

Ai alapú kiberbiztonsági incidensek gyakorlatai Inci-fincik az AI korában

Marsi Tamás
NBSZ NKI



A bot nem alszik, csak targetál



NEMZETI
KIBERBIZTONSÁGI
INTÉZET



Az AI a tömeges támadást személyesnek álcázza

Szia főnök, csak épp nem én vagyok



NEMZETI
KIBERBIZTONSÁGI
INTEZET

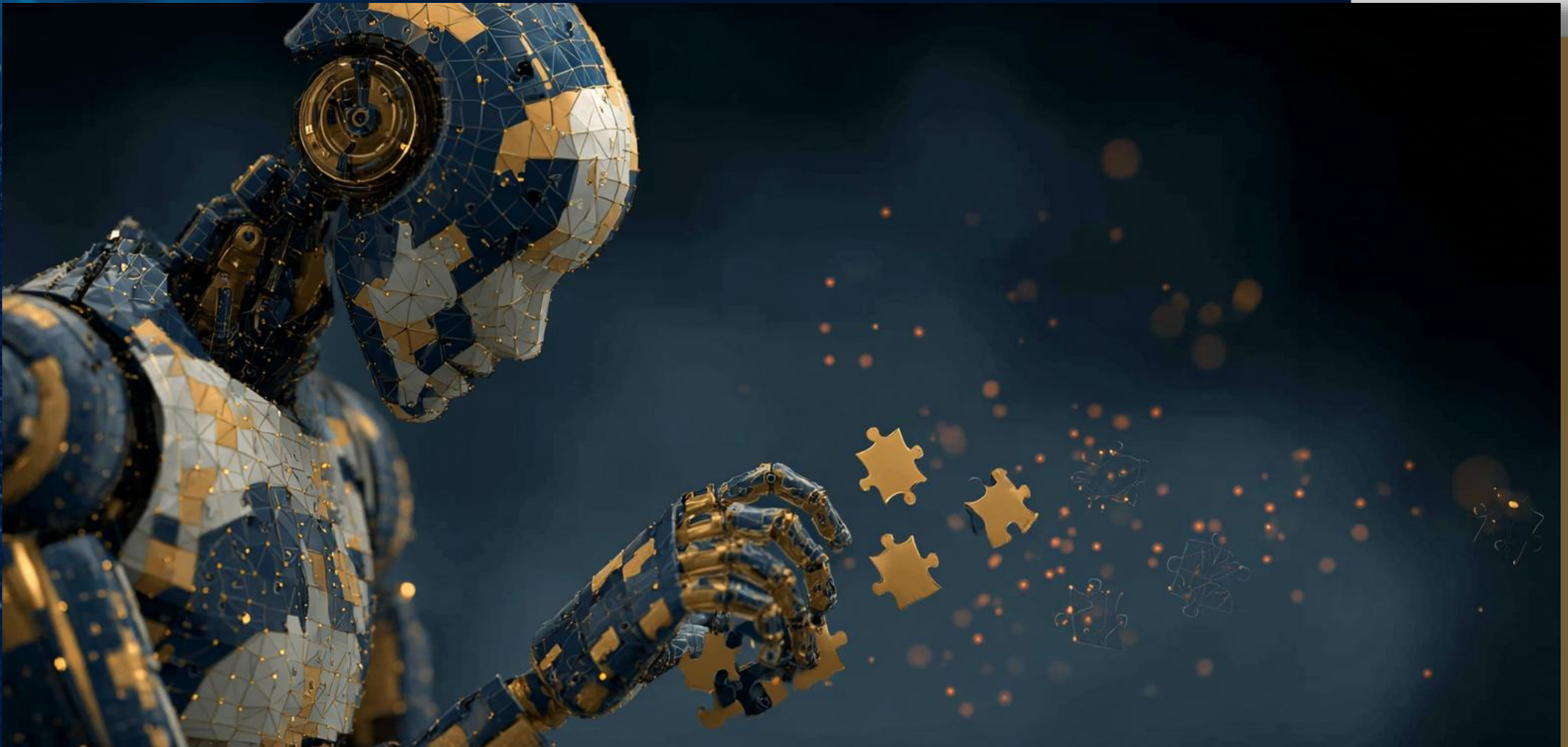


A deepfake nem sci-fi, hanem meeting-meghívó

Malware Lego: összepattint, elküld, baj van



NEMZETI
KIBERBIZTONSÁGI
INTÉZET

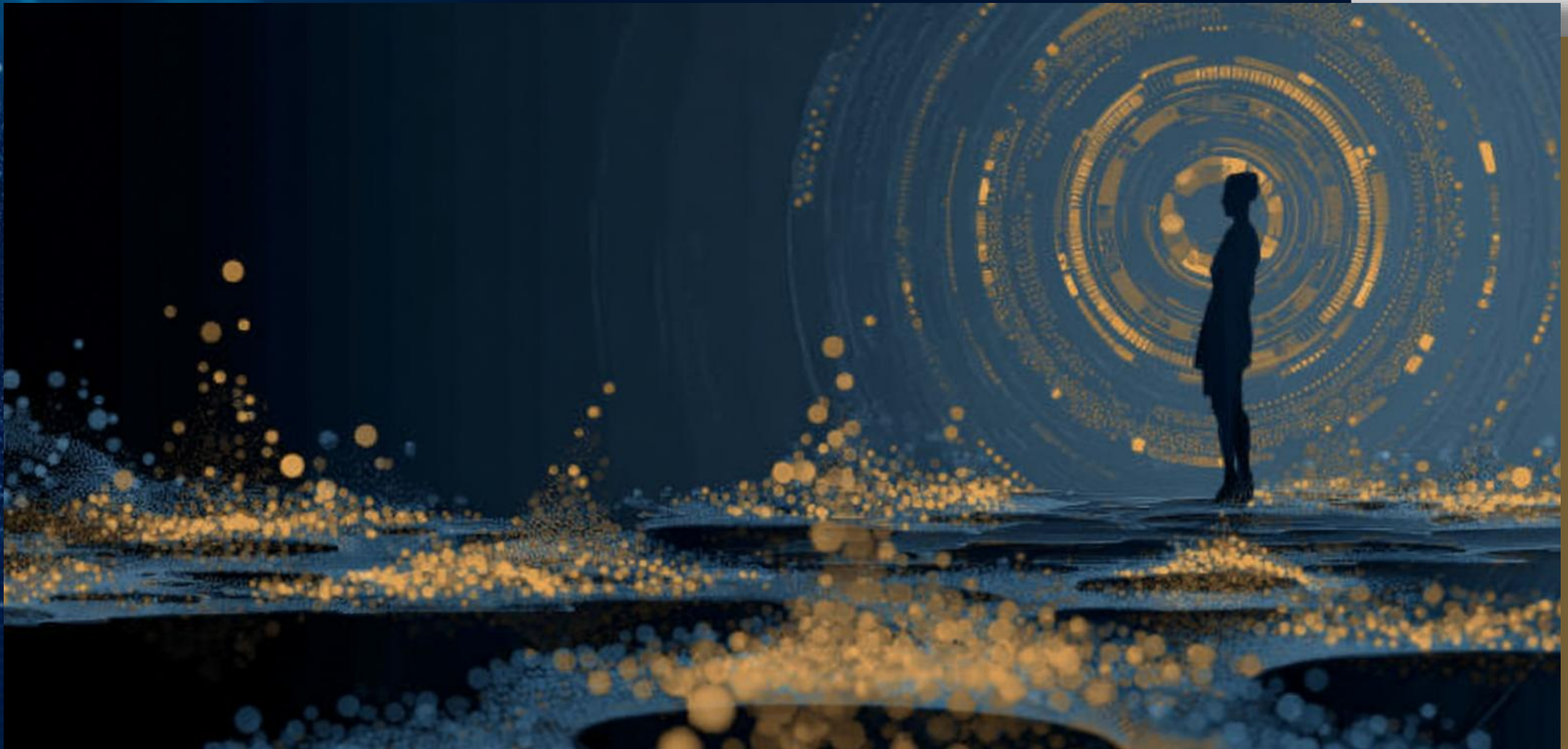


Az AI csökkenti a belépési küszöböt, nem a felelősséget

Letapogatás turbó módban



NEMZETI
KIBERBIZTONSÁGI
INTEZET



Ami régen órákig tartott, AI-val percek alatt térképpé válik

SOC, de koffein helyett modell



NEMZETI
KIBERBIZTONSÁGI
INTÉZET



Az AI nem váltja ki az elemzőt, csak elveszi tőle a favágást

Patch előtt gondolkodj, utána aludj



NEMZETI
KIBERBIZTONSÁGI
INTÉZET

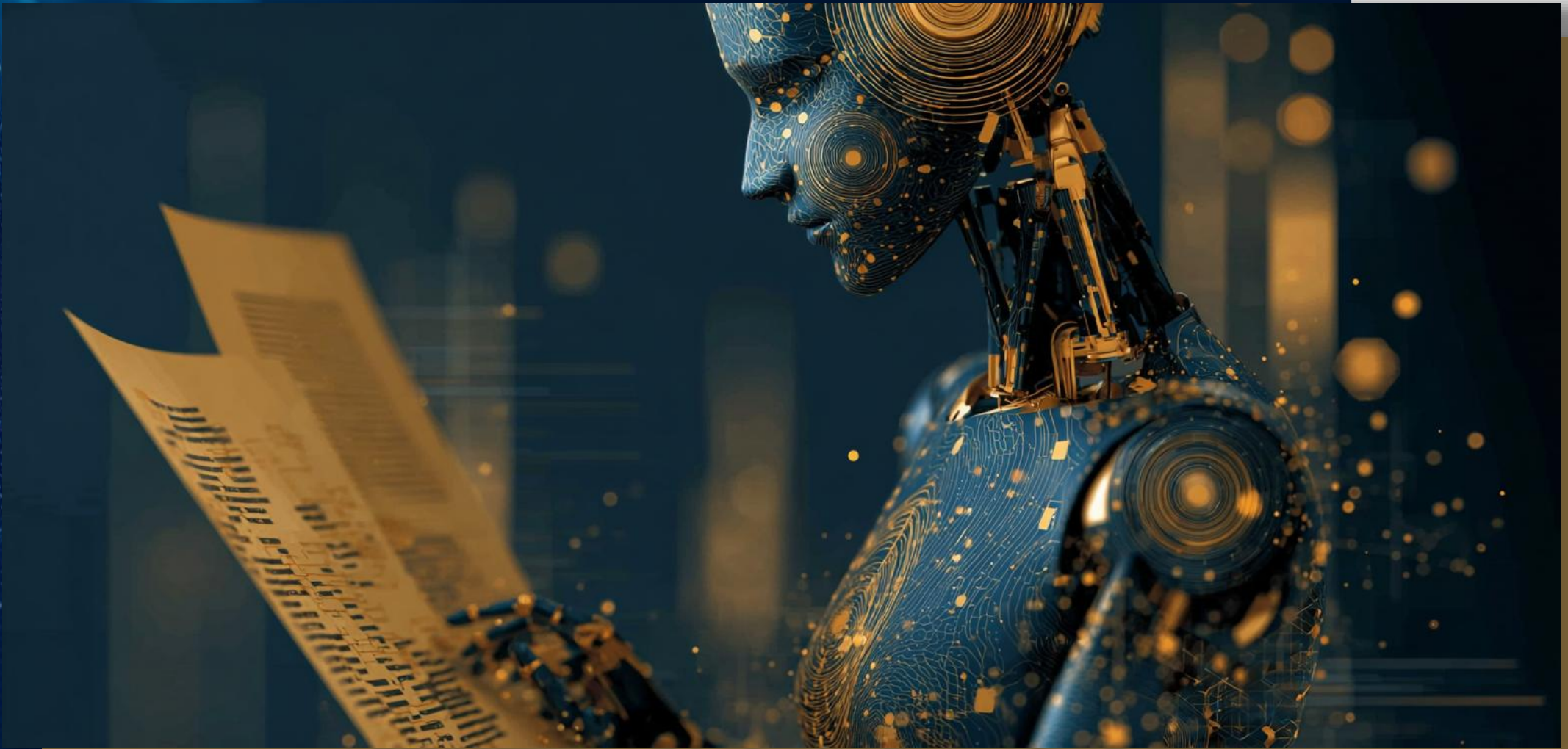


A megelőzés akkor jó, ha unalmasnak tűnik

Compliance: a papírsárkány megszelídítése



NEMZETI
KIBERBIZTONSÁGI
INTÉZET



A megfelelés nem Excel-szenvedés, ha az AI előválogat

Prompt injection: amikor a chatbot elhiszi a cetlit



NEMZETI
KIBERBIZTONSÁGI
INTÉZET



Az AI-rendszer is felhasználó — csak nagyon hiszékeny

Gyakorlat: a tűzriadó, csak digitálisan

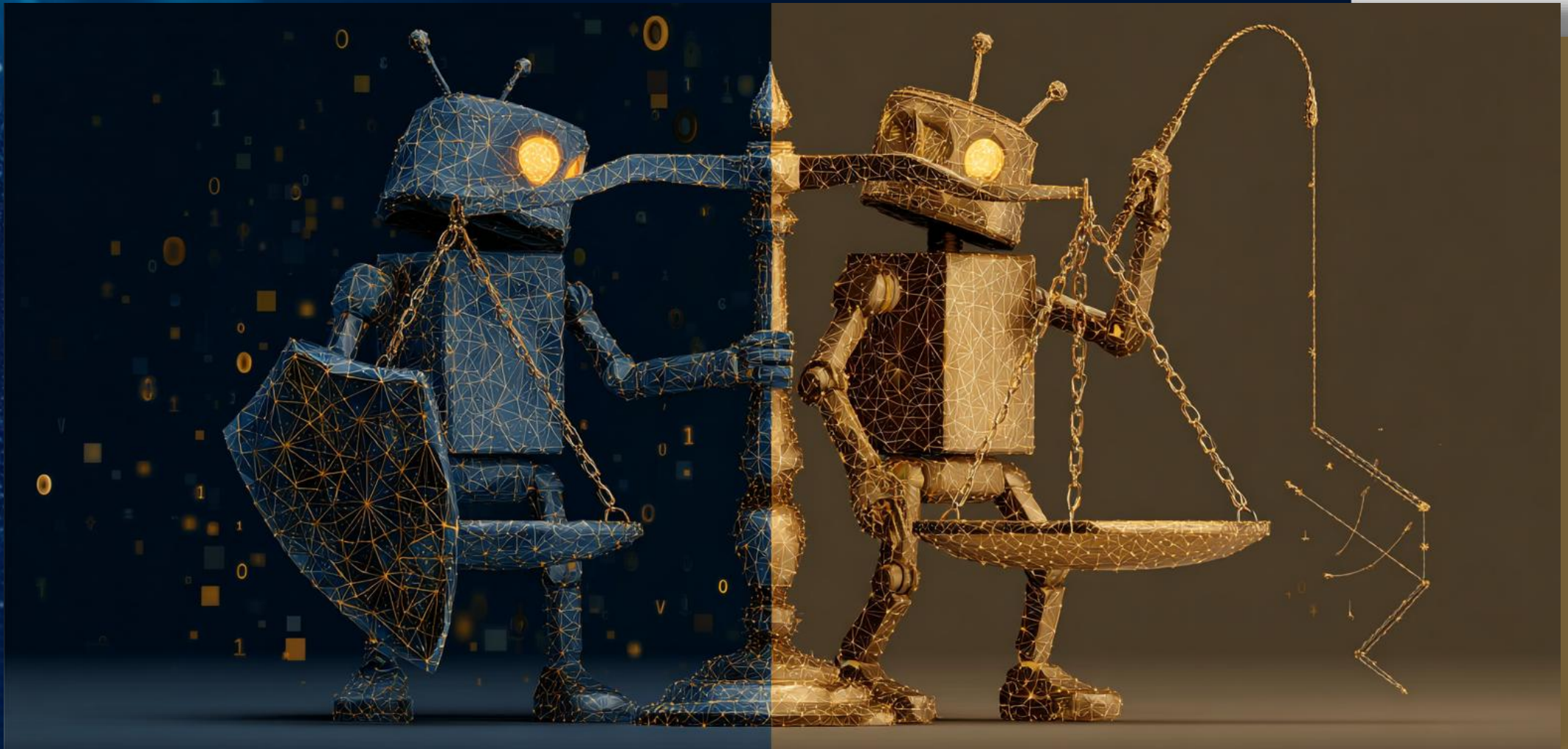


NEMZETI
KIBERBIZTONSÁGI
INTEZET



Incidens közben nem stratégiát írunk, hanem elővesszük

Nem terminátor, csak nagyon gyors gyakornok



Az AI kockázat is, lehetőség is — attól függ, ki tanítja be

Köszönöm a figyelmet!

Marsi Tamás
NBSZ-NKI



 NEMZETI
KIBERBIZTONSÁGI
INTÉZET