Elvárások vs. valóság 2026-ban

A Next Gen SOC anatómiája

Barna Tamás, CISSP, CCSP, Security+
Senior System Engineer · TrendAI

InfoKom 2026 · SOC Evolution szekció

„Patch Tuesday, exploit Wednesday.” Kedden jön a javítás, szerdán a támadás.

Alex Stamos, a Facebook korábbi biztonsági vezetője · RSAC 2026

TrendAI™

Elvárások vs. valóság 2026-ban

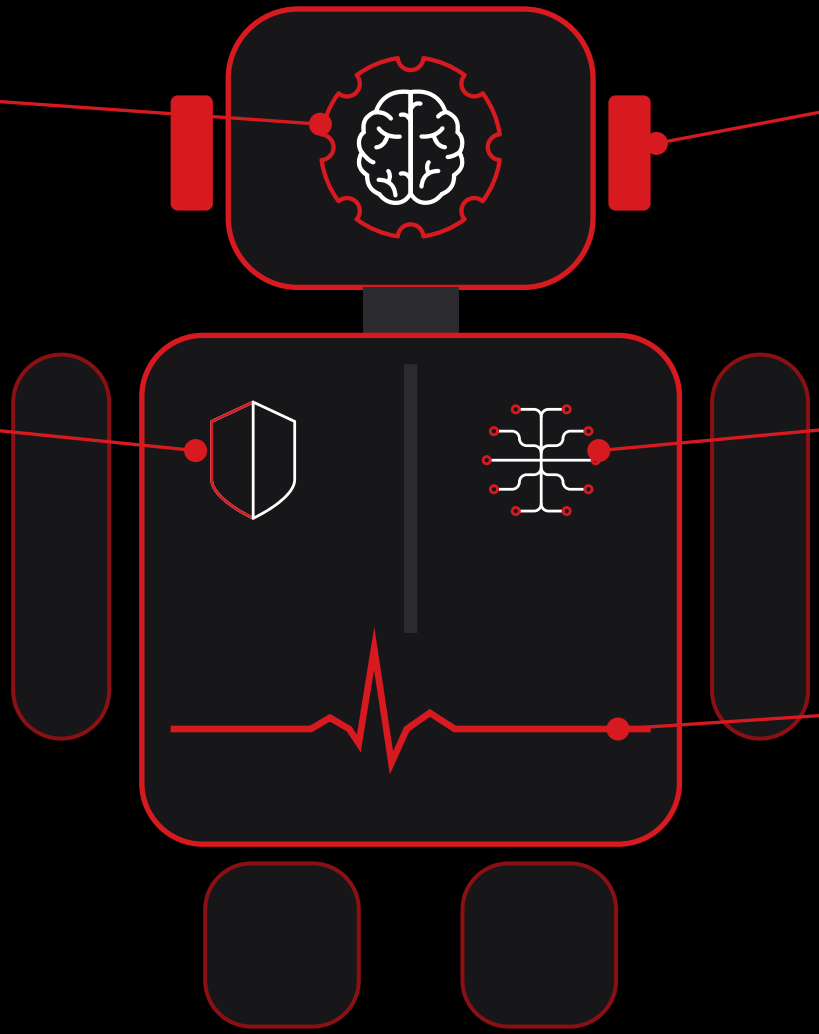
Amit a Next Gen SOC-tól várunk		Ahol a valóság gyakran tart
Előre jelzi a kockázatot	vs.	Riasztás után reagál
Egy platform, egy kép	vs.	Sok eszköz, sok konzol
Üzleti kockázatról beszél	vs.	Technikai riasztásokat számol
Védi és használja az AI-t	vs.	Az AI többnyire láthatatlan

TrendAI™

A páciens: egy Next Gen SOC anatómiája

Agy
AI, amely elemez és cselekszik

Érzékszervek
Láthatóság: felhő, konténer, AI



Immunrendszer
Proaktív megelőzés

Idegrendszer
Platform és egységes adatréteg

Pulzus
Új KPI-ok: MTTD, MTTP, MTTU

KÓRLAP

Páciens: SOC, 2026

Panasz: sok riasztás, kevés kontextus

Terápia: lásd a következő diákat

TrendAI

Érzékszervek: a kódtól a futásig látni kell

Kód	Build	Registry	Deploy	Futás
KOCKÁZAT	KOCKÁZAT	KOCKÁZAT	KOCKÁZAT	KOCKÁZAT
Titkok a repóban, sérülékeny függőségek	Fertőzött image, malware, beégetett kulcs	Elavult, sérülékeny image-ek	Hibás konfiguráció, túl széles jogosultság	Konténerszökés, eltérés a telepített állapottól
Code Security	**Artifact Scanner a CI/CD-ben**	**Agentless Vulnerability & Threat Detection**	**Admission control, CSPM, CIEM**	**Container Security, Server & Workload Protection**

VÉDELMI PONT A TRENDAI VISION ONE-BAN

Microservice-ek és AI-munkaterhelések: minden lépés telemetriája egy adatrétegbe fut (XDR for Cloud, Agentic SIEM)

TrendAI™

Idegrendszer: kevesebb eszköz, több kontextus



Végpont



E-mail



Felhő



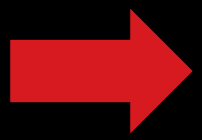
Hálózat



Identitás



Adat





TrendAI Vision One

Egy platform, egy adatréteg

- Konszolidálni: kevesebb konzol és licenc
- Integrálni: kockázat, detekció és válasz együtt
- Egyszerűsíteni: a meglévő SOC átépítése nélkül

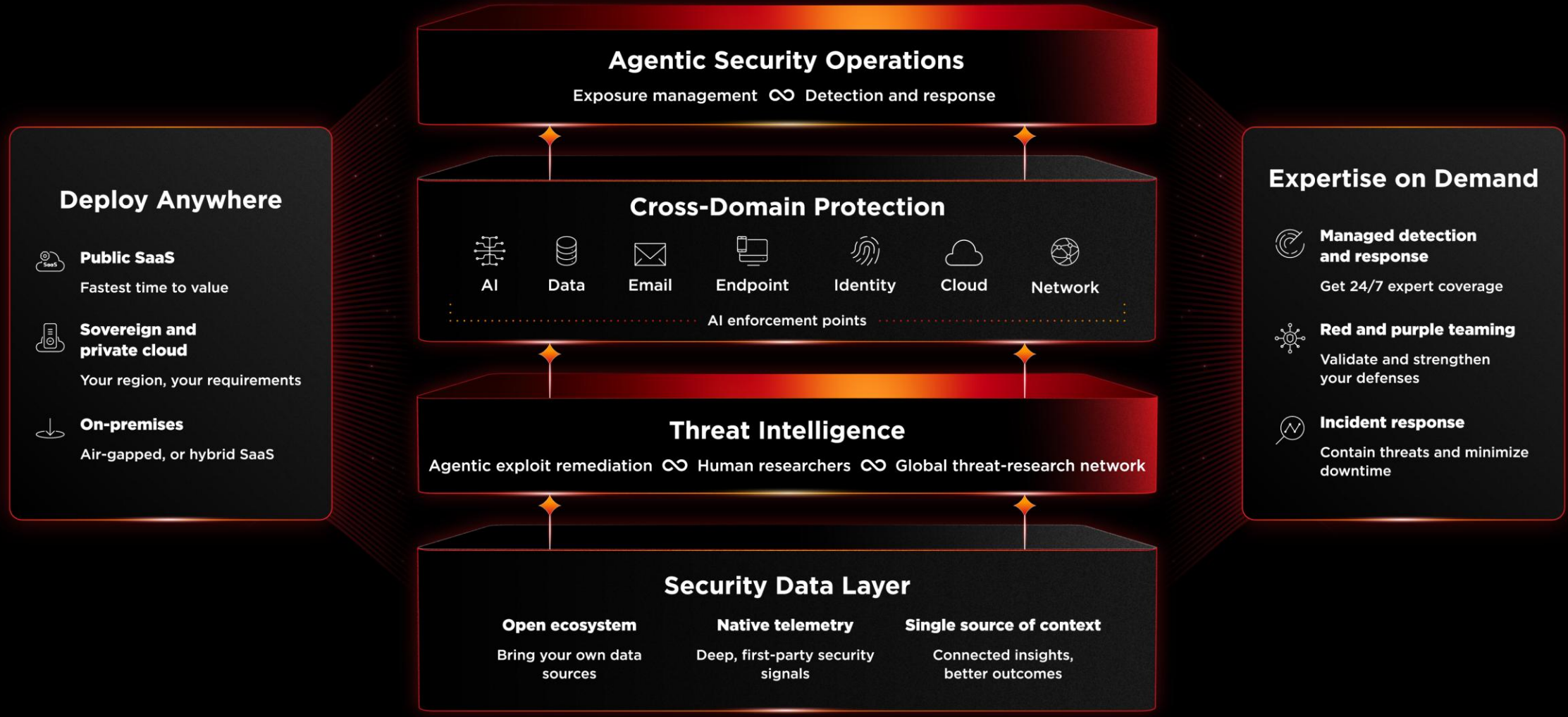
Egy átlagos SOC-ban több mint 40 eszköz fut. Forrás: SAPIO Research a Trend Micro megbízásából, 2021

TrendAI™

TrendAI™
Vision One

One AI-native platform. Agentic operations. Enterprise-wide protection.

Secure, govern, and protect your people, infrastructure, data, and AI.



Agy: AI for Security és Security for AI



AI for Security

Az AI a SOC eszköze

Agentic SIEM és SOAR: korrelál, triázsol, vizsgál, reagál

AESIR: ügynöki sebezhetőség-felderítés és javítás

Claude-modellek a platformban; szuverén környezetben nyílt modellek



Security for AI

Az AI maga is védendő

AI Scanner és AI Guard: a modell és a prompt védelme

Agentic Governance Gateway: kontroll az ügynökök felett

AI-SPM: az AI-eszközök leltára és hibás beállításai

A következő három dia mindkét oldalt kibontja.

TrendAI™

AI for Security: így dolgozik az Agentic SIEM

Az elemző szerepeket és felügyeleti szintet állít, jóváhagy, felülbírál. Minden lépés naplózott.



Adat

Natív szenzorok és külső források egy adatrétegben



Korreláció

A sémát nyelvként kezeli: LLM köti össze a jeleket



Triázs

Priorizált jegy, kevesebb zaj



Vizsgálat

A leletek alapján útvonalat vált, nem checklistát követ



Válasz

Végpont izolálása, fiók felfüggesztése API-n át

900+ támogatott adatforrás

6 natív szenzor: végpont, felhő, e-mail, hálózat, szerver, identitás

7 év archív megőrzés, kereshetően

Számok: gyártói közlés (Trend Micro)

TrendAI™

Security for AI: védelem rétegenként

Felhasználók	**AI Secure Access**	Hozzáférési szabályok külső AI-szolgáltatásokhoz felhasználó, eszköz és hely szerint
Prompt és válasz	**AI Guard**	Futásidejű szűrés: prompt injection, adatszivárgás, káros kimenet
Modell	**AI Scanner**	Ismert támadási technikák tesztje, még élesítés előtt
Ügynökök és eszközök	**Agentic Governance Gateway**	Láthatóság és policy az ügynöki műveletek felett
Infrastruktúra és adat	**AI-SPM és DSPM**	Hibás konfiguráció, hiányzó védőkorlát, kitett érzékeny adat

AI Security Blueprint: egy nézet az összes AI-eszközről és a köztük lévő résekről

TrendAI™

Az ügynököket nem elég védeni: irányítani kell



Élesítés előtt szimulálható, élesítés után visszagörgethető szabályváltozások

TrendAI™

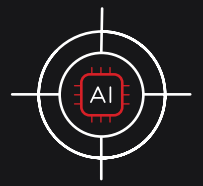
Immunrendszer: a proaktív SOC



01

Mérni

Cyber Risk Exposure Management: a kitettség üzleti hatásként.



02

Szimulálni

Digitális iker: támadási útvonalak próbája élesítés nélkül.



03

Megtalálni

AESIR: a hiba felderítése, mielőtt a támadó találná meg.



04

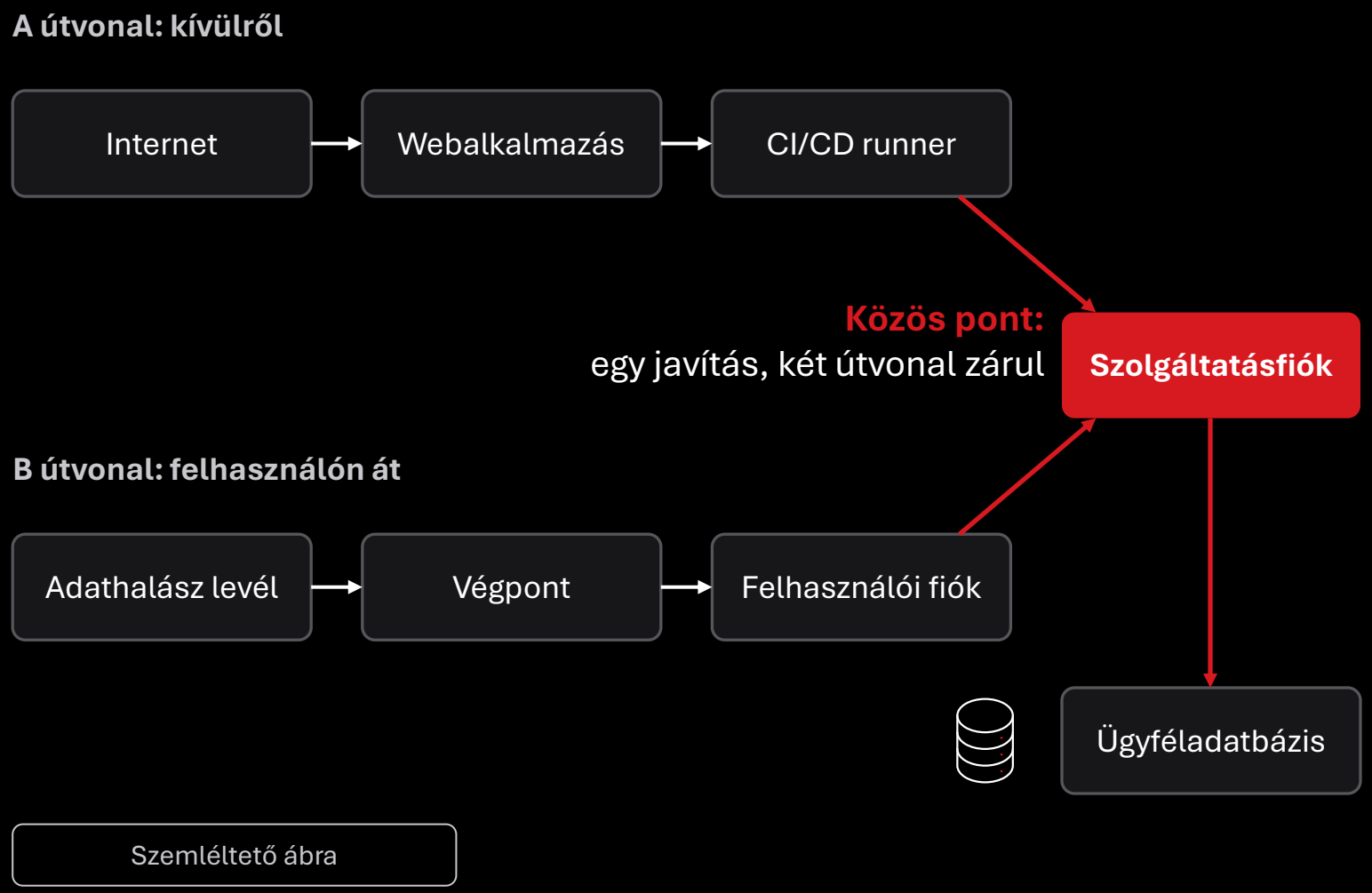
Pajzsolni

Virtual patching: védelem, amíg a javítás megérkezik.

A védekezés a támadás előtt kezdődik.

TrendAI™

Predikció: támadási útvonalak a digitális ikerben



Mit csinál az iker?

Folyamatosan frissülő virtuális másolat az infrastruktúráról

AI-ügynökök támadói taktikákat modelleznek benne

Megmutatja egy új eszköz, szabály vagy architektúra hatását élesítés előtt

IT és OT, helyben és felhőben

TrendAI™

Megelőzés gépi sebességgel: AESIR

Felderítés	Igazolás	Enyhítés	Ellenőrzés
Gyenge pontok keresése a forráskódban, szakértő által hangolt vizsgálattal	Minden találat működő proof of concepttel bizonyított	Detekciós szabály és virtuális patch, a hivatalos javítás előtt	Patch után újravizsgálat, a ZDI kutatásával összevetve

97%

első hely a CyberGym benchmarkon
UC Berkeley · gyártói közlés

1 507 megerősített sebezhetőség 188 nyílt forrású projektből

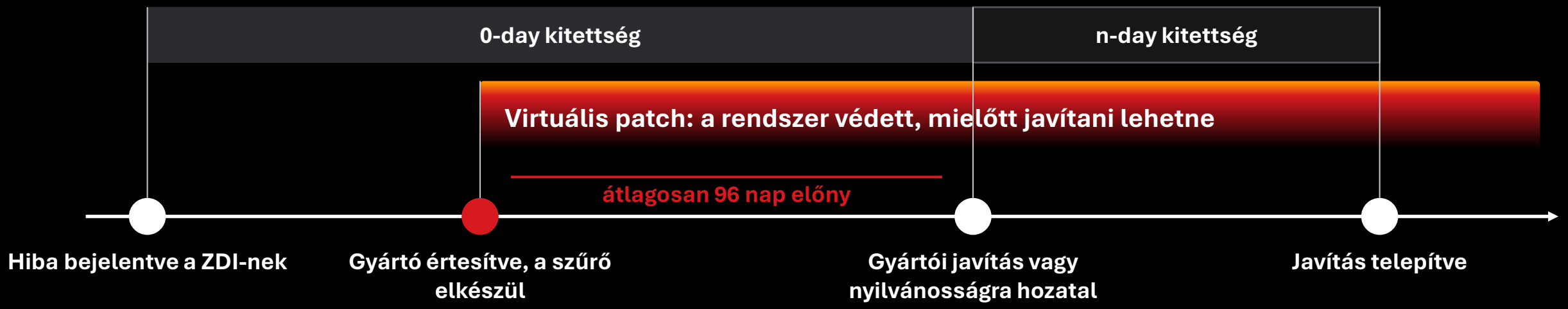
Hét AI-modell több szolgáltatótól, köztük saját üzemeltetésű nyílt modell

Mögötte a Zero Day Initiative több mint 20 év kutatása

Autonomous Vulnerability Discovery: private preview

TrendAI™

Pajzs: virtual patching, védelem a javítás előtt



ÍGY MŰKÖDIK A VEZETÉKEN



Nem helyettesíti a javítást: időt ad rá.

TrendAI

Esettanulmány: PHP2Shell, 2026. október

CVE-2026-109618
Memóriasérülés a memóriahiány kezelése közben

CVE-2026-109619
Use-after-free: kérések között megmaradó állapot

CVSS 4.0: 9,2
Távoli kódfuttatás hitelesítés nélkül

Javítva
PHP 8.2.35, 8.3.36, 8.4.27, 8.5.12

PHP 7.3 és régebbi
Nincs javítás, és nem is lesz

okt. 17.	Első kihasználási kísérlet egy honeypoton, négy nappal a javítás előtt
okt. 20.	A hibák részletei kiszivárognak
okt. 21.	Megjelenik a javítás, és még aznap a nyilvános exploit
okt. 22.	TrendAI kitettség-ellenőrző eszköz és védelmi szabályok
okt. 26.	Mindkét CVE felkerül a CISA KEV-listájára

Ugyanazon a héten: Brotli
CVE-2026-111497: külön hiba a Brotli-dekóderben, szintén CVSS 9,2. Számos futtatókörnyezetbe be van építve, a PHP brotli-bővítményébe is.
Mindkét hiba felderítésében AI-modellek is részt vettek.

Kill chain: hol áll meg a PHP2Shell?

A támadás lépései	Hitelesítetlen kérés a szerverre	OOM-hiba a PHP magjában	Shell a PHP workerből	Webshell a szerveren	Jelszavak, továbblépés
ATT&CK taktika	Initial Access	Execution	Execution	Persistence	Credential Access
Megelőzés virtuális patch	TippingPoint Digital Vaccine szűrők	IPS-szabály 1012754 a szerveren	nem jut el idáig	nem jut el idáig	nem jut el idáig
Észlelés ha mégis átjut		NDR-szabály 6021 és 6023	Workbench: PHP worker shellt indít	Workbench: webshell-aktivitás, Integrity Monitoring	Workbench: hitelesítő fájl elérése

a kihasználási kísérlet a vezetéken vagy a hoszton megáll

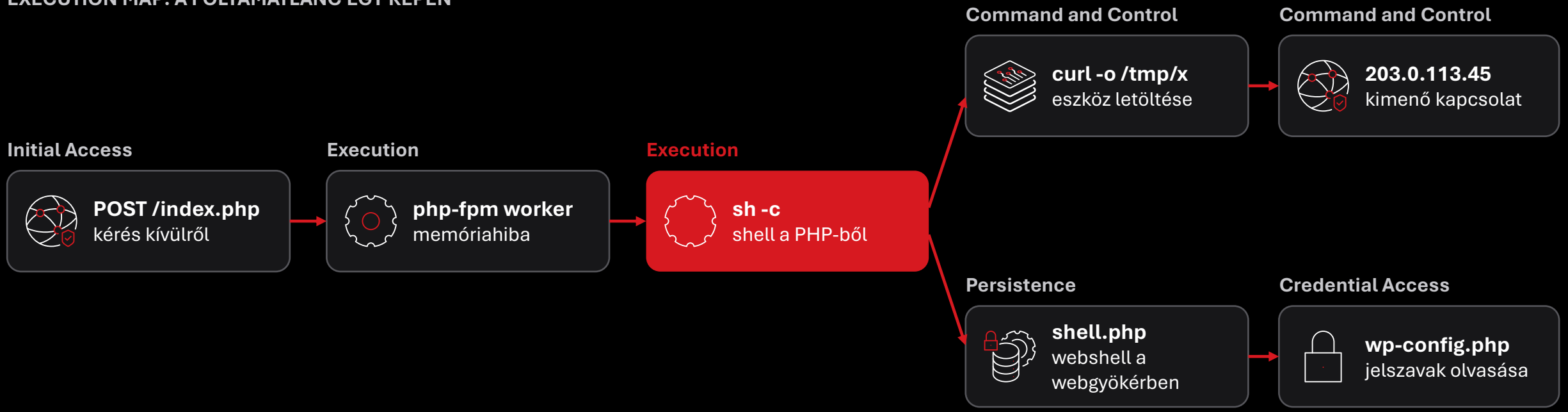
egy platform: hálózat, hoszt és konténer jelei együtt

Találd meg. Pajzsold. Kapd el, ami átcsúszik.

TrendAI™

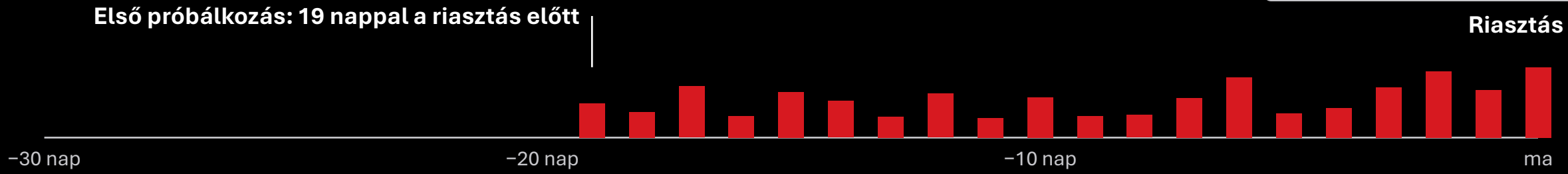
Megértés: mi indított mit, és mióta van bent?

EXECUTION MAP: A FOLYAMATLÁNC EGY KÉPEN



VISSZAMENŐLEGES FORGALOMVIZSGÁLAT, 30 NAP

Szemléltető ábra



TrendAI

Pulzus: új generációs KPI-ok

MTTD

Mean Time to Detect

Mennyi idő alatt vesszük észre?

MTTP

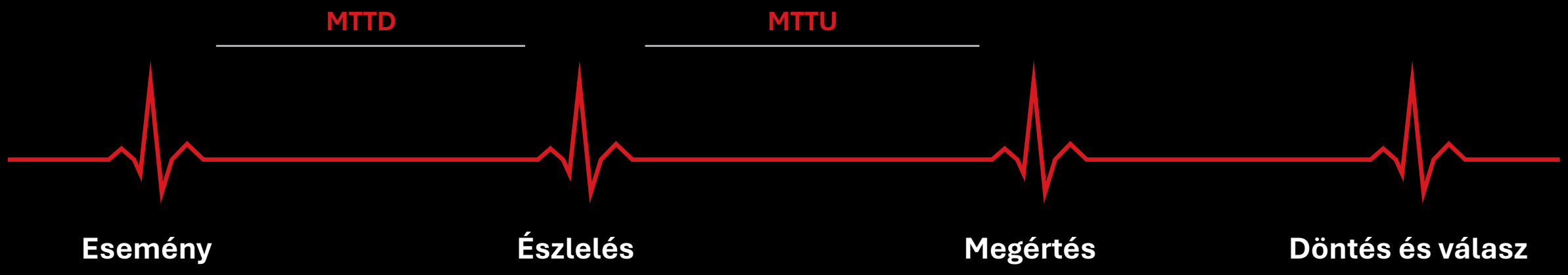
Mean Time to Patch

Mennyi idő alatt zárjuk be a rést?

MTTU

Mean Time to Understand

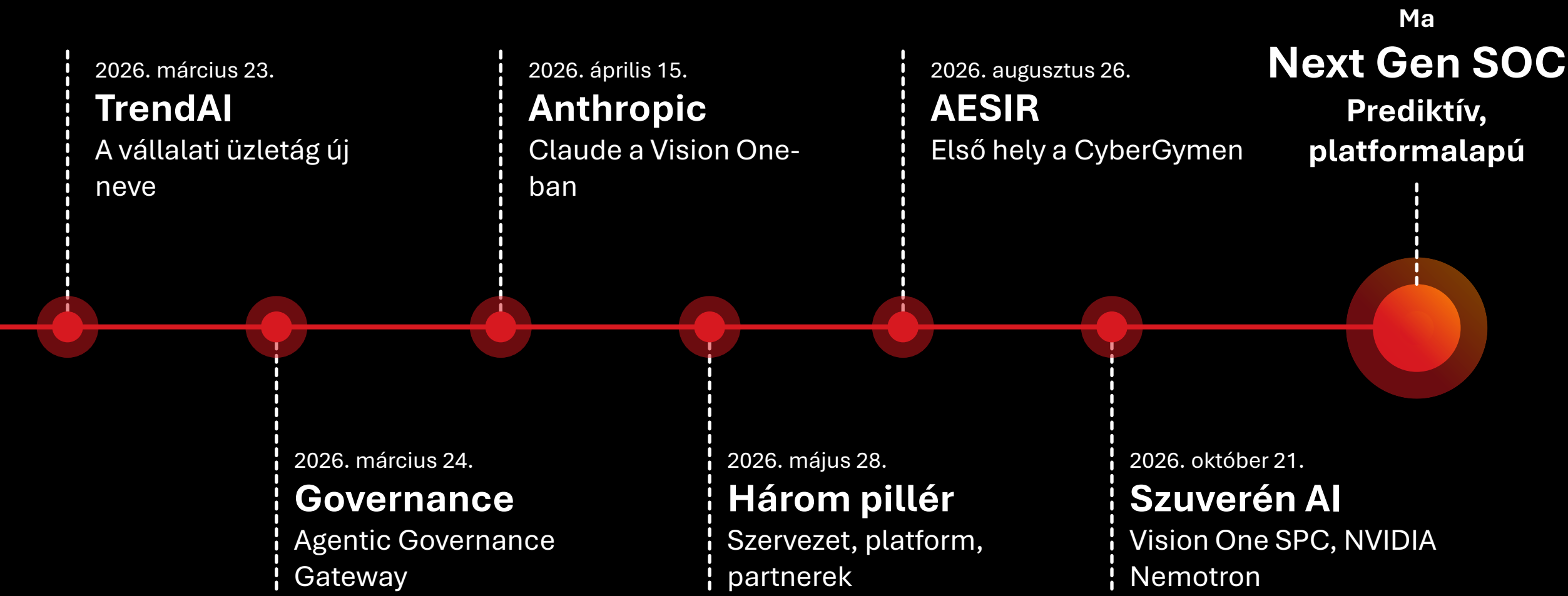
Mennyi idő alatt értjük meg, mit jelent?



A szűk keresztmetszet ma ritkán az észlelés. Sokkal gyakrabban a megértés.

TrendAI™

TrendAI 2026: egy év, egy irány



TrendAI

Recept hétfőre

Rp.

Páciens: az Ön SOC-ja
Adagolás: heti egy lépés



Mérjük a megértési időt
Az észleléstől az üzleti hatás megértéséig.



Számoljuk meg a konzolokat
Hány eszköz kell egy incidens végigviteléhez?



Vegyük leltárba az AI-t
Milyen modellek és ügynökök futnak, és ki látja őket?



Keressük meg a javíthatatlant
Hol fut PHP vagy más, amit nem tudunk azonnal frissíteni?

A cél nem a támadás túlélése.

Hanem a kontrollja.

TrendAI™

Patch Tuesday, exploit Wednesday? Bárcsak.

Szombat	Vasárnap	Hétfő	Kedd	Szerda
okt. 17.	okt. 18.	okt. 19.	okt. 20.	okt. 21.
AHOGY A MONDÁS TARTJA				
			Patch	Exploit
AHOGY A PHP2SHELLNÉL TÖRTÉNT, 2026 OKTÓBERÉBEN				
Első exploit-kísérlet			A részletek kiszivárognak	Patch, és még aznap nyilvános exploit

az exploit négy nappal megelőzte a javítást

Stamos optimista volt.

A Next Gen SOC ott kezd, ahol a támadó: a javítás előtt.

TrendAI™

TrendAI™

Köszönöm a figyelmet!

Lássuk. Értsük. Javítsuk.

Lehetőleg még szombat előtt.

