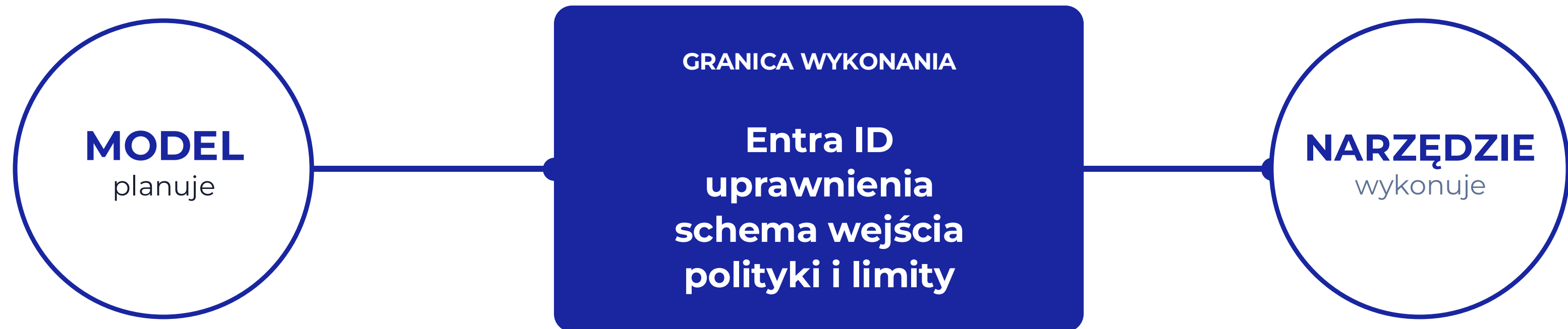


WARSTWA KONTROLI

tożsamość • polityki • telemetria • ewaluacja • limity • audyt

Na Azure składamy system z usług. Model jest jednym z elementów, nie architekturą.

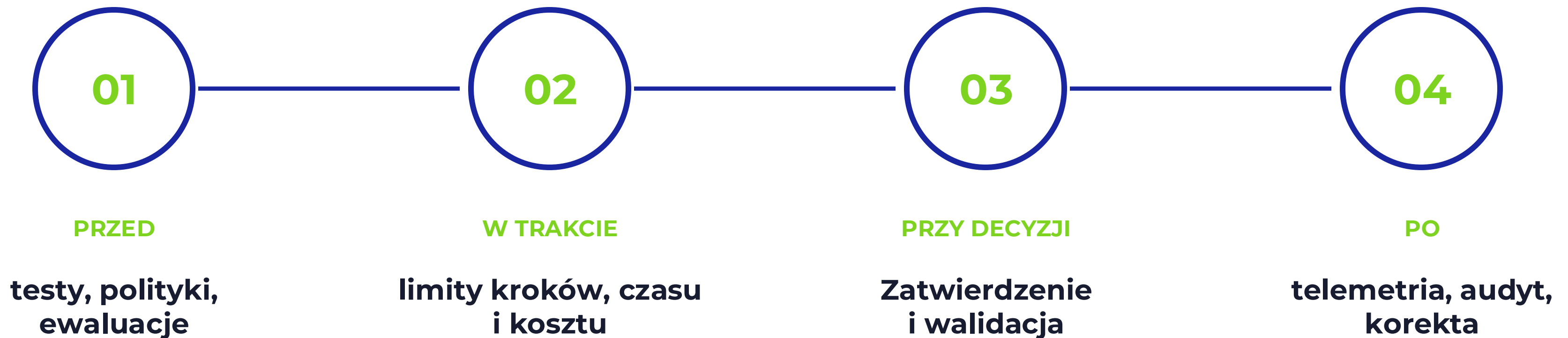
Model proponuje. Tożsamość i API decydują.



- unikalna tożsamość
- najmniejsze uprawnienia
- jawna lista narzędzi
- autoryzacja każdej akcji

Prompt opisuje intencję. Warstwa wykonawcza egzekwuje rzeczywiste granice.

Kontrolujemy przebieg, nie tylko odpowiedź



Circuit breaker • idempotencja • eskalacja do człowieka • pełny ślad decyzji

Wielu agentów tylko wtedy, gdy istnieje realna granica

JEDEN AGENT

Najprostszy start



Mało przekazania, prostszy audyt, niższy koszt.

PRZEKAZANIE

Różne kompetencje



Agent kieruje sprawę do wyspecjalizowanego wykonawcy.

MAKER-CHECKER

Wysoki koszt błędu



Jeden tworzy, drugi weryfikuje przed wykonaniem.

Zaczynaj od jednego agenta. Dziel dopiero przy granicy odpowiedzialności, kompetencji lub skali.

Dobieramy poziom kontroli do problemu

GOTOWE AGENTY	LOW-CODE	PRO-CODE / PaaS	PEŁNA KONTROLA
Microsoft 365 i Dynamics 365	Copilot Studio	Microsoft Foundry	Usługi Azure
najszybsza wartość	szybkie procesy biznesowe	agenci, modele, ewaluacje	własna architektura i runtime

Więcej gotowych mechanizmów

Więcej swobody architektonicznej

To spektrum, nie konkurs produktów. W jednej organizacji te warstwy będą współistnieć.

DEMO

Od zdjęcia do działania

Uszkodzenie drogi staje się
zdarzeniem, oceną i
kontrolowaną akcją.

1

Blob + Event Grid

nowy obraz

2

Azure ML

YOLOX wykrywa uszkodzenie

3

Model multimodalny

opisuje kontekst

4

Agent Foundry

wykonuje 3 akcje

DOZWOLONE AKCJE

zapis obserwacji
prośba o reinspekcję
pilne zgłoszenie

Cztery pytania, które zatrzymują złe wdrożenia

01 Co uruchamia agenta?

Zdarzenie musi być jawne, mierzalne i odtwarzalne.

02 Co agent może zmienić?

Granica narzędzi jest ważniejsza niż swoboda promptu.

03 Kiedy wchodzi człowiek?

Próg zależy od ryzyka, kosztu błędu i odwracalności.

04 Jak udowodnimy, co się stało?

Potrzebujemy tożsamości, telemetryki, audytu i ewaluacji.

Agentic Enterprise zaczyna się tam, gdzie autonomia ma granice, właściciela i ślad audytowy.



Dziękuję

Netwise S.A.

8 Szamocka St.
01-748 Warsaw,
Poland

+48 (22) 3797170

www.netwiseglobal.com

Netwise USA, Inc.

301 Yamato Rd.
Boca Raton,
FL 33431

(800) 994-8224