DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ



Analiza tendințelor în piața forței de muncă IT și de securitate cibernetică în era Inteligenței Artificiale

AUGUST 2026

TLP:CLEAR

Cuprins

1. Rezumat executiv 3
2. Context conceptual și cadre de referință 3
   2.1 Delimitări și profiluri emergente (IT vs. Securitate cibernetică) 3
   2.2 Inteligența Artificială ca factor perturbator 6
   2.3 Cadre și metodologii conexe 8
3. Piața muncii la nivel global 9
   3.1 Tendințe globale și cifre-cheie 9
   3.2 Rolurile dominante, transformate și emergente 12
   3.3 Impactul automatizării și al AI asupra profesiilor din securitate cibernetică 13
4. Piața din România și analiza comparativă 13
   4.1 Stadiul actual, distribuție și angajatori principali 13
   4.2 Comparație România vs. Piețe internaționale (Densitate și adopție IA) 15
   4.3 Bariere structurale și factori de accelerare locali 16
5. Ecosistemul de formare a profesioniștilor în securitate cibernetică 18
   5.1 Actorii ecosistemului 18
   5.2 Universități și programe relevante 19
   5.3 Piața muncii - roluri și specialiști 20
   5.4 Competiții, academii și inițiative de dezvoltare 20
   5.5 Certificări și formare continuă 21
   5.6 Stadiul adopției IA în SOC-urile din România 22
   5.7 Implicații și strategii pentru angajatori 23
6. Riscuri și provocări strategice 24
   6.1 Riscuri operaționale 24
   6.2 Riscuri juridice și de răspundere 24
   6.3 Riscuri de calitate și amenințări emergente 25
   6.4 Riscuri privind reziliența cibernetică 25
7. Tendințe și prognoze 25
   7.1 Evoluția pieței și integrarea rolurilor IA generative 25
   7.2 Scenarii de evoluție pentru România 26
8. Concluzii și recomandări 28
   8.1 Sinteza concluziilor 28
   8.2 Recomandări strategice pentru mediul privat 29
   8.3 Recomandări pentru instituțiile publice și guvernamentale 30
9. Bibliografie 30

Anexe 32

Anexa 1 - Acronime și abrevieri 32

Anexa 2 - Glosar de termeni 34

Anexa 3 - Notă metodologică 35

1. Rezumat executiv

Piața forței de muncă de IT și de securitate cibernetică traversează o restructurare generată simultan de Inteligența Artificială (IA) și de noul cadru de reglementare al Uniunii Europene (UE) (Directiva NIS2, AI Act, EU Cyber Resilience Act - CRA, Cyber Solidarity Act - CSA). Constatarea centrală este aceea că IA nu slăbește piața, ci o polarizează. Automatizează sarcinile de rutină și rolurile de intrare (SOC L1, analiști, threat intel), amplifică cererea pentru roluri complexe de integrare, guvernanță și apărare activă și generează poziții noi cu salarii atractive (AI Security Engineer, AI Red Teamer, MLSecOps, Prompt Security Analyst, AI Governance Officer). Rezultatul este o "piramidă inversată": presiune pe segmentul mid/senior și transformarea traseului clasic de formare profesională a juniorilor.

La nivel global, raportul WEF Future of Jobs 2025[1] estimează o rată de transformare structurală a pieței muncii de 22% până în 2030 (170 de milioane de locuri de muncă nou create și 92 de milioane eliminate) și anticipează că 39% dintre competențele-cheie actuale devin parțial sau total inutile. Securitatea cibernetică ocupă locul 2 mondial în topul competențelor cu cea mai rapidă creștere, imediat după IA și Big Data. Automatizarea afectează cel mai puternic exact rolurile care constituie tradițional poarta de intrare în profesie: analiștii SOC de nivel 1, analiștii de securitate și cei de threat intelligence. Pe măsură ce sarcinile repetitive specifice acestor roluri sunt preluate de sisteme automatizate, organizațiile reduc recrutarea la nivel de intrare, iar traseul clasic prin care juniorii acumulau experiență se îngustează. Efectul se propagă în timp: fără un flux constant de juniori care să avanseze, cererea se concentrează pe specialiștii mid și senior existenți, un segment deja deficitar, accentuând dezechilibrul structural al pieței.

România intră în această tranziție dintr-o poziție fragilă: circa 207.800 de specialiști ICT în 2025, reprezentând doar 2,7% din populația ocupată - penultimul loc în UE, înaintea Greciei (2,5%). Mai mult, numărul specialiștilor ICT s-a contractat față de 2024 (221.600), în contrast cu trendul ascendent la nivelul UE. Forța de muncă în domeniul securității cibernetice este estimată prin proxy la 12.000–13.000 de specialiști cu un deficit imediat de 2.200–2.500 și un deficit structural proiectat pentru 2030 între sub 15.000 (optimist) și peste 40.000 (pesimist), cu 21.000–35.000 în scenariul realist. Directiva NIS2, transpusă prin OUG nr. 155/2024, transformă deficitul latent în unul acut: 5000-10.000 de entități esențiale și importante de entități intră sub obligații, incluzând desemnarea unei persoane responsabile cu securitatea cibernetică, care trebuie să urmeze un curs de specialitate în termen de 12 luni (art. 14 alin. (4)), precum și obligații de formare pentru organele de conducere.

Analiza arată că pipeline-ul nu suferă de structură, ci de debit și retenție. Lanțul competițional funcționează, dar pipeline-ul pierde la intrare (stagii insuficiente) și la vârf (emigrarea segmentului de experiență), iar domeniul securității cibernetice nu este măsurat statistic separat. Ipoteza centrală a raportului este că: utilizarea tehnologică a IA depășește adopția organizațională, organizațiile folosind deja IA pe scară largă fără roluri, politici sau guvernanță dedicate (*Shadow AI*), iar provocarea următorilor ani este reducerea acestui decalaj.

Miza finală este suveranitatea digitală. Recomandările principale: scalarea internship-ului și a formării alternative și măsuri de retenție pentru segmentul de experiență.

2. Context conceptual și cadre de referință

2.1 Delimitări și profiluri emergente (IT vs. Securitate cibernetică)

Eurostat operează cu o categorie largă de „specialiști ICT”, în timp ce literatura de specialitate și cadrele europene (ENISA, ECSF[2]) converg spre ideea că „forța de muncă în domeniul securității cibernetice” reprezintă un subgrup funcțional, definit atât prin roluri specifice, cât și prin combinații de competențe distincte de restul IT-ului.

Forța de muncă IT, așa cum este surprinsă în statisticile Eurostat, acoperă întregul spectru de profesii din sfera digitală: dezvoltare de aplicații, administrare de infrastructură, suport tehnic, analiză de date, management de proiecte IT etc., fără a diferenția între roluri cu responsabilități de securitate și cele strict

[1] https://www.weforum.org/publications/the-future-of-jobs-report-2025/ [Accesat la data de 29 mai 2026].

orientate pe livrarea de funcționalități. Eurostat definește **specialiștii ICT** pe baza clasificării ISCO-08[2][3] (grupele 25 și 35), incluzând dezvoltatori software, administratori de rețele, analiști de date și profesioniști asociați. În contrast, ENISA, prin European Cybersecurity Skills Framework (ECSF)[4], definește un nucleu de **12 roluri profesionale** de securitate cibernetică (Tabel 1), care împart un set comun de competențe orientate pe protecția confidențialității, integrității și disponibilității sistemelor și datelor.

Tabel 1. Roluri profesionale de securitate cibernetică conform ECSF

#	Profil ECSF	Echivalent în limba română
1	Chief Information Security Officer (CISO)	Director securitate IT
2	Cyber Incident Responder	Specialist răspuns la incidente
3	Cyber Legal, Policy & Compliance Officer	Expert juridic și conformitate
4	Cyber Threat Intelligence Specialist	Specialist informații de amenințare
5	Cybersecurity Architect	Arhitect securitate cibernetică
6	Cybersecurity Auditor	Auditor securitate cibernetică[5]
7	Cybersecurity Educator	Formator/educator securitate cibernetică
8	Cybersecurity Implementer	Implementator soluții de securitate
9	Cybersecurity Researcher	Cercetător securitate cibernetică
10	Cybersecurity Risk Manager	Manager risc cibernetic
11	Digital Forensics Investigator	Specialist investigații digitale
12	Penetration Tester	Expert în teste de penetrare

ECSF conectează rolurile de securitate cibernetică la e-Competence Framework[6] (EN 16234-1), permițând distingerea clară între competențele „de bază” ICT (dezvoltare, operare, suport) și competențele specifice securității (strategie de securitate, managementul riscului, guvernanță, operațiuni de securitate, investigații digitale). *ISC2 Cybersecurity Workforce Study* confirmă faptul că, în practică, multe organizații separă deja funcțional echipele IT de echipele de securitate cibernetică, funcționând cu posturi dedicate (SOC analysts, security engineers, GRC specialists, cloud security architects), chiar dacă toate se încadrează statistic în aceeași umbrelă ICT.

Totodată, ENISA prezintă faptul că în rândul entităților din sectoarele de criticitate ridicată chestionate anual, ponderea personalului cu normă întreagă de securitate a informației (IS FTE) în totalul personalului IT a scăzut pentru al patrulea an consecutiv: de la 13% în 2020, la 12% în 2021, 11,9% în 2022, 11,1% în 2023 și 10,6% în 2024[7] - cel mai scăzut nivel înregistrat de când se efectuează acest tip de studiu. ENISA precizează însă că această scădere este una relativă, nu absolută: ponderea personalului de securitate cibernetică s-a redus pentru că echipele IT în ansamblu au crescut mai rapid, iar bugetele s-au orientat cu

[2] https://isco-ilo.netlify.app/en/isco-08/ [Accesat la data de 15 iunie 2026].
[3] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Glossary:ICT_specialists [Accesat la data de 15 iunie 2026].
[4]https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20User%20Manual.pdf [Accesat la data de 15 iunie 2026].
[5] https://www.dnsc.ro/vezi/document/dnsc-raport-privind-auditul-de-securitate-cibernetica-in-romania [Accesat la data de 6 iulie 2026]
[6] https://esco.ec.europa.eu/en/about-esco/escopedia/escopedia/european-e-competence-framework-e-cf [Accesat la data de 6 iulie 2026].
[7] https://www.enisa.europa.eu/sites/default/files/2026-02/NIS%20Investments%202025%20-%20Main%20report.pdf [Accesat la data de 15 iunie 2026].

prioritate către tehnologie și servicii externalizate. Datele nu indică reduceri ale personalului de securitate existent.

Pe măsură ce sarcinile de analiză de rutină se automatizează, organizațiile creează un strat nou de roluri centrate pe IA; dintre organizațiile care au adăugat roluri noi, 34% au introdus *AI/ML security specialists*, 32% *AI security engineers*, 30% *AI governance analysts*, 23% *AI red teamers* și 19% *AI ethics specialists* - tendință care indică instituționalizarea securității și guvernanței IA ca domenii de sine stătătoare (2026 SANS|GIAC Cybersecurity Workforce Research Report).

IA nu rezolvă deficitul de talente, ci îi schimbă forma: **60% dintre organizații** consideră lipsa de competențe drept provocarea principală, depășind pentru prima dată deficitul de personal (40%). La nivel individual, **95% dintre echipele de securitate raportează cel puțin un deficit de competențe,** IA fiind cel mai frecvent citat (41%), urmată de *cloud security* (36%) și discipline tradiționale precum *risk assessment* (29%), *application security* (28%) sau GRC[8] (27%)[9]. Majoritatea organizațiilor răspund prin structurarea rolurilor după cadre precum NICE[10] sau ECSF (a căror adopție a crescut de la 46% în 2025 la 56% în 2026) și prin investiția în certificări profesionale ca mecanism principal de validare: 64% le folosesc ca metodă de verificare a competențelor, iar 58% le consideră „foarte" sau „extrem" de importante la angajare[11]. Acest trend către competențe măsurabile este susținut și de prognozele CompTIA[12], conform cărora peste 90% dintre companii investesc moderat sau intens în abordări „skills-based workforce", cu accent pe *upskilling* și *cross-skilling* al personalului existent, inclusiv pe dimensiunea IA.

În analiza transformărilor generate de digitalizare și inteligență artificială, patru concepte sunt esențiale: automatizare, digitalizare, upskilling și reskilling. Împreună, ele acoperă întregul spectru al transformării: de la schimbarea tehnologică a proceselor (automatizare, digitalizare) la schimbarea profilului profesional al angajaților (upskilling, reskilling). În practică, acești termeni sunt folosiți adesea amestecat, iar scopul lor este să propună o schemă operațională clară, utilizabilă în cercetare, evaluare de politici sau design de programe (ex. programe de formare, intervenții active pe piața muncii).

Automatizarea este prezentată ca înlocuirea sarcinilor repetitive prin sisteme algoritmice, pornind de la sensul clasic de „funcționare automată a instalațiilor și proceselor cu intervenție umană minimă". În limbaj de politică publică, această definiție permite diferențierea intervențiilor care vizează reducerea volumului de muncă umană în taskuri de rutină.

Digitalizarea este definită ca transformarea proceselor analogice în fluxuri digitale, ceea ce corespunde definițiilor utilizate în ghidurile de digitalizare la nivel european și național (trecerea de la hârtie, semnătură fizică, procese manuale la formulare, baze de date și fluxuri informatizate). Aceasta este o precondiție tehnologică – creează infrastructura și datele necesare – dar nu implică automat, de una singură, schimbări în volumul sau structura muncii. Ulterior, peste procesele digitalizate, se pot construi soluții de automatizare și eficientizare cu ajutorul soluțiilor IA.

Upskilling-ul este prezentat ca aprofundarea competențelor în cadrul aceluiași rol, ceea ce corespunde utilizării curente în literatură pentru „upskilling continuu" sau „continuous professional development". Exemplul „analist SOC tradițional → AI-augmented SOC analyst" indică faptul că rolul formal rămâne similar, dar profilul de competențe se extinde (de exemplu, lucrul cu playbook-uri automatizate, interpretarea rezultatelor unor modele IA, utilizarea unor noi tool-uri), ceea ce este esențial în discuțiile despre impactul AI asupra locurilor de muncă din securitate cibernetică.

Reskilling-ul este definit ca recalificare integrală pentru un rol distinct, în linie cu utilizarea termenului în programe de politici active pe piața muncii și inițiative de tranziție profesională. Exemplul „administrator de sisteme → AI Security Engineer" ilustrează un salt de profil, care implică programe de formare mai lungi, schimbarea familiei ocupaționale și redesenarea parcursului profesional, ceea ce este relevant pentru planificarea strategiilor de workforce în cybersecurity (de ex. trecerea din roluri tradiționale IT în roluri specializate pe securitatea IA).

[8] Guvernare, Risc și Conformitate (*Governance, Risk, and Compliance*)
[9] https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study [Accesat la data de 29 mai 2026].
[10] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center [Accesat la data de 6 iulie 2026].
[11] https://www.sans.org/mlp/2026-evolving-cybersecurity-workforce-ai-compliance-talent [Accesat la data de 29 mai 2026].
[12] https://www.comptia.org/en-us/resources/research/it-industry-outlook-2026/ [Accesat la data de 29 mai 2026].

Tabel 2. Automatizare, digitalizare și dezvoltarea competențelor: definiții operaționale

Direcții strategice	Definiție operațională
Automatizare	Înlocuirea sarcinilor repetitive prin sisteme algoritmice (reduce ponderea muncii umane în execuția task-urilor de rutină).
Digitalizare	Transformarea proceselor analogice în fluxuri digitale (precondiție tehnologică, fără implicații directe asupra forței de muncă).
Upskilling	Aprofundarea competențelor existente ale unui angajat în rolul său actual (ex.: analist SOC tradițional → AI-augmented SOC analyst).
Reskilling	Recalificare integrală pentru un rol diferit (ex.: administrator de sisteme → AI Security Engineer; presupune programe extinse de formare).

2.2 Inteligența Artificială ca factor perturbator

Inteligența Artificială reconfigurează rapid munca în securitate cibernetică, erodează rolurile de entry-level și împinge organizațiile să regândească recrutarea de talente în jurul competențelor, nu al titulaturilor. Studiul *ISC² CyberSecurity Workforce Report 2025*[9] arată că 69% dintre echipe fie au integrat deja, fie testează activ tool-uri de AI security, iar 63% dintre utilizatori raportează un boost semnificativ de productivitate. Impactul asupra rolurilor este dublu:

- **Incident responder**: IA este folosită pentru corelarea log-urilor, prioritizarea incidentelor și generarea de *playbook*-uri; organizațiile cu utilizare extinsă a IA și automatizării în operațiunile de securitate înregistrează costuri per breșă cu până la 34%[13] mai mici față de cele care nu folosesc aceste tehnologii.
- **Penetration tester/red team**: echipele combină tool-uri generative și agenți specializați pentru *reconnaissance*, generarea de *payload*-uri și *chaining* de vulnerabilități, crescând acoperirea testelor și frecvența execuției prin modelele PTaaS continuu.

OECD estimează că aproximativ 27% din locurile de muncă din țările OECD prezintă risc ridicat de automatizare[14]. Scorul mediu de expunere la IA pentru profesioniștii IT este 0,88/1,00 - printre cele mai ridicate dintre toate ocupațiile[15].

Raportul WEF Future of Jobs 2025, publicat în ianuarie 2025, reprezintă una dintre cele mai cuprinzătoare analize prospective a pieței muncii globale pentru orizontul 2025-2030. Bazat pe perspectivele a peste 1.000 de angajatori de top din 22 clustere industriale și 55 de economii, reprezentând peste 14 milioane de angajați, raportul oferă un cadru de referință esențial pentru analiza impactului IA. WEF FoJ 2025 documentează că ponderea sarcinilor exclusiv umane scade de la 47% în 2025 la 34% în 2030, în timp ce colaborarea om-mașină crește de la 30% la 33%, iar automatizarea totală urcă de la 22% la 33%[16].

Analiza distinge trei mari categorii de evoluție sub impactul IA:

- **Roluri automatizabile**: SOC L1 (triage, enrichment), scanare manuală a vulnerabilităților, audit de conformitate de rutină. AI-SOAR-ul autonom acoperă deja peste 75% din sarcinile operaționale la organizațiile pilot.

[13] https://www.ibm.com/reports/data-breach [Accesat la data de 16 iunie 2026].
[14] https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/07/oecd-employment-outlook-2023_904bcef3/08785bba-en.pdf [Accesat la data de 16 iunie 2026].
[15] https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/10/who-will-be-the-workers-most-affected-by-ai_fb7fcccd/14dc6f89-en.pdf [Accesat la data de 16 iunie 2026].
[16] https://www.weforum.org/publications/the-future-of-jobs-report-2025/ [Accesat la data de 16 iunie 2026].

- **Roluri transformate**: Incident Responder (MTTR redus cu 90%), Penetration Tester asistat de IA (creștere de 27 puncte procentuale în acoperirea vulnerabilităților), Threat Hunter (corelație în timp real cu volume mari de telemetrie).
- **Roluri nou create**: AI Security Engineer, AI Red Teamer/Adversarial ML Specialist, MLSecOps Engineer, Prompt Security Analyst, AI Governance Officer, plus rolul Cyber Security Governance Manager (Manager Executiv în Guvernanța Securității Cibernetice) introdus, în luna ianuarie 2026 de DNSC, în proiectul de decizie pentru aprobarea standardului de pregătire a membrilor organelor de conducere ale entităților esențiale și importante[17].

La nivel global, *WEF Future of Jobs 2025*[18] estimează o rată de transformare structurală a pieței muncii de 22% din piața muncii până în 2030: 170 de milioane de locuri de muncă noi create, față de 92 de milioane de locuri de muncă existente dispărute, dintr-un set de date de 1,2 miliarde de locuri de muncă analizate. Separat, raportul estimează că 39% din competențele-cheie actuale ale forței de muncă vor suferi transformări semnificative sau vor deveni depășite în același interval.

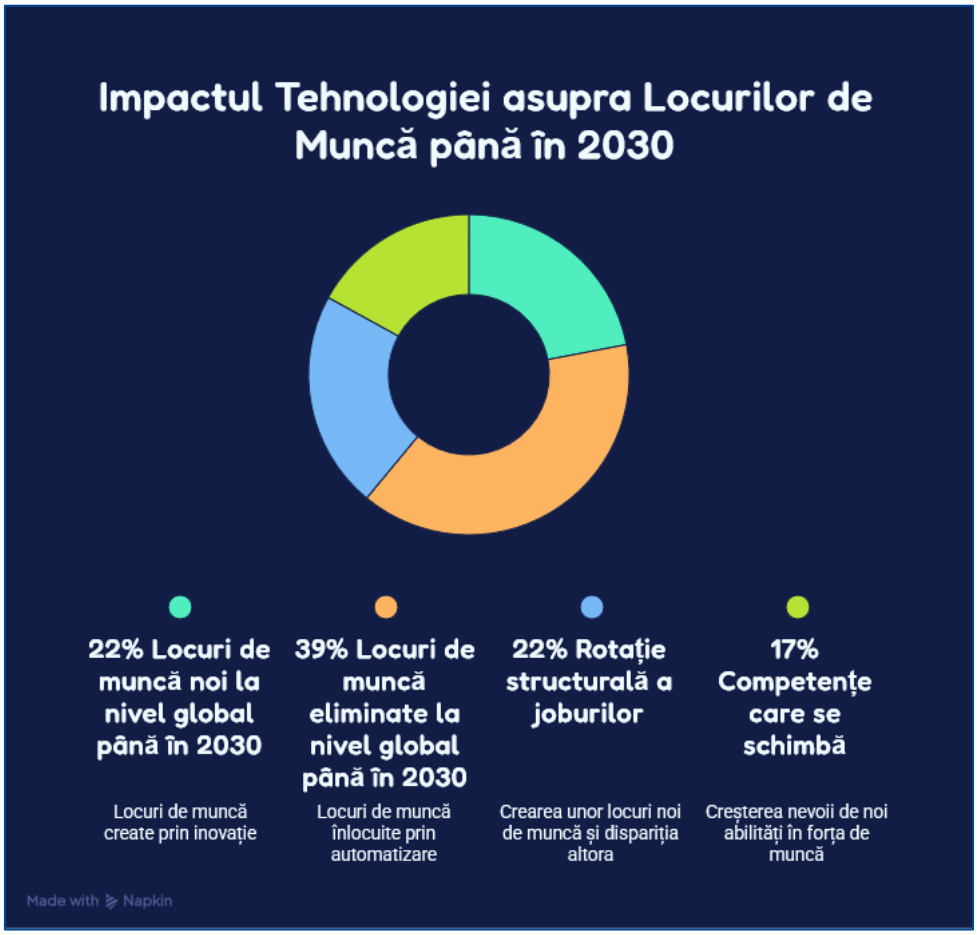


Figura 1. Impactul tehnologiei asupra locurilor de muncă până în 2030 (Sursa: WEF Future of Jobs 2025)

Datele empirice indică faptul că IA este folosită mai întâi pentru a elimina munca manuală și a automatiza fluxurile, nu pentru a reduce imediat resursa umană. 49% din organizații raportează reducerea timpului de analiză manuală, iar 48% raportează automatizarea workflow-urilor, față de doar 16–18% care invocă reducerea efectivă de personal. Automatizarea afectează puternic exact în rolurile care tradițional reprezentau poarta de intrare în profesie: SOC și analiști de securitate (32% reduceri raportate), analiști de threat intelligence (26%) și personalul care răspunde la incidente de securitate cibernetică (22%). Rezultatul este o „piramidă inversată”: presiune maximă pe rolurile *mid/senior/expert*, în timp ce *entry-level-ul* devine teoretic ușor de acoperit, dar practic mai greu de format, pentru că traseul clasic de

[17] https://www.dnsc.ro/vezi/document/proiect-decizie-dnsc-certificari-de-securitate-cibernetica [Accesat la data de 22 iunie 2026]
[18] https://reports.weforum.org/docs/WEF_Future_of_Jobs_Report_2025.pdf [Accesat la data de 16 iunie 2026].

acumulare a experienței prin sarcini repetitive este eliminat de AI, conform studiului *SANS CyberSecurity Workforce 2026*.

IA generativă este percepută ca un amplificator de productivitate: dintre profesioniștii în securitate cibernetică care utilizează activ instrumente IA, 63% raportează un câștig semnificativ de productivitate[9]. Percepțiile impactului asupra fluxului de recrutare de talente entry-level sunt însă divergente. Pe de o parte, 86% dintre organizații consideră că IA generativă poate contribui la atragerea talentului entry-level în securitate cibernetică, iar 58% se așteaptă ca aceasta să accelereze integrarea noilor angajați[9]; profesioniștii înșiși văd IA drept catalizator de carieră, 73% anticipând crearea de roluri mai specializate. Pe de altă parte, datele structurale arată că IA automatizează tocmai sarcinile de triaj care au constituit istoric punctul de intrare în carieră (SOC Tier 1), ridicând problema formării următoarei generații de specialiști[19]. Soluția emergentă este redefinirea pozițiilor entry-level în jurul supravegherii, validării și rafinării muncii sistemelor IA, mai degrabă decât al execuției directe a sarcinilor de triaj.

2.3 Cadre și metodologii conexe

Cadrul ECSF (European Cybersecurity Skills Framework), publicat de ENISA în septembrie 2022 și desemnat referențial UE prin Comunicarea privind Academia de Competențe[20], sintetizează 12 profiluri de rol cu descrieri detaliate ale misiunii, livrabilelor, cunoștințelor (K) și abilităților (S). Cele 12 profiluri ECSF (Tabel 1) cunosc o transformare diferențiată sub impactul IA. Rolurile predominant tehnico-operaționale (Cyber Incident Responder, Penetration Tester, Cybersecurity Implementer) sunt cele mai expuse augmentării prin IA, în timp ce rolurile cu componentă de management și conformitate (CISO, Compliance Officer, Risk Manager) integrează IA preponderent ca instrument de suport decizional. Această polarizare se regăsește și la nivelul percepției profesioniștilor în securitate cibernetică: 73% consideră că IA va genera noi competențe specializate, iar 72% anticipează o nevoie sporită de abordări strategice în domeniu, conform studiului ISC2 din 2025[9].

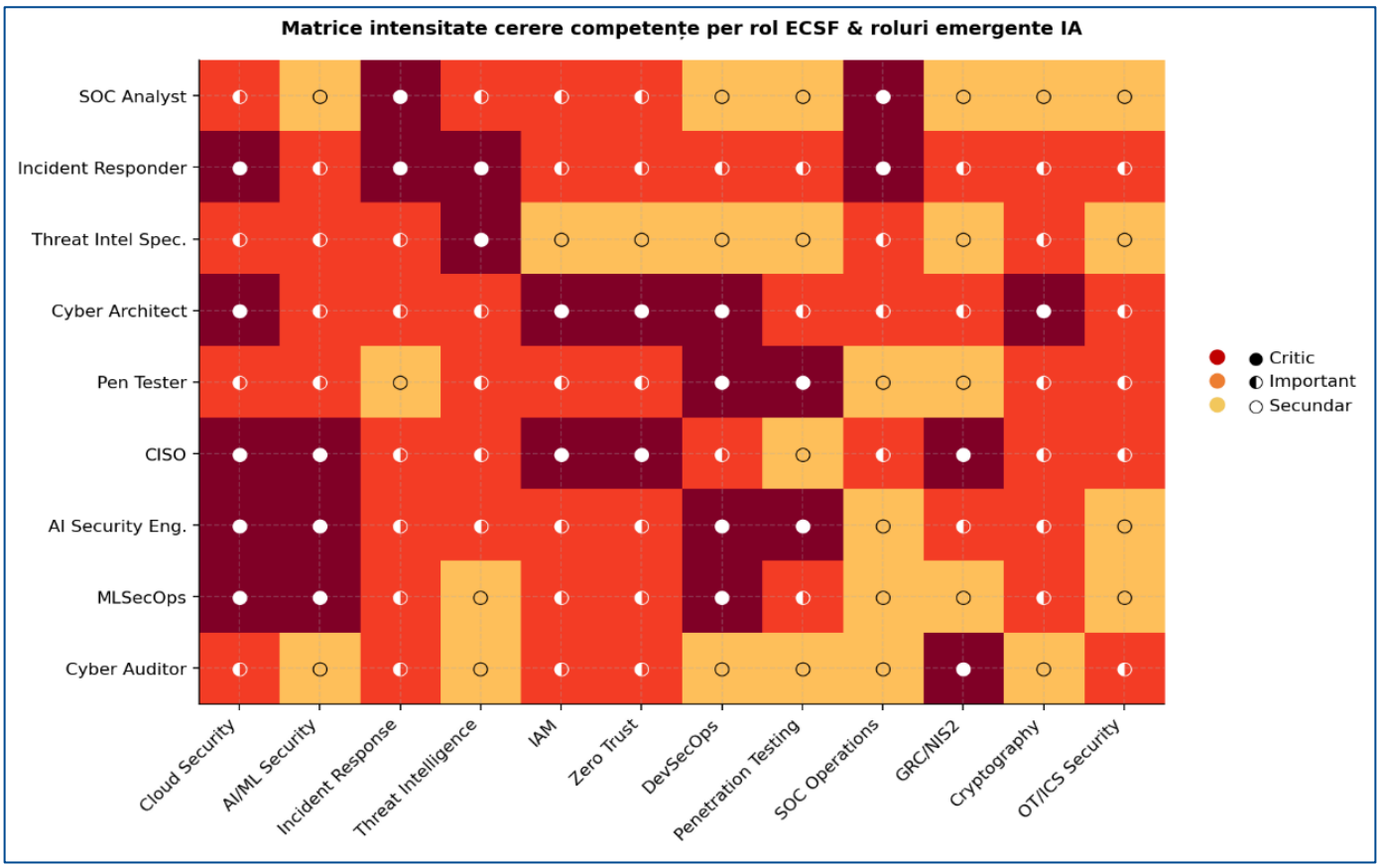


Figura 2. Matricea de intensitate a cererii de competențe pe roluri ECSF în era IA

[19] https://www.sans.org/white-papers/2026-cybersecurity-workforce-research-report [Accesat la data de 16 iunie 2026].
[20] https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf [Accesat la data de 16 iunie 2026].

Matricea de intensitate a cererii de competențe pe roluri[21] (*Figura 2*), construită prin sinteza cadrelor ECSF (ENISA), NICE SP 800-181 Rev.1, WEF Future of Jobs 2025 și ENISA NIS Investments 2024, evidențiază o concentrare a criticității pe competențele de *Cloud Security*, *IAM* și *SOC Operations*, esențiale atât pentru rolurile tradiționale (*CISO*, *Cyber Architect*, *Incident Responder*), cât și pentru cele emergente centrate pe IA (*AI Security Engineer*, *MLSecOps*). Rolurile hibride precum *AI Security Engineer* și *MLSecOps* prezintă un profil de competențe extins, care combină cerințe critice specifice securității cloud și *DevSecOps*[22] cu nevoi ridicate pe zona *AI/ML Security*, confirmând tendința de convergență între disciplinele tradiționale de securitate cibernetică și noile specializări de guvernanță și securitate a sistemelor IA. În contrast, rolurile de audit (auditor de securitate cibernetică) și testare (expert în testarea de penetrare) păstrează un profil de competențe mai concentrat, cu criticitate ridicată punctuală pe *GRC/NIS2*, respectiv *Incident Response*, reflectând specializarea funcțională specifică fiecărui rol în cadrul organizației de securitate.

Dincolo de cadrul european ECSF, o abordare complementară este oferită de standardul NIST SP 800-181 Rev. 1[23], publicat de Institutul Național de Standarde și Tehnologie din SUA, care adoptă o structură modulară bazată pe Task-Knowledge-Skill (TKS), cu 7 categorii de roluri și 11 arii de competențe în versiunea actuală (v2.2.0, aprilie 2026[24]), inclusiv noua zonă de competență *AI Security*.

La nivel de politică publică, această nevoie de standardizare a competențelor este susținută prin EU Cybersecurity Skills Academy[25], lansată la 18 aprilie 2023, se structurează pe 4 piloni: (1) generare de cunoștințe prin educație/formare, (2) pledge-uri și diversitate de gen, (3) vizibilitate pentru finanțare/proiecte, (4) metodologie de monitorizare a pieței.

3. Piața muncii la nivel global

3.1 Tendințe globale și cifre-cheie

Deficitul global de specialiști în securitate cibernetică a atins 4,8 milioane[26] de posturi neocupate în 2024, la un total de circa 5,5 milioane de profesioniști activi. Ceea ce înseamnă o creștere a gap-ului de 19% față de anul precedent, pe fondul stagnării efective a forței de muncă active. În 2025, ISC[2] a renunțat la publicarea unei noi estimări numerice a gap-ului, subliniind că lipsa de competențe specifice a depășit ca prioritate lipsa de personal: 95% dintre respondenți raportează cel puțin un gap de competențe, iar 59% declară nevoi de competențe critice sau semnificative, în creștere de la 44% în 2024[9].

Aceste tendințe globale se reflectă și la nivelul UE, unde raportul NIS Investments 2024[27] indică faptul că 32% dintre organizațiile participante se confruntă cu dificultăți la recrutare în toate domeniile de securitate cibernetică, iar o pondere semnificativă a personalului de securitate nu dețin certificări profesionale în domeniul securității cibernetice. Cel mai alarmant indicator este procentul de 89% al organizațiilor care declară un deficit de personal specializat necesar pentru conformitatea cu cerințele Directivei NIS2. Această cifră arată clar faptul că implementarea cadrului de reglementare este frânată în principal de constrângeri legate de resursa umană, mai degrabă decât de bariere tehnice, financiare sau organizaționale. Practic, chiar dacă organizațiile dispun de resursele necesare pentru investiții tehnologice, absența unui personal suficient de calificat rămâne principalul obstacol în atingerea nivelului de conformitate impus de legislație.

În ceea ce privește sursele de recrutare, datele arată că 34% dintre angajați provin din roluri non-cyber, în timp ce doar 18% au fost recrutați dintr-un rol deja existent în domeniul securității cibernetice.

---

[21] Notă metodologică: Matricea de mai sus a fost generată cu asistența inteligenței artificiale, pe baza sintezei realizate din cadrele ECSF (ENISA), NICE SP 800-181 Rev.1, WEF Future of Jobs 2025 și ENISA NIS Investments 2024. Reprezentarea vizuală are caracter ilustrativ și de sistematizare a informațiilor din sursele citate, nefiind un rezultat statistic publicat oficial de instituțiile menționate. Nivelurile de criticitate atribuite fiecărei perechi rol-competență reflectă o interpretare calitativă a modelului LLM folosit, iar validarea acestora prin studii empirice suplimentare este recomandată înaintea utilizării în decizii de politică sau resurse umane.

[22] https://www.dnsc.ro/vezi/document/dnsc-analiza-pietei-devsecops-in-romania [Accesat la data de 16 iunie 2026].

[23] https://csrc.nist.gov/pubs/sp/800/181/r1/final [Accesat la data de 16 iunie 2026].

[24] https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/current-version/change-logs [Accesat la data de 16 iunie 2026].

[25] https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy [Accesat la data de 16 iunie 2026].

[26] https://www.isc2.org/Insights/2024/10/Cybersecurity-Workforce-INSIGHTS-October-2024 [Accesat la data de 22 iunie 2026].

[27] https://www.enisa.europa.eu/sites/default/files/2024-11/CSPA%20-%20NIS%20Investments%20-%202024_0.pdf [Accesat la data de 29 mai 2026].

Această diferență semnificativă evidențiază o tendință tot mai pronunțată de reconversie profesională, prin care organizațiile preferă să dezvolte intern competențe de securitate cibernetică în rândul angajaților cu background diferit, decât să concureze pe o piață restrânsă de specialiști deja formați. Această strategie poate reprezenta o soluție viabilă pe termen scurt pentru acoperirea posturilor vacante, dar implică totodată costuri și timp considerabile pentru formare, precum și riscul unui nivel inegal de competențe în cadrul echipelor.



Figura 3. Statistici privind forța de muncă în securitate cibernetică (Sursa: ENISA NIS Investments 2024)

În ansamblu, aceste statistici confirm faptul că deficitul de forță de muncă din securitatea cibernetică nu este doar o problemă cantitativă, legată de numărul insuficient de candidați, ci și una calitativă, determinată de lipsa certificărilor formale și de necesitatea reconversiei profesionale masive. Combinația dintre aceste două dimensiuni indică faptul că eforturile de conformare cu cerințele Directivei NIS2 vor rămâne dependente, în mod critic, de politici sustenabile de formare, certificare și dezvoltare a talentelor la nivel european.

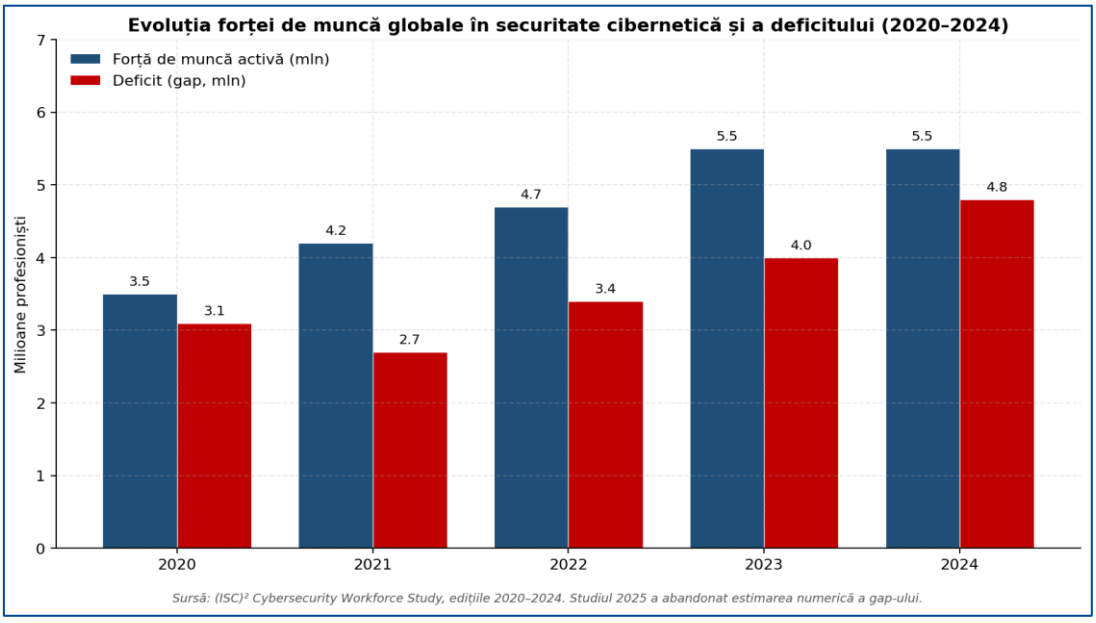


Figura 4. Evoluția forței de muncă în securitate cibernetică la nivel global 2020-2024 (Sursa: ISC2)

Figura 4 prezintă evoluția forței de muncă active în securitate cibernetică și a deficitului de personal în perioada 2020-2024, oferind o imagine dinamică a decalajului. Graficul confirmă vizual tendința descrisă anterior: în timp ce numărul specialiștilor activi a crescut moderat, deficitul s-a adâncit constant, atingând cele 4,8 milioane de posturi neocupate raportate pentru 2024. Această reprezentare grafică pregătește terenul pentru analiza cauzelor structurale ale gap-ului, tratată în continuare prin prisma competențelor.

Dincolo de dimensiunea cantitativă a deficitului, ISC2 documentează și modul în care tehnologia, inclusiv automatizarea și inteligența artificială, va remodela locurile de muncă din securitate cibernetică până în 2030. Această perspectivă explică de ce, în 2025, ISC2 a renunțat la o estimare numerică simplă a gap-ului, concentrându-se în schimb pe lipsa de competențe specifice, un fenomen mai profund decât simpla insuficiență de personal. Astfel, accentul se deplasează de la criza de volum de forță de muncă către criza de competențe, care domină discursul actual din industrie și pregătește terenul pentru cifrele UE prezentate în continuare.

Piața globală a IA în securitate cibernetică este estimată să crească de la 25,53 miliarde USD în 2026 la 50,83 miliarde USD în 2031 (CAGR 14,8%)[28]. Gartner estimează că **42% din organizații** folosesc sau pilotează deja asistenți IA pentru detecție și răspuns, iar 46% suplimentar planifică implementarea în următorul an[29]. Raportul CompTIA IT Industry Outlook 2026[12] confirmă faptul că **94% dintre companii** intenționează să investească în training AI-specific în 2026, iar securitatea cibernetică și confidențialitatea datelor rămâne preocuparea principală în strategia de securitate.

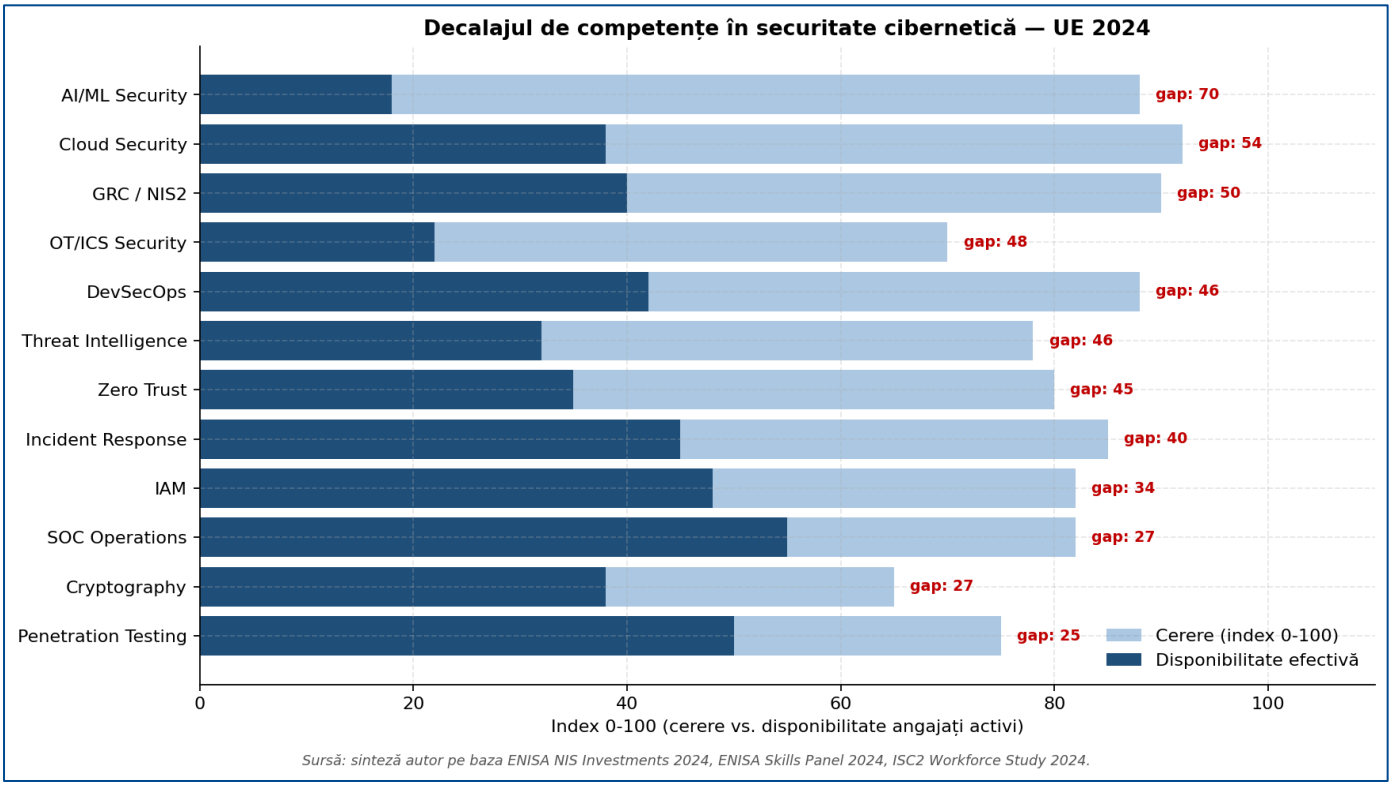


Figura 5. Gap-ul de competențe la nivel UE - domenii cu deficit cel mai acut

Figura 5 detaliază domeniile din UE afectate cel mai acut de deficitul de competențe, oferind o defalcare granulară a problemei introduse anterior prin cifrele ENISA privind dificultățile de recrutare și lipsa certificărilor. Vizualizarea completează astfel narativa europeană, arătând nu doar câți profesioniști sunt necesari, ci și în ce arii specifice se concentrează deficitul, informație relevantă pentru prioritizarea investițiilor în formare.

World Economic Forum (WEF) identifică o polarizare clară a pieței muncii: securitatea cibernetică ocupă locul 2 în topul competențelor cu cea mai mare rată de creștere, după AI și Big Data, confirmând relevanța strategică a investițiilor în domeniu[1]. Raportul WEF documentează răspunsul angajatorilor la această

[28] https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-in-cybersecurity-market-224985247.html [Accesat la data de 22 iunie 2026].
[29] https://www.cynet.com/blog/gartner-hype-cycle-2025-cybersecurity-ai-assistants-and-ai-soc-agents/ [Accesat la data de 22 iunie 2026].

tranziție: 85% planifică programe de *upskilling* și *reskilling*; 70% intenționează să recruteze personal cu competențe noi în IA; 50% planifică să reorienteze afacerile în răspuns la IA; 40% anticipează reducerea numărului de angajați în roluri automatizabile; 63% identifică decalajul de competențe drept principala barieră în transformarea afacerii.

Tabel 3. Competențe emergente și competențe în declin

Competențe în ascensiune (2025-2030)	Competențe în declin (2025-2030)
IA și Big Data (locul 1)	Îndemânare manuală și precizie fizică
Rețele și securitate cibernetică (locul 2)	Procesare manuală a datelor
Alfabetizare tehnologică (locul 3)	Raportare financiară standardizată
Gândire creativă	Traducere multilingvă directă
Reziliență, flexibilitate, agilitate	Atenție rutinară și memorie procedurală
Leadership și influență socială	Activități administrative repetitive

Tabelul nr. 3 pune în oglindă competențele în ascensiune (IA și Big Data, rețele și securitate cibernetică, alfabetizare tehnologică) cu cele în declin (procesare manuală a datelor, activități administrative repetitive) pentru orizontul 2025-2030, conform Future of Jobs Report al WEF. Poziționarea securității cibernetice pe locul 2 în topul competențelor cu cea mai mare rată de creștere confirmă, într-un format vizual direct, argumentul central al subcapitolului: investițiile în acest domeniu rămân strategice, chiar în contextul transformărilor aduse de IA. Tabelul încheie astfel logic secțiunea, legând tendințele globale de deficit cu direcția clară de evoluție a pieței muncii pe termen mediu.

3.2 Rolurile dominante, transformate și emergente

Piața muncii în securitate cibernetică nu se restructurează uniform: diferite roluri cunosc traiectorii distincte în funcție de gradul lor de expunere la automatizare și de cererea nouă generată de reglementare și IA. Rolurile dominante în prezent - Security Analyst, Cloud Security Engineer, GRC Specialist, CISO - rămân în cerere ridicată, dar conținutul lor se modifică semnificativ. Security Analyst L1/L2 migrează spre supravegherea și calibrarea agenților IA; GRC Specialist integrează cerințe Directiva NIS2, DORA și AI Act; iar CISO devine responsabil de o agendă dublă: securitate operațională și guvernanță IA.

Rolurile în transformare accelerată includ: *Incident Responder* - automatizarea triajului și a răspunsului standard reorientează rolul dinspre execuția procedurilor spre *threat hunting* și supravegherea agenților automați; *Penetration Tester* - augmentat de IA generativă, care extinde acoperirea testării, cu expertiza umană concentrată pe scenarii complexe și validarea rezultatelor; *Threat Intelligence Analyst* - corelarea volumelor mari de telemetrie este preluată de sisteme automate, focusul uman deplasându-se spre interpretare strategică și contextualizare.

Rolurile emergente cu cerere imediată și salarii premium includ:

- **AI Security Engineer** - securizarea sistemelor și pipeline-urilor IA; salarii estimate 150.000–250.000 USD în SUA.
- **AI Red Teamer/Adversarial ML Specialist** - testarea robusteții modelelor IA contra atacurilor adversariale.
- **MLSecOps Engineer** - integrarea securității în ciclul de viață al modelelor ML.
- **Prompt Security Analyst** - detectarea și prevenirea prompt injection, jailbreaking și data leakage prin LLM.
- **AI Governance Officer** - conformitate cu AI Act, auditare modele, transparență și etică.

- **Cyber Security Governance Manager** - rol formal introdus de DNSC în proiectul de decizie din ianuarie 2026 pentru entitățile reglementate de Directiva NIS2 din România.

3.3 Impactul automatizării și al AI asupra profesiilor din securitate cibernetică

Impactul IA nu este omogen și nu înseamnă înlocuire, ci mai degrabă augmentare și redistribuire a sarcinilor. Datele SANS 2026 arată că 49% din organizații reduc timpul de analiză manuală și 48% automatizează workflow-urile, dar numai 16–18% reduc efectiv headcount-ul[30]. Studiul CSA pe 148 de analiști SOC a documentat că 94% dintre analiști au evaluat IA mai pozitiv după utilizare practică, fără detractori[31]. Automatizarea răspunsului la incidente produce reduceri substanțiale ale timpului mediu de răspuns (MTTR, Mean Time to Respond). De exemplu, Microsoft raportează că integrarea capabilităților de automatizare din Microsoft Sentinel a permis companiei OMV reducerea MTTR la jumătate, iar asistentul Security Copilot reduce MTTR cu aproximativ 30%[32]. Noile roluri (AI Security Engineer, AI Red Teamer, MLSecOps) au salarii estimate între 100.000–250.000 USD în SUA, cu premium 15–25% față de roluri MLOps clasice.

Impactul IA se produce în cascadă, cu efecte de ordin doi care sunt mai importante decât reducerile directe de posturi:

- **Impactul de ordinul 1:** Automatizarea task-urilor repetitive (triage, log correlation, enrichment, raportare) → eliberare de capacitate umană pentru cazuri complexe;
- **Impactul de ordinul 2:** Erodarea traseului clasic de entry-level (SOC Tier 1 ca „școală practică") → criză de pipeline de talente pe termen mediu;
- **Impactul de ordinul 3:** Crearea de roluri noi care cer combinarea cunoștințelor cyber cu AI, ML și data science → premium salarial de 15–25% față de roluri MLOps clasice.

Raportul WEF documentează că ponderea sarcinilor exclusiv umane va scădea de la 47% în 2025 la 34% în 2030, în timp ce colaborarea om-mașină crește de la 30% la 33%, iar automatizarea totală urcă de la 22% la 33%. Concluzia operațională pentru angajatori: **AI nu va goli piața IT/cybersecurity, ci o va polariza** - reducând cererea pentru roluri simple și crescând cererea pentru roluri complexe de integrare, guvernanță și apărare activă.

În acest context, adaptabilitatea la schimbare devine una dintre cele mai valoroase competențe de pe piața muncii, inclusiv pentru angajatorii din IT și securitate cibernetică. Raportul *Future of Jobs 2025* al World Economic Forum arată că, pe lângă competențele tehnice legate de AI, big data, rețele și cybersecurity, cresc puternic în importanță și competențele de tip „resilience, flexibility and agility", alături de curiozitate și învățare continuă, pe fondul faptului că 39% dintre competențele-cheie ale forței de muncă sunt așteptate să se schimbe până în 2030. Pentru angajatori, acest lucru înseamnă că valoarea unui profesionist nu mai este dată doar de setul actual de cunoștințe, ci de capacitatea de a învăța rapid, de a se recalibra operațional și de a integra noile tehnologii în fluxurile de lucru. În domeniul securității cibernetice, unde AI schimbă simultan atât instrumentele de apărare, cât și profilul amenințărilor, adaptabilitatea devine esențială pentru utilizarea responsabilă a noilor tehnologii, pentru actualizarea competențelor și pentru reacția eficientă la riscuri emergente.

4. Piața din România și analiza comparativă

4.1 Stadiul actual, distribuție și angajatori principali

Piața românească a forței de muncă în domeniul IT și securitate cibernetică reflectă, la o scară mai redusă, aceleași tensiuni structurale observate la nivel european: un decalaj persistent între cererea de competențe digitale și oferta de specialiști calificați, accentuat de particularitățile economice și demografice locale. România se poziționează într-un context regional aparte, cu un sector IT&C care a cunoscut o expansiune susținută în ultimul deceniu, dar care a început să resimtă, începând cu 2024, semnele unei corecții de piață similare celor înregistrate în alte economii europene. Analiza comparativă

[30] https://www.sans.org/mlp/2026-evolving-cybersecurity-workforce-ai-compliance-talent [Accesat la data de 29 mai 2026].
[31] Dropzone AI/CSA - 148 SOC Analyst Study, https://www.dropzone.ai/blog/soc-analysts-ai-perception-148-study
[32] https://www.microsoft.com/en/customers/story/25951-omv-aktiengesellschaft-microsoft-sentinel [Accesat la data de 29 mai 2026]

a indicatorilor naționali față de mediile UE permite identificarea atât a punctelor forte ale ecosistemului românesc, cât și a vulnerabilităților care ar putea afecta capacitatea țării de a-și atinge obiectivele de digitalizare și conformitate cu cadrul de reglementare european.

Distribuția geografică a forței de muncă IT și de securitate cibernetică este puternic concentrată în câteva hub-uri majore. Estimările de industrie arată că **București, Cluj-Napoca, Timișoara și Iași** concentrează cea mai mare parte a specialiștilor IT, în timp ce Cluj, Timișoara și Iași funcționează ca noduri regionale în creștere. Centrele de livrare pentru multinaționale, precum IBM, Cognizant, Accenture, Orange Business Services, Thales, CrowdStrike sunt localizate aproape exclusiv în aceste hub-uri, ceea ce confirmă un model de polarizare teritorială specific economiei digitale și pieței de securitate cibernetică.

Conform Eurostat, **în 2024** avea aproximativ **221.600** de specialiști ICT ocupați (valoare estimată), în creștere față de **196.200 în 2023**, dar urmată de o scădere la **circa 208.800 în 2025** (estimare)[33]. Indicatorul Eurostat măsoară persoanele ocupate în ocupații de specialist ICT în ansamblul economiei, conform definiției OECD bazate pe clasificarea ISCO-08, și nu totalul angajaților din sectorul IT&C.

În același timp, un studiu Bestjobs menționează faptul că în 2024 oferta de joburi în IT&C s-a redus cu 21% față de 2023, semnalând o corecție puternică a pieței după anii de expansiune accelerată.

Din perspectiva cererii din partea companiilor, datele Eurostat indică faptul că aproximativ 16% dintre companiile din România (cu cel puțin 10 angajați) au specialiști ICT angajați, unul dintre cele mai scăzute procente din UE, ceea ce sugerează faptul că densitatea redusă de specialiști nu este doar o problemă de ofertă, ci și de grad de digitalizare și maturitate tehnologică la nivelul companiilor. De subliniat este faptul că **27,3% dintre specialiștii ICT sunt femei** - locul 2 în UE după Estonia.

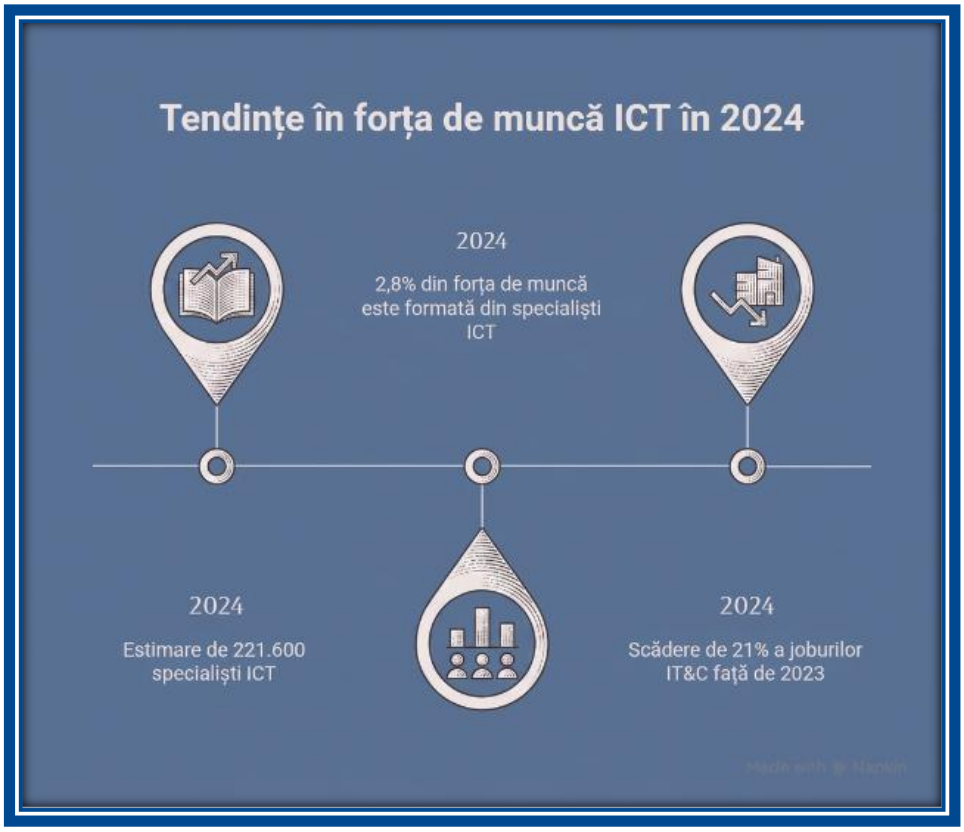


Figura 6. Tendințe în forța de muncă ICT in 2024

România înregistrează în 2024 un paradox notabil pe piața IT: numărul absolut de angajați a atins un record istoric în contextul în care oferta de locuri de muncă s-a contractat semnificativ față de anii precedenți.

După scăderea înregistrată în 2023, numărul de angajați în IT a crescut din nou în 2024 până la circa 221.600 (estimare Eurostat), evoluție explicată atât prin recuperarea unor proiecte amânate, cât și prin efectul modificărilor fiscale care au făcut mai puțin atractive formele de colaborare de tip PFA și au determinat o parte dintre profesioniști să treacă pe contracte de muncă. Sectorul IT rămâne cel mai bine

[33] https://ec.europa.eu/eurostat/databrowser/view/isoc_sks_itspt/default/table?lang=en [Accesat la data de 23 iunie 2026]

remunerat din economie, cu salarii nete care, pentru roluri de DevOps, Frontend sau Data Engineering, pornesc frecvent de la aproximativ 1.600 EUR net pentru poziții mid-level și pot depăși 4.000–4.500 EUR[34][35] net pentru profesioniști seniori. Eliminarea facilităților fiscale pentru angajații din IT, decisă prin OUG 156/2024 și aplicabilă veniturilor începând cu ianuarie 2025, este considerată de analiza de specialitate un factor de risc major: schimbarea reduce atractivitatea fiscală a României pentru investiții în tehnologie, creează percepția de instabilitate și poate accelera migrația sau relocarea profesioniștilor cu înaltă calificare[36].

4.2 Comparație România vs. Piețe internaționale (Densitate și adopție IA)

Conform Eurostat, în 2024 doar **2,8%**[37] din forța de muncă ocupa roluri de specialiști ICT, față de **5,0% media UE-27**, ceea ce plasează România cu un decalaj de **2,2 puncte procentuale** sub media europeană. Suedia (8,6%) și Finlanda (7,8%) se află în vârful clasamentului, în timp ce România este apropiată ca pondere de Bulgaria (4,6%) și Polonia (4,5%), în timp ce România este apropiată ca pondere de Bulgaria (4,6%) și Polonia (4,5%), în zona inferioară a distribuției[38].

Studiile salariale regionale indică faptul că salariile specialiștilor în securitate cibernetică din România sunt semnificativ mai reduse decât în Europa de Vest, adesea la aproximativ jumătate din nivelurile practicate în țări precum Germania, Olanda sau Franța, ceea ce explică interesul multinaționalelor pentru extinderea centrelor de securitate la București sau Cluj[39]. Rapoarte recente sugerează că unele state vest-europene și baltice (precum Irlanda, Estonia și Olanda) alocă o parte din bugetul IT pentru inițiative de AI în securitate cibernetică, în timp ce în România investițiile dedicate rămân, de regulă, reduse.

România își păstrează un avantaj de cost salarial față de media europeană în industria IT și în securitate cibernetică, aspect confirmat de statisticile europene privind câștigurile și de rapoartele regionale de piață. Întrucât nu există serii statistice oficiale armonizate pe roluri specifice de securitate cibernetică, comparațiile numerice exacte între România și media UE trebuie tratate cu prudență.

Acest cost mai redus al forței de muncă continuă să atragă investiții și centre de operațiuni tehnologice în România. Avantajul se erodează însă treptat în rolurile senior și în competențele rare, unde cererea europeană în creștere pentru specialiști ICT și de securitate cibernetică exercită presiune ascendentă asupra salariilor.

În era IA, competitivitatea României va depinde tot mai puțin de nivelul mai redus al salariilor și tot mai mult de capacitatea de a forma specialiști cu competențe hibride, aflate la intersecția dintre dezvoltarea software, securitatea cibernetică și tehnologiile IA.

Instrumente de finanțare, europene și naționale, care pot accelera închiderea decalajului în România includ Digital Europe Programme, care a alocat pentru perioada 2021–2024 aproximativ 194 milioane EUR pentru SOC-uri, formare profesională și susținerea European Cybersecurity Competence Centre (ECCC)[40]. Pentru 2025–2027, bugetul total al programului, care acoperă cybersecurity, IA și competențe digitale, se ridică la 1,3 miliarde EUR, iar din această sumă ECCC gestionează un Work Programme dedicat de 390 milioane EUR, orientat spre noi tehnologii, IA și tranziția post-cuantică[41].

La nivel național, Planul Național de Redresare și Reziliență (PNRR) a alocat inițial aproximativ 5,976 miliarde EUR pentru digitalizare în ansamblu[42]. În completarea investițiilor destinate digitalizării administrației și consolidării infrastructurilor digitale, Componenta C7 – Transformare digitală include și intervenții dedicate dezvoltării capitalului uman în domeniul securității cibernetice, prin Investiția I15 –

[34] https://wise-step.ro/blog/it-salaries-romania-2026/#:~:text=DevOps%2Fcloud%20engineers%20(4%2C099%20EUR) [Accesat la data de 24 iunie 2026]
[35] https://www.newtech.ro/en/blog-it-salaries-january-2026/ [Accesat la data de 24 iunie 2026]
[36] https://reference-global.com/download/article/10.2478/picbe-2024-0050.pdf [Accesat la data de 24 iunie 2026]
[37] https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250708-2 [Accesat la data de 23 iunie 2026]
[38] https://ec.europa.eu/eurostat/databrowser/view/isoc_sks_itspt__custom_17278796/bookmark/bar?lang=en&bookmarkId=8e1da841-1ad2-4da8-bd9a-e7c5ba51111d&c=1751011232681 [Accesat la data de 23 iunie 2026]
[39] https://static.germantechjobs.de/market-reports/European-Transparent-IT-Job-Market-Report-2024.pdf [Accesat la data de 23 iunie 2026]
[40] https://digital-strategy.ec.europa.eu/en/news/digital-europe-programme-fuels-digital-transformation-and-skills-development-across-europe [Accesat la data de 2 iulie 2026]
[41] https://cybersecurity-centre.europa.eu/news/eccc-finance-eur-390-million-cybersecurity-projects-under-digital-europe-programme-2025-2027-2025-03-28_en [Accesat la data de 2 iulie 2026]
[42] https://www.emip.ro/post/digitalizare-prin-pnrr [Accesat la data de 2 iulie 2026]

«*Crearea de noi competențe de securitate cibernetică pentru societate și economie*», cu o alocare de 8.694.159,00 lei fără TVA, 1.762.120 Euro.

4.3 Bariere structurale și factori de accelerare locali

România continuă să beneficieze de un avantaj de cost relevant în industria IT și, prin extensie, în domeniul securității cibernetice, însă acest avantaj trebuie interpretat cu prudență metodologică. Sursele oficiale europene confirmă faptul că nivelul general al veniturilor salariale din România rămâne printre cele mai reduse din UE, dar nu oferă o defalcare suficient de granulară pe roluri precum SOC L1-L2, Pentester, Cyber Architect sau CISO[43]. Datele Eurostat privind statisticile salariale arată că România se află în grupul țărilor cu cele mai mici venituri mediene din UE, ceea ce susține ideea că firmele care operează din România pot accesa competențe IT și cyber la costuri semnificativ sub nivelul Europei de Vest.

În paralel, rapoartele de piață IT din România și Europa Centrală și de Est indică o convergență treptată a salariilor, în special pentru rolurile senior și pentru competențele rare, ceea ce sugerează faptul că

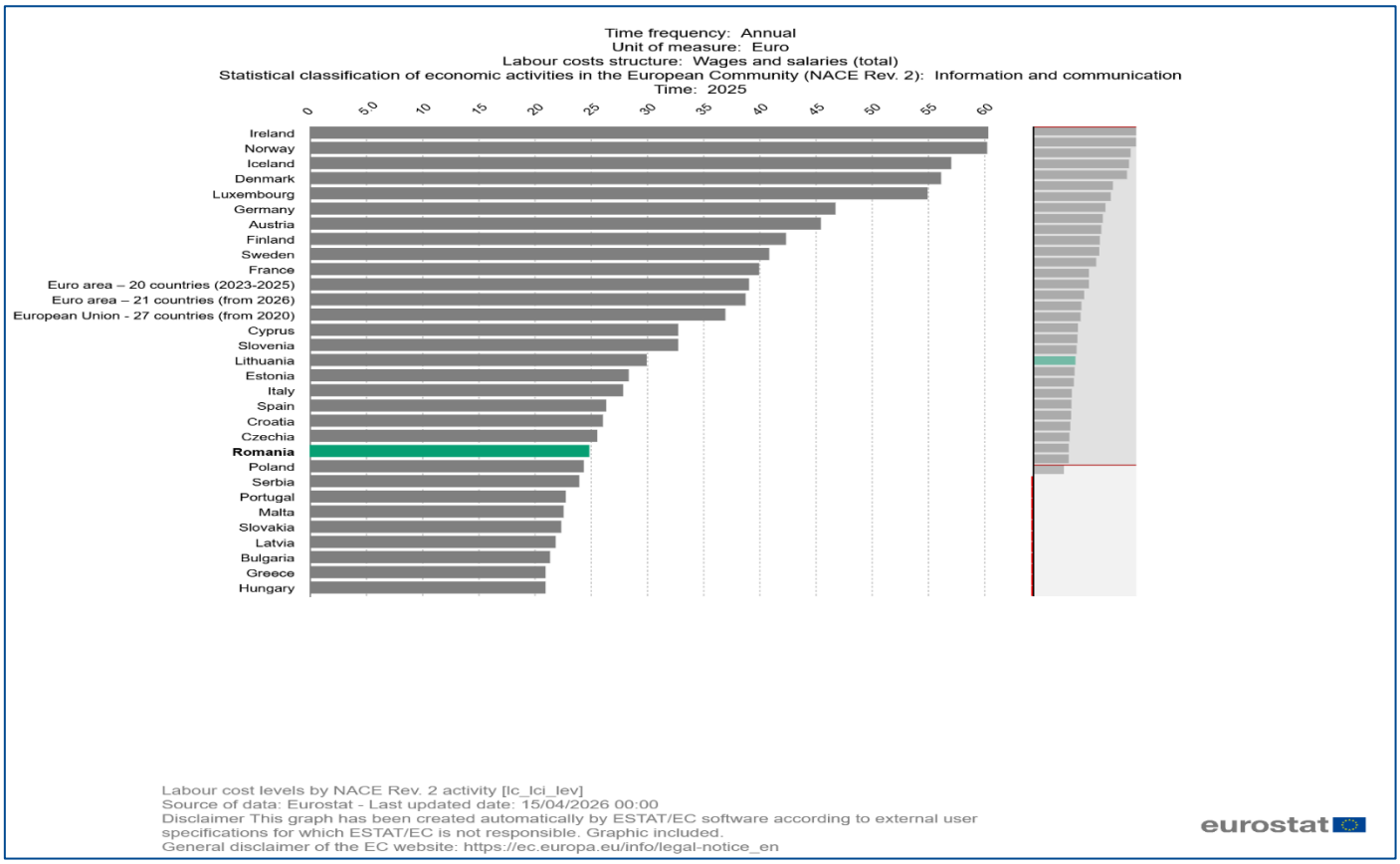


Figura 7. Clasificarea statistică Eurostat a costurilor salariale pentru companiile din domeniul IT (2025)

avantajul de cost se menține, dar se comprimă în segmentele cu valoare adăugată ridicată[44][45]. Această tendință este relevantă mai ales pentru rolurile aflate la intersecția dintre securitate cibernetică și IA. În măsura în care cererea europeană pentru competențe avansate crește mai repede decât oferta, diferențialul salarial al României poate funcționa ca accelerator local pentru atragerea de proiecte, dar și ca sursă de presiune asupra retenției, deoarece profesioniștii foarte bine pregătiți devin tot mai ușor integrabili în piețe externe prin muncă remote sau contractare internațională[46][47].

Prima barieră structurală este lipsa unei transparențe statistice suficiente la nivel de roluri în domeniul securității cibernetice și AI-related. Eurostat publică date solide pentru sectorul IT în ansamblu și pentru câștigurile salariale agregate, însă nu există o bază oficială europeană care să permită comparații

[43] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Wages_and_labour_costs [Accesat la data de 24 iunie 2026]
[44] https://pirvanescu.com/blog/2026-03-14-tech-salaries-romania-vs-western-europe/ [Accesat la data de 24 iunie 2026]
[45] https://static.germantechjobs.de/market-reports/European-Transparent-IT-Job-Market-Report-2024.pdf [Accesat la data de 24 iunie 2026]
[46] https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study [Accesat la data de 24 iunie 2026]
[47] https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20260527-2 [Accesat la data de 24 iunie 2026]

standardizate între România și media UE pentru roluri precum Pen Tester, AI Security Engineer sau CISO[48][49]. Pentru un raport strategic, această absență obligă la utilizarea unor combinații de surse private, ghiduri salariale, platforme de recrutare și studii sectoriale, care au metodologii eterogene și nu sunt perfect comparabile între țări.

A doua barieră este comprimarea treptată a avantajului de cost în zona de senioritate ridicată. Analizele salariale regionale arată că diferența dintre România și Europa de Vest rămâne mai pronunțată la nivel entry și mid-level, dar se reduce în cazul rolurilor de arhitectură, leadership și expertiză rară. Ceea ce ne indică faptul că modelul tradițional bazat exclusiv pe arbitraj salarial devine mai puțin sustenabil pentru specializările unde competitivitatea depinde de experiență, certificări, expunere la tehnologii emergente și integrare în ecosisteme globale de inovare[50].

A treia barieră este presiunea de piață generată de digitalizarea accelerată și de creșterea cererii pentru specialiști ICT în ansamblul UE. Numărul specialiștilor ICT din Uniunea Europeană a continuat să crească, ajungând la 10,45 milioane în 2025, adică 5,0% din totalul angajaților, ceea ce confirmă competiția tot mai intensă pentru talent tehnologic[51]. În acest context, piețele cu bază mai redusă de competențe specializate, precum România, se confruntă cu riscul ca o parte disproporționată din profesioniștii de top să fie absorbiți de angajatori externi sau de filiale cu bugete globale[52].

Un efect colateral al creșterii cererii europene de competențe ICT și securitate cibernetică este intensificarea migrației externe a profesioniștilor seniori din România. Analize recente ale sectorului ICT local arată că, deși numărul angajaților a crescut cu peste 50% în ultimul deceniu, o parte considerabilă a talentului cu experiență ridicată este atrasă de piețele vest-europene, fie prin relocare, fie prin contracte remote directe. În securitate cibernetică, unde deficitul de competențe este recunoscut oficial la nivelul UE, această dinamică accentuează golurile de expertiză internă: companiile din România concurează nu doar între ele, ci și cu angajatori din state membre cu bugete salariale mult mai mari, interesați în mod special de roluri precum SOC senior, penetration tester, cyber architect sau CISO.

Principalul factor de accelerare local este combinația dintre costul relativ competitiv și masa critică deja formată în centre urbane precum București, Cluj-Napoca, Iași și Timișoara. Chiar dacă datele publice nu permit o comparație salarială exactă pe fiecare rol din domeniul securității cibernetice, rapoartele de piață indică faptul că România rămâne semnificativ sub vestul Europei ca nivel de salarizare, dar dispune de o bază profesională suficient de matură pentru a susține activități cu valoare adăugată în dezvoltare software, operațiuni de securitate și servicii de inginerie.

Al doilea accelerator este potențialul de convergență între deficitul european de competențe din domeniul securității cibernetice și capacitatea României de a furniza talent la cost relativ mai mic. Rapoartele privind piața europeană a competențelor din domeniul securității cibernetice arată că deficitul de personal rămâne ridicat, iar organizațiile caută tot mai frecvent soluții de extindere a bazei de recrutare, inclusiv prin dezvoltarea de roluri entry-level și junior-level. Pentru România, acest lucru creează o fereastră de oportunitate: rolurile SOC, *engineering* și *secure development* pot fi scalate mai ușor decât rolurile executive, cu condiția existenței investițiilor în formare, certificare și retenție.

Al treilea accelerator este tendința de repoziționare a pieței de la cost către competențe hibride. Pe măsură ce IA schimbă cerințele pentru forța de muncă IT și securitate cibernetică, avantajul local nu mai este dat doar de salarii mai mici, ci și de capacitatea de a produce specialiști care combină software engineering, securitate, guvernanță și competențe aplicate de IA. În lipsa acestei tranziții, avantajul salarial riscă să rămână captiv în segmentele operaționale; în prezența ei, România poate urca spre roluri mai bine plătite și mai greu de relocat[9].

Pentru România, semnalul important nu este doar „câte joburi dispar", ci „ce tip de competențe devin obligatorii". Tendințele sintetizate în Future of Jobs Report 2025 și în analizele OECD indică faptul că până în 2030 aproximativ 39% dintre competențele de bază ale forței de muncă se vor schimba, cu creșteri puternice pentru abilitățile legate de IA și Big Data, securitate cibernetică, competențe digitale avansate și gândire analitică. În acest context, angajatorii vor favoriza tot mai mult profilurile hibride, care combină

[48] https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Earnings_statistics [Accesat la data de 24 iunie 2026]
[49] https://ec.europa.eu/eurostat/web/labour-market/database [Accesat la data de 24 iunie 2026]
[50] https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/02/building-a-skilled-cyber-security-workforce-in-europe_6abaf769/3673cd60-en.pdf [Accesat la data de 24 iunie 2026]
[51] https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20260527-2 [Accesat la data de 24 iunie 2026]
[52] https://www.isc2.org/Insights/2025/06/cybersecurity-hiring-trends-study [Accesat la data de 24 iunie 2026]

dezvoltare software, lucrul cu date, înțelegerea securității și „AI literacy", adică abilitatea de a lucra eficient cu sisteme IA și automatizări, nu doar utilizarea ocazională a unor unelte generative[53][54].

Pentru specialiștii din IT și securitate cibernetică, implicația este clară: cei care își adaugă competențe de IA, cloud și securitate au cele mai bune perspective de carieră, în timp ce rolurile bazate pe sarcini repetitive sau suport operațional standardizat vor fi cele mai expuse presiunii automatizării. Rapoartele WEF și analizele privind impactul IA indică un scenariu de polarizare a pieței, în care cererea scade pentru joburile cu conținut automatizabil și crește pentru joburile complexe, de integrare, guvernanță, reziliență și apărare cibernetică.

Studiile recente asupra utilizării la scară largă a instrumentelor de tip copilot[55] arată că o parte semnificativă a sarcinilor de producție textuală, documentare sau analiză standardizată poate fi automatizată sau cel puțin accelerată substanțial, ceea ce reduce timpul necesar pentru activitățile de volum, dar nu elimină nevoia de expertiză umană pentru proiectare, validare și decizie. Pentru sectorul IT românesc, aceasta înseamnă că o pondere considerabilă a joburilor junior și a activităților de suport va fi restructurată sau reconfigurată în următorii ani, așa cum sugerează deja analizele macroeconomice privind impactul IA asupra pieței muncii din România, în special în zone precum entry-level IT, call-centre și operațiuni administrative[56].

Nici raportul WEF și nici literatura de specialitate nu susțin un scenariu de înlocuire totală a forței de muncă IT, ci mai degrabă un model de augmentare, în care tehnologia preia sarcinile repetitive și eliberează spațiu pentru activități cu valoare adăugată mai mare. Future of Jobs Report 2025 arată că 85% dintre angajatori intenționează să investească în *upskilling* și *reskilling* până în 2030, iar 63% consideră „skill gaps" principala barieră în calea transformării business-ului, ceea ce confirmă că soluția dominantă este recalificarea, nu concedierea pe scară largă. Totuși, acest model de augmentare implică o schimbare profundă a fișelor de post și o cerință crescută de alfabetizare digitală avansată la toate nivelurile, ceea ce poate deveni atât barieră structurală, cât și factor de accelerare pentru organizațiile capabile să investească sistematic în competențe.

5. Ecosistemul de formare a profesioniștilor în securitate cibernetică

5.1 Actorii ecosistemului

Ecosistemul românesc de formare în securitate cibernetică reunește trei tipuri principale de actori economici, fiecare cu un rol distinct în absorbția și dezvoltarea forței de muncă specializate: companii autohtone cu focus tehnologic, filiale ale multinaționalelor și furnizori dedicați de formare/certificare. Acesta nu se limitează la instituțiile de învățământ și furnizorii de certificare, ci include și angajatorii, deoarece aceștia joacă un rol activ în modelarea competențelor practice ale viitoarei forțe de muncă, printr-un mecanism de „formare prin colaborare industrie-academie". Practic, companiile intervin în punctele în care educația universitară clasică nu poate ține pasul cu evoluția rapidă a amenințărilor cibernetice și a tehnologiilor asociate, oferind expunere practică, infrastructură și mentorat direct din partea specialiștilor activi în domeniu.

Bitdefender, deși nu este un furnizor de cursuri certificate, a construit unul dintre cele mai extinse parteneriate universitate-industrie din România: compania a contribuit la dezvoltarea programelor de licență și masterat în securitate cibernetică la Universitatea din București, Universitatea Tehnică din Cluj-Napoca și Universitatea „Alexandru Ioan Cuza" din Iași, cu cursuri predate direct de angajați ai companiei[57]. Peste 1.000 de studenți au trecut prin aceste programe de pregătire, unii ajungând ulterior în roluri strategice chiar în cadrul companiei. Compania a investit și în infrastructură fizică, precum laboratorul de peste 50.000 EUR oferit Universității Politehnica București, și susține financiar cadrele didactice prin

[53] https://www.weforum.org/stories/2025/01/future-of-jobs-report-2025-jobs-of-the-future-and-the-skills-you-need-to-get-them/ [Accesat la data de 24 iunie 2026]
[54] https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/02/building-a-skilled-cyber-security-workforce-in-europe_6abaf769/3673cd60-en.pdf [Accesat la data de 24 iunie 2026]
[55] Instrumente bazate pe IA care asistă utilizatorul în realizarea unor sarcini, prin generarea de sugestii, conținut sau soluții.
[56] https://think.ing.com/snaps/how-romanias-growth-shift-and-ai-are-reshaping-the-jobs-market/ [Accesat la data de 24 iunie 2026]
[57] https://unibuc.ro/bursele-anis-2026-editia-a-ix-a-ofera-granturi-de-5-000-de-euro-pentru-inovatie-in-educatia-universitara/ [Accesat la data de 2 iulie 2026]

programe precum Bursele ANIS, alături de alte companii tech[58][59]. De asemenea, oferă burse de cercetare, stagii ("Stagii pe Bune") și tabere internaționale de securitate cibernetică (Global Cybersecurity Camp) pentru studenți români.

Safetech Innovations[60], una dintre puținele firme românești dedicate integral securității informației, listată la Bursa de Valori București (BVB), funcționează ca un canal important de formare practică prin programe de pregătire și formare: compania s-a angajat să pregătească profesioniști IT în competențe de cybersecurity, ethical hacking și CERT/CSIRT, oferind stagiarilor expunere directă în cadrul unui SOC operațional 24x7. Această formare „la locul de muncă" completează educația teoretică din universități cu experiență operațională reală, esențială într-un domeniu unde practica evoluează mai rapid decât curricula academică[61].

Companii precum IBM, Microsoft, Oracle, HP, Endava, Stefanini, Accenture, Atos, Capgemini, Luxoft, NTT Data și Cognizant[62] operează centre de dezvoltare și livrare de servicii în România, care includ frecvent echipe dedicate securității cibernetice (SOC-uri, servicii gestionate, consultanță GRC) integrate în structurile lor globale. Aceste centre contribuie semnificativ la cererea de forță de muncă calificată local, absorbind o parte importantă a absolvenților de programe tehnice și de securitate din țară.

TÜV Austria România, RQM Certification, CertInspect Register, Business Generator, KPMG Advisory, Fiatest, APSAP, Institutul Național de Cercetare-Dezvoltare în Informatică - ICI București, Cyburg, Antech Consulting și Euro Jobs completează acest segment, oferind servicii conexe de certificare, evaluare a conformității și formare profesională, fiind de asemenea autorizați ca furnizori de servicii de formare de către DNSC[63], esențiale pentru alinierea competențelor pieței la cerințele legislative naționale (Legea 362/2018, OUG 155/2024) și internaționale. Ecosistemul include și companii specializate exclusiv în educație profesională de securitate cibernetică, care livrează programe de pregătire în formate variate, de exemplu „la locul de muncă", virtual cu lector sau în ritm propriu (self-paced), prin formatori autorizați de organizații internaționale de referință precum CompTIA, ISC2, GIAC, EC-Council, Offensive Security sau Mile2, fără a se limita la acestea. În România, actori precum Bittnet Training și ComputerLand operează ca centre de formare acreditate pentru mai multe dintre aceste organisme de certificare, oferind cursuri EC-Council, CompTIA, Mile2 și Offensive Security atât în format fizic, cât și online. Tendința recentă arată o extindere a acestui segment: în 2026, Exclusive Networks România și-a diversificat portofoliul de training independent de vendor prin parteneriate cu CompTIA, EC-Council, ISC^2, Mile2 și OffSec, cu programe aliniate explicit cerințelor Directivei NIS2.

Această structură pe trei paliere - companii autohtone specializate, multinaționale cu prezență locală și furnizori de formare/certificare - reflectă un ecosistem în care cererea de competențe, generată de multinaționale și companiile românești, este susținută de o infrastructură de certificare aliniată tot mai strâns la standardele europene de securitate cibernetică.

5.2 Universități și programe relevante

Ecosistemul românesc de formare a specialiștilor în IT și securitate cibernetică poate fi citit simultan în două chei. Ca lanț de conversie a competențelor, el adaugă succesiv valoare: universitățile dau baza teoretică, competițiile și comunitățile validează abilitățile practice, certificările aduc standardizare și lizibilitate, internship-urile mediază tranziția spre muncă, iar piața rolurilor junior realizează selecția. Ca pâlnie, însă, lanțul are două scurgeri: o îngustare progresivă la fiecare etaj, pe măsură ce baza largă de absolvenți IT se reduce la nucleul restrâns care intră efectiv în roluri de securitate, și o pierdere la vârf, prin emigrare și prin muncă la distanță prestată exclusiv pentru angajatori străini. Directiva NIS2 transformă deficitul latent într-unul acut, mutând întrebarea de politică publică de la „cât producem" la „cât reținem și cât de repede familiarizăm juniorii".

[58] https://sal.cs.unibuc.ro/burse-si-premii-acordate-de-bitdefender/ [Accesat la data de 2 iulie 2026]
[59] https://community.bitdefender.com/en/discussion/91324/bitdefender-and-the-polytechnica-university-of-bucharest-inaugurated-a-state-of-the-art-computer-lab [Accesat la data de 2 iulie 2026]
[60] https://www.safetechinnovations.com/about [Accesat la data de 2 iulie 2026]
[61] https://www.digitalsme.eu/digitalsme4skills/participating-companies/safetech-innovations/ [Accesat la data de 2 iulie 2026]
[62] Enumerarea multinaționalelor de mai sus nu reflectă o ierarhizare a angajatorilor și nu este exhaustivă. Lista are caracter ilustrativ, incluzând companii multinaționale cu centre de dezvoltare sau livrare de servicii în România despre care există informații publice privind activități relevante pentru securitatea cibernetică. Nu toate aceste companii operează divizii dedicate exclusiv securității cibernetice în România, iar ponderea activității de securitate cibernetică în cadrul centrelor locale variază semnificativ de la o companie la alta.
[63] https://www.dnsc.ro/pagini/formatori-si-furnizori-de-servicii-de-formare [Accesat la data de 2 iulie 2026]

Universitățile cu profil de informatică, automatică și calculatoare furnizează baza tehnică și funcționează ca infrastructură de pre-recrutare, prin parteneriate și practică. Facultatea de Matematică și Informatică (FMI) din cadrul Universității Babeș-Bolyai (UBB) menționează explicit o rețea de firme partenere. Stratul de securitate cibernetică este real și divers - masterul UBB din consorțiul EIT Digital, masterul „Cyber Security" de la UTBV Brașov, programul „Security and Applied Logic" al Universității din București, ofertele UAIC Iași și Politehnica București, plus componenta militară a Academiei Tehnice Militare. Problema nu este existența programelor, ci debitul. Cea mai recentă cifră publică indică circa 8.700 de absolvenți TIC[64], în creștere cu aproximativ 22% față de 2014, dar într-un ritm mai lent decât creșterea efectivului de salariați. Nu există o statistică dezagregată pentru absolvenții *de securitate cibernetică* - o limitare metodologică care, în sine, justifică o recomandare către INS. Efectivul total IT a atins în 2024 un număr de 195.929 de angajați[65] (ANIS)/estimat la 221.600 de specialiști TIC (Eurostat), divergența venind din definiții. Dar raportat la populația ocupată, ponderea rămâne printre cele mai mici din UE.

5.3 Piața muncii - roluri și specialiști

Este cel mai important punct de filtrare, cu două componente care trag în direcții opuse. Cererea structurală e puternică: se estimează faptul că, pentru conformarea cu cerințele OUG 155/2024, circa 12.000 de companii vor avea nevoie de personal de securitate cibernetică, în condițiile în care deficitul este de aproximativ 6.000 de oameni cu experiență - de unde miza pe juniori. Deficitul direct de specialiști este estimat la 2.200 – 2.500 de persoane, iar platformele listau peste o sută de posturi vacante explicite. Conjunctura de intrare, în schimb, s-a înăsprit în 2026: mai mulți candidați, mai puține oferte, mai puține internship-uri cu conversie clară, presiune din partea AI pe sarcinile entry-level - o „fază de selecție economică" a IT-ului. Cele două nu se contrazic: cererea pe mid/senior coexistă cu o piață de intrare aflată într-o fază ciclică mai strânsă, iar efectul net este o barieră de intrare mai înaltă, în care diploma, proiectele, comunitatea și certificările devin factori cumulativi, nu alternative. Remunerația rămâne atractivă, încadrată pentru analist între 1.300 – 2.000 € net la intrare și pentru specialist între 2.000 – 4.500 € net (cifre indicative, din agregatoare de recrutare).

Forța de muncă cu experiență nu apare spontan, ci prin acumulare productivă; de aceea densitatea ecosistemului de intrare contează direct pentru viteza de maturizare. România produce o bază decentă, dar pierde masiv tocmai la nivelurile de experiență: conducerea DNSC[66] vorbește de zeci de mii de specialiști IT plecați și câteva mii care lucrează din țară exclusiv pentru firme străine, iar un raport al Băncii Mondiale (date 2019) estima că ~40% dintre absolvenții de studii superioare (24–64 ani) au emigrat. Pâlnia se îngustează astfel a doua oară, la trecerea junior → mid/senior, transformând rolurile cu experiență în resursa cea mai disputată. Inițiative precum cele ale Cluj IT Cluster, care tratează consolidarea capacității în securitate cibernetică drept prioritate strategică națională, confirmă că problema e una de capacitate sistemică. Pentru calibrare, ISC2 estimează un deficit de 347.000 de specialiști în Europa și de câteva milioane global - deci o problemă de retenție și competitivitate, nu de absență a talentului.

5.4 Competiții, academii și inițiative de dezvoltare

Este, paradoxal, cel mai bine structurat nivel și cel care funcționează cel mai explicit ca punte spre piața muncii, validând competențe aplicate și creând rețele profesionale timpurii. UNbreakable România (Bit Sentinel + Orange), ediția 2025 (a opta), a adunat aproape 1.700 de înscriși[67]; la etapa individuală, 87% nu aveau un loc de muncă, 80% își doreau un internship, iar 60% participau pentru prima dată - semn că programul atrage constant talent nou. Ediția 2026 a lansat un format centrat pe securitatea cibernetică în era IA. Lanțul este instituționalizat: etapele naționale (UNbreakable, Olimpiada de Securitate Cibernetică) alimentează finala Romanian Cyber Security Challenge, din care se selectează, prin bootcamp, echipa de 11 pentru European Cybersecurity Challenge - organizată de DNSC cu SRI/Cyberint și Asociația Națională pentru Securitatea Sistemelor Informatice (ANSSI), cu sprijinul Orange, Bit Sentinel și CyberEDU.

[64] https://media.hotnews.ro/assets/document/2022/02/9/25356644-0.pdf [Accesat la data de 2 iulie 2026]
[65] https://anis.ro/events/studiul-de-industrie-anis-itc-devine-liderul-exporturilor-de-servicii-si-depaseste-pragurile-din-anul-anterior-la-contributia-la-pib-taxe-si-valoare-adaugata/ [Accesat la data de 2 iulie 2026]
[66] https://www.linkedin.com/pulse/rom%C3%A2nia-nevoie-s%C4%83-%C3%AE%C8%99i-preg%C4%83teasc%C4%83-motiveze-%C8%99i-p%C4%83streze-dan-cimpean/ [Accesat la data de 2 iulie 2026]
[67] https://unbreakable.ro/44-de-tineri-vs-un-agent-ai-confruntarea-de-cybersecurity-care-a-rescris-finala-unbreakable-romania-2026/ [Accesat la data de 2 iulie 2026]

DefCamp completează acest ecosistem printr-un format orientat spre învățare practică și transfer direct de competențe către industrie. Pe lângă conferința propriu-zisă, evenimentul găzduiește competiții Capture the Flag (CTF), laboratoare și „sate tematice" dedicate unor domenii precum securitatea IoT, automotive, hardware, cloud, OSINT sau IA, oferind participanților posibilitatea de a lucra pe scenarii apropiate de mediul operațional[68]. Aceste activități contribuie la dezvoltarea competențelor tehnice aplicate, facilitează interacțiunea cu angajatori și specialiști din industrie și completează formarea academică prin experiență practică.

Tranziția de la formare la ocupare se face prin stagii, ca mecanism de testare reciprocă și infrastructură de absorbție a talentului. În privat, Bitdefender susține stagii plătite („Stagii pe Bune"), cinci centre de R&D și masterate co-dezvoltate cu universități din București, Cluj, Iași și Timișoara; Orange derulează locuri de practică pe componente operaționale (SOC, gestiunea vulnerabilităților) cu Politehnica București; târgurile de cariere indică internshipuri plătite (4.000 lei) și roluri de junior (5.000 lei). În public, Programul Oficial de Internship al Guvernului 2026 oferă 200 de locuri în 41 de organizații-gazdă (iulie–august), iar DNSC funcționează ca instituție-gazdă. Limitarea este de scară: numărul de stagii cu profil real de securitate rămâne mic raportat la cei aproximativ 80% dintre participanții la competiții care își doresc unul. Aici se produce prima îngustare serioasă a pâlniei.

5.5 Certificări și formare continuă

Certificările completează formarea universitară cu standarde internaționale și oferă rute de reconversie, făcând competențele lizibile și comparabile pentru angajatori. Cantitativ, nivelul e dominat de Cisco Networking Academy (peste 25 de ani de prezență și 163.000 de cursanți în total): aproximativ 93 de academii active, circa 14.600 de cursanți pe an. De asemenea este important de menționat faptul că 30% dintre cursanți și instructori sunt femei, ceea ce plasează România pe primul loc în UE la acest indicator. Se adaugă certificările Microsoft și ISC^2, tot mai des cerute în anunțuri, precum și componenta locală (rețeaua ECDL/ICDL de centre acreditate, ICI București, școli informale de IT). Relevanța e subliniată de un dezechilibru european: conform EuroBarometrului[69], circa trei sferturi dintre cei care ocupă roluri de securitate cibernetică în UE nu dețin calificări sau certificări formale în domeniu - formarea alternativă nu e accesoriu, ci una dintre principalele căi reale de intrare.

Un exemplu relevant de certificare alternativă, accesibilă și pan-europeană, este EITCA/IS (Information Technologies Security Academy)[70], parte a cadrului European IT Certification guvernat de Institutul EITCI, organizație non-profit cu sediul la Bruxelles. Programul este poziționat la nivelul 6 EQF[71] și grupează 12 certificări EITC individuale într-un curriculum de aproximativ 180 de ore, implementat integral online, fără condiții prealabile de acces și care poate fi parcurs în ritm propriu. Tematic, acoperă o gamă largă de subiecte, de la teoria complexității și criptografie (clasică și cuantică) la securitatea rețelelor, administrarea sistemelor și testarea de penetrare a aplicațiilor web. Accesibilitatea este susținută printr-o schemă de subvenționare asociată Digital Skills and Jobs Coalition (DSJC), care reduce substanțial costul de participare. Spre deosebire de certificările profesionale de nivel senior precum CISSP sau OSCP, EITCA/IS funcționează mai degrabă ca un strat de atestare fundamentală, vendor-neutră, util în special pentru semnalarea competențelor transferabile la intrarea în domeniu. Această poziționare îl încadrează firesc în logica rutelor alternative de formare, confirmând observația că, pentru o parte importantă a forței de muncă din domeniul securității cibernetice, certificarea neformală rămâne o cale reală de acces în profesie.

[68] https://def.camp/hacking-village/[Accesat la data de 2 iulie 2026].
[69] https://europa.eu/eurobarometer/surveys/detail/3176 [Accesat la data de 2 iulie 2026].
[70] https://eitca.org/how-it-works/ [Accesat la data de 2 iulie 2026].
[71] https://en.wikipedia.org/wiki/European_Information_Technologies_Certification_Academy [Accesat la data de 2 iulie 2026]

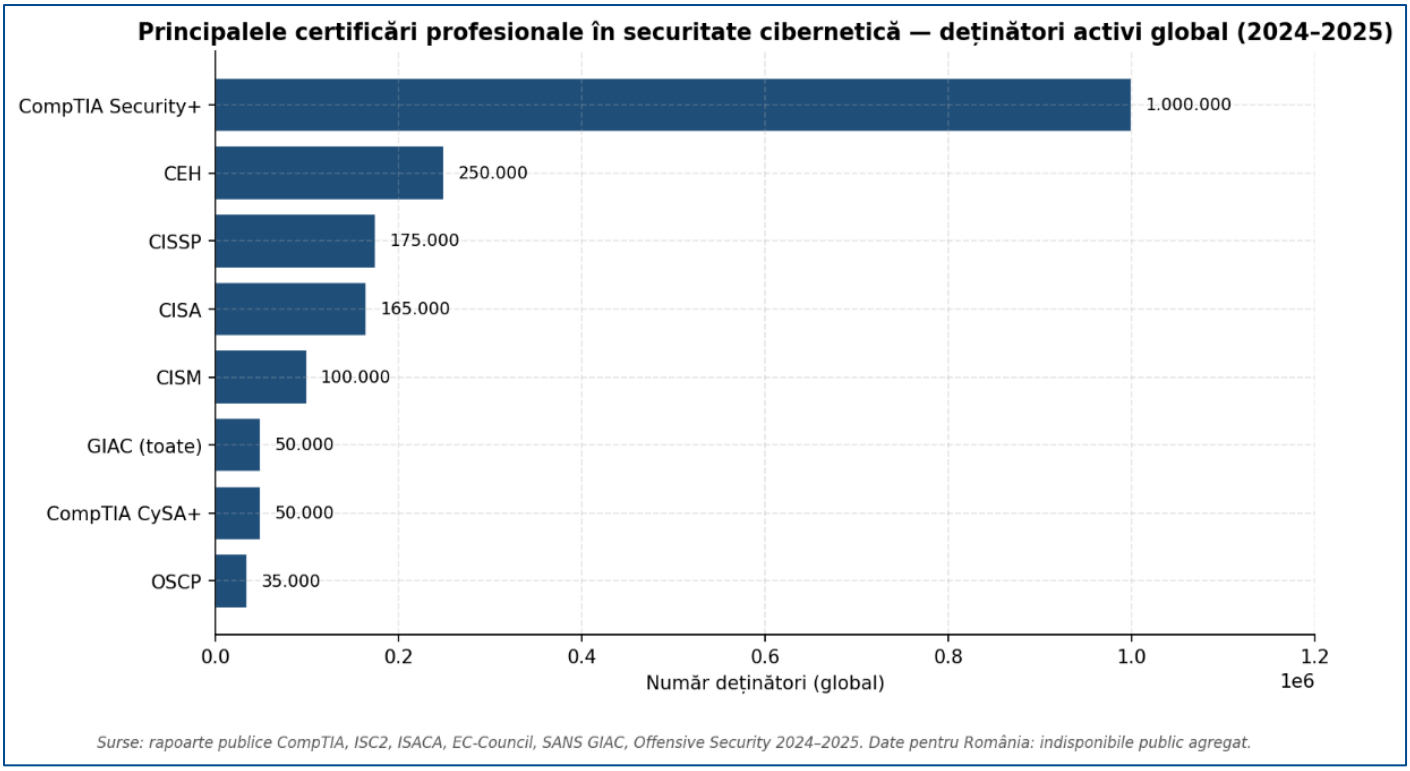


Figura 8. Distribuția globală a celor mai relevante certificări profesionale în securitate cibernetică

Figura 8 prezintă distribuția globală a celor mai relevante certificări profesionale în securitate cibernetică, iar lectura ei dezvăluie un decalaj direct relevant pentru adopția IA. Stocul global de competențe certificate este dominat de certificări profesionale consacrate precum Security+, CEH, CISSP, CISA și CISM, cu peste 1,6 milioane de titulari activi.

Tabel 4. Opțiuni de formare și certificare în securitate cibernetică

Categorie	Exemple	Caracteristici
Certificări profesionale	CISSP, CISM, CISA, CRISC, CEH, OSCP, Sec+, GIAC	Recunoaștere internațională; cost 300–2.000 EUR
Programe universitare RO	UPB (AC + Digital4Security), ASE, Babeș-Bolyai	60–120 ECTS; ARACIS; acoperă ECSF
Bootcamps	Furnizori locali, online (Cybrary, INE)	3–9 luni; cost variabil; intensitate ridicată
On-the-job	Programe interne angajatori	Mentorat; durată extinsă
Atestări EU online	EITCA/IS (EITCI, EQF 6)	12 certificări EITC, aproximativ 180 ore; integral online; subvenție DSJC

5.6 Stadiul adopției IA în SOC-urile din România

Certificările dedicate acestui domeniu abia încep să apară și nu au acumulat încă o masă critică de deținători. Cu alte cuvinte, în momentul în care organizațiile - inclusiv SOC-urile - încep să integreze IA în operațiuni, o fac cu o forță de muncă formată preponderent în paradigma anterioară acestui val tehnologic. Decalajul dintre competențele existente și cele necesare nu este, prin urmare, o problemă specific românească, ci una structurală, pe care contextul național doar o amplifică. La nivel global, 28% dintre organizații au integrat deja instrumente de IA în operațiunile de securitate, iar alte 41% se află în faze de

testare sau evaluare[72]; date comparabile la nivel UE sau regional nu sunt disponibile public în surse instituționale. Pe piața locală, furnizori precum Bitdefender (GravityZone PHASR, cu IA proprietară) și Safetech Innovations (platforma ThreatEcho, cu triaj asistat de IA) au integrat componente de IA în produsele proprii, iar mai mulți MSSP[73] autohtoni au inițiat pilotarea agenților de IA pentru operațiuni SOC. Adopția rămâne însă concentrată în jurul unui număr restrâns de actori maturi, fără a se fi generalizat la nivelul pieței.

Această tranziție pune o presiune directă asupra competențelor. Pe măsură ce instrumentele de IA pătrund în fluxurile SOC, profilul cerut analistului se deplasează de la execuția sarcinilor de rutină - tocmai cele automatizate - către validarea, integrarea și supravegherea sistemelor automatizate. Setul de competențe care devine prioritar pentru forța de muncă din domeniul securității cibernetice în era IA include:

- **AI/ML fundamentals** - înțelegerea modelelor de machine learning, a limitărilor lor și a modului în care se evaluează performanța.
- **Prompt engineering** - scrierea, testarea și optimizarea prompturilor pentru sisteme GenAI și agenți.
- **LLM integration** - conectarea modelelor mari de limbaj la aplicații, API-uri și fluxuri de business.
- **MLOps/model operations** - implementarea, monitorizarea, controlul versiunilor și întreținerea modelelor în producție.
- **Data engineering și data quality** - pregătirea datelor, pipeline-uri, curățare și guvernanță, întrucât performanța IA depinde de calitatea datelor.
- **AI security/model security** - protecția modelelor, a datelor și a sistemelor împotriva atacurilor, biasului și scurgerilor de informații.
- **AI governance și compliance** - managementul riscurilor, audit, etică și conformitate, în special în industrii reglementate.
- **Automation with AI tools** - utilizarea IA pentru codare asistată, testare, documentare, suport și analiză.

Dintre acestea, competențele de *AI security* și *AI governance* sunt cele care leagă cel mai direct adopția IA de mandatul de securitate, transformând integrarea IA dintr-un risc operațional necontrolat într-o capabilitate guvernată.

5.7 Implicații și strategii pentru angajatori

Din perspectiva angajatorilor, provocarea principală nu este lipsa totală a candidaților, ci decalajul dintre competențele disponibile și cele solicitate de piață. Analiza indică faptul că ecosistemul din România produce absolvenți, participanți la competiții și persoane certificate, însă numărul pozițiilor de intrare și al programelor de practică rămâne insuficient raportat la cererea generată de OUG 155/2024 și de transformarea digitală accelerată. În aceste condiții, strategiile bazate exclusiv pe recrutarea de specialiști deja formați devin din ce în ce mai costisitoare și mai puțin sustenabile.

Organizațiile sunt încurajate să trateze programele de internship, mentoring și dezvoltare internă drept mecanisme de construire a propriului pipeline de talente, nu doar instrumente de recrutare punctuală. Datele analizate sugerează că una dintre cele mai importante oportunități pentru angajatori este valorificarea bazei existente de candidați proveniți din competiții, comunități tehnice, programe universitare și rute alternative de formare, într-un context în care cererea pentru specialiști cu experiență depășește constant oferta disponibilă.

În paralel, se observă o deplasare graduală de la recrutarea bazată exclusiv pe diplome și experiență formală către evaluarea competențelor demonstrabile. Participarea la competiții, proiectele practice, certificările și experiența tehnică aplicată devin indicatori tot mai relevanți ai potențialului profesional, în special pentru rolurile de intrare și pentru domeniile emergente asociate IA.

[72] https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study [Accesat la data de 29 mai 2026].
[73] https://www.dnsc.ro/vezi/document/dnsc-raport-privind-piata-nationala-de-furnizori-de-servicii-de-securitate-gestionate [Accesat la data de 29 mai 2026].

Adoptarea IA modifică, totodată, profilul competențelor căutate. Accentul se deplasează progresiv de la executarea sarcinilor repetitive către capacitatea de validare, integrare și supraveghere a sistemelor automatizate. În acest context, investițiile în alfabetizare IA, utilizarea responsabilă a sistemelor generative și dezvoltarea competențelor de *AI Security*, guvernanță și conformitate pot reprezenta un avantaj competitiv semnificativ. Pe termen mediu, diferența dintre organizații nu va fi determinată exclusiv de accesul la tehnologie, ci de capacitatea acestora de a dezvolta și reține personal capabil să utilizeze tehnologiile AI în condiții de siguranță, eficiență și conformitate.

O observație interesantă rezultată din analiza principalelor platforme de recrutare din România (LinkedIn Jobs, eJobs, BestJobs și Hipo) este reprezentarea relativ redusă a rolurilor care solicită explicit competențe asociate inteligenței artificiale. În ciuda atenției acordate public IA-ului și a volumului ridicat de investiții și discuții din ultimii doi ani, numărul de poziții care menționează în mod direct competențe precum LLM engineering, *AI Governance*, *AI Security*, *Human-AI Teaming* sau *MLOps* rămâne limitat în comparație cu rolurile tradiționale din IT și securitate cibernetică.

Această observație nu trebuie interpretată automat ca o lipsă a adopției IA. Dimpotrivă, există numeroase indicii că organizațiile utilizează deja sisteme bazate pe IA pentru automatizarea proceselor, generarea de conținut, analiză, asistență operațională sau suport decizional. O explicație posibilă este că, pentru majoritatea organizațiilor, valoarea imediată a IA nu derivă din dezvoltarea de modele proprii, ci din integrarea unor servicii și platforme existente în procesele de lucru curente. În acest scenariu, competențele asociate IA sunt absorbite gradual în roluri deja existente (dezvoltatori software, analiști SOC, specialiști GRC, arhitecți cloud, administratori de platforme), fără a genera imediat o categorie distinctă și vizibilă de ocupații.

Din această perspectivă, piața muncii poate reflecta cu întârziere transformările produse de IA. Adoptarea tehnologică poate evolua mai rapid decât actualizarea fișelor de post, a organigramelor și a mecanismelor de recrutare.

Pentru angajatori, o primă implicație strategică este necesitatea formalizării utilizării IA în cadrul organizației: identificarea proceselor în care aceste sisteme sunt deja folosite, definirea responsabilităților, dezvoltarea competențelor interne și integrarea mecanismelor de guvernanță și control. În absența acestora, fenomenul cunoscut sub denumirea de *Shadow AI* – utilizarea informală sau insuficient guvernată a instrumentelor IA de către angajați – poate deveni mai răspândit decât sugerează structurile organizaționale și anunțurile de recrutare.

O a doua implicație privește reziliența operațională. Organizațiile care își restructurează procesele și forța de muncă pe baza utilizării unor servicii IA externe (comerciale) trebuie să ia în calcul și riscurile asociate dependenței de furnizori, modificărilor comerciale, constrângerilor de acces, cerințelor de conformitate sau schimbărilor de reglementare. Similar altor servicii digitale critice, utilizarea IA ar trebui însoțită de planuri de continuitate, mecanisme alternative de lucru și păstrarea competențelor umane necesare pentru operarea proceselor esențiale. Pe termen mediu, avantajul competitiv nu va deriva exclusiv din accesul la tehnologie, ci din capacitatea organizațiilor de a integra, securiza și guverna aceste sisteme într-un mod sustenabil.

6. Riscuri și provocări strategice

6.1 Riscuri operaționale

Deficitul structural de specialiști în IT și securitate cibernetică amplifică dificultățile de recrutare și retenție, generează presiune salarială constantă, prelungește timpul de ocupare a posturilor cu experiență și crește dependența organizațiilor de un număr limitat de experți. La nivel global, necesarul de forță de muncă a crescut cu aproximativ 8% într-un an, conform studiului ISC2 din 2024[74], iar în piețe europene mature precum Germania deficitul s-a adâncit cu circa 15% într-un singur an, pe fondul noilor cerințe de reglementare, în timp ce forța de muncă activă a stagnat. Această divergență, cerere în creștere peste o ofertă aproape constantă, este motorul deficitului structural.

6.2 Riscuri juridice și de răspundere

[74] https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study [Accesat la data de 29 mai 2026].

Deficitul de competențe și adoptarea accelerată a soluțiilor bazate pe IA sporesc riscul de neconformitate cu cerințele legislative și de apariție a unor situații în care responsabilitatea pentru deciziile asistate de IA nu este clar delimitată. Utilizarea IA în SOC fără un cadru clar de responsabilitate ridică probleme de imputabilitate atunci când agentul IA ia decizii eronate. În măsura în care sistemul de IA este clasificat ca fiind cu risc ridicat, conformitatea cu Art. 4 (alfabetizare IA), Art. 14 (supraveghere umană) și Art. 15 (acuratețe, robustețe și securitate) din AI Act[75] devine obligatorie; obligația de alfabetizare IA (Art. 4) se aplică, însă, transversal.

În același timp, presiunea exercitată asupra organizațiilor de a implementa rapid cerințele directivei NIS2 transferă responsabilități directe către organele de conducere. Răspunderea conducerii este consacrată de Art. 20[76] din Directiva NIS2, transpus în legislația națională prin OUG nr. 155/2024, care impune organelor de conducere ale entităților esențiale și importante să aprobe și să supravegheze măsurile de management al riscurilor de securitate cibernetică și să urmeze formare în domeniu, sub sancțiunea răspunderii personale. Suplimentar, pentru entitățile esențiale, este prevăzută, ca măsură de ultimă instanță aplicabilă până la remedierea deficiențelor, posibilitatea interzicerii temporare a exercitării funcțiilor de conducere de către persoanele cu responsabilități la nivel de director executiv sau reprezentant legal (Art. 32(5)(b) NIS2).

6.3 Riscuri de calitate și amenințări emergente

Accelerarea adopției IA și presiunea asupra dezvoltării rapide a competențelor amplifică atât riscurile privind calitatea capitalului uman, cât și expunerea la amenințări emergente. Rapoartele ENISA atrag atenția că certificările formale nu echivalează cu competențele reale. Programele bazate pe examen pot fi promovate fără experiență practică relevantă.

În paralel, utilizarea pe scară tot mai largă a IA favorizează apariția unor noi categorii de amenințări, precum adversarial ML, LLM malware și prompt injection, clasat pentru al doilea an consecutiv pe primul loc în OWASP Top 10 for LLM Applications[77].

Impactul acestor amenințări este deja vizibil și în plan financiar: în cazul Arup[78] (ianuarie 2024), o videoconferință falsificată prin tehnologia deepfake a determinat transferul fraudulos a 25,6 milioane USD, unul dintre cele mai importante incidente documentate de acest tip.

6.4 Riscuri privind reziliența cibernetică

Deficitul de specialiști și dificultățile de retenție pot afecta capacitatea organizațiilor de a preveni, detecta și răspunde eficient la incidente de securitate cibernetică. Reducerea oportunităților de formare pentru personalul aflat la început de carieră, combinată cu dependența tot mai mare de instrumente bazate pe IA, poate conduce la diminuarea expertizei operaționale și la creșterea riscului de configurări eronate, răspuns întârziat la incidente și utilizare necorespunzătoare a tehnologiilor emergente. În contextul extinderii obligațiilor impuse de Directiva NIS2, aceste vulnerabilități pot afecta reziliența cibernetică atât la nivel organizațional, cât și la nivel național.

7. Tendințe și prognoze

7.1 Evoluția pieței și integrarea rolurilor IA generative

Analiza tendințelor actuale sugerează că impactul IA asupra pieței muncii nu se va manifesta predominant prin apariția unui număr mare de profesii complet noi, ci prin transformarea graduală a rolurilor existente. Deși discursul public este dominat de concepte precum AI Engineer, Prompt Engineer sau LLM Specialist, datele din piața muncii indică o evoluție diferită: competențele asociate IA sunt integrate progresiv în ocupații deja consacrate din dezvoltare software, securitate cibernetică, analiză de date, cloud și guvernanță. În consecință, este probabil ca următorii ani să fie caracterizați mai degrabă de proliferarea profilurilor hibride decât de apariția unor categorii profesionale complet separate.

Pe măsură ce utilizarea IA se extinde, competențele asociate acesteia tind să devină o componentă transversală a activității profesionale. Similar modului în care utilizarea internetului, a serviciilor cloud

[75] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689 [Accesat la data de 29 mai 2026].
[76] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555 [Accesat la data de 29 mai 2026].
[77] https://genai.owasp.org/llmrisk/llm01-prompt-injection/ [Accesat la data de 29 mai 2026].
[78] https://www.cnn.com/2024/05/16/tech/arup-deepfake-scam-loss-hong-kong-intl-hnk [Accesat la data de 29 mai 2026].

sau a instrumentelor Office a devenit o competență de bază pentru majoritatea profesiilor digitale, utilizarea sistemelor IA și capacitatea de validare a rezultatelor generate automat sunt susceptibile să devină competențe standard pentru o parte semnificativă a forței de muncă din IT și securitate cibernetică. Diferențierea competitivă se va muta gradual de la simpla utilizare a instrumentelor către capacitatea de evaluare critică, integrare și supraveghere a acestora.

În paralel, extinderea utilizării IA este de așteptat să genereze o cerere crescută pentru competențe asociate controlului, securității și guvernanței. Cerințele introduse prin AI Act, Directiva NIS2, DORA și alte inițiative europene vor favoriza dezvoltarea unor roluri orientate spre AI Security, AI Governance, Model Risk Management, audit și conformitate. Aceste roluri nu vor exista izolat, ci vor apărea în principal ca extensii ale funcțiilor deja existente de securitate, risc, conformitate și management tehnologic.

Transformarea cea mai vizibilă este probabil să apară la nivelul rolurilor de intrare în profesie (respectiv rolurile de nivel junior). Activitățile repetitive utilizate tradițional pentru formarea juniorilor se află printre cele mai expuse automatizării, ceea ce poate reduce eficiența traseelor clasice de dezvoltare profesională bazate pe acumularea graduală de experiență operațională. În acest context, competițiile tehnice, laboratoarele practice, simulările, programele de mentorat și modelele accelerate de formare vor dobândi o importanță tot mai mare în procesul de pregătire a noilor generații de specialiști.

În ansamblu, IA pare să funcționeze mai degrabă ca o *tehnologie de infiltrare* decât ca una de substituție. În loc să creeze o categorie complet nouă de profesii, aceasta modifică progresiv conținutul majorității rolurilor existente, schimbând competențele necesare, modul de lucru și relația dintre om și tehnologie. Din această perspectivă, principala provocare a următorilor ani nu va fi apariția unor profesii complet noi, ci adaptarea accelerată a celor deja existente.

Tabel 5. Impactul automatizării și al AI asupra rolurilor IT și cybersecurity până în 2030

Domeniu	Tendință până în 2030	Impact probabil
IA/data/cloud	Creștere puternică	Creștere netă mare de joburi
Cybersecurity avansat	Creștere puternică	Cerere mai mare pentru seniori și roluri hibride
SOC și operațiuni IT	Automatizare parțială	Mai puține sarcini manuale, roluri mai analitice
Helpdesk/suport repetitiv	Automatizare ridicată	Creștere mică sau stagnare
Sarcini administrative simple	Automatizare ridicată	Risc de reducere semnificativă

7.2 Scenarii de evoluție pentru România

Orizontul 2027–2030 este caracterizat de un grad ridicat de incertitudine, determinat atât de ritmul implementării inițiativelor europene și naționale de dezvoltare a competențelor (PNRR, Digital Europe Programme, EU-INSPIRE), cât și de viteza cu care organizațiile private vor adopta și integra noile cerințe generate de Directiva NIS2, AI Act și transformarea accelerată a pieței muncii. În acest context, prognoza exactă a dimensiunii forței de muncă din domeniul securității cibernetice este dificilă, motiv pentru care analiza utilizează o abordare bazată pe scenarii.

Scenariile prezentate nu reprezintă predicții, ci traiectorii plauzibile construite pornind de la ipoteze diferite privind creșterea ofertei de specialiști, absorbția absolvenților, retenția personalului și evoluția cererii. Elementul comun tuturor scenariilor este menținerea unei cereri ridicate de competențe în securitate cibernetică, alimentată simultan de presiunile de reglementare, digitalizarea accelerată și integrarea tehnologiilor bazate pe IA.

Figura 10 ilustrează evoluția estimată a forței de muncă din domeniul securității cibernetice din România până în 2030, comparativ cu cererea proiectată, precum și dimensiunea deficitului care persistă în toate

scenariile analizate. Chiar și în ipoteza favorabilă, ritmul de creștere a ofertei rămâne inferior ritmului de creștere al cererii, ceea ce sugerează că problema deficitului de competențe nu va fi eliminată în intervalul analizat, ci doar atenuată.

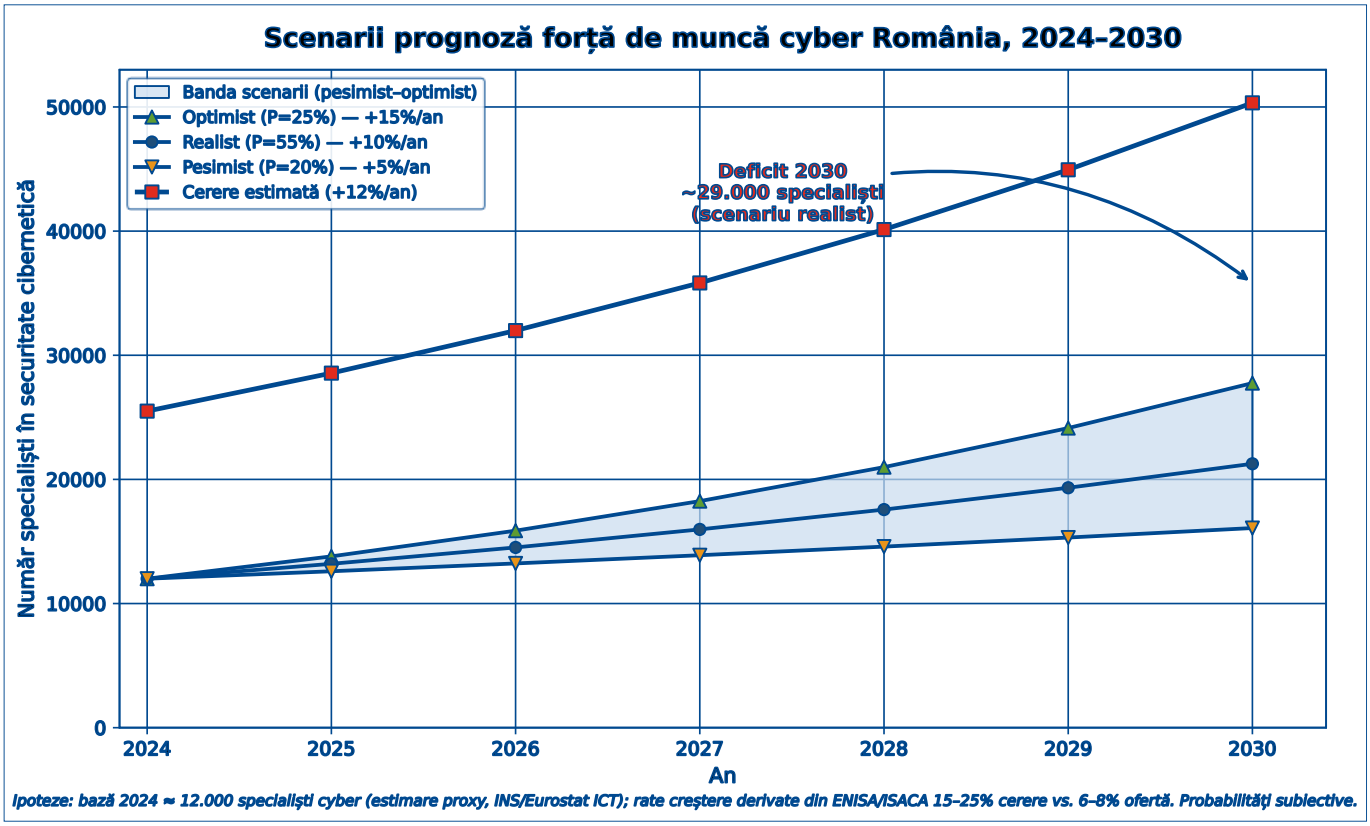


Figura 10. Scenarii de prognoză pentru forța de muncă din domeniul securității cibernetice în România (orizont 2030)

Scenariul optimist (P=25%): rată de creștere 15%/an a ofertei (datorită PNRR și DEP), absorbție 80% a absolvenților, asumare integrală a Directivei NIS2 de către sectorul privat. Numărul de specialiști din domeniul securității cibernetice depășește 24.000 până în 2030, deficitul scade sub 15.000. Investițiile externe în centre de excelență cresc, salariile se apropie de 70% din media UE (PPP).

Scenariul realist (P=55%): rată de creștere 10%/an, implementarea parțială a PNRR (acoperire 70% formatori până la termen), cerere +12%/an. Forța de muncă din domeniul securității cibernetice atinge ~19.000 în 2030, cu deficit între 21.000 și 35.000. România rămâne sub media UE, dar în trend ascendent.

Scenariul pesimist (P=20%): rată de creștere 5%/an, întârzieri majore PNRR, intensificarea migrației externe. Deficitul depășește 40.000, conformarea cu Directiva NIS2 se realizează preponderent prin furnizori externi MSSP. Riscul de pierdere a contractelor strategice (apărare, infrastructuri critice) este semnificativ.

Orizontul 2027–2030 conturează o evoluție cu trei traiectorii principale pentru România. În scenariul realist, deficitul de specialiști din domeniul securității cibernetice se va stabiliza între 21.000 și 35.000 de posturi, în funcție de eficiența programelor PNRR și EU-INSPIRE, precum și de capacitatea universităților de a absorbi cererea.

Deși valorile absolute diferă semnificativ între scenarii, toate conduc către aceeași concluzie: principala provocare pentru România nu este generarea cererii, ci **capacitatea de a transforma interesul existent** pentru domeniu în specialiști operaționali și de a reține personalul cu experiență. În acest sens, diferența dintre scenarii este determinată mai puțin de evoluția tehnologiei și mai mult de eficiența politicilor de formare, retenție și integrare a forței de muncă.

Notă metodologică. Proiecția reprezintă o analiză de scenarii cu probabilități subiective, nu o prognoză univocă. Nivelul de bază pentru 2024 este un proxy derivat din ponderea specialiștilor ICT în ocuparea totală (Eurostat[79]), restrâns la rolurile din domeniul securității cibernetice și triangulat cu estimări

[79] https://ec.europa.eu/eurostat/databrowser/view/isoc_sks_itspt/default/bar?lang=en [Accesat la data de 2 iulie 2026].

independente. Linia cererii aplică definiția ISC2 a deficitului de forță de muncă (necesar pentru securizare adecvată, nu vacanțe deschise), cu un raport necesar/existent calibrat pe valoarea globală ISC2. Ratele de ofertă (5/10/15%) încadrează rata medie istorică de creștere a ocupării ICT în UE (~4,8%/an, Eurostat), cu scenariile superioare reflectând ipoteza unei creșteri accelerate în domeniul securității cibernetice sub efectul intervențiilor de politică (PNRR, Digital Europe Programme). Probabilitățile (25/55/20%) sunt estimări de judecată. Scenariile prezentate au caracter exploratoriu și au fost elaborate prin combinarea judecății expertului cu ipoteze de lucru, repere statistice disponibile și instrumente de analiză asistată digital, motiv pentru care trebuie interpretate ca exerciții de orientare strategică, nu ca predicții deterministe.

8. Concluzii și recomandări

Traseul românesc este funcțional, dar selectiv, și e mai degrabă un sistem interdependent decât o succesiune rigidă: inserția profesională depinde tot mai puțin de o singură acreditare și tot mai mult de combinarea educației, practicii, validării și experienței. Privit ca pâlnie, pipeline-ul nu suferă de lipsă de structură - etajele există, iar unele (lanțul competițional) funcționează exemplar - ci de **debit și retenție**: oferta de competențe crește mai lent decât cererea, securitatea cibernetică nu este urmărită distinct în statisticile pieței muncii, oportunitățile de practică relevantă rămân limitate, accesul în profesie s-a îngustat în 2026, iar emigrarea continuă să reducă baza de specialiști cu experiență. Directiva NIS2 nu atenuează deficitul în timp, ci îl face urgent acum. Implicația de politică publică este dublă: scalarea etajelor de internship și formare alternativă (singurele care operează juniorii rapid) plus dezagregarea statistică a fluxului de absolvenți din domeniul securității cibernetice, respectiv măsuri de retenție (fiscale, salariale, de mediu de lucru). Un pipeline nu se repară doar lărgindu-i gura, ci și astupându-i scurgerile.

8.1 Sinteza concluziilor

Raportul conduce spre șase concluzii principale:

- Transformare structurală, nu contracție. Piața forței de muncă din domeniul securității cibernetice traversează o restructurare generată simultan de IA și de noul cadru de reglementare UE (Directiva NIS2, AI Act, CRA, Cyber Solidarity Act). IA nu golește piața, ci o polarizează: reduce cererea pentru rolurile de rutină și de intrare și o amplifică pentru rolurile complexe de integrare, guvernanță și apărare activă.
- Fragilitate structurală cu un paradox. România are unul dintre cele mai mari decalaje relative din UE (2,8% specialiști ICT din populația ocupată, față de 5,0% media UE), dar simultan una dintre cele mai ridicate ponderi de femei în ICT din Uniunea Europeană. Baza de formare este decentă; pierderea se produce la nivelurile de experiență, prin emigrare și prin muncă la distanță pentru angajatori străini.
- Impact diferențiat al IA. Automatizarea afectează cel mai puternic rolurile de intrare (SOC L1/L2, unde 40–80% dintre sarcini devin automatizabile), erodând traseul clasic de formare a juniorilor, dar generează cinci roluri noi cu salarii premium: AI Security Engineer, AI Red Teamer, MLSecOps Engineer, Prompt Security Analyst și AI Governance Officer.
- Directiva NIS2 transformă deficitul latent în deficit acut. Obligațiile Directivei NIS2 (transpuse prin OUG 155/2024) vizează 10,000 de entități esențiale și importante[80], cu cerință de certificare a conducerii în 12 luni, generând o cerere imediată de formare.
- O fereastră de oportunitate de 3–5 ani, condiționată de execuție. PNRR (componenta C7-I15, 25 milioane EUR pentru 5.000 de formatori, coordonata de **Ministerul Cercetării, Inovării și Digitalizării (MCID)**[81]) aduce finanțare directă pentru formarea la nivel național, iar participarea la proiectul european EU-INSPIRE (buget total 19,48 milioane EUR, din care 9,64 milioane EUR finanțare UE, consorțiu de 23 de parteneri cu DNSC ca partener) contribuie prin transfer de

[80] https://agerpres.ro/economic/2026/03/16/dinu-dnsc-piata-romaneasca-de-securitate-cibernetica-estimata-la-circa-200-de-milioane-de-euro-este---1537682 [Accesat la data de 18 iulie 2026].
[81] https://www.fonduri-easi.ro/fisa-proiect/23/planul-national-de-redresare-si-rezilienta/603/c7-i15-crearea-de-noi-competente-de-securitate-cibernetica-pentru-societate-si-economie-consultare-publica [Accesat la data de 2 iulie 2026].

curriculum și acreditare. Valorificarea acestei ferestre depinde de execuția efectivă, nu doar de alocare.

- Miza strategică este suveranitatea digitală. Ratarea acestei ferestre ar consolida decalajul față de țintele Digital Decade 2030 și ar adânci dependența de furnizori MSSP externi pentru conformarea cu Directiva NIS2 și CRA, cu consecințe directe asupra sectoarelor de apărare și infrastructură critică.

Analiza principalelor platforme de recrutare din România (LinkedIn Jobs, eJobs, BestJobs, Hipo) relevă o discrepanță aparentă: numărul pozițiilor care solicită explicit competențe precum LLM engineering, AI Governance, AI Security, Human-AI Teaming sau MLOps rămâne redus, iar multe organizații recrutează în continuare pe profiluri tradiționale. Această absență nu trebuie interpretată ca lipsă a adopției IA. Dimpotrivă, organizațiile, publice și private, utilizează deja sisteme IA în activitatea curentă, de la automatizarea proceselor și instrumente de tip copilot până la generarea de analize și recomandări operaționale, uneori formal și guvernat, alteori informal și insuficient controlat, fenomen cunoscut sub numele de *Shadow AI*.

Ipoteza centrală a raportului este că adopția tehnologică a IA depășește semnificativ adopția instituțională, adică viteza cu care organizațiile își adaptează structurile, politicile, mecanismele de guvernanță și practicile de recrutare. Consecința este paradoxală: o organizație poate utiliza IA pe scară largă fără a crea roluri dedicate, fără a modifica fișele de post și fără mecanisme adecvate de responsabilitate și verificare, situație în care *Shadow AI* devine comportamentul implicit, nu excepția. Riscurile asociate, de securitate, de conformitate și de tip *confabulație* (generarea de conținut plauzibil, dar incorect, documentată în literatura de specialitate), sunt descoperite de regulă abia după adoptare. Piața muncii și structurile instituționale par să reprezinte ultimul nivel al transformării, în timp ce tehnologia a modificat deja procesele și modul de lucru.

Dacă ipoteza este corectă, provocarea majoră a următorilor ani nu va fi adopția IA în sine, ci reducerea acestui decalaj.

8.2 Recomandări strategice pentru mediul privat

Pentru angajatori, provocarea principală nu este lipsa totală a candidaților, ci decalajul dintre competențele disponibile și cererea pieței, în condițiile în care recrutarea exclusiv de specialiști deja formați devine tot mai costisitoare și mai puțin sustenabilă. Din analiză rezultă cinci direcții de acțiune.

1. **Reskilling intern ca sursă primară de talent.** Reorientarea personalului IT existent spre roluri de securitate cibernetică, prin programe sponsorizate de certificare, este de regulă mai eficientă decât recrutarea externă, în special pentru rolurile L3–L4, unde oferta de piață este cea mai rară. Raportul propune ca obiectiv acoperirea a 25% din necesarul nou de specialiști prin reconversie internă în următorii trei ani - o țintă conservatoare, având în vedere că 34% dintre rolurile de securitate cibernetică la nivel european sunt deja ocupate prin tranziții din alte domenii[27]. Datele de retenție întăresc urgența: 28% dintre profesioniști au luat în calcul schimbarea carierei, iar probabilitatea declarată de a rămâne în organizația actuală scade de la 75% pe orizontul de un an la 66% pe doi ani[9], dezvoltarea internă fiind astfel o necesitate, nu o opțiune.
2. **Parteneriate educaționale duale.** Combinarea universităților (Universitatea Politehnica București, Academia de Studii Economice, Universitatea Babeș-Bolyai, UVT), a furnizorilor de bootcamp și a celor acreditați de DNSC oferă un canal de formare mai rapid și mai adaptat decât recrutarea punctuală, și devine necesară pentru conformarea cu Directiva NIS2 și AI Act.
3. **Adoptarea ECSF ca referențial.** Utilizarea cadrului ECSF pentru descrierile de posturi, planurile de carieră și evaluarea performanței aduce lizibilitate și comparabilitate competențelor, facilitând atât recrutarea, cât și mobilitatea internă.
4. **Tratarea internshipului ca infrastructură, nu ca recrutare punctuală.** Programele de internship, mentorat și dezvoltare internă construiesc propriul pipeline de talente. Cea mai valoroasă resursă subutilizată o reprezintă baza existentă de candidați din competiții, comunități tehnice și rute alternative de formare, într-un context în care cererea pe roluri cu experiență depășește constant oferta.
5. **Asigurarea participării active și a sustenabilității contribuției DNSC la proiectul european EU-INSPIRE** (consorțiu de 23 de parteneri, formare la nivel de master în securitate cibernetică și IA),

cu valorificarea transferului de curriculum și a mecanismelor de acreditare la nivel național după încheierea proiectului în 2028.

În paralel, se observă o deplasare de la recrutarea bazată exclusiv pe diplome și experiență formală către evaluarea competențelor demonstrabile, participarea la competiții, proiectele practice și certificările devenind indicatori tot mai relevanți ai potențialului, în special pentru rolurile de intrare și pentru domeniile emergente asociate IA.

8.3 Recomandări pentru instituțiile publice și guvernamentale

Pentru sectorul public, recomandările vizează atât valorificarea ferestrei de finanțare, cât și corectarea limitărilor structurale și metodologice identificate în raport.

1. **Program național coordonat de upskilling și reskilling**, construit pe experiența Investiției I15 din PNRR (25 de milioane de euro, 1.126 de organizații autoevaluate pe cadrul CyFun până în iunie 2026) și continuat prin Programul Europa Digitală. Ciclul PNRR se închide la 31 august 2026, iar DEP expiră la finalul lui 2027, ceea ce face din acoperirea intervalului până la operaționalizarea Fondului European pentru Competitivitate, din 2028, prima condiție de continuitate. Constrângerea nu este alocarea, ci execuția: la 95% din perioada de implementare a PNRR, România îndeplinise circa 61% din jaloane și ținte. Extinderea raportării publice existente pe proiecte.pnrr.gov.ro cu indicatori de competențe transformă transparența progresului în instrument de disciplină a implementării.
2. **Integrarea ECSF și a cadrului NICE în curriculele universitare** din învățământul tehnic și economic, pentru a alinia formarea la rolurile reale de pe piață și a reduce decalajul dintre absolvire și operaționalizare.
3. **Finanțarea formării formatorilor pentru cerințele Directivei NIS2 și standardizarea Deciziei DNSC** (aflată în consultare publică din 17 iunie 2026), pentru a evita fragmentarea pieței de certificare și apariția unor standarde paralele, neomogene.

9. Bibliografie

[1] Parlamentul European și Consiliul UE, "Directiva (UE) 2022/2555 - DIRECTIVA NIS2," 2022. Disponibil: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

[2] Parlamentul European și Consiliul UE, "Regulamentul (UE) 2024/1689 - AI Act," 2024. Disponibil: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689

[3] Parlamentul European și Consiliul UE, "Regulamentul (UE) 2024/2847 - Cyber Resilience Act," 2024. Disponibil: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2847

[4] Parlamentul European și Consiliul UE, "Regulamentul (UE) 2025/38 - Cyber Solidarity Act," 2025. Disponibil: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32025R0038

[5] Guvernul României, "OUG nr. 155/2024," Monitorul Oficial, 2024. Disponibil: http://www.upt.ro/img/files/legislatie/2024/OUG_155_2024.pdf

[6] Guvernul României, "Strategia de Securitate Cibernetică a României 2022–2027," 2022. Disponibil: https://securitatea-cibernetica.ro/documente/Strategia-de-securitate-cibernetica-a-Romaniei.pdf

[7] ENISA, "European Cybersecurity Skills Framework (ECSF)," 2022. Disponibil: https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf

[8] ENISA, "2024 Report on the State of Cybersecurity in the Union," dec. 2024. Disponibil: https://www.enisa.europa.eu/publications/2024-report-on-the-state-of-the-cybersecurity-in-the-union

[9] ENISA, "NIS Investments 2024," nov. 2024. Disponibil: https://www.enisa.europa.eu/sites/default/files/2024-11/CSPA%20-%20NIS%20Investments%20-%202024_0.pdf

[10] ENISA, "ENISA Threat Landscape 2024," sept. 2024. Disponibil: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[11] ISC2, "Cybersecurity Workforce Study 2024," oct. 2024. Disponibil: https://www.isc2.org/Insights/2024/10/ISC2-Workforce-Study-AI-Growth-Opportunity

[12] ISC2, "Cybersecurity Workforce Study 2025," dec. 2025. Disponibil: https://www.isc2.org/Insights/2025/12/2025-ISC2-Cybersecurity-Workforce-Study

[13] OECD, "Building a Skilled Cyber Security Workforce in Europe," 2024. Disponibil: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/02/building-a-skilled-cyber-security-workforce-in-europe_6abaf769/3673cd60-en.pdf

[14] OECD, "Employment Outlook 2023 - AI and the Labour Market," 2023. Disponibil: https://www.oecd.org/content/dam/oecd/en/publications/reports/2023/07/oecd-employment-outlook-2023_904bcef3/08785bba-en.pdf

[15] OECD, "Who Will Be the Workers Most Affected by AI?," oct. 2024. Disponibil: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/10/who-will-be-the-workers-most-affected-by-ai_fb7fcccd/14dc6f89-en.pdf

[16] Eurostat, "ICT specialists in employment - DDN-20250708-2," iul. 2025. Disponibil: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250708-2

[17] Eurostat, "Towards Digital Decade targets for Europe," 2024. Disponibil: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Towards_Digital_Decade_targets_for_Europe

[18] WEF, "Future of Jobs Report 2025," ian. 2025. Disponibil: https://www.weforum.org/publications/the-future-of-jobs-report-2025/

[19] WEF, "Global Cybersecurity Outlook 2025," ian. 2025. Disponibil: https://www.weforum.org/publications/global-cybersecurity-outlook-2025/

[20] NIST, "Workforce Framework for Cybersecurity (NICE Framework) - SP 800-181 Rev.1," nov. 2020. Disponibil: https://csrc.nist.gov/pubs/sp/800/181/r1/final

[21] NIST, "AI Risk Management Framework 1.0," ian. 2023. Disponibil: https://www.nist.gov/itl/ai-risk-management-framework

[22] Gartner/Cynet, "Hype Cycle for Security Operations 2025," 2025. Disponibil: https://www.cynet.com/blog/gartner-hype-cycle-2025-cybersecurity-ai-assistants-and-ai-soc-agents/

[23] Forrester, "AI Job Impact Forecast US 2025–2030," 2025. Disponibil: https://www.forrester.com/report/the-forrester-ai-job-impact-forecast-us-2025-2030/RES190071

[24] MarketsandMarkets, "AI in Cybersecurity Market Report," 2025. Disponibil: https://www.marketsandmarkets.com/Market-Reports/artificial-intelligence-in-cybersecurity-market-224985247.html

[25] OWASP, "Top 10 for LLM Applications 2025 - LLM01 Prompt Injection," 2025. Disponibil: https://genai.owasp.org/llmrisk/llm01-prompt-injection/

[26] Microsoft, "Digital Defense Report 2024," 2024. Disponibil: https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024

[27] KELA, "2025 AI Threat Report," 2025. Disponibil: https://info.kela.com/hubfs/Reports/KELA%20Report%20-%202025%20AI%20Threat%20Report.pdf

[28] DeepStrike, "Deepfake Statistics 2025," 2025. Disponibil: https://deepstrike.io/blog/deepfake-statistics-2025

[29] FBI IC3/Ninjio, "FBI IC3 2025 Report Summary," 2025. Disponibil: https://ninjio.com/blog/fbi-why-85-of-cybercrime-losses-in-2025-point-to-a-human-problem/

[30] Comisia Europeană, "EU Cybersecurity Skills Academy," 2023. Disponibil: https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy

[31] Comisia Europeană, "Pact for Skills - Digital Skills Platform," 2020. Disponibil: https://digital-skills-jobs.europa.eu/en/initiatives/european-initiatives/pact-skills

[32] MCID/Fonduri Easi, "PNRR C7-I15 DNSC - Fișa proiect," 2024. Disponibil: https://www.fonduri-easi.ro/fisa-proiect/23/planul-national-de-redresare-si-rezilienta/603/c7-i15-crearea-de-noi-competente-de-securitate-cibernetica-pentru-societate-si-economie-consultare-publica

[33] Agerpres, "România implementează proiectul EU-INSPIRE," iul. 2025. Disponibil: https://agerpres.ro/english/2025/07/10/romania-implementing-project-to-bridge-cybersecurity-skills-gap--1467354

[34] UPB, "Advanced Cybersecurity - Master of Science," 2024. Disponibil: https://international.upb.ro/admission/study-offers/program/advanced-cybersecurity

[35] Digital4Security, "UPB Hybrid Master in Cybersecurity Management," 2024. Disponibil: https://www.digital4security.eu/hybrid-masters/

[36] OSGG, "Regulament 559/2021 - Atestare auditori SC," 2021. Disponibil: https://www.universuljuridic.ro/regulamentul-pentru-atestarea-si-verificarea-auditorilor-de-securitate-cibernetica-prezentare-generala-osgg-nr-559-2021/

[37] Clujit.ro, "Analiză DNSC Draft Rules 2026," 2026. Disponibil: https://www.clujit.ro/Directiva NIS2-in-romania-how-dnscs-draft-rules-shape-cybersecurity/

[38] Research and Markets, "Romania Cybersecurity Market Share Analysis," 2025. Disponibil: https://www.researchandmarkets.com/reports/5997117/romania-cybersecurity-market-share-analysis

[39] Dropzone AI/CSA, "SOC Analyst AI Perception Study (148)," 2026. Disponibil: https://www.dropzone.ai/blog/soc-analysts-ai-perception-148-study

[40] Palo Alto Networks, "Security Operations in 2025 and Beyond," dec. 2024. Disponibil: https://www.paloaltonetworks.com/blog/2024/12/security-operations-in-2025-and-beyond/

Anexe

Anexa 1 - Acronime și abrevieri

AI - Artificial Intelligence (inteligența artificială; termenul englez, folosit în compuși precum AI Act, AI Security)

AI Act - Artificial Intelligence Act (Regulamentul UE 2024/1689 privind inteligența artificială)

ANIS - Asociația Patronală a Industriei de Software și Servicii (România)

ANSSI - Asociația Națională pentru Securitatea Sistemelor Informatice

ARACIS - Agenția Română de Asigurare a Calității în Învățământul Superior

ASE - Academia de Studii Economice din București

BVB - Bursa de Valori București

CAGR - Compound Annual Growth Rate (rată de creștere anuală compusă)

CEH - Certified Ethical Hacker

CISA - Certified Information Systems Auditor

CISM - Certified Information Security Manager

CISO - Chief Information Security Officer (director de securitate a informației)

CISSP - Certified Information Systems Security Professional

CompTIA - Computing Technology Industry Association (asociație profesională IT)

CRA - Cyber Resilience Act (Regulamentul UE 2024/2847 privind reziliența cibernetică)

CRISC - Certified in Risk and Information Systems Control

CSA - Cloud Security Alliance

CTF - Capture the Flag (competiție practică de securitate cibernetică)

DEP - Digital Europe Programme (Programul Europa Digitală)

DNSC - Directoratul Național de Securitate Cibernetică (instituția națională, România)

DORA - Digital Operational Resilience Act (Regulamentul UE 2022/2554 privind reziliența operațională digitală)

DSJC - Digital Skills and Jobs Coalition (Coaliția pentru competențe și locuri de muncă digitale)

ECCC - European Cybersecurity Competence Centre (Centrul European de Competențe în Securitate Cibernetică)

ECDL/ICDL - European/International Certification of Digital Literacy (certificarea europeană/internațională a competențelor digitale)

ECSF - European Cybersecurity Skills Framework (Cadrul european al competențelor în securitate cibernetică)

ECTS - European Credit Transfer and Accumulation System (Sistemul european de credite transferabile)

EIT - European Institute of Innovation and Technology (Institutul European de Inovare și Tehnologie)

EITC - European Information Technologies Certification (certificare europeană individuală în tehnologia informației)

EITCA - European Information Technologies Certification Academy (Academia europeană de certificare în tehnologia informației)

EITCI - European Information Technologies Certification Institute (institutul care guvernează cadrul EITC/EITCA)

ENISA - European Union Agency for Cybersecurity (Agenția Uniunii Europene pentru Securitate Cibernetică)

EQF - European Qualifications Framework (Cadrul european al calificărilor)

EU-INSPIRE - INnovative multi-diSciPlinary Industry-focused cybersecurity education for upskilling and ReskIlling the EU workforce (proiect european DEP, consorțiu de 23 de parteneri; DNSC partener)

FMI - Facultatea de Matematică și Informatică

FTE - Full-Time Equivalent (echivalent normă întreagă)

GenAI - Generative AI (inteligență artificială generativă)

GIAC - Global Information Assurance Certification

GRC - Governance, Risk and Compliance (guvernanță, risc și conformitate)

ICI - Institutul Național de Cercetare-Dezvoltare în Informatică (ICI București)

ICT - Information and Communication Technology (tehnologia informației și comunicațiilor; v. TIC)

INS - Institutul Național de Statistică (România)

IoT - Internet of Things (internetul lucrurilor)

IR - Incident Response (răspuns la incidente)

ISACA - Information Systems Audit and Control Association (asociație profesională)

ISC2 - International Information System Security Certification Consortium (Consorțiul Internațional pentru Certificarea Securității Sistemelor Informatice)

ISCO - International Standard Classification of Occupations (Clasificarea internațională standard a ocupațiilor; în text, ISCO-08)

IT - Information Technology (tehnologia informației)

LFS - Labour Force Survey (Ancheta asupra forței de muncă, Eurostat)

LLM - Large Language Model (model de limbaj de mari dimensiuni)

ML - Machine Learning (învățare automată)

MLOps - Machine Learning Operations (operațiuni pentru modele de învățare automată)

MLSecOps - Machine Learning Security Operations (operațiuni de securitate pentru sistemele de învățare automată)

MSSP - Managed Security Service Provider (furnizor de servicii de securitate gestionate)

MTTR - Mean Time To Respond (timp mediu de răspuns)

NICE - National Initiative for Cybersecurity Education (Inițiativa Națională pentru Educație în Securitate Cibernetică, SUA/NIST)

NIS2 - Network and Information Security Directive 2 (Directiva privind securitatea rețelelor și a sistemelor informatice, UE 2022/2555)

NIST - National Institute of Standards and Technology (Institutul Național de Standarde și Tehnologie, SUA)

OECD - Organisation for Economic Co-operation and Development (Organizația pentru Cooperare și Dezvoltare Economică)

OSCP - Offensive Security Certified Professional

OSINT - Open-Source Intelligence (informații din surse deschise)

OUG - Ordonanță de Urgență a Guvernului

OWASP - Open Worldwide Application Security Project (proiect deschis pentru securitatea aplicațiilor)

PFA - Persoană Fizică Autorizată

PNRR - Planul Național de Redresare și Reziliență

PPP - Purchasing Power Parity (paritatea puterii de cumpărare)

PTaaS - Penetration Testing as a Service (testare de penetrare ca serviciu)

R&D - Research and Development (cercetare-dezvoltare)

SANS - SANS Institute (SysAdmin, Audit, Network, Security Institute; organizație de formare în securitate)

Security+ - CompTIA Security+ (certificare profesională; în text și ca Sec+)

SES - Structure of Earnings Survey (Ancheta privind structura câștigurilor salariale, Eurostat)

SOAR - Security Orchestration, Automation and Response (orchestrare, automatizare și răspuns în securitate)

SOC - Security Operations Center (centru de operațiuni de securitate)

SRI - Serviciul Român de Informații

TIC - Tehnologia Informației și Comunicațiilor (echivalentul românesc pentru ICT)

TKS - Task-Knowledge-Skill (model sarcină-cunoștințe-deprindere, NIST)

UAIC - Universitatea „Alexandru Ioan Cuza” din Iași

UBB - Universitatea Babeș-Bolyai din Cluj-Napoca

UPB - Universitatea Politehnica din București

UTBV - Universitatea Transilvania din Brașov

UVT - Universitatea de Vest din Timișoara

WEF - World Economic Forum (Forumul Economic Mondial)

Anexa 2 - Glosar de termeni

Adversarial ML - Tehnici de atac asupra modelelor de învățare automată, prin care un actor manipulează intrările de date, datele de antrenament sau interogările pentru a induce erori, a extrage informații despre model sau a-i ocoli mecanismele de apărare (evasion, data poisoning, model extraction).

Alfabetizare IA (AI literacy) - Ansamblul de competențe minimale care permit unei persoane să utilizeze sisteme de IA în cunoștință de cauză, înțelegându-le posibilitățile, limitele și riscurile. Concept definit în Art. 3(56) din AI Act.

Augmentare a forței de muncă (workforce augmentation) - Extinderea capacităților unui lucrător prin instrumente de IA, în care tehnologia preia sarcinile repetitive și eliberează timp pentru activități cu valoare adăugată mai mare, fără a înlocui integral rolul uman.

Data poisoning - Inserarea deliberată de date malițioase în setul de antrenament al unui model, pentru a corupe modelele rezultate sau pentru a induce comportamente ascunse de tip backdoor, activabile ulterior de atacator.

Deepfake - Conținut audio sau video sintetizat cu ajutorul IA, care imită fidel o persoană reală. Frecvent folosit în fraude, inginerie socială și dezinformare.

Early-adopter - Organizație sau piață aflată într-o fază timpurie de adopție a unei tehnologii, care o integrează înaintea majorității, dar fără ca utilizarea să fie încă generalizată sau matură.

Human-AI teaming - Modelul de lucru în care oamenii și sistemele de IA colaborează ca o echipă, cu repartizarea sarcinilor între cele două și cu accent pe supravegherea, validarea și corectarea umană a rezultatelor generate automat.

Jailbreaking - Manipularea unui model de IA prin intrări construite special pentru a-i ocoli restricțiile de siguranță și politicile de utilizare, determinându-l să genereze conținut pe care în mod normal l-ar refuza. Spre deosebire de prompt injection, care vizează instrucțiunile aplicației, jailbreaking-ul vizează limitele comportamentale ale modelului însuși.

Piramidă inversată - Situația în care presiunea de pe piața muncii cade pe rolurile mid, senior și expert, în timp ce rolurile de intrare devin teoretic ușor de acoperit, dar greu de format, pentru că automatizarea elimină sarcinile repetitive prin care juniorii acumulau tradițional experiență.

Prompt engineering - Practica de a scrie, testa și optimiza instrucțiunile (prompturile) date sistemelor de IA generativă și agenților, astfel încât rezultatele să fie corecte, relevante și controlabile.

Prompt injection - Manipularea unui model de limbaj prin instrucțiuni malițioase incluse în intrare, pentru a-i ocoli restricțiile sau a-l determina să execute acțiuni neautorizate.

Reskilling vs. upskilling - Reskilling înseamnă recalificarea integrală a unei persoane pentru un rol diferit (de exemplu, administrator de sisteme devenit AI Security Engineer); upskilling înseamnă aprofundarea competențelor în rolul actual (de exemplu, analist SOC tradițional devenit analist SOC asistat de IA).

Securitate cibernetică - Ansamblul de activități, măsuri și standarde pentru protejarea sistemelor informatice, a datelor și a utilizatorilor împotriva accesului neautorizat, atacurilor și deteriorării.

Shadow AI - Utilizarea informală, neoficială sau insuficient guvernată a instrumentelor de IA de către angajați, în afara politicilor și mecanismelor de control ale organizației. Poate deveni comportamentul implicit într-o organizație aflată în tranziție, generând riscuri ascunse de securitate, conformitate și calitate a rezultatelor.

Threat hunting - Activitatea proactivă de căutare a amenințărilor și a semnelor de compromitere într-o rețea, înainte ca acestea să declanșeze alerte automate, bazată pe ipoteze formulate de analist și pe corelarea unor volume mari de telemetrie.

Zero Trust - Model de securitate care nu acordă încredere implicită niciunei entități, interne sau externe. Fiecare cerere de acces este verificată explicit, pe principiul „nu te încrede niciodată, verifică întotdeauna”.

Anexa 3 - Notă metodologică

Surse utilizate. Documentul valorifică surse primare oficiale (Eurostat LFS, ENISA, OECD, ISC^2, INS, DNSC, Comisia Europeană, NIST) și surse secundare recunoscute (WEF, Gartner, Forrester, McKinsey, Microsoft, KELA, Brainspotting, ANIS, ISACA). Pentru toate datele cantitative principale, raportul oferă citare cu link activ în secțiunea de bibliografie și prin footnote-uri inline. Cifrele referitoare la România provin în principal din Eurostat 2024–2025, INS și raportările de piață ANIS/Brainspotting. Lipsa datelor publice oficiale DNSC pentru forța de muncă cyber este explicit semnalată.

Ipoteze de modelare a scenariilor. Baza de pornire este estimată la ~12.000 specialiști cyber în România în 2024 (proxy proporțional, calculat pe baza populației și a ratei de IS FTE/IT FTE la nivelul UE, de 5,9%). Rate anuale de creștere considerate: 5% (pesimist), 10% (realist), 15% (optimist). Cererea internă este modelată la +12%/an în scenariul realist, peste rata globală de ~8%/an a necesarului raportată de ISC2, pentru a reflecta șocul de cerere generat de intrarea în vigoare a Directivei NIS2 (12.000–15.000 de entități noi sub obligații). Este o ipoteză de lucru, nu o rată preluată ca atare dintr-o sursă. Probabilitățile subiective P=25% (optimist), P=55% (realist), P=20% (pesimist) reflectă judecata expertului analitic, raportată la indicatori macroeconomici.

Limite ale analizei. Datele publice oficiale pentru România privind forța de muncă în domeniul securității cibernetice sunt limitate; DNSC nu publică estimări proprii ale numărului de specialiști activi. Cifrele pentru salarii în domeniul securității cibernetice în UE sunt fragmentare (Eurostat SES nu segmentează pe rol). Comparabilitatea WEF FoJ 2023 ↔ 2025 este limitată de schimbarea metodologiei. Toate previziunile sunt sensibile la viteza de adopție a IA.

Autori: Adriana Simionescu, Bogdan Radu

Această publicație este licențiată sub CC-BY 4.0 "Cu excepția cazului în care se specifică altfel, reutilizarea acestui document este autorizată sub licența Creative Commons Attribution 4.0 International (CC BY 4.0) (https://creativecommons.org/licenses/by/4.0/). Aceasta înseamnă că reutilizarea este permisă, cu condiția menționării corespunzătoare și a indicării oricăror modificări".

TLP: CLEAR = Destinatarii pot transmite informația oricui, nu există limitări privind divulgarea. TLP:CLEAR se poate folosi atunci când informațiile prezintă un risc minim de utilizare abuzivă, în conformitate cu normele și procedurile aplicabile pentru publicare. Sub rezerva regulilor standard ale drepturilor de autor, informațiile TLP:CLEAR pot fi partajate fără restricții.
Informațiile și opiniile conținute în acest document sunt furnizate "ca atare" și fără garanții. Referirea din prezentul document la orice produse, procese sau servicii comerciale specifice prin denumire comercială, marcă comercială, producător sau în alt mod nu constituie sau implică aprobarea, recomandarea sau favorizarea acestuia de către Directoratul Național de Securitate Cibernetică (DNSC), iar aceste îndrumări nu vor fi utilizate în scopuri publicitare sau de aprobare a produselor.