Fale wdrożenia - właściwa kolejność

1. Fale

Fala	Czas	Zakres	Owner	Kryterium przejścia
Fala 0 - Freeze, zachowanie linków i inwentaryzacja	0-1 dzień	Nie nadpisywać /ai-truth; utworzyć nowy root /Common-Source-of-Truth/start; zrobić indeks starych linków i materiałów źródłowych.	Operator + Dev	Redirecty nie wymuszone; /ai-truth pozostaje archiwum/praca wcześniejsza.
Fala 1 - Pakiet P0 do wysłania rano	1 dzień	Landing, CST core, PPP P0, Dev/Security, Dokumenty, Formularze kontaktowe, mapa modułów.	Content + Dev	Można wysłać partnerom bez paneli operacyjnych.
Fala 2 - Intake + Evidence + Legal Trigger	2-3 dni	Formularze, statusy, rejestr claimów, evidence graph, regulatory trigger engine, export PDF/CSV.	Dev + Legal + Security	Każde zgłoszenie ma ID, status, ownera i ślad dowodowy.
Fala 3 - Dev MVP i data model	3-7 dni	JSON schema, API endpoints, storage, RBAC, audit log, seed data, status.json, health endpoints.	Dev	MVP działa lokalnie/staging; brak ukrytej autonomii agentów.
Fala 4 - Dashboardy i playbooki P1	1-2 tygodnie	Incident Board, Evidence Board, Legal Live Board, PPP Board, playbooki phishing/ransomware/AI incident/data leak.	DevSecOps + Ops	Działają pierwsze widoki i procedury.
Fala 5 - Agent services i automatyzacje kontrolowane	2-4 tygodnie	WATCH/IDENT/PROOF w trybie read-only/analitycznym; Agent Action Inventory; kill switch; human approval.	Agent Ops + Security	Zero działań aktywnych bez zgody operatora.
Fala 6 - Skalowanie PPP / GO CONTROLLED	4+ tygodnie	Materiały dla instytucji, prezentacja, pilotaż P0/P1, model finansowania, raport skuteczności.	Strategy + Legal + Dev	Decyzja: zakończyć / rozszerzyć / pełne partnerstwo.

2. Co robić teraz

Najpierw: opublikować statyczny P0 i pakiet dokumentów.

Nie najpierw: dashboardy, aktywne agenty, automatyczne monitorowanie BigTech, przypisywanie odpowiedzialności.

3. Fala 0 - checklist

- [ ] Nie kasować /ai-truth.
- [ ] Utworzyć /Common-Source-of-Truth/start.
- [ ] Zrobić mapę wcześniejszych linków.
- [ ] Ustalić statusy DRAFT/P0/P1/P2/LIVE.
- [ ] Dodać informację: materiał strategiczny, nie porada prawna.
- [ ] Oznaczyć symulacje i realne zdarzenia jako różne klasy.

4. Fala 1 - P0 publikacyjny

- [ ] Landing.
- [ ] Common Source of Truth.
- [ ] Regulatory Trigger Engine.
- [ ] Incident/report intake.
- [ ] Evidence Graph opisowy.
- [ ] PPP P0 offer.
- [ ] Dev/Security rules.
- [ ] Documents index.

5. Fala 2 - rejestry i dowody

- [ ] Claims registry.
- [ ] Sources registry.
- [ ] Evidence registry.
- [ ] Incidents registry.
- [ ] Legal triggers.
- [ ] Disputes/appeals.
- [ ] Export PDF/CSV/JSON.

6. Fala 3 - techniczny MVP

- [ ] API.
- [ ] JSON schemas.
- [ ] RBAC.
- [ ] Audit log.
- [ ] status.json.
- [ ] /health.
- [ ] backup.
- [ ] deployment checklist.

7. Fala 4 - operacyjna

- [ ] Incident Board.
- [ ] Evidence Board.
- [ ] Legal Live Board.
- [ ] PPP Board.
- [ ] Human Risk Board.
- [ ] Playbooki.
- [ ] Szkolenia L0-L2.

8. Fala 5 - agentowa

- [ ] Agent Action Inventory.
- [ ] WATCH read-only.
- [ ] IDENT analytical.
- [ ] PROOF evidence packaging.
- [ ] Brak SHIELD/REPAIR/JUSTICE bez zgody i podstaw.
- [ ] Operator veto.
- [ ] Kill switch.

9. Fala 6 - partnerstwo i skalowanie

- [ ] Pakiet P0 dla instytucji.
- [ ] Raport skuteczności.
- [ ] Model finansowania.
- [ ] List intencyjny.
- [ ] Pilotaż GO CONTROLLED.
- [ ] Decyzja o P2/P3.