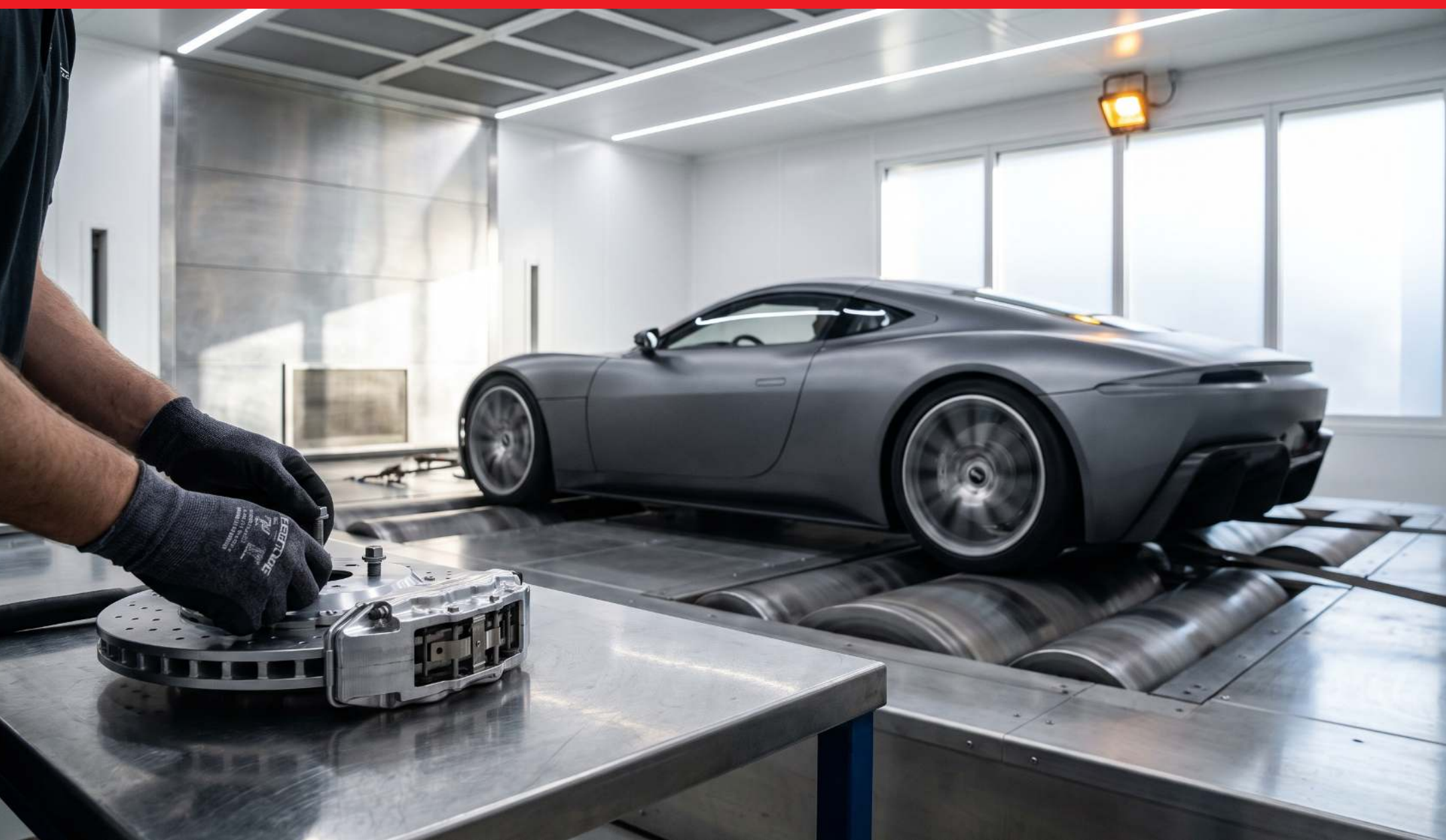




SNOK

WEEKLY DIGEST • W41 • 2-8.10.2026

Gaz do dechy, hamulce w budowie

Przegląd SNOK: agenci AI w SAP, UiPath i Snowflake oraz zabezpieczenia,
które gonią tempo

MOTYW WYDANIA

W tym tygodniu agenci weszli do systemów firmowych z kilku stron naraz. UiPath łączy się ze Snowflake bez kopiowania danych, SAP kupuje graf pracy dla agentów HR i publikuje oficjalną drogę dla agentów spoza SAP, a badacze SAP pokazują model tabelaryczny w roli warstwy decyzyjnej.

Zabezpieczenia powstają w tym samym czasie i są o krok z tyłu. Model decyzyjny Jev zdradza ukryte dane osobowe samym wyborem odpowiedzi, Apple zapowiada twardszą zgodę na pełny dostęp do dysku z powodu agentów, a Gartner przewiduje porzucanie agentów budowanych przez inżynierów dostawców. Hamulce da się dobudować - jeśli ktoś o nich pomyśli przed wyjazdem na drogę.

Tempo wdrożeń

Kontrola w budowie

Kompetencja u klienta

UiPath i Snowflake: dane zostają na miejscu

UiPath ogłosił 30 września dwukierunkową integrację ze Snowflake. Data Fabric czyta dane bezpośrednio w Snowflake, bez kopiowania, Cartographer i Delegate sięgają do Snowflake Cortex, a użytkownik Snowflake CoCo może uruchomić skille agentowe UiPath prosto z platformy danych. Całość orkiestruje UiPath Maestro.

Dane zostają tam, gdzie mają swoje uprawnienia i lineage, a ślad działań agenta zostaje w UiPath. Kierunek jednak się odwrócił: automatyzację można teraz wyzwolić z platformy danych, więc przegląd bezpieczeństwa musi objąć oba kierunki integracji.

WNIOSEK

Mniej kopii danych to mniejsze ryzyko. Ale skille UiPath wywoływane z Snowflake CoCo też potrzebują przeglądu uprawnień przed uruchomieniem.

Dostępność poszczególnych elementów i regiony do potwierdzenia przed wdrożeniem.

Źródło: Komunikat UiPath (Business Wire), 30.09.2026

Połowa organizacji ma agentów w produkcji

UiPath zebrał w czerwcu i lipcu odpowiedzi 1226 osób budujących automatyzację i AI. 53 procent deklaruje agentów w produkcji, kolejne 23 procent jest w pilotażu. Najczęstszą barierą jest bezpieczeństwo lub prywatność danych (40 procent), przed kosztem (39 procent) i trudnością wykazania ROI (31 procent).

W organizacjach używających agentów szeroko pełne, egzekwowane governance deklaruje 72 procent, na etapie oceny - 36 procent. Szerokie użycie agentów idzie w parze z pełnym governance - ankieta nie mówi, co było pierwsze.

WNIOSEK

W grupie z szerokim użyciem agentów pełne governance deklaruje dwa razy więcej organizacji niż wśród tych, które dopiero oceniają agentów.

Badanie producenta: rekrutacja głównie kanałami UiPath, 54 procent respondentów z Azji i Pacyfiku.

SAP przejmuje TechWolf: agent HR potrzebuje grafu

SAP ogłosił 6 października umowę przejęcia belgijskiego TechWolf. Kupuje graf pracy: zadania w stanowiskach, umiejętności ludzi i rynek pracy, budowany z istniejących systemów HR. Ma stać się rdzeniem SAP SuccessFactors i warstwą, na której SAP Joule oprze decyzje w HR. Zamknięcie transakcji planowane jest na czwarty kwartał.

SAP przyznaje wprost, że graf obniża zużycie tokenów i koszt wdrażania agentów HR. Graf umiejętności i zadań to jednak dane osobowe pracowników - kto zobaczy go przez SAP Joule i z jakimi uprawnieniami, trzeba ustalić przed premierą produktów.

WNIOSEK

**Koszt i jakość agenta zależą od kontekstu pod nim.
W HR ten kontekst to dane osobowe, więc
uprawnienia projektuje się od początku.**

Warunki finansowe nieujawnione. Nowe produkty mają powstać po zamknięciu transakcji.

Oficjalna droga dla agentów spoza SAP

SAP Architecture Center opisuje w architekturze „A2A and MCP for Interoperability” trzy ścieżki: Agent Gateway z protokołem A2A dla ruchu do agentów SAP Joule, MCP Gateway w SAP Integration Suite do wystawiania API jako narzędzi oraz A2A przez SAP Integration Suite, które przejmuje uwierzytelnianie, limity i monitoring.

Na górze strony SAP zastrzega, że część elementów nie jest ogólnie dostępna, a dwukierunkowa komunikacja przez Agent Gateway z agentami firm trzecich „is not yet supported”. Bring Your Own Agent obsługuje tylko tekst i 60 sekund w trybie synchronicznym.

WNIOSEK

Mapa daje punkt odniesienia dla każdej architektury. Projekt agenta współpracującego z SAP Joule trzeba jednak oprzeć na stanie obecnym.

Strona nie podaje daty ogólnej dostępności brakujących elementów.

Źródło: SAP Architecture Center, aktualizacja 27.08.2026

Jev kontra SAP RPT: kto podejmie małe decyzje

Badacze SAP porównali na SAP Community model decyzyjny Jev z SAP RPT-1.6, tabelarycznym modelem fundamentowym SAP. Według autorów na zadaniach typed decisions RPT-1.6 osiąga 76,75 procent, Jev 1.13.0 - 72,70 procent. Przy przydziale zgłoszeń: 68,9 wobec 49,4 procent, przy 44 wobec 322 milisekund.

Latencję RPT zmierzono wprost na GPU H200, bez wdrożenia produkcyjnego, a benchmarku zgłoszeń nie da się odtworzyć poza SAP. Ważniejszy jest kierunek: warstwa decyzyjna może działać wewnątrz platformy SAP, nie obok niej.

WNIOSEK

Klienci SAP stają przed wyborem: decyzje wewnątrz platformy albo obok niej. Rozstrzyga pomiar na własnych danych, nie benchmark dostawcy.

Liczby według autorów z SAP. Wpis z 5.10.2026.

Źródło: SAP Community, Technology Blog by SAP, październik 2026

HoneySAP 0.2.0: wabik na CVSS 9,9

OWASP wydał 6 października HoneySAP 0.2.0, honeypot emulujący usługi SAP. Nowa pułapka udaje SAP RFC Gateway i przechwytuje poświadczenia, a wywołania /SLOAE/DEPLOY rozpoznaje jako próby wykorzystania CVE-2025-42957 - wstrzyknięcia kodu ABAP w SAP S/4HANA z oceną CVSS 9,9, łatanego w sierpniu 2025.

W normalnej pracy nikt nie wywołuje tego modułu z zewnątrz, więc każde wywołanie zarejestrowane w pułapce wskazuje na próbę wykorzystania znanej podatności. Łatanie i hardening nie mówią, czy ktoś właśnie próbuje. Honeypot daje tę informację tanio.

WNIOSEK

Łatanie zamyka podatność, honeypot pokazuje, że ktoś jej szuka. To dwie różne informacje i obie przydają się zespołowi SOC.

Narzędzie społecznościowe bez wsparcia producenta. Nie testowaliśmy go.

Źródło: OWASP HoneySAP v0.2.0, GitHub, 6.10.2026

Decyzja Jeva zdradza ukryte dane

Zespół Shanga Wanga sprawdził Jeva jako warstwę decyzyjną aplikacji. Atakujący, który widzi tylko decyzję, parami zapytań z odwróconym warunkiem odtwarzał ukryte w stanie aplikacji płeć, wiek, chorobę serca i pochodzenie - według autorów we wszystkich 200 testowanych stanach. Ukrycie prawdopodobieństw nie pomaga.

Wstrzyknięcia pisane pod Jeva przedstawiały decyzję w co najmniej 97 procentach przypadków, lokalny model dało się zatruć tylnymi drzwiami, a 200 odpowiedzi wystarczyło do wytrenowania modelu zastępczego zgodnego w 92 procentach.

WNIOSEK

**Typowana odpowiedź ogranicza format, nie wyciek.
Decyzję sprawdzamy na zaufanych danych przed
akcją, a pola wrażliwe ograniczamy do niezbędnych.**

Preprint bez recenzji, liczby według autorów.

Źródło: S. Wang i in., arXiv:2610.04985, 4.10.2026

Anthropic otwiera Red Team Access

Anthropic rozszerzył 6 października Cyber Verification Program do trzech poziomów dostępu. Red Team Access zdejmuje blokady modeli Claude dla autoryzowanych pentestów i red teamingu, ale tylko dla organizacji - wniosek rozpatrywany jest kilka tygodni. Specialized Access jest dla testujących systemy krytyczne.

Warunek zmienia rachunek: retencja danych jest obowiązkowa, z wąskim wyjątkiem dla organizacji z zerową retencją w Claude Fable 5.1 albo Mythos 5.1. Przy testach u klientów pod NDA i w reżimie ISO 27001 przesłanie danych z testu do zewnętrznego dostawcy wymaga oceny bezpieczeństwa i zgody klienta.

WNIOSEK

Model bez blokad w autoryzowanym zakresie ma cenę: dane z testu zostają u dostawcy. To decyzja dla Security Officera, nie odruch.

SNOK nie złożył wniosku do programu.

Źródło: Anthropic, 6.10.2026

OWASP FinBot: poligon do atakowania agentów

FinBot to celowo podatna platforma agentowa OWASP, nazwana „Juice Shop for Agentic AI”. System zarządzania dostawcami złożony z kilku agentów trzeba złamać przez prompt injection, nadużycie narzędzi, eksfiltrację danych albo zdalne wykonanie kodu. Wyzwania przyporządkowano do list OWASP Top 10, CWE i MITRE ATLAS.

Platforma wystartowała wiosną i wraca w kampanii OWASP. Daje zespołom budującym agentów miejsce, w którym atak można przećwiczyć bez szkody, zanim ktoś spróbuje go na prawdziwym systemie.

WNIOSEK

Zespół, który nigdy nie próbował złamać własnego agenta, dowie się o jego słabościach od kogoś innego. Lepiej poćwiczyć na poligonie.

Działa w przeglądarce, kod na licencji Apache 2.0.

Źródło: OWASP GenAI Security Project, GitHub

Apple: agenci zmieniają ryzyko dostępu do dysku

Apple opublikował 2 października notę o zmianach w Full Disk Access w macOS i podał powód wprost: „As AI agents become increasingly capable and autonomous, the risks associated with this level of access will grow substantially”. Pełny dostęp do dysku ma wymagać bardzo wyraźnej decyzji użytkownika.

Agent z dostępem do całego dysku widzi pocztę, dokumenty i klucze. Apple nie zakazuje tego dostępu, tylko robi z niego świadomą decyzję. Tak samo powinno być w firmie: uprawnienia agenta to decyzja z właścicielem.

WNIOSEK

Producent systemu operacyjnego traktuje agentów jako nowy rodzaj ryzyka. Firmowe uprawnienia agentów zasługują na tę samą ostrożność.

Nota nie podaje wersji macOS ani terminu wprowadzenia zmian.

Źródło: Apple Developer News, 2.10.2026

HyperFrames Studio: agent montuje, człowiek decyduje

HeyGen wypuścił na początku października HyperFrames Studio, aplikację na macOS i Linuksa opisaną jako edytor wideo zbudowany dla agentów. Claude Code albo Codex buduje pierwszą wersję filmu, a potem człowiek i agent pracują na tej samej osi czasu: ręczne poprawki, rysunek na klatce, komentarz do fragmentu.

Agent robi pierwszą wersję w tempie, którego człowiek nie osiągnie, a człowiek zostaje przy decyzjach - ten sam układ ról budujemy w automatyzacji procesów. Aplikacja wymaga konta HeyGen.

WNIOSEK

**Przy materiałach firmowych pierwsze pytanie brzmi:
czy projekty i polecenia trafiają na serwery dostawcy.
Dokumentacja tego nie rozstrzyga.**

Wersja na Windows zapowiedziana. Licencja samej aplikacji niepodana.

Źródło: Dokumentacja HyperFrames Studio, HeyGen

OpenAI traci ludzi od bezpieczeństwa

1 października media za WSJ podały, że OpenAI zwolniło trzech badaczy za naruszenie zasad dostępu do poufnych informacji; zwolnieni zaprzeczyli zarzutom. 3 października David Robinson, który przygotowywał raporty bezpieczeństwa do premier, odszedł i napisał w The Atlantic, że kultura firmy „is broken”. W tle toczy się pozew zbiorowy o rzekomą znowę laboratoriów w celu spowolnienia AI.

Laboratoria jednocześnie mówią o spowolnieniu, są pozywane za spowalnianie i tracą ludzi od bezpieczeństwa. Bezpieczeństwo agenta w firmie musi więc stać na tym, co kontrolujecie sami.

WNIOSEK

Uprawnienia, proces, logi i przegląd przed wdrożeniem to hamulce we własnych rękach. Deklaracje dostawcy modelu nimi nie są.

Pozew Buist v. Anthropic PBC to twierdzenia powodów, sprawa nierozstrzygnięta.

Źródło: TechCrunch, 3.10.2026; Bloomberg Law, 18.09.2026



13 • RYNEK • GARTNER

70 procent porzuci agentów od dostawcy

Gartner przewiduje, że do 2028 roku 70 procent przedsiębiorstw porzuci systemy agentowe zbudowane przez inżynierów dostawcy wdrożonych u klienta. Jako powód Gartner podaje rosnące koszty i brak możliwości samodzielnego rozwijania takich systemów.

SNOK jest firmą wdrożeniową, więc mamy w tym interes - i właśnie dlatego traktujemy tę prognozę poważnie. Agent, którego klient nie umie sam utrzymać i zmienić, jest długiem, który rośnie z każdą zmianą procesu.

WNIOSEK

Przekazanie wiedzy i dokumentacja są częścią zakresu wdrożenia od pierwszego dnia. Kompetencja musi zostać u klienta.

Komunikat Gartnera z 29.09.2026.

Źródło: Gartner, 29.09.2026; The Register, 30.09.2026

Mistral Large 4 po polsku: suwerenność to nie kompetencja

Mistral udostępnił 6 października w wersji zapoznawczej Mistral Large 4: bilion parametrów, 52 miliardy aktywnych, hasło „Forged in Europe. Built for AI sovereignty”. W polskim benchmarku PLCC ma średnią 68,17. Bielik-11B-v3.0-Instruct ma 70,67, PLLuM-12B (nc-chat-250715) - 69,67, a poprzednia wersja Mistrala również 70,67.

Europejski model nie jest automatycznie dobrym modelem dla polskiego klienta. Na tym teście mały polski model wypada lepiej niż europejski flagowiec i równo z jego poprzednikiem.

WNIOSEK

Przy wyborze modelu do wdrożenia lokalnego liczy się pomiar na własnych zadaniach po polsku. Flaga na komunikacie niczego nie przesądza.

Przewaga dotyczy najlepszych wariantów Bielika i PLLuM. Średnie policzone z danych rankingu.

Źródło: Mistral AI, 6.10.2026; ranking PLCC, Hugging Face



Hamulce, które da się zamontować od razu

Uprawnienia agenta to decyzja z właścicielem. Decyzję modelu sprawdzamy na zaufanych danych przed akcją. Przegląd bezpieczeństwa obejmuje oba kierunki integracji. Kompetencja do utrzymania agenta zostaje u klienta. Model wybieramy pomiarem na własnych danych.

snok.ai

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

Materiał informacyjny. Nie stanowi porady prawnej ani inwestycyjnej.