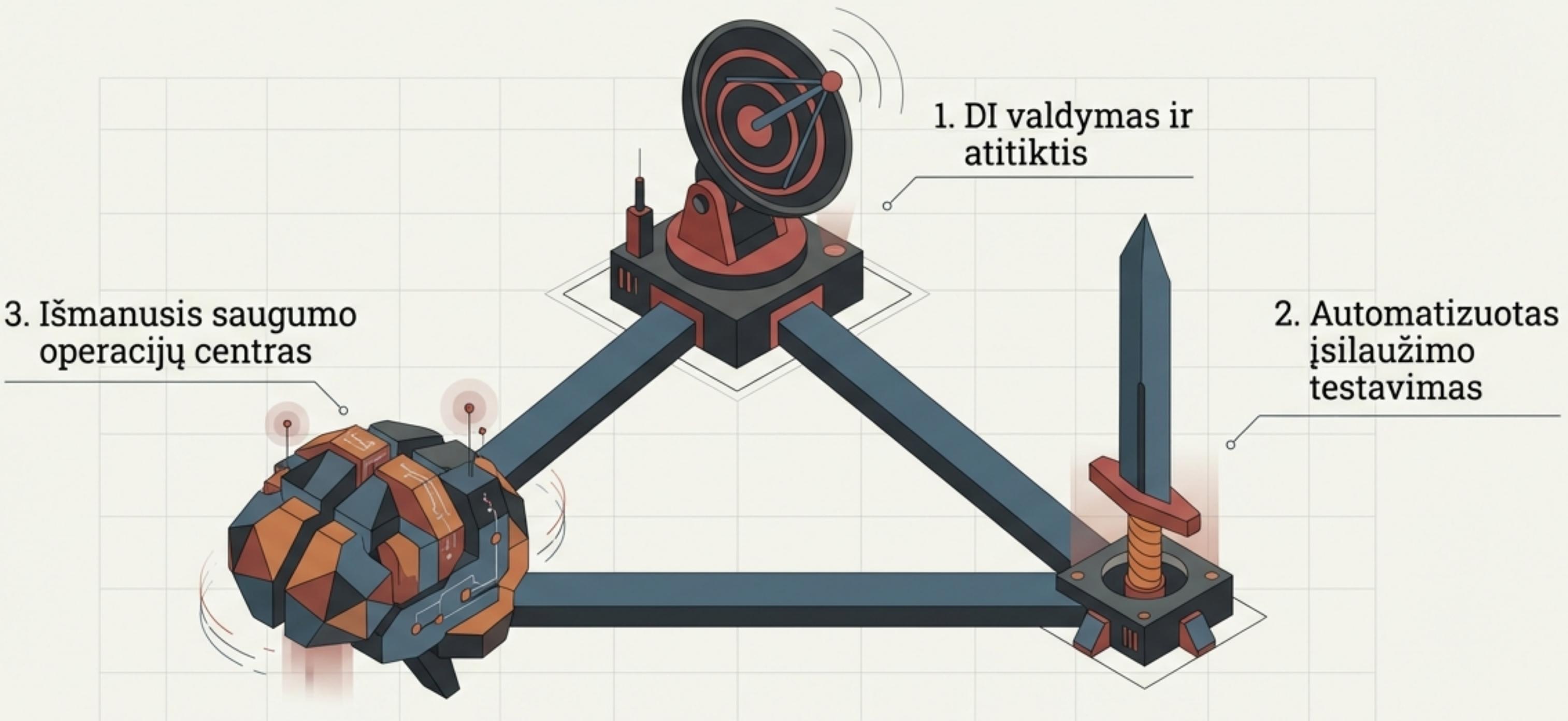


Autonominės kibernetinės gynybos trejybė

Perejimas nuo reaktyvios gynybos prie prognozuojamo atsparumo.



STRATEGIJA NUOLAT KINTANČIAI SKAITMENINEI ERDVEI

Kodėl senieji gynybos metodai nebeveikia?

Skaitmeninė erdvė kinta mašininiu greičiu, tačiau gynyba vis dar priklauso nuo žmogaus reakcijos laiko.



Momentiniai patikrinimai

Saugumas vertinamas tik audito metu, paliekant didžiulus „aklus“ laiko tarpus.



Rankinis darbas

Priklausomybė nuo skaičiuoklių (spreadsheets) ir lėtėjančių procesų.

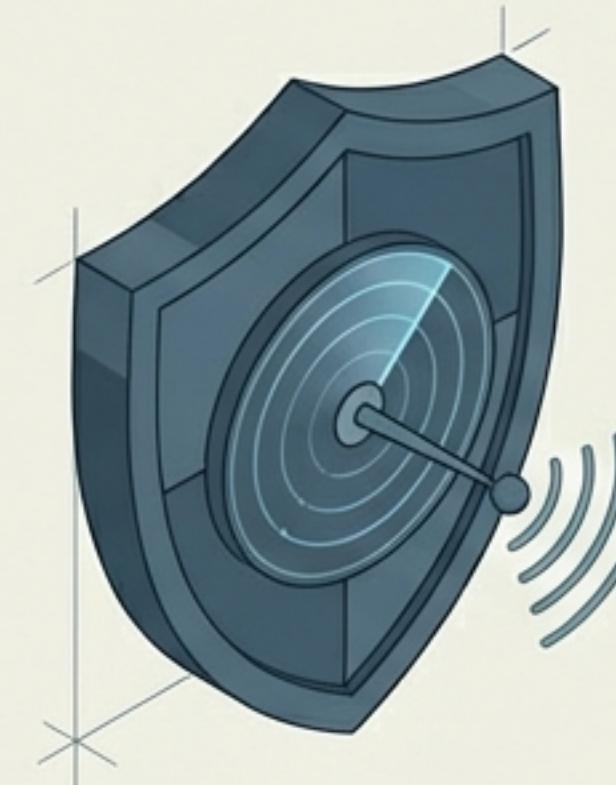


Įspėjimų nuovargis

Analitikai skėsta informaciniame triukšme ir klaidinguose pavojaus signaluose.

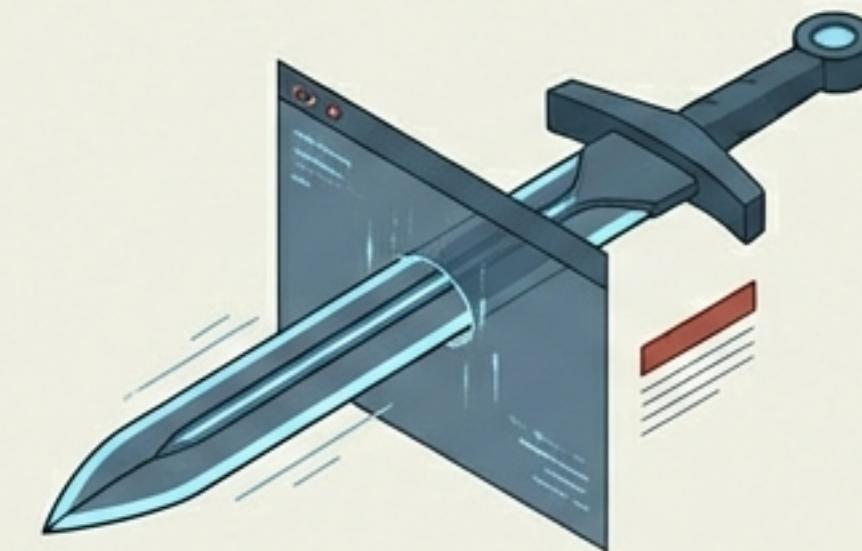
Trys autonominės sistemos ramsčiai

Visos inovacijos veikia kaip vieninga dinamiška apsaugos sistema, gebanti veikti realiuoju laiku be nuolatinio žmogaus įsikišimo.



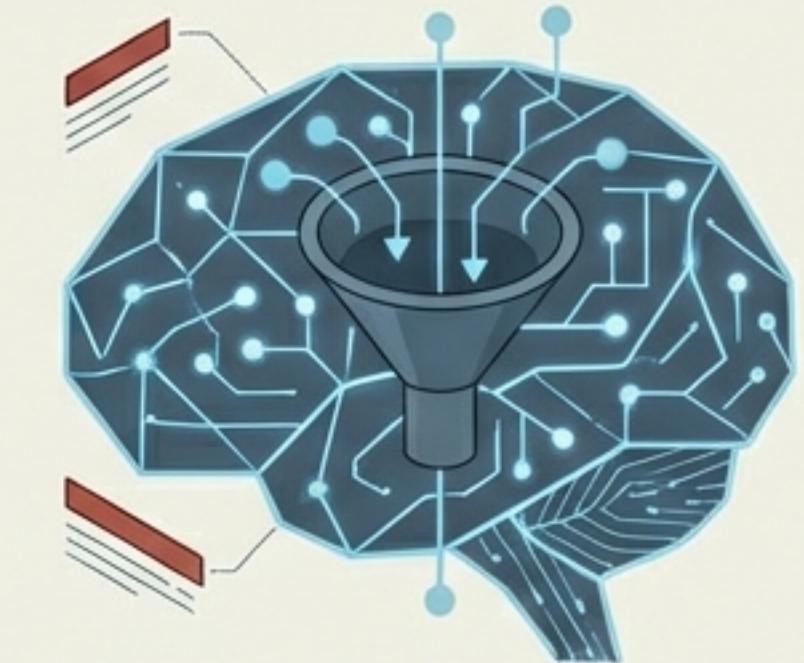
DI GRC (Skydas/Radaras)

Nepertraukiamas skaitmeninis stebėjimas. Pakeičia létus rankinius auditus.



DI Pentesting (Kardas)

Automatizuotas įsilaužimo testavimas. Nuolatinė programišių atakų imitacija.

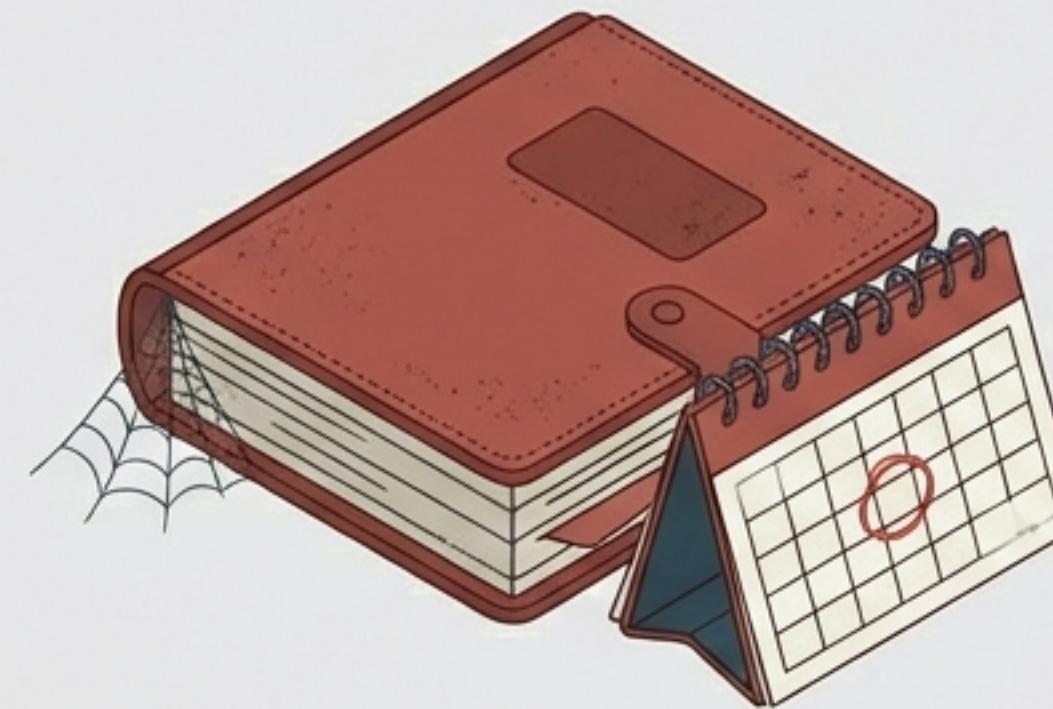


DI SOC (Smegenys)

Išmanusis operacijų centras. Savarankiškas reagavimas ir klaidingų signalų filtravimas.

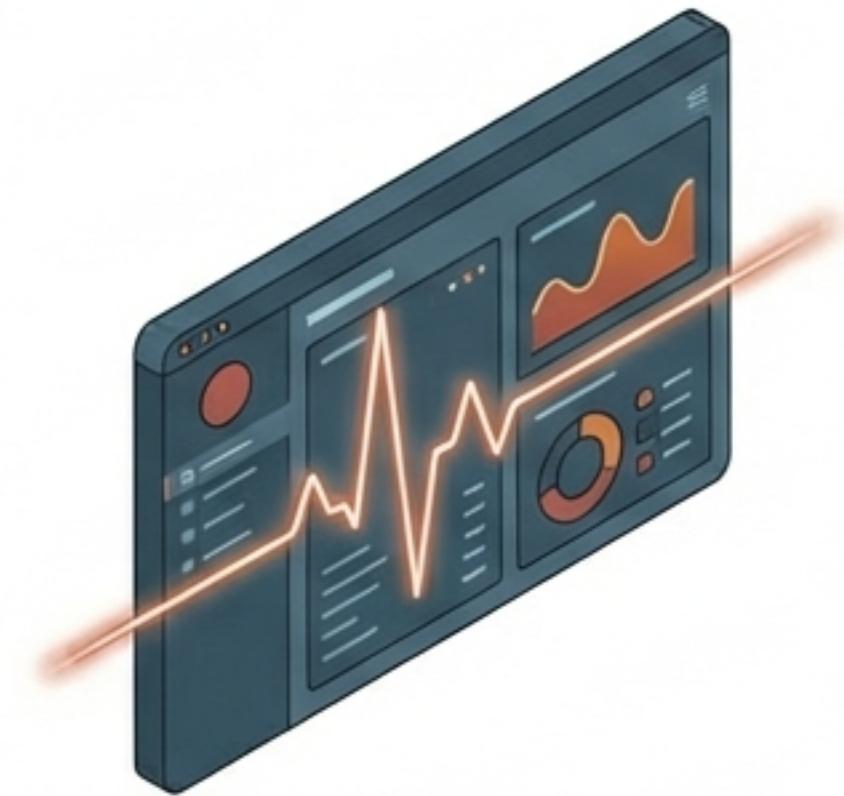
DI GRC: Nuo „audito sezono“ prie nuolatinės stebėsenos

TADA (Tradicinis būdas)



- „Laiko momento“ (Point-in-time) nuotrauka
- Pasenusios taisykłės
- Reaktyvus dokumentų pildymas

DABAR (Autonominis būdas)



- 24/7 atitikties matomumas
- Realaus laiko informacijos suvestinės (dashboards)
- Proaktyvus valdymas

Atitiktis neturi būti vienkartinis įvykis – tai turi būti nuolatinė organizacijos būsena.

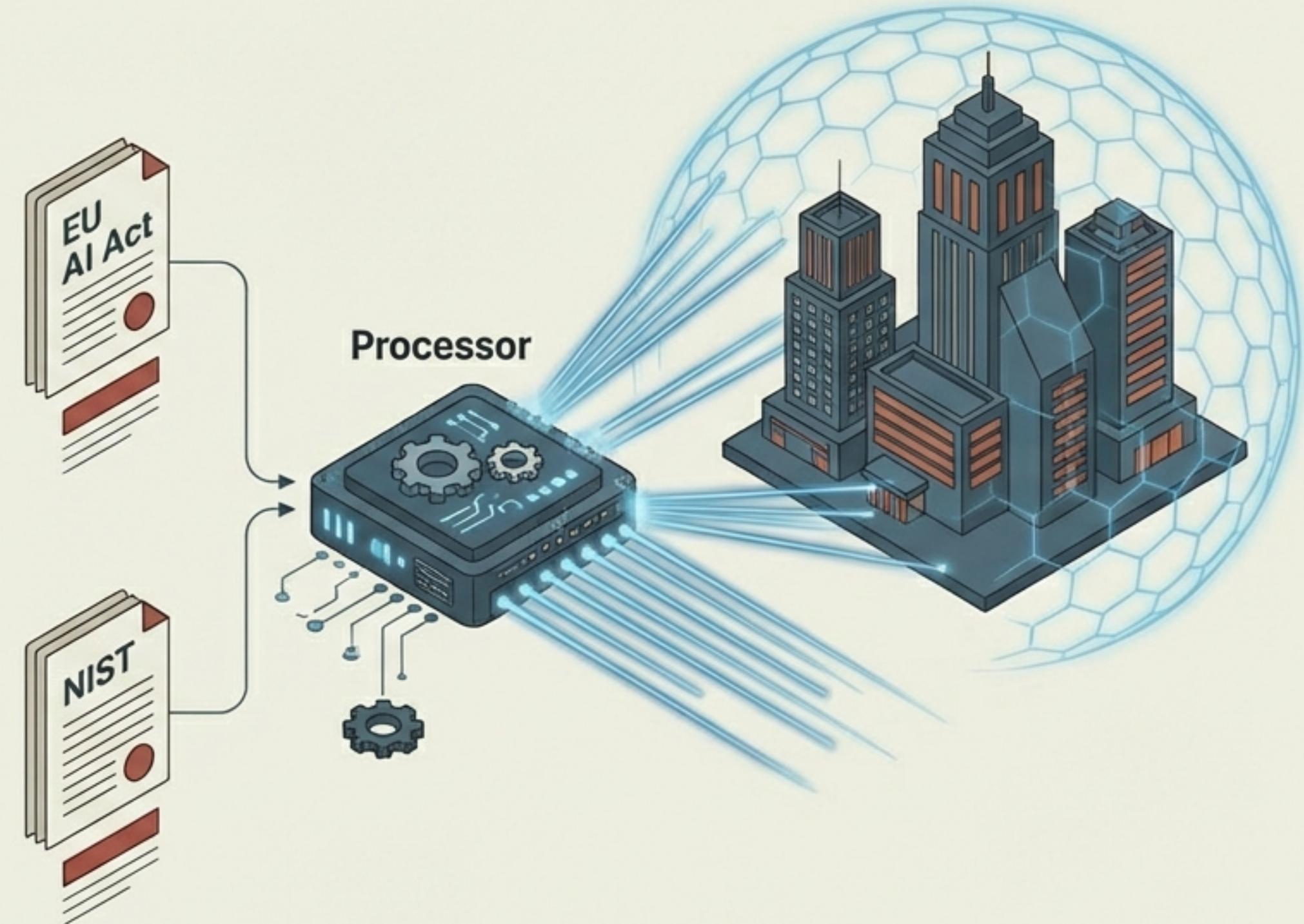
Kaip veikia išmanioji valdysena?

Automatizuotas taisyklių susiejimas

DI akimirksniu nuskaito naujus reglamentus (pvz., ES DI aktą ar NIST standartus) ir automatiškai susieja juos su jūsų kontrolės mechanizmais.

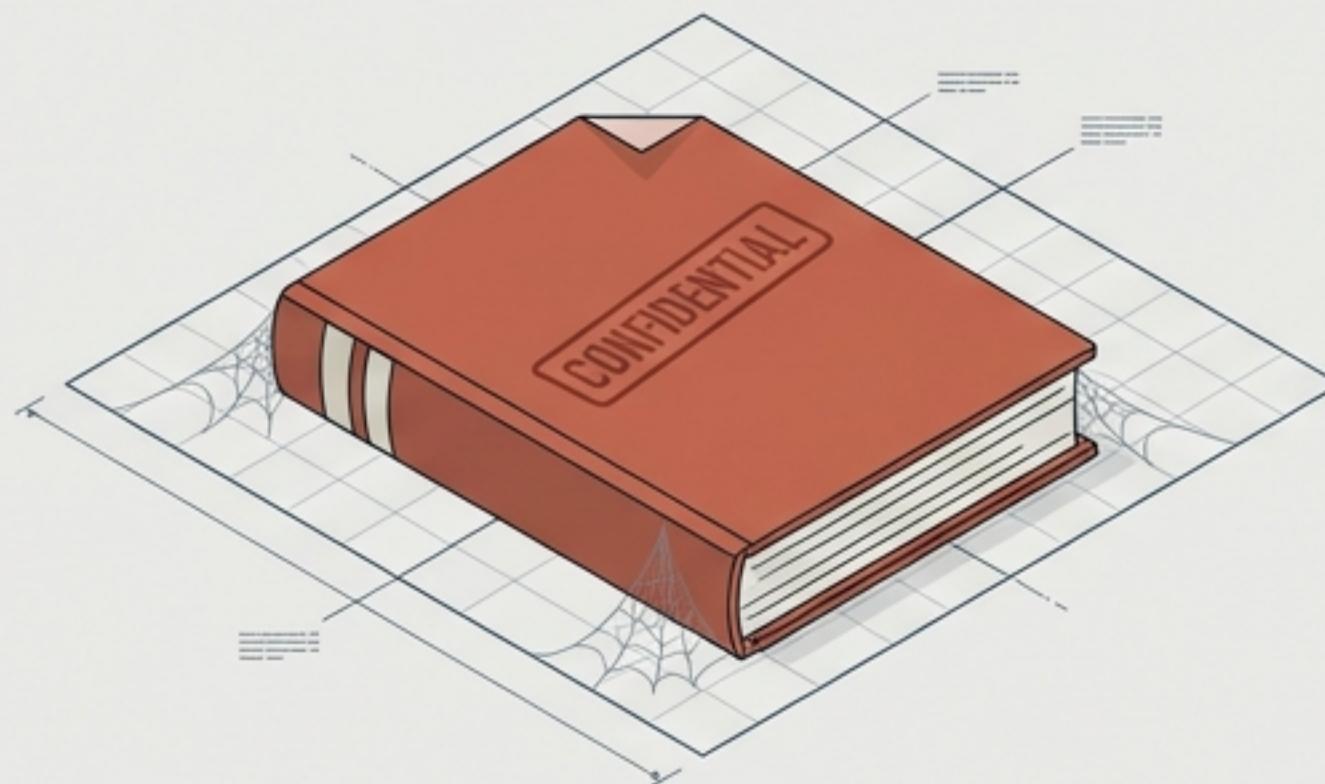
Prognozuojamas rizikos vertinimas

Naudojant vidinius duomenis, sistema prognozuoja, kurie verslo padaliniai turi didžiausią tikimybę patirti pažeidimą, dar prieš jam įvykstant.



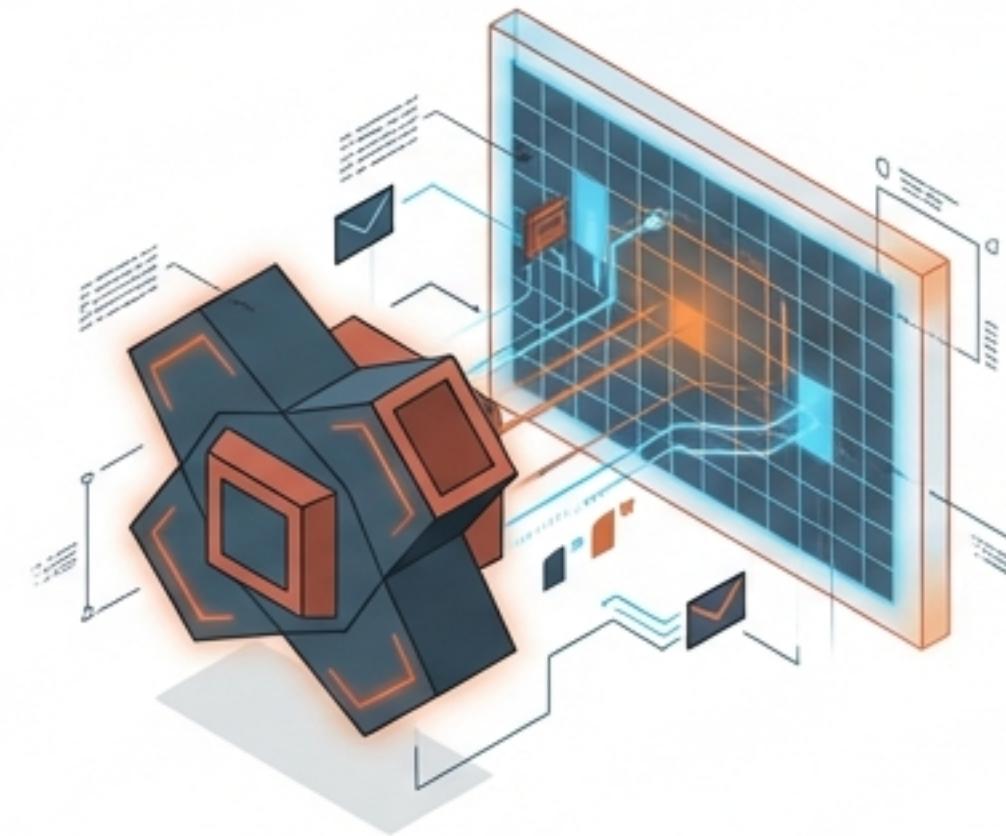
DI Pentesting: Nuo statinių ataskaitų prie dinamiško puolimo

TADA (Tradicinis būdas)



- Brangūs, lėti metiniai skenavimai
- Fiksuojama tik tos dienos saugumo būklė

DABAR (Autonominis būdas)

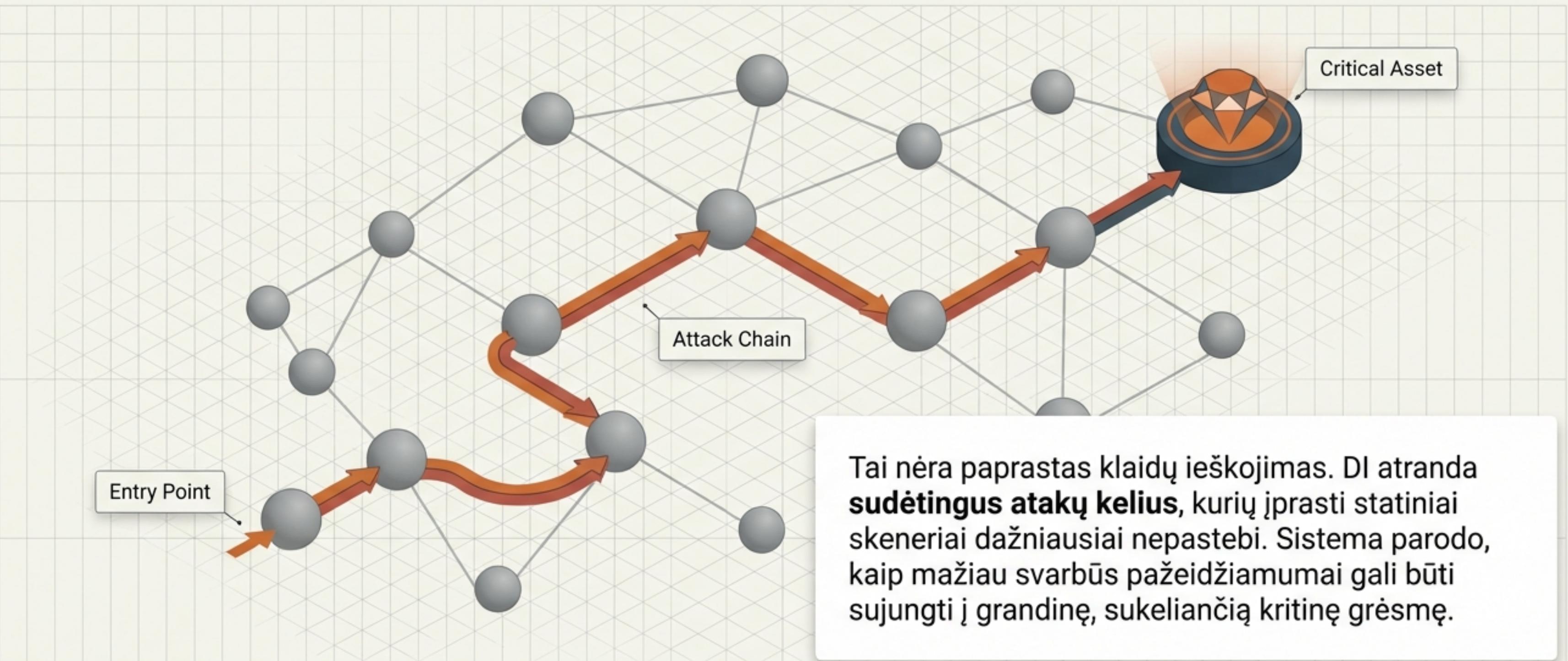


- Nuolatinis priešpriešinis testavimas (Continuous Adversarial Testing)
- Vyksta 24/7

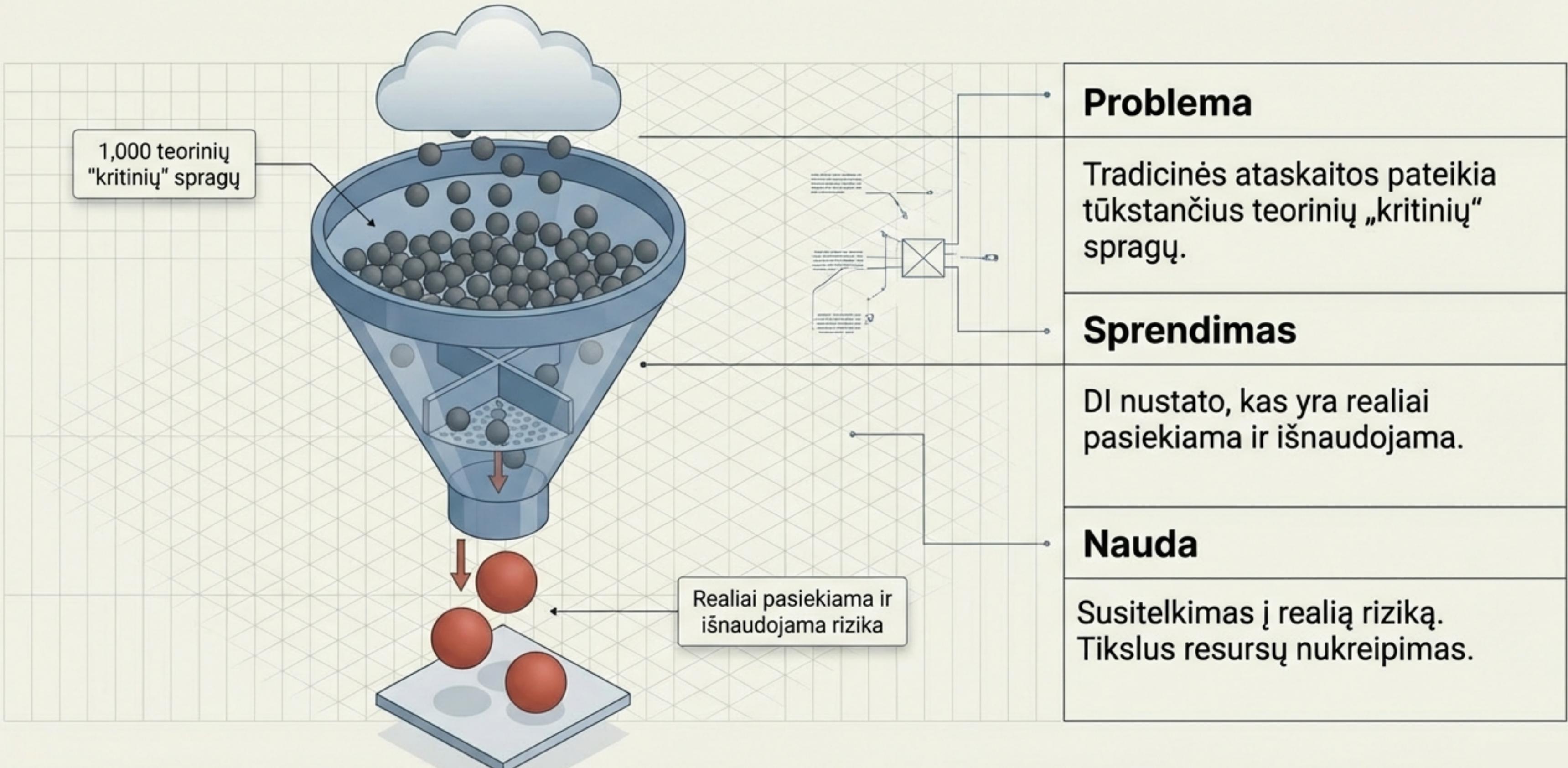
Hakeriai dirba be išeiginiu, todėl jūsų atsparumo testavimas taip pat negali sustoti.

Automatizuota išnaudojimo simuliacija

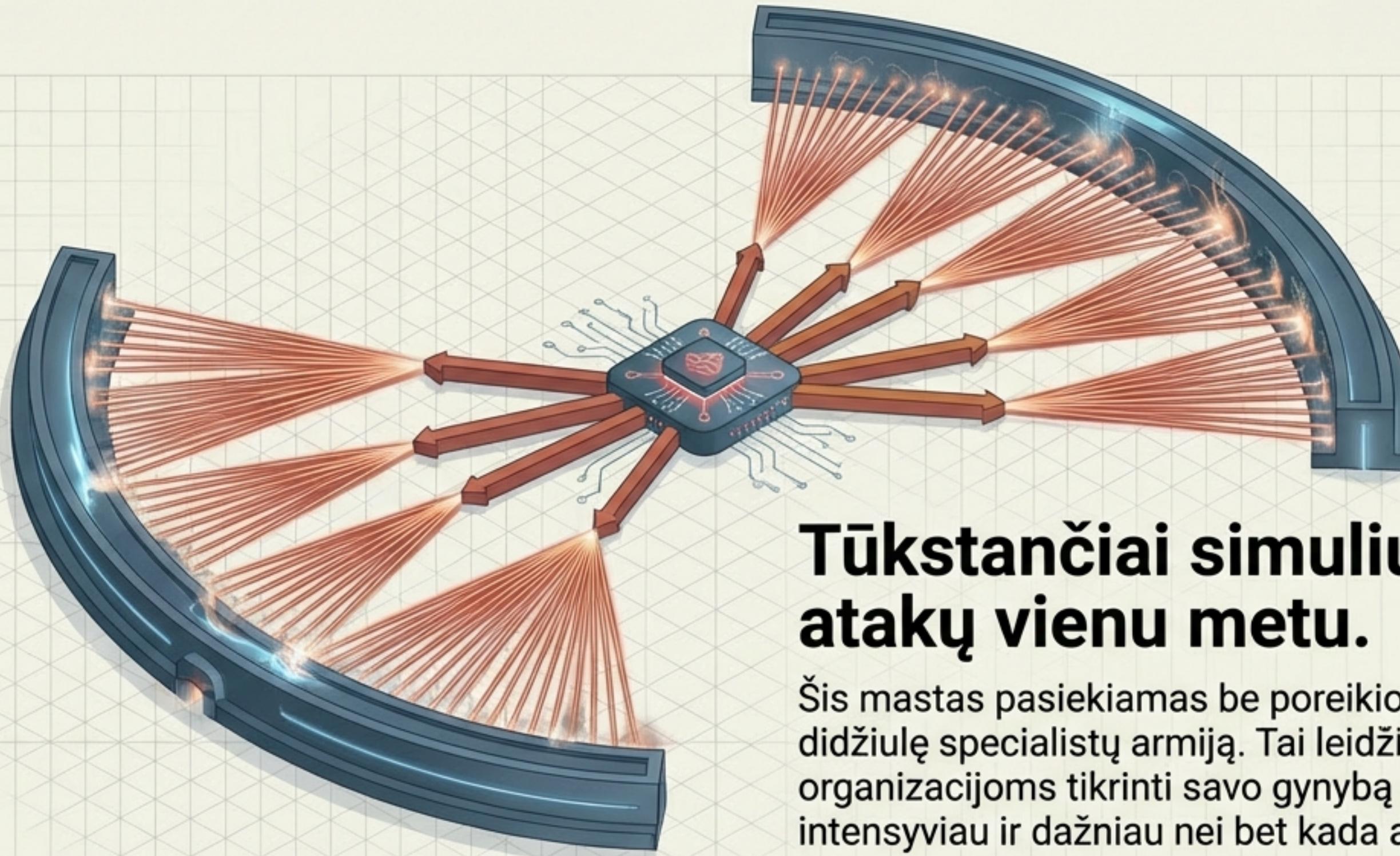
DI „agentai“ geba emuliuoti realaus hakerio elgseną.



Išmanus pažeidžiamumų prioritetizavimas



„Red Teaming“ operacijos dideliu mastu

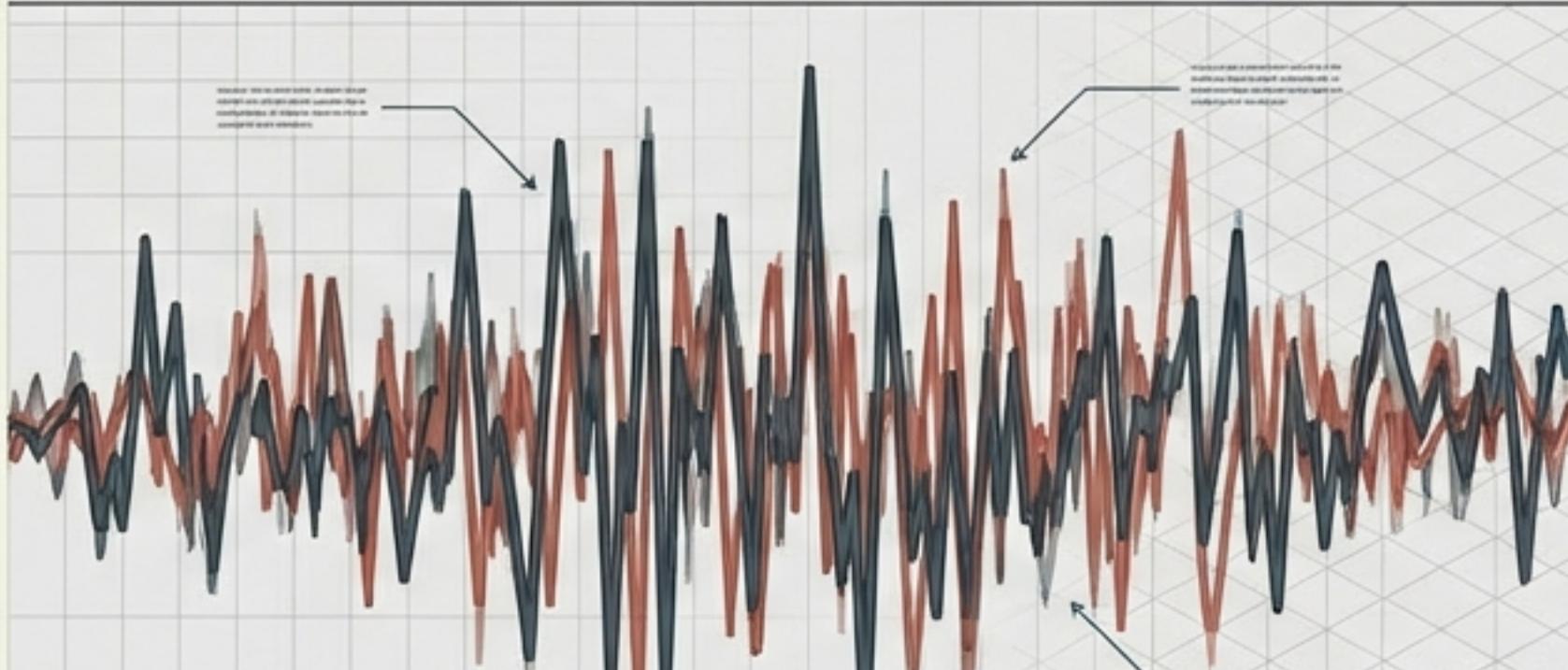


**Tūkstančiai simuliuotų
atakų vienu metu.**

Šis mastas pasiekiamas be poreikio samdyti didžiulę specialistų armiją. Tai leidžia organizacijoms tikrinti savo gynybą daug intensyviau ir dažniau nei bet kada anksčiau.

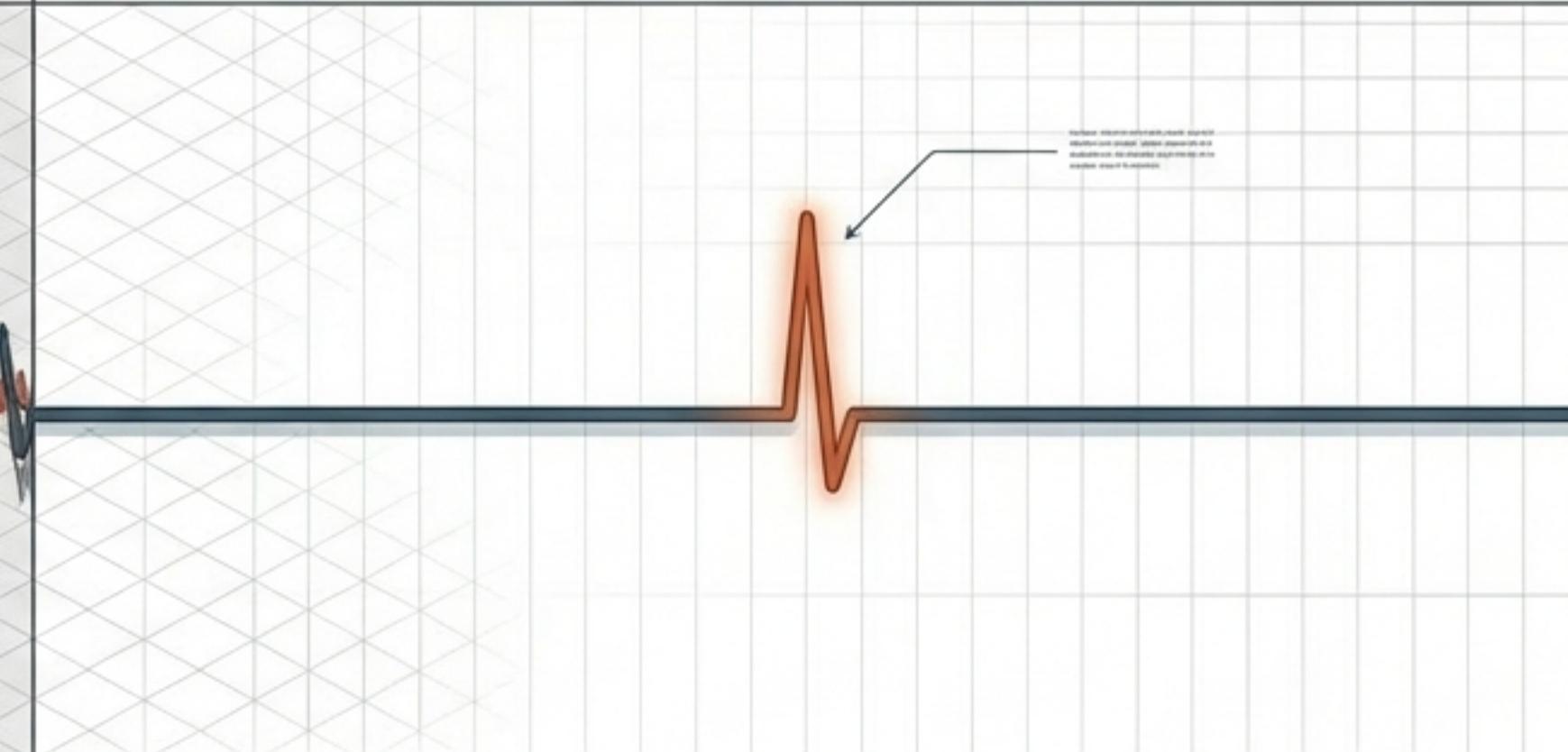
DI SOC: Pabaiga įspėjimų nuovargiui

TADA (Tradicinis būdas)



Analitikai apkrauti tūkstančiais pranešimų
Lėtas reagavimas
Informacinis triukšmas

DABAR (Autonominis būdas)



Automatizuotas problemų sprendimas
Dėmesys tik esminiamams signalams

Kai viskas yra „skubu“, niekas nėra skubu. DI sugrąžina fokusą.

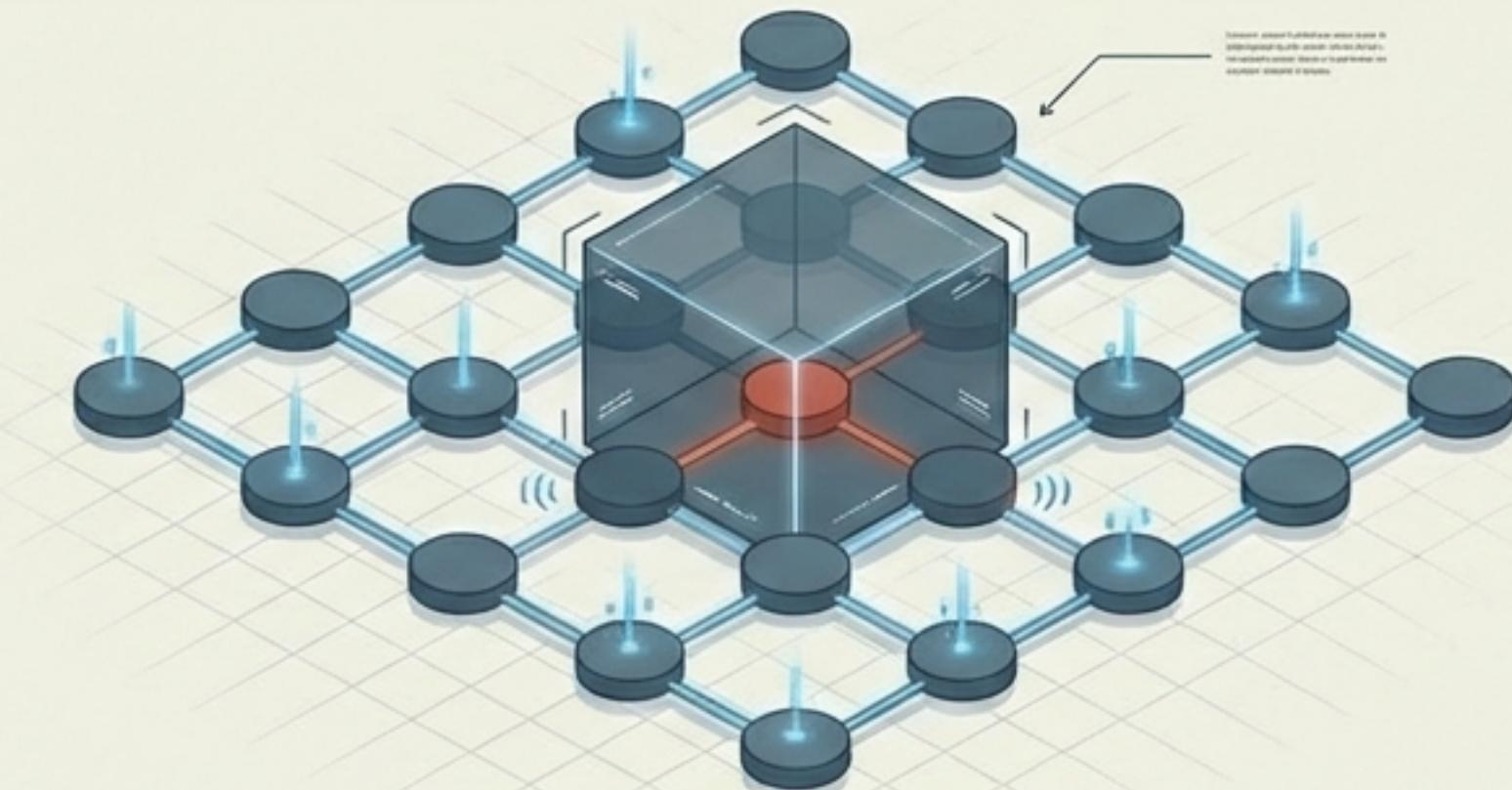
Išmaniojo reagavimo mechanizmas

1. Triukšmo filtravimas



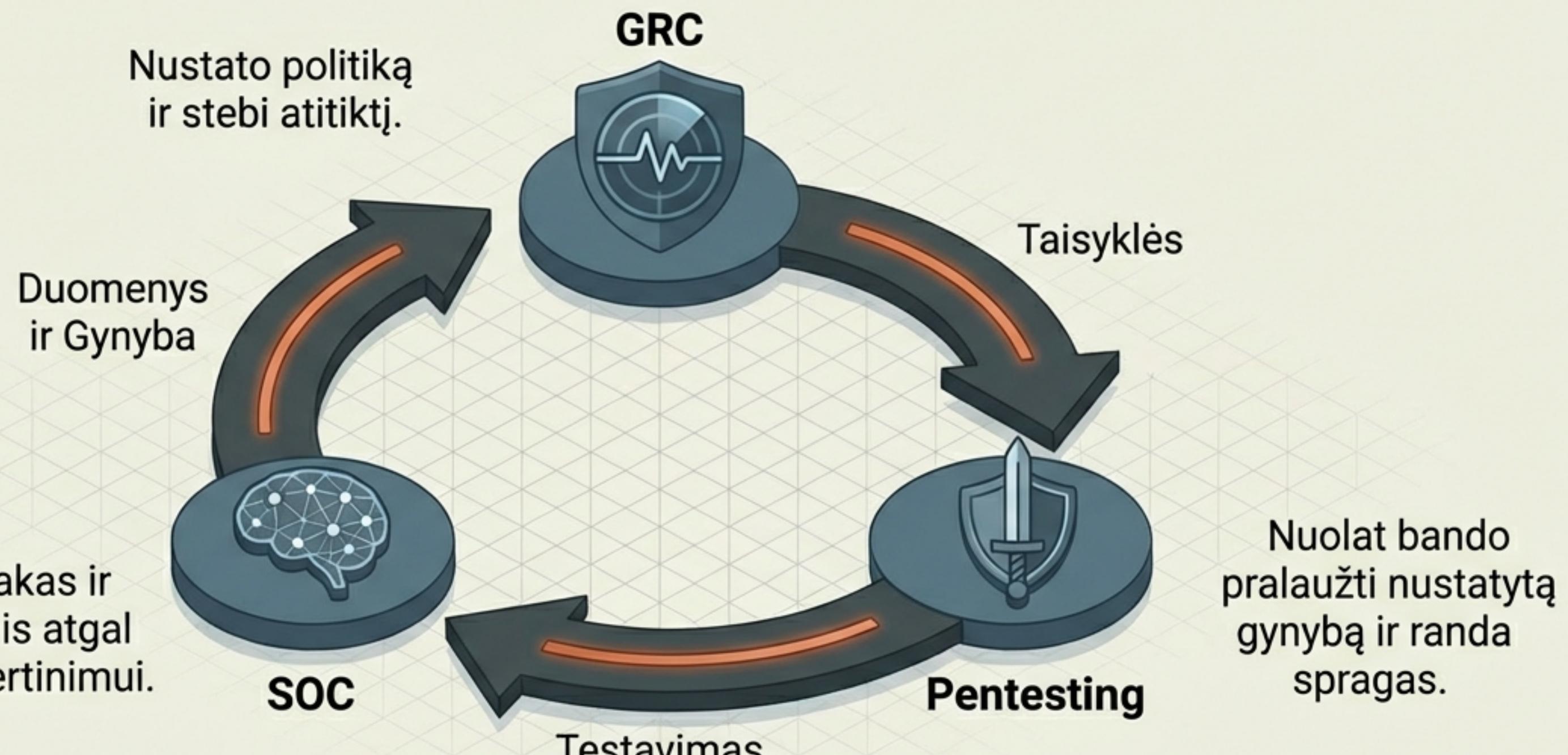
DI eliminuoja **95% klaidingų pavojaus signalų** (false positives), palikdamas tik tikrąsias grėsmes.

2. Autonominis atsakas



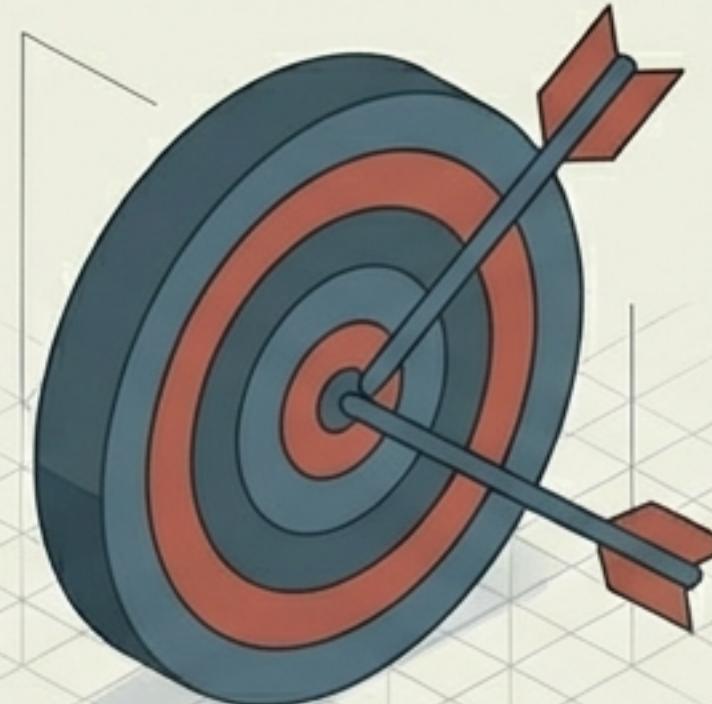
Savarankiški reagavimo veiksmai realiu laiku. Sistema „gydosi“ pati, izoliuodama grėsmes be žmogaus delsimo.

Sinergija: Kaip veikia visa trejybė?



Duomenų srautas tarp komponentų sukuria savaimė besimokančią sistemą.

Pagrindinė nauda organizacijai



Fokusas į realią riziką

Atmetamos teorinės grėsmės, sprendžiamos tik realiai išnaudojamos spragos.



Efektyvus resursų paskirstymas

Saugumo komandos dirba su esminiais signalais, o ne informaciniu triukšmu.

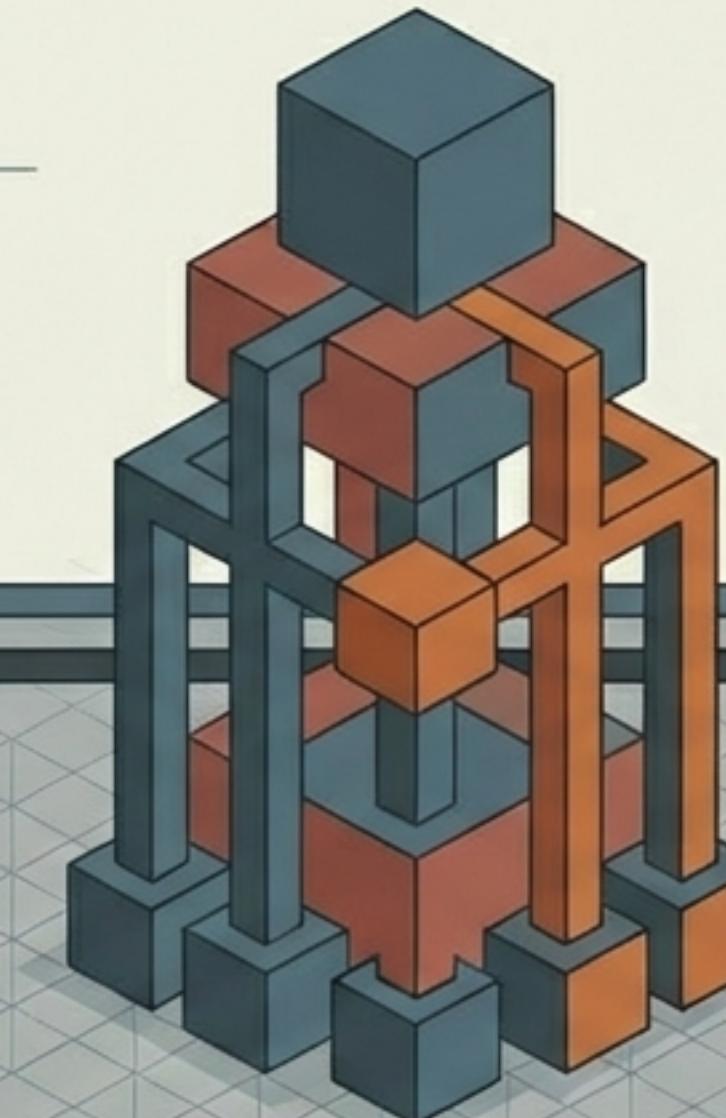


Proaktyvus saugumas

Spragos užtaisomos dar prieš piktavaliams spėjant jomis pasinaudoti.

Ateities perspektyva: Prognozuojamas atsparumas

Tai nėra tik nauji įrankiai –
tai strateginis pokytis.



Organizacijos privalo pereiti nuo reaktyvaus problemų sprendimo prie modelio, kuris numato ir neutralizuja grėsmes automatiškai. Tai vienintelis būdas išlikti saugiems nuolat kintančioje skaitmeninėje erdvėje.

Priimkite autonominę ateitį.

Gynyba mašininiu greičiu realaus pasaulio grėsmėms.

