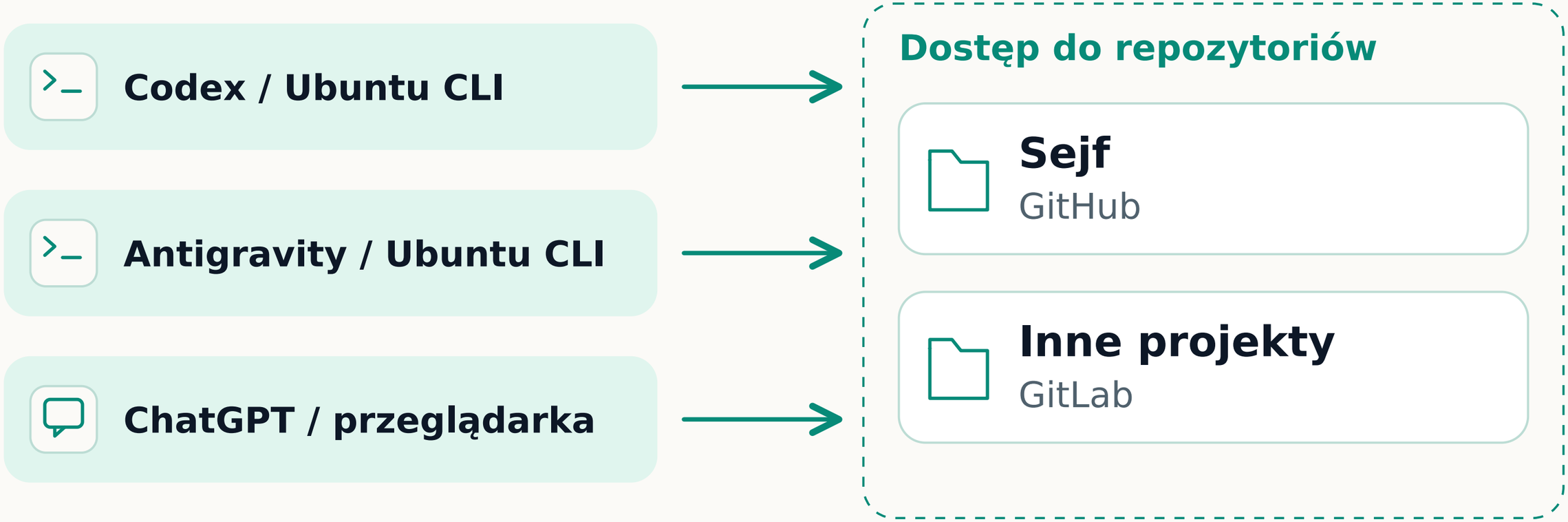
Mój warsztat pracy

Wspólny kontekst zapisujemy w plikach



Dostęp zależy od narzędzia i uprawnień

Sejf: wiedza, do której można wrócić

Obsidian
Edytuj notatki

→

Markdown + OKF
Porządkuj wiedzę

→

Git
Porównuj wersje

Wybrane pola pliku prompt_injection.md

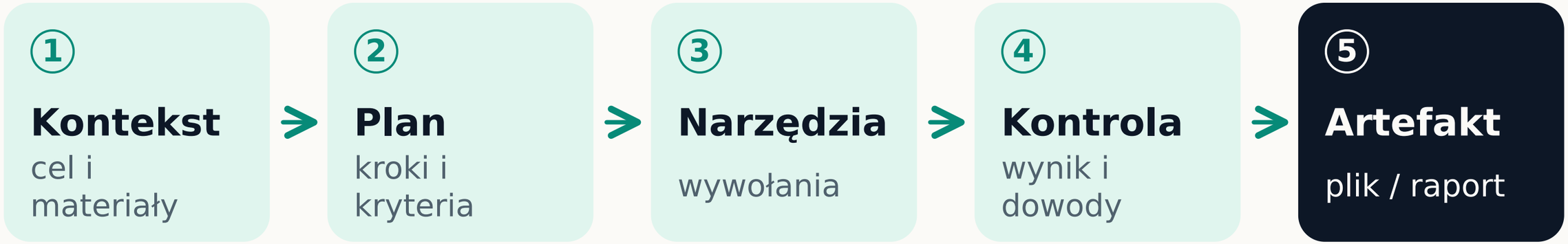
```
---
type: Concept
timestamp: 2026-11-15T00:00:00Z
---

# Iniekcja promptu (prompt injection) i jailbreak
```

O dostępie decyduje człowiek

Jedna sesja, wiele kroków

Schemat przebiegu pracy



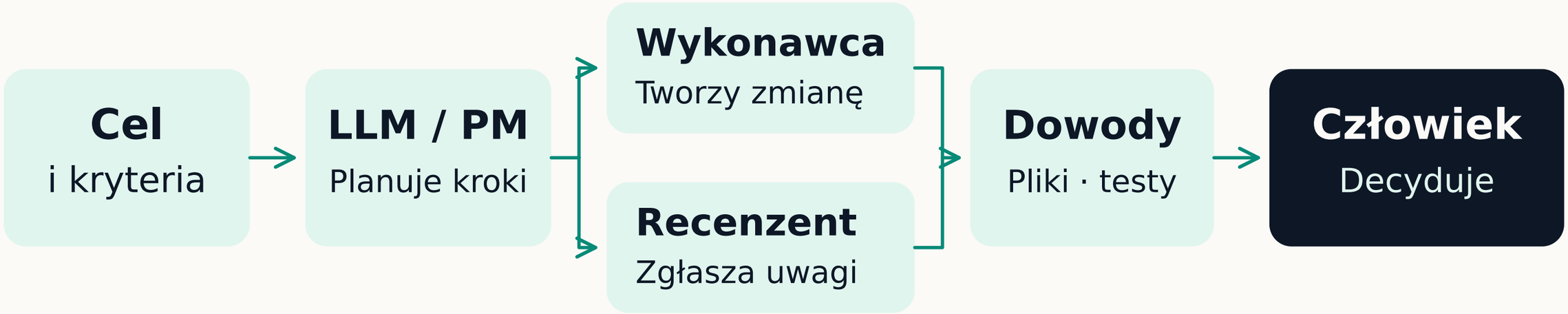
Wywołanie narzędzia może się nie udać

Sprawdź wynik / zapisz ograniczenie

Uruchomienie to jeszcze nie wynik

AI NINJAS #20 · WARSZTAT

LLM jako PM



ŚLAD ZADANIA

Zgłoszenie → gałąź → zmiana → PR/MR → akceptacja

Plan przekładamy na sprawdzalny rezultat

Generator, krytyk, weryfikator

01

Generator

Tworzy propozycję

Przedstawia warianty

02

Krytyk

Szuka błędów i luk

Stawia mocne zarzuty

03

Weryfikator

Sprawdza twierdzenia

Test · źródło · obliczenie

Zgodność modeli nie zastępuje dowodu

Co działa, co trzeba potwierdzić

Dostępne artefakty

- ✓ Notatki i źródła
- ✓ Repozytoria i historia
- ✓ Zgłoszenia i PR
- ✓ Wyniki kontroli

Do potwierdzenia

- ○ Stała praca w tle
- ○ Skuteczna delegacja
- ○ Aktualny stan runtime

Schemat procesu, nie telemetria systemu

Człowiek określa cel, dostęp i akceptuje skutki