TREĆA NACIONALNA KONFERENCIJA NKS-a

KIBERNETIČKA SIGURNOST

ČOVJEK U SREDIŠTU

NKS NACIONALNO KOORDINACIJSKO SREDIŠTE

CARNET

CyberArrange
RESILIENCE WITH EASE

Osiguravanje ažurnosti sigurnosnih treninga uporabom velikih jezičnih modela

dr. sc. Ivan Kovačević

Funded by the European Union
NextGenerationEU

Co-funded by the European Union

O predavaču

dr. sc. Ivan Kovačević

Istraživač, Direktor

- Doktorirao na Sveučilištu u Zagrebu, Fakultetu Elektrotehnike i Računarstva
- Dugogodišnje iskustvo istraživanja i razvoja u specifičnim područjima kibernetičke sigurnosti
- Sudjelovanje i vođenje u nizu istraživačkih projekata, veći broj radova objavljenih u međunarodnim časpisima i zbornicima konferencija
- Osnivač poduzeća CyberArrange Security Solutions; Technical Expert Cloud Solutions u AVL-AST

www.linkedin.com/in/ivan-kovačević-1ba42985

CyberArrange Security Solutions d.o.o.

CyberArrange
RESILIENCE WITH EASE

- Osnovana kao spin-off doktorskog istraživanja s FER-a
- Provedba R&D projekata u kibernetičkoj sigurnosti
- Istraživanje i razvoj u području primjene umjetne inteligencije u kibernetičkoj sigurnosti
- Razvoj inovativnih usluga u kibernetičkoj sigurnosti

www.cyberarrange.com

Statistike iz prakse (ENISA, SANS)

47%

organizacija u EU prijavljuje nedostatak kvalificiranih kibernetičkih stručnjaka

27%

organizacija pretrpilo napade izravno povezane s nedostatkom vještina zaposlenika

36%

organizacija nema budžeta za ulaganje u kibernetičku sigurnost

Alati su sve produktivniji i nametljiviji, a ljudi koji njima upravljaju sve ranjiviji

Kibernetičke prijetnje evoluiraju brže od programa obuke

Oslanjanje na alate često zapostavlja ulogu čovjeka koji drži središnju ulogu

Vježbe u kibernetičkoj sigurnosti

Tehničke vježbe

Simulirane računalne mreže i računala (kibernetički poligoni)

Vježbe za pojedinačne stručnjake

Vježbe crvenog i plavog tima (interaktivni kibernetički napadi)

Tehnički artefakti za forenziku

Analiza logova / zapisnika

Vježba oporavka sustava

Vježbe za netehničko osoblje

Minimum: phishing vježbe

Tabletop - “ratna soba” s upravom, pravnom službom, tehničkim managerima, PR-om i sl.

- Igranje uloga u scenariju napada s ozbiljnim posljedicama za poslovanje
- Vježba donošenja odluka pod pritiskom, vježba komunikacije
- Validacija i dorada politika i procedura, revizija tehničkih mjera

Motivacija: gdje postojeći pristupi zakazuju?

Postojeći pristup	Ključni nedostaci
Ručna priprema scenarija	Zahtijeva dugotrajan angažman stručnjaka, vremenski zahtjevan proces s velikim troškovima
Generički scenariji	Generička infrastruktura IT sustava i rizici često se bitno razlikuju u odnosu na ciljnu organizaciju
CTF platforme	Pojedinačni zadaci ne uče timsku obranu, već pojedine tehničke vještine; scenariji često nisu povezani s aktualnim rizicima organizacije

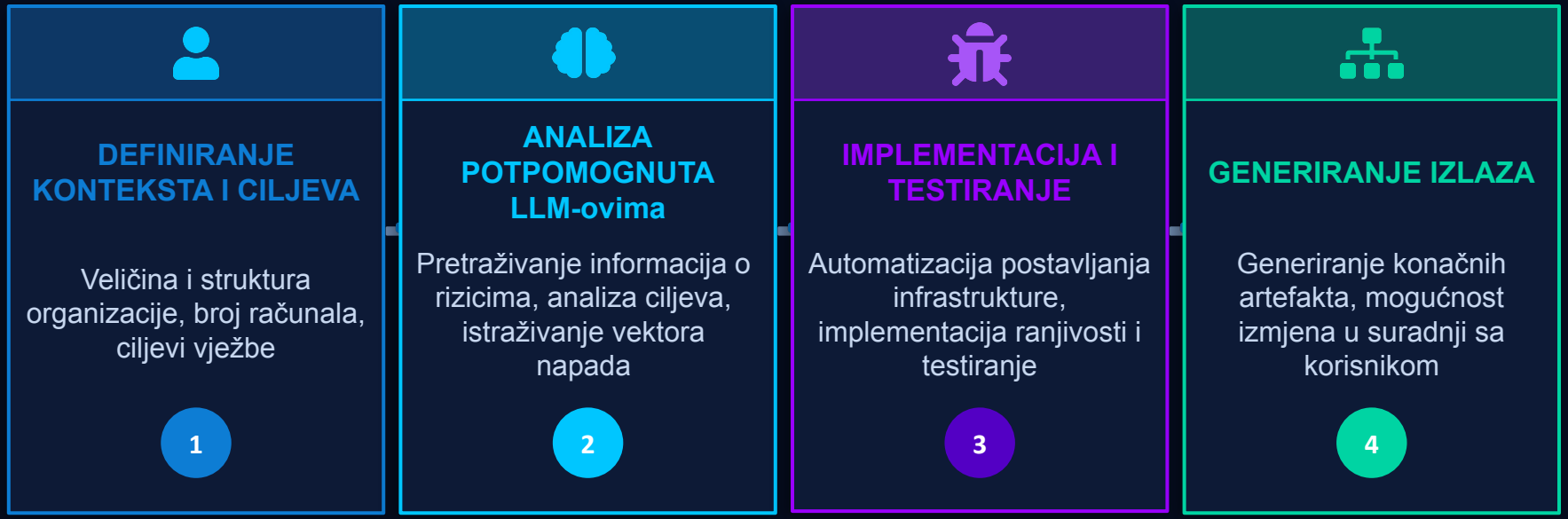
Ideja: Istražiti mogućnost primjene dubokih jezičnih modela (LLM-ova) u ovom području

Praktični problemi primjene LLM-ova

KLJUČNI RIZICI	METODE ZA UBLAŽAVANJE RIZIKA
LLM stvara nerealistične scenarije	Hibridni pristup - kombiniranje LLM-a s potpornim alatima i ekspertnim pravilima
Generirani scenariji nemaju smisla u kontekstu realnih potreba organizacije	Instruktor uvijek mora imati kontrolu - AI kao asistent, a ne kao zamjena za stručnjaka
Zastarjelo i nerelevantno znanje o ranjivostima i napadima	Automatizirana izgradnja i ažuriranje grafa znanja iz vanjskih izvora CTI
LLM generira tehnički neispravne scenarije koje nije moguće pokrenuti u poligonu	Uporaba fleksibilnih predložaka i automatskih testova, povratne informacije

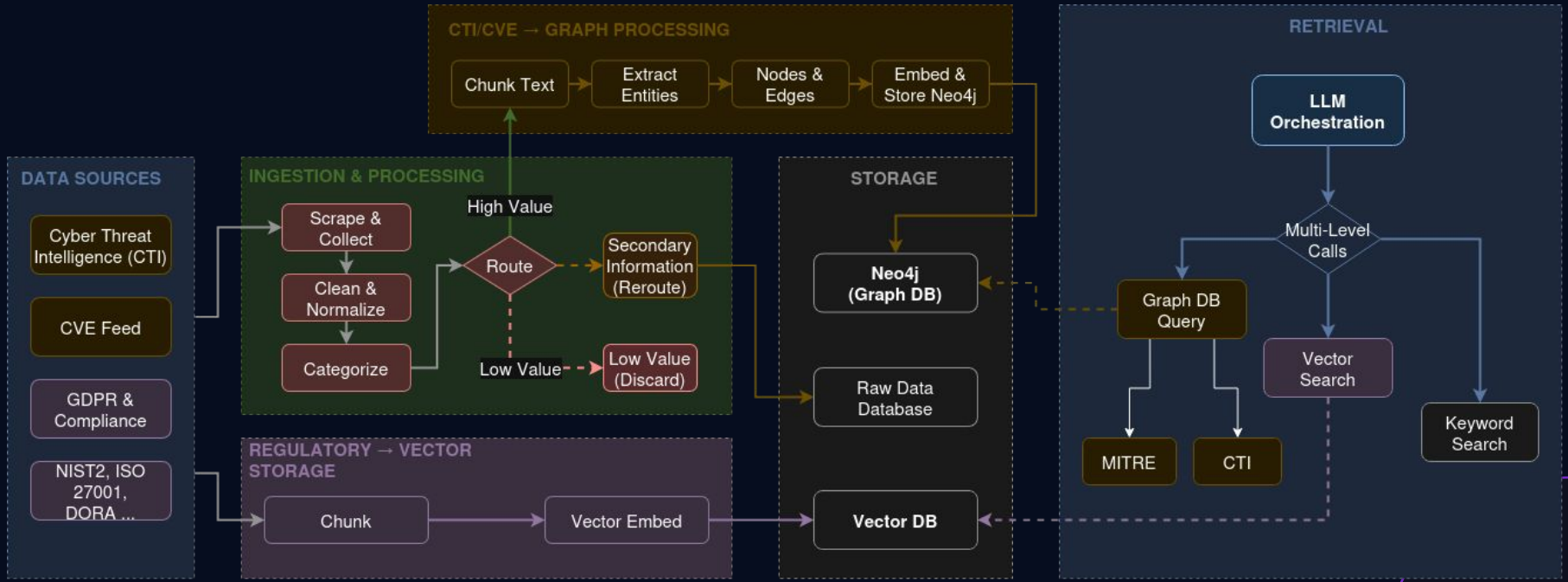
Transparentnost o rizicima ključna je za izgradnju povjerenja u sustav.

Razvijeni proces generiranja vježbe

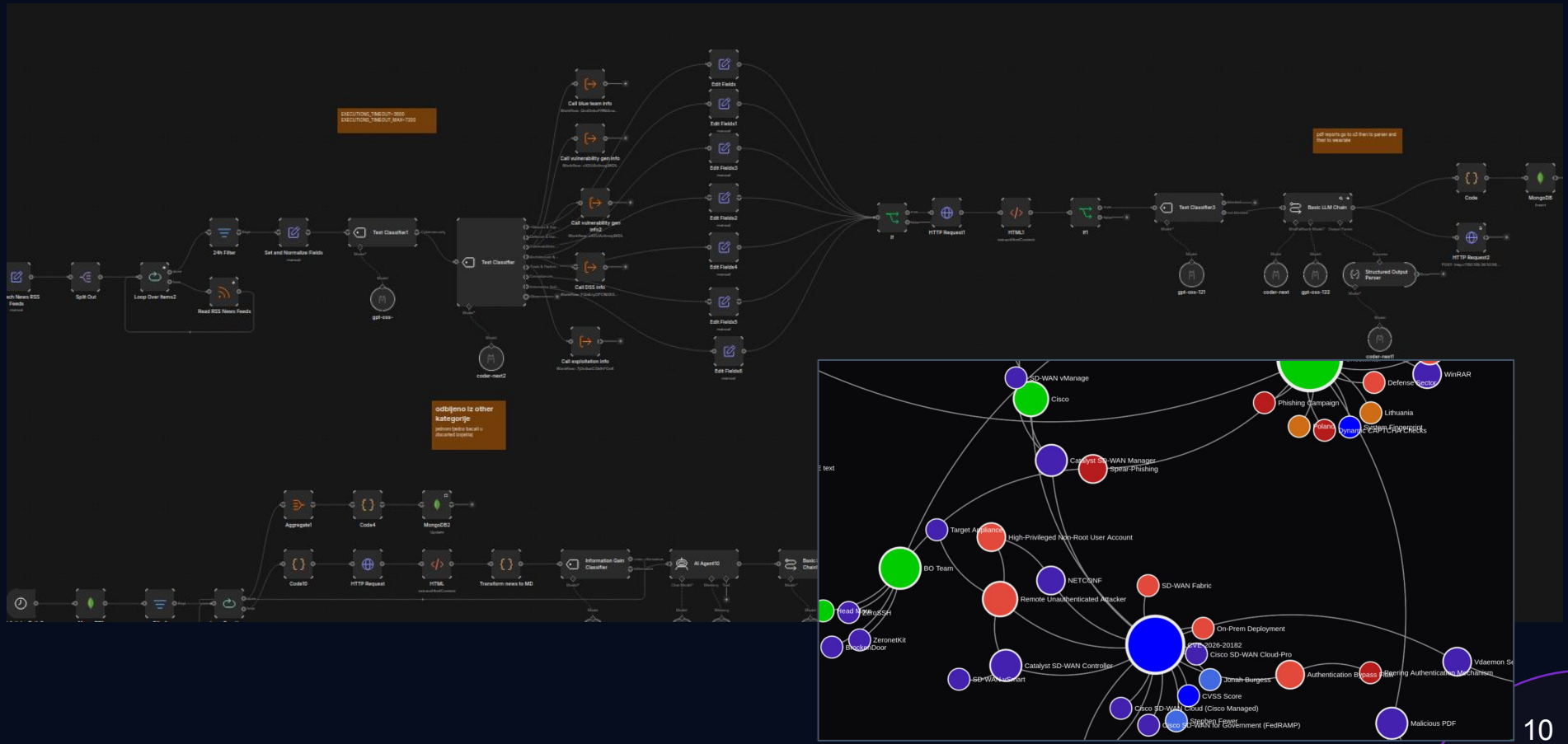


Ključne značajke: LLM orkestrira, a komponente osiguravaju ispravnost i tehničku izvedivost vježbe

Pregled prikupljanja i obrade podataka (1)



Pregled prikupljanja i obrade podataka (2)



Primjer generirane vježbe (1)

Definirao korisnik

- Mala IT firma
- Linux
- Javna web stranica
- Pohranjuju informacije o klijentima i izvorni kod
- Cilj: eksfiltracija podataka

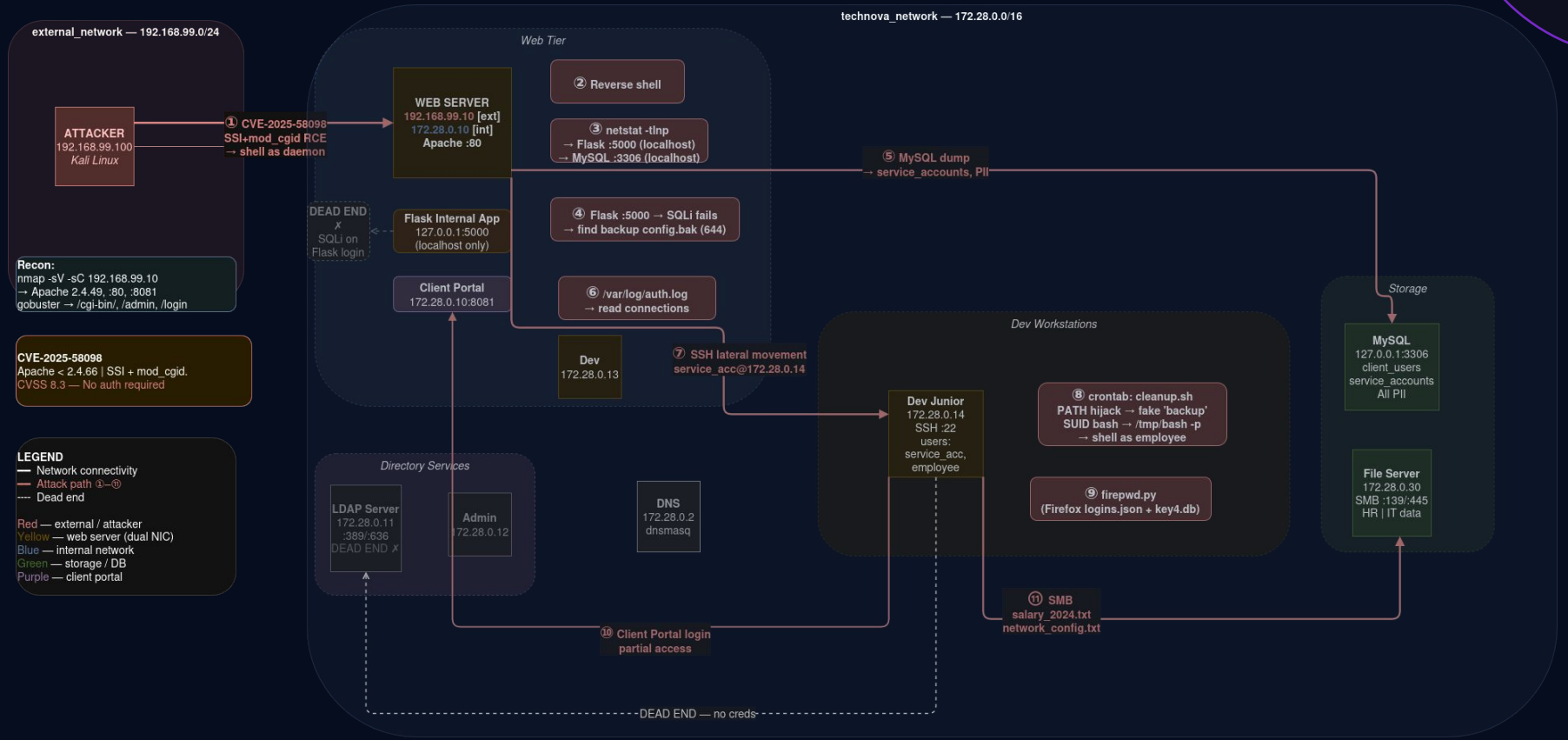
Definirano algoritmima temeljenim na pravilima

- Računalna infrastruktura
- Softverski paketi
- Pravila vatrozida
- Segmentacija mreže

Potpomognuto LLM-om

- Apache ranjivost kao inicijalni vektor
- Ranjivosti u konfiguraciji
- Dodatan server za pohranu podataka
- Detaljni korisnički podaci i prava

Primjer generirane vježbe (2)



Potencijalni prostor za suradnju u daljnjem istraživanju i razvoju

Dodatni izvori podataka o prijetnjama i ranjivostima

Dodatni izvori podataka o IT sustavima organizacija

Feedback na tehničke i tabletop vježbe

Reference i izvori

REGULATIVA

ENISA — NIS2 Directive Implementation Report (2024)	*enisa.europa.eu*
Europska komisija — Directive (EU) 2022/2555 (NIS2)	*eur-lex.europa.eu*
Zakon o kibernetičkoj sigurnosti RH	*narodne-novine.nn.hr*

INDUSTRIJA I ISTRAŽIVANJA

ENISA NIS Investments 2025	*enisa.europa.eu/publications*
SANS 2025 Security Awareness Report	*sans.org/mlp*
SANS 2026 Workforce Report	*sans.org/white-papers*

Kontakt:
ivan.kovacevic@cyberarrange.com

LinkedIn QR kod:

Hvala na pažnji.