AI alapú biztonsági monitoring megoldások

Sajó Péter

InfoSec Üzletág Igazgató, EURO ONE Zrt.

2026. 04. 23.

EIVOK

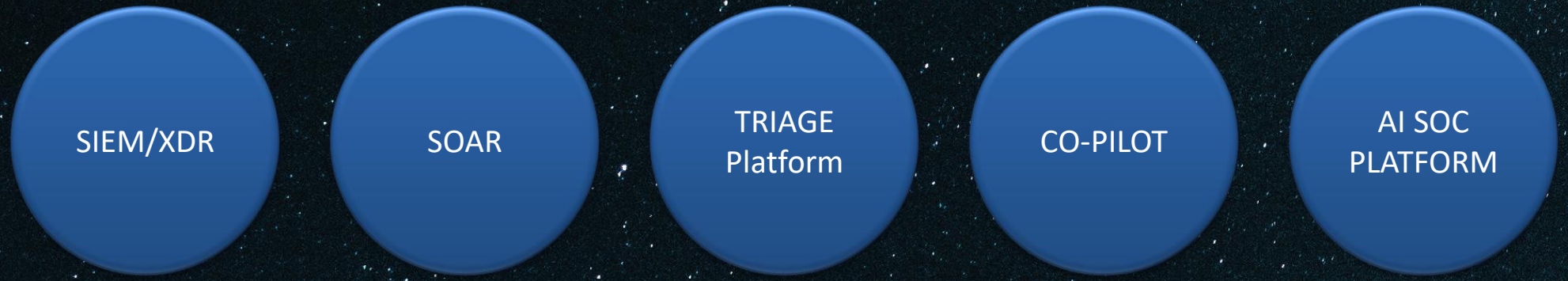
A valóság ma: Riasztás cunami

- A riasztások 40%-át nem elemzik
- A SOC csapatok 61% figyelmen kívül hagy riasztásokat, melyek később sajnos kritikusnak minősülhetnek
- MTTI átlagosan 70perc vs phising támadások <60perc
- „Szükséges kockázat”: 57%-a detekciós szabályokat töröl, rendszerek logolását állítja le
- Burn out általában 2,5 év
- Egy tapasztalt elemző felvétele 4-5 hónap (10-12 jelölt meghallgatása után)
- Egy új elemző betanulása minimum 2 hónap

Megoldás?

- AI washing – mindenhol AI
- AI for security – TOP 3 prioritás
- 88% akinél ma nincs AI a következő évben elkezdi a tesztelést
- 60% SOC taskok 2028-ra
- 70% nagy SOC pilotolni fognak AI agent megoldásokat
- 83%-a szerint legalább 50%-át az AI fogja végezni

Milyen megközelítések léteznek?



Mik a különbségek?

- ML/GenAI/Agentic AI/saját vagy nagy LLM használata?
- On-prem/Cloud/Hybrid?
- Incidens kezelés teljessége?
- Alert/Teljes kontextus?
- Kezelt SOC feladatok teljessége (Triage, L2/L3 elemzés, Hunting, SOAR, etc)?
- Data Privacy?
- Átláthatóság?
- Költség struktúra?
- Termék vízió és roadmap?

Eredmények 9 hónap éles tesztelés után

Hagyományos, de fejlett SOC		Agentic AI használatával (Az elemzők 100%-a támogatta a rendszer bevezetését)
20-45 perc	Átlagos incidens várakozási idő	0 perc
15 perc (2,5 perc – 2 óra)	Átlagos humán validálási idő elemzési idő	1,5 perc
70%	Átlagos fals pozitív arány	70%, de az AI mindent kiszűrt!
minden ügyfélnél létezik	Incidens backlog	MEGSZÜNT
5x8	Átlagos szolgáltatási idő	7x24
20-30 perc	Riport írás időigénye	0 perc

Intelmek, tanácsok

- Nagyon sok megközelítés létezik a piacon
- Nagyon eltérő elvárásokkal találkozunk
- Teljes Autonómia nem létezik jelenleg
- Tartsuk szem előtt az érzékeny adatok kezelését, biztonságát is
- Figyeljünk a rejtett költségekre

Today AI in the SOC is the biggest

„BUSINESS ENABLER”


Köszönöm a
figyelmet
euro one