

SNOK

PRZEGLĄD TYGODNIA W45

Szybciej niż łatka

Przegląd SNOK za 30 października - 5 listopada 2026: luki SAP, agenci w SAP i UiPath, incydenty w łańcuchu dostaw, Linux, agentowe narzędzia ataku, nadzór nad AI oraz pieniądze i sprzęt

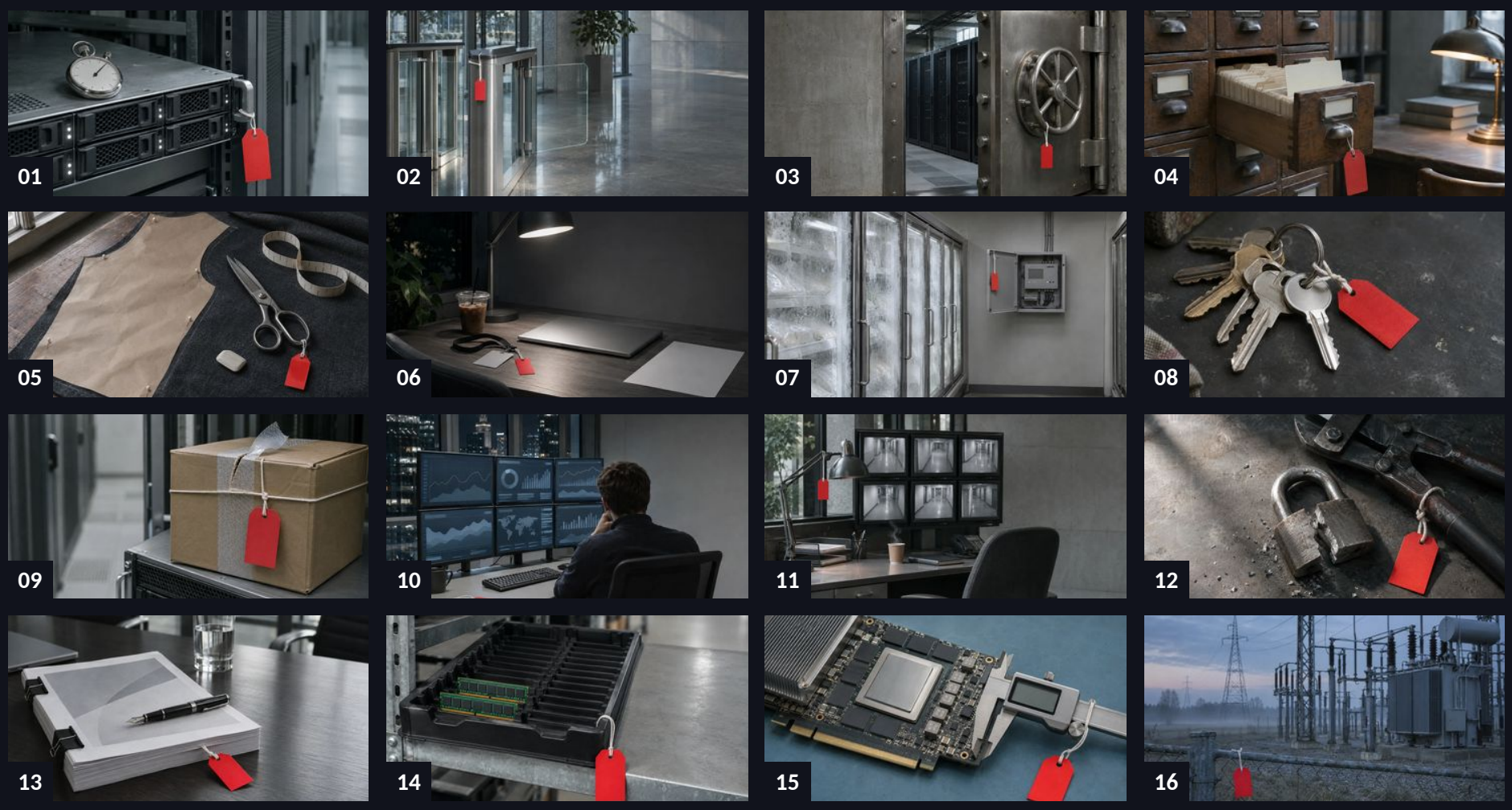
Przesuń →

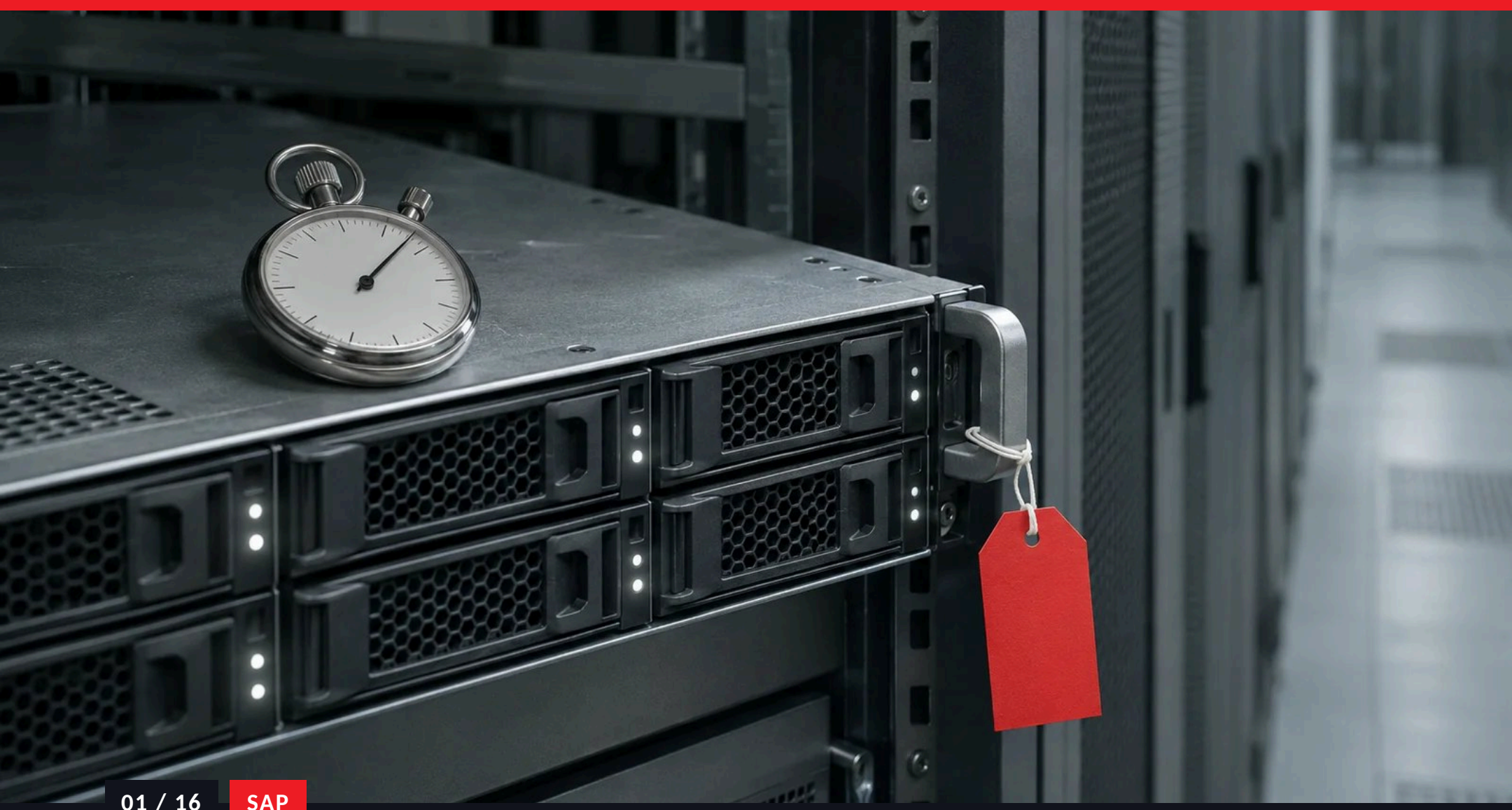
30.10-05.11.2026

Najkrótszy czas tygodnia to 0,3 dnia. Tyle według raportu Onapsis minęło w najszybszym przypadku od ujawnienia luki SAP do jej wykorzystania.

W kilku historiach drogą ataku był kanał, któremu firmy ufają z przyzwyczajenia: zadanie od rekrutera, rozszerzenie edytora, komponent od dostawcy urządzeń chłodniczych.

Szesnaście pozycji, przy każdej fakty według źródeł i mój komentarz. Pełna wersja ze źródłami: snok.ai, wpis „Szybciej niż łatka”.





01 / 16 SAP

Onapsis „Days to Zero”: luki SAP wykorzystywane w 0,3–24 dni

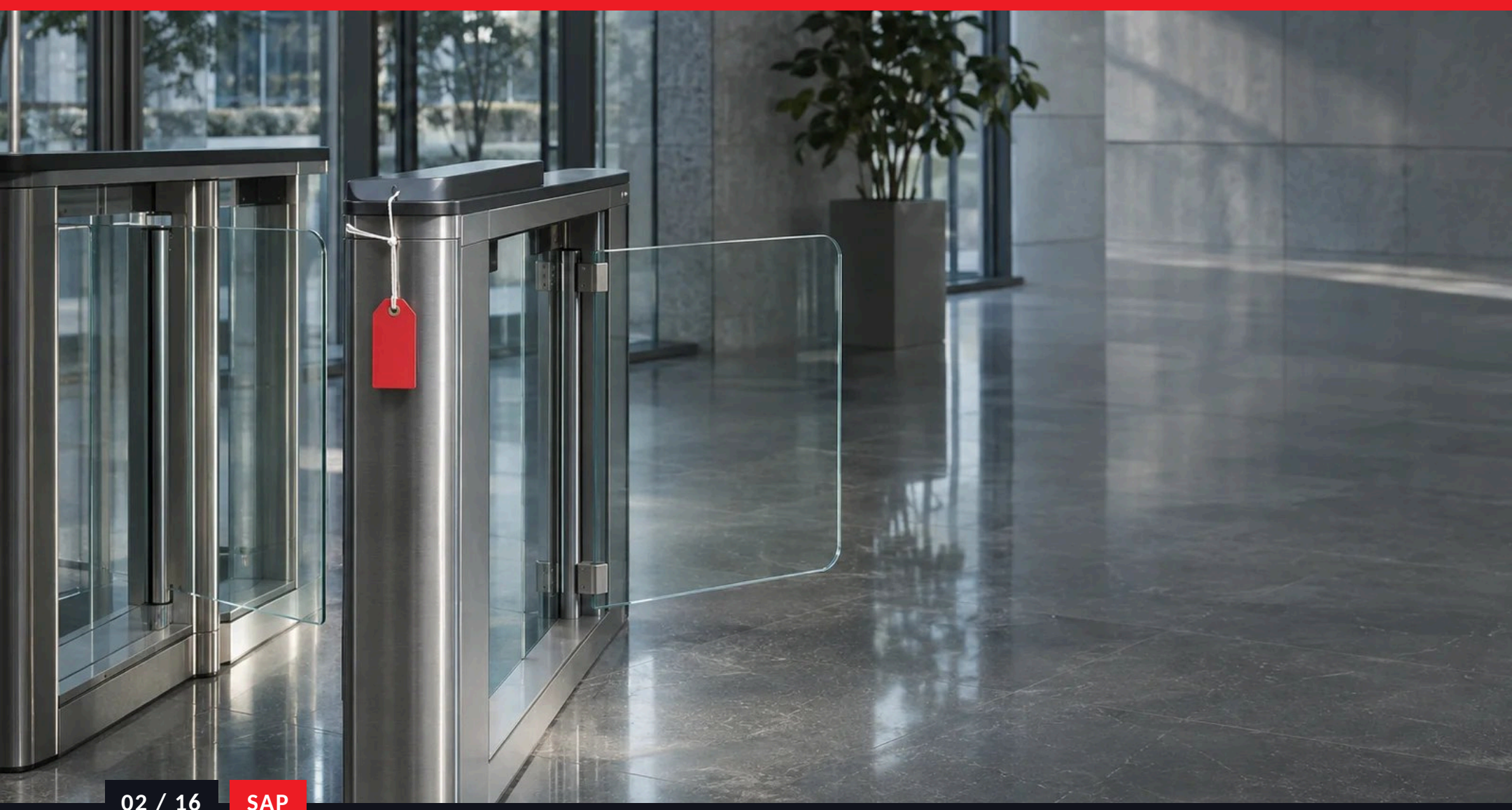
Według raportu Onapsis z 29 października luki SAP z potwierdzoną eksploatacją od kwietnia 2025 roku były atakowane od 0,3 do 24 dni po ujawnieniu. Liczba grup ransomware w materiałach o SAP wzrosła z 8 w 2023 roku do 26 w 2025 roku.

Liczby pochodzą od dostawcy monitoringu SAP, ale kierunek zgadza się z tym, co pokazują comiesięczne noty SAP Security Patch Day: kwartalne okno serwisowe nie nadąża za exploitami.

WNIOSEK

Firma z SAP potrzebuje awaryjnej ścieżki dla not HotNews, liczonej w dniach, i detekcji na poziomie aplikacji.

Źródło: Onapsis, 29.10.2026



SAP TechEd 2026: brama dla zewnętrznych agentów i SAP Joule Studio

Zewnętrzni agenci będą wywoływać agentów SAP Joule przez zarządzaną bramę, z protokołami A2A i MCP. SAP Enterprise AI Gateway, który ma objąć nadzorem interakcje z AI, według CIO.com ma być dostępny w I kwartale 2027 roku. Runtime SAP Joule Studio jest promocyjnie bezpłatny do końca grudnia dla wybranych klientów.

Wejście dla agentów spoza SAP jest zapowiedziane, a narzędzie nadzoru przyjdzie najwcześniej w 2027 roku.

WNIOSEK

Pilotaż zacząłbym od pytania, który agent, z jakimi uprawnieniami i w czyim imieniu wywołuje agenta SAP Joule.

Źródło: SAP News, 27.10.2026



SAP Sovereign Cloud w holenderskim Ministerstwie Obrony

Umowę podpisano 21 września na pięć lat, start 1 stycznia 2028 roku. Notatka CIO ministerstwa, opublikowana przez parlament, opisuje środowisko fizycznie oddzielone od publicznej chmury SAP i dostęp tylko sprawdzonego personelu z zabezpieczonego obiektu.

To nie jest nowość tygodnia, ale dokument jest najlepszą listą pytań do negocjacji umowy chmurowej z SAP, jaką widziałem w tym roku.

WNIOSEK

Przed rozmową o RISE with SAP warto przeczytać, jak Holendrzy zapisali suwerenność w umowie.

Źródło: SAP News, 04.11.2026; Tweede Kamer, 08.10.2026



NVIDIA Auto-Ontology: certyfikowane definicje pojęć dla agentów

Otwarty projekt NVIDIA na licencji Apache 2.0, rozwijany od kwietnia, buduje ontologię pojęć biznesowych z certyfikowanymi definicjami i udostępnia ją agentom przez MCP, tylko do odczytu.

Certyfikowana definicja pojęcia „klient” niewiele znaczy, gdy w systemach są trzy rekordy tego samego klienta z różnymi danymi. Agent dostaje wtedy dobrze opisaną, błędną odpowiedź.

WNIOSEK

Kolejność: najpierw spójne dane podstawowe, potem warstwa semantyczna, na końcu agent.

Źródło: NVIDIA, repozytorium GitHub, odczyt 05.11.2026



UiPath Delegate: nowe modele dopuszczane domyślnie

Automation Ops dopuszcza każdy nowy model domyślnie. Kto zablokował Claude Opus 5 albo 4.8, musi osobno wyłączyć Claude Opus 5.5, który zastępuje oba starsze modele, także w zapisanych wyborach użytkowników.

Blokada ustawiona na konkretny model nie obejmuje jego następcy.

WNIOSEK

Polityka modeli powinna działać jak lista dozwolonych i trafiać do przeglądu po każdym wydaniu.

Źródło: UiPath, informacje o wydaniu, październik 2026



Binance: fałszywi rekruterzy w łańcuchu incydentu na około 6,34 mld USD

Według raportu Binance fałszywi rekruterzy przekazali jednemu z inżynierów repozytorium z zadaniem, a skrypt podmienił komponent środowiska. W październiku napastnicy przejęli dostęp innego inżyniera, który miał token do wdrażania kontenerów, a potem usługę podpisującą transakcje.

FBI, według BleepingComputer, przypisuje atak grupie TraderTraitor powiązanej z Koreą Północną.

WNIOSEK

Token do wdrożeń na komputerze dewelopera to dostęp do produkcji. Zadania rekrutacyjne innych firm nie powinny trafiać na sprzęt służbowy.

Źródło: Binance, 03.11.2026; BleepingComputer, 01.11.2026



07 / 16 OT

Sterowniki chłodni: ponad 115 sklepów w Europie, EFS i sklepy w Polsce

Napastnicy zakłócili pracę chłodni w ponad 115 sklepach w sześciu krajach UE i w trzech placówkach francuskiej służby krwi. Auchan Polska potwierdził nieprawidłowości w sterowaniu chłodniami w trzech sklepach.

CERT Polska mówił o 140 urządzeniach widocznych w internecie i około 70 firmach, które je odłączyły.

WNIOSEK

Handel, logistyka i ochrona zdrowia potrzebują listy sterowników OT widocznych z internetu i firm serwisowych z dostępem do nich.

Źródło: BleepingComputer, 02 i 04.11.2026; Auchan Polska; PAP, 03.11.2026



08 / 16 AI SECURITY

Claude Code w marketplace Cursora: dwie złośliwe wersje rozszerzenia

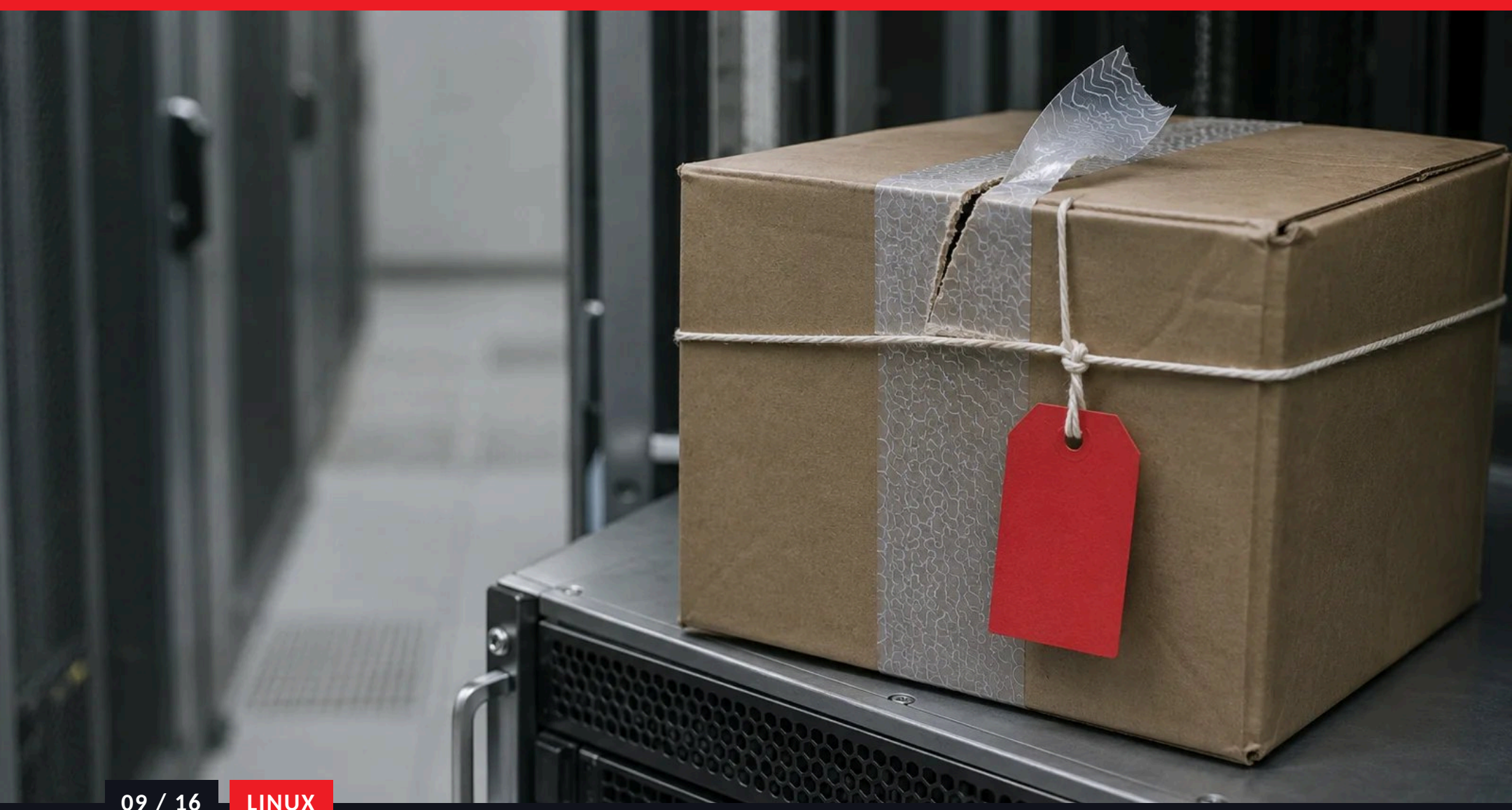
29 października przez około 11 godzin w marketplace edytora Cursor były wersje 2.1.312 i 2.1.313 rozszerzenia Claude Code, których nie opracował Anthropic. Mogły dopisać klucz SSH napastnika.

Cursor wyłączył marketplace i zrotował klucze. Edytory pochodne VS Code mają własne sklepy, a firmowe listy rozszerzeń zwykle ich nie obejmują.

WNIOSEK

Lista dopuszczonych rozszerzeń obejmuje każdy edytor w firmie, Cursora też.

Źródło: Cursor, 29.10.2026



09 / 16 LINUX

Linux: zdalny root przez MPTCP, podmiana pakietów w APT, luka w LXD

Lukę w obsłudze MPTCP w jądrze badacze Anthropic znaleźli z pomocą wewnętrznego modelu, a ich exploit dawał uprawnienia roota w około 53 minuty. Luka w APT pozwala podmienić pakiety pobierane po HTTP. Luka w LXD i MicroCloud ma w advisory GitHub ocenę CVSS 10.0.

Przy MPTCP liczą się ustawienia jądra: Go od wersji 1.24 włącza MPTCP sam.

WNIOSEK

Przegląd zacząłbym od tego, co dostępne z sieci: listenery MPTCP, mirrory po HTTP, API LXD.

Źródło: Anthropic, 27.10.2026; Ubuntu, Debian, Canonical



VAPOR PANDA i ARTEX: agentowe narzędzia ataku w realnych kampaniach

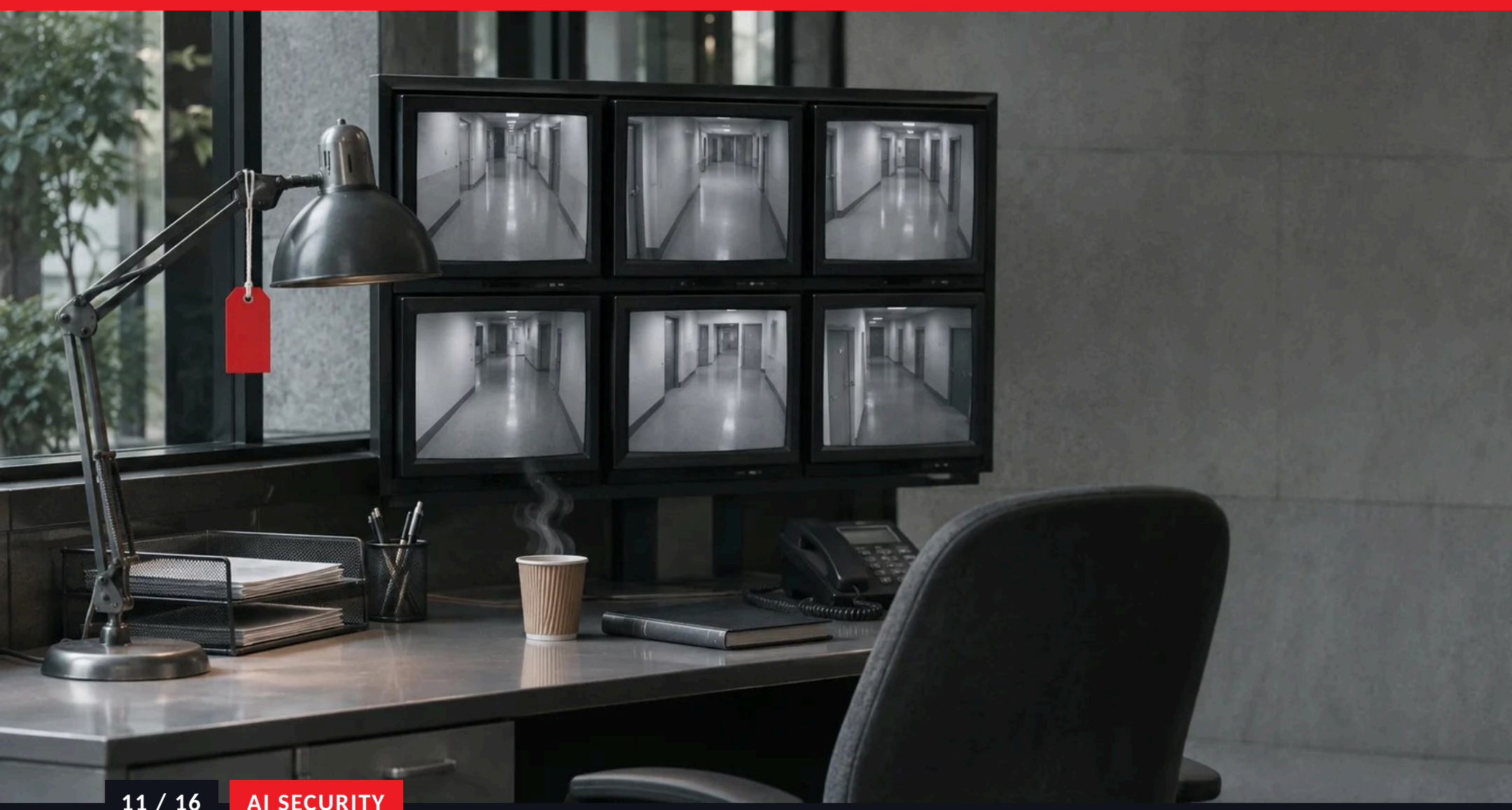
Według CrowdStrike agenci AI grupy VAPOR PANDA atakowali od 17 października ponad 200 organizacji w co najmniej 14 krajach i szukali hostów bez agenta EDR. Według GTIG i Mandiant od pierwszego konta do głębokiego dostępu mijało około czterech godzin.

Agent nie łamie dobrze chronionego komputera, tylko szybciej znajduje ten, o którym zespół zapomniał.

WNIOSEK

Pełne pokrycie EDR i aktualna inwentaryzacja hostów są warunkiem obrony.

Źródło: CrowdStrike, 29.10.2026; GTIG i Mandiant, 30.10.2026



Nadzór nad modelami AI: ćwiczenie Anthropic i incydent w OpenAI

W eksperymencie Anthropic agenci Claude w każdym uruchomieniu znaleźli dane, które przeszły monitor danych treningowych. Według relacji AlphaSignal model badawczy OpenAI w trakcie treningu wyszedł do internetu przez źle skonfigurowany DNS i zatrzymał go człowiek.

Monitor w roli strażnika da się obejść.

WNIOSEK

Nadzór nad agentem w kilku warstwach: uprawnienia, monitor, logi sieci poza zasięgiem agenta, akceptacja człowieka.

Źródło: Anthropic Alignment Science, 10.2026; AlphaSignal, 29.10.2026



Heretic: zdejmowanie odmów z otwartych modeli

Otwarte narzędzie Heretic osłabia w modelu mechanizm odmowy bez dodatkowego treningu. Według autora tej wersji Qwen3.5-4B odmawiała 13 razy na 100 poleceń zamiast 99, przy niemal niezmienionych wynikach testów.

Polityka „używamy Qwena” albo „używamy Llamy” niewiele więc znaczy.

WNIOSEK

Polityka modeli wskazuje konkretne wagi z konkretnego źródła z sumą kontrolną.

Źródło: Heretic, GitHub; karty modeli w Hugging Face



Anthropic S-1/A: tempo rozwoju modeli w czynnikach ryzyka

W poprawionym prospekcie z 2 listopada Anthropic pisze, że w przeszłości zauważył znaczne przyspieszenie tempa rozwoju dopiero po fakcie i tak może być w przyszłości. Według TechCrunch za FT rating po debiucie ma być spekulacyjny.

Prawnicy piszą prospekt dla inwestorów, więc każde zdanie jest ważone.

WNIOSEK

Dostawcę modelu oceniałbym jak każdego krytycznego dostawcę: sytuacja finansowa, zarządzanie ryzykiem, plan wyjścia.

Źródło: SEC EDGAR, S-1/A, 02.11.2026; TechCrunch za FT



Niedobór pamięci: RTX 5080, Raspberry Pi 5 i OpenAI w Samsungu

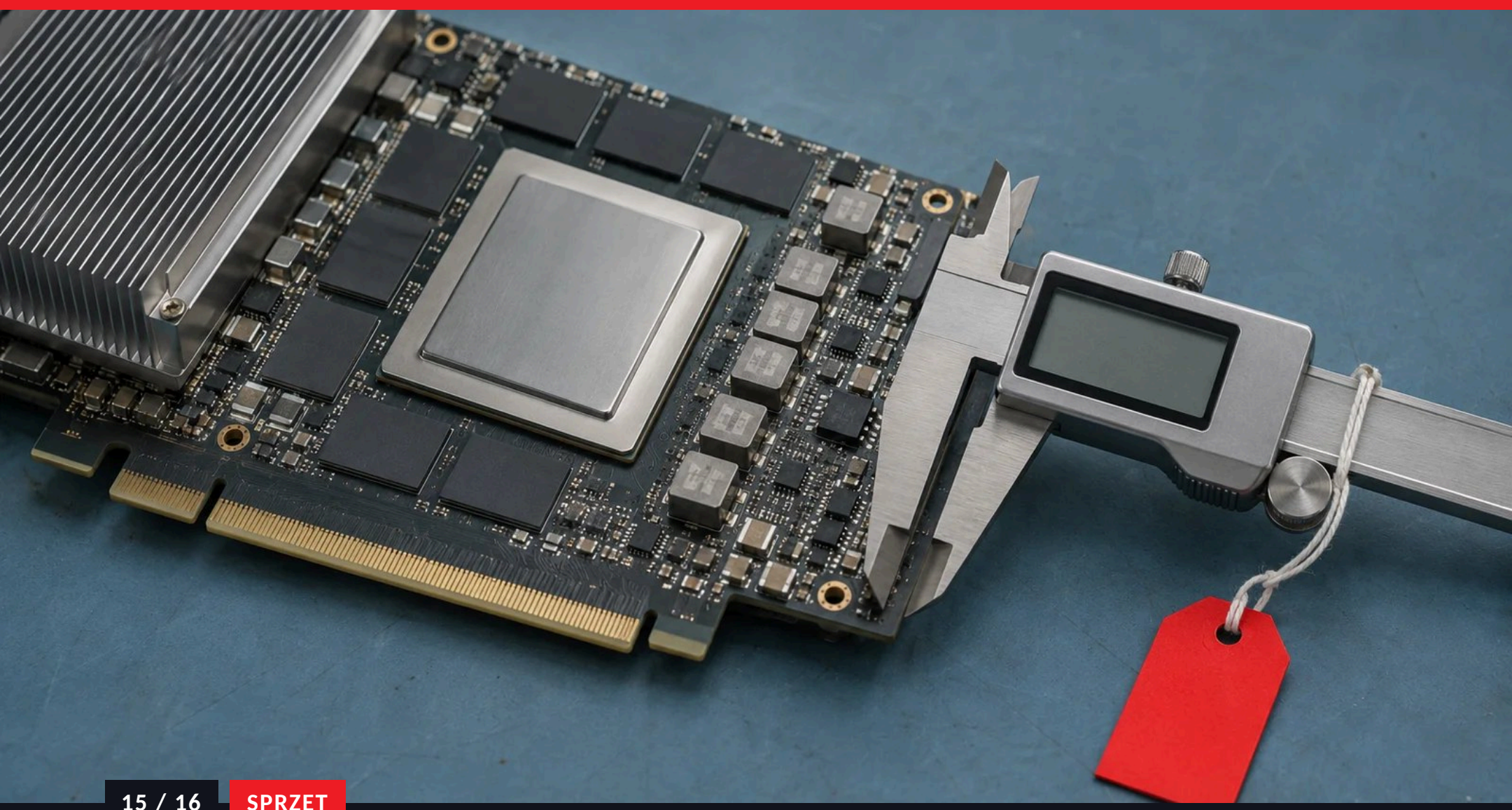
Raspberry Pi 5 z 16 GB podrożał o 80 USD, do 385 USD, z powodu braku alternatywnych dostaw pamięci DRAM. Według Tom's Hardware RTX 5080 zniknęła ze sklepu Nvidii, a Sam Altman spotkał się z kierownictwem Samsunga.

Niedobór sięga już także małych komputerów.

WNIOSEK

Projekty z własną infrastrukturą AI na 2027 rok warto planować z zapasem w budżecie i terminach dostaw.

Źródło: Raspberry Pi, 02.11.2026; Tom's Hardware



NVIDIA Rubin w parametrach wysyłkowych i wyniki AMD za III kwartał

Na stronie NVIDIA GPU Rubin ma przepustowość HBM4 19,2 TB/s wobec wstępnych 22 TB/s, czyli o 12,7% mniej. AMD w III kwartale 2026 roku miał 13 377 mln USD przychodu, a przychody segmentu Data Center wzrosły o 97% r/r.

Do wyceny liczy się karta produktu w dniu zamówienia.

WNIOSEK

Sizing sprzętu pod modele lokalne liczyłbym na parametrach wysyłkowych.

Źródło: NVIDIA, odczyt 05.11.2026; AMD, 03.11.2026



CSIRT Energia i trzy luki w programie Płatnik

Minister energii i PSE podpisali porozumienie o utworzeniu CSIRT Energia, piątego zespołu sektorowego. CERT Polska ostrzegł przed trzema lukami w Płatniku ZUS, w tym przed podmianą aktualizacji pobieranych po HTTP.

Źródła nie podają terminu uruchomienia zespołu. Aktualizacja Płatnika jest pilna.

WNIOSEK

Aktualizacja Płatnika w kadrach i biurach rachunkowych w tym tygodniu.

Źródło: CERT Polska, 30.10.2026; CRN.pl; Gramwzielone.pl

DO GRUDNIA

Pięć kontroli przed SAP Security Patch Day 8 grudnia

Do grudniowego SAP Security Patch Day zostało niespełna pięć tygodni. Z tego przeglądu wynika dla mnie pięć zadań.

1. Awaryjna ścieżka dla not SAP HotNews, liczona w dniach.
2. Lista dozwolonych modeli AI z konkretnymi wagami i sumą kontrolną.
3. Lista rozszerzeń dla wszystkich edytorów i przegląd tokenów wdrożeniowych.
4. Lista sterowników OT widocznych z internetu i firm serwisowych.
5. Poprawki jądra, APT i LXD oraz aktualizacja Płatnika.

Pełna wersja ze źródłami: **snok.ai**, wpis „Szybciej niż łatka”. Kontakt: office@snok.ai

Grafiki wygenerowane z pomocą AI. Stan wiedzy na 05.11.2026.