ITAPA 2026 | Litauszki Pavol

Nízky rozpočet , vysoké očakávania

Nasadenie AI na L1 mení ekonomiku ZoKB

KDE ORGANIZÁCIE MÍŇAJÚ NEEFEKTÍVNE?

Slepý nákup licencií

Investície do SIEM krabíc bez konfigurácie a reakcie na výstupy

Cesta k ZoKB bez nových nákupov

Väčšina organizácií nevyužíva bezpečnostný potenciál stackov (M365 E3/E5), ktoré už dnes platia.

Zákon o kybernetickej bezpečnosti (ZoKB) sa dá splniť bez masívnych investícií do nových nástrojov.

MÁM OBMEDZENÝ ROZPOČET.
KAM INVESTOVAŤ?

Tri opatrenia s najvyšším ROI (pomer cena/výkon):

01

Nekompromisné MFA

Vynútené bez výnimiek. Odstrihne drvivú väčšinu útokov na identitu.

02

Immutable Zálohy

Zálohy imúnne voči ransomvéru. Definitívna garancia biznis kontinuity.

03

Zdieľané L1 AI + MDR

Externý monitoring a zmluvný Incident Response partner na zavolanie.

VYNÚTENÁ HYGIENA: OPATRENIA ZA 0 €

Efektívne využitie nástrojov dokáže pokryť obrovskú časť požiadaviek.

”Zamykanie staníc a odoberanie lokálnych admin práv nestojí nič. Napriek tomu to v slovenskej praxi chýba.”

Čo zapnúť hneď teraz cez GPO/MDM:

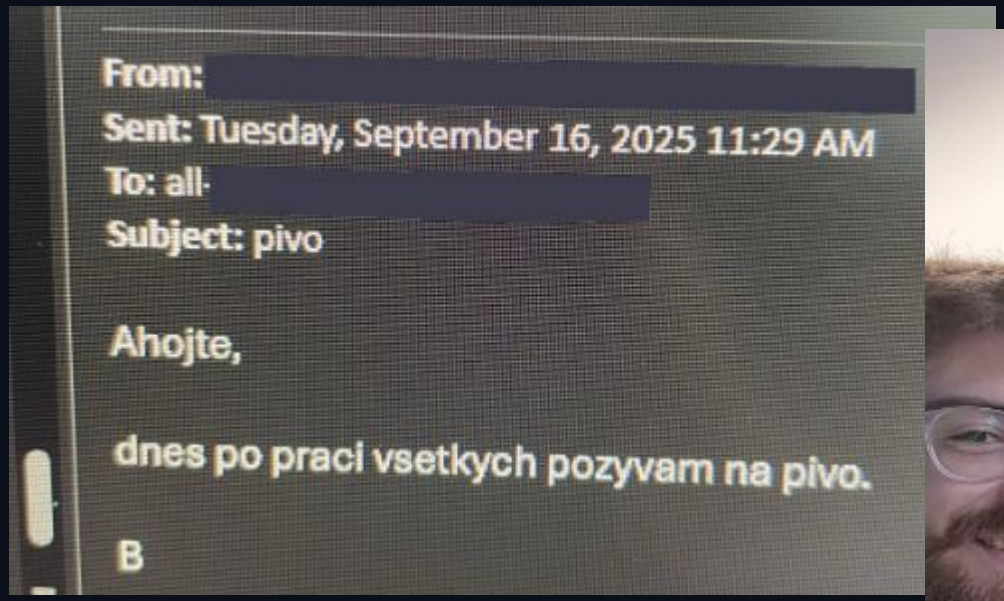
„Ctrl-alt del“ & local admin nestojí nič a v praxi chýba

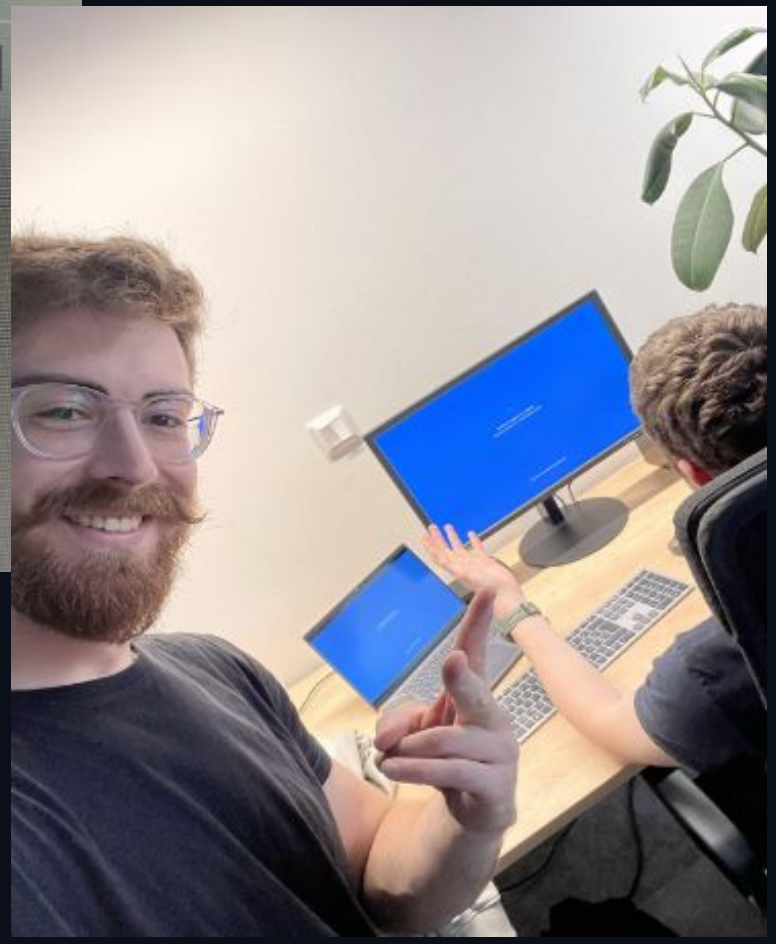
Striktné odoberanie administrátorských práv používateľom.

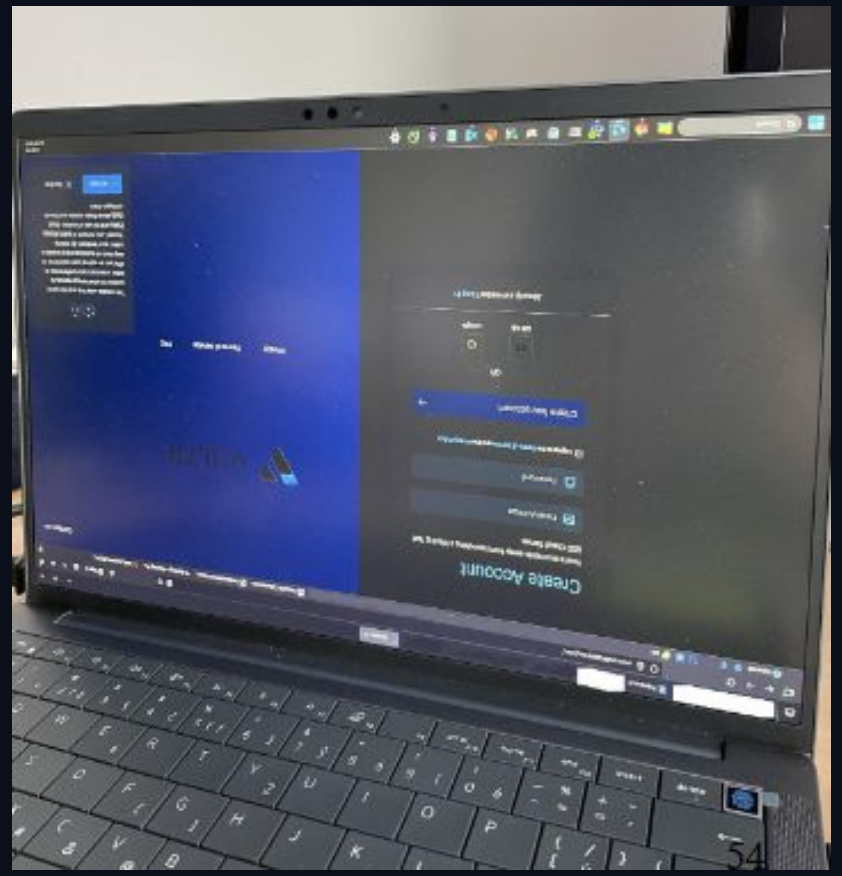
Vynútené šifrovanie diskov.

Centralizovaný patch management OS a kritických aplikácií.

VYNÚTENÁ HYGIENA: OPATRENIA ZA 0 €







DÁTA Z PRAXE:
RÝCHLOSŤ REAKCIE (MTTR)

Porovnanie času od vzniku alertu po jeho kompletnú triáž, obohatenie o kontext a počiatočné rozhodnutie:

Tradičný manuálny monitoring (L1 analytik)

~ 25 až 40 minút (závisí od rôznych faktorov)

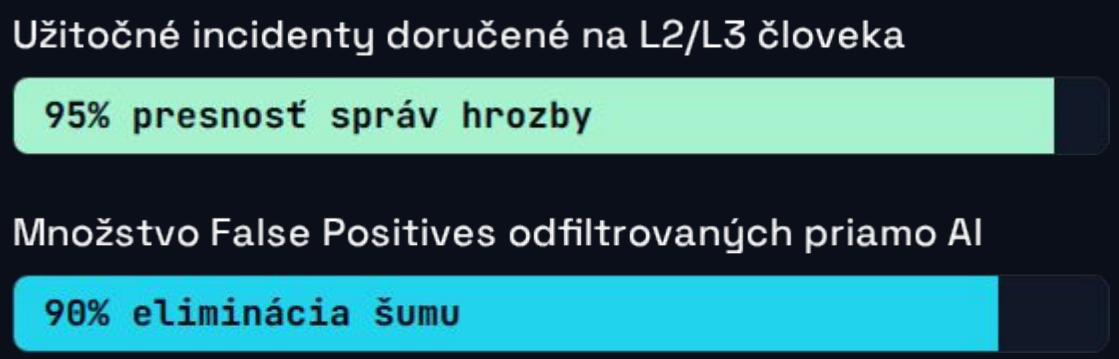
Náš model: L1 obohatené AI automatizáciou

< 15 sekúnd

DÁTA Z PRAXE:
ÚSPEŠNOSŤ FILTRÁCIE ALERTOV

Korelačný model AI vyrieši značnú časť šumu.

Seniorný inžinier (L2/L3) tak dostáva na stôl len **reálne, validované incidenty** s kompletným kontextom.



EKONOMIKA SOC: PREČO JE AI MODEL LACNEJŠÍ?

🖩 Interný 24/7 SOC

- Potreba 5–6 full-time na pokrytie zmien
- Mzdové náklady, fluktuácia, riziko
- **Finančne nedostupné pre stredné organizácie.**

⚡ Zdieľané MDR s AI L1 vrstvou

- Fixná, škálovateľná cena za službu, žiadne personálne réžie.
- Automatizovaná prvá línia znáša 100% záťaže bez ohľadu na objem logov.
- **Úspora > 75% nákladov** oproti budovaniu internej infraštruktúry.

AKO ROZDELIŤ ROZPOČET NIEKOĽKO TISÍC EUR?

Úloha v SecOpsS	*Tradičný manuálny prístup*	*Hybridný model (AI + MDR)*
Zber kontextu hrozby	15 – 30 minút (preklikávanie konzol)	**< 10 sekúnd (automatizované API)**
Filtrácia False Positives	závislá od pozornosti unaveného človeka	**90% eliminácia cez trénované modely**
Zákonná lehota ZoKB	riziko nestihnutia (víkendy, noci)	**garantovaná (SLA externého partnera)**

ZoKB nemôže zničiť váš biznis

Zákon o kybernetickej bezpečnosti (ZoKB) sa dá splniť bez masívnych investícií do nových nástrojov.

Čo očakáva auditor / zákon:

Komplexný auditovaný monitoring, okamžitá triáž a formálna eskalačná matica do 60 minút.

Ďakujem za Vašu pozornosť