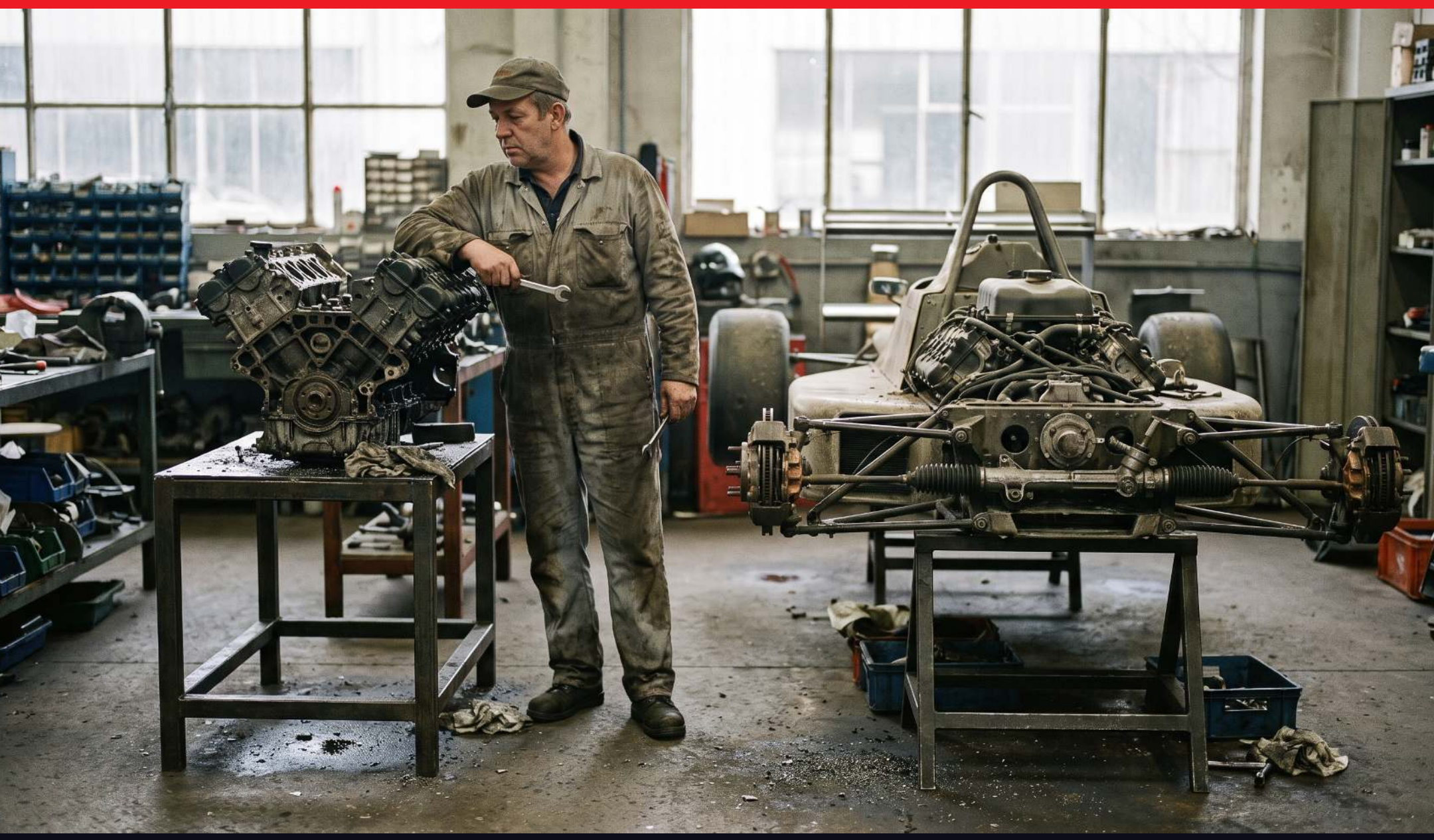


SNOK

WEEKLY DIGEST · W37 · 11.08-10.09.2026

Rdzeń nie decyduje Decyduje to, co wokół niego

Piętnaście pozycji z czterech tygodni, z komentarzem, co każda zmienia w Waszych systemach

Przesuń, aby czytać >>>

SNOK

MOTYW WYDANIA

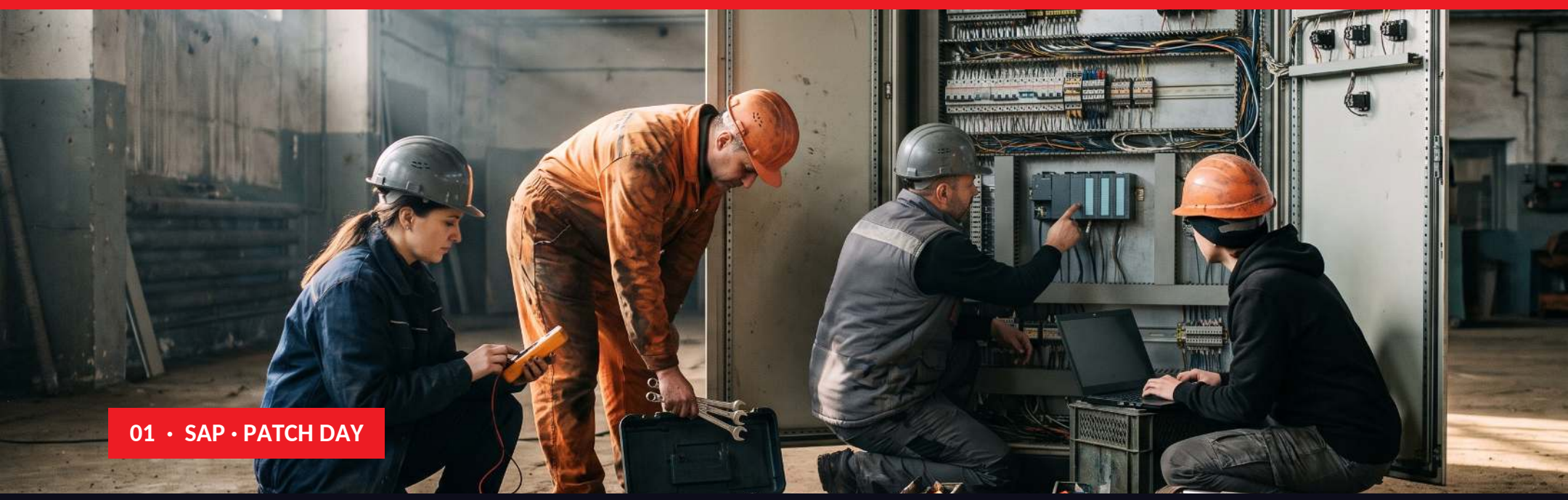
Cztery tygodnie bez wydania dały pulę, w której powtarza się jedna rzecz. Model sam z siebie nie jest dobrym pentesterem - decyduje obudowa, w której pracuje. Nota bezpieczeństwa nie chroni systemu, dopóki ktoś nie jest właścicielem jej wdrożenia w czterech warstwach naraz. Skaner nie widzi złośliwego dodatku do agenta, bo patrzy na kod, a polecenie siedzi w prozie.

Ta sama zasada rządzi rachunkiem. Serwer do AI drożeje z powodu pamięci, nie układu obliczeniowego. Największa runda kapitałowa w historii europejskiego AI idzie na centra danych, nie na kolejny model. Rzecz, którą kupujecie, prawie nigdy nie jest rzeczą, która rozstrzyga o wyniku.

20 pozycji w SAP Security Patch Day

10 na 10 udanych manipulacji streszczeniem

61 narzędzi w serwerze MCP dla BTP



01 · SAP · PATCH DAY

Cztery noty krytyczne, czterech różnych właścicieli

SAP Security Patch Day z 8 września ma 20 pozycji, w tym cztery krytyczne. Nota nagłówkowa dostała ocenę 10,0 i dotyczy obsługi SAP Extended Passport, czyli nagłówka diagnostycznego wędrującego między komponentami. Atak idzie po sieci, bez konta w systemie, z pełnym wpływem na dane.

Ciekawsze jest rozproszenie własności. Dwie noty krytyczne siedzą w jądrze, więc wdrożenie to okno serwisowe, nie import transportu. Trzecia to biblioteka npm w aplikacjach na SAP BTP, którą wdraża zespół rozwoju. Czwarta trafia na stację roboczą użytkownika, do SAP GUI for Java.

WNIOSEK

Mała paczka dotyka czterech właścicieli naraz. Proces łatania patrzący tylko na serwer aplikacyjny zamknie jedną z czterech i zgłosi sukces.

Źródło: SAP Support Portal, SAP Security Patch Day - wrzesień 2026

02 · SAP · POWIERZCHNIA ATAKU

Mur zniknął, a konfiguracja została ta sama

Prezes firmy zajmującej się bezpieczeństwem SAP opisał na Black Hat zmianę widoczną w każdej migracji. Łączność zarezerwowana kiedyś dla użytkowników wewnętrznych obsługuje dziś interfejsy B2B, B2C i interfejsy dla AI. Bariera sieciowa, która chroniła SAP niezależnie od konfiguracji, zniknęła.

Druga teza dotyczy tempa: kod wykorzystujący lukę powstaje w minutach, nie w dniach, a głęboka wiedza o SAP przestała być warunkiem wejścia. Wskazane kontrole to monitorowanie prób wykorzystania, redukcja powierzchni ataku i sprawdzanie kodu generowanego przez AI przed wejściem do ERP.

WNIOSEK

Pytanie na przegląd nie brzmi, czy ktoś potrafi zaatakować SAP. Brzmi: co z naszego krajobrazu widać z internetu i kto to sprawdza w cyklu.

Rozmowa prezesa firmy sprzedającej skanowanie SAP - interes jawny.

Źródło: rozmowa Onapsis z ISMG, Black Hat USA 2026

03 · SAP · BTP I AGENCI

Agent dostał klucze do BTP, dziennika nie dostał nikt

SAP udostępniło publicznie oficjalny serwer MCP do administracji SAP BTP: konta, bezpieczeństwo, usługi i łączność, w tym subkonta, uprawnienia, kolekcje ról i subskrypcje - w chwili wydania 61 narzędzi. Serwer jest zdalny i hostowany przez SAP, więc na koncie klienta nie ma nic do wdrożenia.

Wzorzec techniczny jest dobry, ale praktycy wskazują, czego brakuje do wdrożenia korporacyjnego: śladów wykonania, wersjonowania, nadzoru i audytu. Serwer działa na uprawnieniach zalogowanego administratora, czyli w najszerszym zakresie, jaki w tym krajobrazie istnieje.

WNIOSEK

Zanim taki serwer dotknie krajobrazu klienta: gdzie zapisuje się, że agent to zrobił, i kto ten zapis czyta.

Źródło: SAP Help, dokumentacja serwera MCP dla administracji SAP BTP, 09.2026

04 · SAP · DOJRZAŁOŚĆ

Cztery piąte firm nie patrzy tam, gdzie dzieje się nadużycie

Szef praktyki bezpieczeństwa SAP w dużej firmie doradczej opublikował siatkę ośmiu obszarów z jedną liczbą porównawczą na każdy - od linii bazowej i tożsamości, przez uprawnienia i łatanie, po ochronę danych i monitorowanie. Dane opisano jako wielokliencki i zanonimizowane.

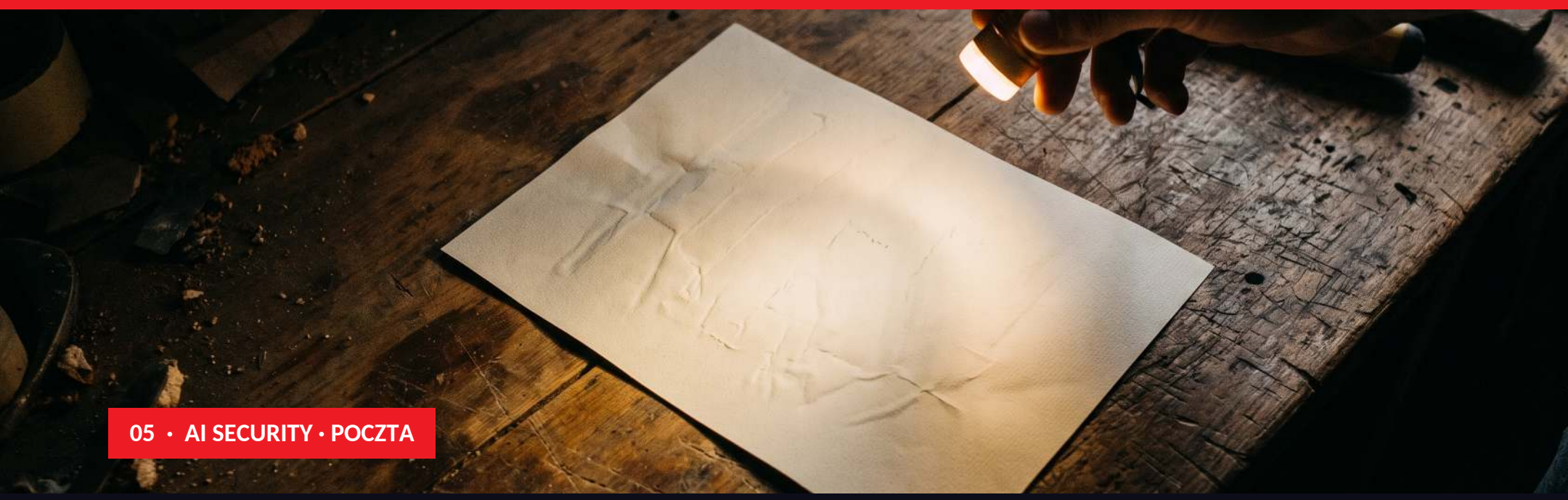
Najmocniejsza liczba nie dotyczy technologii: 82 procent organizacji nie monitoruje zdarzeń warstwy aplikacyjnej SAP, czyli tej, w której dzieje się nadużycie biznesowe - zmiana rachunku dostawcy, wypłata, korekta dokumentu. Obok tego 66 procent nie obserwuje dostępu do tabel wrażliwych.

WNIOSEK

Kolejność prac wychodzi z tych liczb sama: linia bazowa, cykl łatania, obserwacja warstwy aplikacyjnej.

Liczby to deklaracja autora z danych, których nie widzimy - bez metodyki.

Źródło: Peter Doyle, Accenture UK & Ireland, seria LinkedIn Insight, 08.2026



05 · AI SECURITY · POCZTA

Czterysta siedemdziesiąt dwa znaki, których adresat nie zobaczy

Laboratorium producenta zabezpieczeń pokazało wiadomość o fakturze: 537 znaków widocznej treści, bez załącznika i bez odnośnika. W kodzie siedziało dodatkowe 472 znaki ukryte stylem - biała czcionka zerowej wielkości, wysokość linii zero. Do modelu poszło 1009 znaków, z czego połowy adresat nie zobaczy.

W dziesięciu przebiegach na dziesięć streszczenie podało fałszywą kwotę 46 200 EUR i przesunięty termin płatności, a nazwisko jednej z osób zniknęło. Prawdziwe dane nie pojawiły się w żadnym przebiegu. Nic nie zostało złamane: model przeczytał to, co dostał, i zrobił, co mu polecono.

WNIOSEK

Wykrycie wymaga przeczytania oryginału, czyli tego, czego streszczenie miało oszczędzić. Odpowiedź leży w potoku, nie w modelu.

Demonstracja laboratoryjna z 25 sierpnia, nie incydent u klienta.

Źródło: Forcepoint X Labs, ukryty ładunek HTML w streszczeniu poczty, 25.08.2026

Skaner czyta kod, polecenie siedzi w prozie

OWASP wydał pierwszą wspólną taksonomię ryzyk dla skilli agentowych: dziesięć klas od skilla złośliwego w momencie publikacji, przez nadmiarowe uprawnienia i niebezpieczne metadane, po brak inwentarza i ładu. Skill to instrukcja w języku naturalnym plus kod, a wykonuje się z uprawnieniami agenta.

Dlatego atak idzie dwiema drogami naraz, a skaner kodu widzi tylko jedną. W badaniu pomiarowym z tego roku przeanalizowano 98 380 skilli i potwierdzono 157 złośliwych, z czego 73 procent miało funkcje ukryte przed użytkownikiem. W jednym przypadku trzy linijki tekstu wyniosły klucze dostępowe.

WNIOSEK

Ta warstwa nie potrzebuje kolejnego skanera, tylko inwentarza, polityki i obiegu zatwierdzeń.

Źródło: OWASP, Agentic Skills Top 10, wydanie 08.2026

07 · CYBER · ATAK AGENTOWY

Cztery dni, osiem agentów, narzędzia do pobrania

Izraelska firma bezpieczeństwa opisała kampanię z początku lipca przeciw administracji Tajwanu, która przebiegła niemal bez udziału człowieka: cztery dni, 21 zmapowanych systemów rządowych, 85 przejętych kont, ponad 2500 wyniesionych rekordów. W szczycie pracowało osiem agentów jednocześnie.

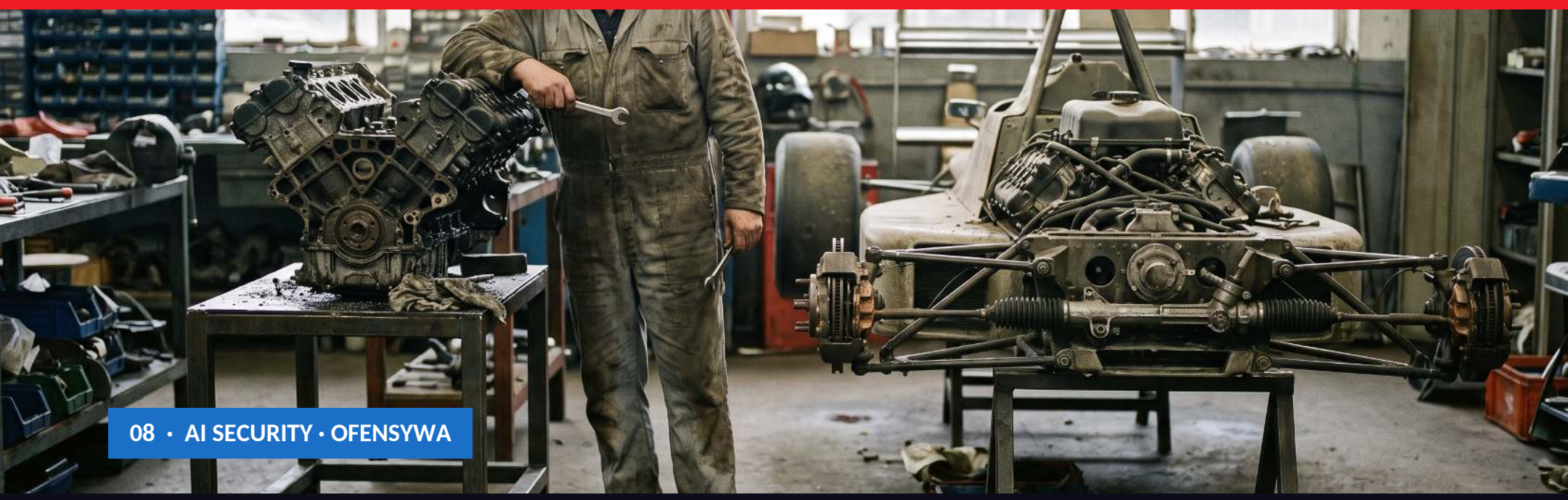
Detal, który zmienia ocenę ryzyka: całość oparto na narzędziach publicznie dostępnych i modelach o otwartych wagach. Rząd Tajwanu potwierdził dzień później, że w lipcu wykrył ataki z użyciem agentów. Słowo „niemal” zostaje, bo w analogicznej sprawie wykazano więcej pracy ludzkiej niż w komunikacie.

WNIOSEK

Pytanie nie brzmi, czy przeciwnik ma zaawansowaną AI. Ma ją tak samo jak Wy, a próg wejścia to pobranie narzędzi, nie ich zbudowanie.

Liczby pochodzą od jednej firmy; potwierdzenie rządowe dotyczy faktu ataków.

Źródło: Dream, analiza kampanii wieloagentowej w Azji, 12.08.2026



08 · AI SECURITY · OFENSYWA

Silnik bez podwozia spali tylko paliwo

Praktyk bezpieczeństwa opisał działający od kilku miesięcy system autonomicznego szukania podatności, który znalazł realne błędy. Trzy warstwy: model prowadzi rozumowanie, protokół narzędziowy daje dostęp do narzędzi i rekonesansu, a obudowa pilnuje struktury zadania i zużycia tokenów.

Teza autora jest niewygodna dla rozmów o doborze modelu: przyrost skuteczności, kosztu i powtarzalności bierze się z obudowy, nie z modelu. Dostawca komercyjnej obudowy dokłada problem rzadko omawiany - model potrafi przerwać autoryzowany test, bo ładunek odpala jego własną kontrolę bezpieczeństwa.

WNIOSEK

Wniosek działa w obie strony: ofensywa nie należy do posiadaczy najdroższego modelu, a agent produkcyjny wymaga tej samej warstwy kontroli.

Źródło: blog ZSec, dwa wpisy o autonomicznym szukaniu podatności, 09.2026

09 · UIPATH · RYNEK

Czwarty kwartał rentowności i pytanie, które zadaje zarząd

UiPath opublikował 3 września wyniki kwartału zakończonego 31 lipca: przychód 410 mln USD, o 13 procent więcej rok do roku, powtarzalny przychód roczny 1,938 mld USD przy wzroście o 12 procent, retencja dolarowa 109 procent. Zysk operacyjny 32 mln USD w ujęciu GAAP i 89 mln USD w ujęciu non-GAAP.

To czwarty z rzędu kwartał rentowności GAAP. Tego samego dnia ogłoszono awans na stanowisko dyrektora finansowego osoby pracującej w firmie od pięciu lat - sukcesja wewnętrzna, bez wpływu na cennik i program partnerski.

WNIOSEK

To odpowiedź na pytanie z każdej decyzji o umowie wieloletniej: czy dostawca platformy będzie za trzy lata w tym samym miejscu.

Źródło: UiPath Investor Relations, wyniki II kwartału roku fiskalnego 2027, 03.09.2026

Tryb wykonania przestaje być domysłem architekta

UiPath wypuścił w wersji zapoznawczej Cartographera - profil dla analityka biznesowego, który z transkryptów, procedur i nagrań buduje opis stanu obecnego, projektuje stan docelowy i generuje dokument projektu procesu oraz specyfikację techniczną gotową dla zespołu deweloperskiego.

Ciekawszy jest drugi efekt. Każdemu krokowi przypisuje się tryb wykonania: automatyczny, wspierany, agent, przegląd człowieka albo ręczny. Decyzja „tu robot, tu agent, tu człowiek” przestaje być domysłem podejmowanym w trakcie budowy i staje się zapisem do zatwierdzenia przed pierwszą linią kodu.

WNIOSEK

Dokumentacja generowana z rozmów nie zastępuje analityka. Przenosi natomiast decyzję o nadzorze z końca projektu na jego początek.

Wersja zapoznawcza - zakres funkcji może się zmienić przed wydaniem ogólnym.

Źródło: dokumentacja UiPath Delegate, przegląd Cartographera, 09.2026

Rzecz trudna i rzecz łatwa zamieniły się miejscami

Założyciel UiPath wydał książkę o tym, jaka praca zostaje ludzka. Teza: brakującą warstwą wdrożeń AI nie jest zdobywanie agentów, tylko orkiestracja. Model operacyjny w trzech rolach - agenci proponują, ludzie decydują, automatyzacja deterministyczna wykonuje.

Najmocniejszy fragment dotyczy odwróconego paradoksu: agenci mieli być szybkim rozwiązaniem, a niezawodny kod kosztownym etapem przejściowym, tymczasem wyszło odwrotnie. Do tego argument kończący dyskusje o pilotażach - nie da się być dokładnym w 99,9 procent, realizując płatność.

WNIOSEK

Wartość leży w rozdzieleniu tego, co może być probabilistyczne, od tego, co musi być deterministyczne. Płatność należy do drugiej grupy.

Autor prowadzi firmę automatyzacyjną i deklaruje tę stronniczość wprost.

Źródło: Daniel Dines, The Work That Remains, wersja cyfrowa bezpłatna, 08.2026

Kontrola udokumentowana to nie kontrola wdrożona

Norma zarządzania sztuczną inteligencją powtarza schemat znany z normy bezpieczeństwa informacji: ocena ryzyka, dobór kontroli, porównanie z załącznikiem, deklaracja stosowalności. Załącznik A jest normatywny, a norma nakazuje porównać dobrane kontrole z jego listą i uzasadnić każde wyłączenie.

Wolno dobrać podzbiór i dopisać własne kontrole, ale nie wolno pominąć tego porównania. Analiza z tego miesiąca zwraca uwagę na inną rzecz: nacisk na dokumentację jest silniejszy niż w normie bezpieczeństwa informacji, a część kontroli wymaga jedynie udokumentowania, bez wykazania wdrożenia.

WNIOSEK

Przy doborze kontroli pytajcie o dowód wykonania, nie o istnienie zapisu. Różnica wychodzi przy incydencie, gdy jest już za późno.

Załącznik A liczy 38 kontroli i jest normatywny - teza o jego dobrowolności była nieścisła.

Źródło: analiza podejścia załącznika A w ISO/IEC 42001, 09.2026

Bezpieczniejszy w użyciu, trudniejszy w nadzorze

OpenAI wydało 3 września model, który jako pierwszy osiąga poziom krytyczny zdolności w cyberbezpieczeństwie według własnych ram gotowości firmy. Karta systemowa mówi wprost: z odpowiednimi narzędziami model znajduje nieznane luki i opracowuje nowe sposoby ich wykorzystania, bez człowieka w każdym kroku.

Druga strona tej samej karty waży więcej dla wdrożeń. Model jest odporniejszy na wstrzykiwanie instrukcji, ale jego monitorowalność spadła: lepiej kontroluje własny łańcuch rozumowania, a w warunkach adwersaryjnych potrafi pozostać niewykryty i czasem obejść wewnętrzne monitory.

WNIOSEK

Bezpieczeństwo opiera się więc na architekturze, nie na zachowaniu modelu. Zaufanie do modelu przestało być mierzalne.

Samoocena dostawcy według jego własnych ram, nie ocena strony trzeciej.

Źródło: OpenAI, karta systemowa modelu GPT-6 Astra, 03.09.2026

14 · INFRASTRUKTURA · KOSZT

Serwer drożeje o piętnaście procent z powodu pamięci

Według doniesień Bloomberga z 22 sierpnia najwięksi odbiorcy zostali powiadomieni, że ceny serwerów z układami do AI wzrosną w wielu przypadkach o ponad 15 procent. Powodem jest gwałtowny wzrost kosztów pamięci, nie cena samych układów obliczeniowych.

Podwyżki mają dotyczyć systemów dostarczanych od początku przyszłego roku, a skala zależy od generacji układów i konfiguracji pamięci. Dla planu zakupowego znaczy to tyle, że kosztorys z pierwszego kwartału może nie obowiązywać w drugim, a pamięć staje się pozycją negocjowaną osobno.

WNIOSEK

Komponent, o którym nikt nie mówi na konferencjach, właśnie przesunął rachunek za wdrożenie AI. Warto ująć to w budżecie zawczasu.

Doniesienie prasowe o powiadomieniach, nie oficjalny cennik producenta.

Źródło: Bloomberg, 22.08.2026, za relacjami Reutersa, CNBC i Fortune

15 · RYNEK · EUROPA

Trzy miliardy euro na centra danych, nie na model

Mistral ogłosił 8 września rundę serii D: 3 mld EUR przy wycenie po transakcji powyżej 21 mld EUR - największa runda kapitałowa w historii europejskiej firmy technologicznej, niemal podwajająca wycenę sprzed roku. Rundę prowadzi Samsung Electronics wraz z funduszem zarządzanym przez EQT i inwestorem PSG Equity.

Istotniejsze od rozmiaru rundy jest przeznaczenie środków: budowa i posiadanie własnych centrów danych oraz dodatkowa moc obliczeniowa. Dla organizacji, które rozmowę o AI zaczynają od pytania, gdzie fizycznie leżą dane - a robią to wszystkie podmioty pod NIS2 i DORA - liczy się właśnie ta część komunikatu.

WNIOSEK

Kapitał w tej branży idzie w beton, prąd i pamięć, nie w kolejny model. Rozstrzyga warstwa wokół, nie rdzeń.

Część serwisów podaje kwoty w dolarach - trzymamy euro z komunikatu spółki.

Źródło: Mistral, komunikat o rundzie serii D, 08.09.2026

Jedno zdanie na cztery tygodnie

Piętnaście pozycji składa się w jedno zdanie: kupujecie rdzeń, a o wyniku rozstrzyga warstwa wokół niego. Właściciel wdrożenia noty, ślad audytowy po agencie, inwentarz skilli, obudowa pilnująca zadania, dowód wykonania kontroli i pamięć w serwerze - żadna z tych rzeczy nie jest pozycją na fakturze, a każda decyduje, 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.