

SNOK

PRZEGLĄD TYGODNIA W46

Klucz pod wycieraczką

Przegląd SNOK za 6-12 listopada 2026: SAP Security Patch Day, agenci w UiPath i w sprzedaży biletów, OpenSSH i Outlook, phishing kodem urządzenia, sekrety w plikach agentów, nowe modele OpenAI i Anthropic, rezygnacja prezesa Nvidii

Przesuń →

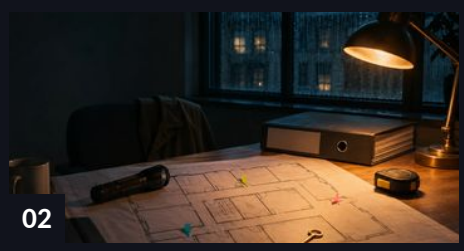
6-12.11.2026

Cztery noty SAP mają ocenę 10,0 i dotyczą komponentów, które odbierają ruch z sieci. Luka w OpenSSH otwiera się w określonej konfiguracji bardzo długim hasłem. Agent kodujący zapisuje czasem hasła w pliku ustawień, który użytkownicy dodają do publicznych repozytoriów.

W kilku tematach tego tygodnia dostęp leżał tam, gdzie każdy może zajrzeć.

Opisuję trzynaście tematów, przy każdym podaję fakty według źródeł i swój komentarz. Pełna wersja ze źródłami jest na snok.ai, we wpisie „Klucz pod wycieraczką”.

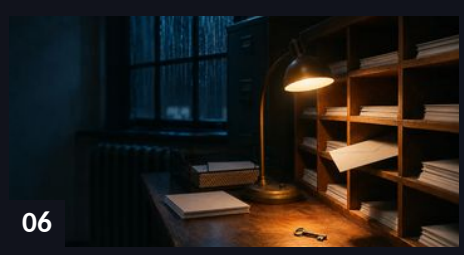

01


02


03


04

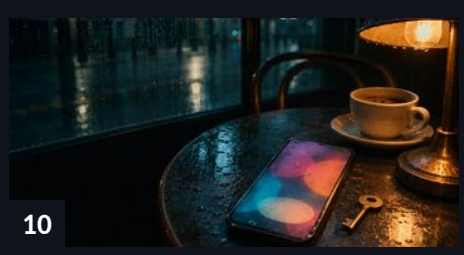

05

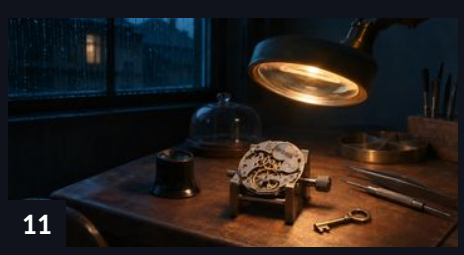

06


07

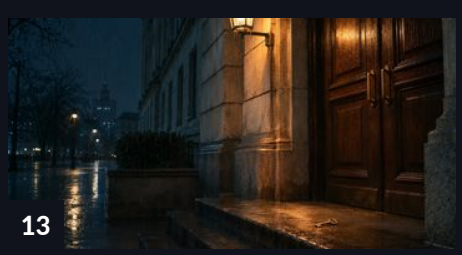

08


09


10


11


12


13



01 / 13 SAP

SAP Security Patch Day: 42 pozycje i cztery noty z oceną 10,0

10 listopada SAP opublikował 42 pozycje, w tym dziewięć krytycznych. Cztery noty mają ocenę CVSS 10,0: ICM w AS ABAP, SAP Web Dispatcher, SAP Gateway i usługa SAML2 w AS ABAP.

Maksymalna ocena oznacza atak przez sieć, bez uprawnień i bez udziału użytkownika. Wszystkie cztery dotyczą warstwy wejściowej: HTTP, RFC i logowania federacyjnego. SAP nie podaje, czy luki są wykorzystywane. Kolejny Patch Day wypada 8 grudnia.

WNIOSEK

W tym miesiącu zaplanowałbym wymianę jądra i sprawdził, które instancje ICM, Web Dispatchera i Gatewaya są osiągalne spoza sieci wewnętrznej.

Źródło: SAP Security Notes, 10.11.2026



OWASP SAP Pentest Playbook: otwarty zbiór technik testowania SAP

Projekt OWASP Core Business Application Security rozwija publiczny zbiór technik testów penetracyjnych SAP na licencji CC BY 4.0. Repozytorium prowadzi SecuritySilverbacks od maja 2025 roku, ostatnia zmiana pochodzi z 7 listopada. Wśród sponsorów jest SecurityBridge, którego jesteśmy partnerem.

To inicjatywa społeczności w statusie Incubator, bez statusu normy OWASP. Przydaje się jako wspólny słownik zarządu, zespołu Basis i wykonawcy testu.

WNIOSEK

Przed kolejnym pentestem SAP warto zapytać wykonawcę, które techniki z tej listy obejmuje, a które pomija.

Źródło: GitHub, SecuritySilverbacks; OWASP



UiPath partnerem startowym Gemini for healthcare

Przez UiPath MCP Server Gemini może uruchomić automatyzację, sprawdzić jej postęp albo przekazać zadanie agentowi UiPath, przy dotychczasowych uprawnieniach i audycie platformy. Integracja jest w wersji preview dla wspólnych klientów UiPath i Google Cloud.

Model prowadzi rozmowę, a wykonanie przechodzi przez platformę z uprawnieniami i audytem. Dostępność w UE nie jest potwierdzona.

WNIOSEK

Wzorzec „model wywołuje zarządzaną automatyzację przez MCP” warto ocenić na własnym procesie już teraz.

Źródło: UiPath, 10.11.2026



United nie pozwala zewnętrznym agentom AI kończyć rezerwacji

Według The Verge, za Wall Street Journal, United Airlines nie pozwoli zewnętrznym asystentom AI dokończyć rezerwacji w imieniu użytkownika. Agenci mogą nadal wyszukiwać i pokazywać loty.

Linia uzasadnia decyzję ochroną danych, ryzykiem niezamierzonych zakupów i wymogami informacyjnymi przy sprzedaży biletu. Linia dopuszcza ponowne rozważenie decyzji.

WNIOSEK

Integracja agenta z cudzym systemem powinna być uzgodniona i uwierzytelniona.

Źródło: The Verge, 11.11.2026



05 / 13 CYBER

SSHole: obejście logowania hasłem w OpenSSH na musl

CVE-2026-123158 dotyczy sshd na Linuksie z musl i bez PAM, z logowaniem hasłem. Dla niektórych kont z gwiazdką w polu hasła działa każde hasło dłuższe niż 256 bajtów, do 1024, jeśli w systemie jest inne konto z poprawnym hashem. Alpine ma takie ustawienia domyślnie.

Obejście jest w OpenSSH 10.6p2. CISA wpisała lukę do katalogu wykorzystywanych podatności 9 listopada. Dropbear i systemy z glibc lub PAM nie są podatne.

WNIOSEK

Najpierw warto zrobić inwentaryzację obrazów i urządzeń na musl, a do aktualizacji ustawić PasswordAuthentication no, po sprawdzeniu logowania kluczem.

Źródło: OpenSSH; CISA KEV



06 / 13 CYBER

Microsoft Patch Tuesday: jedna wykorzystywana luka, w Outlooku

Według Tenable Microsoft załatał 1093 luki we własnych produktach, a ze 142 lukami w Edge - 1235. Jedyna oznaczona jako wykorzystywana to CVE-2026-124194 w Outlooku: otwarcie spreparowanego pliku wiadomości ujawnia skrót NTLMv2. Ocena umiarkowana, CVSS 6,5, termin CISA 24 listopada.

Poprawka idzie kanałem Microsoft 365 Apps, nie zbiorczą aktualizacją Windows.

WNIOSEK

Zespół, który łata tylko serwery i system, tej poprawki nie zobaczy. Noty SAP i poprawki Microsoftu to w tym tygodniu dwa osobne kanały.

Źródło: Tenable; BleepingComputer; CISA KEV



Phishing kodem urządzenia pod szyldem wydarzeń AI

Push Security opisał fałszywe zaproszenia na wydarzenia z markami OpenAI i SpaceX, z nagrodami w rodzaju trzech miesięcy ChatGPT Pro. Ofiara wpisuje kod na prawdziwej stronie Microsoftu i sama autoryzuje urządzenie napastnika.

Przejęty token Entra otwiera aplikacje podłączone przez logowanie jednokrotne (SSO), w tym Microsoft 365, Salesforce, Atlassian i SAP.

WNIOSEK

Poprawny adres strony nie chroni. Nie wpisujcie kodu, jeśli to nie Wy zaczęliście logowanie; w Entra pomaga ograniczenie device code.

Źródło: Push Security; BleepingComputer, 05.11.2026



Claude Code: hasła w pliku „nie pytaj ponownie”

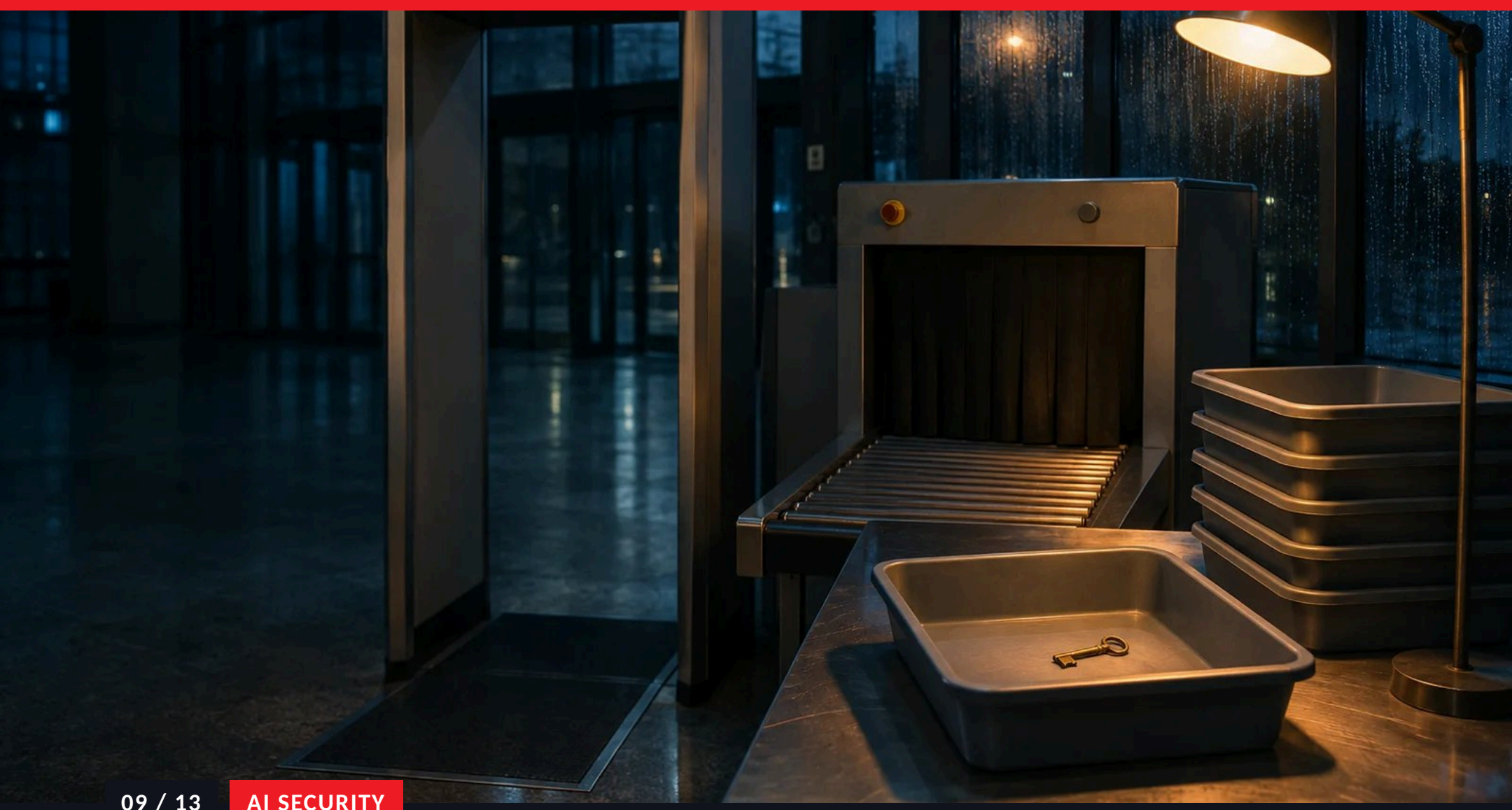
Według The Hacker News Apiiro znalazło sekrety w 1122 ze 104 185 kopii pliku .claude/settings.local.json w publicznych repozytoriach, łącznie 1379 różnych sekretów: hasła do baz, dane SSH, tokeny i klucze AWS. Żaden z dwóch skanerów, gitleaks i TruffleHog, nie wykrył ich w 215 plikach.

Plik zapisuje komendy zatwierdzone opcją „don't ask again”, czasem z hasłem w treści. Do repozytorium dodają go użytkownicy; Claude Code nie wpisuje go do .gitignore projektu.

WNIOSEK

Katalogi agentów kodujących warto traktować jak pliki .env: dopisać do .gitignore, przeskanować historię i zmienić znalezione hasła.

Źródło: The Hacker News za Apiiro, 07.11.2026



OpenAI GPT-6 Cyber dla wąskiego grona badaczy

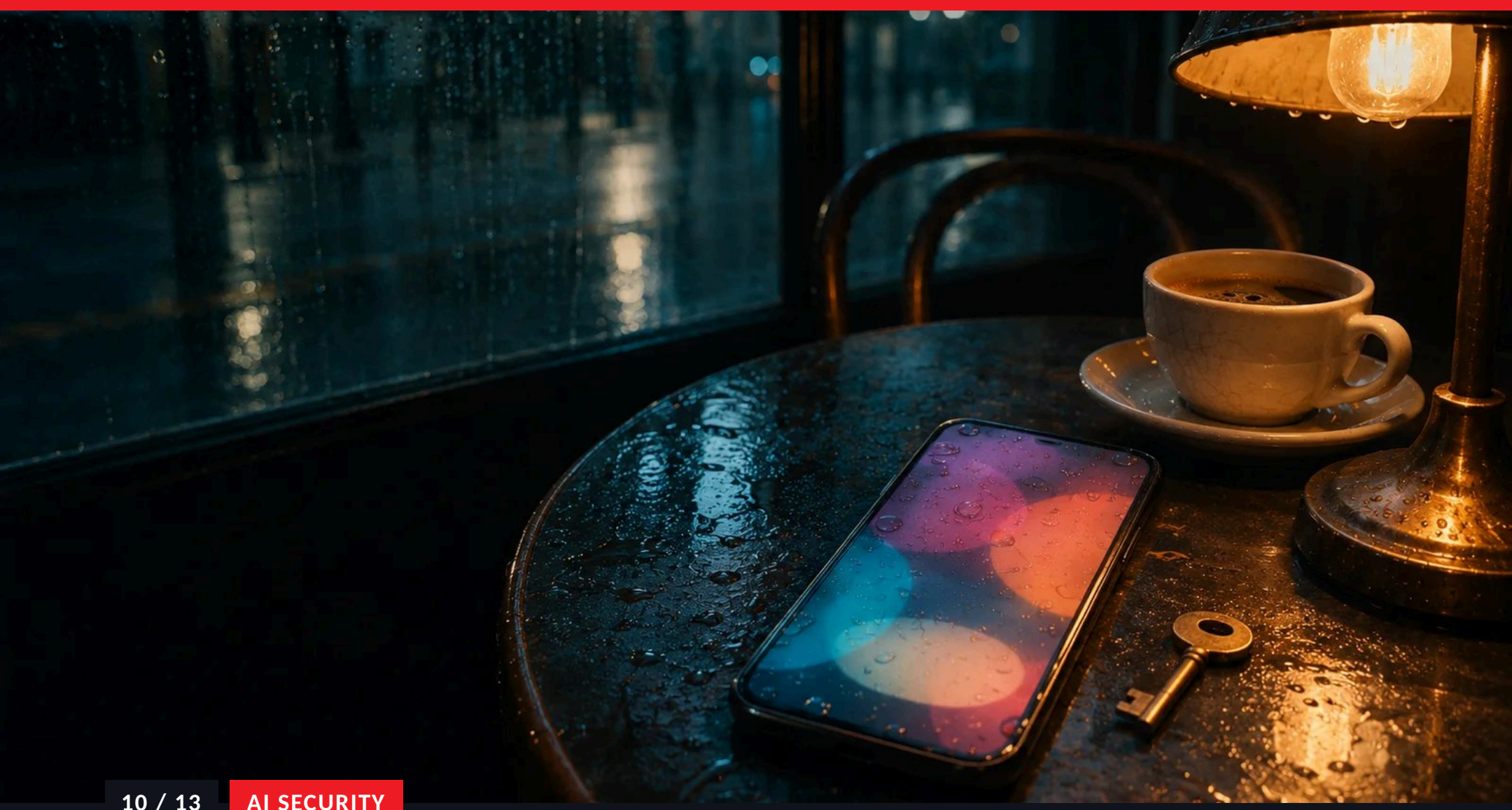
OpenAI ogłosiło GPT-6 Cyber dla wybranych klientów programu Daybreak Red. Według OpenAI przygotował exploity dla 948 podatności w jądrze Linux i znalazł 81 nieznanych luk w Firefoksie. Biuletyn Mozilli MFSA 2026-118 przypisuje OpenAI 41 wpisów; 81 może obejmować inne biuletyny.

Liczby pochodzą od producenta. Biuletyny Mozilli i komunikaty OpenSSH już wymieniają zgłoszenia przygotowane z pomocą AI.

WNIOSEK

Jeśli zgłoszeń luk będzie przybywać, w budżecie na przyszły rok uwzględniłbym krótszy cykl poprawek.

Źródło: BleepingComputer; TechCrunch; Mozilla



Agent mobilny widzi co innego niż człowiek

Preprint „When Agents See Differently” z arXiv: 546 zadań, 13 aplikacji, 5 frameworków agentowych i 3 modele.

Średni wskaźnik wprowadzenia agenta w błąd, czyli wyboru kontrolki wskazanej przez atakującego, wyniósł 77,4 procent w ewaluacji statycznej i 67,2 procent w dynamicznej, na poziomie aplikacji.

WNIOSEK

Przy czynnościach nieodwracalnych automatyzacja oparta na obrazie ekranu potrzebuje potwierdzenia człowieka.

Źródło: arXiv 2609.16732 (preprint)



Claude Fable 5.2 i Mythos 5.2: cena za token niższa o 20 procent

Ten sam model bazowy z różnymi zabezpieczeniami: Fable dla wszystkich, Mythos dla zweryfikowanych organizacji. Względem wersji 5.1 cena spadła z 10 do 8 USD za milion tokenów wejściowych i z 50 do 40 USD za wyjściowe.

Oba modele częściej niż ostatnie modele Anthropic sygnalizują podejrzenie, że są oceniane. Wymagają 30-dniowej retencji danych, tryb zero data retention tylko za zgodą Anthropic.

WNIOSEK

Przed zmianą modelu klient objęty NIS2 albo DORA powinien sprawdzić retencję i testować agenta w warunkach bliskich produkcji.

Źródło: Anthropic, 09.11.2026



Nvidia: rezygnacja Jensena Huanga

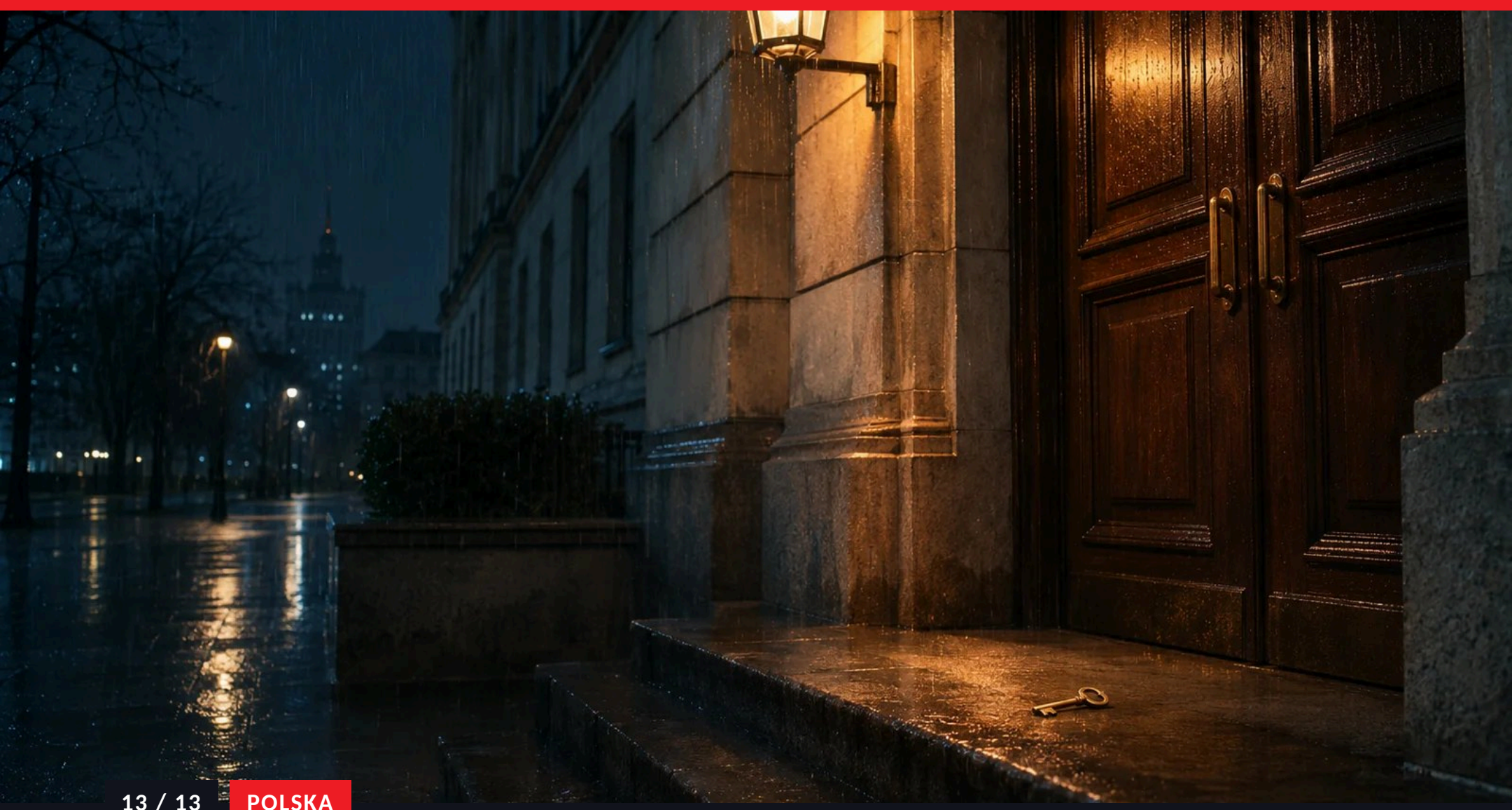
11 listopada rada dyrektorów przyjęła rezygnację Jensena Huanga ze skutkiem natychmiastowym. Obowiązki CEO pełni Colette Kress, przewodniczącym rady został Harvey C. Jones. Zgłoszenie do SEC nie podaje przyczyny.

Rezygnacja przyszła po dwóch tygodniach doniesień mediów o prezesie; spółka ich z nią nie łączy. Wyniki za III kwartał roku fiskalnego 2027: 17 listopada.

WNIOSEK

Nvidia ma tymczasowe kierownictwo, więc przy zakupach infrastruktury AI na 2027 rok warto mieć wariant zapasowy.

Źródło: Nvidia, 8-K, 11.11.2026



Ministerstwo Cyfryzacji i Microsoft: porozumienie o cyberodporności

Według CRN.pl i PAP współpraca obejmuje wymianę informacji o zagrożeniach, ochronę przestarzałych systemów, szybkie przywracanie usług i wykorzystanie AI w zespołach obrony administracji i infrastruktury krytycznej.

Komunikatu ministerstwa nie znaleźliśmy. Z relacji mediów nie wynikają nowe obowiązki prawne dla firm.

WNIOSEK

Priorytety administracji to przestarzałe systemy i ciągłość usług. Ocena skutków dla KSC i NIS2 wymaga komunikatu ministerstwa.

Źródło: CRN.pl; PAP, 10.11.2026

DO 8 GRUDNIA

Pięć rzeczy do sprawdzenia przed 8 grudnia

Do grudniowego SAP Security Patch Day zostały niespełna cztery tygodnie.
Z przeglądu wybrałem pięć miejsc, w których dostęp mógł zostać pod wycieraczką.

1. Które instancje ICM, SAP Web Dispatcher i SAP Gateway są osiągalne spoza sieci wewnętrznej.
2. Które obrazy kontenerów i urządzenia mają OpenSSH na musl i logowanie hasłem.
3. Czy poprawka Outlooka z kanału Microsoft 365 Apps została sprawdzona osobno.
4. Kto naprawdę potrzebuje przepływu device code w Microsoft Entra.
5. Czy katalogi .claude, .cursor i .gemini są w .gitignore i czy ich historię przeskanowano.

Pełna wersja ze źródłami: **snok.ai**, wpis „Klucz pod wycieraczką”. Kontakt: office@snok.ai

Grafiki wygenerowane z pomocą AI. Stan wiedzy na 12.11.2026.