11 - BIGTECH DEPENDENCY I EU TECH STACK

Cel dokumentu

Ten dokument porządkuje dwa powiązane filary: monitoring zależności od BigTech oraz budowę własnego, audytowalnego i suwerennego stosu technologicznego UE.

Pozycja w architekturze CST

/Common-Source-of-Truth/bigtech
/Common-Source-of-Truth/bigtech/dependency-map
/Common-Source-of-Truth/eu-tech-stack
/Common-Source-of-Truth/eu-tech-stack/roadmap

Cel monitoringu BigTech

Monitoring BigTech ma ustalić, od jakich dostawców zależy jednostka publiczna, gdzie znajdują się dane, jakie usługi są krytyczne, jakie są ryzyka lock-in, jakie są ryzyka prawne i operacyjne, czy istnieje alternatywa UE oraz które systemy można przenieść, zreplikować lub uniezależnić.

Tabela zależności BigTech

Pole	Opis
Dostawca	Microsoft, Google, Amazon, Meta, Apple, OpenAI, Oracle itd.
Usługa	chmura, poczta, AI, reklama, komunikacja, repozytorium
Krytyczność	niska / średnia / wysoka / krytyczna
Dane	publiczne / wewnętrzne / osobowe / wrażliwe
Lokalizacja danych	UE / poza UE / nieustalone
Ryzyko lock-in	niskie / średnie / wysokie
Alternatywa UE	tak / nie / częściowo
Koszt migracji	niski / średni / wysoki
Priorytet zmiany	P0 / P1 / P2 / P3
Rekomendacja	utrzymać / zabezpieczyć / zastąpić / zbudować własne

Kategorie monitoringu BigTech

Kategoria	Ryzyko	Działanie
Chmura	lock-in, dane, jurysdykcja	multi-cloud, sovereign cloud, backup
AI	zależność od modeli zewnętrznych	własne modele, routing, kontrola danych
Poczta	phishing, zależność operacyjna	DMARC, backup, alternatywa
Komunikatory	prywatność, ciągłość	komunikacja szyfrowana, własny kanał
Reklama/social	manipulacja, deepfake	monitoring, takedown, provenance
Repozytoria	supply chain	mirror, SBOM, podpisy
Systemy mobilne	zależność OS	polityka MDM, alternatywy
Identyfikacja	konta zewnętrzne	własne IAM, SSO, passkeys

Kierunki własnych technologii UE

K0NSULT powinien proponować budowę albo integrację własnych europejskich rozwiązań: komunikacja, OS, soft do monitoringu i incident response, hardware/certyfikowane urządzenia, lokalne AI i roje agentowe, sovereign cloud, tożsamość cyfrowa, evidence layer, system zgłoszeń, certyfikacja zdarzeń, repozytorium danych i modeli oraz narzędzia cyberobrony.

Matryca własnych technologii

Obszar	Rozwiązanie własne	Cel
Komunikacja	K0-COMM	bezpieczna komunikacja publiczna i kryzysowa
AI	K0-AI	własne modele, routing, agenci
OS	K0-OS	bezpieczne środowisko pracy
Cyber	K0-SHIELD	defensywa, detekcja, reagowanie
Dowody	K0-PROOF	certyfikacja zdarzeń i dowodów
Dane	K0-DATA	suwerenna warstwa danych
Tożsamość	K0-ID	identyfikacja osób, systemów, agentów
Monitoring	K0-WATCH	monitoring incydentów i BigTech
Szkolenia	K0-ACADEMY	operatorzy, obserwatorzy, kontrolerzy
Raporty	K0-REPORT	raporty regulacyjne i decyzyjne
Hardware	K0-NODE	certyfikowane węzły bezpieczeństwa
Backup	K0-ZERO	Punkt Zero, restore, odporność

Rekomendacja priorytetu

1. Najpierw mapować zależności, nie migrować chaotycznie. 2. Oceniać krytyczność i typ danych. 3. Tworzyć kopie bezpieczeństwa i alternatywne kanały komunikacji. 4. Własne komponenty rozwijać od warstwy dowodowej, raportowej i monitorującej. 5. Dopiero później planować pełne przejście na własne AI, komunikację i infrastrukturę.