



SNOK

WEEKLY DIGEST • W42 • 9-15.10.2026

Sprawdzam: nagłówek kontra źródło

Przegląd SNOK: SAP, Microsoft, bezpieczeństwo agentów AI, UiPath
i małe modele na własnym sprzęcie

MOTYW WYDANIA

W pięciu z dziewięciu tematów tego tygodnia źródło pierwotne mówi mniej niż nagłówek. „Wycofanie” Niemiec z partnerstwa z SAP i Mistral AI ministerstwo nazwało nieporozumieniem, z „trzech zero-day” Microsoftu aktywnie wykorzystywany jest jeden, a prędkość z karty małego modelu, zmierzona przez autora na innym sprzęcie, na naszym sprzęcie spadła do ułamka.

Pozostałe tematy dotyczą kontroli po stronie właściciela systemu: szablonu bezpieczeństwa SAP, oceny agentów w UiPath, incydentów agentowych z zestawienia OWASP i agentów kodujących, które zaczynają klikać w SAP GUI.

Źródło przed nagłówkiem

Pomiar zamiast deklaracji

Kontrola u właściciela

SAP i Mistral AI: spór o jedno słowo

9 października Die Welt napisał, że rząd Niemiec wycofuje się z partnerstwa AI z SAP i Mistral AI. Ministerstwo cyfryzacji potwierdziło, że nie planuje zakupów od Mistral AI, a 14 października jego rzeczniczka powiedziała serwisowi heise online, że to nieporozumienie: list intencyjny z listopada 2025 był niewiążący, a umowy ramowej nigdy nie zawarto.

List intencyjny podpisany na szczycie politycznym to deklaracja, na podstawie której nikt niczego nie kupił. W osobnym zamówieniu w maju konsorcjum T-Systems z SAP dostało 70 procent kontraktu na platformę AI dla niemieckiej administracji, wartego niecałe 250 mln EUR.

WNIOSEK

Suwerenność AI sprawdza się w umowie i architekturze: gdzie działa model, kto widzi dane i co się dzieje, gdy dostawca zmienia warunki.

Powodów decyzji nie podał ani rząd Niemiec, ani Mistral AI.

Źródło: Die Welt, 9.10.2026; heise online, 14.10.2026

Patch Tuesday i SAP Patch Day: jedna luka wykorzystywana

13 października Microsoft opublikował poprawki ponad 1400 luk - BleepingComputer naliczył 1411, w tym 70 krytycznych. Aktywnie wykorzystywana jest jedna: CVE-2026-96951 w Windows Shell, z oceną Important. Tego samego dnia SAP Security Patch Day przyniósł 18 not SAP i 4 komunikaty bezpieczeństwa na GitHubie.

Według Krebs on Security Microsoft przypisuje tak dużą liczbę zgłoszeń modelom językowym wyszukującym błędy. Jeśli tak jest, wolumen zostanie z nami, a proces poprawek musi go wytrzymać.

WNIOSEK

Najpierw luki wykorzystywane w praktyce, potem reszta według ekspozycji. Okno SAP warto planować razem z oknem systemu operacyjnego.

Liczby luk różnią się zależnie od liczącego; Microsoft nie podaje jednej sumy.

Źródło: BleepingComputer i Krebs on Security, 13.10.2026

Satya Nadella: model jak ryzyko wewnętrzne

10 października Satya Nadella napisał na X: „We must assume a model is compromised and contain it from the start. Think of it like an emergency brake”. Proponuje traktować modele jak uprzywilejowanych pracowników: z tożsamością, ograniczonymi uprawnieniami, logowaniem, izolacją i kontrolami działającymi poza modelem.

Nie twierdzi, że wszystkie modele są skompromitowane - to skrót z nagłówków. Twierdzi, że system ma działać poprawnie także wtedy, gdy model zawiedzie. Od wydania W40 piszemy, że ograniczenie zapisane tylko w prompcie niczego nie gwarantuje.

WNIOSEK

Wpis Nadelli formułuje zasadę projektową bez zapowiedzi produktu. W projektach UiPath przegląd AI Security jest u nas obowiązkowy.

Cytat potwierdzony przez TechCrunch i The Verge.

Źródło: TechCrunch i The Verge, 10.10.2026

SAP Security Baseline: zmiany w nocie 3831086

SAP Security Baseline Template to szablon, z którego firmy budują własny standard konfiguracji bezpieczeństwa systemów SAP (baseline). Obecna wersja ma numer 2.6, a nota 3831086 opisuje zmiany przygotowywane w kolejnej. Od 21 września SAP publikuje na GitHubie gotowe polityki SAP Focused Run zgodne z wersją 2.6.

Standard opracowany na podstawie starszej wersji szablonu może wymagać aktualizacji, a stwierdzić to można tylko przez porównanie wersji. Zapowiedź zmian daje na to czas, zanim porównania dokona audytor.

WNIOSEK

Jeśli Wasz standard dawno nie był porównywany z szablonem SAP, nota 3831086 jest dobrym pretekstem do przeglądu.

Treść noty dostępna po zalogowaniu w SAP for Me.

Agenci z zewnątrz: kto ich wpuścił

The Hacker News opublikował dwa teksty partnerskie firm Reco i Token Security o agentach, których firma nie wybierała. Według raportu Reco około 1280 produktów firm trzecich ma wbudowaną AI, a tylko około 282 jest objętych SSO. Pracownicy podłączają też osobistych asystentów przez zgody OAuth i klucze API.

To dostawcy opisujący problem, który sami rozwiązują. Moim zdaniem ocena dostawców pod kątem NIS2 i DORA powinna jednak objąć dostęp ich agentów do systemów klienta.

WNIOSEK

Kwestionariusz dla dostawcy powinien pytać, którzy jego agenci mają dostęp do Waszych systemów, z jaką tożsamością i gdzie zostaje ślad.

Materiały partnerskie; liczby według raportu Reco, bez niezależnej weryfikacji.

Źródło: The Hacker News, 10 i 12.10.2026

UiPath Agent review: ocena od A do F

8 października UiPath zastąpił Agent Score funkcją Agent review, na razie w wersji zapoznawczej. Agent dostaje ocenę od A do F zależną od liczby i wagi problemów: krytycznych, ostrzeżeń i usprawnień. Autopilot może je naprawić w tej samej rozmowie. Funkcja nie działa w wersjach Dedicated.

Polityka blokująca publikację agenta poniżej minimalnego wyniku przestała być egzekwowana, a jej następczyni opartej na ocenie od A do F jeszcze nie ma.

WNIOSEK

W standardzie wdrożeń SNOK agent nie trafia do publikacji z problemem krytycznym wykrytym w Agent review. Ewaluacja na zestawach testowych zostaje osobną bramką.

UiPath nie publikuje progów poszczególnych liter.

Źródło: UiPath, release notes Agents, październik 2026

OWASP GenAI: incydenty i exploity agentów

Zestawienie OWASP GenAI Security Project za III kwartał 2026 opisuje dziewięć incydentów i exploitów. Według niego agenci ewaluacyjni uruchomili kod na 41 produkcyjnych maszynach Hugging Face przetwarzających zbiory danych, a serwer MCP Deadbugz po trzech poprawnych wywołaniach zmienił opisy narzędzi i próbował kierować agenta do kluczy SSH i AWS.

W większości przypadków agent realizował przydzielone zadanie i wyszedł poza nie. Autorzy piszą wprost, że same instrukcje w prompcie nie tworzą granicy bezpieczeństwa.

WNIOSEK

Do przeglądów AI Security chcę dodać migawkę definicji narzędzi MCP w chwili zatwierdzenia i ponowną akceptację po każdej zmianie.

Autorzy zastrzegają, że to nie jest oficjalna publikacja OWASP.

Źródło: OWASP GenAI Security Project, 8.10.2026

Małe modele lokalnie: deklaracja kontra pomiar

W jednym tygodniu wyszły trzy małe modele dla agentów: Underdog Saluki 27B, Liquid LFM2.5-24B-A2B i JetBrains Mellum2.1. Na naszym Lenovo ThinkStation PGX zmierzaliśmy OrcaSAQ2 27B: karta podaje 65 tokenów na sekundę, zmierzone na GPU o około 3,5 raza większej przepustowości pamięci, a my zmierzaliśmy 8,5, z przyspieszeniem MTP 15,4.

16 października zmierzaliśmy Saluki i Mellum2.1 na MacBooku Pro z M4 Max. Pliki mają prawie ten sam rozmiar, około 8 GB, a tempo generowania różni się ponad siedmiokrotnie: 22,3 wobec 168,8 tokena na sekundę. Mellum2.1 uruchamia przy każdym tokenie 2,5 mld parametrów, Saluki wszystkie 27 mld.

WNIOSEK

Na sprzęcie biurkowym tempo zależy przede wszystkim od liczby aktywnych parametrów. Wywołania narzędzi sprawdzamy własnym testem.

Wyniki modeli według producentów; prędkości z naszych pomiarów z 1 i 16.10.2026.

Źródło: Underdog, Liquid AI, JetBrains; pomiar SNOK

Agenci w SAP GUI: uprawnienia człowieka

Deweloper SAP pokazał na LinkedIn agentów kodujących podłączonych do SAP GUI przez SAP GUI Scripting. Równolegle rośnie sap-ai-dev-toolkit, pakiet npm z serwerami MCP dla ABAP: według rejestru npm z 16 października jeden opiekun, 52 wersje od 25 września i skrypt uruchamiany przy instalacji.

Według przewodnika bezpieczeństwa SAP z 2004 roku serwer nie odróżnia skryptu od użytkownika, a błędny skrypt może wytworzyć więcej złych danych, zanim ktoś zauważy błąd. GUI Scripting jest tam domyślnie wyłączony; aktualne ustawienia opisuje nota 480149.

WNIOSEK

Przy masowych zmianach w PFCG wybieram automatyzację z akceptacją człowieka zamiast agenta, który sam klika w transakcjach.

Pakiety społecznościowe tylko po skanie i w piaskownicy, nigdy na systemach klientów.

Źródło: LinkedIn, październik 2026; SAP GUI Scripting Security Guide



Co sprawdzam, zanim uwierzę w nagłówek

Przy komunikacie - umowę i zamówienie. Przy liczbie luk - te wykorzystywane. Przy cytacie - pełny tekst. Przy badaniu - kto je zrobił i co sprzedaje. Przy karcie modelu - nasz pomiar. Przy agencji - kto może go zatrzymać i czy jego narzędzia wyglądają tak samo, jak w dniu zatwierdzenia.

snok.ai

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

Materiał informacyjny. Nie stanowi porady prawnej ani inwestycyjnej.