

10 - DEV SOC OPERATOR EXECUTION

Cel techniczny

Zbudować system, który umożliwi podmiotowi publicznemu wykrywanie incydentów, klasyfikowanie incydentów, zabezpieczanie dowodów, monitorowanie BigTech, raportowanie do kierownictwa i organów, wdrażanie zabezpieczeń, dokumentowanie szkód, szkolenie operatorów, rozwijanie własnych narzędzi i skalowanie rozwiązania na kolejne jednostki.

Pozycja w architekturze CST

```
/Common-Source-of-Truth/dev  
/Common-Source-of-Truth/soc-operator  
/Common-Source-of-Truth/api  
/Common-Source-of-Truth/reports
```

Moduły MVP

Moduł	Funkcja	Priorytet
K0-INCIDENT	rejestr incydentów	P0
K0-PROOF	dowody, hashe, chain of custody	P0
K0-DASH	panel centralny	P0
K0-WATCH	monitoring źródeł	P0
K0-PLAYBOOK	procedury reakcji	P1
K0-REPORT	raporty	P1
K0-BIGTECH	mapa zależności BigTech	P1
K0-AI-GOV	rejestr systemów AI	P1
K0-TRAIN	szkolenia	P2
K0-SHIELD	mechanizmy obronne	P2
K0-JUSTICE	szkody i organy	P2
K0-EU-STACK	własne technologie UE	P3

Minimalny przepływ danych

```
SOURCE  
CERT / logi / formularz / OSINT / operator / system AI  
-> INTAKE  
normalizacja, deduplikacja, priorytet  
-> CLASSIFY  
typ, sektor, miejsce, aktywo, sprawca A0-A5  
-> PROOF  
dowód, hash, status: CONFIRMED/GAP/DISPUTED  
-> RESPONSE  
playbook, zadania, właściciel  
-> REPORT  
raport kierowniczy, techniczny, prawny  
-> MONITOR  
trend, skuteczność, ryzyko resztkowe
```

Tabele danych MVP

public_private_projects

Pole	Opis
project_id	ID projektu
public_entity	podmiot publiczny
private_partner	KONSULT / partnerzy
model	P0 / pilot / PPP / serwis / konsorcjum

Pole	Opis
scope	zakres
status	proposed / P0 / pilot / active / closed
legal_basis	PPP / umowa / MoU / grant / inne
risk_split	podział ryzyk
funding_model	bezpłatny / abonament / grant / PPP
next_decision	kolejna decyzja

bigtech_dependencies

Pole	Opis
dependency_id	ID zależności
vendor	dostawca
service	usługa
category	chmura / AI / poczta / komunikacja / reklama / repo / IAM
criticality	low / medium / high / critical
data_type	public/internal/personal/sensitive
jurisdiction	EU / non-EU / unknown
lock_in_score	0-100
alternative_eu	yes/no/partial
migration_priority	P0/P1/P2/P3
recommendation	maintain / secure / replace / build own

deployment_actions

Pole	Opis
action_id	ID działania
project_id	projekt
phase	CONF / SYNC / CONNECT / EXECUTE / REPORT / MONITOR
title	nazwa
owner	właściciel
priority	P0/P1/P2/P3
status	open / in progress / done / verified
evidence_id	dowód wykonania
due_date	termin
risk	ryzyko

Endpointy MVP

```

POST /api/ppp/projects
GET /api/ppp/projects
GET /api/ppp/projects/:id
POST /api/deployment/actions
PATCH /api/deployment/actions/:id
GET /api/deployment/actions?project_id=
POST /api/bigtech/dependencies
GET /api/bigtech/dependencies
PATCH /api/bigtech/dependencies/:id
POST /api/incidents
GET /api/incidents
POST /api/incidents/:id/evidence
GET /api/reports/p0/:project_id
GET /api/reports/pilot/:project_id
GET /api/reports/bigtech/:project_id
GET /api/reports/board/:project_id

```

Widoki panelu

Widok	Zakres
Decyzyjny	status projektu, etap, ryzyka, incydenty, BigTech, decyzja
Techniczny	integracje, logi, incydenty, podatności, aktywa, działania naprawcze
Prawny	AI Act, NIS2/KSC, RODO, PPP, zgody, raporty, terminy
BigTech	dostawcy, krytyczność, dane, lock-in, alternatywa UE
Skalowania	gotowe moduły, jednostki do wdrożenia, koszty, ryzyka, harmonogram

Roadmapa sprintów

Sprint	Zakres
Sprint 0	szablon P0, checklisty, raport P0, prezentacja, zgoda na zakres
Sprint 1	projekty PPP, statusy, role, podział ryzyk, finansowanie
Sprint 2	incydenty, dowody, statusy dowodowe, eksport PDF/CSV, dashboard
Sprint 3	BigTech Dependency Map, lock-in, dane, alternatywy UE
Sprint 4	CONF/SYNC/CONNECT/EXECUTE/REPORT/MONITOR, playbooki, dashboard
Sprint 5	EU Tech Stack, priorytety rozwoju, koszty, granty/PPP

Zasada końcowa dla dev

System nie ma być tylko CRM-em do incydentów. Ma być operacyjnym mechanizmem odporności państwa:

ANALIZA -> KONFIGURACJA -> SYNCHRONIZACJA -> POŁĄCZENIE -> WYKONANIE -> RAPORT -> MONITORING -> SKALOWANIE -> SUWERENNOŚĆ TECHNOLOGICZNA