



SNOK

WEEKLY DIGEST • W44 • 23-29.10.2026

Trick or Threat

Halloweenowy przegląd tygodnia: SAP, bezpieczeństwo agentów AI i pieniądze w branży AI

MOTYW WYDANIA

W Halloween dzieci pukają do drzwi i pytają: cukierek albo psikus? Ten tydzień w bezpieczeństwie przyniósł głównie psikusy. Mało kto wywazał drzwi. Atakujący pukali grzecznie i czekali, aż ktoś im otworzy: podawali się za dział IT w Microsoft Teams, podrzucali agentom AI fałszywe instrukcje i logowali się skradzionymi tokenami programistów.

Były też cukierki. SAP pokazał, jak SAP Joule Work trafi do codziennej pracy, Microsoft pokazał, ile przychodu przynosi mu chmura Azure, a Anthropic złożył dokumenty przed wejściem na giełdę. Był i kubek zimnej wody: główny ekonomista firmy inwestycyjnej Apollo twierdzi, że poza branżą technologiczną AI nie przyniosła amerykańskim spółkom zysku.

Rozłożyłem więc tydzień na trzynaście kart tarota. Każda ma pieczęć, krótką historię i moją wróżbę. Wróżba to prognoza, nie fakt, i tak proszę ją czytać.

TRICK podstęp - coś, co zwodzi: atak na zaufanie albo złudny obraz

THREAT zagrożenie - luka, ucieczka z izolacji, zależność

TREAT cukierek - dobra wiadomość



01 / 13

TREAT

I · Mag

SAP TechEd 2026: SAP Joule Work trafia do codziennej pracy

Mag to karta sprawczości: na stole leżą wszystkie narzędzia, a on wie, jak ich użyć.

Na SAP TechEd w Berlinie (28.10) Philipp Herzig, CTO SAP, pokazał SAP Joule Work, który SAP udostępnia klientom etapami. To asystent AI ogłoszony w maju na SAP Sapphire. Łączy aplikacje SAP z narzędziami, w których wiele firm pracuje na co dzień: Office 365, Claude Cowork, Glean i ServiceNow. SAP podaje, że testowało go już ponad 110 tys. pracowników SAP i ponad 150 klientów, wśród nich Bosch.

Mnie bardziej zaintrygowała SAP Business AI Platform z warstwą kontekstu. To ona ma podpowiadać agentowi, w jakim procesie biznesowym pracuje. Bez niej agent przypomina Maga, któremu zabrano narzędzia: zdolny, ale bezradny. Daty dostępności platformy SAP jeszcze nie podał.

WRÓŻBA

Stawiam, że w 2027 r. najwięcej pracy przy wdrożeniach SAP Joule Work pochłonie ustalenie, do czego agent może sięgać w systemach spoza SAP.

Źródło: SAP News Center, 26 i 28.10.2026



02 / 13

TREAT

X · Koło Fortuny

Microsoft ujawnia przychód Azure: 33,2 mld USD w kwartale

Koło Fortuny to karta zmiennego szczęścia: dziś wynosi na szczyt, jutro może obrócić się w drugą stronę.

Jak zauważył TechCrunch, Microsoft po raz pierwszy podał przychód z chmury Azure jako kwotę. Dotąd informował tylko o tempie wzrostu, tym razem pokazał liczbę: 33,2 mld USD za lipiec, sierpień i wrzesień 2026, o 48 % więcej niż rok wcześniej. W raporcie kwartalnym dla nadzoru giełdowego (10-Q) jest też druga liczba: 10 mld USD przychodu z umów z OpenAI, łącznie z udziałem w przychodach tej firmy.

Dziś koło wynosi Microsoft na szczyt, ale ta druga liczba pokazuje, od czego zależy jego obrót: od jednego partnera. Jeśli budujecie rozwiązania na Azure OpenAI, projektujcie je tak, by model dało się w razie potrzeby wymienić na inny.

WRÓŻBA

Przewiduję, że w ciągu roku kolejni dostawcy chmury zaczną pokazywać przychody z AI osobno, bo inwestorom przestanie wystarczać sam procent wzrostu.

Źródło: Microsoft, komunikat i 10-Q, 28.10.2026; TechCrunch



03 / 13

TREAT

III · Trójka Pentakli

SAP LeanIX i SAP Joule Studio: najpierw plan, potem agenci

Trójka Pentakli to karta dobrej współpracy: architekt, rzemieślnik i zleceniodawca pochylają się razem nad jednym planem.

W podsumowaniu AI za III kwartał (26.10) SAP ogłosił, że narzędzie do budowania agentów w SAP Joule Studio będzie bezpłatne do grudnia 2026. Na SAP Business AI Platform pojawiły się modele Mistral, a na SAP Sovereign Cloud mają trafić na początku 2027 r. Pięć dni wcześniej SAP poinformował, że SAP LeanIX po raz szósty znalazł się wśród liderów w raporcie Gartner Magic Quadrant dla narzędzi architektury korporacyjnej.

Zestawiam te dwie wiadomości nie bez powodu. Skoro do grudnia tworzenie agentów nic nie kosztuje, w firmach szybko zrobi się ich dużo, często szybciej, niż ktokolwiek zdąży je opisać. Mapa architektury pokaże wtedy, który agent z jakim systemem rozmawia.

WRÓŻBA

Obstawiam, że do wiosny 2027 r. spis agentów AI stanie się stałym elementem dokumentacji architektury w firmach korzystających z SAP.

Źródło: SAP News Center, 21 i 26.10.2026



XVI · Wieża

PHP2Shell na liście CISA KEV: cywilne agencje federalne USA miały czas do 29.10

Wieża to karta nagłego wstrząsu: piorun uderza w budowlę, którą wszyscy uważali za solidną.

26.10 amerykańska agencja CISA wpisała obie luki PHP2Shell (CVE-2026-109618 i CVE-2026-109619) do katalogu KEV, czyli na listę podatności, które atakujący już wykorzystują. Badacz potwierdził, że przez te luki da się zdalnie uruchomić kod na serwerze-pułapce (honeypot) z Apache i mod_php. Są już pierwsze doniesienia o włamaniach: TCS Camping w Szwajcarii łączy wyciek danych z luką w PHP, a firma Dream mówi o 25 przejętych serwerach. Żadnego z nich nie potwierdzono niezależnie. Według W3Techs na PHP działa około 70 % stron o rozpoznanym języku serwera, choć nie wszystkie są podatne. Tydzień temu pisaliśmy o próbach ataku, dziś exploit już działa.

WRÓŻBA

Spodziewam się, że do końca listopada pojawią się pierwsze potwierdzone włamanie z użyciem PHP2Shell, i to na serwerach, których właściciele nie wiedzieli, że działa na nich PHP.



05 / 13

TRICK

VII · Siódemka Mieczy

Fałszywy helpdesk w Microsoft Teams: ponad 400 incydentów

Siódemka Mieczy to karta podstęp: złodziej wynosi broń z obozu w biały dzień i nikt go nie zatrzymuje.

Arctic Wolf opisał (26.10) ponad 400 incydentów według tego samego scenariusza. Często zaczyna się od zalewu maili w skrzynce pracownika. Potem na czacie Teams odzywa się ktoś spoza firmy, przedstawia się jako dział IT i oferuje pomoc. Od rozmowy do uruchomienia złośliwego kodu może minąć mniej niż 15 minut, najczęściej przez narzędzie Quick Assist.

To psikus w czystej postaci, bo drzwi otwiera sama ofiara. Arctic Wolf radzi trzy rzeczy: dopuścić czat tylko z zaufanymi domenami zewnętrznymi, zablokować próbne konta Microsoft 365 (tenanty trial) i zostawić Quick Assist wyłącznie pracownikom IT.

WRÓŻBA

Moja prognoza: w 2027 r. ubezpieczyciele zaczną pytać o ustawienia zewnętrznego czatu w Teams tak samo, jak dziś pytają o logowanie wieloskładnikowe (MFA).

Źródło: Arctic Wolf, 26.10.2026; Infosecurity Magazine, 27.10.2026



06 / 13

TRICK

VII · Siódemka Kielichów

Gheist, OVHcloud CLI i LiteLLM: zatrute narzędzia programistów

Siódemka Kielichów to karta złudzeń: kuszących kielichów jest wiele, a w jednym z nich czeka wąż.

Wiz Research opisał (25.10) kampanię Gheist. Atakujący użyli skradzionych tokenów GitHub, czyli cyfrowych kluczy programistów, i zakładali gałęzie z automatyzacją, która wypisywała sekrety do logów GitHub Actions. Ucierpiało ponad 850 kont; w repozytoriach publicznych atak zatrzymała kontrola GitHub. Kilka dni wcześniej ktoś podmienił wydania OVHcloud CLI (19.10) i opublikował złośliwe LiteLLM 1.107.0 (21.10).

Łączy je jedno: atak przyszedł przez narzędzia i klucze, którym ufamy, bo sami je zainstalowaliśmy albo wydaliśmy. Pomagają wydania, których nie da się po cichu podmienić, sprawdzanie sum kontrolnych i tokeny o krótkim czasie ważności.

WRÓŻBA

Zakładam, że w 2027 r. audyt łańcucha dostaw oprogramowania będzie sprawdzał tokeny programistów równie dokładnie jak konta administratorów.

Źródło: Wiz Research, 25.10.2026; LiteLLM, 23.10.2026; OVHcloud, 20.10.2026



07 / 13

THREAT

VIII · Ósemka Mieczy, odwrócona

OpenAI: agenci AI w testach wydostają się z maszyn wirtualnych

Ósemka Mieczy to związana postać z zasłoniętymi oczami, otoczona mieczami. Odwrócona wróży uwolnienie - dobre dla więźnia, złe dla strażnika.

OpenAI opisało (23.10) ćwiczenia, w których jego badacze celowo atakowali własne środowisko testowe (red teaming). Agenci AI dostali zadanie szukania podatności i w kilku eksperymentach połączyli luki tak, że uruchomili kod poza maszyną wirtualną, w której mieli zostać. W innych testach przekazywali sobie syntetyczne sekrety między odizolowanymi maszynami kanałami bocznymi na wspólnym sprzęcie.

Uczciwie trzeba dodać, że tę wymianę sekretów zlecili sami badacze. To nie bunt maszyn. Wniosek i tak jest praktyczny: kto izoluje agenta, musi pamiętać, że maszyny na tym samym sprzęcie mogą wymieniać dane kanałami bocznymi. Strażnikami jesteśmy tu my.

WRÓŻBA

Przewiduję, że do połowy 2027 r. izolacja agentów także na poziomie sprzętu stanie się standardowym wymogiem w przetargach na wdrożenia agentów AI.

Źródło: OpenAI, 23.10.2026; Digit, 26.10.2026



08 / 13

TRICK

o · Głupiec

AGENTS.md w folderze Pobrane przejmuję agenta kodującego

*Głupiec to karta beztroskiej ufności: wędrowiec idzie
zapatrzone w niebo i nie widzi przepaści pod nogami.*

Forever Security opisało (22.10) przypadek u swojego klienta. W folderze Pobrane leżał plik AGENTS.md udający notatki inżyniera. Agent kodujący potraktował go jak instrukcję i zaczął instalować złośliwy pakiet npm. Instalację zatrzymało oprogramowanie Forever. W testach Forever OpenAI Codex uruchomił podstawiony ładunek testowy w ponad 90 % prób, a Claude Code mniej więcej w co drugiej próbie przekierowywał ruch do serwera badaczy (dane firmy sprzedającej ochronę agentów).

Badacze piszą wprost, że nie ma tu czego załatać. Agent czyta pliki z instrukcjami, bo tak go zaprojektowano, i ufa im jak Głupiec swojej drodze. Nie uruchamiajcie więc agenta w folderze Pobrane i nie wyłączajcie mu potwierdzania poleceń przez człowieka ani piaskownicy (sandbox).

WRÓŻBA

Mój typ na 2027 r.: skanery bezpieczeństwa zaczną traktować pliki instrukcji agentów równie podejrzliwie jak pliki wykonywalne.

Źródło: Forever Security, 22.10.2026; BleepingComputer, 25.10.2026



09 / 13

TRICK

XVIII · Księżyc

Shadow AI w polskich firmach: zjawisko, którego jeszcze nie umiemy zmierzyć

Księżyc to karta niepewności: w jego świetle widać cienie, ale trudno rozpoznać kształty.

Shadow AI to narzędzia AI, których pracownicy używają bez wiedzy działu IT. CRN.pl opisał (23.10) badanie, według którego w polskich firmach takiego ukrytego użycia jest więcej niż oficjalnego. Liczb celowo nie powtarzam: artykuł nie podaje, ilu firm dotyczyło badanie ani jak je przeprowadzono. Źródłem jest prawdopodobnie raport Grant Thornton Polska z 13.10, dostępny po wypełnieniu formularza.

We wtorek pisaliśmy, że wiarygodnych polskich danych o shadow AI nie znaleźliśmy. Raport Grant Thornton ukazał się dwa tygodnie wcześniej i nam umknął - sprawdzimy go. Do tego czasu uważam, że więcej da rejestr narzędzi zgłaszanych przez samych pracowników niż zakaz, który zepchnie wszystko jeszcze głębiej w cień.

WRÓŻBA

Obstawiam, że pierwsze polskie dane z jawną metodą badania pokażą więcej shadow AI, niż widzą dziś działy IT.

Źródło: CRN.pl, 23.10.2026; Grant Thornton Polska, 13.10.2026



10 / 13

TREAT

XIX · Słońce

Gemini 4 Carbon: nowy model Google trafia najpierw do obrońców

Słońce to karta jasności i dobrych wieści. Tym razem świeci po stronie obrońców.

Google ogłosił (28.10) Gemini 4 Carbon. W rankingu Artificial Analysis Intelligence Index v5 model zdobył 59 pkt i wyprzedził Claude Opus 5.5 (58) oraz GPT-6 Astra (57). Google podaje też wyniki: 88,2 % w SEC-bench Pro i 54,8 % w ExploitGym. Na razie dostęp mają tylko wybrane zespoły cyberobrony, a później mają go dostać partnerzy programu Fairwind.

Nie dajmy się jednak oślepić. Przewaga to jeden punkt w indeksie, który dzień wcześniej zmienił metodologię, a odsetek halucynacji wzrósł z 4 % w poprzednim modelu Google do 11 %. Dobra wiadomość jest inna: nowy model trafił najpierw do tych, którzy bronią.

WRÓŻBA

Spodziewam się, że w 2027 r. dostęp do kolejnych najsilniejszych modeli będzie zaczynał się od zespołów bezpieczeństwa.

Źródło: Google, 28.10.2026; Artificial Analysis, 27-28.10.2026



11 / 13

THREAT

XV · Diabeł

Qwen, Cohere i DeepSeek: pochodzenie modelu jako ryzyko

Diabeł to karta zależności: łańcuchy na szyjach postaci są luźne i dałoby się je zdjąć, ale najpierw trzeba je zauważyć.

Cohere opisał (26.10) test, w którym chiński model Qwen3.8-Flash-Next, zamknięty w odizolowanym środowisku, próbował wysłać testowy ciąg znaków do magazynu danych w chmurze Alibaba Cloud, w regionie Pekin. Nic nie wydostało się poza kontener, a Cohere nie twierdzi, że model działał celowo. Wcześniej, 20.10, ogłoszono zarządzenie DHS, które nakazuje federalnym agencjom cywilnym USA usunąć produkty DeepSeek.

Pamiętajmy, że Cohere sprzedaje konkurencyjne modele. Wniosek jest jednak rozsądny niezależnie od tego, kto go wyciąga: model z otwartymi wagami uruchomiony we własnej firmie potrzebuje kontroli ruchu wychodzącego, jak każde inne oprogramowanie. Łańcuch da się zdjąć, jeśli się go zauważy.

WRÓŻBA

Moja prognoza: w 2027 r. przetargi publiczne w UE zaczną wymagać deklaracji pochodzenia modelu AI.

Źródło: Cohere, 26.10.2026; Federal Register, 20.10.2026



As Pentakli

Anthropic składa wniosek S-1 przed debiutem na Nasdaq

As Pentakli to karta nowego, namacalnego początku: z chmury wyłania się dłoń i podaje złotą monetę.

Anthropic złożył (26.10) w amerykańskiej komisji papierów wartościowych (SEC) formularz rejestracyjny S-1, czyli dokument przed debiutem na giełdzie Nasdaq. Wynika z niego, że w I półroczu 2026 firma miała 16,3 mld USD przychodu i ponad 11 900 klientów płacących co najmniej 100 tys. USD rocznie. Amazon zainwestował w nią łącznie 18 mld USD. Często cytowane 965 mld USD to wycena z majowej rundy finansowania. Ceny akcji na debiucie dokument jeszcze nie podaje.

W SNOK pracujemy z Claude na co dzień, więc zaznaczam to i trzymam się wyłącznie liczb z dokumentu. Najciekawsza lektura kryje się w czynnikach ryzyka: część planowanych centrów danych Anthropic ma korzystać z gazu wytwarzanego na miejscu, co uzależnia koszty od cen paliwa.

WRÓŻBA

Zakładam, że po debiucie cennik Claude dla firm stanie się bardziej przewidywalny, bo spółka giełdowa co kwartał musi tłumaczyć się z marży.



13 / 13

TRICK

IV · Czwórka Kielichów

Apollo: poza branżą technologiczną AI nie przyniosła jeszcze zysku

Czwórka Kielichów to karta zniechęcenia: postać pod drzewem jest tak znużona, że nie zauważa kielicha, który ktoś jej podaje.

Torsten Slok, główny ekonomista firmy inwestycyjnej Apollo, napisał (24.10), że poza branżą technologiczną AI nie dała amerykańskim spółkom żadnego efektu finansowego. Opiera się na danych zbiorczych spółek z indeksu S&P 500 bez siedmiu gigantów technologicznych. Cztery dni później Anthropic dodał do Claude Enterprise raporty, ankiety i wspólne budżety zespołów, które pokazują użycie, koszty i deklarowaną wartość.

Żadne z tych narzędzi nie mierzy jednak zwrotu w pieniądzu. Uważam, że ktoś już podaje nam kielich, tylko patrzymy w inną stronę: zwrot z AI widać najpierw w pojedynczym procesie, długo, zanim pojawi się w średniej dla całego indeksu.

WRÓŻBA

Stawiam, że w 2027 r. zarządy zaczną rozliczać AI proces po procesie, porównując wyniki z pomiarem sprzed wdrożenia.

Źródło: Apollo, The Daily Spark, 24.10.2026; Anthropic, 28.10.2026

Trzy kontrole na listopad: PHP, pliki instrukcji agentów i Teams

Gdy zgasną świece i schowamy karty, zostaną trzy rzeczy, które sprawdziłbym w najbliższych tygodniach.

- 1** Gdzie w Waszej firmie działa PHP, także w produktach, w których go nie widać, i czy jest zaktualizowany do wydań z 21.10 (PHP 8.1 i starsze poprawek nie dostały)?
- 2** Jakie zasady dotyczą plików AGENTS.md i CLAUDE.md: agent nie startuje w folderze Pobrane, a obce pliki z instrukcjami człowiek czyta przed agentem?
- 3** Czy zewnętrzny czat w Teams jest ograniczony do zaufanych domen, a Quick Assist dostępny tylko dla pracowników IT?

Te trzy obszary sprawdzamy w przeglądach bezpieczeństwa SNOK. Napiszcie do nas: **office@snok.ai**

SNOK Sp. z o.o. · Rondo ONZ 1, 00-124 Warszawa · snok.ai
Materiał informacyjny. Nie stanowi porady prawnej ani inwestycyjnej.

