SHADOW AI NA HALI PRODUKCYJNEJ · REPORTAŻ Z TRZECIEJ ZMIANY

Jest 2:40, trzecia zmiana, linia stoi. Właśnie wtedy Twoja fabryka zaczyna uczyć cudzą AI.

Twój najlepszy inżynier właśnie oddał kawałek fabryki obcemu modelowi. Nie ze złej woli, tylko z braku lepszego narzędzia. Za tę noc zapłacą cztery osoby w Twojej firmie, każda inną walutą. A branża dalej udaje, że to problem działu IT.

Daniel Stram i Jakub Duda
Head of Sales i CTO co.brick AI · 25 minut czytania

01

Noc, w której nikt nie zrobił nic złego

Marek ma trzydzieści osiem lat i dwanaście lat w utrzymaniu ruchu. Na hali mówią o nim, że „zawsze coś wymyśli". Jest wtorek, 2:40 nad ranem. Linia trzecia stanęła na serwonapędzie z kodem F-27. Nikt na zmianie nie widział tego kodu od dwóch lat. Dyżurny z IT odbierze najwcześniej o siódmej. Serwis producenta pracuje w dni robocze. Na hali stoi czterech operatorów, a każda godzina przestoju kosztuje więcej, niż Marek zarabia w miesiącu.

78%

używających AI w pracy przynosi własne narzędzia

MICROSOFT WTI · n = 31 000

89%

użycia AI w firmach jest niewidoczne dla zespołów bezpieczeństwa

LAYERX · 2025

8,2 GB

miesięcznie wypływa do nieautoryzowanych AI z jednej organizacji

NETSKOPE · 2026

43%

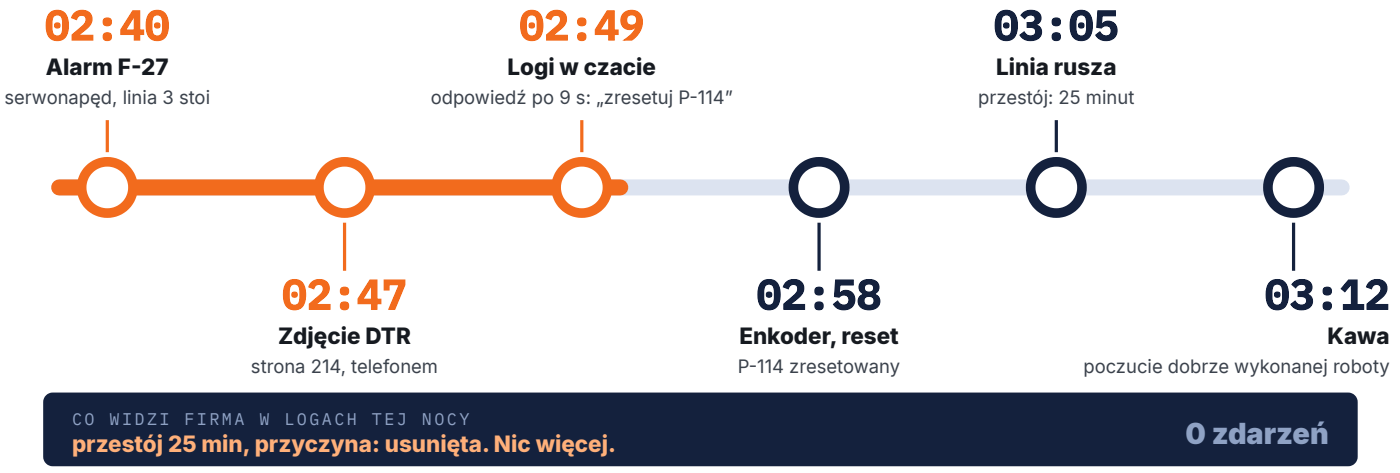
organizacji po naruszeniu miało incydent z shadow AI. Rok wcześniej: 20%

IBM / PONEMON 2026 · n = 602

Marek robi to, co zrobiłby każdy dobry inżynier w 2026 roku. Wyciąga telefon. Fotografuje stronę dokumentacji techniczno-ruchowej, czyli „DTR", z tabelą kodów błędów. Wkleja ostatnie sto linii logu ze sterownika. Pisze do darmowego asystenta AI: „linia stoi, kod F-27, co sprawdzić najpierw". Asystent odpowiada w dziewięć sekund. Uprzejmie, konkretnie, z numerowaną listą. Enkoder, parametr P-114, reset. O 3:05 linia rusza. O 3:12 Marek idzie na kawę z poczuciem, że uratował zmianę. Bo uratował.

Nikt tej nocy nie zrobił nic złego. I właśnie dlatego ta historia jest groźna. Bo w tym samym czasie, w którym linia wracała do rytmu, z Twojej fabryki wyszło coś, czego nie da się już zawrócić.

OŚ CZASU JEDNEJ NOCNEJ ZMIANY



Darmowy czat nie jest narzędziem. Jest kanałem. Po drugiej stronie stoi model, którego regulamin mówi, że może uczyć się na tym, co wkleisz.

CO OPUŚCIŁO ZAKŁAD MIĘDZY 2:47 A 2:49?

```
// upload 1 · zdjęcie, 3,1 MB
DTR_serwonapęd_linia3.pdf, s. 214
→ tabela kodów błędów producenta
→ nastawy fabryczne P-100…P-140
→ numer seryjny, wersja firmware

// upload 2 · tekst, 100 linii
02:38:41 AXIS3 ERR F-27
02:38:41 TEMP 71.4 LOAD 96%
02:38:40 RECIPE_ID 4471-B
02:38:40 ORDER 88213 / KLIENT_A
…
// konto: prywatne · logi firmowe: brak
```

Numer receptury i identyfikator klienta w logu to nie wymysł: w telemetrii Harmonic Security co szósta ekspozycja danych wrażliwych szła przez darmowe konto prywatne, do którego firma nie ma żadnego wglądu. Ani ograniczonego. Żadnego.

Sztuczna inteligencja, czyli „AI", weszła do Twojej fabryki nie przez dział zakupów, tylko przez kieszeń Marka. Bez przetargu, bez oceny ryzyka, bez podpisu prezesa. Literatura nazywa to „shadow AI", czyli AI w cieniu: użycie narzędzi AI do zadań służbowych bez autoryzacji firmy i z pominięciem oceny ryzyka[2]. Cloud Security Alliance, czyli „CSA", organizacja zajmująca się bezpieczeństwem chmury, ujmuje różnicę między tym a starym „shadow IT" w trzech słowach: systemy AI „learn, remember, and act". Uczą się, pamiętają, działają[1]. Dropbox przechowywał plik. Model językowy plik czyta, streszcza, zapamiętuje w kontekście rozmowy i czasem trenuje na nim kolejną wersję siebie.

Jest w tym też dobra wiadomość, o której rzadko się mówi. Twoi ludzie już przeprowadzili pilotaż AI: bez budżetu, bez kryteriów sukcesu i bez logów. Wiesz więc, że AI im pomaga, bo inaczej by po nią nie sięgali. Nie wiesz tylko, co przy okazji wyszło z firmy. Dlatego wdrożenie firmowej AI zamienia ryzyko niewidoczne na takie, którym można zarządzać.

> **Twoi ludzie już przeprowadzili pilotaż AI: bez budżetu, bez kryteriów sukcesu i bez logów. Nie wiesz tylko, co przy okazji wyszło z firmy.**

Problem jest już w Twojej firmie. Australijska agencja badawcza CSIRO przepytała 27 operatorów infrastruktury krytycznej: 26 z nich miało obserwowalne shadow AI[4]. Jedyny wyjątek to organizacja, która zablokowała wszystko na samym początku i, jak zobaczysz dalej, prawdopodobnie tylko przestała to widzieć. Ty jeszcze o tym nie wiesz. Ale Marek wie. I nic Ci nie powie, bo według KPMG na polskiej próbie 1 082 osób ponad połowa używających AI nie ujawnia tego i prezentuje wyniki jako własne[15].

02

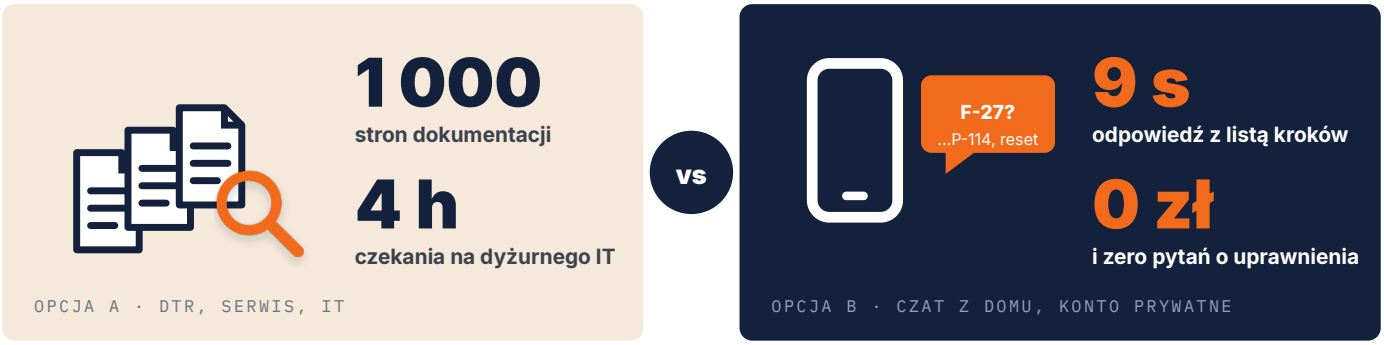
Anatomia błędu. Dlaczego Marek to zrobił?

Zanim sięgniesz po regulamin, wejdź na chwilę w buty Marka. Jeśli Twoja pierwsza myśl to „naruszenie dyscypliny", właśnie popełniasz drugi błąd tej nocy. Ten będzie droższy niż pierwszy.

Zastanówmy się razem. Marek miał do wyboru: czekać cztery godziny na IT, dzwonić do serwisu, który nie odbierze, albo zapytać narzędzie, które zna z domu, bo w nim planuje wakacje i sprawdza dzieciom wypracowania. Według PagerDuty 89 procent pracowników najpierw odkryło narzędzie AI prywatnie, a dopiero potem przyniosło je do pracy[6]. Nie dostali go od firmy. Przynieśli własne, jak śrubokręt, który lepiej leży w ręce niż ten z magazynu.

Marek nie jest sabotażystą. Badacze z International Journal of Computer Applications nazywają takich ludzi „constructive-intent threat", czyli zagrożeniem o konstruktywnych intencjach: pracownik chce dobrze i właśnie dlatego eksponuje dane[21]. Badanie 357 szwedzkich lekarzy dochodzi do tego samego z drugiej strony: nieautoryzowane użycie AI to sygnał niezaspokojonych potrzeb zawodowych, nie akt nielojalności[3]. Lekarz pyta czat o diagnozę, bo chce pomóc pacjentowi. Mechanik wkleja kod błędu, bo linia stoi. Obaj biorą na siebie ryzyko, którego nie rozumieją, w imię celu, który rozumieją doskonale.

WYBÓR MARKA O 2:40



Wybór Marka o 2:40: tysiąc stron dokumentacji z lupą albo narzędzie, które czyta log w dziewięć sekund. Problem nie polega na tym, że wybrał drugie. Problem polega na tym, że drugie nie było Wasze.

CO MÓWIĄ PRACOWNICY UŻYWAJĄCY AI W PRACY?

PagerDuty / Wakefield 2026, n = 1 250 · ostatni słupek: Microsoft UK 2025, cyt. za Axis Intelligence

Spójrz na te liczby jeszcze raz, bo mówią coś niewygodnego o Tobie, nie o Marku. 81 procent pracowników uważa, że kierownictwo działa według innych zasad. 39 procent wolałoby używać AI, nie mówiąc o tym nikomu; w dużych firmach blisko połowa[6]. Sharp Europe dodaje, że 44 procent menedżerów w Europie używa AI potajemnie, żeby wyglądać na bardziej kompetentnych[22]. Marek widzi, jak zachowują się jego szefowie, i wyciąga wnioski.

Jest jeszcze mechanizm, który badacze ze Szwecji nazwali paradoksem rozkładu ryzyka i korzyści. Korzyść jest natychmiastowa i osobista: linia rusza, Marek jest bohaterem zmiany. Ryzyko jest odroczone i organizacyjne: wyciek receptury zaboli za pół roku, kogoś innego, w innym dziale. Żaden człowiek nie wygrywa z taką asymetrią o 2:40 nad ranem. Respondent z badania CSIRO ujął to w zdaniu, które warto zapamiętać: „if you don't give them the tools, they'll find a way to get the tools". Jeśli nie dasz im narzędzi, sami znajdą sposób, żeby je zdobyć[4].

> **Jeśli nie dasz im narzędzi, sami znajdą sposób, żeby je zdobyć.**

PARADOKS, Z KTÓRYM NIKT NIE WYGRYWA O 2:40

Petersson i in., JMIR 2026: shadow AI to „professional governance problem rather than merely a technical one".

To zmienia optykę. Shadow AI nie jest naruszeniem dyscypliny. Jest sygnałem, że w Twojej infrastrukturze brakuje czegoś, co Marek musiał sobie dorobić sam. Ludzie tacy jak on to najambitniejsi „hakerzy efektywności" w firmie. Zamiast ich karać, warto ich znaleźć. Ale najpierw rachunek.

03

Kaskada ryzyka. Kto za to zapłaci?

Cztery osoby zapłacą za tę noc. Każda inną walutą i z opóźnieniem. Rachunek przyjdzie, gdy nikt nie będzie już pamiętał faktury.

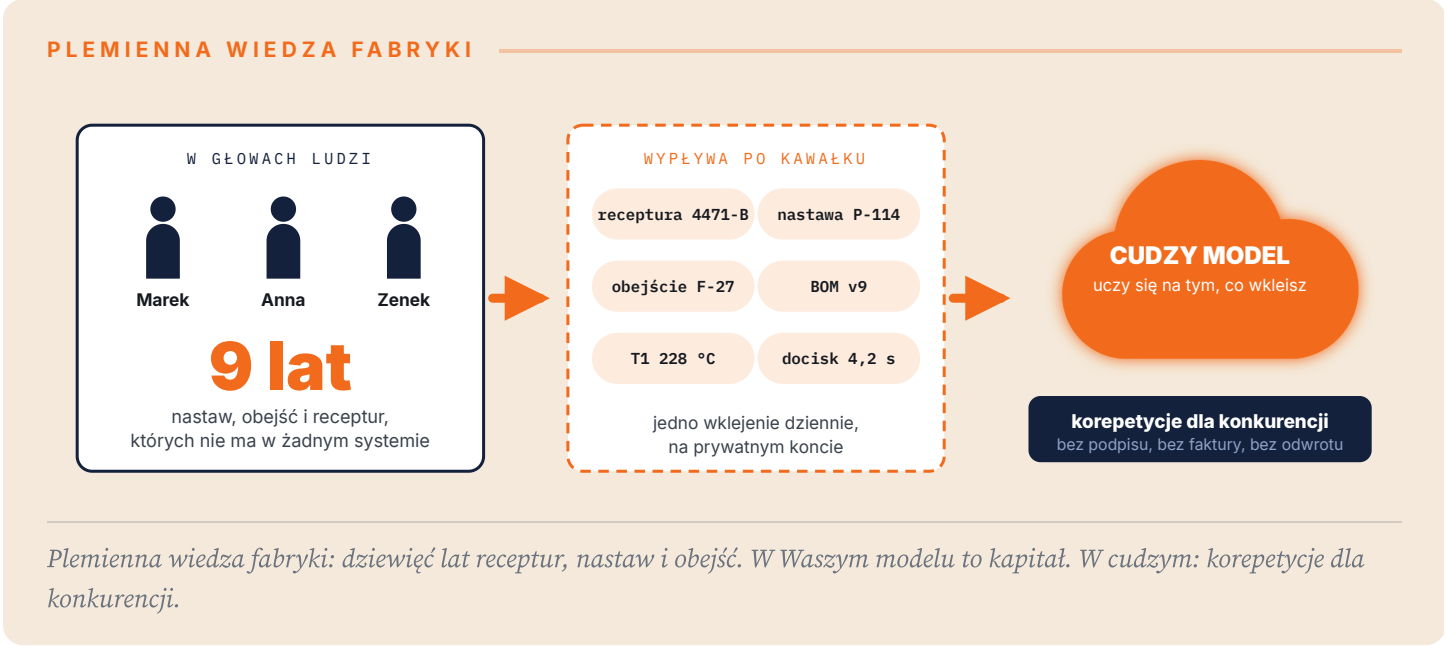
CEO

Wyciek DNA firmy

WŁAŚCICIEL · PREZES

przewaga konkurencyjna
własność intelektualna
wycena spółki

Wróćmy do logu Marka. Był w nim numer receptury 4471-B. Tydzień później technolog Anna, chcąc skrócić cykl na wtryskarce, wkleiła do tego samego darmowego czatu pełną kartę procesu: temperatury stref, czasy docisku, materiał, dostawcę granulatu i tolerancje. Poprosiła o optymalizację. Dostała dobrą odpowiedź. A model dostał coś znacznie cenniejszego: Waszą recepturę, którą doskonaliliście przez dziewięć lat.



Plemienna wiedza fabryki: dziewięć lat receptur, nastaw i obejść. W Waszym modelu to kapitał. W cudzym: korepetycje dla konkurencji.

Darmowe konta większości czatów domyślnie pozwalają dostawcy uczyć kolejne modele na wprowadzanych treściach. To nie jest teoria spiskowa, to jest regulamin, którego nikt nie czyta. Wprowadzenie autorskich procedur optymalizacyjnych do publicznego AI to darmowe korepetycje dla Waszej konkurencji. Jeśli oddajesz modelowi swój unikalny proces, tracisz jedyną przewagę, której nie da się kupić na targach. IBM podaje, że 40 procent naruszeń z udziałem shadow AI obejmuje kradzież własności intelektualnej, a rekord IP jest najdroższym typem rekordu w całym raporcie: 178 dolarów za sztukę[8]. W telemetrii Harmonic Security kod źródłowy i algorytmy stanowiły 30 procent eksponowanej treści, dokumenty prawne i M&A 38 procent[7]. Nie e-maile. Nie notatki ze spotkań. Rzeczy, które stanowią wartość firmy.

Nie jest to scenariusz teoretyczny. W 2023 roku inżynierowie działu półprzewodników Samsunga w ciągu niespełna trzech tygodni trzykrotnie wkleili do ChatGPT poufne materiały, w tym kod źródłowy i notatki ze spotkania. Firma odpowiedziała zakazem narzędzi generatywnej AI na urządzeniach służbowych[27]. Jeśli ten problem dotknął jednego z największych producentów elektroniki na świecie, to nie jest problem „małych firm bez działu IT".

DARMOWE KOREPETYCJE DLA KONKURENCJI

Mechanizm uproszczony: dane wpływają na model statystycznie, nie jako kopia. Ryzyko biznesowe jest jednak realne i nie da się go cofnąć.

TWÓJ NAVIER-STOKES

8 września 2026 OpenAI ogłosiło, że jego wewnętrzny system rozwiązał problem Naviera-Stokesa, jedną z największych nierozwiązanych zagadek matematyki. Kilkanaście godzin wcześniej Tristan Buckmaster z Uniwersytetu Nowojorskiego opublikował oświadczenie: razem z Leventem Alpöge od roku pracowali nad tym samym kierunkiem, korzystając między innymi z narzędzi OpenAI, i obawiali się, że informacja o ich postępach trafiła do firmy. OpenAI w oświadczeniu z 8 września 2026 napisało, że „choć to mało prawdopodobne, nie może wykluczyć", że zanonimizowane dane z korzystania z jego produktów pomogły ulepszyć modele. W aktualizacji tego oświadczenia z 10 września OpenAI zadeklarowało, że zapytania matematyków nie mogły wpłynąć na wynik. Spór ma też tło rywalizacji, bo Alpöge pracuje w konkurencyjnej firmie Anthropic. Nie rozstrzygamy, kto ma rację[28,29,30].

Dla fabryki ważne są trzy rzeczy. Po pierwsze, jedni z najlepszych matematyków na świecie nie mieli jak sprawdzić, co stało się z tym, co wpisali, bo zapis istniał tylko u dostawcy. Po drugie, sam dostawca w pierwszym oświadczeniu nie mógł wykluczyć, że dane z korzystania z jego produktów pomogły ulepszyć modele. Nie wiemy, z jakich kont korzystali. Wiemy, że w kontach konsumenckich trenowanie na wpisywanych treściach jest u części dostawców, w tym OpenAI, domyślnie włączone, dopóki użytkownik go nie wyłączy. Biznesowe API, z którego korzysta co.brick, działa inaczej: na umowie, bez trenowania na danych klienta i z rezydencją danych w UE. Po trzecie, prezes OpenAI Sam Altman przyznał w rozmowie z Axios (8 września 2026), że firma uruchomiła wysiłek wart miliony dolarów po pogłoskach, że konkurencja jest blisko rozwiązania[30].

Receptura, nastawy regulatorów, program sterownika czy sposób na awarię wypracowany przez dwadzieścia lat to Wasz Navier-Stokes. Pytanie nie brzmi, czy ktoś go ukradnie. Pytanie brzmi: czy w razie sporu będziecie mieć dowód?

Jest jeszcze coś, o czym prezes powinien wiedzieć, zanim usłyszy to od rady nadzorczej. 7 maja 2026 amerykański CB Financial złożył do Komisji Papierów Wartościowych i Giełd (SEC) raport 8-K, którego przyczyną było shadow AI[23]. To znaczy, że shadow AI może stać się zdarzeniem, które trzeba ujawnić inwestorom. Nie jest problemem informatycznym. Jest cichą kradzieżą własności intelektualnej, którą firma sama sobie organizuje, po jednym fragmencie dziennie.

CFO

Ukryta bomba w bilansie

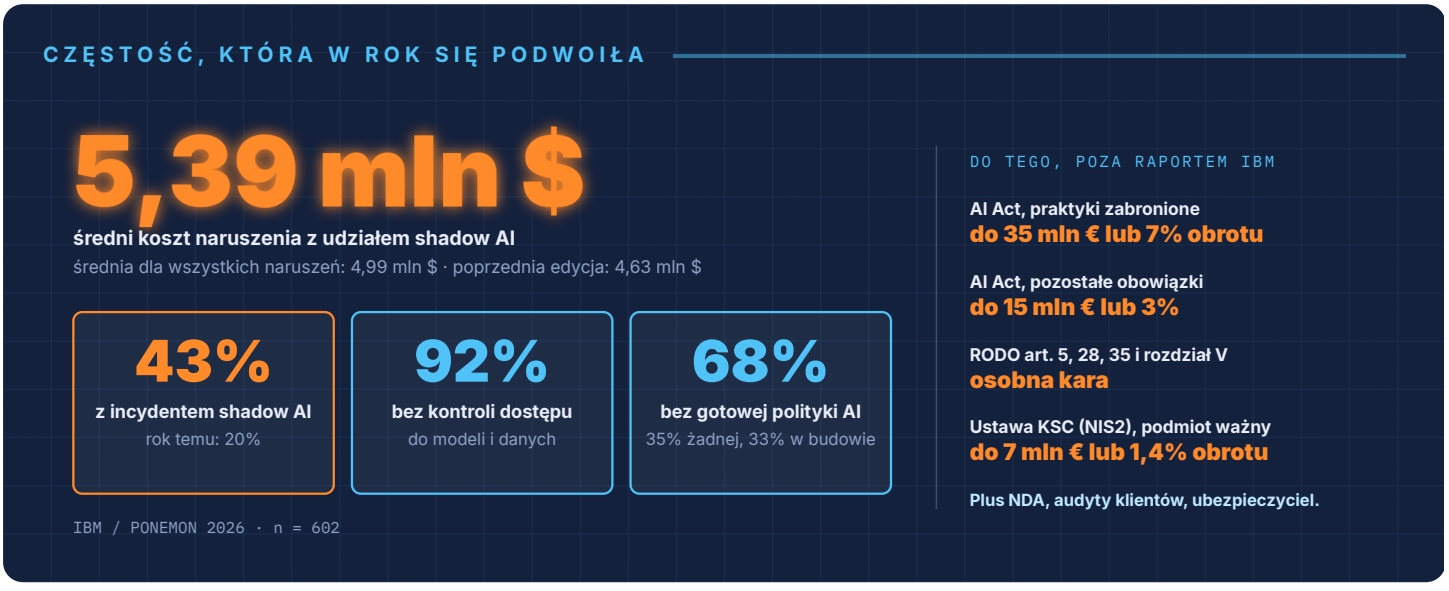
DYREKTOR FINANSOWY

koszt naruszenia
kary i compliance
NDA z klientami

Chłodno i po kolei. W logu Marka było „ORDER 88213 / KLIENT_A". Ten klient podpisał z Wami umowę o zachowaniu poufności, czyli „NDA", która zabrania przekazywania danych zamówień stronom trzecim. Dostawca darmowego czatu jest stroną trzecią. Nie ma znaczenia, że nikt nie chciał źle. Ma znaczenie, że w razie sporu nie potrafisz udowodnić, dokąd dane poszły i czy zostały usunięte, bo transakcja odbyła się na koncie prywatnym.

Liczby z raportu IBM i Ponemon Institute opublikowanego 29 lipca 2026, na próbie 602 organizacji[8]: incydent z udziałem shadow AI miało 43 procent naruszonych organizacji. Rok wcześniej 20 procent. Naruszenie z shadow AI kosztuje średnio 5,39 miliona dolarów, przy średniej dla wszystkich naruszeń 4,99 miliona; w poprzedniej edycji było to 4,63 miliona. Wśród organizacji, które przeżyły incydent związany z AI, 92 procent nie miało właściwej kontroli dostępu do modeli i danych. 68 procent nie miało gotowej polityki zarządzania AI: 35 procent żadnej, 33 procent dopiero ją pisało. Tylko 29 procent regularnie audytuje pod kątem niesankcjonowanego AI. Skutki incydentów z shadow AI: w 49 procentach utrata lub kompromitacja danych, w 42 procentach zakłócenie operacji, w 35 procentach straty reputacyjne, a co piąty zakończył się karą regulatora. Prawie nikt, komu się to przydarzyło, nie miał zabezpieczeń. Nie dlatego, że zawiodły. Dlatego, że ich nie było.

> **Prawie nikt, komu się to przydarzyło, nie miał zabezpieczeń. Nie dlatego, że zawiodły. Dlatego, że ich nie było.**



Unijne rozporządzenie o sztucznej inteligencji, czyli „AI Act", obowiązuje etapami, a latem 2026 zmieniono jego harmonogram[25]. Kary za praktyki zabronione obowiązują już od sierpnia 2025. Od 2 sierpnia 2026 stosuje się przepisy o przejrzystości z artykułu 50 (użytkownik musi wiedzieć, że rozmawia z AI, a treści generowane muszą być oznaczone) oraz nadzór i kary dla dostawców modeli ogólnego przeznaczenia. Obowiązki dla systemów wysokiego ryzyka przesunęła nowelizacja nazywana „Digital Omnibus", w mocy od 27 lipca 2026: na 2 grudnia 2027 dla systemów samodzielnych z załącznika III, w tym zarządzanie pracownikami i infrastruktura krytyczna, i na 2 sierpnia 2028 dla AI wbudowanej w maszyny i urządzenia

z załącznika I. Odroczone, nie odwołane. Złagodzono też artykuł 4: firma ma „podejmować działania wspierające" kompetencje AI załogi, a nie ich „zapewniać". Dla zakładu, w którym 9 na 10 osób używa publicznych narzędzi AI, a 7 na 10 nigdy nie przeszło szkolenia, to nie jest ulga. To jest opis stanu faktycznego, który ktoś kiedyś przeczyta w protokole.

Polska ma już własną ustawę o systemach sztucznej inteligencji, ogłoszoną 27 lipca 2026[26]. Powołała ona organ nadzoru, Komisję Rozwoju i Bezpieczeństwa Sztucznej Inteligencji, do której od 28 października 2026 każdy może złożyć skargę. Komisja prowadzi kontrole i nakłada kary według stawek AI Act. Żeby wiedzieć, w której klasie ryzyka się jest, trzeba najpierw wiedzieć, jakie systemy AI się ma: typ, dostawca, zastosowanie, przepływy danych[1]. Nie da się zinwentaryzować tego, czego się nie widzi, a według LayerX 89 procent użycia AI w firmach jest niewidoczne dla organizacji[9]. Ubezpieczyciele cyber dodają już pytania o AI do kwestionariuszy. Audytorzy klientów też. Darmowe aplikacje oznaczają darmowe kłopoty, tylko rozłożone na raty, których wysokości nikt nie zna.

Drugi rachunek przychodzi z innej strony i przemysł go nie zauważył, bo nie ma w nazwie „AI". Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa, czyli „KSC", która wdraża unijną dyrektywę NIS2, obowiązuje od 3 kwietnia 2026 i po raz pierwszy obejmuje produkcję: maszyn i urządzeń, chemikaliów, żywności, wyrobów medycznych, pojazdów[26]. Średnie i duże zakłady z tych branż muszą same zgłosić się do wykazu podmiotów do 3 października 2026, do 3 kwietnia 2027 mają wdrożyć system zarządzania bezpieczeństwem informacji, a poważny incydent zgłaszają w 24 godziny. Kary: do 10 milionów euro lub 2 procent obrotu dla podmiotów kluczowych, do 7 milionów euro lub 1,4 procent dla ważnych, z osobistą odpowiedzialnością kierownictwa. Log sterownika z parametrami procesu wklejony na prywatnym koncie do publicznego modelu przestaje być w tej ustawie anegdotą. Zaczyna być zdarzeniem, o którym trzeba zdecydować, czy je zgłosić.

Trzeci rachunek jest najstarszy i najłatwiejszy do wystawienia. Ogólne rozporządzenie o ochronie danych, czyli „RODO", shadow AI narusza niemal z definicji, jeśli w wklejanej treści są dane osobowe. Artykuł 5 mówi o rozliczalności: musisz wiedzieć, co i gdzie jest przetwarzane. Nie wiesz. Artykuł 28 wymaga umowy z każdym, komu powierzasz dane osobowe. Z darmowym kontem pracownika w publicznym czacie takiej umowy nie ma. Rozdział V ogranicza przekazywanie danych poza Europejski Obszar Gospodarczy, a dane z wielu popularnych czatów są przetwarzane poza nim. Artykuł 35 wymaga oceny skutków przy przetwarzaniu wysokiego ryzyka. Nikt jej nie zrobił. W edycji 2025 IBM podał, że 65 procent naruszeń z udziałem shadow AI eksponuje dane osobowe klientów[8].

Ślepy punkt infrastruktury

CIO

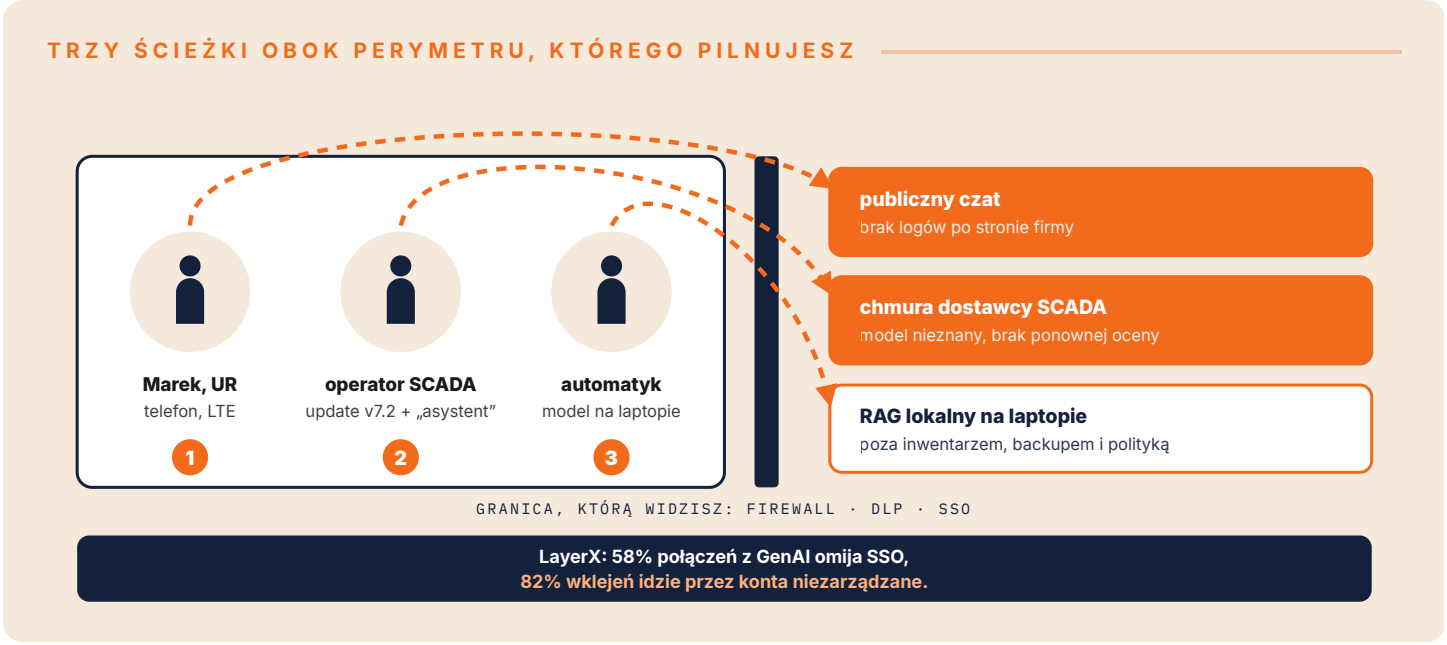
DYREKTOR IT · CISO

widoczność egress
data governance
tożsamość i OAuth

Macie dobrze skonfigurowany firewall, system zapobiegania wyciekom danych, czyli „DLP", logowanie jednokrotne, czyli „SSO", i listę zablokowanych domen z ChatGPT na pierwszym miejscu. Marek zrobił zdjęcie telefonem i wysłał je przez LTE z konta prywatnego. Wasz perymetr zobaczył zero pakietów. To nie jest luka w konfiguracji. To jest kanał, którego perymetr z definicji nie obejmuje.

Wasz perymetr zobaczył zero pakietów. To nie jest luka w konfiguracji. To jest kanał, którego perymetr z definicji nie obejmuje.

CSIRO opisuje trzy ścieżki, którymi shadow AI omija kontrolę[4]. Pierwsza to obejście granicy: dane płyną do publicznych narzędzi poza siecią firmową, jak u Marka. Druga to nieoceniona ekspansja możliwości: dostawca systemu nadzoru, czyli „SCADA", systemu realizacji produkcji, czyli „MES", albo systemu utrzymania ruchu, czyli „CMMS", dodaje w aktualizacji „inteligentnego asystenta", a nikt nie robi ponownej oceny, bo system jest przecież zatwierdzony. Jeden z respondentów: „no transparency of what model it is at any time". Trzecia to utrata obserwowalności przez obejście governance: uprzywilejowani technicznie użytkownicy stawiają lokalne modele i budują własne pipeline'y poza jakimkolwiek nadzorem. Marek to ścieżka pierwsza. Wasz dostawca SCADA to ścieżka druga. Wasz najlepszy automatyk, który „coś testuje na laptopie", to ścieżka trzecia.



Skala tego, co przechodzi obok, jest już zmierzona. LayerX: 32 procent ruchu danych z firmy na konta prywatne odbywa się przez generatywną AI, co czyni ją największym pojedynczym kanałem eksfiltracji w przedsiębiorstwie; 77 procent pracowników wkleja dane do promptów, 82 procent wklejeń idzie przez konta niezarządzane, 58 procent połączeń omija SSO[9]. Netskope: przeciętna organizacja generuje 223 zdarzenia z danymi wrażliwymi miesięcznie i wysyła 8,2 gigabajta do nieautoryzowanych narzędzi AI[12]. Harmonic: w asystentach do kodu 12,8 procent promptów zawiera poświadczenia dostępowe[7].

Dwa ryzyka z katalogu CSIRO zasługują na osobną uwagę, bo klasyczne zabezpieczenia są na nie ślepe. Pierwsze: rozszerzenie dostępu przez wnioskowanie. Pracownik ma legalny dostęp do logów maszyn i grafiku zmian, wkleja je do AI z prośbą o analizę i dostaje wnioski, do których uprawnień nie miał: obciążenie konkretnych osób, korelacje z absencją, w opisanym przez CSIRO przypadku dane

wynagrodzeniowe. Żadna kontrola dostępu nie została naruszona. Kontrola dostępu oparta na rolach, czyli „RBAC", kontroluje odczyt, a nie syntezę. Drugie: prompt injection. CSA nazywa to klasą podatności, która najwyraźniej odróżnia shadow AI od shadow IT; podatność EchoLeak (CVE-2025-32711, CVSS 9,3) pozwalała wyciągnąć dane z Microsoft 365 Copilot bez jednego kliknięcia ofiary[1]. A w sierpniu 2025 skradzione tokeny OAuth jednej integracji dały napastnikom dostęp do ponad 700 organizacji naraz. CSA sugeruje zacząć inwentaryzację właśnie od audytu grantów OAuth, bo to „often the most durable evidence".

WALLED GARDEN W PRAKTYCE

Walled garden w praktyce: zamknięta architektura, która przyjmuje na siebie chaos, zanim dotrze do ludzi i zanim ludzie poniosą go do publicznej chmury.

Wniosek dla CIO jest jeden i niewygodny. Jeśli sami nie dostarczycie bezpiecznej, zamkniętej architektury, tak zwanego walled garden, ludzie sami zintegrują dane firmowe z niezabezpieczonym API z zewnątrz. Już to robią. Pytanie brzmi tylko, czy będziecie to widzieć. Da się to zrobić bez dotykania sterowania: aplikacja na poziomie 4, odczyt danych przez DMZ, wyjście do modeli tylko z IT. Jak dokładnie, pokazujemy w sekcji 09.

PM Halucynacje na taśmie

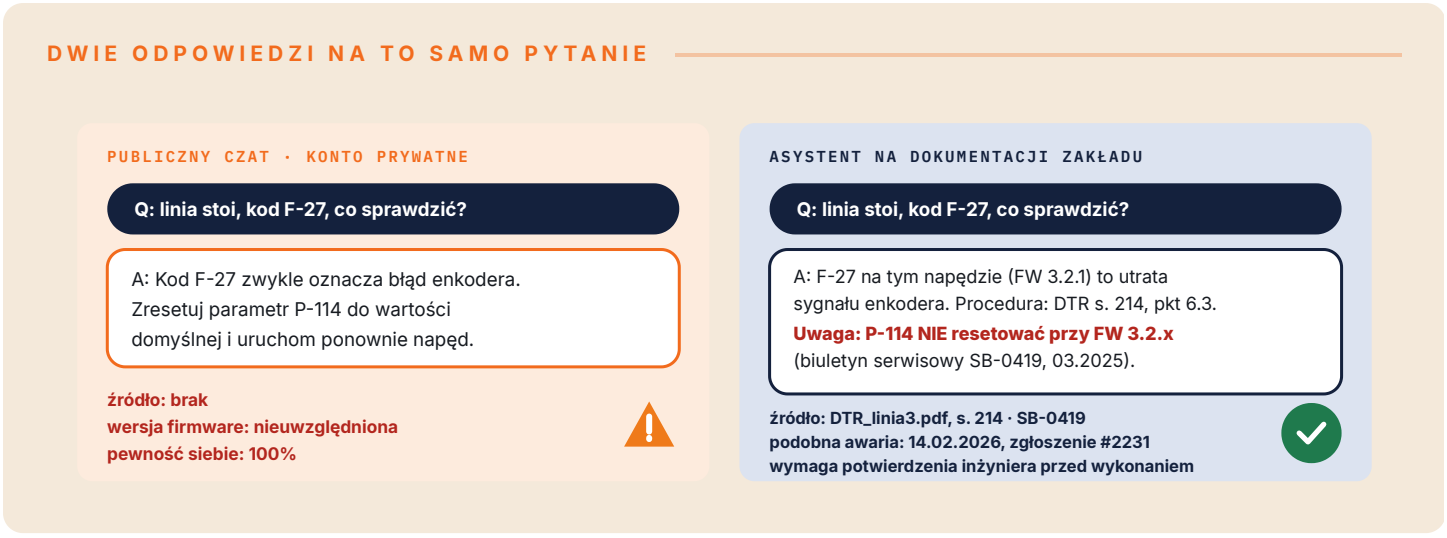
KIEROWNIK ZAKŁADU

OEE · MTTR · jakość
bezpieczeństwo ludzi
koszt złej partii

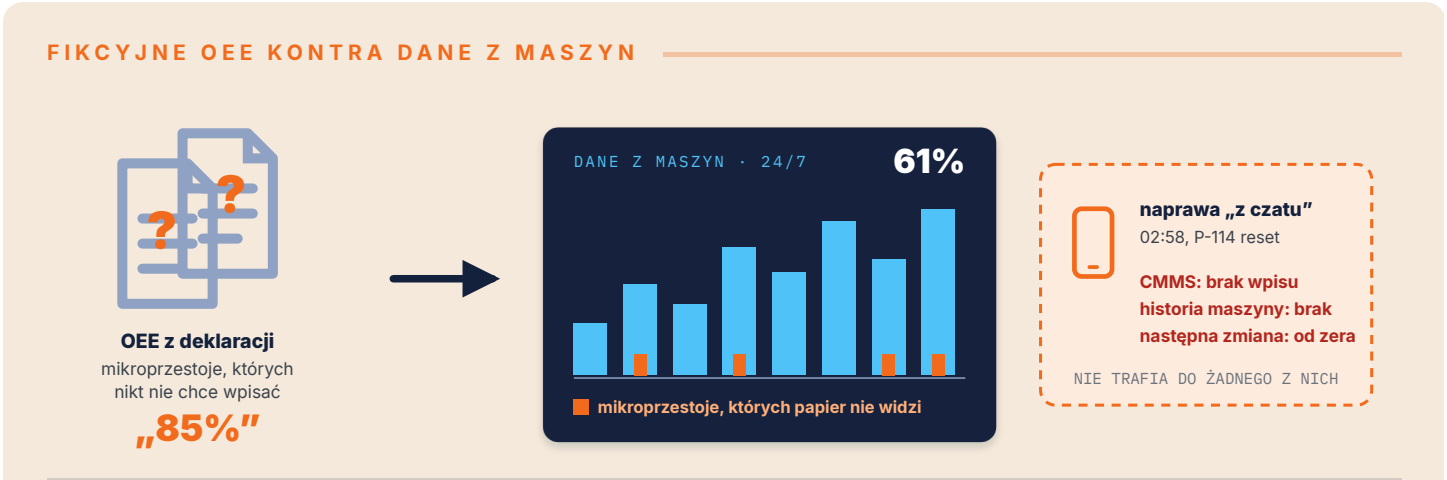
Wróćmy raz jeszcze do Marka, bo w jego historii jest jeszcze jeden szczegół. Czat kazał zresetować parametr P-114. Marek zresetował i linia ruszyła. Ale skąd czat wiedział, że P-114 to właściwy parametr dla tego napędu, tej wersji firmware, tej konfiguracji? Nie wiedział. Zgadł, na podstawie milionów cudzych instrukcji. Linia ruszyła, ale biuletyn serwisowy producenta mówi, że przy tej wersji firmware parametru P-114 nie wolno resetować. Skutek może przyjść za tydzień, na innej zmianie, i nikt nie połączy go z nocą Marka. Sztuczna inteligencja, gdy brakuje jej danych, ma tendencję do zmyślania faktów z pełnym przekonaniem. W literaturze nazywa się to halucynacją, a CSIRO wpisuje na listę dziewięciu ryzyk jako utratę integralności decyzyjnej: „we don't know the quality of the outcome"[4]. Do tego dochodzi automation bias, czyli ludzka skłonność do ufania maszynie bardziej niż sobie, zwłaszcza o 2:40 nad ranem.

Wyobraź sobie tę samą noc z innym parametrem. Operator pieca pyta czat o nastawę temperatury dla nowego stopu. Dostaje liczbę wyglądającą rozsądnie. Efektem nie będzie zabawna literówka w e-mailu. Efektem będzie partia tysiąca wadliwych detali wykryta w kontroli jakości u klienta, uszkodzona wykładzina

pieca wartego miliony albo, w najgorszym scenariuszu, bezpośrednie zagrożenie dla ludzi na zmianie. Ojowa i współautorzy w swojej taksonomii wydzielają dla takich zastosowań osobną, najwyższą kategorię: safety-critical[2]. A ostrzeżenia typu „ChatGPT może się mylić" nie pomagają: randomizowane badanie kontrolowane pokazało, że nie zmieniają zachowania użytkowników ani o włos[11].



Jest też cichszy koszt, który Plant Manager zna z własnych raportów. Wskaźnik efektywności wyposażenia, czyli „OEE", liczony z papierowych deklaracji operatorów jest fikcją: ukrywa mikroprzestoje, których nikt nie chce wpisać. Shadow AI pogłębia tę fikcję, bo naprawy „z czatu" nie trafiają ani do CMMS, ani do historii maszyny. Marek naprawił linię, ale system utrzymania ruchu o tym nie wie. Następna zmiana zacznie od zera. CSIRO nazywa to normalizacją ryzyka: powtarzane drobne obejścia stają się rutyną, a brak widocznej szkody uzasadnia tolerancję, aż do dnia, w którym szkoda staje się widoczna[4].



Fikcyjne OEE z papierowych deklaracji kontra dane prosto z maszyn. Naprawa „z czatu" nie trafia do żadnego z nich.

CZTERY OSOBY, CZTERY WALUTY, JEDNA NOC

2:40

PREZES

9 lat

receptura w cudzym modelu

40% naruszeń z shadow AI to kradzież własności intelektualnej

waluta: przewaga, która nie wraca

DYREKTOR FINANSOWY

5,39 mln $

koszt naruszenia z shadow AI

plus AI Act, RODO, KSC, NDA, ubezpieczyciel, audyt klienta

waluta: rachunek po roku

DYREKTOR IT · CISO

89%

użycia AI niewidoczne

zdjęcie DTR przez LTE omija firewall, DLP, SSO i listę blokad

waluta: widoczność

KIEROWNIK ZAKŁADU

P-114

reset z czatu, bez źródła

halucynacja w nastawie pieca to partia albo człowiek

waluta: partia i bezpieczeństwo

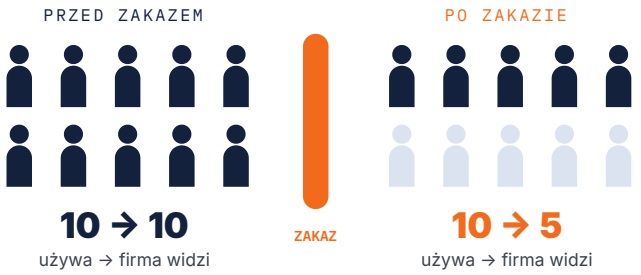
Cztery ścieżki, jeden punkt startu. Żadna z tych osób nie dowie się o tym pierwsza. Pierwszy wie Marek.

04

Odruch, który pogarsza sprawę

Pierwsza reakcja każdego zarządu na poprzedni rozdział brzmi: zablokować. Duże banki, m.in. JPMorgan, Citi, Goldman Sachs i Deutsche Bank, ograniczyły dostęp do ChatGPT już w 2023 roku. Rok później Salesforce zmierzył, że 72 procent pracowników sektora finansowego używa niesankcjonowanych narzędzi AI (liczba za omówieniem Axis Intelligence, nie za raportem pierwotnym)[10]. Zakaz nie zmniejszył użycia. Zmniejszył widoczność użycia. Ten sam wyciek, tylko bez logów. Zakaz ChatGPT ma mniej więcej taką skuteczność jak tabliczka „nie karmić gołębi". Gołębie nie czytają, a ludzie z bułką w kieszeni przechodzą na drugą stronę placu.

CO NAPRAWDĘ ROBI ZAKAZ?



CSA 2026: po zakazie około połowa pracowników dalej używa AI przez konta prywatne. Reszta w telefonach, poza zasięgiem jakiegokolwiek monitoringu.

JAPONIA: ROK OD KONT PRYWATNYCH DO FIRMOWYCH

Netskope 2026[12]. Ta zmiana nie zbiegła się z blokadą, tylko z upowszechnieniem firmowych narzędzi, które były równie wygodne jak te zakazane. Unseen Security: zatwierdzona alternatywa obniża użycie niezatwierdzonych o 89 procent[13].

Jeden wyjątek, który potwierdza regułę: wszystkie 27 organizacji z badania CSIRO zablokowało DeepSeeka po dyrektywie rządowej i to zadziałało. Blokada konkretnego narzędzia, z powodem, który da się wypowiedzieć na hali bez zająknięcia, jest egzekwowalna. Blokada kategorii „AI" nie jest, bo ta kategoria obejmuje już Twoją wyszukiwarkę, edytor tekstu i prawdopodobnie lodówkę w kuchni socjalnej.

> **Zakaz to nie polityka, tylko odroczenie decyzji. Marek nie potrzebuje kary. Potrzebuje narzędzia, które o 2:40 odpowie szybciej niż publiczny czat i na warunkach zakładu, nie dostawcy.**

05

A w Polsce? Nikt nie zapytał człowieka przy maszynie

Badania o AI w Polsce istnieją: KPMG, PwC, ESET razem z DAGMA, Sharp, WEBCON, Salesforce, AMP. Każde mierzy pracownika biurowego, uśrednionego po branżach. Żadne nie wydzieliło produkcji, utrzymania ruchu ani technologii.

9 NA 10 UŻYWA · NIKT NIE PYTAŁ HALI

Nie ma prac dyplomowych ani doktoratów, nie ma programu Narodowego Centrum Badań i Rozwoju, czyli „NCBR". Polska Agencja Rozwoju Przedsiębiorczości, czyli „PARP", ma jeden poradnik[18]. Poradnik to nie badanie. Jedyny polski artykuł recenzowany dotyczy dziennikarzy i dodaje do definicji słowo, którego brakuje w literaturze anglosaskiej: użycie „nieautoryzowane lub nieujawniane"[17]. Nie tylko brak zgody. Ukrywanie.

POLSKA NA DZIESIĘĆ OSÓB (KPMG, N = 1 082)

KPMG / UNIVERSITY OF MELBOURNE 2025 · POLSKA · n = 1 082

Stąd hipoteza, którą chętnie damy sobie obalić: luka świadomości w polskim przemyśle jest realna, bo nikt nie zapytał kierownika utrzymania ruchu, co wkleja do czatu i dlaczego. A skoro nie wiemy, nie mamy ani przepisów pisanych z myślą o produkcji, ani procesów higieny używania AI na hali. Tak jak kiedyś trzeba było nauczyć ludzi mycia rąk, zanim ktokolwiek uwierzył w bakterie. Różnica: na bakterie czekaliśmy kilkadziesiąt lat. Wyciek już trwa.

CZTERY POWODY, JEDNO LUSTRO

Cztery powody, dla których AI nie trafia na halę oficjalnie. Strach o własność intelektualną, silosy danych w dziesiątkach niepołączonych systemów, ulotne know-how odchodzących ekspertów i fikcyjne OEE z papierowych raportów.

I te same cztery powody, dla których trafia tam nieoficjalnie. Marek nie boi się o IP, bo nikt mu nie powiedział, że powinien. Nie łączy silosów, bo wkleja to, co ma pod ręką. Uzupełnia ulotne know-how z czatu. I zamiast poprawiać OEE, pogłębia jego fikcję, bo naprawy z czatu nie trafiają do żadnego systemu. Shadow AI jest lustrem, w którym zakład widzi wszystko, czego nie zrobił.

06

Wyjście z cienia. Plan ratunkowy

Zakazywanie AI to walka z wiatrakami. Zamiast tego proponujemy trzy ruchy i jedną miarę dojrzałości. Ruchy wymagają współpracy prezesa, finansów, IT i zakładu jednocześnie. Miara mówi, gdzie jesteś.

01 Znajdź ukrytych championów AI. Marka i Annę. Zamiast ich karać, zrób z nich liderów wdrożenia.

Anonimowa ankieta wśród utrzymania ruchu, technologów i konstruktorów: z czego korzystasz, do czego, co wklejasz. Pięć pytań, bez nazwisk, z amnestią ogłoszoną na piśmie. W CSIRO jedna organizacja po włączeniu DLP zobaczyła 1 300 zdarzeń w miesiąc; wcześniej widziała zero, bo nie patrzyła. Ci, którzy używają AI najwięcej, to Twoi przyszli liderzy wdrożenia. Dziś są w cieniu. Wyciągnij ich na światło i daj im pierwszy dostęp do narzędzia z punktu drugiego.

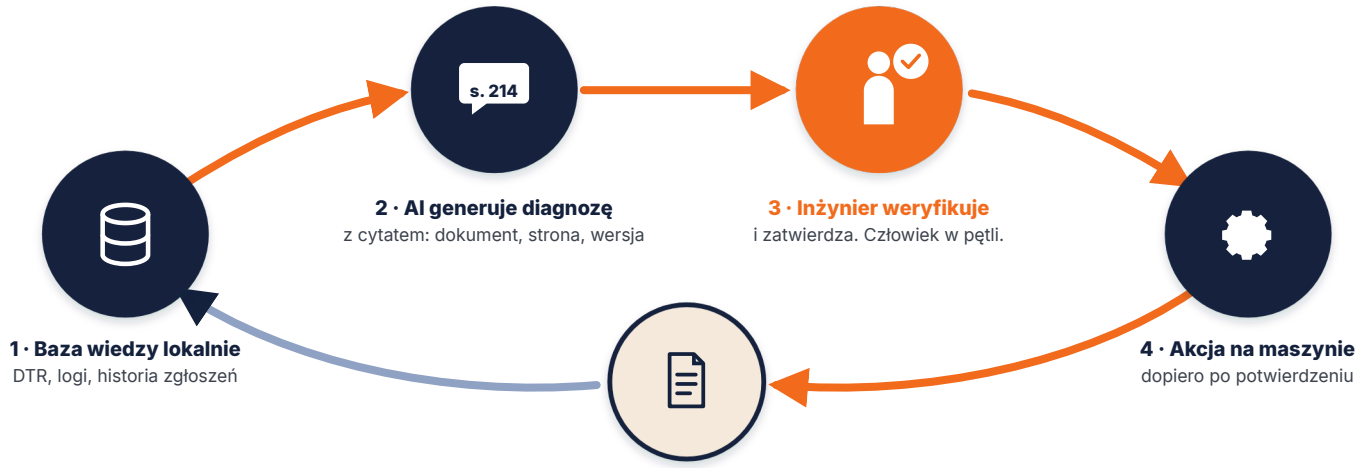
02 Daj im coś lepszego niż to, po co sięgają po cichu. Własny model albo licencja firmowa, przy której dostawca nie trenuje modeli na Waszych danych.

Warunek konieczny: równie wygodne jak publiczny czat. Trzy kliknięcia więcej niż ChatGPT w telefonie i ChatGPT wygra. Zawsze. Dla utrzymania ruchu znaczy to: odpowiedź na kod błędu w sekundy, ale z Waszej dokumentacji, z numerem strony DTR, z historią podobnych awarii i z wymaganiem potwierdzenia przez inżyniera (porównanie w rozdziale o halucynacjach). Architektura do wyboru: chmura prywatna, hybrydowa albo SaaS. W hybrid i private cloud baza wiedzy, dokumentacja i historia zgłoszeń zostają w Waszej infrastrukturze; w SaaS są przechowywane w wydzielonym środowisku co.brick AI w UE, na Waszej umowie powierzenia i z możliwością eksportu w każdej chwili. Do modelu językowego trafia tylko fragment potrzebny do odpowiedzi, przez biznesowe API z umową i bez trenowania na Waszych danych. Jeśli macie sieć OT, dane z niej wychodzą jednokierunkowo. Każde pytanie zostawia ślad po Waszej stronie: kto pytał, o co i na podstawie jakich źródeł. Minimalne wymagania CSA dla każdego narzędzia z danymi firmowymi: umowa powierzenia, ocena dostawcy, brak retencji między sesjami, potwierdzenie zasad przez pracownika[1].

03 Jedna, jasna polityka. Trzy koszyki, wydrukowane i powieszone przy stanowiskach.

Wolno wkleić wszędzie (instrukcja BHP, ogólne pytanie techniczne). Wolno tylko do narzędzia firmowego (logi, DTR, zgłoszenia, korespondencja z klientem). Nie wolno nigdzie poza zamkniętym systemem (receptury, BOM, program PLC, rysunki, dane osobowe, cokolwiek objęte NDA). Plus jedno nazwisko z shadow AI w celach rocznych; nie komitet, nie „IT razem z HR". Polski Przemysł: odpowiedzialność za AI jest dziś rozproszona między pięć funkcji i żadna nie zarządza więcej niż jedną czwartą[19]. Shadow AI rośnie dokładnie w tej szczelinie.

PĘTLA, W KTÓREJ CZŁOWIEK JEST OSTATNIM KROKIEM



AI generuje diagnozę z cytatem ze źródła. Inżynier weryfikuje i zatwierdza. Dopiero potem akcja na maszynie. Wynik wraca do bazy wiedzy.

Tak wygląda polityka, która działa. Nie jako PDF w intranecie, tylko jako pętla wbudowana w narzędzie: model nie zgaduje, bo każda odpowiedź ma link do konkretnej strony instrukcji. Człowiek nie jest kontrolą po fakcie, tylko ostatnim krokiem przed akcją.

Marek dostaje to samo, co dostał z darmowego czatu, plus trzy rzeczy, których tam nie było: źródło, log i pewność, że jego pytanie zostało w firmie. To jest różnica między „nie wolno" a „nie trzeba".

GDZIE JESTEŚ: PIĘĆ POZIOMÓW DOJRZAŁOŚCI

Areebi, indeks z maja 2026, źródło 14 (synteza wtórna)
ISACA 2026: 38% firm ma kompleksową politykę, 12% ma przetestowaną procedurę wyłączenia AI

Monitoring, nie kara. Organizacje z badania CSIRO, które sobie radzą, mówią wprost: „not to block, it's to monitor, to understand, to educate, and respond". Z jednym ostrzeżeniem: monitoring pracowników w Unii wymaga proporcjonalności, minimalizacji, limitów przechowywania, transparentności i oceny skutków z udziałem przedstawicieli załogi[2]. Monitoring, który sam łamie RODO, nie leczy problemu z RODO.

07

Sześć niewygodnych prawd dla polskiego przemysłu

Można ten tekst zamknąć i uznać, że kary są tańsze niż zmiana. Wiele zakładów tak zrobi, bo tak jest szybciej. Dla tych, które planują dalej niż jeden kwartał, mamy sześć rzeczy, których branża nie chce usłyszeć.

1 2 3 4 5 6

PRAWDA 1

Polski przemysł ma politykę AI tak samo, jak ma politykę używania długopisów.

Tylko co trzecia polska firma ma jakiekolwiek zasady użycia AI[16]. Globalnie kompleksową politykę ma 38 procent, a przetestowaną procedurę wyłączenia AI 12 procent[24]. W tym samym czasie 90 procent Polaków używających AI w pracy sięga po narzędzia publiczne. Firma bez polityki nie jest neutralna. Ona już ma politykę: „róbcie, co chcecie, tylko nie mówcie".

PRAWDA 2

Zakaz ChatGPT to jedyna inwestycja w bezpieczeństwo, która zwiększa ryzyko.

Po zakazie połowa ludzi przechodzi na konta prywatne, a firma traci ostatnią szansę na jakikolwiek log[1,4]. Sektor bankowy sprawdził to za Ciebie w 2023 roku: zakazy nie zmniejszyły użycia AI, tylko jego widoczność[10]. Jeśli Twoja odpowiedź na shadow AI to lista zablokowanych domen, nie masz programu bezpieczeństwa. Masz program przenoszenia problemu do telefonów.

PRAWDA 3

Kto do końca 2027 nie zbuduje własnego AI, dostanie AI od dostawcy SCADA. W jego cenie, na jego warunkach, z jego modelem.

Dostawcy systemów OT już dokładają „asystentów" w aktualizacjach, bez ponownej oceny i bez przejrzystości, jaki model stoi za odpowiedzią[4]. Firma, która nie ma własnej architektury, nie wybierze, czy chce AI. Wybierze tylko, od kogo i za ile. To jest utrata suwerenności nad danymi procesowymi dokonana przez zaniechanie.

PRAWDA 4

Odroczenie AI Act do grudnia 2027 to nie prezent. To ostatni rok, w którym inwentaryzacja AI jest tania.

Wysokie ryzyko przesunięto, ale kary za praktyki zabronione obowiązują od 2025, przejrzystość od sierpnia 2026, a do polskiej Komisji od 28 października można składać skargi[25,26]. Klasyfikacji nie zrobi się bez inwentarza, a inwentarza nie zrobi się w Excelu wieczorem przed kontrolą, bo 89 procent użycia AI jest niewidoczne[9]. Rejestr wymaga, żeby AI weszło głównymi drzwiami: przez zatwierdzoną platformę z logiem. Firmy, które to odkładają, nie odkładają papierologii. Odkładają moment, w którym będą w stanie cokolwiek udowodnić.

PRAWDA 5

Wiedza, która wypłynęła, nie wraca. Kto liczy zwrot z wdrożenia AI, niech policzy też koszt bierności.

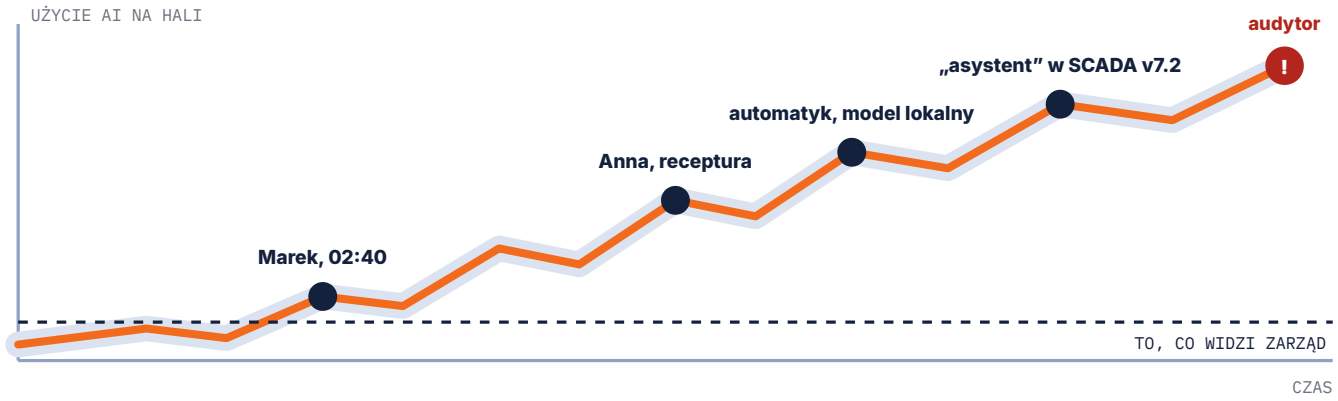
Hasło można zmienić, kartę zablokować, umowę renegocjować. Receptury, która trafiła do modelu trenującego na danych użytkowników, nie da się odwołać. 40 procent naruszeń z udziałem shadow AI to kradzież własności intelektualnej[8]. Bierność nie jest opcją zerową. Jest opcją z ujemną stopą zwrotu, tylko nikt jej nie wpisuje do arkusza.

PRAWDA 6

Następna fala to nie czat, tylko agenci. Będą działać w Waszych systemach z prędkością maszyny.

82 procent dyrektorów IT mówi, że pracownicy tworzą agentów szybciej, niż da się to nadzorować; 53 procent organizacji doświadczyło już przekroczenia uprawnień przez agenta[1]. W fabrykach jeszcze ich nie ma. CSIRO: „just chat"[4]. To jest ostatni moment, w którym problem ma formę wklejonego tekstu, a nie autonomicznego procesu z dostępem do CMMS.

KRZYWA, KTÓRĄ KTOŚ JUŻ NARYSOWAŁ



Krzywa adopcji AI w przemyśle nie czeka na politykę. Rośnie z politykami i bez nich. Różnica polega na tym, kto ją narysował.

Prawda, która spina pozostałe. Krzywa adopcji AI w Waszym zakładzie już istnieje. Narysowali ją Marek i Anna, po cichu, na prywatnych kontach, w tempie, którego żaden dział nie planował. Pytanie nie brzmi, czy ją narysować. Pytanie brzmi, czy zarząd chce ją zobaczyć, zanim narysuje ją audytor.

> **Branża lubi mówić, że „AI to jeszcze nie ten etap". Ten etap już się odbył, tylko bez niej. O 2:40, na koncie prywatnym, w telefonie najlepszego inżyniera.**

08

Poniedziałek rano. Narzędzia, nie hasła

Cztery rzeczy da się zrobić bez budżetu i bez dostawcy. Macierz, która mówi, co wolno wkleić i gdzie. Harmonogram w trzech horyzontach. Dziesięć pytań na najbliższe posiedzenie zarządu. I lista wymagań dla każdego, kto chce sprzedać Wam AI.

MACIERZ: CO WOLNO WKLEIĆ I DOKĄD

WRAŻLIWOŚĆ DANYCH ↓ · WPŁYW NA DECYZJĘ →

	informacja „co to znaczy?"	**rekomendacja** „co sprawdzić?"	**decyzja / działanie** „ustaw parametr na..."
publiczne instrukcja BHP, norma, katalog	**publiczny czat OK**	**publiczny czat OK**	**narzędzie firmowe**
wewnętrzne logi maszyn, zgłoszenia, grafiki	**narzędzie firmowe**	**narzędzie firmowe**	**zamknięty system** + potwierdzenie inżyniera
poufne DTR, receptury, BOM, program PLC	**zamknięty system** ze źródłem	**zamknięty system** + potwierdzenie inżyniera	**zamknięty system** + podpis, ślad audytowy
regulowane / safety dane osobowe, NDA, nastawy krytyczne	**zamknięty system** ochrona danych osobowych	**zamknięty system** + podpis, ślad audytowy	**nigdy bez człowieka** safety-critical, IEC 61508

na podstawie wymiarów D1 i D2 z taksonomii Ojowy i in. (2026)

Ta sama zasada, którą Ojowa i współautorzy opisują w pięciu wymiarach, w wersji do powieszenia przy stanowisku. Nie klasyfikujesz narzędzia po nazwie. Klasyfikujesz parę: jakie dane i do jakiej decyzji. Pytanie o kod błędu z instrukcji producenta może iść do publicznego czatu. Ten sam kod z logiem zawierającym numer zamówienia klienta już nie. Zamknięty system to narzędzie firmowe z umową powierzenia, bez trenowania na Waszych danych, z izolacją danych i ze śladem pytań po Waszej stronie.

DZIESIĘĆ PYTAŃ NA NAJBLIŻSZE POSIEDZENIE ZARZĄDU

1. **Ile narzędzi AI działa dziś w firmie?** Jeśli odpowiedź brzmi „zero" albo „tylko Copilot", nikt nie sprawdzał.
2. **Kto ma shadow AI w celach rocznych?** Jeśli pięć osób po trochu, to nikt.
3. **Co wkleił do publicznego czatu nasz najlepszy technolog w tym miesiącu?** Nie wiesz. To jest odpowiedź.
4. **Który z naszych dostawców SCADA, MES, CMMS dodał AI w ostatniej aktualizacji?** Na którym poziomie sieci siedzi, gdzie przetwarza dane i czy cokolwiek zapisuje do sterowania?
5. **Czy potrafimy dziś wygenerować inwentarz systemów AI, o który zapyta Komisja Rozwoju i Bezpieczeństwa SI albo audytor klienta?** Z klasą ryzyka i przepływami danych. I czy jesteśmy w wykazie KSC, jeśli powinniśmy?
6. **Ile z naszych umów NDA zabrania przekazywania danych stronom trzecim?** Dostawca darmowego czatu jest stroną trzecią.
7. **Czy ubezpieczyciel cyber pytał nas o AI?** Jeśli jeszcze nie, zapyta przy odnowieniu.
8. **Ile razy w tym roku maszyna została naprawiona „z czatu" i nie trafiło to do historii maszyny?** Zapytaj mistrzów zmian, nie system.
9. **Czy mamy dla utrzymania ruchu narzędzie szybsze niż publiczny czat?** Jeśli nie, decyzja o shadow AI już zapadła. Bez nas.
10. **Co zrobimy, gdy pierwszy pracownik postawi agenta z dostępem do CMMS?** Nie „czy". „Gdy".

TRZY HORYZONTY: CO PO KOLEI

DZIŚ

Zobacz

0 DO 90 DNI

- Anonimowa ankieta z amnestią
- Audyt grantów OAuth i kont na domenie firmowej u dostawców AI
- Podstawowy DLP na kanałach do publicznych modeli
- Jedno nazwisko z shadow AI w celach rocznych

Wynik: pierwsza liczba większa od zera

90 DNI

Uporządkuj

90 DNI DO 12 MIESIĘCY

- Katalog narzędzi z klasą ryzyka
- Macierz danych przy stanowiskach
- Pilot bezpiecznej alternatywy na jednej linii, z mierzonym czasem
- Inwentarz systemów AI pod AI Act, w tym AI w systemach dostawców
- Sprawdzenie, czy zakład podlega KSC

Pytanie do każdego dostawcy OT o AI

12 MIESIĘCY

Utrwal

PO 12 MIESIĄCACH

- AI w cyklu życia systemów: ocena przed, monitoring po
- Kwartalny przegląd telemetrii i polityki
- Procedura wyłączenia AI przetestowana, nie tylko spisana
- Zasady dla agentów, zanim pojawi się pierwszy

Kolejność za Cloud Security Alliance (Three-Horizon Framework, 2026). Większość firm zaczyna od środka, czyli od polityki, i dlatego większość polityk jest martwa: opisuje narzędzia, których nikt nie zinwentaryzował, dla ludzi, których nikt nie zapytał.

SZEŚĆ WYMAGAŃ DLA KAŻDEGO, KTO CHCE SPRZEDAĆ WAM AI

DANE

Zero treningu na Waszych danych, na piśmie.

Umowa powierzenia i wyraźny zapis, że wejścia nie trafiają do treningu ani do innych klientów. Brak retencji danych u dostawcy modelu.

LOKALIZACJA

Model i dane w Waszym perymetrze albo w wydzielonym środowisku w UE.

Odczyt z sieci OT tylko przez DMZ, bez portów przychodzących, bez zapisu do sterowania. Jeśli dostawca nie umie narysować na modelu Purdue, którędy płyną dane, nie wie tego.

ŹRÓDŁO

Każda odpowiedź z cytatem: dokument, strona, wersja.

Odpowiedź bez źródła to halucynacja w garniturze. W utrzymaniu ruchu to warunek bezpieczeństwa, nie wygody.

CZŁOWIEK

Działanie na maszynie tylko po potwierdzeniu inżyniera.

AI proponuje, człowiek zatwierdza, system zapisuje kto i kiedy. Bez tego nie ma śladu audytowego, a bez śladu nie ma zgodności.

PRZEJRZYSTOŚĆ

Wiecie, jaki model stoi za odpowiedzią i kiedy się zmienił.

„No transparency of what model it is at any time" to cytat z badania, nie warunek umowy. Zmiana modelu wymaga powiadomienia i ponownej oceny.

WYJŚCIE

Procedura wyłączenia i eksport wiedzy w otwartym formacie.

Baza wiedzy, którą zbudujecie, jest Wasza. Dostawca, który nie umie jej oddać, nie sprzedaje narzędzia. Sprzedaje uzależnienie.

Wymaganie pierwsze obejmuje minimum Cloud Security Alliance dla każdego narzędzia z danymi firmowymi[1]. Pozostałe wynikają z badania CSIRO i z doświadczenia z hali. Wydrukuj tę listę i połóż na stole przed każdą prezentacją dostawcy. Także naszą: w sekcji 09 zestawiamy ją punkt po punkcie z tym, jak sami ją spełniamy.

ROZDZIAŁ 09 Z 09

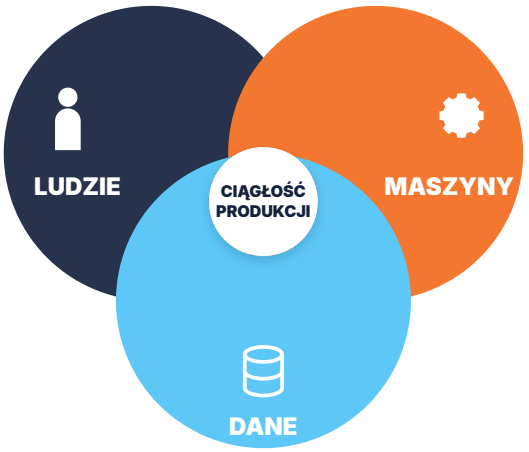
09

Jak to wygląda, kiedy działa

Bezpieczna alternatywa musi być równie wygodna jak publiczny czat i działać na warunkach firmy: z umową, bez trenowania na jej danych i z pełnym śladem po jej stronie. Wokół tego warunku zbudowaliśmy co.brick. Poniżej, jak to wygląda w zakładzie.

LUDZIE, MASZYNY, DANE

Osobno w każdym zakładzie:
ludzie z kompetencjami,
maszyny z danymi,
AI, która potrafi je czytać.



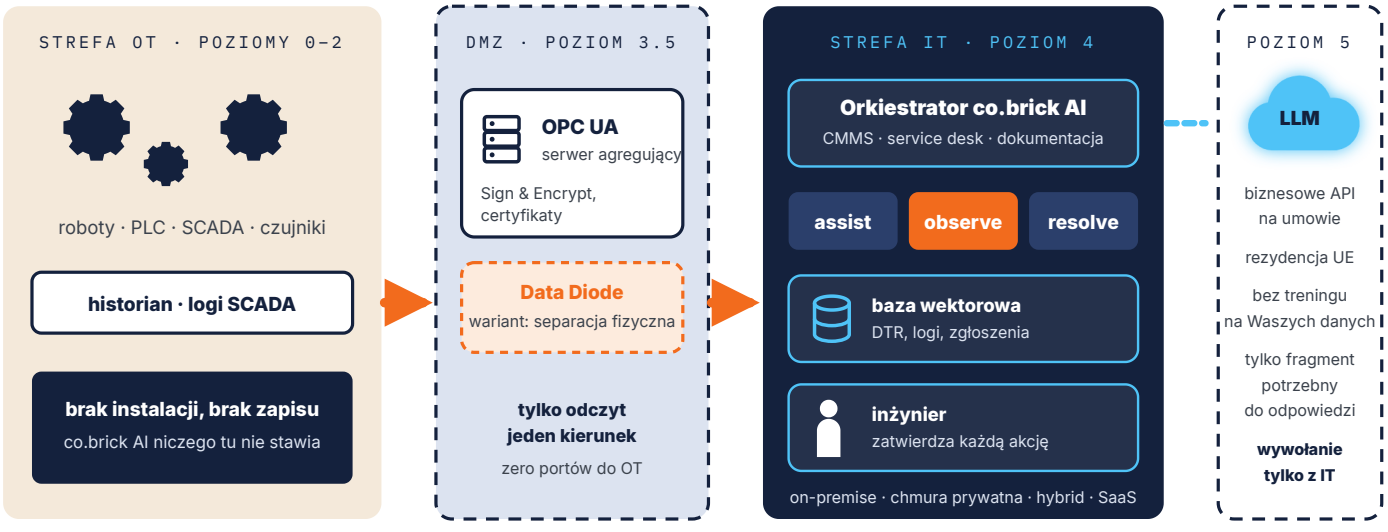
Shadow AI powstaje tam,
gdzie nikt nie połączył
tych trzech okręgów,
więc ludzie robią to sami,
telefonem, o 2:40.

Ludzie, maszyny, dane. Środek rysunku to ciągłość produkcji.

Trzy okręgi, które każdy zakład ma osobno. Ludzi z kompetencjami, maszyny z danymi i AI, która potrafi je czytać. Shadow AI powstaje dokładnie tam, gdzie nikt nie połączył tych trzech okręgów w jedno narzędzie, więc ludzie robią to sami, telefonem, o 2:40.

co.brick buduje ten środek na warunkach firmy: z umową, bez trenowania na jej danych, z pełnym śladem po jej stronie i z człowiekiem jako ostatnim krokiem przed każdą akcją na maszynie.

ARCHITEKTURA: OT, DMZ, IT I WYJŚCIE DO MODELI



Wariant on-premise: zero ingerencji w sieć OT, logi SCADA płyną jednokierunkowo, orkiestrator i bazy wektorowe w perymetrze fabryki. Platforma co.brick może też działać w Waszej chmurze prywatnej, hybrydowo albo jako SaaS. W hybrid i private cloud baza wiedzy, dokumentacja i historia zgłoszeń zostają w Waszej infrastrukturze; w SaaS są przechowywane w wydzielonym środowisku co.brick AI w UE, na Waszej umowie powierzenia i z możliwością eksportu w każdej chwili. Do modelu językowego trafia tylko fragment potrzebny do odpowiedzi, przez biznesowe API z umową i bez trenowania na Waszych danych. Dioda danych na rysunku to wariant dla zakładów, które wymagają fizycznej separacji sieci OT; standardowo odczyt idzie przez agregujący serwer OPC UA albo broker w przemysłowej DMZ. To jest różnica między „wkleił do czatu" a „zapytał firmowy system".

Tyle tytułem ilustracji. Teraz zakres technologiczny, który potwierdzamy na piśmie przed każdym wdrożeniem. To nie są deklaracje marketingowe, tylko warunki brzegowe, w których co.brick AI działa u klientów z produkcją, i granice, których nie przekraczamy[31].

POTWIERDZONY ZAKRES TECHNOLOGICZNY CO.BRICK AI

- **Nie dotykamy sterowania.** W warstwie czujników, PLC i SCADA (poziomy 0 do 2 modelu Purdue) niczego nie instalujemy i niczego nie zapisujemy. Dane trafiają wyżej wyłącznie przez istniejące interfejsy odczytowe.
- **Odbieramy dane tylko do odczytu i tylko przez DMZ.** Punkt odbioru dla observe stoi na poziomie 3 / 3.5: agregujący serwer OPC UA albo broker w przemysłowej DMZ. Nie ma bezpośrednich połączeń IT → OT i nie otwieramy portów przychodzących do strefy OT.
- **OPC UA obsługujemy standardowo,** w trybie Sign & Encrypt z certyfikatami. MQTT (broker w DMZ, TLS), Modbus TCP (wyłącznie przez bramkę lub konwerter na poziomie 2/3), odczyt z historianów SQL (konto tylko do odczytu, replika w DMZ) i inne protokoły włączamy w projekcie, po weryfikacji konkretnego środowiska.
- **Aplikacje działają na poziomie 4,** w IT firmy albo w chmurze prywatnej: assist, resolve, analityka i asystent observe. Tam też działają integracje z bazą wiedzy, CMMS i systemem zgłoszeń klienta.
- **Modele językowe wywołujemy wyłącznie z poziomu 4.** Nigdy ze strefy OT. W wariantach hybrid i SaaS są to biznesowe LLM z rezydencją danych w UE albo modele hostowane w zasobach co.brick AI; w private cloud modele w tenancie klienta albo fizycznie u klienta.
- **Alerty trafiają do ludzi, nie do maszyn.** Zdarzenie wykryte przez observe tworzy zgłoszenie w resolve. Decyzję i akcję na maszynie podejmuje inżynier.
- **Trzy modele wdrożenia do wyboru:** SaaS, hybrid i private cloud. Hosting u niezależnego dostawcy, na przykład w polskim centrum danych, to lokalizacja, a nie osobny model: na umowie co.brick AI jest to SaaS, na umowie klienta private cloud.
- **Serwery z GPU nie są warunkiem.** Domyślnie nie wymagamy ich od klienta; są potrzebne tylko wtedy, gdy klient chce uruchamiać modele fizycznie u siebie. W hybrid wystarczy VM Linux/Windows lub Kubernetes, VPN serwisowy i wyjście API do modeli. W SaaS: konektory do źródeł danych. Edge AI przy maszynach nie jest dziś standardem.
- **Dokumentację przejmujemy w całości.** assist importuje, wektoryzuje i utrzymuje bazę wiedzy; porządkowanie dokumentacji robimy razem z Wami. Wiele źródeł i systemów różnych dostawców jednocześnie, analiza schematów i wykresów osadzonych w dokumentacji, izolacja danych na poziomie kolekcji (osobno dla linii, osobno dla działów), skanowanie przyrostowe w tle.
- **Baza sama pilnuje swojej jakości.** Nowe dokumenty można weryfikować od razu po dodaniu; system wykrywa sprzeczności, luki, nieaktualne artykuły i dane osobowe. Dane z CMMS włączamy przez eksport lub integrację. W hybrid i private cloud baza wiedzy, dokumentacja i historia zgłoszeń zostają w Waszej infrastrukturze; w SaaS są przechowywane w wydzielonym środowisku co.brick AI w UE, na Waszej umowie powierzenia i z możliwością eksportu w każdej chwili.

Poniżej ten sam zakres w trzech rysunkach: gdzie stoimy w sieci, jak wychodzą dane i gdzie mieszka model.

SZEŚĆ WYMAGAŃ Z SEKCJI 08 I JAK JE SPEŁNIAMY

Wymaganie	Jak spełnia je co.brick AI
Dane	Biznesowe API z umową, bez trenowania na Waszych danych, umowa powierzenia, brak retencji danych u dostawcy modelu.
Lokalizacja	Tylko odczyt przez DMZ, modele wywoływane wyłącznie z poziomu 4, trzy modele wdrożenia z rezydencją danych w UE.
Źródło	Każda odpowiedź ze wskazaniem dokumentu, strony i wersji.
Człowiek	AI proponuje, inżynier zatwierdza; alerty trafiają do ludzi, nie do maszyn.
Przejrzystość	Zmiana modelu lub promptów wymaga zgody klienta i jest odnotowana w dzienniku zmian.
Wyjście	Eksport bazy wiedzy w otwartym formacie w każdej chwili.

Warunki umowne (retencja historii rozmów, tryb zmian, eksport) zapisujemy w umowie wdrożeniowej, bo tam jest ich miejsce.

GDZIE MIESZKA CO.BRICK AI W MODELU PURDUE?

Granicę między OT a IT wyznacza klient i jej przebieg zależy od jego architektury. Można za to jasno powiedzieć, gdzie w modelu Purdue mieszczą się produkty co.brick AI: w warstwie sterowania nie instalujemy niczego i niczego do niej nie zapisujemy. Przekaz dla działów OT jest prosty: co.brick AI tylko czyta dane[31].

JAK DANE WYCHODZĄ Z MASZYN: TYLKO ODCZYT, PRZEZ DMZ

STANDARD

OPC UA

Połączenie w trybie Sign & Encrypt z certyfikatami, najlepiej przez agregujący serwer OPC UA w DMZ. Obsługiwane standardowo.

NA PROJEKT

MQTT

Broker w DMZ, transmisja szyfrowana TLS. Możliwe po weryfikacji konkretnego środowiska.

NIGDY WPROST

Modbus TCP

Protokół nie ma własnych zabezpieczeń, dlatego nigdy nie łączymy się z nim bezpośrednio. Dane przechodzą przez bramkę lub konwerter na poziomie 2/3.

NA PROJEKT

Historian SQL

Dedykowane konto tylko do odczytu, najlepiej do repliki bazy w DMZ. Żadnego zapisu do bazy produkcyjnej.

Tak fizycznie wyciągamy dane z maszyn bez otwierania hali na świat. Niezależnie od protokołu schemat jest ten sam: tylko odczyt, przez DMZ, bez portów przychodzących do strefy OT. Modbus TCP nie ma własnych zabezpieczeń, dlatego z nim nigdy nie łączymy się bezpośrednio[31].

TRZY MODELE WDROŻENIA

	SaaS chmura co.brick AI	**Hybrid** chmura prywatna lub lokalna klienta	**Private cloud** środowisko klienta
Aplikacja co.brick AI	Chmura co.brick AI	Chmura prywatna lub lokalna klienta	Środowisko klienta
Modele językowe	Biznesowe LLM w chmurze komercyjnej (rezydencja danych w UE) albo lżejsze modele w zasobach co.brick AI	API do biznesowych LLM (rezydencja UE) albo do modeli hostowanych przez co.brick AI	Modele w tenancie chmurowym klienta albo fizycznie u klienta, na serwerach z GPU
Wymagania po stronie klienta	Tylko dostęp do źródeł danych (konektory)	VM Linux/Windows lub Kubernetes, VPN serwisowy, wyjście API do modeli	Jak w hybrid, plus infrastruktura pod modele (GPU w wariancie on-premise)
Gdzie leży baza wiedzy	**Hybrid i private cloud: u klienta. SaaS: wydzielone środowisko co.brick w UE, umowa powierzenia. Ślad pytań zawsze po stronie klienta.**		

Domyślnie nie wymagamy od klienta serwerów z GPU. Są potrzebne tylko wtedy, gdy klient chce uruchamiać modele fizycznie u siebie. Hosting u niezależnego dostawcy, na przykład w polskim centrum danych, nie jest osobnym modelem, tylko lokalizacją: jeśli usługa działa na umowie co.brick AI, to jest SaaS, jeśli na umowie klienta, to private cloud. Edge AI, czyli modele uruchamiane przy maszynach, nie należy dziś do standardowych wariantów[31].

TRZECH CYFROWYCH EKSPERTÓW

assist
INŻYNIER WIEDZY

Firmowa baza wiedzy z AI: DTR, instrukcje, procedury, historia serwisowa. Każda odpowiedź ze wskazaniem źródła. Wykrywa sprzeczności, luki, nieaktualne artykuły i dane osobowe.

do 2x szybszy onboarding

observe
STRAŻNIK MASZYN

Telemetria z maszyn i linii w jednym miejscu. Asystent odpowiada o stan parku maszynowego w języku naturalnym. Raporty z danych źródłowych, nie z Excela.

mniej awarii, krótszy MTTR

resolve
PARTNER SERVICE DESKU

AI dla service desku UR i obsługi klienta: zgłoszenie, diagnoza, rozwiązanie z historii podobnych przypadków. AI proponuje, operator zatwierdza. Pełny ślad audytowy.

do 40% krótszy czas zgłoszeń

assist: inżynier wiedzy. *Firmowa baza wiedzy z AI: DTR, instrukcje, procedury, historia serwisowa. Każda odpowiedź ze wskazaniem źródła. Sam wykrywa sprzeczności, luki i nieaktualne artykuły oraz dane osobowe w dokumentacji. Do dwóch razy szybszy onboarding nowych ludzi.* **observe: strażnik maszyn.** *Telemetria z maszyn i linii w jednym miejscu oraz asystent, który odpowiada na pytania o stan parku maszynowego w języku naturalnym. Pomaga ograniczać awarie i skracać czas naprawy; raporty z danych źródłowych, nie z Excela.* **resolve: partner service desku.** *AI dla service desku utrzymania ruchu i obsługi klienta: zgłoszenie, diagnoza, rozwiązanie z historii podobnych przypadków. AI proponuje, operator zatwierdza. Krótszy czas obsługi zgłoszeń, z pełnym śladem audytowym.*

CO ASSIST ROBI ZE STRONĄ 214, KTÓRĄ MAREK FOTOGRAFOWAŁ TELEFONEM?

WIELE ŹRÓDEŁ

Jedna baza z wielu systemów.

assist pracuje równolegle z systemami różnych dostawców i łączy rozproszone informacje w jeden uporządkowany ekosystem, bez uzależnienia od jednego dostawcy.

NIE TYLKO TEKST

Schematy i wykresy też.

System analizuje schematy i wykresy osadzone w dokumentacji technicznej. Tabela kodów błędów ze strony 214 przestaje być zdjęciem w telefonie.

IZOLACJA

Osobno dla linii, osobno dla działów.

Dane są oddzielone na poziomie kolekcji: technolog nie widzi tego, co utrzymanie ruchu, jeśli tak ustalicie. Dostęp według ról.

W TLE

Skanowanie przyrostowe.

Nowe dokumenty można weryfikować od razu po dodaniu. System wykrywa sprzeczności, luki, nieaktualne artykuły i dane osobowe.

Za dokumentację odpowiada moduł assist: przejmujemy import, wektoryzację i utrzymanie bazy, a porządkowanie dokumentacji robimy razem z Wami. Dane z systemów CMMS można włączyć w ramach projektu, przez eksport lub integrację[31]. O 2:40 Marek nie fotografuje DTR. Pyta o kod F-27 i dostaje odpowiedź ze stroną, wersją dokumentu i odnośnikiem do schematu w dokumentacji.

MATRYCA: JAK MAPUJEMY PROBLEMY FABRYKI

	assist inżynier wiedzy	**observe** strażnik maszyn	**resolve** partner service desku
Główny ból UR / HR	Utrata wiedzy eksperckiej, powolny onboarding	Nieprecyzyjne raporty OEE, ukryte mikroprzestoje	Przeciążenie inżynierów trywialnymi zgłoszeniami
Akcja AI	Zamiana know-how w jedno źródło prawdy	Twardy monitoring 24/7 plus łączenie z DTR	Tarcza ochronna i automatyczne podpowiedzi
Mierzalny ROI	**Bezpieczeństwo organizacyjne mimo rotacji kadr**	**Wykrywanie ukrytych strat produkcyjnych**	**Drastyczne skrócenie MTTR, większa przepustowość**
Zamyka shadow AI	Anna nie wkleja receptury: pyta o nią u siebie	Marek nie musi wklejać logów: system już je ma	Kod błędu ma odpowiedź w sekundy, ze źródłem

CO Z TEGO WYNIKA DLA WASZEGO ZAKŁADU?

DLA AUTOMATYKÓW

Wdrożenie nie dotyka sterowania.

Zasada „zero zapisu do OT" nie jest obietnicą handlową, tylko architekturą: co.brick AI stoi na poziomach 3 i 4, czyta przez DMZ i nie ma uprawnień ani połączenia, przez które mogłoby cokolwiek zmienić w sterowniku. To kończy najczęstszy spór między IT a utrzymaniem ruchu, zanim się zacznie.

DLA IT I BEZPIECZEŃSTWA

Cały przepływ da się narysować na modelu Purdue.

Żadnych nowych portów przychodzących do OT, jeden punkt odbioru w DMZ, wyjście do modeli tylko z poziomu 4. To jest dokładnie ta mapa, o którą zapyta audytor KSC i o którą prosi sekcja 08 w wymaganiu drugim. Tu jest gotowa.

DLA ZARZĄDU

Wybór modelu wdrożenia to decyzja o umowie i lokalizacji, nie o serwerach z GPU.

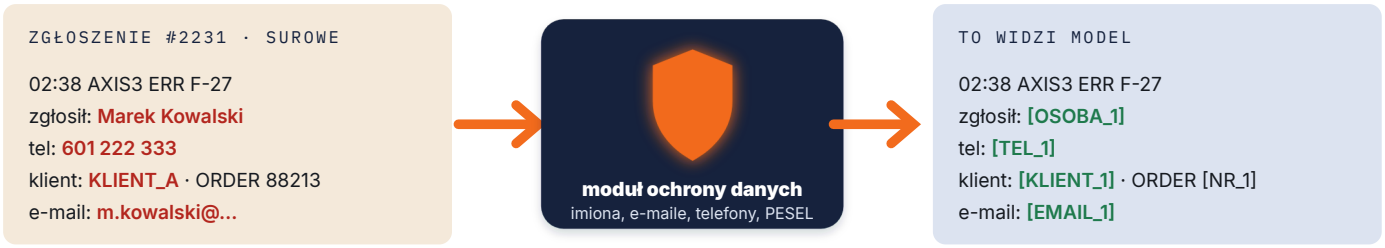
W SaaS po Waszej stronie potrzebne są tylko konektory do źródeł danych. Hybrid wymaga VM i VPN, które IT ma i tak. Private cloud jest dla tych, którzy chcą model fizycznie u siebie. W hybrid i private cloud baza wiedzy zostaje u Was; w SaaS w wydzielonym środowisku co.brick w UE, na umowie powierzenia. Ślad pytań w każdym wariancie należy do firmy.

DLA MARKA

Strona 214 jest w bazie, razem ze schematem.

assist zwektoryzował DTR, instrukcje i historię napraw z wielu systemów naraz. O 2:40 Marek pyta o kod F-27, dostaje odpowiedź ze stroną, wersją dokumentu i odnośnikiem do schematu, a jego pytanie zostaje w firmie. Nie fotografuje niczego telefonem.

OCHRONA DANYCH: CO WIDZI MODEL



Tokeny wracają do postaci czytelnej dopiero po Waszej stronie. Kto pytał, o co i na jakiej podstawie: w Waszym logu.

Ochrona danych. *Moduł ochrony danych w assist wykrywa dane osobowe w dokumentacji i zgłoszeniach (m.in. imiona i nazwiska, adresy e-mail, numery telefonów i PESEL) i zastępuje je tokenami, zanim fragment trafi do modelu. Dostęp do danych według ról. Każde pytanie zostawia ślad po Waszej stronie: kto pytał, o co i na podstawie jakich źródeł. Dla RODO i NDA liczy się właśnie ten ślad, a nie obietnica.*

OD TEORII DO PRAKTYKI W SZEŚĆ TYGODNI

do 40%
krótszy czas rozwiązywania zgłoszeń
POMIARY U KLIENTÓW CO.BRICK

do 2x
szybszy onboarding nowych ludzi
POMIARY U KLIENTÓW CO.BRICK

do 90%
mniej czasu na szukanie wiedzy
POMIARY U KLIENTÓW CO.BRICK

1 Audyt i NDA
TYDZIEŃ 1–2
mapa danych, granica OT/IT, kryteria sukcesu na piśmie

2 Zwinne wdrożenie
TYDZIEŃ 3–5
import dokumentacji, konektory, pilot na jednej linii

3 Działające MVP
TYDZIEŃ 6
mierzony czas odpowiedzi, ślad pytań, decyzja o skali

Liczby pochodzą z pomiarów u klientów co.brick; punkt odniesienia to stan sprzed wdrożenia. Sześć tygodni od NDA do działającego MVP na testowej linii, z kryteriami sukcesu podpisanymi przed startem.

KTO ZA TYM STOI?

Ludzie z hali, nie z prezentacji.

Zespół co.brick wdrażał systemy w zakładach produkcyjnych i zna różnicę między demo a trzecią zmianą. Projektujemy narzędzia dla Marka i Anny, nie dla slajdu.

Zespół, który zbudował Hybris.

Założyciele co.brick współtworzyli hybris, platformę e-commerce klasy enterprise przejętą przez SAP w 2013 roku. Wiemy, jak buduje się oprogramowanie na dekadę, nie na kwartał.

> “

Przekaz dla działów OT jest prosty: co.brick AI tylko czyta dane.

Współpraca z firmą Miary i Wagi.

Pracujemy z firmami, dla których precyzja pomiaru i integralność danych są podstawą biznesu, w tym z firmą Miary i Wagi. Tam nie ma danych, które wyciekły „tylko trochę".

Przestańmy teoretyzować o AI.

Godzinna konsultacja architektury IT/OT z inżynierami co.brick, bez zobowiązań, dla pięciu pierwszych firm, które chcą uwolnić potencjał danych bez ryzyka dla IP. Porozmawiajmy, zanim zrobią to Wasze dane.

Daniel Stram

HEAD OF SALES, CO.BRICK

Rozmawia z zarządami i kierownikami zakładów o tym, co AI może zmienić na hali w kwartał, a czego nie zmieni w dekadę.

LinkedIn

daniel.stram@cobrick.com

Jakub Duda

CTO CO.BRICK AI

Odpowiada za architekturę platformy co.brick AI: granicę OT/IT, modele wdrożenia i to, żeby AI na hali tylko czytała dane, a decyzje zostawiała ludziom.

LinkedIn

cobrick.com

Daniel Stram jest Head of Sales, a Jakub Duda CTO co.brick AI, polskiej firmie budującej systemy AI dla przemysłu, w których warstwa sterowania pozostaje nietknięta, a baza wiedzy, dokumentacja i ślad pytań pozostają pod kontrolą klienta. Marek i Anna są postaciami zbudowanymi z sytuacji opisanych w cytowanych badaniach. Żadne dane klientów co.brick nie zostały wykorzystane. Liczby do 40%, do 2x i do 90% pochodzą z pomiarów u klientów co.brick.

ŹRÓDŁA

1. Cloud Security Alliance, *Shadow AI Infrastructure: The Invisible Enterprise Attack Surface* (11.05.2026) i *Shadow AI Apps* (30.05.2026); w tym EchoLeak CVE-2025-32711 i incydent UNC6395.
2. Ojowa A., Marques M., Gonçalves A., *Shadow AI in Organisations: A Practical Framework for Detection, Risk Classification, and Governance*, Preprints.org, 28.02.2026. Preprint, nierecenzowany.
3. Petersson L., Irgang L., Mauritzon I., Holmén M., *Shadow AI in Swedish Health Care*, J Med Internet Res 2026;28:e93484. n = 357.
4. Baruwal Chhetri M. i in. (CSIRO), *From Frontier to Shadow AI: A Simmering Threat to Assurance and Security in Critical Infrastructure*, arXiv:2606.00088, 23.05.2026. 32 wywiady, 27 organizacji.
5. Microsoft & LinkedIn, *Work Trend Index 2024*, n = 31 000, 31 krajów.
6. PagerDuty / Wakefield Research, *2026 Shadow AI Survey*, n = 1 250, czerwiec 2026, firmy powyżej 500 mln USD, bez ról IT.
7. Harmonic Security, *What 22 Million Enterprise AI Prompts Reveal About Shadow AI in 2025*, 15.01.2026.
8. IBM / Ponemon Institute, *Cost of a Data Breach Report 2026* (29.07.2026), n = 602 organizacje; dane o kradzieży IP i 178 $ za rekord z edycji 2025, n = 600.
9. LayerX, *Enterprise GenAI Security Report 2025* i *Browser Security Report 2025*.
10. Salesforce, *State of the AI Connected Worker* 2024, cyt. za Axis Intelligence.
11. Kıyak Y.S., Coşkun Ö., Budakoğlu I.İ., *"ChatGPT can make mistakes" warnings fail: a randomized controlled trial*, Med. Educ. 60, 2026.
12. Netskope Threat Labs, *Cloud and Threat Report 2026* (telemetria X 2024 do X 2025) oraz *Threat Labs Report: Japan 2026* (dane o kontach prywatnych i firmowych).
13. Unseen Security, *2026 State of Shadow AI*, cyt. za CSA.
14. Areebi Research, *The Shadow AI Index*, opublikowany w maju 2026 (w tytule „Q3 2026"). Synteza wtórna; autorzy ujawniają interes handlowy.
15. KPMG / University of Melbourne, *Trust, attitudes and use of AI 2025*; polska edycja *Sztuczna inteligencja w Polsce. Krajobraz pełen paradoksów*. Polska n = 1 082.
16. AMP, badanie z I półrocza 2025, opublikowane 10.12.2025. Wielkość próby nieujawniona.
17. Marnic D., *Shadow AI w dziennikarstwie. Między etosem a algorytmizacją*, Media Biznes Kultura 1(20), 2026.
18. PARP, *Czym jest shadow AI i czy firmy powinny się go obawiać?*, 11.04.2025 (przypadek Samsung, CybSafe 2024).
19. Wąsiołek-Bartusik M., *Shadow AI: czym jest i jak zagraża firmie?*, Polski Przemysł, 13.08.2026.
20. Microsoft UK, październik 2025, cyt. za Axis Intelligence.
21. Nemure i in., *Shadow AI as an evolution of the insider threat paradigm* (model constructive-intent threat), International Journal of Computer Applications, 2026.
22. Sharp Europe, badanie kadry zarządzającej w Europie, cyt. za Polski Przemysł 2026. Próba nieustalona.
23. CB Financial, raport 8-K do SEC z 7.05.2026, cyt. za CSA / Axis Intelligence: pierwsze ujawnienie giełdowe z powodu shadow AI.
24. ISACA, *AI Pulse Poll*, maj 2026, n = 3 400+.
25. Rozporządzenie (UE) 2024/1689 (AI Act) w brzmieniu po nowelizacji „Digital Omnibus AI", w mocy od 27.07.2026: kary za praktyki zabronione od 2.08.2025, art. 50 i nadzór nad modelami ogólnego przeznaczenia od 2.08.2026; załącznik III od 2.12.2027; załącznik I od 2.08.2028; art. 4 w nowym brzmieniu.
26. Ustawa z 3.07.2026 o systemach sztucznej inteligencji, Dz.U. 2026 poz. 1003 (KRiBSI, piaskownice, skargi, kary według AI Act) oraz ustawa z 23.01.2026 o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, Dz.U. 2026 poz. 252, w mocy od 3.04.2026 (wdrożenie NIS2: wykaz podmiotów do 3.10.2026, system zarządzania bezpieczeństwem informacji do 3.04.2027).
27. Bloomberg, *Samsung Bans ChatGPT, Google Bard, Other Generative AI Use by Staff After Leak*, 2.05.2023.
28. OpenAI, *On the Navier-Stokes Millennium Prize Problem*, 8.09.2026, oświadczenie o danych użytkowników z późniejszymi aktualizacjami (10.09 i 13.09.2026).
29. Buckmaster T., oświadczenie z 7.09.2026.
30. Axios, *OpenAI's historic math solution overshadowed by credit controversy*, 8.09.2026.
31. co.brick AI, *Odpowiedzi na pytania techniczne: topologia sieci (model Purdue), infrastruktura obliczeniowa, protokoły i strumienie danych, format bazy wiedzy*, materiał wewnętrzny, wrzesień 2026.