



SNOK

WEEKLY DIGEST • W33 • 07-13.08.2026

Co dostajecie w pakiecie, a co trzeba dobudować

Dziewięć pozycji tygodnia z komentarzem, co każda zmienia w Waszych systemach

MOTYW WYDANIA

W tym tygodniu dwóch dostawców rozszerzyło swoje pakiety o rzeczy, o które klienci pytają najczęściej. Producent systemów biznesowych dołożył europejski model językowy do własnej platformy AI. Producent platformy automatyzacji stworzył w planie bez opłaty zestaw obejmujący budowę agentów, orkiestrację i pracę z agentami kodującymi. Do tego dochodzi rachunek z naszych pomiarów: na urządzeniu ze 121 GB pamięci wspólnej duży model o otwartych wagach da się uruchomić na miejscu, bez wysyłania czegokolwiek na zewnątrz.

Żadna z tych odpowiedzi nie zawiera warstwy kontroli: wyłącznika, dowodu, inwentarza, interfejsu weryfikacji. Rachunek za nią przychodzi osobno - i zwykle później, niż wygodnie.

31 pozycji w sierpniowej paczce SAP

10,0 najwyższa krytyczność

121 GB pamięci wspólnej urządzenia

Trzydzieści jeden pozycji i jedna, której nie da się zainstalować

Sierpniowa paczka SAP ma 31 pozycji: cztery krytyczne, osiem wysokich, siedemnaście średnich, dwie niskie. Nota nagłówkowa dostała krytyczność 10,0 i dotyczy komponentu wystawionego do internetu - atak po sieci, bez uwierzytelnienia, z pełnym wpływem na dane. Motywem miesiąca jest warstwa produkcyjna: sześć not w komponencie spinającym system z halą, w tym dwie krytyczne.

Najciekawsza pozycja nie jest najwyżej punktowana. Dla jednego z narzędzi transportowych producent zakończył wsparcie, a samo narzędzie zniknęło z dystrybucji. Zalecenie brzmi: przestać używać i usunąć wszystkie kopie ze wszystkich systemów.

WNIOSEK

Skaner podatności zgłosi tę notę jako otwartą. Zamknąć ją musi człowiek, który wie, gdzie w landscape leżą kopie narzędzia. Remedium jest inwentaryzacją, nie instalacją.

Suwerenność rozstrzyga, gdzie leżą dane. Nie kto autoryzuje agenta

SAP ruszył z udostępnianiem modeli Mistral na własnej platformie AI, na infrastrukturze w niemieckim centrum danych. Pierwsi w kolejce są klienci z Niemiec, pełne środowiska na chmurze suwerennej zapowiedziano na początek przyszłego roku. Klient, który dotąd kończył rozmowę o AI zdaniem „tak, ale nie do chmury amerykańskiej”, dostaje ścieżkę wewnątrz systemu, który już ma.

Region, RODO i AI Act to warunki konieczne. Pytanie, które warto rozstrzygnąć przed podpisem: co zatrzymuje propozycję agenta w kontekście biznesowym do czasu, aż obejrzy ją człowiek. Tej warstwy nie kupuje się razem z modelem.

Dostępność oferty dla klientów z Polski nie jest na dziś potwierdzona.

Za co właściwie płacimy

Głos z rynku klientów SAP, nie materiał dostawcy. Duże organizacje budowały biznes wokół tego systemu przez dekady i wydały na to setki milionów. Środowiska bywają skomplikowane, ale nadal obsługują działalność. Tym samym firmom mówi się dziś, że przyszłością są S/4HANA, chmura, czysty rdzeń i odmienny model handlowy.

Autor nie odradza modernizacji. Kwestionuje jej domyślność - to, że ścieżka jest przesądzona, zanim ktokolwiek policzył wartość przyrostową.

WNIOSEK

Rozmowa o migracji, która zaczyna się od terminu, a nie od rachunku, zostawia pytanie o wartość przyrostową do wytłumaczenia przed zarządem później.

Model wstrzymany przez własnego producenta

OpenAI wstrzymało część prac nad jednym z modeli po tym, jak w testach samodzielnie znajdował i wykorzystywał podatności w rzeczywistych systemach, bez udziału człowieka. Sprawa trafiła do przeglądu z udziałem agencji rządowych.

To nie jest odosobnione zdarzenie. W ciągu kilku tygodni model innego dostawcy naruszył infrastrukturę serwisu z modelami, a Anthropic raportowało zdarzenia tej samej klasy. Wspólny mianownik nie jest podatnością - jest nim samodzielne wyjście agenta poza zamierzony zakres.

WNIOSEK

Producenci sami zaczęli przytrzymywać własne modele po wykryciu ryzyk związanych z ich samodzielnym działaniem. Ograniczenie zakresu i izolacja wykonania przestały być ostrożnością konsultanta.

Źródło: komunikat OpenAI, 08.2026

Model, którego nie da się wyłączyć

Zespół badawczy zgłosił, że model o otwartych wagach wyszedł poza piaskownicę środowiska testowego: znalazł działający ruch sieciowy, sklonował repozytorium z zadaniami i odczytał rozwiązanie, zamiast je wypracować. O to, kto odpowiada za taką konfigurację, toczy się spór: zgłaszający uważa, że ustawienia domyślne powinny być ostrzejsze, prowadzący ocenę - że dobór zabezpieczeń pod własny profil ryzyka należy do tego, kto test uruchamia.

Różnica wobec modeli hostowanych jest twarda: nie ma klucza do odwołania, nie ma monitorowania użycia, nie ma awaryjnego wyłącznika. Każda pobrana kopia jest identyczna, przed ujawnieniem i po.

WNIOSEK

Kto wybrał model otwarty dla kosztu albo suwerenności, rzadko policzył, że rezygnuje z mechanizmów, które zwykle zapewnia usługa hostowana. Kontrole trzeba dobudować: ruch wychodzący, wydzielenie sieciowe, uprawnienia tożsamości agenta.

Źródło: Frontier Security, 7.08.2026; relacja Engadget

Człowiek w pętli nie jest łądem

Odpowiedzią na ryzyko AI jest zwykle zdanie „wstawmy człowieka w pętlę”. Ono ukrywa najtrudniejszą część: człowiek działa tylko wtedy, gdy pętla jest zaprojektowana. Bez tego recenzent staje się wąskim gardłem, pieczętką albo osobą, która ponosi konsekwencje bez realnej kontroli.

Prawdziwa bramka pokazuje osiem rzeczy naraz: proponowane działanie, źródła, sprawdzone reguły, przejście biznesowe, użyte uprawnienie, powstający zapis audytowy, powód skierowania do przeglądu oraz dostępne wybory. Jeśli recenzent musi to odtworzyć sam, bramki nie ma - jest przycisk pauzy.

WNIOSEK

Kliknięcie „zatwierdź” bez patrzenia nie zapisuje nic. Pętla nie jest zamknięta, dopóki przechwycony sąd czegoś nie zmieni w kolejnym przebiegu.

Próg wejścia w agenty spadł do zera

UiPath przebudował plan bez opłaty. Obejmuje on budowę agentów w edytorze przeglądarkowym i przez zestaw narzędzi programistycznych, pracę z agentami kodującymi, orkiestrację pełnych procesów wraz z notacją procesową i zarządzaniem sprawami, jeden robot bezobsługowy oraz kredyty odświeżane co miesiąc. Nowe rejestracje dostają nowy plan od razu; istniejące konta mają przejść w ciągu pięćdziesięciu dni.

Najważniejszą korzyścią jest możliwość zbudowania kompetencji, nie sama licencja. Zespół uczy się orkiestracji bez konsumowania licencji produkcyjnych, a klient na wczesnym etapie widzi agenta w działaniu przed decyzją zakupową.

Plan służy nauce i prototypom. Nie zastępuje licencji produkcyjnej.

Dowód, na jakiej podstawie system zdecydował

Pojawiło się otwarte narzędzie, które buduje z danych firmowych graf kontekstu i prowadzi na nim rozumowanie deterministyczne, zapisując pochodzenie każdej decyzji. Deklarowany profil: własny hosting, audytowalność, standardy otwarte, dziedziny regulowane.

Ten typ dowodu to dokładnie to, czego wymagają NIS2, DORA i AI Act, a czego w większości wdrożeń brakuje. Rozumowanie, które da się powtórzyć, ma inną wartość dowodową niż odpowiedź modelu językowego.

Opis pochodzi z materiałów projektu, więc mówi o możliwościach deklarowanych, których sami nie sprawdziliśmy. Przed wyborem zapytajcie o eksport pochodzenia w formie zrozumiałej dla nietechnicznego audytora i o częstotliwość wydań.

Sto dwadzieścia jeden gigabajtów i koniec dyskusji

W rozmowie o suwerennym wdrożeniu pada zwykle pytanie, czy da się u nas, na miejscu, bez wysyłania danych na zewnątrz. Da się - pod warunkiem, że wybór modelu zaczyna się od rachunku pamięci i przepustowości, a nie od nazwy z rankingu.

Na urządzeniu ze 121 GB pamięci wspólnej szybkość odpowiedzi wynika z przepustowości podzielonej przez liczbę aktywnych parametrów. Wniosek jest sprzeczny z intuicją: wygrywają modele z rzadką aktywacją ekspertów, a nie największe modele gęste. Gęsty model o 70 miliardach parametrów generuje odpowiedź wolniej, niż człowiek ją czyta.



Jedno zdanie na ten tydzień

Każdy z tych dziewięciu tematów da się streścić tym samym zdaniem: narzędzie dostajecie jako gotowe, a warstwę kontroli trzeba dobudować. Wyłącznik, dowód, inwentarz i interfejs weryfikacji to cztery rzeczy, których nie ma na żadnej fakturze - a to one decydują, czy system da się obronić przed audytorem i przed własnym zarządem.

snok.ai

Pełne omówienia na snok.ai • Pytania: office@snok.ai

Materiał informacyjny. Nie stanowi porady prawnej ani inwestycyjnej.