Umetna inteligenca za kibernetsko varnost

Tomaž Klobučar, Ramanpreet Kaur, Dušan Gabrijelčič

9. 5. 2023

Vsebina

Umetna inteligenca za kibernetsko varnost

- Metode UI za kibernetsko varnost
- Stanje v Sloveniji
- Predlog usmeritev za razvoj

Ciljni raziskovalni projekt (oznaka V2-2147)

- Javna agencija za raziskovalno dejavnost Republike Slovenije
- Urad vlade Republike Slovenije za informacijsko varnost
- Trajanje: 1. 9. 2021 – 31. 8. 2022

arrs
JAVNA AGENCIJA ZA RAZISKOVALNO DEJAVNOST REPUBLIKE SLOVENIJE
REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE ZA INFORMACIJSKO VARNOST
URSIV

Primeri uporabe UI za kibernetsko varnost

Identifikacija

Primer uporabe UI	Sklepanje	Načrtovanje	Učenje	Komunikacija	Zaznavanje	Hibridno
Upravljanje seznama virov	1	0	4	1	0	2
Upravljanje konfigracije	3	2	2	0	0	0
Avtomatizirano preverjanje varnostnih ukrepov	1	1	1	0	0	0
Avtomatizirana analiza vpliva na poslovanje	1	1	1	0	0	0
Avtomatizirana identifikacija in ocena ranljivosti	3	1	1	13	0	3
Avtomatizirano testiranje programske opreme na podlagi UI (AI-based fuzzing)	1	0	5	9	0	2
Avtomatizirani penetracijski testi	0	0	11	0	0	0
Avtomatizirano iskanje groženj	0	0	2	1	0	0
Modeliranje poti napada	1	1	3	1	0	0
Samodejno upravljanje s tveganji	3	1	5	1	1	0
Napovedovanje tveganj	2	0	13	1	0	0
Razvoj strategije	1	3	0	1	0	0
Stroškovna analiza	1	7	0	0	0	0
Varnost dobavne verige na podlagi UI	2	3	3	0	0	0

Zaščita

Primer uporabe UI	Sklepanje	Načrtovanje	Učenje	Komunikacija	Zaznavanje	Hibridno
Večfaktorsko overjanje	2	0	8	0	3	2
Zaščita na podlagi modeliranja in analize obnašanja	0	0	10	0	0	0
Nadzor dostopa	1	2	2	0	0	0
Varnostno usposabljanje na podlagi UI	0	0	4	3	0	0
Zaščita pred izgubo/odtekanjem podatkov	1	0	19	1	0	0
Zaščita elektronske pošte	1	0	6	7	0	0
Blokada zlonamernih domen	0	1	20	1	0	0
Zaščita neokrnjenosti podatkov	0	0	3	0	0	1
Zaščita pred dezinformacijami	0	0	0	3	0	0
Zaščita podatkov pred izgubo na podlagi UI	1	1	5	0	0	0
Kontekstno odvisno vrednotenje groženj	1	0	3	0	0	0
Zaščita ob upoštevanju trendov izkoriščanja ranljivosti	0	1	1	2	0	0
Analiza zapisov	1	0	14	2	0	0
Inteligentni požarni zid	0	0	3	0	0	0
Sistemi za zaščito pred vdori	0	1	4	0	0	0
Antivirusni sistemi in sistemi za zaščito pred zlonamerno kodo	1	0	19	2	0	0

R. Kaur, D. Gabrijelčič in T. Klobučar, Artificial intelligence for cybersecurity: Literature review and future research directions, Information Fusion, Vol. 97, 101804, https://doi.org/10.1016/j.inffus.2023.101804, 2023.

Primeri uporabe UI za kibernetsko varnost (II)

Odkrivanje

Primer uporabe UI	Sklepanje	Načrtovanje	Učenje	Komunikacija	Zaznavanje	Hibridno
Odkrivanje vdorov	1	1	**149**	7	0	**16**
Odkrivanje zlorab in anomalij	0	0	**70**	5	0	**10**
Varnostno relevantni podatki	**2**	**0**	**11**	1	0	**1**
Analiza obnašanja	0	0	**4**	1	0	0
Preiskovanje temnega spleta	0	0	**2**	13	0	0
Stalno samodejno spremljanje virov groženj	0	0	**2**	22	0	3
Obveščanje v realnem času	0	0	**0**	2	0	2
Honeypot na podlagi UI	0	0	**6**	0	0	0

Odzivanje

Primer uporabe UI	Sklepanje	Načrtovanje	Učenje	Komunikacija	Zaznavanje	Hibridno
Scenariji odziva	**1**	0	**1**	1	0	0
Dinamično upravljanje s primeri odziva	**5**	0	0	1	0	0
Klasifikacija incidenta	**1**	0	**1**	1	0	**1**
Obdelava opozoril in triaža	0	0	**5**	1	0	0
Inteligentni asistent	1	0	**2**	3	0	2
Samodejna izolacija	0	0	4	0	0	**0**
Samodejna sanacija	0	**1**	**8**	0	0	0
Dolgotrajna izboljšava	0	0	**3**	2	0	0

Obnova

Primer uporabe UI	Sklepanje	Načrtovanje	Učenje	Komunikacija	Zaznavanje	Hibridno
Samodejna obnova podatkov	0	1	1	0	0	0
Identifikacija in izbris kontaminiranih podatkov	0	0	1	0	0	0
Dnevniški zapisi in analitika	0	0	0	1	0	1

R. Kaur, D. Gabrijelčič in T. Klobučar, Artificial intelligence for cybersecurity: Literature review and future research directions, Information Fusion, Vol. 97, 101804, https://doi.org/10.1016/j.inffus.2023.101804, 2023.

Stanje v Sloveniji

Ponudniki rešitev

- Analiza temnega spleta, honeypot, odkrivanje varnostnih incidentov v omrežju, storitve centrov za odziv
- Izzivi, spodbude

Uporabniki rešitev

- Komercialne rešitve za identifikacijo groženj in tveganj, odkrivanje varnostnih incidentov in anomalij, zaščito in odziv na incidente

Zbirke podatkov

Potrebe organizacij

- Odkrivanje anomalij in naprednih napadov, vizualizacija/analiza dogajanja v realnem času, pomoč varnostnim strokovnjakom pri odločanju, avtomatizacija odziva, OSINT

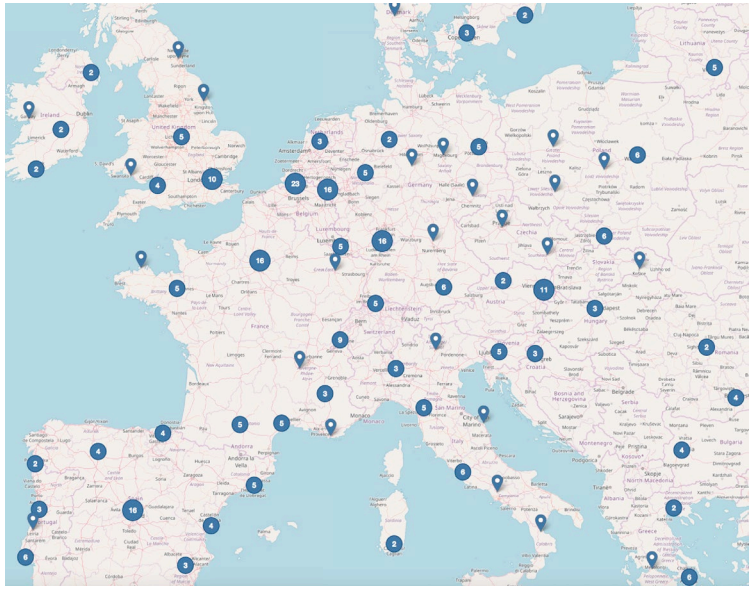
Sodelovanje

- Potreba po sodelovanju
- Možni okviri: aktivnosti nacionalnega dela Evropskega centra za kibernetsko varnost, IKT horizontalna mreža

Primerjava Slovenije z drugimi državami

Precejšnji zaostanek pri razvoju rešitev za kibernetsko varnost na podlagi UI

- Malo znanstvenih objav na obravnavanem področju
- Sodelovanje le pri enem projektu EU za razvoj rešitev
- Brez pomembnejših komercialnih rešitev na trgu
- Konkurenčne prednosti na drugih področjih UI
- Majhna vlaganja na prebivalca



Vir: Cybersecurity Atlas

Oznaka razpisa	Opis	Projekti
H2020-SU-ICT-2018-2020, SU-ICT-01-2018	Dinamično preprečevanje kibernetskih napadov	**SIMARGL** (Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware; https://simargl.eu/)
		CARAMEL (Artificial Intelligence based cybersecurity for connected and automated vehicles; https://www.h2020caramel.eu/)
		CyberSANE (Cyber Security Incident Handling, Warning and Response System for the European Critical Infrastructures; https://www.cybersane-project.eu)
		SAPPAN (Sharing and Automation for Privacy Preserving Attack Neutralization; https://sappan-project.eu)
HORIZON-CL3-2021-CS-01-03	Metode in orodja na podlagi UI za izboljšanje - **robustnosti** sistema (sposobnost sistema, da ohrani svojo začetno stabilno konfiguracijo, zahvaljujoč samotestiranju in samozdravljenju); - **odpornosti** sistema (sposobnost sistema, da predvidi napad z odkrivanjem groženj in nepravilnosti in se mu upre ter omogoči varnostnim analitikom, da pridobijo informacije o kibernetskih grožnjah);	**AI4CYBER** (Trustworthy Artificial Intelligence for Cybersecurity Reinforcement and System Resilience)
		KINAITICS (Cyber-kinetic attacks using Artificial Intelligence)
		LAZARUS (pLatform for Analysis of Resilient and secUre Software)

Oznaka razpisa	Opis	Projekti
	- **odzivnosti** sistema (sposobnost sistema, da se samostojno odzove na napade)	
H2020-SU-SEC-2018-2019-2020, SU-FCT03-2018-2019-2020	Upravljanje z informacijami in tokom podatkov za boj proti kibernetskemu kriminalu in terorizmu	**AIDA** (Artificial Intelligence and advanced Data Analytics for Law Enforcement Agencies)
H2020-SU-AI-2018-2019-2020, SU-AI01-2020	Razvoj načrta raziskav uporabe UI za podporo organom pregona	**ALIGNER** (https://aligner-h2020.eu/)
EDF-2021-CYBER-R	Izboljšava kibernetske obrambe in ravnanja z incidenti s pomočjo UI	/

Predlog usmeritev za razvoj

2023 — 2025 — 2032

Kratkoročna

- Podpora osredotočenim raziskavam
- Oblikovanje interesne skupine
- Oblikovanje srednje in dolgoročne strategije
- Iskanje sinergijskih točk

Srednjeročna

- Spodbujanje prenosa znanja in oblikovanje izobraževalnega programa
- Nadgrajeno sodelovanje med deležniki
- Standardi uvajanja, uporabe in upravljanja rešitev
- Vzpostavitev infrastrukture
- Sinergijsko sodelovanje z AI4SI
- Dobri kazalniki

Dolgoročna

- Krepitev poslovnega sodelovanja
- Nadgradnja infrastrukture
- Prodor na tuje trge
- Razširitev podporne dejavnosti
- Evropske integracije
- Visoki kazalniki

Predlog usmeritev za razvoj (II)

Kratkoročni ukrepi in cilji

- Raziskovalna podpora
  - Kontekstno usmerjena obdelava in triaža varnostnih opozoril
  - Podpora varnostnim strokovnjakom pri odločanju
  - Uporaba znanja iz raziskav UI
    - Avtomatizirana ocena ranljivosti, napovedovanje tveganj, samodejno upravljanje s tveganji
    - Jezikovne tehnologije za celostno večjezikovno obravnavo groženj
    - Učinkovitejše odkrivanje anomalij in varnostnih dogodkov
    - UI, ki jo je mogoče pojasniti
- Sodelovanje
  - Interesna skupina
  - Strategija NpUI za področje kibernetske varnosti
  - Sinergija z drugimi iniciativami na področju UI

Predlog usmeritev za razvoj (III)

Srednjeročni ukrepi in cilji

- Spodbujanje prenosa znanja in oblikovanje izobraževalnega programa
- Oblikovanje standardov uvajanja, uporabe in upravljanja rešitev UI za kibernetsko varnost na nivoju korporativne varnosti
- Vzpostavitev infrastrukture za razvoj UI v kibernetski varnosti
- Podatkovne zbirke
- Platforma za celostno obravnavo in izmenjavo podatkov o grožnjah
- Nadgrajeno sodelovanje

Predlog usmeritev za razvoj (IV)

Dolgoročni ukrepi in cilji

- Krepitev poslovnega sodelovanja in izdelava rešitev za uporabo UI v kibernetski varnosti
- Nadgradnja demonstracijskega centra tehnologij UI v kibernetski varnosti z rešitvami slovenskih podjetij
- Prodor slovenskih proizvajalcev rešitev na tuje trge
- Razširitev podporne dejavnosti platforme za celostno obravnavo groženj na mikro, mala in srednja podjetja
- Povezovanje platform za podatke in celostno obravnavo groženj v prihodnje evropske integracije


ds
dnevi
slovenske
informatike
9. in 10. maj 2023
Kongresni center Bernardin, Portorož
79%
30. konferenca Dnevi slovenske informatike
Soustvarjamo digitrajno Slovenijo

Vprašanja?