BLACK CELL
Protecting critical infrastructures

# 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**

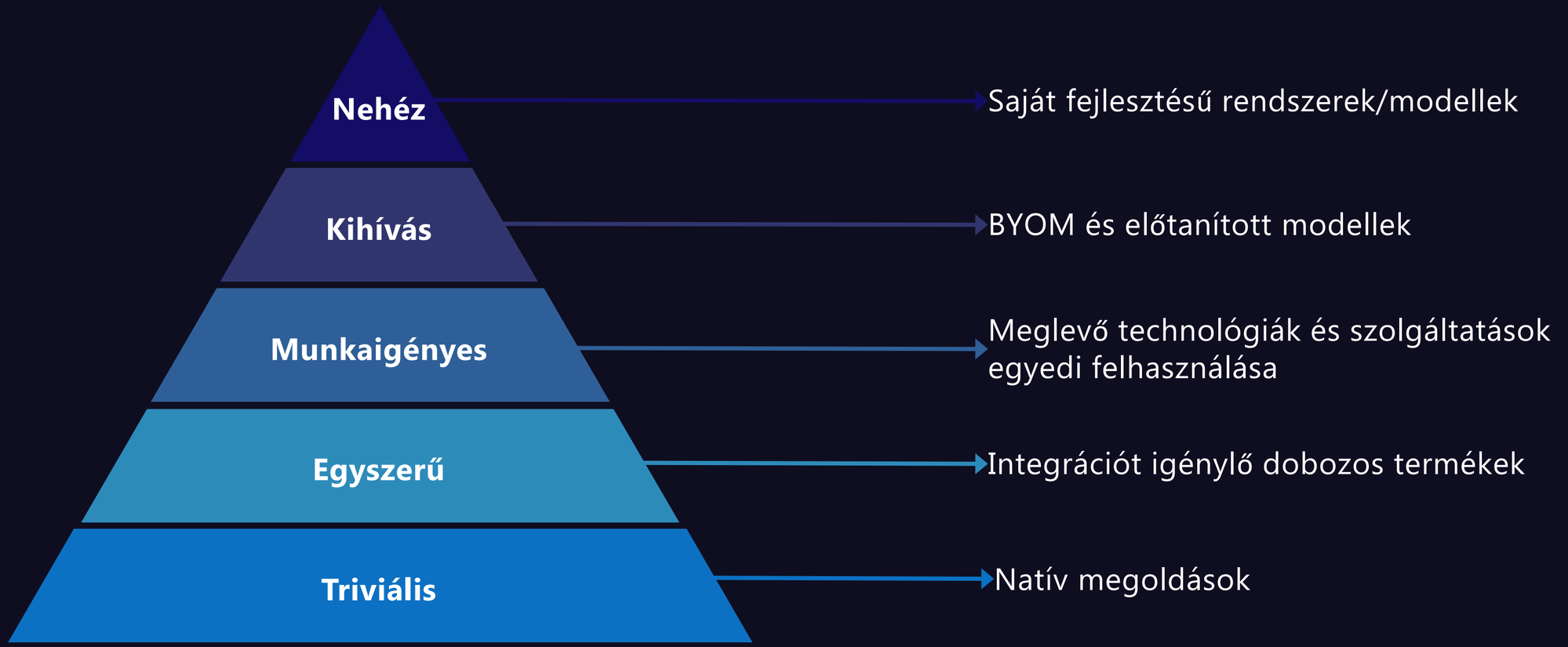
**Formális logika**

**Statisztikai megközelítések**

**Szimbolikus mesterséges intelligencia**

# AI alkalmazásának szintjei

## Az AI rendszerek hozzáadott értéke




TLP:CLEAR

# 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 feltétlenült lesz mesterséges intelligencia.

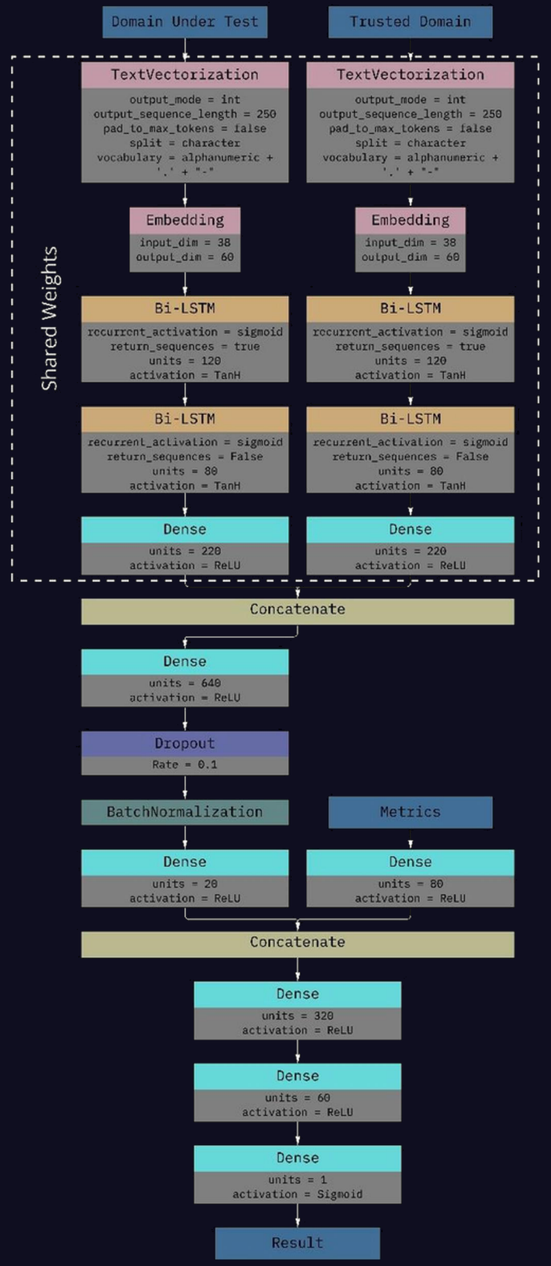
**ovyvwnkjserklcrjwwhcpucyurwjaelg.com**
**Egy CryptoLocker domain.**

**lecanardenchaine.fr**
**Egy francia szatirikus 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.


A riasztás tulajdonságainak modellezése és szimbolikus mesterséges intelligenciai rendszer fejlesztése

A riasztás információtartalmának struktúrálása és átadása egy meglevő klasszifikációs rendszernek

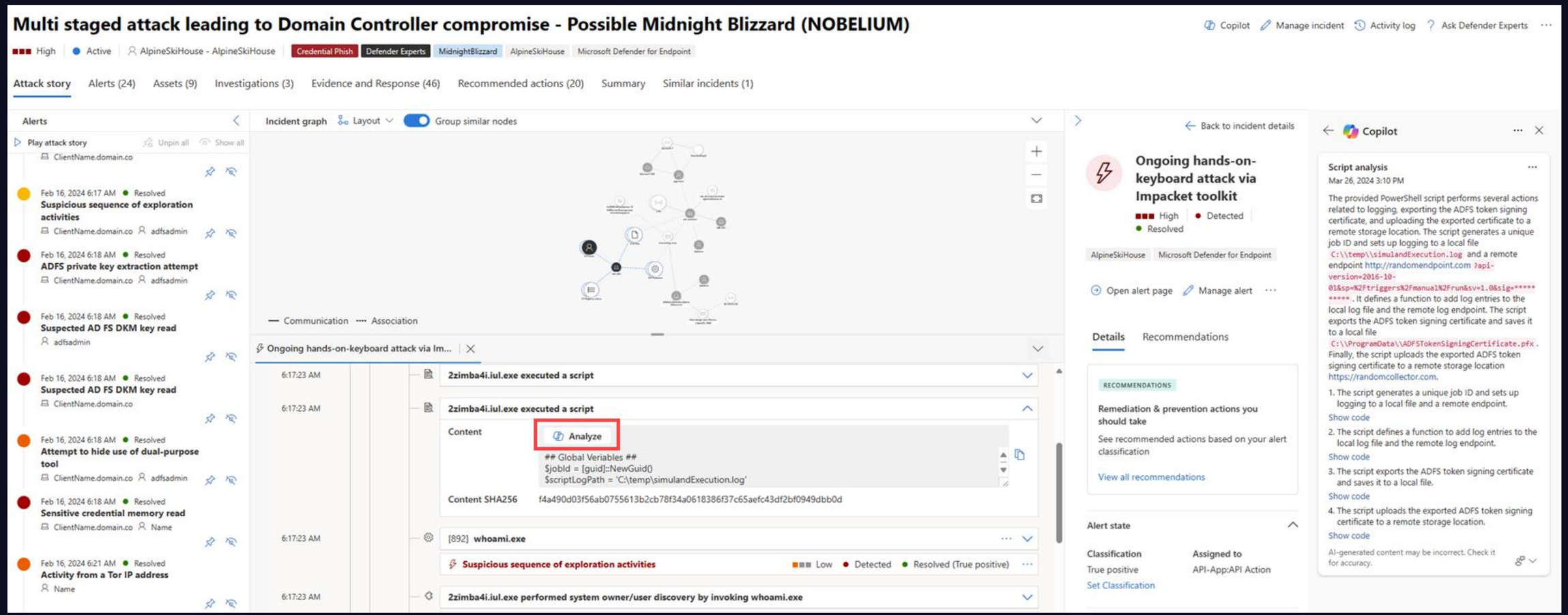
Szolgáltatásként nyújtott AI rendszerek integrációja SIEM rendszerekkel

Piaci incidenskezelési döntéstámogató rendszerek.

# Triázs és Döntéstámogatás

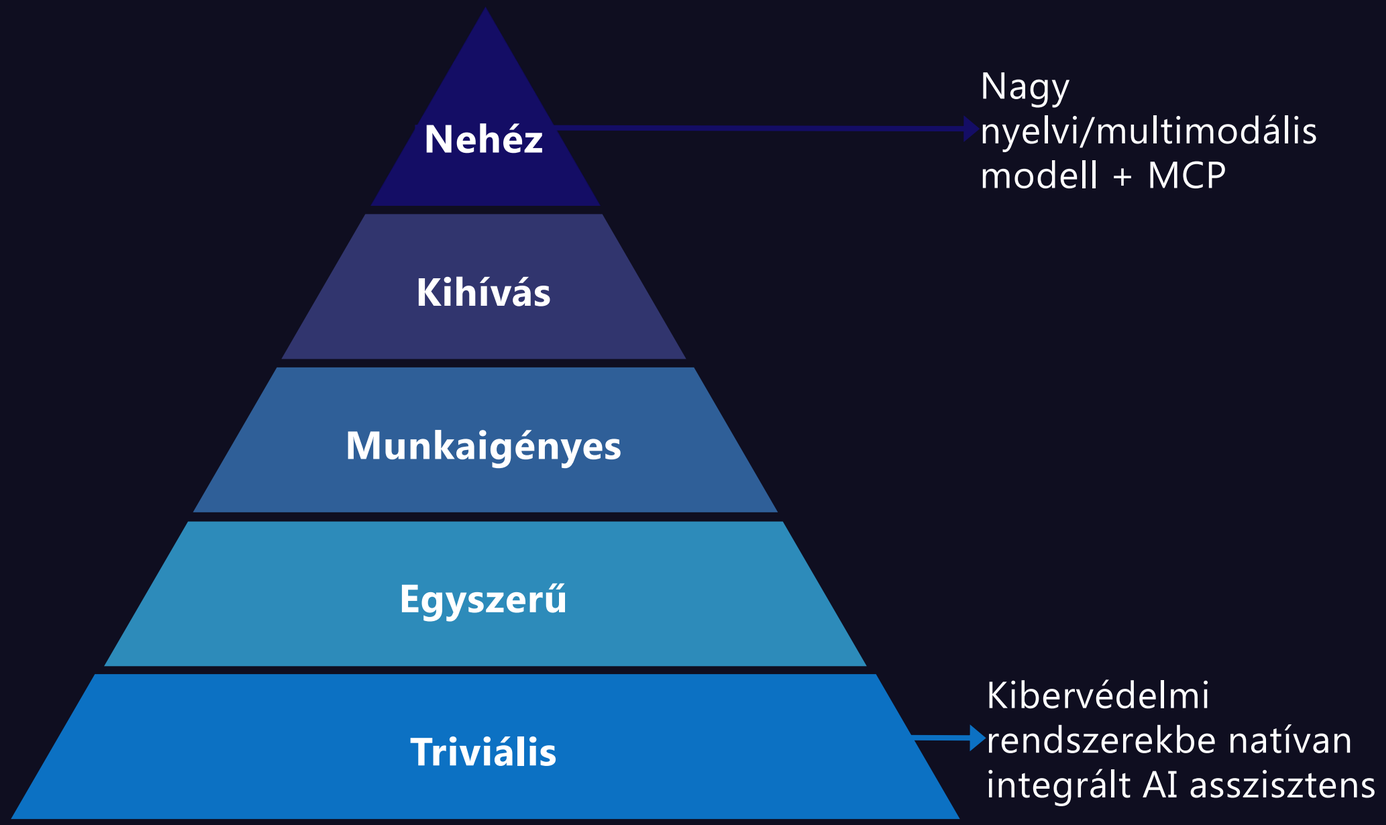
## AI munkafolyamatok

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

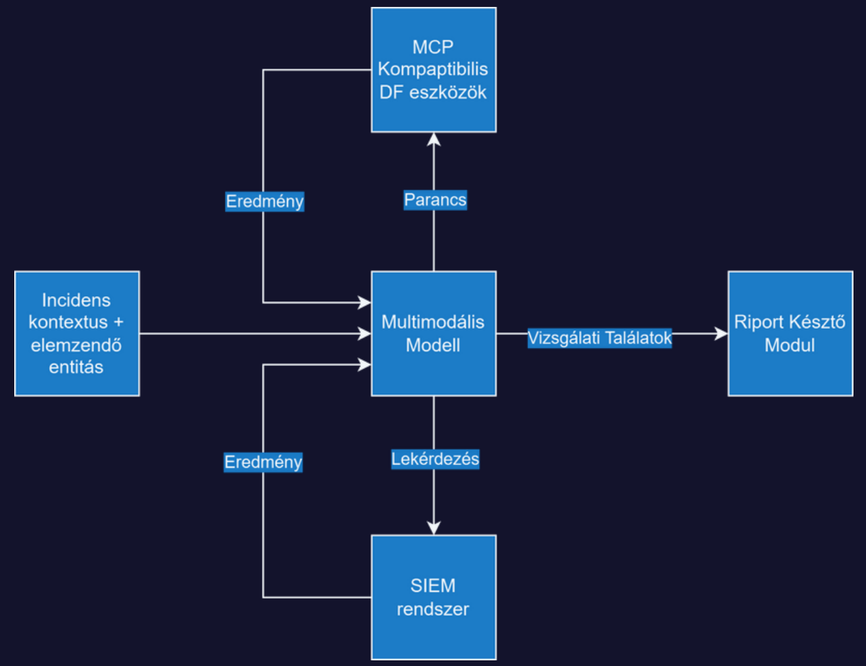


# Digital Forensics
## AI munkafolyamatok

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

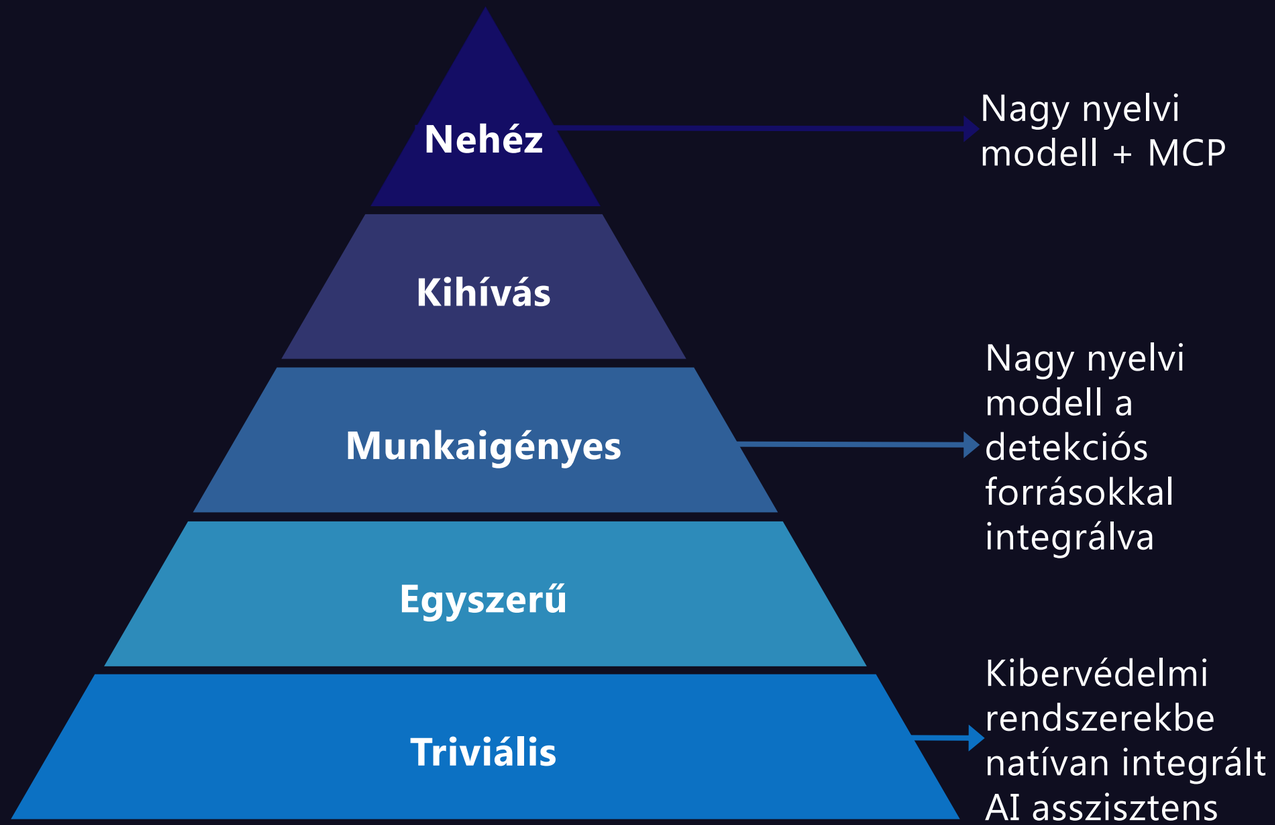


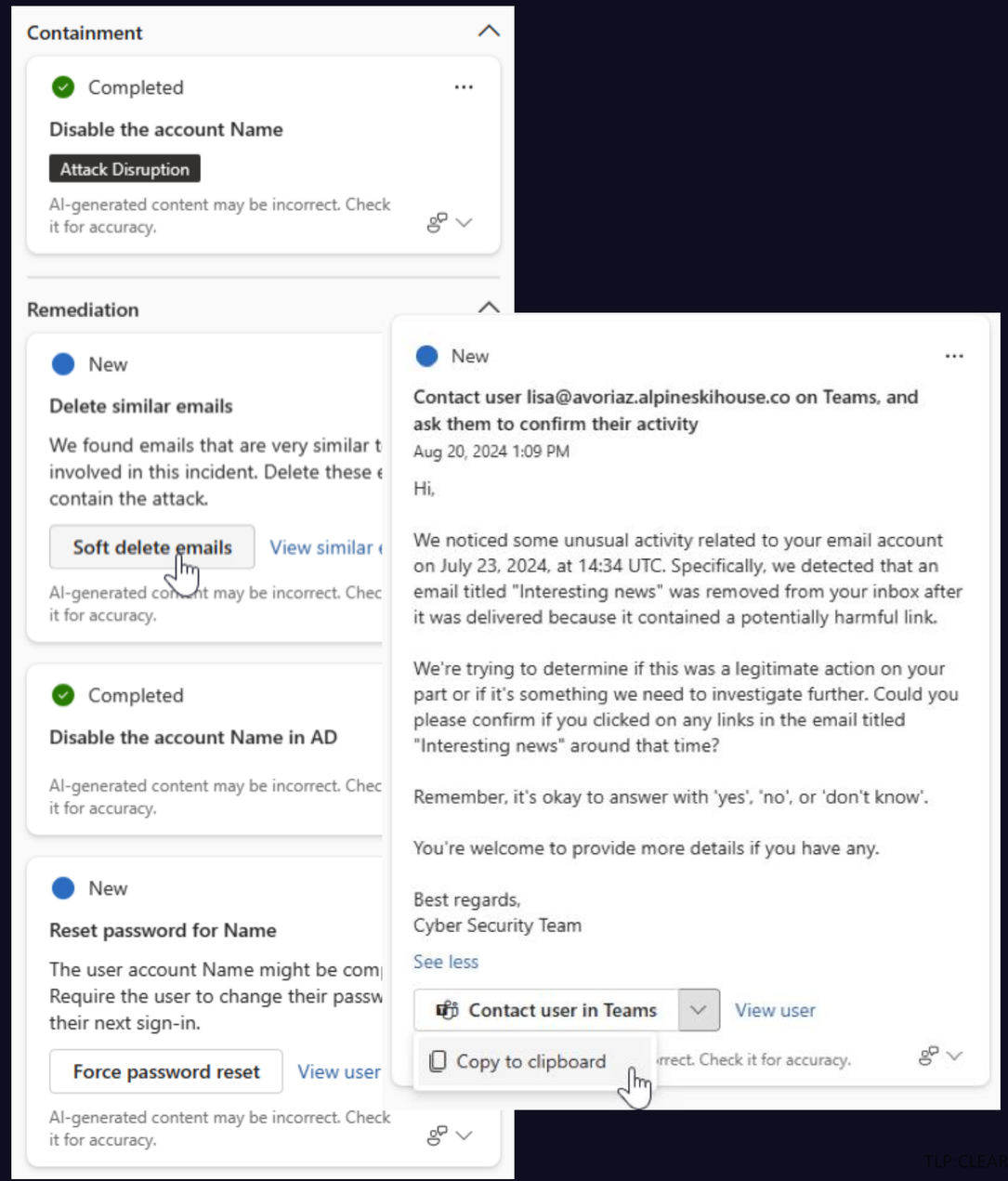

Egy kellően kifinomult modell képes lehet akár a teljes vizsgálati folyamatot véghez vinni.



# Incidenskezelés
## AI munkafolyamatok

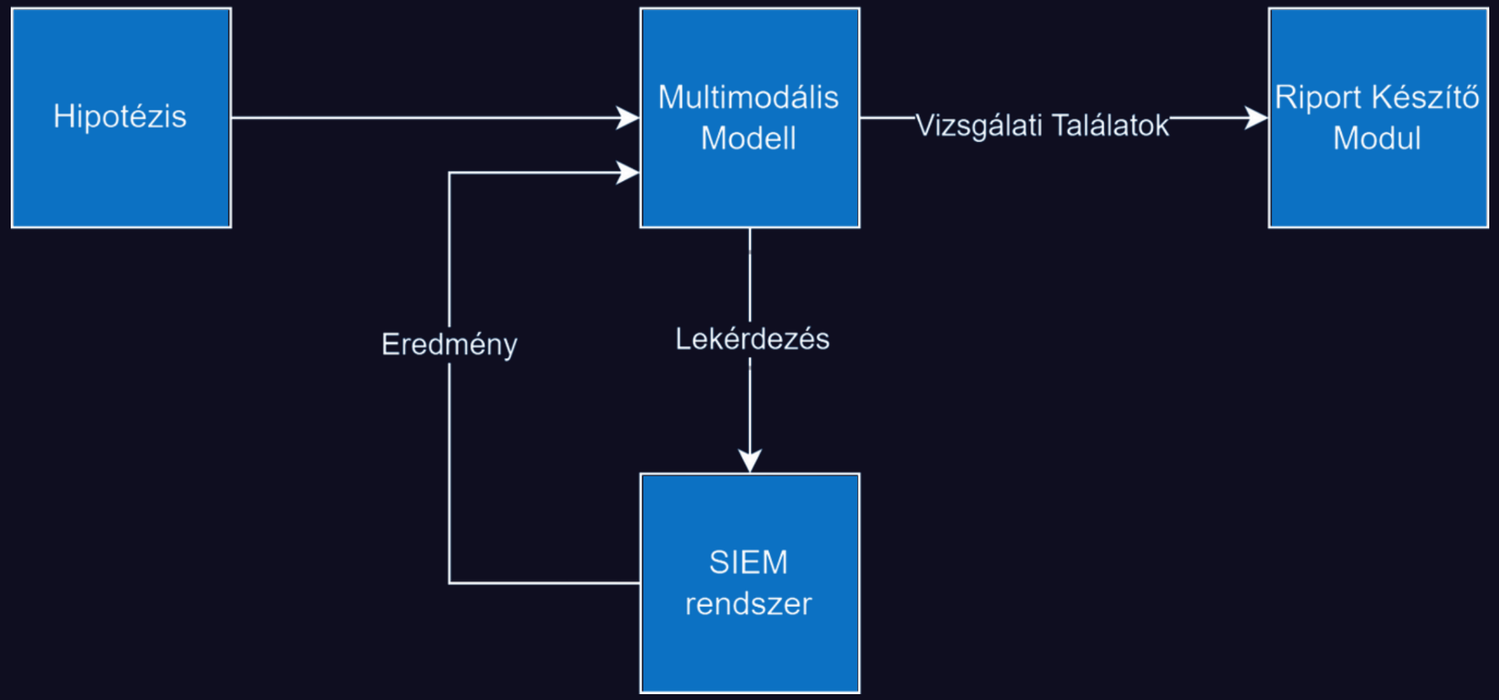
Az AI segíthet a riasztás kontextusának elemzésével beazonosítani a szükséges válaszlépéseket, vagy akár automatizálva véghez is viheti azokat.



# 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.



BLACK CELL
Protecting critical infrastructures

# Köszönöm a figyelmet!

www.blackcell.io