



SNOK

WEEKLY DIGEST • W38 • 11-17.09.2026

Nie narzędzie, tylko droga

Dziesięć pozycji z tygodnia, z komentarzem, co każda zmienia w Waszych systemach

MOTYW WYDANIA

SAP Security Patch Day z 8 września dał notę o ocenie 9,8. Cztery doby później istniał publiczny opis mechanizmu, a tego samego wieczoru działający dowód w labie. To nie jest historia o jednej podatności - to pierwsza z dziesięciu pozycji, w których rozstrzygnięcie ani razu nie brzmiało, które narzędzie kupić.

Za każdym razem brzmiało inaczej: którą drogą pójść. Łatać kernel czy dokręcić parametr komunikacji wewnętrznej. Monitorować jedną drogę do danych bankowych czy wszystkie osiem. Dać agentowi dokument w indeksie czy żywy rekord. Te decyzje zapadają raz, zwykle wcześniej i zwykle przy okazji czegoś innego.

96 godzin od noty do dowodu

8 dróg do tego samego pola

24 klauzule umowne dla AI

Dziewięćdziesiąt sześć godzin od noty do działającego kodu

SAP Security Patch Day z 8 września przyniósł notę 3759472. Luka siedzi w SAP Message Server: brakuje sprawdzenia autentyczności przy zapisie wpisu bramki, więc nieuwierzytelniony klient podaje własny host i port, a kernel rozgłasza tę tożsamość do wszystkich serwerów aplikacyjnych w krajobrazie.

Cztery doby później ukazała się publiczna analiza różnicy w kernelu, a tego samego dnia zespół badawczy miał działający dowód. Przy odtwarzaniu formatu danych pracował asystent kodowania AI, co badacze podają wprost. Ocena 9,8, kategoria HotNews, bez obejścia.

WNIOSEK

Kwartalne okno łatania straciło pokrycie w rzeczywistości - dystans do publicznego kodu liczy się w dniach.

Linia kernela 9.x to główny nurt S/4HANA; kernele 7.x i 8.x nie mają tej rodziny poleceń.

Źródło: SecurityBridge Research Lab i Onapsis, SAP Security Note 3759472, wrzesień 2026

Osiem dróg do tego samego pola

W pokazie producenta zmieniono dane bankowe ośmioma różnymi drogami - przez transakcje alternatywne, mechanizmy transportu, rozwój własny oraz interfejsy i procesy tła. Żadna nie wywołała alertu, bo monitorowana była droga zamierzona, czyli standardowa transakcja.

Druga teza dokłada wymiar czasu. Bezpieczeństwo SAP stoi tam, gdzie sieć stała dwadzieścia lat temu: potrafi wykryć i zgłosić, nie potrafi zatrzymać. Atakującemu wystarcza czas między alertem a reakcją człowieka.

WNIOSEK

Lista ról mówi, kto może wejść drzwiami. Nie mówi, kto wszedł oknem ani jak szybko zostanie stamtąd zdjęty.

Liczba osiem opisuje demonstrację w konkretnym środowisku, nie właściwość systemu.

Źródło: SecurityBridge, Breaking the Rules oraz webinar o danych bankowych, 2026

Siedemdziesiąt osiem plików instrukcji i sześć tysięcy gwiazdek

Publiczny pakiet na GitHub zamienia asystenta kodowania w narzędzie pracy ofensywnej. Policzyliśmy zawartość repozytorium: 78 plików instrukcji w 23 kategoriach, ładowanych na żądanie. Repozytorium powstało w marcu i ma już 6011 gwiazdek.

Istotna jest mechanika, nie pakiet. To nie jest exploit do skompilowania, tylko pliki tekstowe, które ktoś wrzuca do katalogu asystenta. Powierzchnia ataku rośnie o gotową metodykę, a nie o nowe narzędzie.

WNIOSEK

Cudzy plik instrukcji dla agenta to niezaufany kod, nie dokumentacja. Polityka zakupowa takiego przypadku nie obejmuje.

Bramka przed instalacją: skan skilli agentowych pod wstrzyknięcie poleceń i wyciek danych.

Źródło: Repozytorium SnailSploit/Claude-Red, metadane pobrane 17.09.2026

Prawie trzy tysiące komend w pakiecie dystrybucji

Klasyczny launcher komend używanych w testach penetracyjnych został przepisany w języku Go i trafił do oficjalnych repozytoriów dystrybucji Kali Linux. Opis projektu mówi o 247 narzędziach, 2926 komendach i ponad dwustu ściągach.

To nie jest nowy silnik ataku, tylko warstwa produktywności nad narzędziami, które istnieją od lat. Zestawiona z pozycją poprzednią pokazuje, że próg wejścia spada dwoma niezależnymi kanałami naraz.

WNIOSEK

Obrona planuje pracę wobec przeciwnika, który nie musi już pamiętać składni ani kolejności kroków.

Zmierzyliśmy metadane projektu; liczby narzędzi i komend pochodzą z jego opisu.

Źródło: Repozytorium [halilkirazkaya/arsenal-ng](#), metadane pobrane 17.09.2026

Grounding na dokumencie odpowiada na inne pytanie

UiPath opisał warstwę, przez którą agent sięga po żywe rekordy w systemach klienta, zamiast pracować na wektorach zbudowanych z dokumentów. Cztery wymagania: stan bieżący, struktura pozwalająca filtrować i łączyć, modele encji budowane raz oraz uprawnienia i ślad pochodzenia w standardzie.

Wyszukiwanie po podobieństwie odpowie na pytanie o treść polityki zwrotów. Nie odpowie, które zgłoszenia w regionie są po terminie, bo to zapytanie z filtrem i złączeniem, a odpowiedzią jest liczba policzona z wierszy.

WNIOSEK

Projekt zaczęty od wektoryzacji dokumentów kończy się agentem elokwentnym i nieoperacyjnym.

Materiał producenta - zakres wspieranych systemów nie jest w nim wymieniony.

Trzy wzorce orkiestracji na jednym silniku

Orchestrator zarządza wykonawcami, a Maestro prowadzi proces, którego ci wykonawcy są częścią. Pod spodem stoi silnik trwałego wykonania, więc proces zatrzymany na zatwierdzeniu wznowia się dokładnie w miejscu zatrzymania i przeżywa awarię systemu, od którego zależy.

Na tym silniku stoją trzy wzorce. Strukturalny w notacji modelowania procesów, gdy ścieżka jest znana z góry. Skierowany do kodu, gdy logika jest czytelniejsza w repozytorium. Adaptacyjny, gdy następnego kroku nie da się przewidzieć na etapie projektu.

WNIOSEK

Wybór wzorca jest konsekwencją procesu, nie preferencją konsultanta. Pomyłka kosztuje przepisanie, nie przekonfigurowanie.

Kanwa dla deweloperów jest w podglądzie publicznym; daty dostępności ogólnej źródło nie podaje.

Źródło: UiPath, materiały produktowe o Maestro i Maestro Flow, wrzesień 2026



07 • UIPATH • BUDOWA AGENTA

Trzy drogi i koszt wybrania nie tej

Trzy ścieżki budowy agenta są równorzędne: zestaw programistyczny w Pythonie, agenty kodowane przez wiersz poleceń oraz kanwa w przeglądarce. Materiał producenta opisuje wszystkie jako pełnoprawne i nie rozstrzyga, od której zacząć.

To nie jest wybór smaku, tylko rozstrzygnięcie, ile kontroli bierze zespół. Zestaw programistyczny daje najwięcej swobody i najwięcej roboty. Kanwa daje najszybszy start i najmniej wpływu na szczegóły. Wiersz poleceń trzyma kod pod kontrolą wersji.

WNIOSEK

**Rozmowa o drodze na starcie kosztuje godzinę.
Pominięta kosztuje przeróbkę.**

Projektu nie przenosi się między ścieżkami bez przepisania.

Źródło: UiPath, materiał o drogach budowy agenta, wrzesień 2026

Lider kwadrantu i wdrożenie z liczbami

Drugi rok z rzędu pozycja lidera w kwadrancie firmy badawczej dla przetwarzania dokumentów; raport nosi datę 8 września. Równolegle studium przypadku operatora telekomunikacyjnego: trzy agenty w produkcji, roboty w roli narzędzi agenta.

Asystent wiedzy odpowiada w sekundach zamiast w dniach i zdejmuje od 25 do 30 tysięcy roboczogodzin rocznie. Najtrudniejsze zastrzeżenie brzmi jednak inaczej: czy nie kupujemy technologii na wylocie. Wygenerowanie odpowiedzi to nie to samo co domknięcie procesu.

WNIOSEK

Walidacja, progi zatwierdzeń i dziennik audytowy to problemy wykonania, nie problemy inteligencji.

Firma badawcza nie rekomenduje dostawców, a jej publikacje są opiniami, nie stwierdzeniami faktu.

Źródło: Komunikat UiPath dla inwestorów oraz studium przypadku PLDT, wrzesień 2026

Dwadzieścia cztery klauzule i pytanie, kto bierze ryzyko

Praktyk prawa zestawiał katalog postanowień umownych w dwóch rolach: osiemnaście chroniących tego, kto system stosuje, i sześć chroniących dostawcę. Po stronie stosującego wracają te same punkty - zakaz trenowania na danych użytkownika, notyfikacja zmian i realny nadzór człowieka.

Trzy uwagi z dyskusji ważą więcej niż część listy. Trenowanie to nie retencja. Notyfikacja zmian musi obejmować podmiannę modelu bazowego. Odpowiedzialność kontraktowa nie zastępuje potwierdzenia, że system wolno stosować dziś.

WNIOSEK

Zgodność przenosi się z prezentacji do załącznika umowy, gdzie interesy stron są rozbieżne.

To nie jest porada prawna - interpretacje wymagają przeglądu prawnika przed użyciem.

Sto osiemdziesiąt miliardów parametrów przy biurku

Model gęsty o 27 miliardach parametrów mieści się w około 17 gigabajtach po kwantyzacji czterobitowej i niesie kontekst 262 tysięcy tokenów natywnie. Przepis społecznościowy serwuje wariant rzadki o 180 miliardach parametrów na jednym urządzeniu klasy biurkowej.

Druga rzecz jest mniej efektowna i ważniejsza. Trzy warianty tej samej rodziny mają trzy różne reżimy licencyjne, w tym jeden z progiem przychodowym i jeden wyłączający udostępnianie modelu jako usługi.

WNIOSEK

Rozmowa o suwerenności danych przestaje być wyborem, a staje się rachunkiem. Licencję sprawdza się przed wyceną.

Prędkości pochodzą z opisu przepisu jednego autora - nie jest to nasz pomiar.

Źródło: Karta modelu Qwen3.8-27B na Hugging Face oraz przepis społecznościowy, 14.09.2026



Jedno zdanie na ten tydzień

W dziesięciu pozycjach rozstrzygnięcie nie dotyczyło tego, które narzędzie kupić. Dotyczyło drogi: łąta kernela albo parametr komunikacji wewnętrznej, jedna monitorowana droga albo wszystkie osiem, dokument w indeksie albo żywy rekord. Każda z tych decyzji zapada raz i wyznacza, kto później odpowiada, ile to kosztuje i jak szybko da się zareagować.

snok.ai

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

Materiał informacyjny. Nie stanowi porady prawnej ani inwestycyjnej.