AI není náhrada odpovědnosti

Je to způsob, jak ji unést

18. 5. 2026

Realita roku 2026

AI není náhrada odpovědnosti, je to tlak na její systemizaci

- NIS2 / ZoKB – osobní odpovědnost
- AI Act – nutnost auditovatelnosti
- Exponenciální růst dat a alertů
- Kapacity týmů stagnují

» Organizace nejsou schopny unést odpovědnost, kterou na ně regulace klade

Co přináší AI do naší práce

- Odpovědnost nelze škálovat lidmi

„Kolik z Vás má pocit, že stíhá všechny regulatorní požadavky?“

- AI zvyšuje Vaši schopnost odpovědnost unést
- AI nám nepomůže zbavit se odpovědnosti, ale donutí nás ji doopravdy začít řídit.

Jak nás to (z)mění

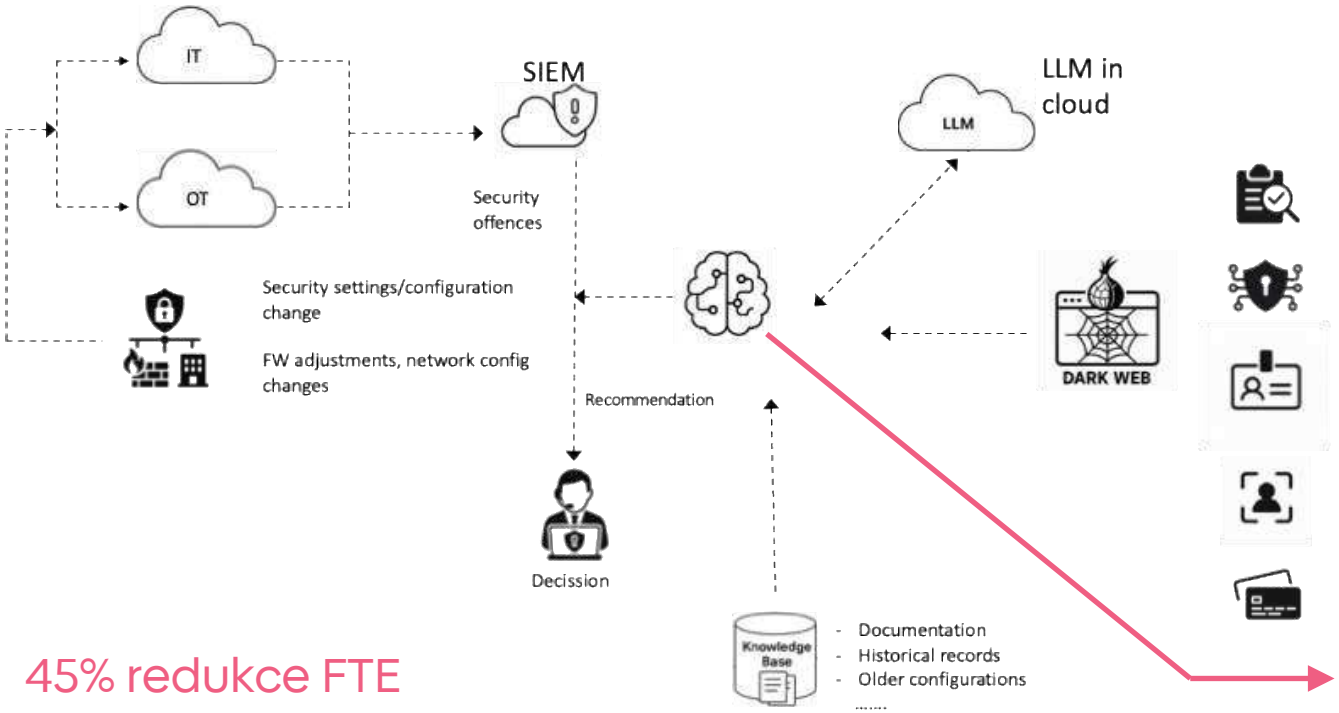
- Atos se mění na Service-as-Software organizaci zaměřené na efektivitu
- Veřejná správa by měla být řízena spíše odpovědností

» Agendy jako digitální služby, řízené pravidly, dat a s podporou AI.“

- AI ve veřejné správě bude o snížení chybovosti, vyšší konzistentnosti a prokazatelnosti rozhodování.

2026: SOC již není služba, je to systém řízený AI

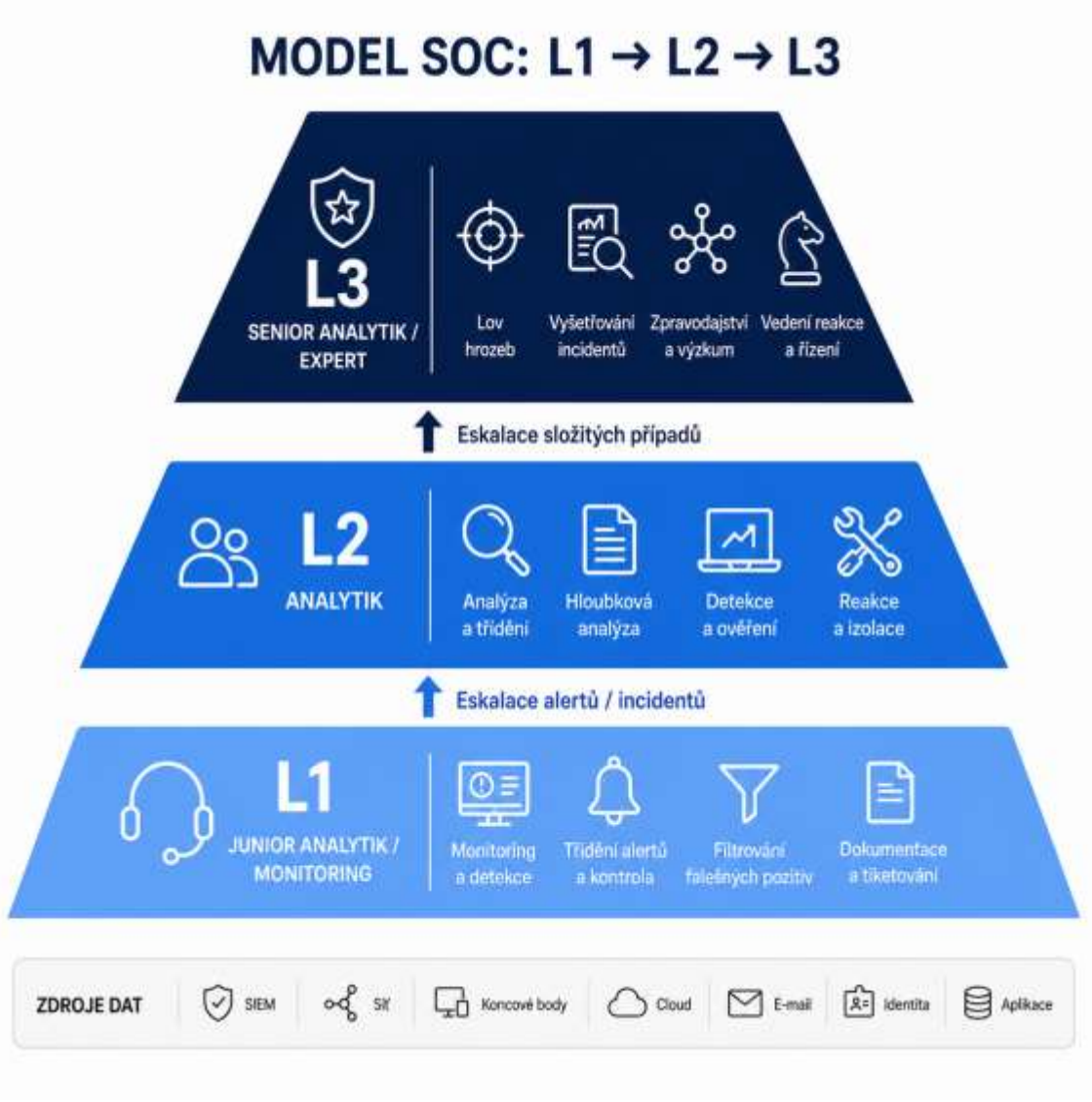
Bezpečnostní monitoring: L1 vrstvu přebírá AI



45% redukce FTE

35% redukce false positives

30% redukce L1 nákladů



Bez AI není ekonomicky možné držet reakční časy, ani kvalitu rozhodnutí

AI v bezpečnostním monitoringu (SOC)

AI nezmenšuje odpovědnost , násobí ji

„SOC se mění ze služby na průběžně se zlepšující systém (service as a software)“

Snížení provozních nákladů o desítky % díky redukci repetitivních činností.

Doposud

- Manuální analýza
- Zpožděná rozhodnutí
- Odpovědnost roste
- Kapacitní limity

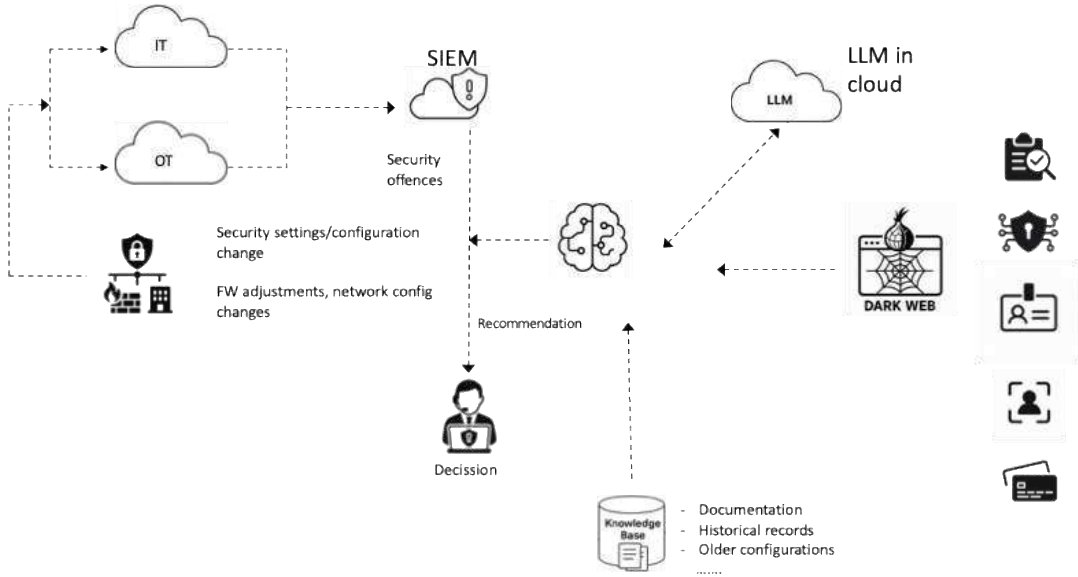
Jak nás to (z)mění

- AI-assisted analytika a rozhodování
- AI nepřebírá odpovědnost, zvyšuje rozhodovací kapacitu
- Automatizace

„Rozdíl není v nástrojích. Je v schopnosti rozhodovat v čase.“

Typický SOC incident (phishing case)

- Bez AI: 3 hodiny, 2 lidé
- S AI: 20 minut, 1 člověk



AI v penetračním testování

Jednorárový pentest již neodpovídá realitě. 80% zranitelností vzniká mezi pentesty.

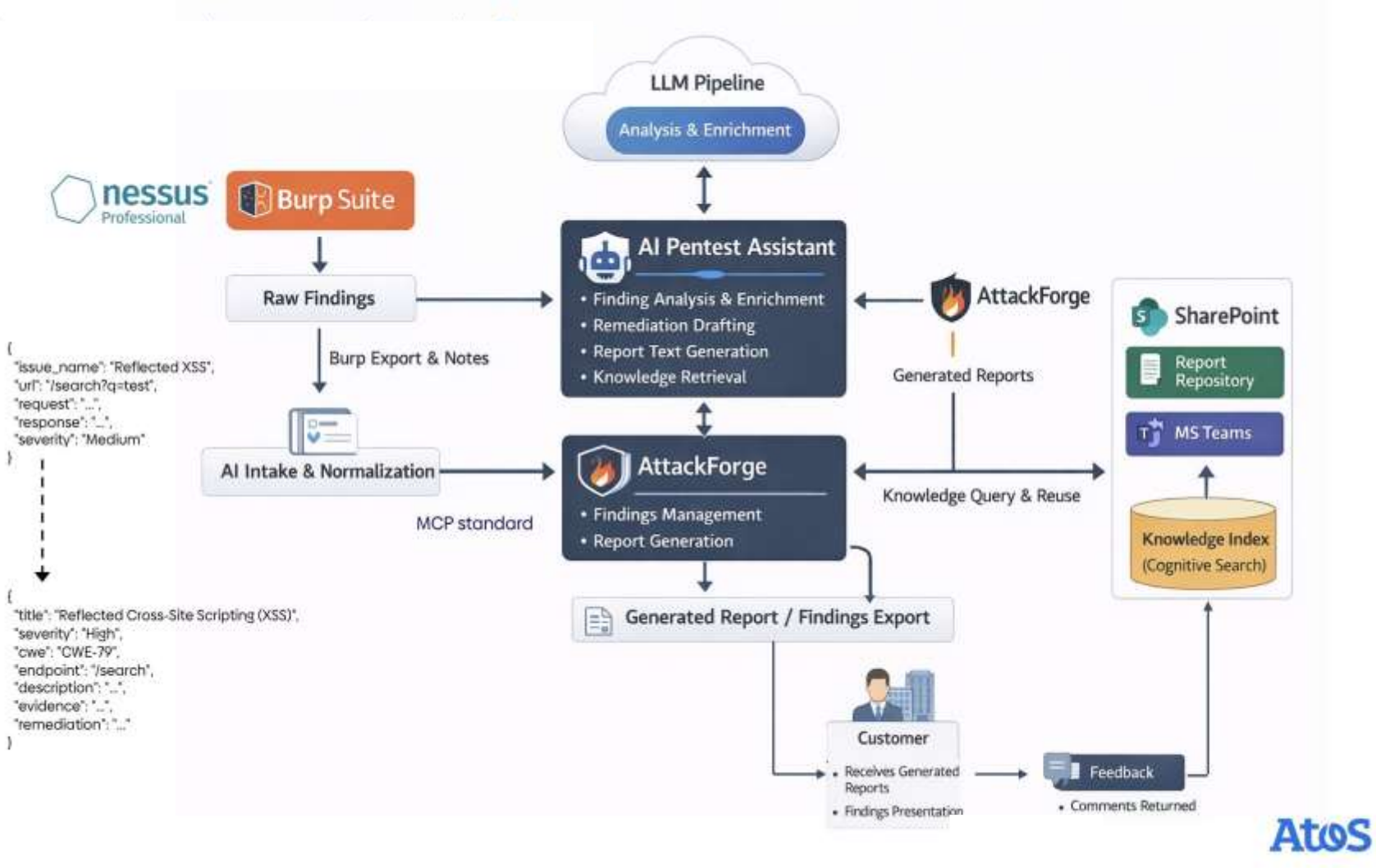
Jednorázový pentest neprokazuje bezpečnost — jen historický stav

Průměrná doba exploit: 2-3 týdny

Pentest 1x ročně = slepota 364 dní

- „Systém otestujete.“
- „Za dva týdny ho někdo změní.“
- „Za měsíc vznikne zranitelnost.“
- „A za půl roku přijde útok.“
- „A vy máte poslední pentest… půl roku starý.“

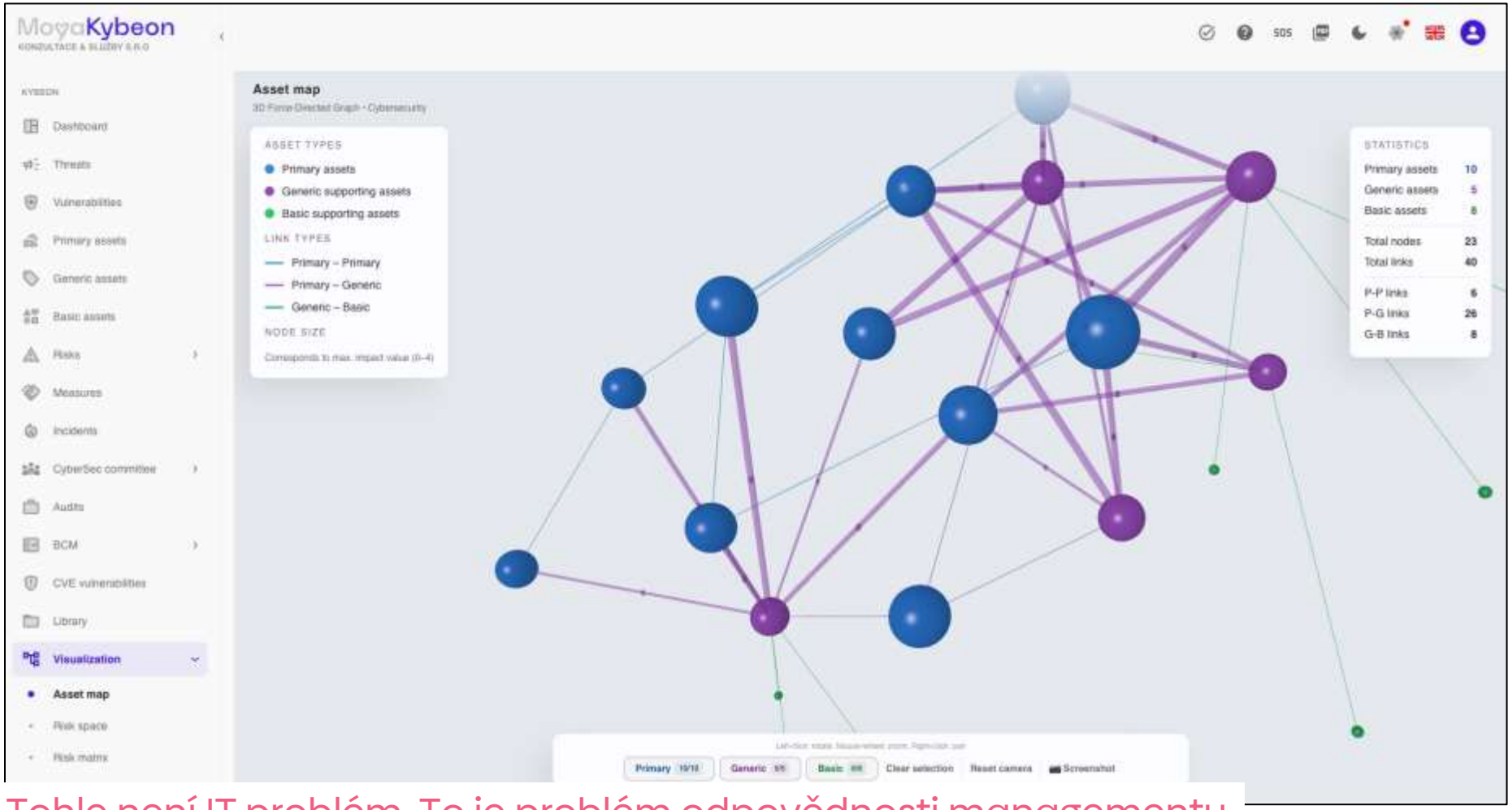
Bez kontinuální validace nelze unést odpovědnost za bezpečnost.



Governance: AI Act mění pravidla hry

Nestačí rozhodovat správně. Musíte být schopni prokázat, jak jste rozhodli.

Bez AI nepůjde zajistit auditovatelnost rozhodnutí v reálném čase



Tohle není IT problém. To je problém odpovědnosti managementu

Změna přístupu: s AI již bezpečnost nelze řídit jako projekt

Odpovědnost se nedá outsourcovat

Doposud

- Projekt
- Audit
- Ruční analýza
- Fragmentované nástroje

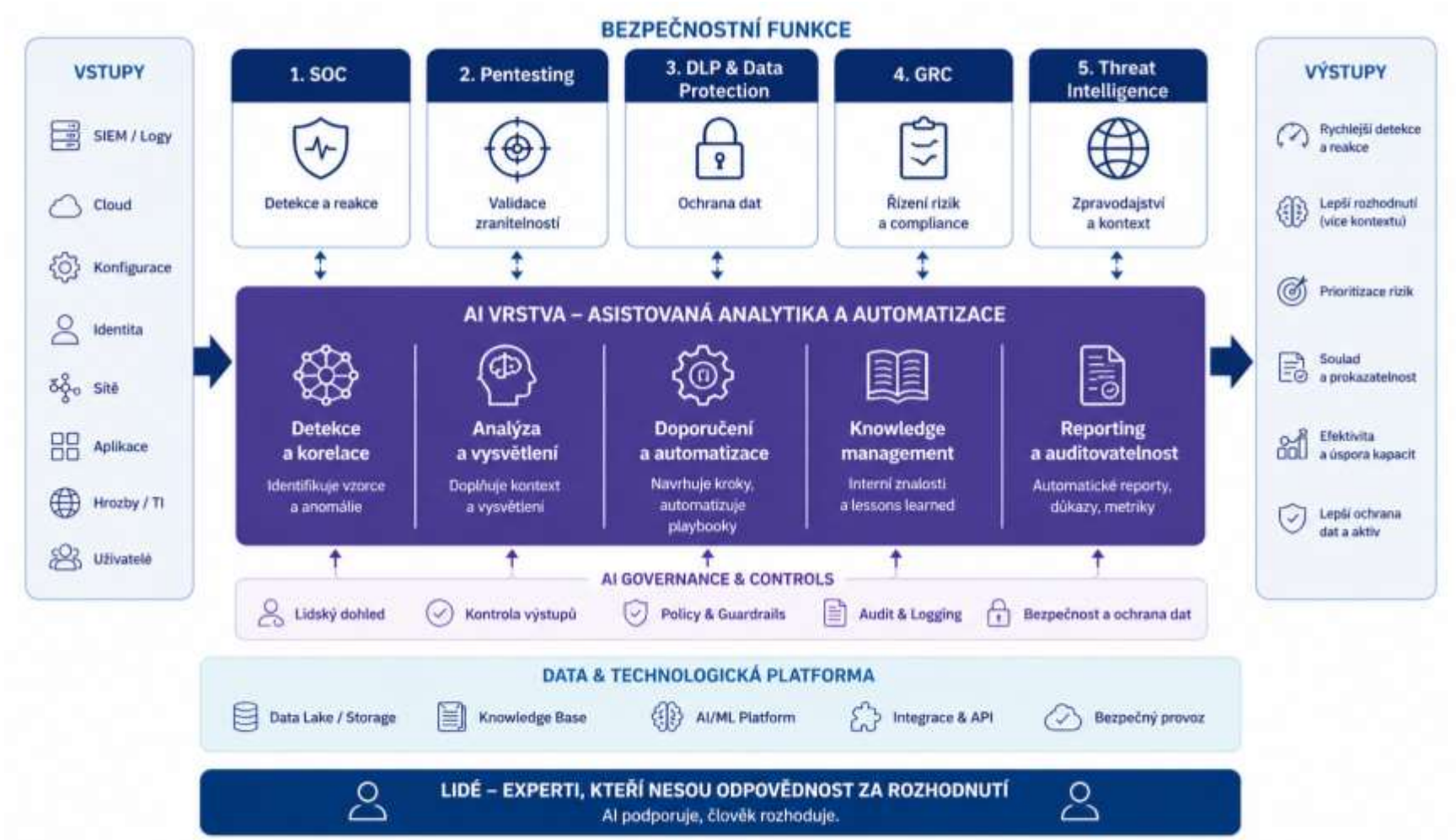
Do budoucna

- Kontinuální systém
- Continuous compliance
- Real-time rozhodování
- AI-assisted operations
- Integrovaný ekosystém

„Pokud bezpečnost nefunguje jako software, tedy kontinuálně, měřitelně a škálovatelně …
…tak s nástupem AI ji již není možné řídit.“

AI v oblasti bezpečnosti

Service as a Software: kontinuální, řízený a auditovatelný systém



Dopady

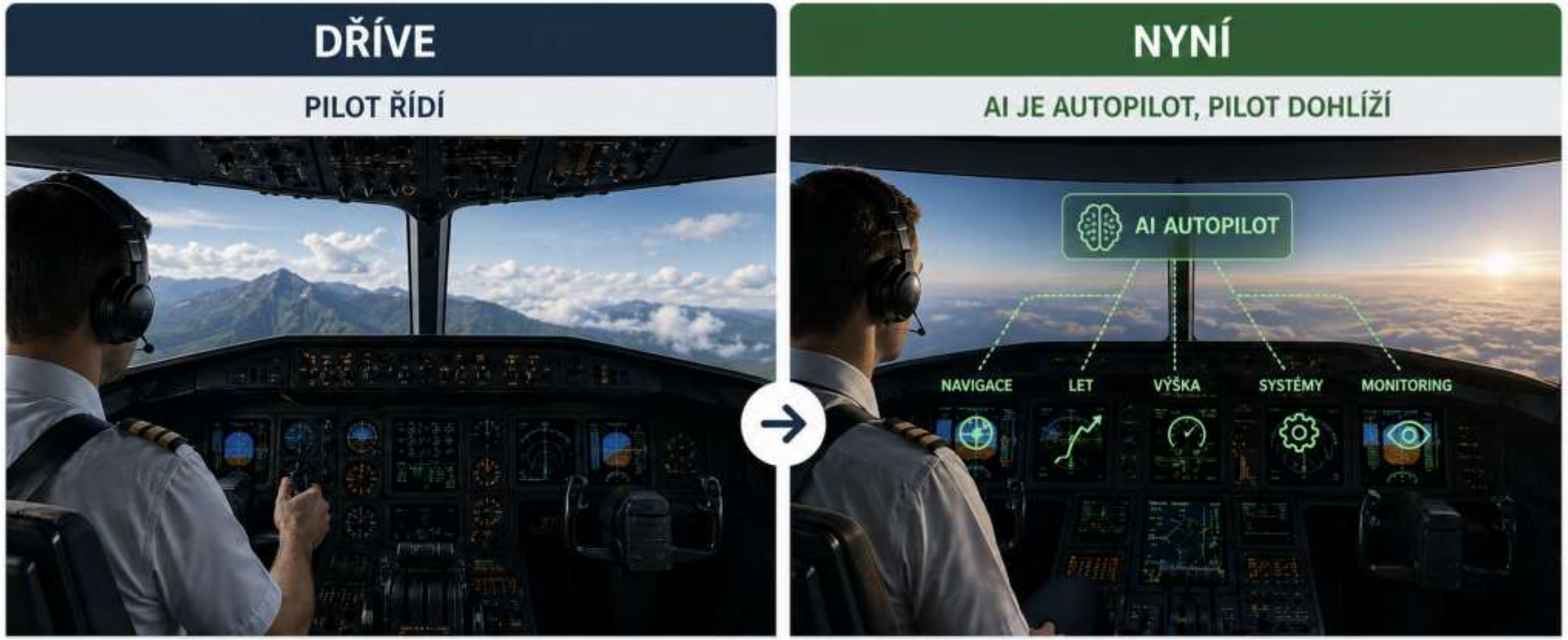
- Prokazatelnost
- Nižší závislost na konkrétních lidech
- Standardizace rozhodování
- Automatizace díky AI

Service as a Software

„Services as a Software Company není use-case, je to nový operační model firmy

- Bez AI nejde o to, že budete pomalejší…….bez AI nebudete schopni být odpovědní**.**
- AI není náhrada experta, **nahrazuje práci, která experta brzdí.**

„Pilot nezmizel. Jen už neřídí každou akci.“



Bez AI nebudete schopni být odpovědní

Tomáš Hlavsa
tomas.hlavsa@atos.net

Atos