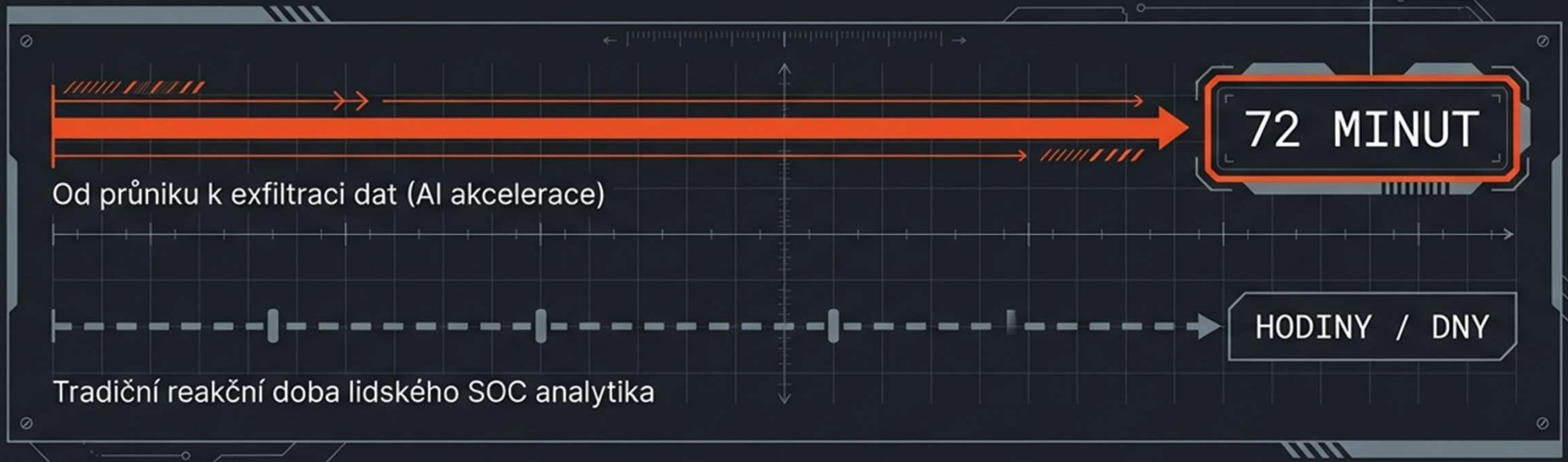
Od viditelnosti k automatizované obraně: Zero Trust architektura pro IoT/ICS

Progresivní transformace průmyslové bezpečnosti v éře konvergence.

Lukáš Březina
CTO, Taktik a.s.

Rychlost útoků v roce 2026: Ztrácíme luxus času.

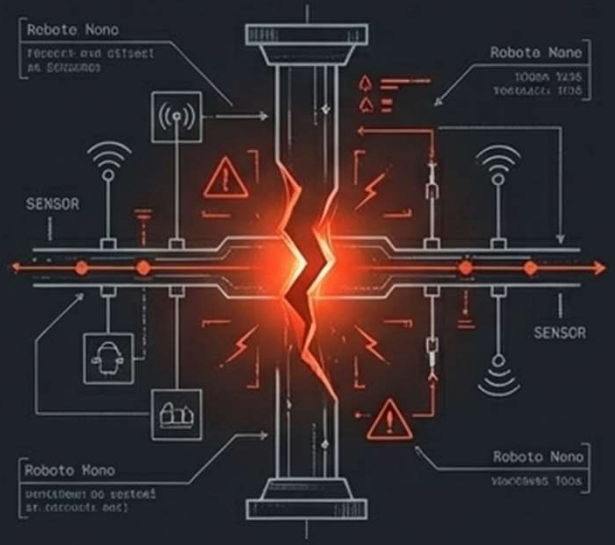
90 % dnešních průniků zneužívá identity a neřízená zařízení.



Útočníci plně automatizují.
Lidský analytik nedokáže reagovat včas.

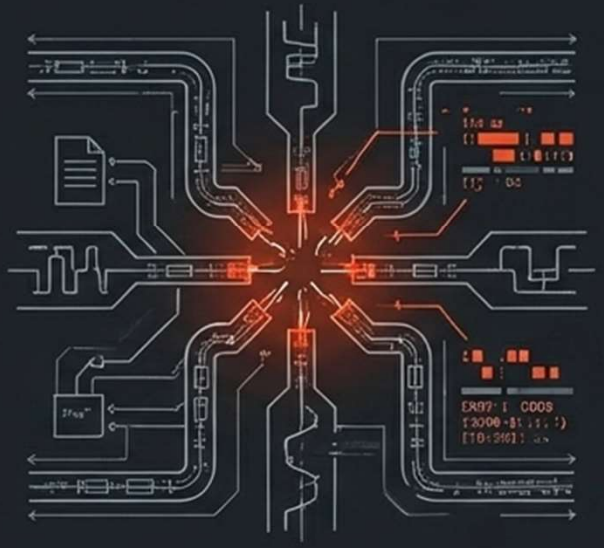
Tři fatální mýty, které ohrožují kritickou infrastrukturu.

Mýtus viditelnosti



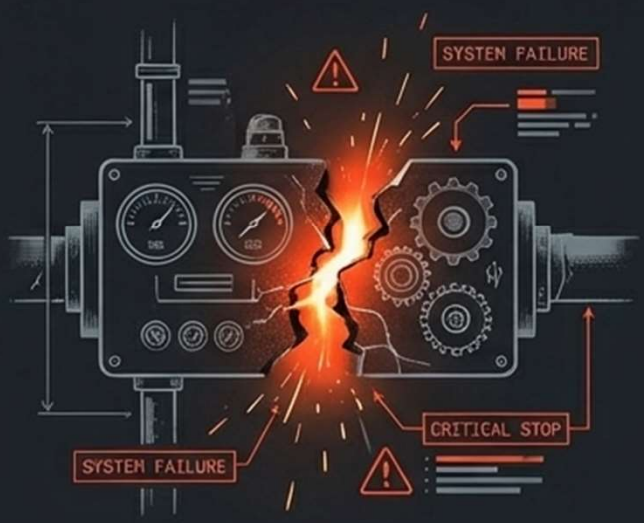
Pouhý monitoring a detekce anomálií stačí k obraně.

Mýtus komplexity



Segmentace vyžaduje složité NAC a nepřehledné overlay sítě.

Mýtus nedotknutelnosti



Zastaralé výrobní systémy nelze chránit bez odstávek a restartů.

Mýtus #1: Pouhá viditelnost a detekce anomálií stačí.

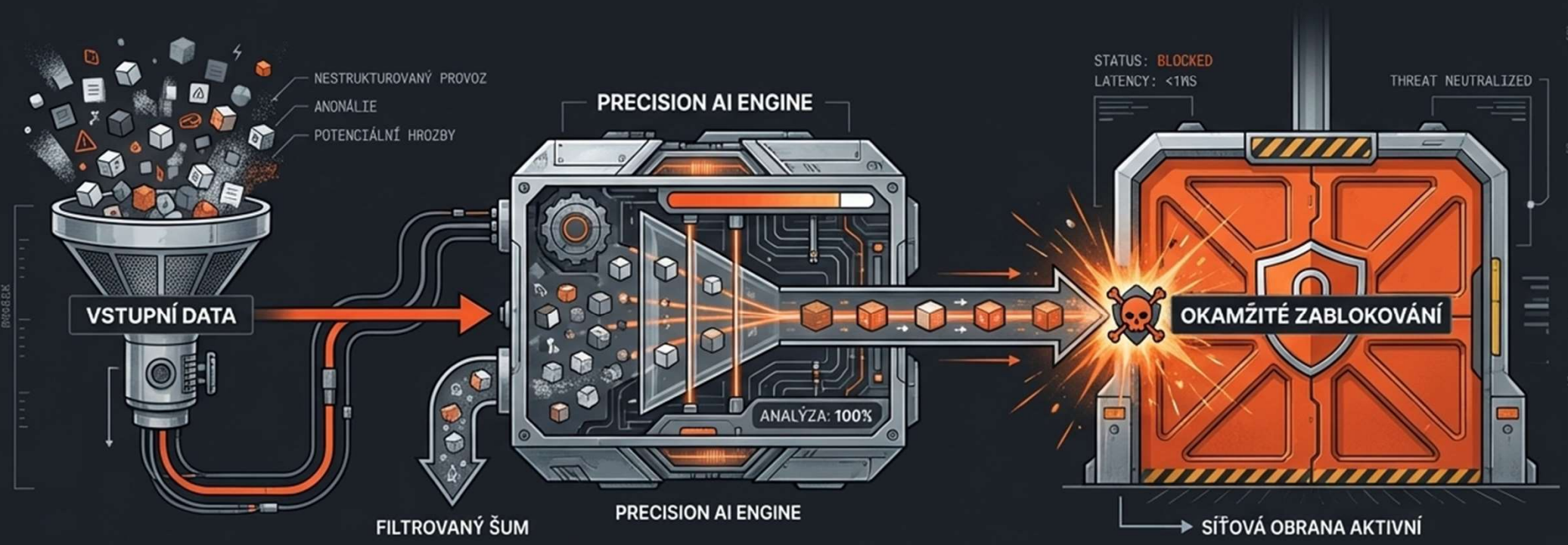
Competitor software

The Visibility-Enforcement Gap

Pasivní sledování provozu dělá z vaší organizace pouze “velmi dobře informovanou oběť”.

Generování tisíců alertů o anomáliích pro SOC analytiky neřeší probíhající útok, který dosáhne cíle za pár minut.

Realita: Strojová rychlost vyžaduje automatizovanou obranu.



PRECISION AI

Eliminace analytického šumu a identifikace reálných hrozeb.

AGENTIC AI

Autonomní systémy, které vyhodnocují komplexní alerty v reálném čase.

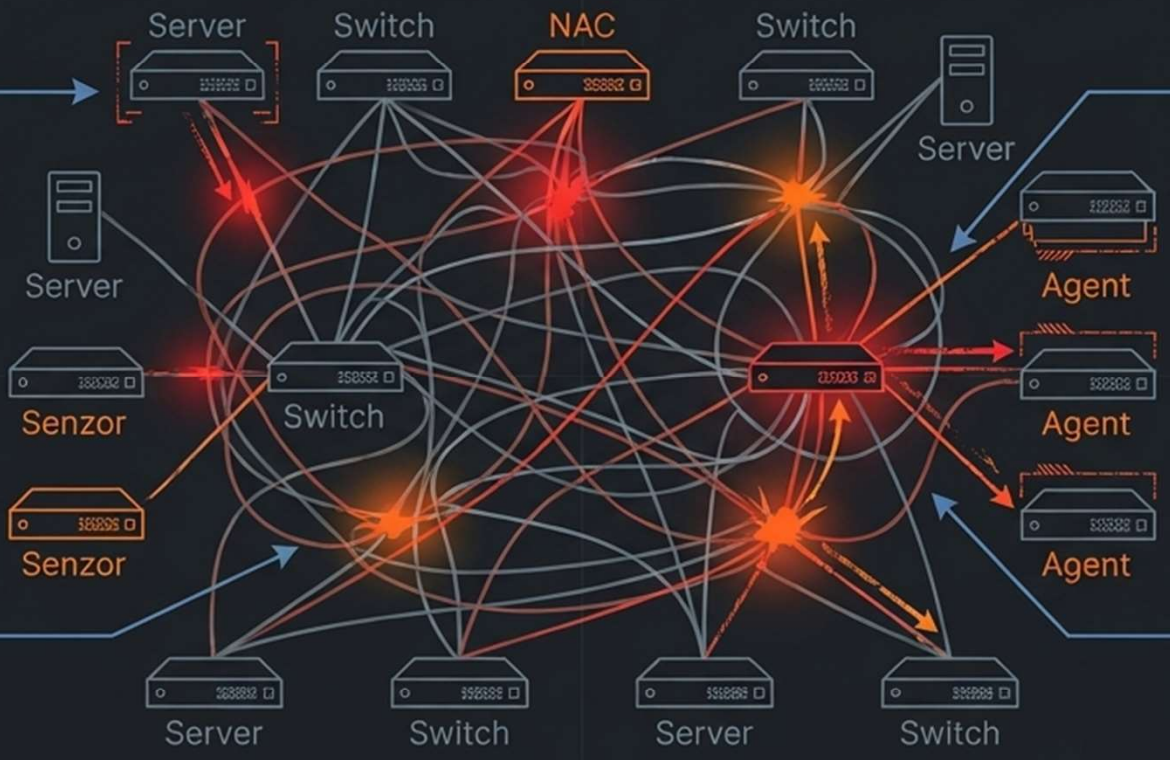
UZAVŘENÝ CYKLUS

Nativní blokování hrozeb na úrovni sítě bez čekání na lidské schválení.

Mýtus #2: Segmentace vyžaduje složité NAC a nové senzory.

Samostatné NAC servery

Dedikované SPAN senzory

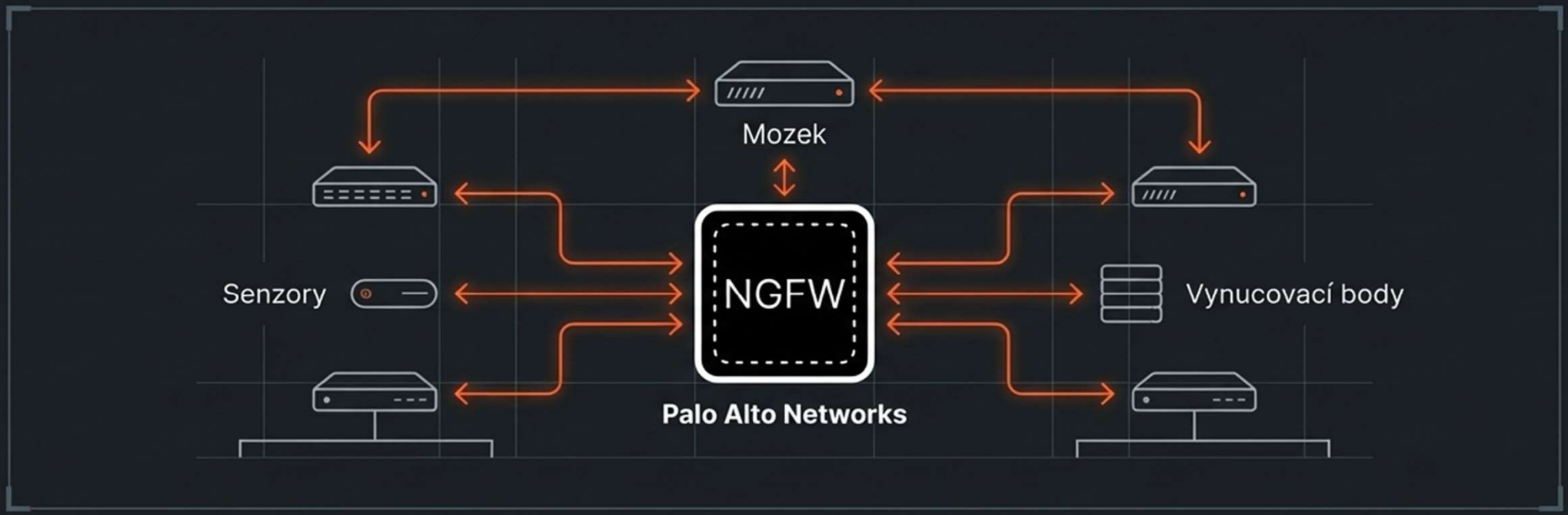


Těžkopádní softwaroví agenti

Složité overlay sítě

Zvyšování komplexity v OT prostředí rapidně zvyšuje provozní riziko, náklady a pravděpodobnost lidské chyby.

Realita: Nativní Zero Trust pomocí stávajících firewallů.

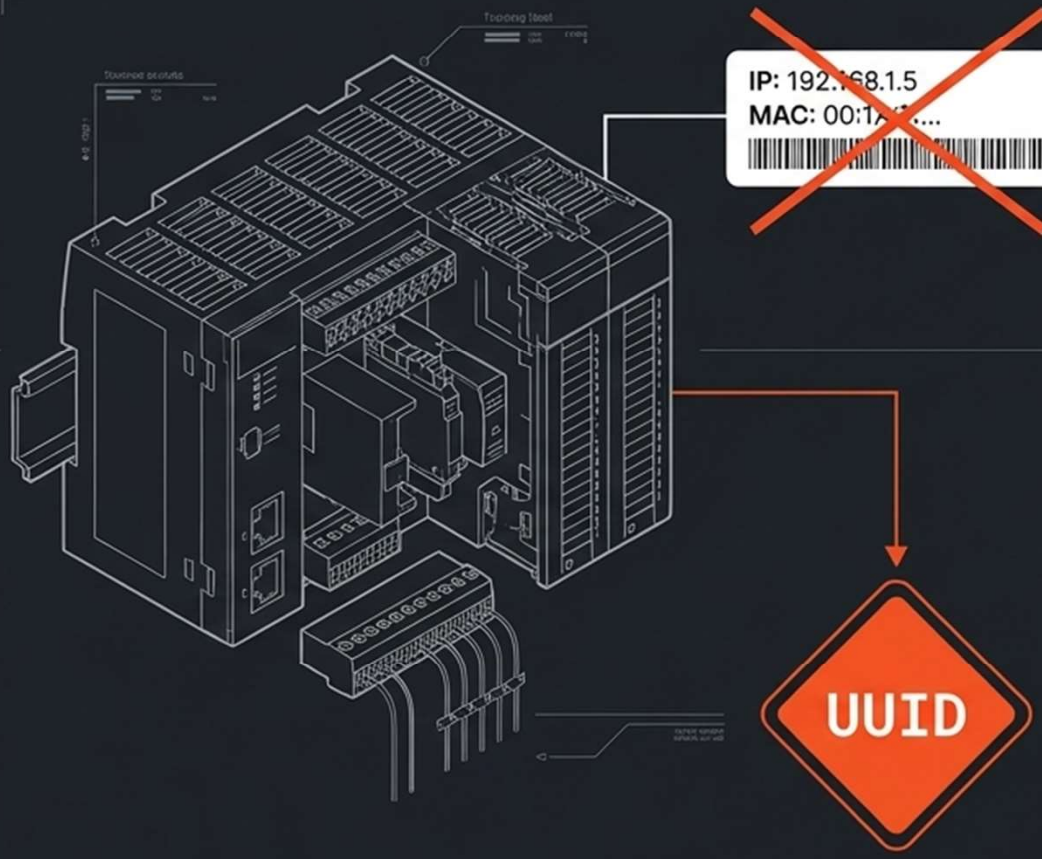


Nulový nový hardware:
Využití existujících NGFW jako inteligentních senzorů.

Bez narušení sítě:
Single-pass architektura pro IT i OT.

Nativní mikrosegmentace:
Prosazování politik přímo na perimetru i uvnitř sítě bez dalších vrstev.

Identita je nový perimetr: Advanced Device-ID.



MOŽNOSTI ADVANCED DEVICE-ID

1 PAN-OS 12.1

Zavedení konceptu jedinečného UUID pro každé aktivum.

2 Hloubkové profilování

Využití více než 2 000 atributů (výrobce, OS, verze firmwaru, běžící aplikace, komunikační vzorce).

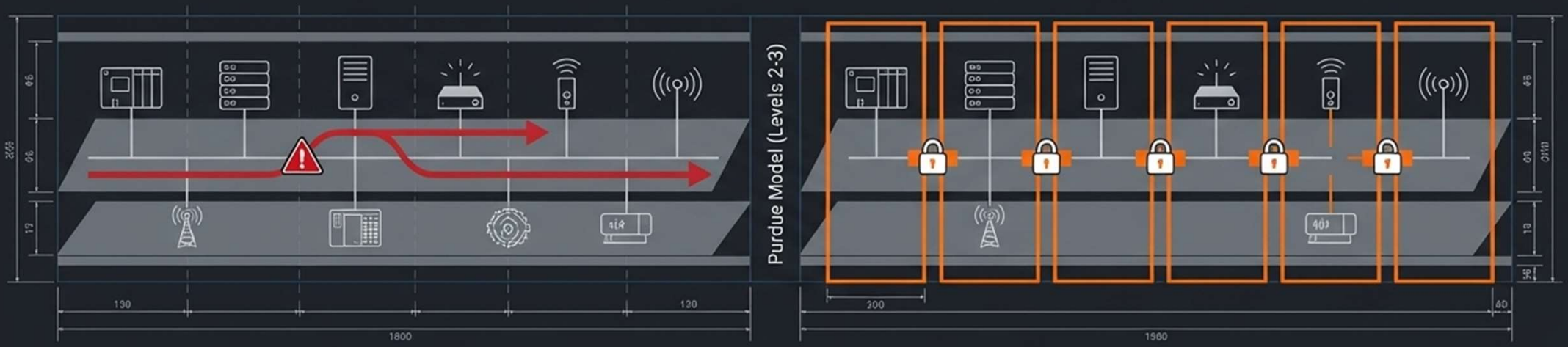
3 Dynamický kontext

Identita putuje se zařízením napříč celou sítí.

Zásady nejmenšího privilegia bez manuální dřiny.

PŘEDTÍM

POTOM

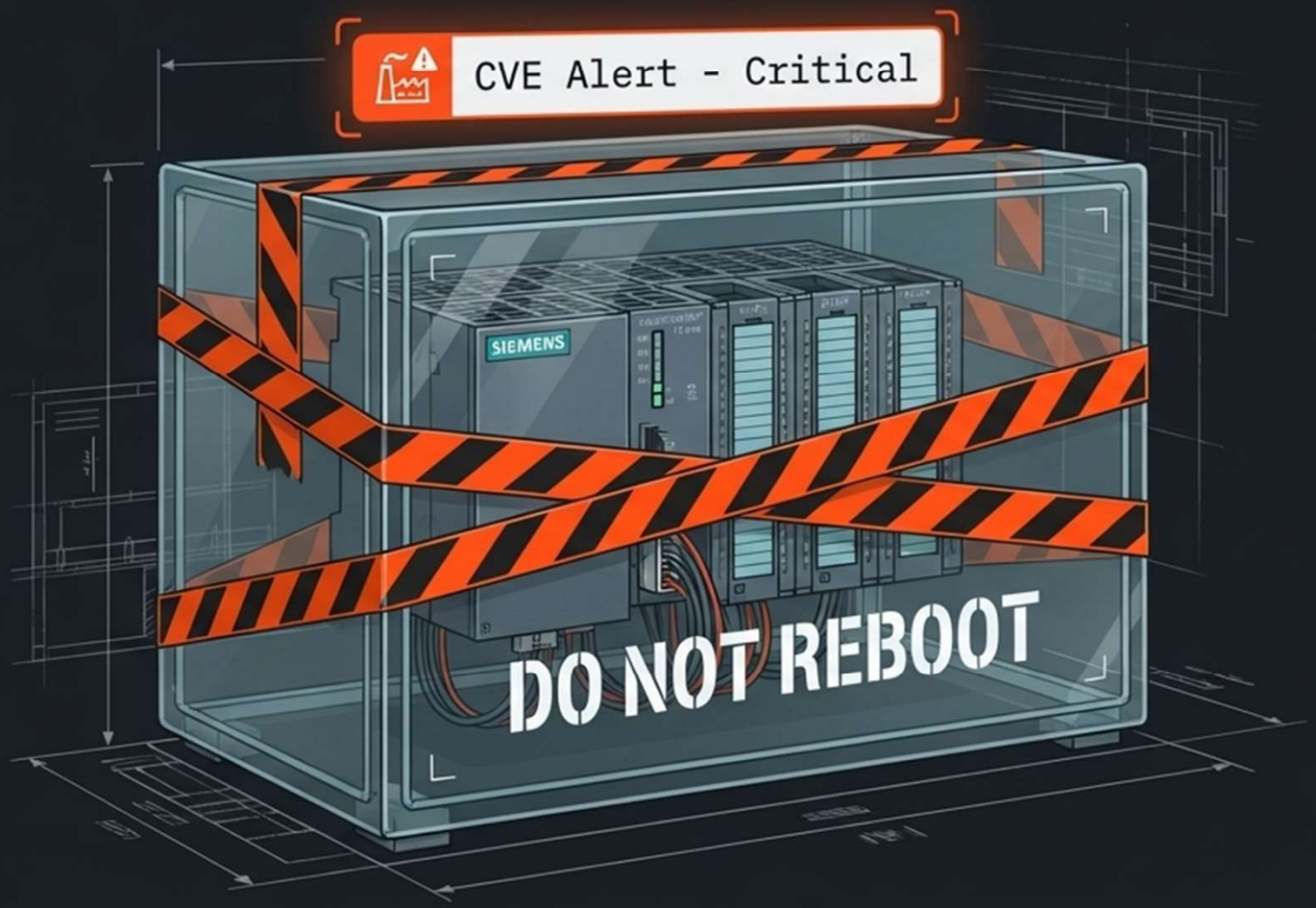


1. Sledování baseline (normálního chování) pomocí ML.

2. Automatické generování doporučení politik (Policy Rule Recommendations).

3. Blokování laterálního pohybu a vynucení **Least-Privilege**.

Mýtus #3: Výroba se nesmí zastavit, legacy systémy nelze chránit



Největší dilema OT bezpečnosti: Zastaralé, nezáplatovatelné systémy.

- Nelze instalovat agenty.
- Odstávka kvůli aktualizaci stojí miliony.
- Výsledek: Systém zůstává inherentně a trvale zranitelný.

Realita:

Guided Virtual Patching (Virtuální záplatování)

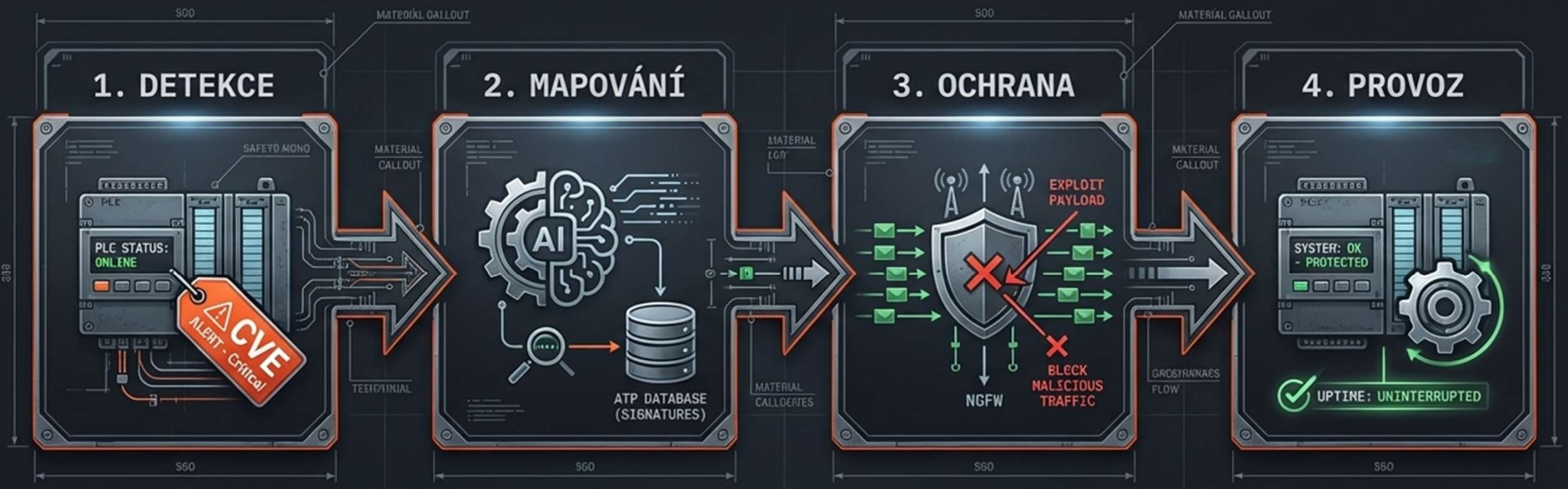
- Metoda ochrany starých a nezáplatovatelných ICS/OT systémů přímo na síťové úrovni.
- Využívá existující Threat signatury k blokování známých zranitelností (CVE).
- Nevyžaduje zásah do koncových zařízeni ani restarty.

Žádná odstávka výroby: Implementace nevyžaduje přerušení kritických procesů, zajišťuje nepřetržitý provoz.

Žádné restarty zařízení: Koncová zařízení (např. staré PLC) nemusí být restartována, což eliminuje riziko selhání.

Ochrana zranitelností v reálném čase: Okamžitá blokace hrozeb na síťové vrstvě dříve, než dosáhnou zranitelného systému.

Prevence bez odstávek v praxi: Jak to funguje.



Inter

Device Security odhalí nebezpečné CVE na legacy PLC.

Inter

Systém AI automaticky přiřadí odpovídající signaturu z Advanced Threat Prevention (ATP).

Inter

NGFW začne aktivně blokovat pouze specifický exploit payload přímo v síťovém provozu.

Inter

Ikona PLC ukazuje, že zařízení nadále nerušeně funguje.

Rozšíření Zero Trust na okraj sítě: Bezpečný vzdálený přístup.

Klíčové vlastnosti:

Inter Roboto Mono

- Prisma Access Browser & Privileged Remote Access.
- Izolace relací a nahrávání aktivity (Session recording).
- Just-in-Time přístup (pouze pro schválené okno údržby).

Proč platformní přístup vítězí: Srovnání trhu CPS 2026.

	Palo Alto Networks	Vendor “A”	Vendor “B”
Vynucování obrany (Enforcement)	Nativní, inline přímo na firewallu.	Závislé na API integraci s třetími stranami.	Závislé na integraci s třetími stranami.
Dodatečné senzory	Žádné (využívá stávající firewally).	Vyžaduje fyzické span-port senzory.	Nutné nasadit virtuální sondy.
Uživatelská zkušenost	Unifikovaná platforma (SCM) pro IT i OT.	Oddělené konzole pro různé typy hrozeb.	Fragmentované rozhraní, chybí jednotný přehled.

Konkurence hrozby vidí. My je vidíme a nativně blokujeme.

Od pasivního sledování k aktivní ochraně

Unifikovaná viditelnost
(NGFW jako senzor)

Identita jako základ
(Advanced Device-ID)

Automatizovaná obrana
(Guided Virtual Patching)

Neviditelná hrozba vyžaduje autonomní reakci

Lukáš Březina, CTO, Taktik a.s. | Palo Alto Networks