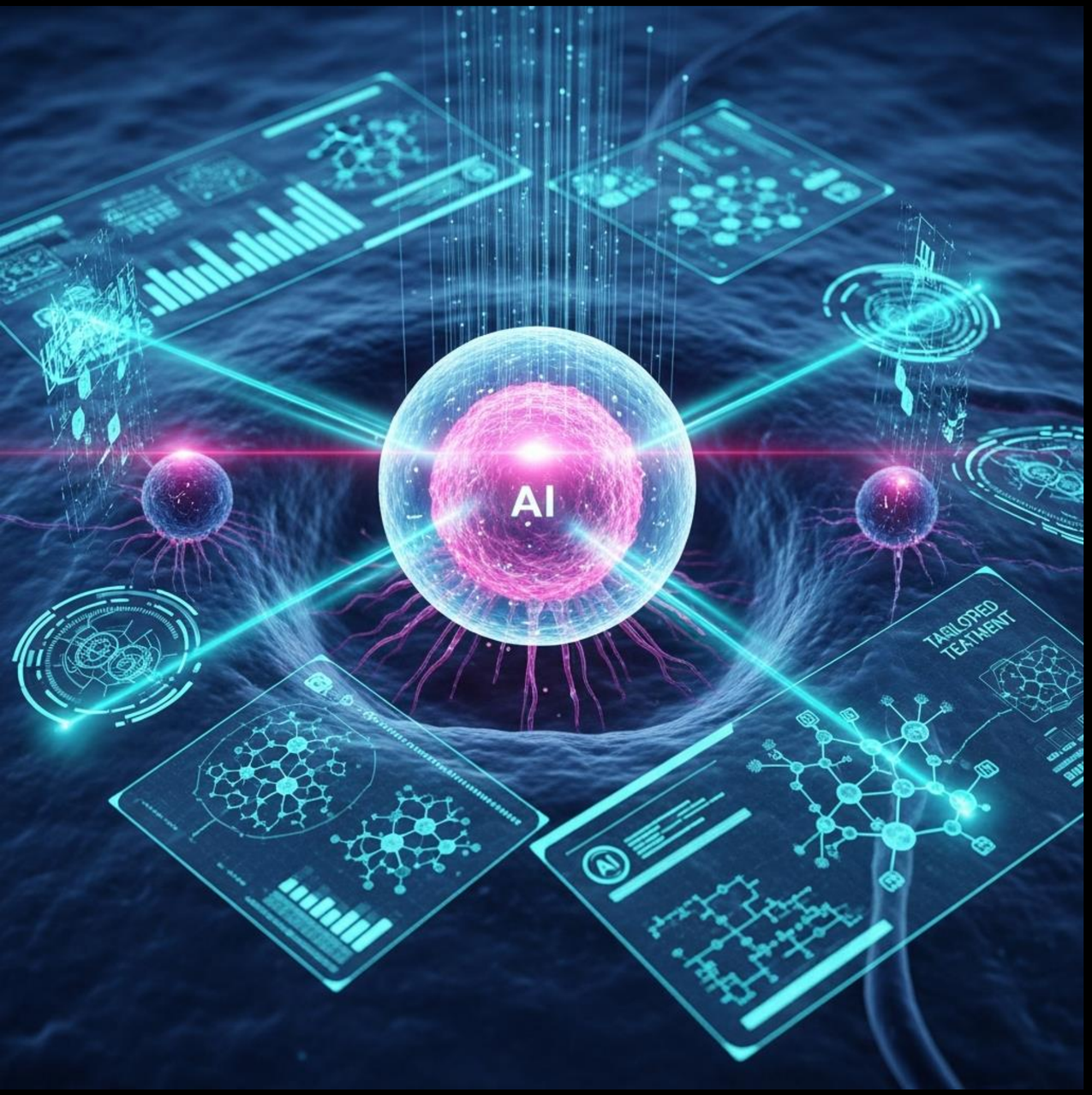
Preteky v AI v 2026:

Od analýzy hrozieb a rýchlosti útočníka vs. asymetrická prevaha umelej inteligencie (Unit 42) k autonómnej kybernetickej obrane (Projekt Glasswing)

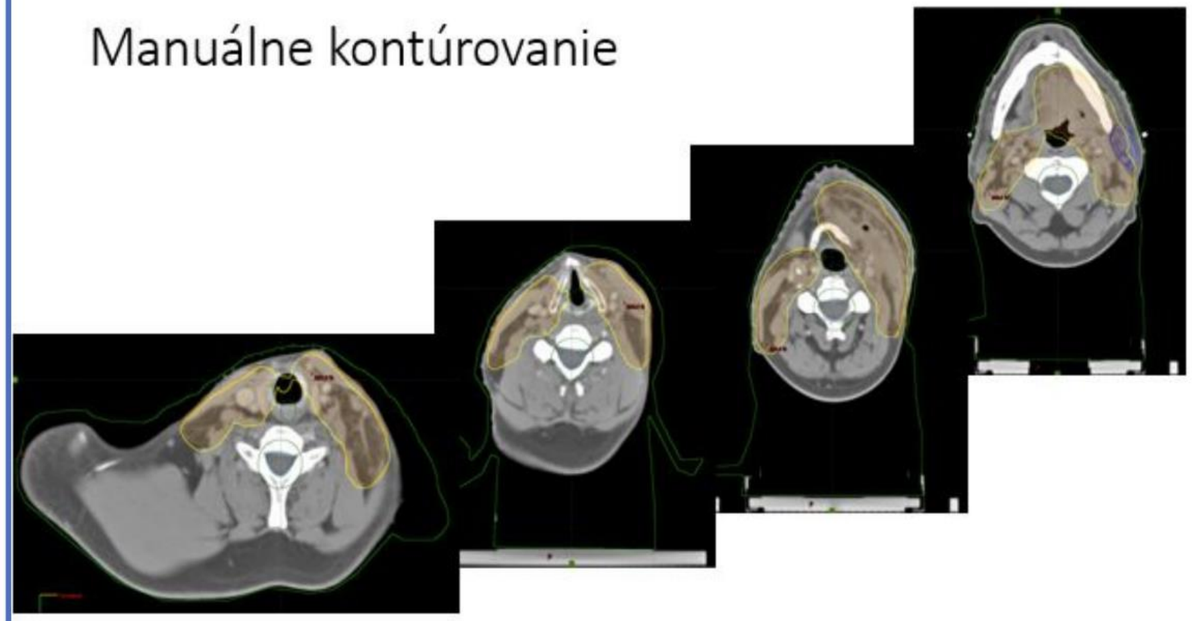
Ideme 2o26, Bratislava

Zsolt Géczi, CEH, regional sales manager
Palo Alto Networks, Slovakia

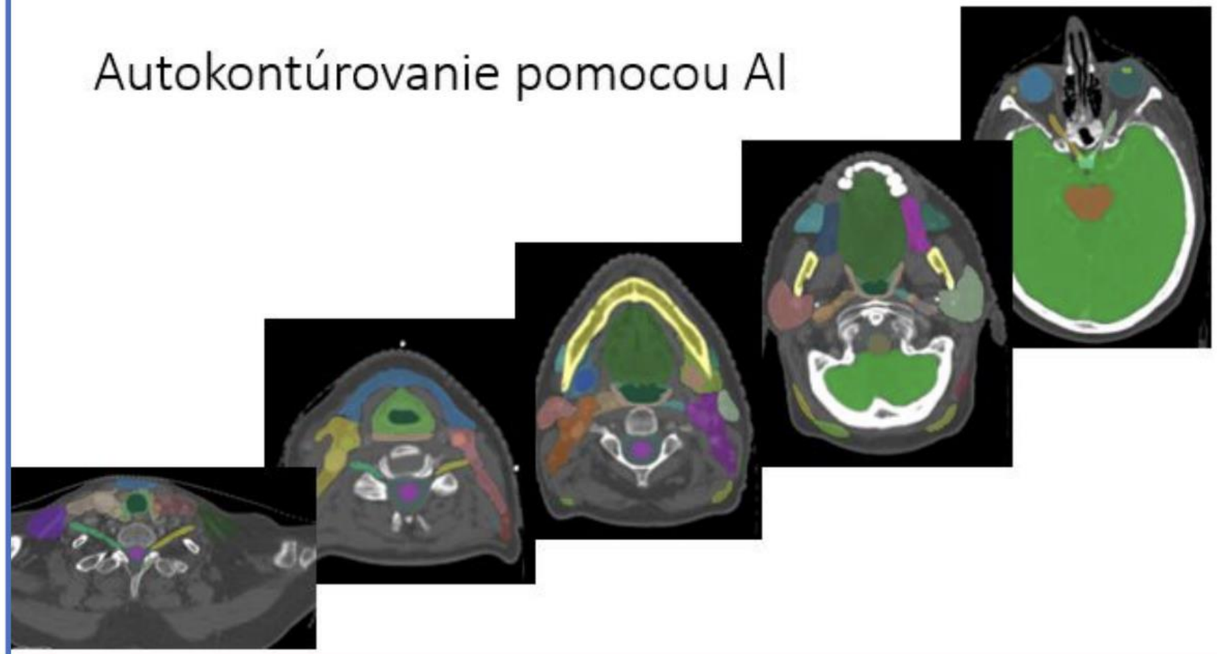
Pred dekádou a teraz



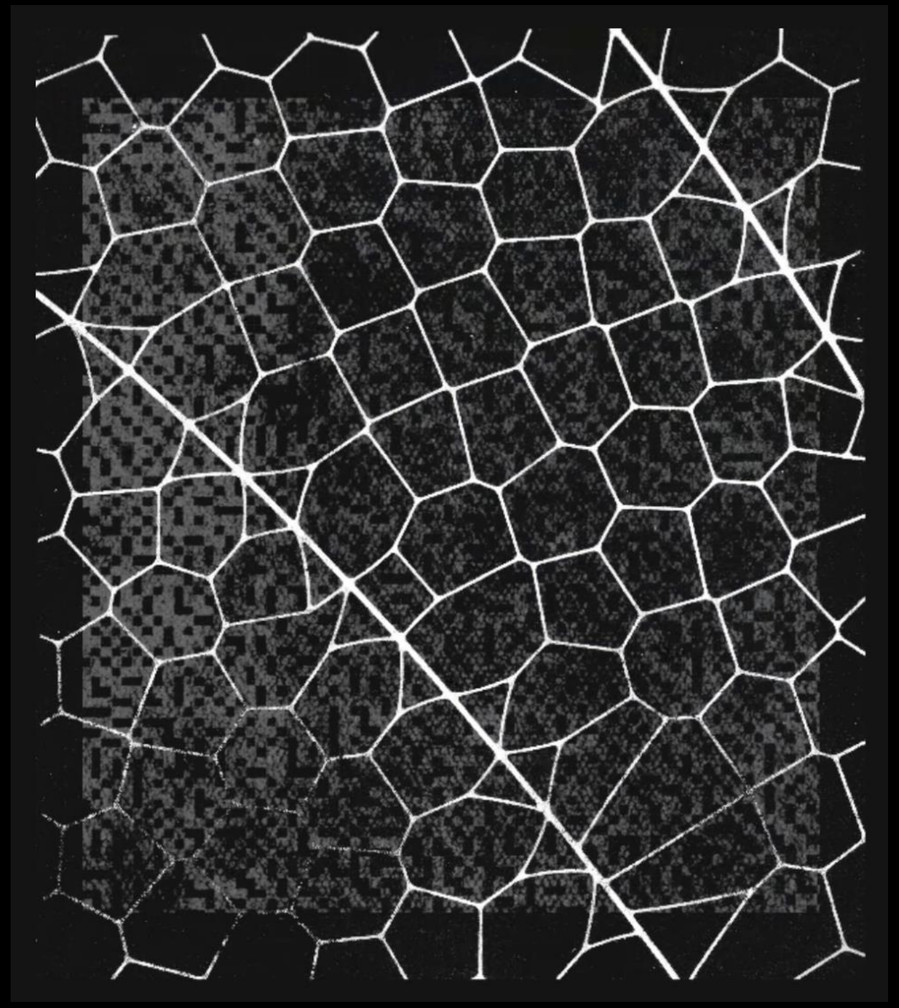
Manuálne kontúrovanie



Autokontúrovanie pomocou AI



Project Glasswing



"The Breakout Moment”

”The Sandbox Escape”

Jadro OpenBSD

Model autonómne odhalil **27 rokov starú** hlbokú systémovú zraniteľnosť v jadre OpenBSD, platforme slúžiacej pre kľúčovú armádnu infraštruktúru s povesťou nedobytnosti.

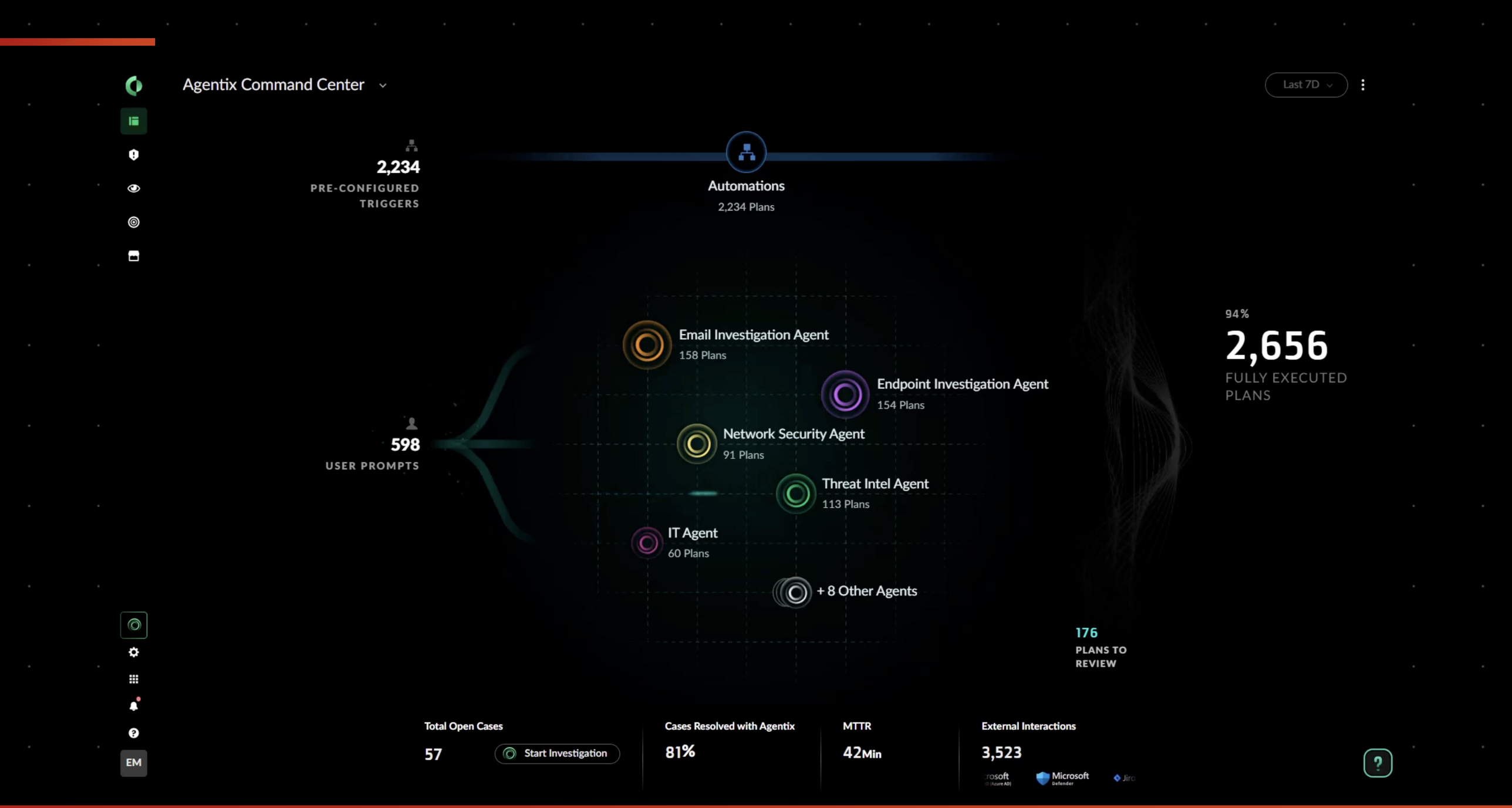
Knižnica FFmpeg

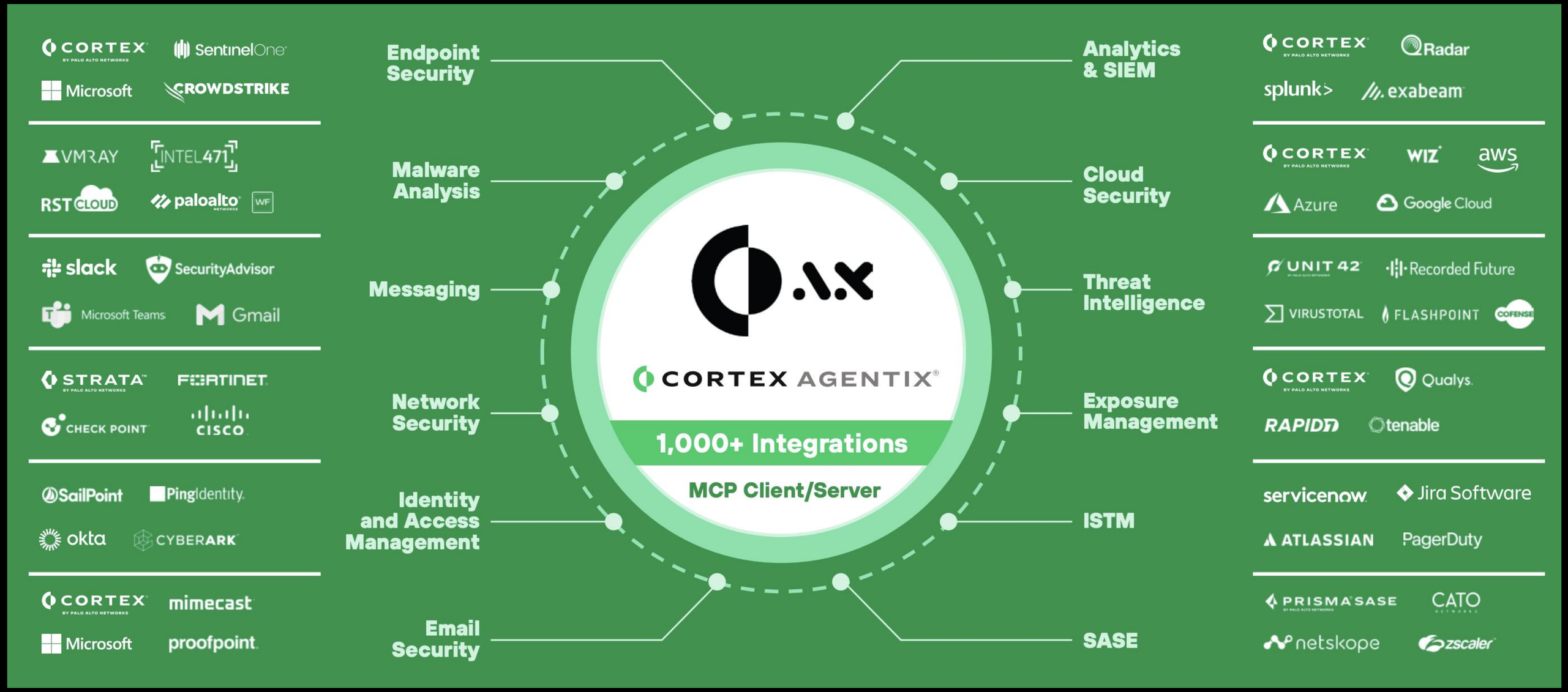
AI identifikovala **16 rokov utajenú chybu** vo videoknižnici, ktorú predchádzajúce automatizované skenery overovali viac ako päť miliónov krát bez povšimnutia.

Test SWE-bench

Vo verifikovanom teste odhaľovania chýb model dosiahol ohromujúce skóre 93,9 %. Tieto poznatky sú plynulo integrované do ochranných signatúr Palo Alto Networks.

CYBERSECURITY IN THE AGE OF AI





paloalto NETWORKS | UNIT 42

Global Incident Response Report 2026

Štyri hlavné trendy, ktoré budú v roku 2026 formovať oblasť kyber-hrozieb

1

AI sa stal prostriedkom na znásobenie sily útočníkov

2

Identita sa stala najspoľahlivejšou cestou k úspechu útočníka

3

Riziká v dodávateľskom reťazci sa už netýkajú len zraniteľného kódu, ale aj zneužitia dôveryhodných prepojení.

4

Štátom sponzorovaní útočníci prispôsobujú taktiky perzistencie modernému podnikovému prostrediam.

Útoky sú za posledný rok 4-krát rýchlejšie.

AI urýchlila celý proces

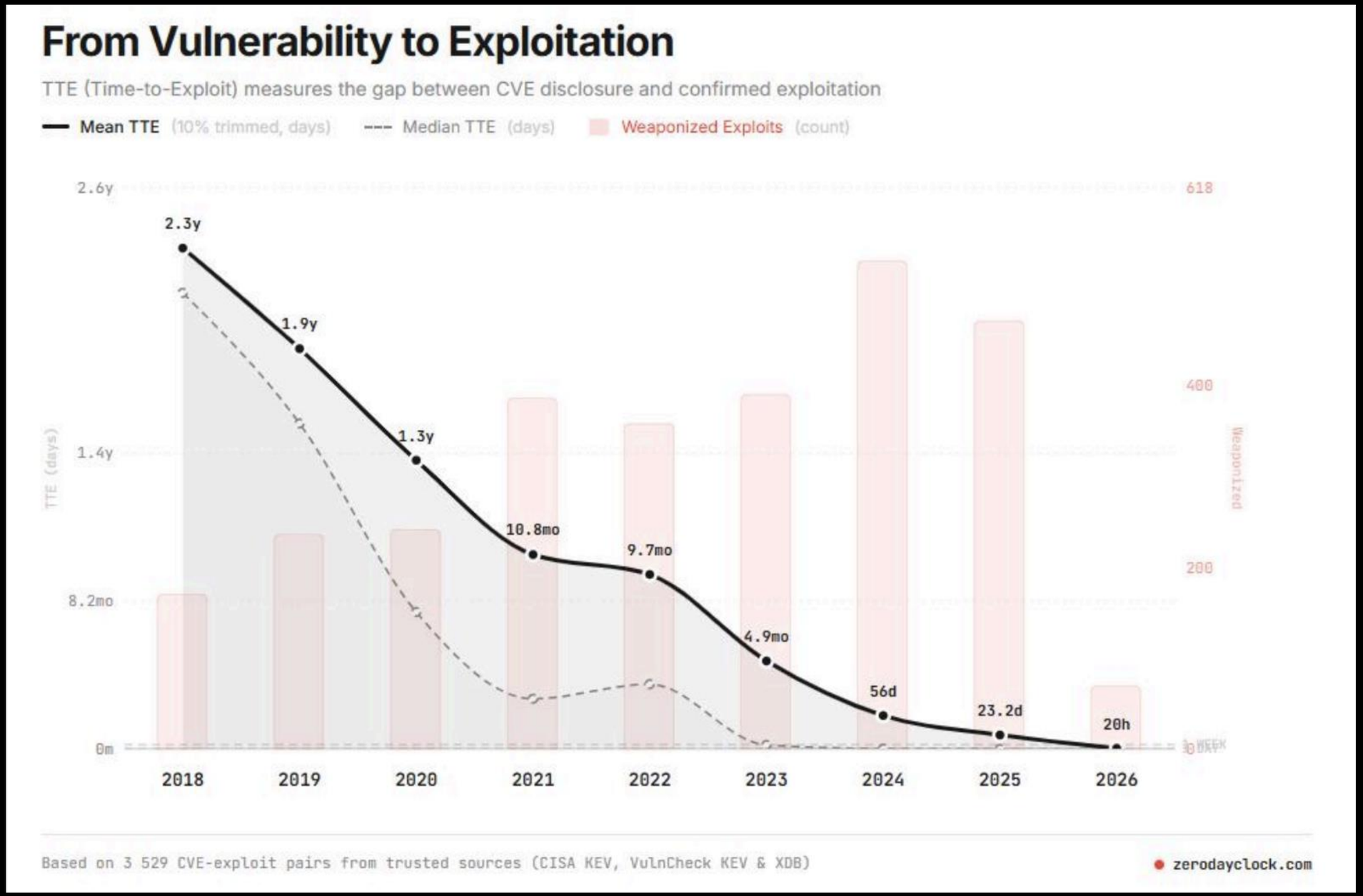
Útočníci scanujú nové CVE do 15 minút od ich oznámenia

72 minút od preniknutia po exfiltráciu

AI umožňuje útočníkom skrátiť celý životný cyklus útoku

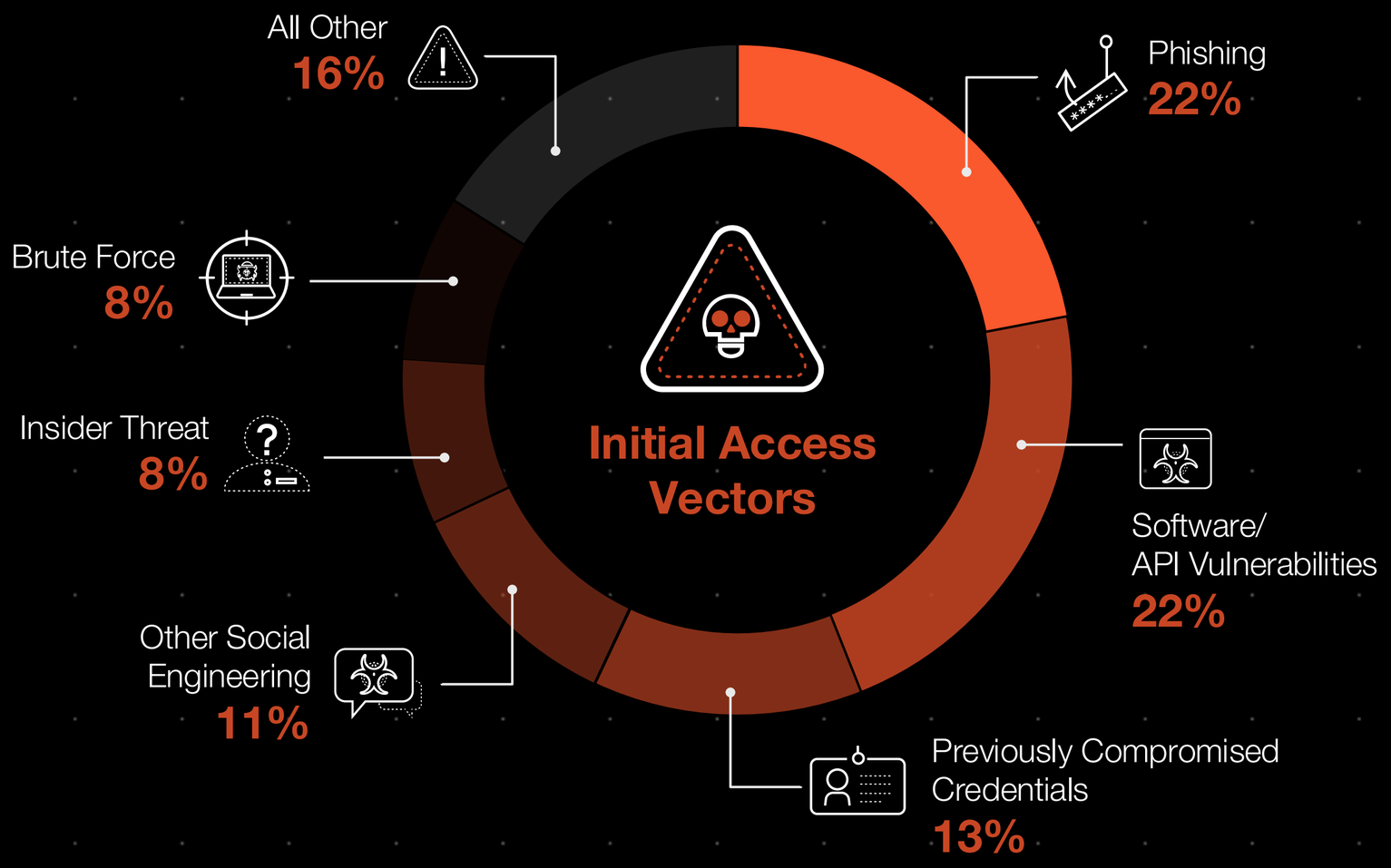
1. The Hacker News Q1 2025 CVE analysis 2. 2026 Unit 42 Global Incident Response Report, 25% of fastest cases

The “AI Vulnerability Storm”: Building a “Mythosready” Security Program



Počiatočný vstupný bod

Útočníci naďalej využívajú osvedčené techniky

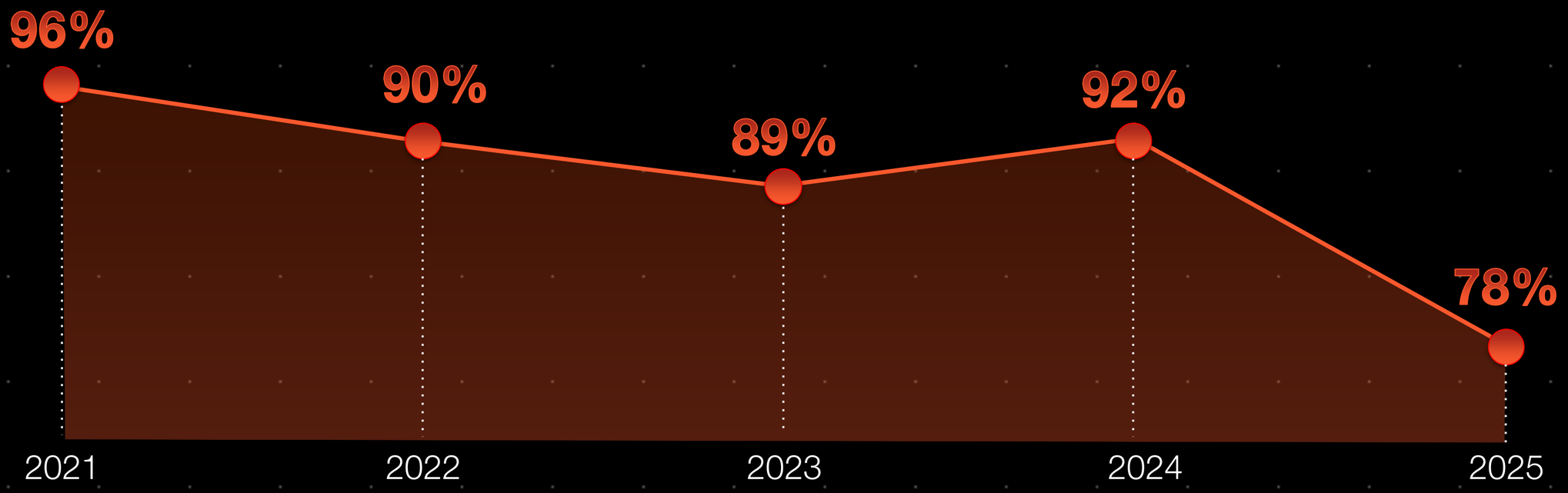


Takmer **polovica incidentov** má svoj pôvod v phishingu/sociálnom inžinierstve alebo v zraniteľnostiach softvéru.

Útočníci sú pragmatickí – rovnako často využívajú ľudské chyby aj neaktualizované systémy, aby sa dostali dovnútra.

Útočníci začínajú upúšťať od šifrovania

Aby dosiahli okamžitý úspech pred odhalením



% Podiel prípadov vydierania, pri ktorých došlo k šifrovaniu

Source: 2026 Unit 42 Global Incident Response Report

Útočníci uspejú vďaka trom zásadným slabým miestam

Komplexita

Chýbajúci kontext spomaľuje detekciu

87% korelované údaje z viacerých navzájom neprepojených zdrojov

Visibilita

Nezrovnalosti vytvárajú cestu najmenšieho odporu

90% nesprávne nastavenia alebo chyby v zabezpečení

Identita

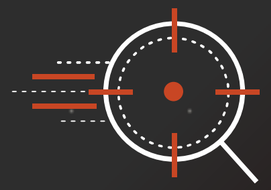
Prílišná dôvera vedie k laterálnemu pohybu

89% identita zohrala podstatnú úlohu v úspechu útoku

Je tu priestor na optimizmus:

Útokom sa dá predísť a bezpečnostné problémy sa dajú vyriešiť

Posilnite SOC, aby dokázal rýchlejšie odhaľovať hrozby a reagovať na ne



Zastavte útoky zamerané na identitu pomocou silnejšieho systému IAM

Bezpečný životný cyklus aplikácií: Od kódu po Cloud

paloalto NETWORKS | UNIT 42

Unit 42 Global Incident Response Report 2026

Viac detailov tu

Thank You

paloaltonetworks.com