

SNOK

PRZEGLĄD TYGODNIA W48

Rachunek za AI

Przegląd SNOK za 20-26 listopada 2026: doniesienia o redukcji etatów w SAP, Kingfisher na SAP ECC, Onapsis o kodzie z AI, SAP Joule Work, UiPath dla agentów kodujących, Gartner o incydentach agentów, Cairn według AWS, Kongres USA o chińskich modelach, Nvidia, Autopay i ePUAP

Przesuń →

20-26.11.2026

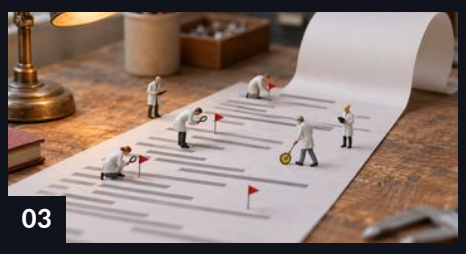
Bloomberg napisał, że SAP rozważa likwidację co najmniej 10 000 stanowisk w restrukturyzacji związanej z AI. Kingfisher buduje AI na danych z SAP ECC zamiast płacić za migrację, a w DoorDash wymiana jednego modelu może zająć do sześciu miesięcy. AI coraz częściej przychodzi z kwotą i terminem.

W badaniu Gartnera 95% z 298 liderów infrastruktury i operacji IT wskazało incydent z agentem AI, a wyłączniki agentów ma 15% organizacji. Według OpenAI exploit jądra Linuksa kosztował średnio 1 279 USD w kredytach API. Koszt znalezienia luki da się już podać w dolarach, a koszt zarządzania agentami dopiero zaczynamy liczyć.

Pełna wersja ze źródłami jest na snok.ai, we wpisie „Rachunek za AI”.

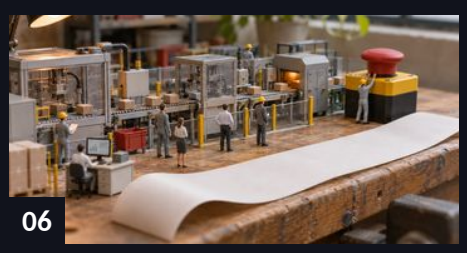

01

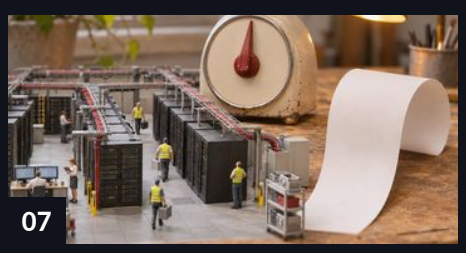

02


03

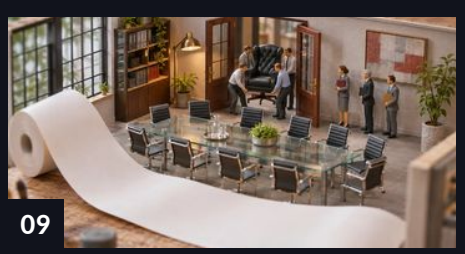

04


05


06


07


08


09


10


11



SAP rozważa likwidację co najmniej 10 000 stanowisk

Według Bloomberga z 26 listopada SAP rozważa likwidację co najmniej 10 000 stanowisk, co najmniej 9% załogi, w restrukturyzacji związanej z AI. Liczba może się zmienić po negocjacjach z przedstawicielami pracowników. SAP niczego nie potwierdził; na koniec września zatrudniał 113 076 osób w przeliczeniu na pełne etaty.

Jeśli redukcja obejmie sprzedaż i zespoły obsługujące klientów, firmom może ubyć kontaktów po stronie SAP w czasie decyzji o migracji.

WNIOSEK

Sprawdziłbym, które eskalacje, rozmowy licencyjne i wsparcie migracji opierają się dziś na jednej osobie po stronie SAP.

Źródło: Bloomberg i CNBC, 26-27.11.2026; SAP Q3 2026



02 / 11 SAP

PwC i Kingfisher: AI w rozmowie o migracji SAP

PwC mówi w The Register, że AI coraz częściej staje się argumentem za migracją, bo do starszych systemów trudniej je zastosować. Kingfisher w 2025 roku odrzucił przejście z SAP ECC na SAP S/4HANA, przeniósł ECC do Google Cloud, wsparcie oddał Rimini Street, a AI buduje na danych z ERP.

Podstawowe utrzymanie SAP ERP 6.0 kończy się z końcem 2027 roku, a opcjonalne rozszerzone, za dopłatą dwóch punktów procentowych, trwa do końca 2030.

WNIOSEK

Rozmowę zacząłbym od procesu i danych dla AI, a przy pozostaniu na ECC ustaliłbym, kto dostarczy poprawki bezpieczeństwa.

Źródło: The Register, 20.11.2026; SAP Support



Onapsis o kodzie generowanym przez AI w SAP

Onapsis podaje, że od 41% do 62% kodu generowanego przez AI zawiera podatności, nie wskazując badań i nie zawężając liczb do ABAP. Proponuje kontrole w środowisku programisty (SAP Build Code, SAP Joule), w repozytorium (ATC, SCI) i w potoku wdrożeń (SAP TMS, SAP ChaRM).

Trzy punkty kontroli mają sens bez względu na to, ile z tego zakresu dotyczy ABAP: jeśli asystent AI przyspiesza pisanie kodu, przegląd dopiero przed transportem może nie nadążyć.

WNIOSEK

Pierwszy test: czy reguły ATC obejmują kontrole bezpieczeństwa i uruchamiają się przy każdym zatwierdzeniu zmiany.

Źródło: Onapsis, 20.11.2026



SAP Joule Work i agenci z SAP BTP

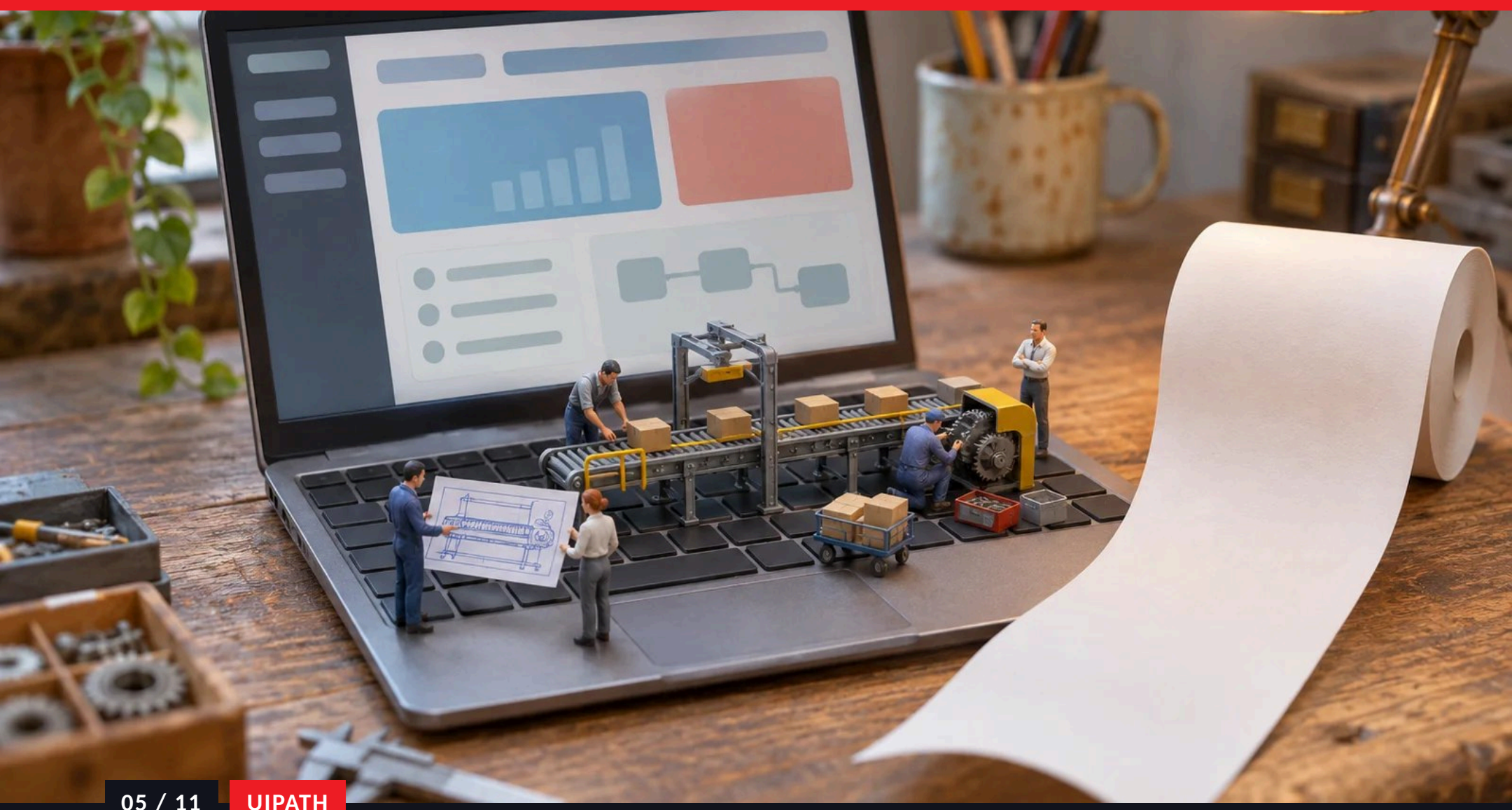
SAP łączy Joule Work z Microsoft Work IQ, którego funkcje wchodzą etapami: agenci z Copilot Studio mają przekazywać zadania agentom Joule. W Joule Work agent działa w środowisku zarządzanym przez SAP, ale dziś sięga tylko do systemów SAP połączonych w ramach formacji. Systemy innych firm, on-premise i SAP BW są poza zasięgiem.

Ekspert SAP radzi, żeby duże systemy agentowe zostawić na koncie BTP klienta i poczekać na A2A.

WNIOSEK

Przed przeniesieniem agentów policzyłbym, ile ich połączeń prowadzi do systemów spoza SAP albo on-premise.

Źródło: SAP News Center, 20.11; SAP Community, 23.11.2026



05 / 11 UIPATH

UiPath dla agentów kodujących: Skills, CLI uip i Maestro

Społeczność UiPath ogłosiła na 12 grudnia spotkanie o budowaniu automatyzacji w Claude Code. UiPath Skills to pakiety instrukcji instalowane poleceniem uip, dla Claude Code, Cursora, GitHub Copilot, Gemini, Codex i OpenCode. Repozytorium działa od stycznia i obejmuje także UiPath Maestro.

Agent kodujący buduje z ich pomocą automatyzacje UiPath bezpośrednio z Claude Code albo Cursora. Moim zdaniem rośnie przez to znaczenie miejsca, w którym automatyzacja trafia pod kontrolę.

WNIOSEK

Przed pierwszą automatyzacją z agenta kodującego ustaliłbym, kto zatwierdza schemat procesu w UiPath Maestro.

Źródło: Dokumentacja UiPath; GitHub UiPath/skills; forum UiPath



06 / 11 AI SECURITY

Gartner: incydent z agentem AI w 95% badanych organizacji

W badaniu 298 liderów infrastruktury i operacji IT z USA i Wielkiej Brytanii 95% wskazało incydent związany z agentem AI w swojej organizacji w ciągu roku. 70% uważa, że agenci działają w bezpiecznych granicach, a automatyczne wyłączniki agentów ma 15%. Komunikat nie definiuje incydentu.

Gartner zaleca inwentaryzację agentów i traktowanie ich jak tożsamości maszynowych.

WNIOSEK

Zacząłbym od listy agentów, ich uprawnień i osoby, która może każdego z nich zatrzymać.

Źródło: Gartner, 16.11.2026



Cairn według AWS i koszt exploita według OpenAI

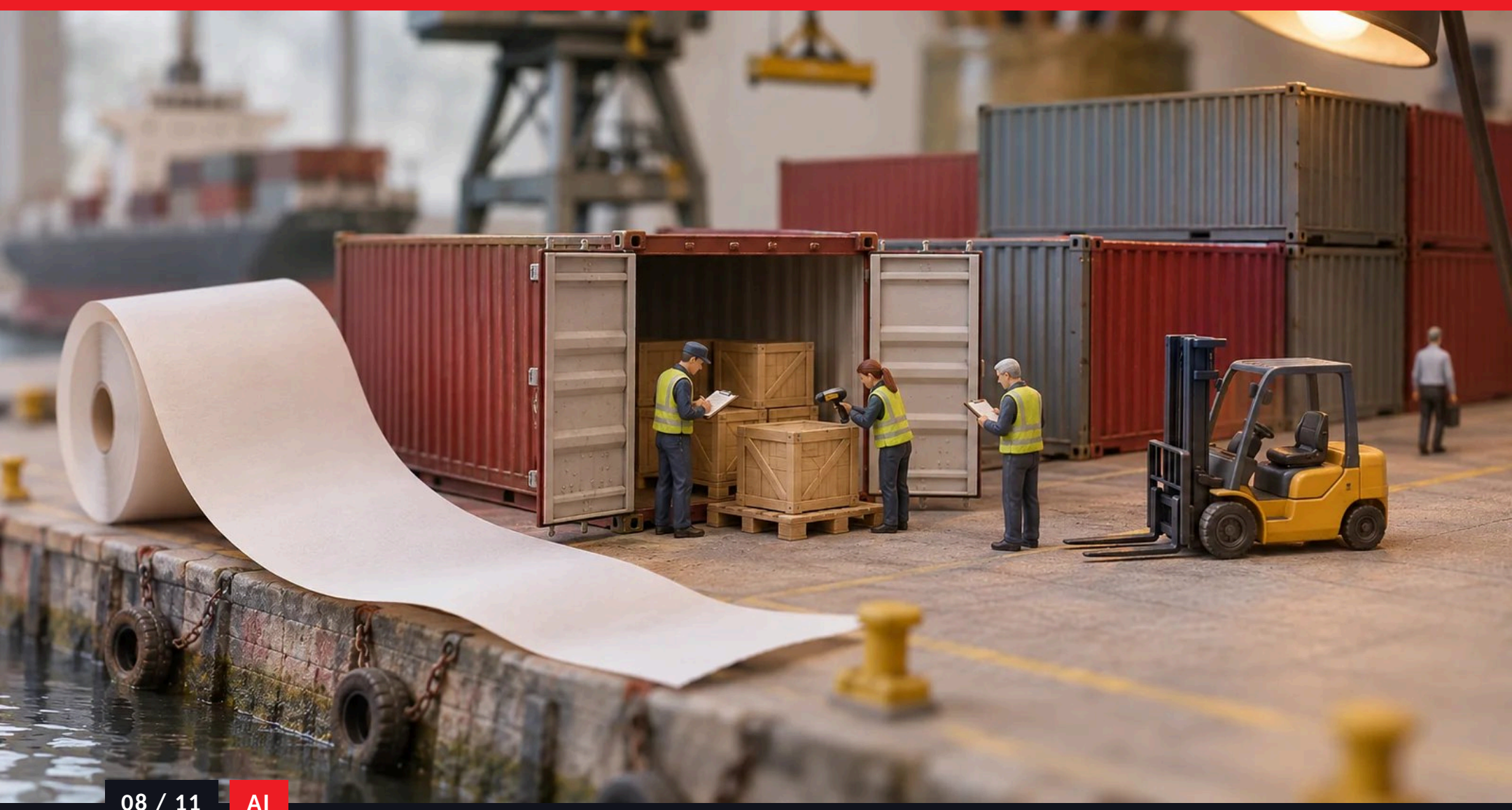
AWS opisał agentów frameworka Cairn, których używał sprawca wiązany przez AWS z Chinami z umiarkowaną pewnością. Od mapowania API aplikacji AI do obrazowania medycznego do zapisu dowolnych plików doszli w około 11 minut, a później uzyskali uprawnienia root. AWS z wysoką pewnością ocenia lukę jako wcześniej nieznaną.

OpenAI podało 4 listopada, że analiza jądra Linuksa jego modelem kosztowała średnio 1 279 USD w kredytach API na działający exploit.

WNIOSEK

Pierwsza lista do przejrzenia: aplikacje AI przyjmujące pliki od użytkowników są osiągalne z internetu.

Źródło: AWS Security Blog, 20.11.2026; OpenAI, 4.11.2026



Kongres USA o chińskich modelach open weight w firmach

Raport dwóch komisji Izby Reprezentantów opisuje Airbnb z modelami Qwen w obsłudze klienta, model Composer 2 w Cursorze zbudowany na Kimi K2.5 i DoorDash, gdzie wymiana jednego modelu może zająć do sześciu miesięcy. Rekomenduje standard pochodzenia modeli i wykaz komponentów AI.

Rekomendacje komisji nie są wiążące. Pochodzenie modelu staje się jednak pytaniem z audytu dostawcy.

WNIOSEK

Spisałbym modele w narzędziach i produktach firmy, łącznie z bazowymi tam, gdzie dostawca je podaje.

Źródło: Raport komisji Izby Reprezentantów, 20.11.2026



09 / 11 RYNEK

Nvidia przywraca Jensena Huanga po 11 dniach

23 listopada rada Nvidii przywróciła Huanga na stanowiska prezesa, CEO i członka rady, a przewodniczącym rady pozostaje Harvey C. Jones. Według Decrypt senacka komisja bankowa wyznaczyła przesłuchanie Huanga na 3 grudnia.

Już 17 listopada rada powołała komitet ds. bezpieczeństwa narodowego i kontroli eksportu, więc kontrola eksportu staje się w Nvidii sprawą zarządu.

WNIOSEK

Plan zakupów sprzętu na 2027 rok powinien zakładać dłuższe terminy dostaw i wariant zapasowy.

Źródło: Nvidia, 12.11, 17.11 i 23.11.2026; Decrypt



Autopay: nieautoryzowany dostęp i możliwy wyciek danych kart

Autopay stwierdził 11 listopada nieautoryzowany dostęp do infrastruktury. Według spółki napastnicy mogli uzyskać adresy e-mail, telefony podane przy doładowaniach, adresy IP i dane kart. Spółka nie potwierdziła skopiowania danych, ale tego nie wyklucza, i ocenia, że atak nosił cechy automatyzacji wspieranej przez AI.

Bank spółdzielczy pisał o ponad 22 tys. rekordów danych kartowych, ale nie wymienia Autopay.

WNIOSEK

Umowa z operatorem płatności powinna mówić, jakie dane klientów przechowuje i kiedy powiadomi o incydencie.

Źródło: Niebezpiecznik i CRN.pl, 19.11.2026; BS Sochaczew, 18.11.2026



ePUAP: dziewięć dni ograniczonego działania

Ministerstwo Cyfryzacji przywróciło 19 listopada pełne działanie ePUAP po incydencie wykrytym 10 listopada. Analizę prowadzono z udziałem NASK i ABW. Ministerstwo nie znalazło śladów rozszerzenia ataku poza zidentyfikowany obszar.

Na pytanie o dostęp do danych COI nie odpowiedziało. Przestój platformy, przez którą firmy składają pisma, to koszt liczony w terminach.

WNIOSEK

Sprawdziłbym, czy firma ma opisaną procedurę awaryjną na wypadek przestoju ePUAP, a skutki prawne omówiłbym z prawnikiem.

Źródło: Ministerstwo Cyfryzacji, 19.11.2026; Sekurak

PRZED BUDŻETEM NA 2027

Pięć spraw do rozstrzygnięcia przed budżetem na 2027 rok

Pytania wynikają z pozycji tego przeglądu.

1. Którzy agenci AI działają w Waszej firmie, kto jest właścicielem każdego z nich i kto może go zatrzymać?
2. Czy reguły ATC sprawdzają bezpieczeństwo kodu ABAP przy każdej zmianie, także pisanej z asystentem AI?
3. Jakie modele, łącznie z bazowymi, działają w Waszych narzędziach i ile trwałaby wymiana jednego z nich?
4. Które aplikacje AI przyjmujące pliki od użytkowników są osiągalne z internetu?
5. Jak wygląda procedura awaryjna, gdy ePUAP albo operator płatności przestanie działać na tydzień?

Pełna wersja ze źródłami: **snok.ai**, wpis „Rachunek za AI”. Kontakt: office@snok.ai

Grafiki wygenerowane z pomocą AI. Stan wiedzy na 27.11.2026. Tekst nie jest poradą prawną, podatkową ani inwestycyjną.