

AI egy SOC-nál

Készítette

Black Cell Magyarország Kft.

Mit értünk AI alatt?

AI a SOC szolgálatában

A mesterséges intelligencia egy olyan koncepció, amely magában foglal minden olyan rendszert, amely az emberi intelligencia és kognitív képességek szimulálására törekszik. Egy biztonsági műveleti központ (SOC) kontextusában az AI célja a biztonsági elemzők döntéshozatali és érvelési képességeinek utánozása/automatizálása. Mivel a mesterséges intelligencia egy rendkívül tág fogalom, amely rengeteg megközelítést takar, könnyen lehet, hogy egy SOC-ban már eleve jelen vannak AI-alapú eszközök vagy megoldások.



**Gépi
tanulás**



**Formális
logika**



**Statisztikai
megközelítések**

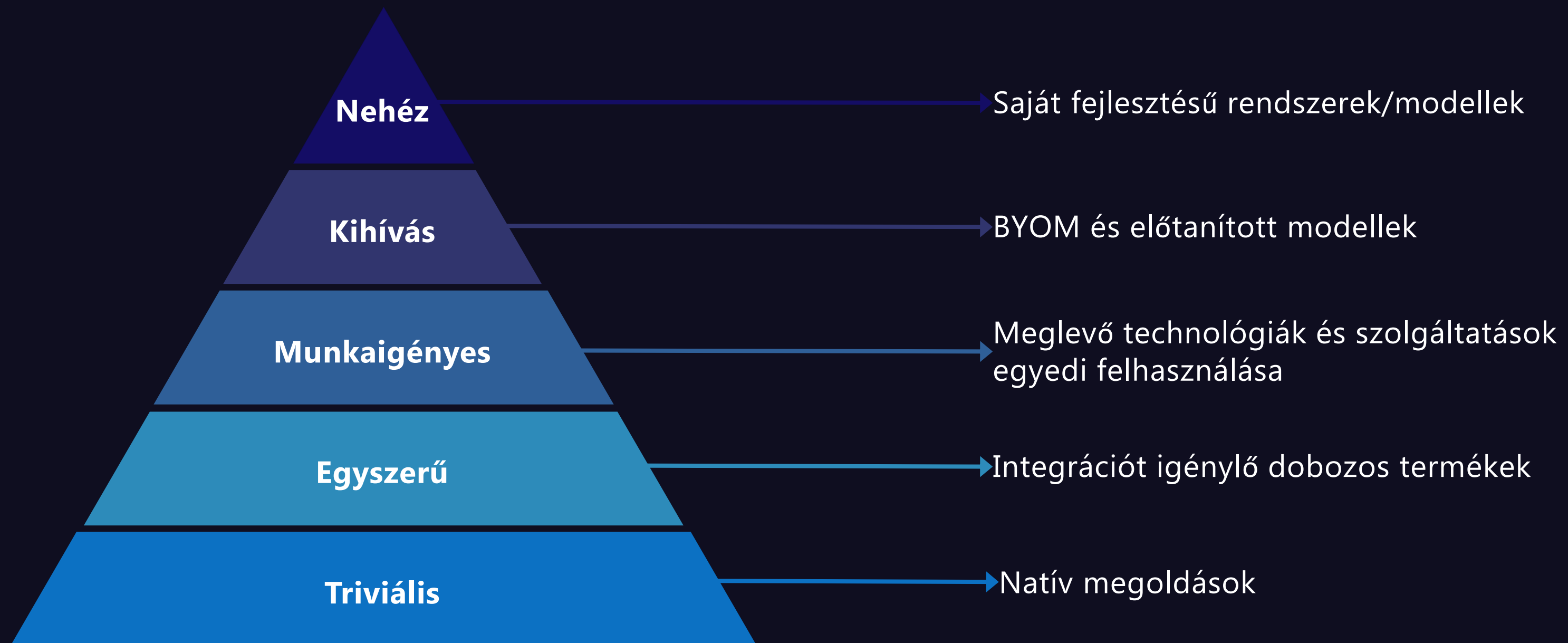


**Szimbolikus
mesterséges
intelligencia**



AI alkalmazásának szintjei

Az AI rendszerek hozzáadott értéke



Automatizálható munkafolyamatok



Detekció



Triázs



DFIR



Fenyegetésvadászat*



**Riport Készítés /
Dokumentáció****

Detekció

AI munkafolyamatok

Az AI célja ebben a kontextusban az észlelési képességek javítása nagy mennyiségű adat (pl. naplók, fájlok, hálózati csomagok) emberi intelligenciával történő elemzésével.



Az emberi képesség amelyet reprodukálni szeretnénk, lehet kevésbé összetett is. Azonban egy ilyen rendszer nem feltétlenül lesz mesterséges intelligencia.



ovyvwnkjserklcrjwwhpcucyurwjaelg.com
Egy CryptoLocker domain.



lecanardenchaine.fr
Egy francia satirikus újság domain-je.

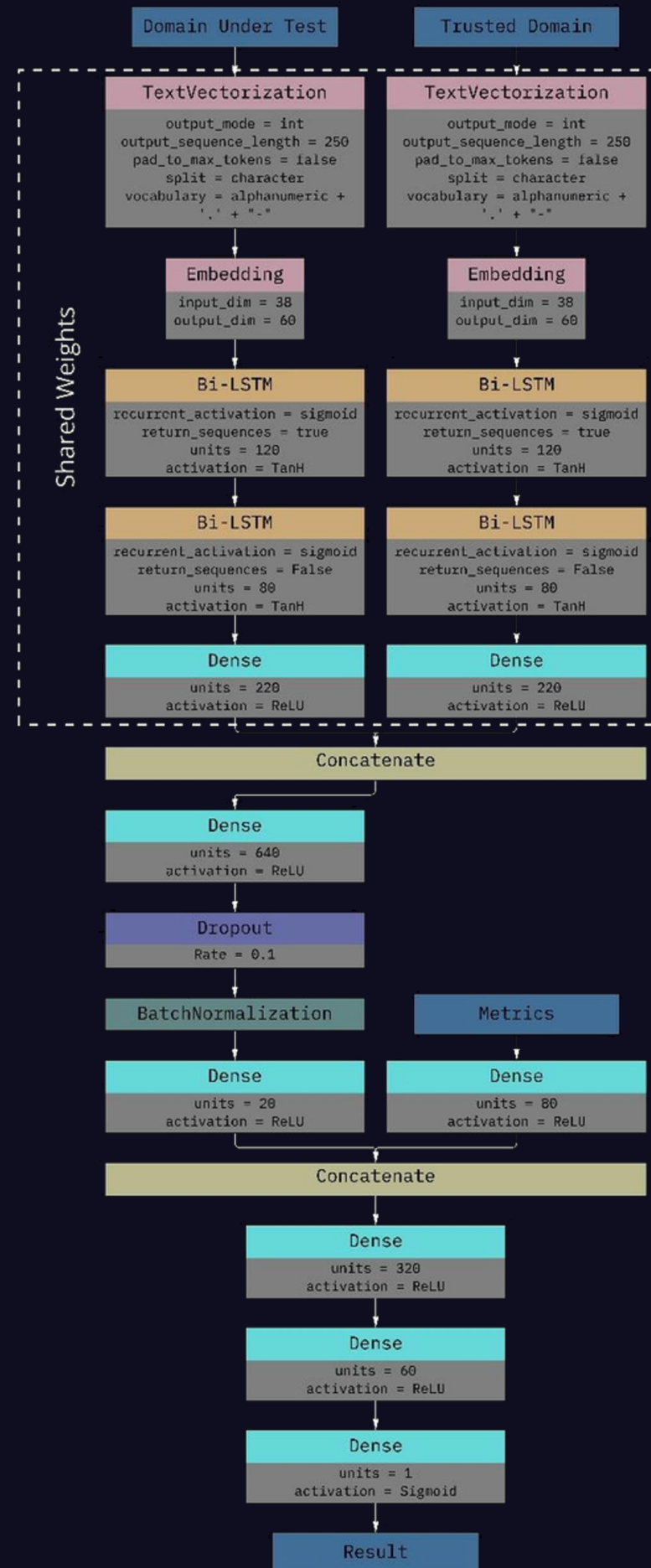


basketdifficultinstead.net
Egy Suppobox domain.

Detekció

AI munkafolyamatok

Az AI rendszer állhat kisebb érzékelőkből.



Triázs és Döntéstámogatás

AI munkafolyamatok

Az AI célja egy adott riasztás osztályozása, a kontextus és kapcsolódó események alapján. Mindezt az emberi elemzők gondolatmeneteinek emulálásával teszi.



Triázs és Döntéstámogatás

AI munkafolyamatok

Az AI rendszernek nem muszáj a teljes incidenssel kapcsolatosan döntést hoznia. Elegendő ha az elemzőt támogatja ebben.

The screenshot displays the Microsoft Defender Security Center interface for a specific incident titled "Multi staged attack leading to Domain Controller compromise - Possible Midnight Blizzard (NOBELIUM)". The incident is classified as High and Active. The interface is divided into several sections:

- Alerts:** A list of alerts on the left, including "Suspicious sequence of exploration activities", "ADFS private key extraction attempt", "Suspected AD FS DKM key read", "Attempt to hide use of dual-purpose tool", "Sensitive credential memory read", and "Activity from a Tor IP address".
- Incident graph:** A central network diagram showing the relationships between various entities involved in the attack.
- Timeline:** A list of events at the bottom, such as "2zimba4i.iul.exe executed a script" and "[892] whoami.exe".
- AI Analysis (Copilot):** A panel on the right titled "Ongoing hands-on-keyboard attack via Impacket toolkit". It provides a detailed script analysis of a PowerShell script, including its purpose (logging, exporting certificates) and a list of recommendations for remediation and prevention.

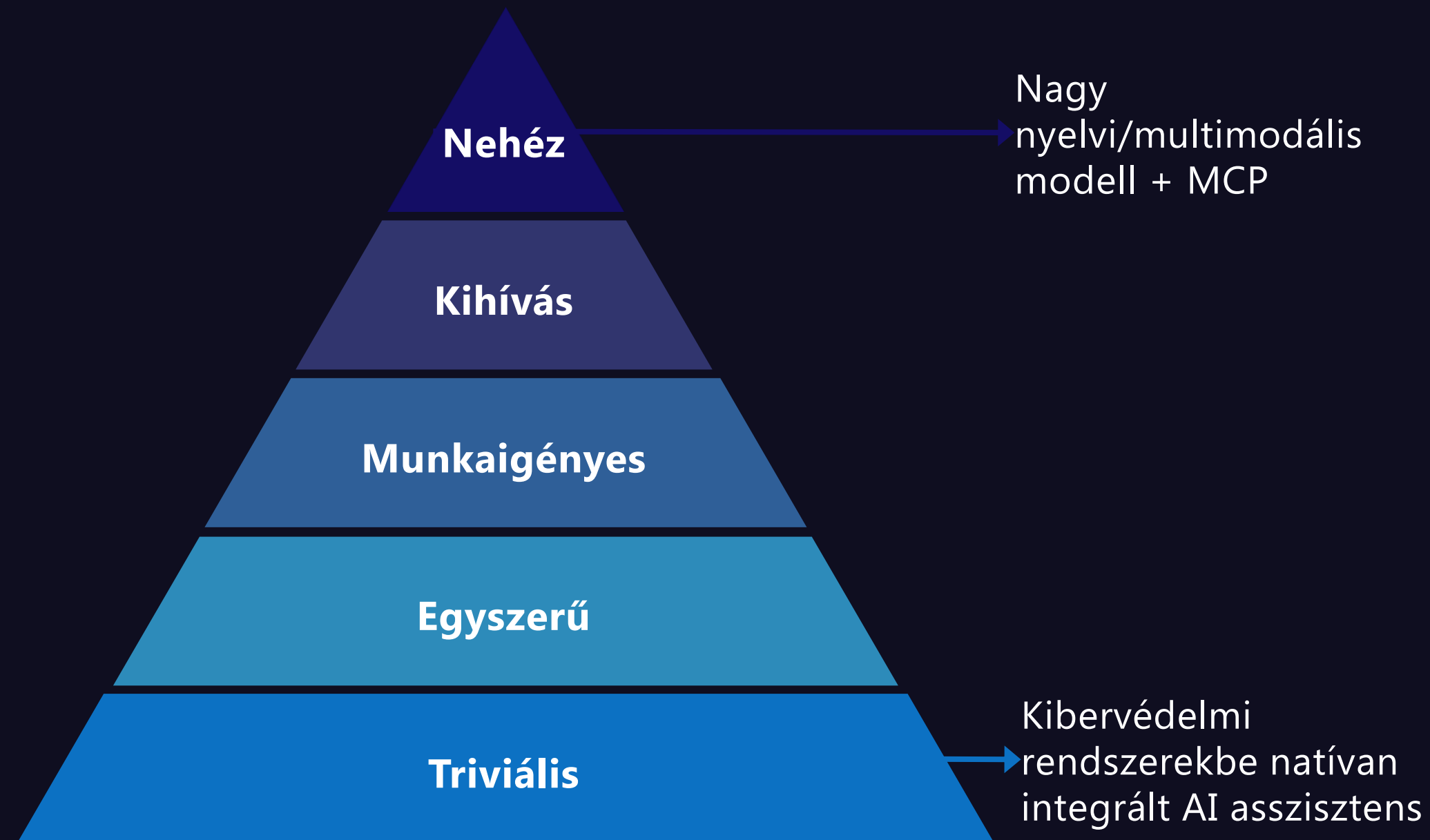
The AI analysis section includes the following details:

- Script analysis:** Mar 26, 2024 3:10 PM. The script performs logging, exports the ADFS token signing certificate, and uploads it to a remote storage location.
- Recommendations:** A list of four actions to take, such as "The script generates a unique job ID and sets up logging to a local file and a remote endpoint."
- Alert state:** True positive, Assigned to API-App:API Action.

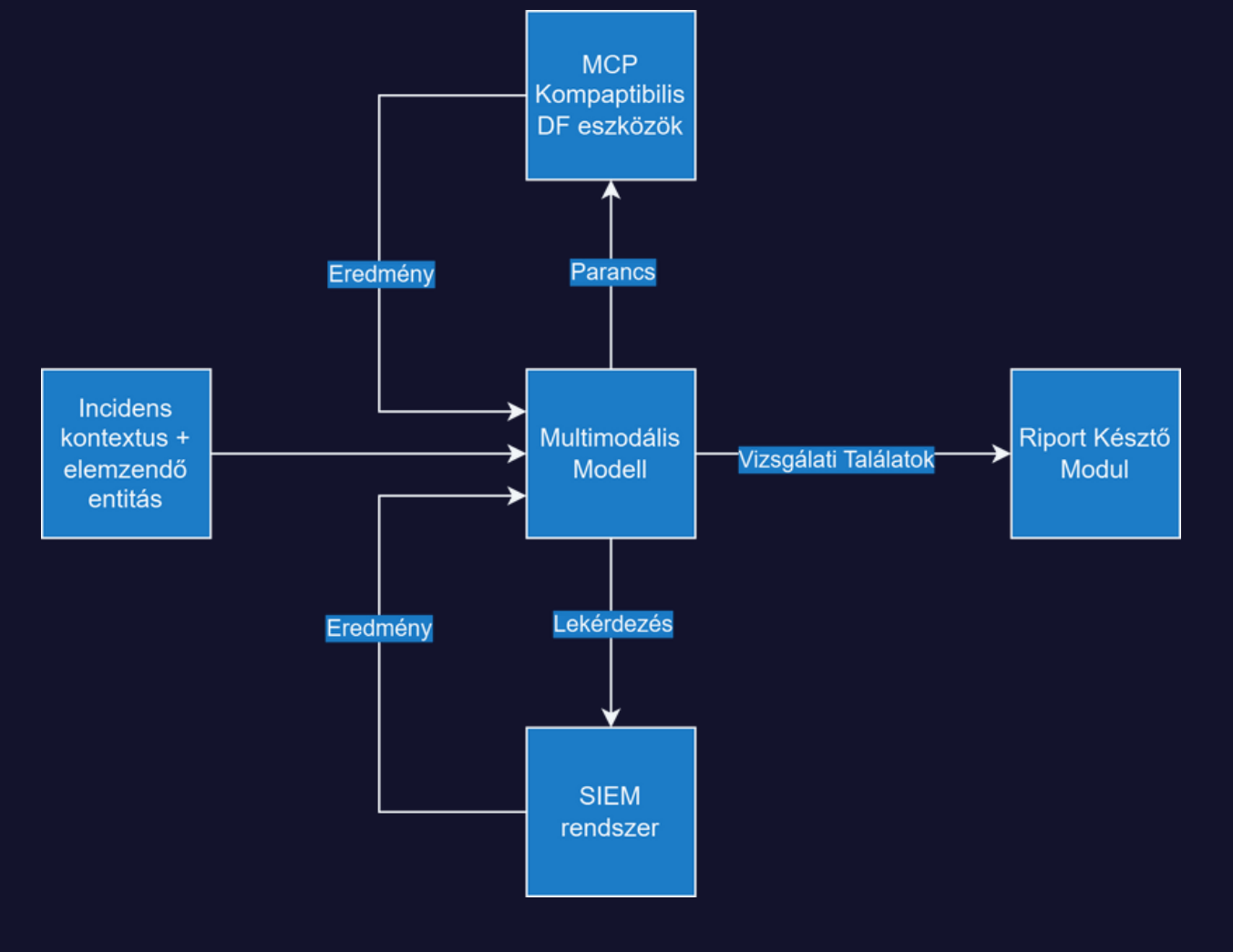
Digital Forensics

AI munkafolyamatok

Egy összetett AI rendszer célja a kártékony minták elemzése, valamint a vizsgálat során szerzett digitális nyomok korrelálására az incidens kontextusához köthető eseményekkel.

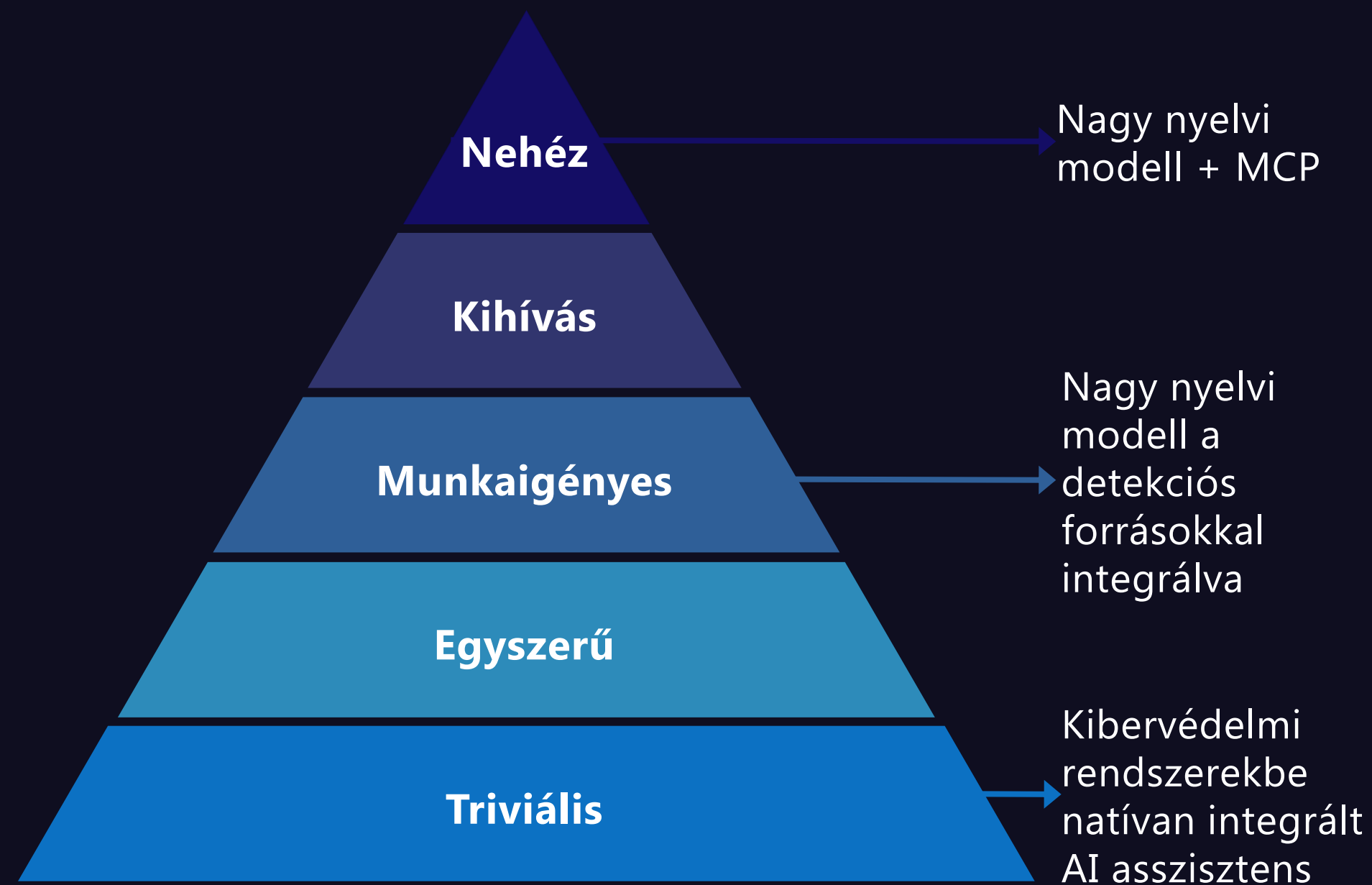


Egy kellően kifinomult modell képes lehet akár a teljes vizsgálati folyamatot véghez vinni.



Incidenskezelés AI munkafolyamatok

Az AI segíthet a riasztás kontextusának elemzésével beazonosítani a szükséges válaszlépéseket, vagy akár automatizálva véghez is viheti azokat.



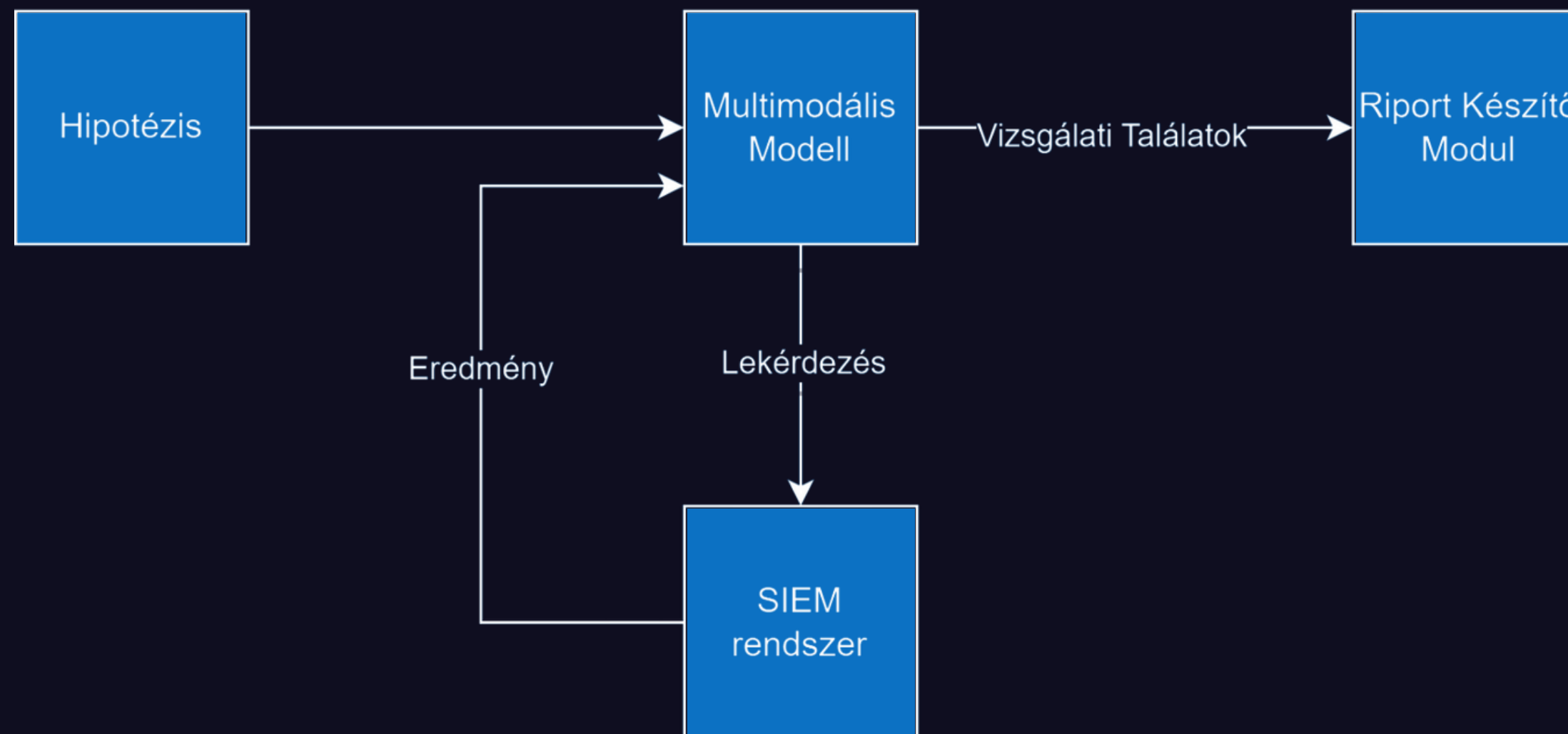
This block contains several screenshots from a Microsoft 365 security interface, illustrating AI-generated remediation tasks and a Teams message:

- Containment:** A task titled "Disable the account Name" with a status of "Completed". It includes a button for "Attack Disruption" and a warning: "AI-generated content may be incorrect. Check it for accuracy."
- Remediation:** A task titled "Delete similar emails" with a status of "New". It includes a button for "Soft delete emails" and a warning: "AI-generated content may be incorrect. Check it for accuracy."
- Remediation:** A task titled "Disable the account Name in AD" with a status of "Completed". It includes a warning: "AI-generated content may be incorrect. Check it for accuracy."
- Remediation:** A task titled "Reset password for Name" with a status of "New". It includes a button for "Force password reset" and a warning: "AI-generated content may be incorrect. Check it for accuracy."
- Teams Message:** A message from the "Cyber Security Team" to "Contact user lisa@avoriaz.alpineskihouse.co on Teams, and ask them to confirm their activity". The message includes details about unusual activity on July 23, 2024, and asks for confirmation. It includes buttons for "Contact user in Teams" and "Copy to clipboard".

Fenyegetésvadászat

AI munkafolyamatok

Az AI a hipotézis-alapú fenyegetésvadászatot azzal támogathatja, hogy képes értelmezni a kompromittálódásra vonatkozó feltételezést, és ennek mentén lekérdezéseket indítani a SIEM rendszerben a hipotézis alátámasztására vagy elvetésére. Ez a megközelítés jelenleg inkább elméleti jellegű, korlátozott gyakorlati alkalmazással és kutatási háttérrel.



Köszönöm a figyelmet!

