ANDREWS IT ENGINEERING IT Engineering

SOC vezető tapasztalatAI

Az új ipari forradalomtól az éles LLM-megoldásokig — egy SOC mindennapjai a mesterséges intelligenciával.

Zámbó Marcell
SOC vezető · Andrews IT Engineering

A (KIBER)BIZTONSÁG GYAKORLATAI VOL. 2 · 2026.05.29 · LUDOVIKA

A NAGY KÉP

Új ipari forradalom — már a fejünkből is kiszervezünk

Eddig a motorikus, ismételhető, algoritmizálható munkát adtuk a gépnek. Most a gondolkodást, a döntést és a cselekvést is.

EDDIG — KISZERVEZVE A GÉPHEZ

- Ismételhető feladatok
- Számolás
- Algoritmizálható munka

→

MOST — EZT IS KISZERVEZZÜK

- Gondolkodás
- Döntéshozatal
- Cselekvés / megvalósítás

Új kérdések, új félelmek — és a szabályozás a fasorban sincs. A kérdés: mit teszünk, ha nem várhatunk rá?

A KERET

AI-Ready — négy pillér, amire az átállás épül

I. PILLÉR

Szabályozás és megfelelés

EU AI Act, NIS2, cégszintű AI-policy, adatosztályozás, incidenskezelés.

II. PILLÉR

Technikai architektúra

LLM-agnosztikus felépítés, vendor lock-in mitigáció, kódminőség, költség.

III. PILLÉR

Folyamat és szervezet

Szerepkörök újradefiniálása, human-in-the-loop, review és mérés.

IV. PILLÉR

Képzés és enablement

Hands-on workshop, vezetői tájékoztató, folyamatos mentoring.

Alverad × Andrews — AI-transzformációs munkacsoport

A pillérek megvalósítására, felmérésére és kutatására/kísérletezésére hoztuk létre. Nem PowerPoint-stratégia — éles megvalósítás.

A munkavállalói valóság — négy csoport

Nézzük a szervezeti és képzési pillért közelről: egy csapatban négy markánsan eltérő viszonyulás él egymás mellett.

01

Tudatosan nem használja

Tiltott, nem teheti, vagy elvi döntés. A kérdés: a tiltás megfontolt, vagy csak a szabályozatlanságot fedi el?

02

Használja — de nem tudja

Beépített AI-funkciók a napi eszközeiben. „Árnyék-AI": kontroll és tudatosság nélkül.

03

Fél tőle vagy csalódott

Félti a munkáját, és/vagy elégedetlen a képességekkel — valós korlát miatt, vagy mert hiányzik a tudás a jó használathoz.

04

Élvezi — és hatékonyabb

Beépíti a munkafolyamataiba, jobb eredménytermékeket és szoftvert állít elő. Itt realizálódik a valódi érték.

A vezető dolga mind a négy csoport kezelése — nem a 4-es csoport ünneplése, hanem az 1-3 átvezetése.

GOVERNANCE & LLM-OPS

Szabályozottság, nyomon követhetőség, megbízhatóság

01 · Szabályozottság & enablement

Céges keret + képzés

- AI/LLM-használat szabályozottsága cégszinten
- Bevezetés-támogatás: oktatás
- Szerepköri leírások módosítása

02 · Prompt-tár & provenance

Verziózott prompt-tárak + „vízjelezés"

- Verziózott, megosztott prompt-tárak
- Egy eredménytermékről tudni kell: melyik **alkalmazás**, melyik **LLM-modell**, melyik **prompt** hozta létre

03 · LLM-monitoring

Működik-e, és józan-e?

- 1) Elérhető-e, működik-e a szolgáltatás?

2) Periodikus hallucináció-/drift-vizsgálat — **mikor és hogyan vesszük észre, ha az LLM-ünk elkezdett megbolondulni?**

A provenance és a monitoring nélkül az AI-eredmény nem auditálható és nem megbízható — köthető az ökoszisztéma „mérés" rétegéhez.

Az MI-biztonság ökoszisztémája — hét keret, egy háló

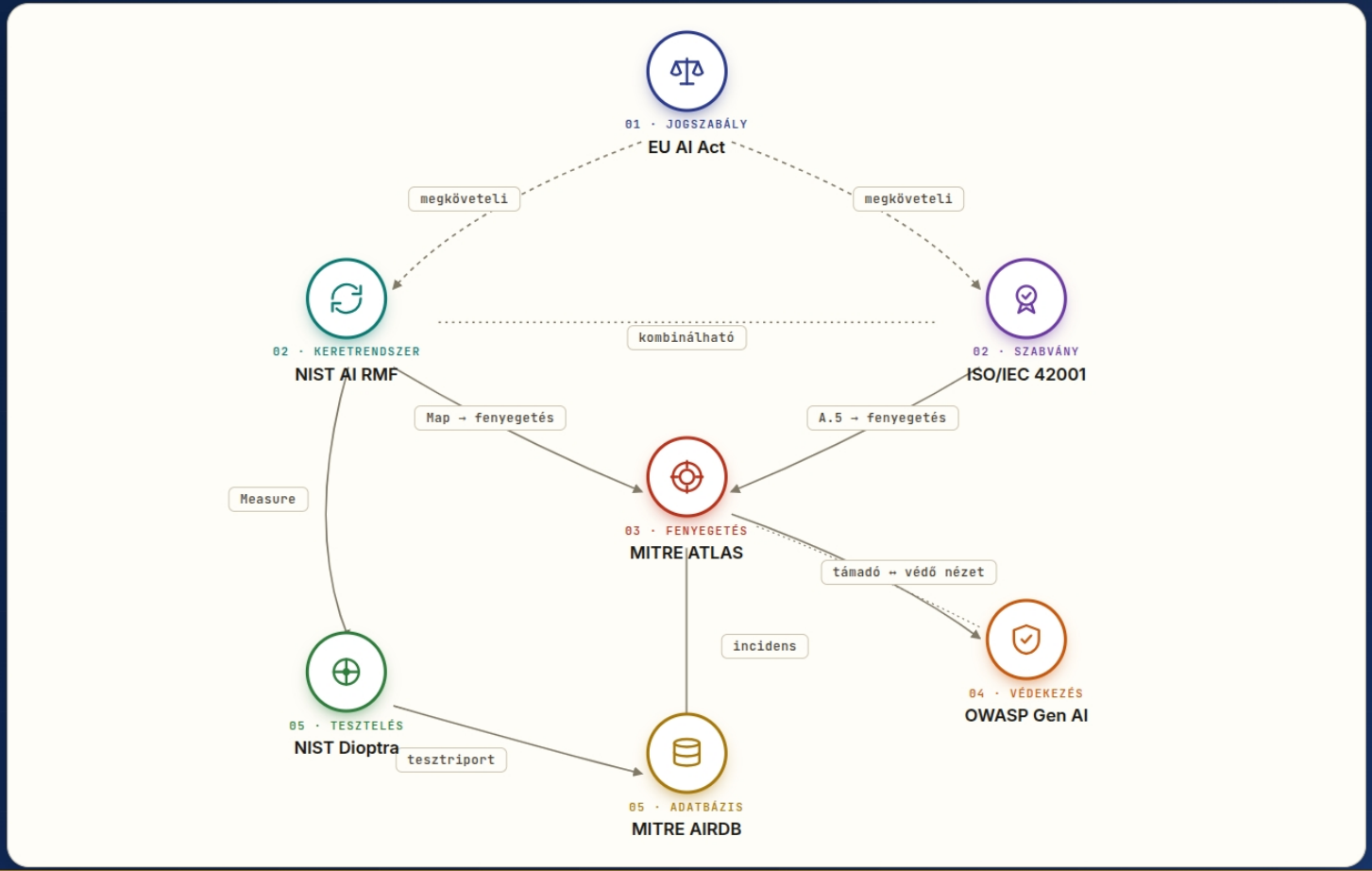
01 **Jogi alap**
Mit kell tenni? — EU AI Act

02 **Irányítás**
Hogyan szervezzük? — NIST AI RMF, ISO 42001

03 **Fenyegetés**
Mi ellen? — MITRE ATLAS

04 **Védekezés**
Hogyan védjük? — OWASP Gen AI

05 **Mérés**
Mivel követjük? — NIST Dioptra, MITRE AIRDB



A TECHNIKAI PILLÉR — INNEN A SEXY RÉSZ

AI a termékeinkben — három éles példa

NATO LOCKED SHIELDS 2026

sansin / expo-bridge

DFIR-asszisztens · Velociraptor

- FastAPI-bridge az EXPO gyakorlatplatform és a Velociraptor között
- Beágyazott LLM-asszisztens: 122 tool, multi-turn ReAct
- Approval-gate-ek (T0/T1/T2), provider-absztrakció
- 200+ endpoint, 50-100 analyst

ALERT-TRIAGE

soc-analyst-web

AI alert-triage + kampányelemzés

- 3 párhuzamos elemzés: technikai · security · vezetői
- MITRE ATT&CK, bulk kampánydetektálás
- **Maszkolás**: PII tokenizálás az LLM előtt, visszafejtés
- Prompt-injection szűrés, Sigma-lefedettség

AI HONEYPOT

Honaipot

Megtévesztés mesterséges intelligenciával

- Magas-interakciós SSH honeypot
- LLM emulál meggyőző Linux-shellt
- Rögzíti a támadói tevékenységet — törölt fájlokat is

imssp × KFI — LLM a SIEM motorjában

A saját SIEM-ünk (imssp) éles kutatás-fejlesztése: a SOC hatékonyságának növelése nagy nyelvi modellekkel — lokálisan futtatható, testreszabható modellel.

Automatizált log-feldolgozás
Eseménynaplók normalizálása, onboarding-támogatás.

Intelligens whitelist-generálás
Zaj-elnyomó szabályok automatikus javaslata a forrásnál.

Automatizált riasztásszabály
Detection-rule generálás és hangolás támogatása.

Természetes nyelvű magyarázat
A riasztási szabályokra és az incidensek kiváltó okaira — gyorsabb, megalapozottabb döntés.

Lokális, testreszabható modell
Csökkenti az adatszivárgás és a hibás következtetések kockázatát.

NIS2-támogatás
A magasabb szintű kiberbiztonsági követelmények teljesítéséhez.

Megépített építőkövek a gyakorlatból: **Log Coverage Analyzer** (LLM javasol hiányzó winlogbeat/filebeat-konfigot) · **Reduce WL Noise by AI** (LLM generál zaj-elnyomó Logstash-filtert).

SZINTÉZIS

A kettő együtt — LLM a fejlesztésben ÉS a termékben

A FEJLESZTÉSBEN

LLM-támogatott fejlesztés

- A KFI-projektjeinkben nap mint nap LLM-mel fejlesztünk
- Gyorsabb prototípus, több éles tapasztalat
- „Amit tanácsolunk, azt magunk is csináljuk" — nem könyvből tanultuk

A TERMÉKBEN

LLM mint képesség

- Triage, log- és detection-engineering, megtévesztés, DFIR-asszisztens
- Maszkolás, lokális modell, approval-gate-ek — felelős használat
- Az éles termék visszatáplálja a fejlesztési gyakorlatot

A kör bezárul: gyorsabb fejlesztés → jobb termék → több éles tapasztalat → még jobb fejlesztés. Ez különböztet meg a tanácsadótól.

RENDSZERSZINTŰ HATÁS

A SOC-CMM tükrében — mind az öt domaint érinti

Amiről eddig beszéltünk, nem pontmegoldás: a SOC Capability Maturity Model mind az öt domainjében mozdít.

01 · BUSINESS
Üzlet & governance
- EU AI Act · NIS2 · ISO 42001
- Adatvédelem — lokális modell
- Vendor lock-in kezelése

02 · PEOPLE
Emberek
- A négy munkavállalói csoport
- Szerepkörök újradefiniálása
- Oktatás · human-in-the-loop

03 · PROCESS
Folyamat
- Detection- / use case engineering
- Prompt-tár & provenance
- LLM-monitoring (hallucináció/drift)

04 · TECHNOLOGY
Technológia
- imssp SIEM × LLM
- soc-analyst-web · sansin · Honaipot
- Maszkolás · lokális/nyílt LLM

05 · SERVICES
Szolgáltatások
- Triage · DFIR-asszisztens
- NL incidens-magyarázat
- Log management

Az AI nem egy doboz a sarokban — mind az öt domaint mozdítja. Ezért rendszerszinten kell kezelni, nem eszközönként.

TANULSÁG

Az AI nem a kezünkből veszi ki a munkát — a fejünkből. Ezért nem várunk a szabályozásra: kerettel, governance-szel és éles termékekkel csináljuk.

FOLYTATJUK A PANELBEN — 12:20, „AI VEZÉRELT A BIZTONSÁG GYAKORLATBAN"

- Human-in-the-loop
- Bizalom vs. sebesség
- Túl sok / túl kevés automatizálás
- Vendor lock-in
- AI az AI ellen

ANDREWS IT ENGINEERING

NEKÜNK AZ ÖN BIZTONSÁGA AZ ELSŐ!

Az LLM-alapú biztonság nem kérdés — a hogyan az.

Az Alverad × Andrews AI-transzformációs munkacsoport a szabályozástól az architektúrán és a folyamatokon át a képzésig kíséri az LLM-átállást — éles termékekkel és mérnöki felelősséggel.

Zámbó Marcell · SOC vezető | andrews.hu | info@andrews.hu | +36 1 428 0600

1138 Budapest, Tomori utca 32. | LinkedIn | GitHub