Analiza competențelor

Proiectul învățământului superior din Moldova – DATASEA

Răzvan Rughiniș

razvan.rughinis@upb.ro

Analiza competențelor necesare

Obiective

- Identificarea competențelor esențiale pentru Știința datelor și Securitate informațională
- Identificarea competențelor acoperite parțial / neacoperite în programele UTM
- Instruire
- Formularea noilor planuri de învățământ

Metodologie

- Analiza planurilor de învățământ de la universități de top din România, UE și SUA
- Sinteza competențelor tipice incluse în curricula

Context social și tehnologic

Tendințe și provocări | Automatizare

Automatizarea și AI

- Creșterea automatizării sarcinilor de rutină
- Necesitatea de a colabora cu sisteme AI
- Provocarea de a rămâne relevanți într-un mediu în schimbare rapidă

Învățare continuă și adaptabilitate

- Nevoia de actualizare constantă a competențelor
- Importanța învățării pe tot parcursul vieții
- Adaptarea la noi tehnologii și metodologii

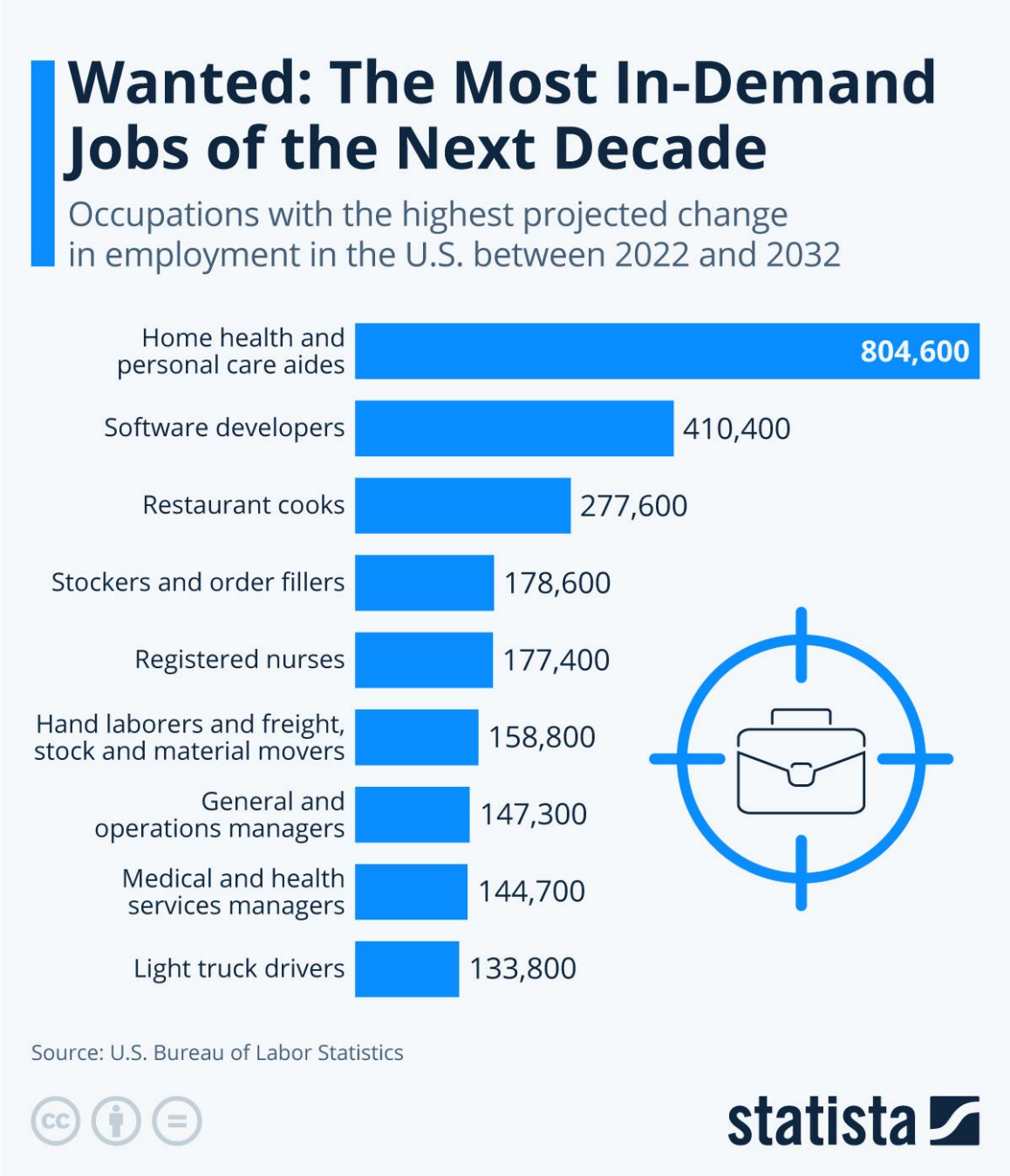
Which Jobs Have a Future?

Jobs forecast to grow the most worldwide between 2023 and 2027*

Jobs with the largest employment gains*	Fastest-growing jobs**
1. Agricultural equipment operators	1. AI and Machine Learning specialists
2. Heavy truck and bus drivers	2. Sustainability specialists
3. Vocational education teachers	3. Business intelligence analysts
4. Mechanics and machinery repairers	4. Information security analysts
5. Business development professionals	5. FinTech engineers
6. Building frame and related trades workers	6. Data analysts and scientists
7. University and higher education teachers	7. Robotics engineers
8. Electrotechnology engineers	8. Agricultural equipment operators

* Based on absolute increase in jobs between 2023 and 2027
** Based on relative increase in number of jobs between 2023 and 2027
Source: WEF Future of Jobs Report 2023

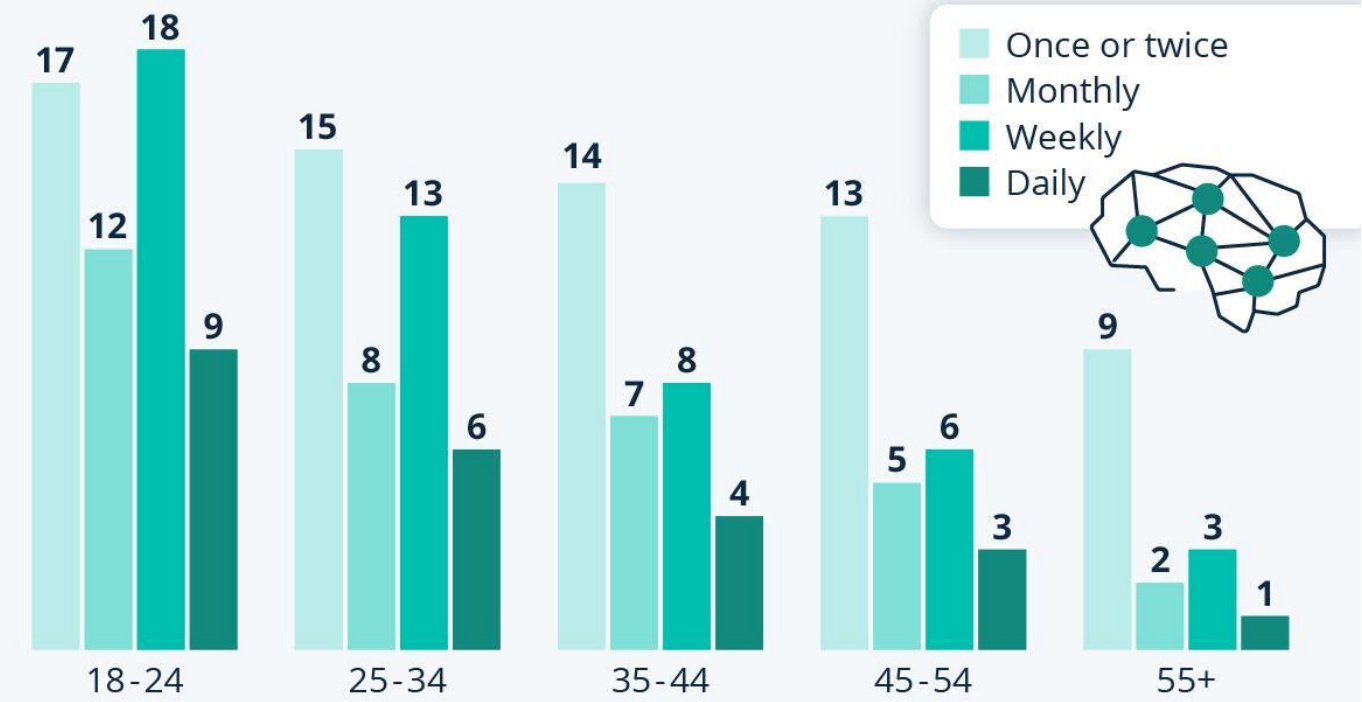
Creșterea proiectată a numărului de locuri de muncă, SUA



Sursa

ChatGPT Still Light-Years Away From Universal Adoption

Share of respondents using ChatGPT in the following frequencies, by age group (in %)



12,217 online respondents (18+ y/o) in Argentina, Denmark, France, Japan, UK and the US surveyed Mar. 28-Apr. 30, 2024

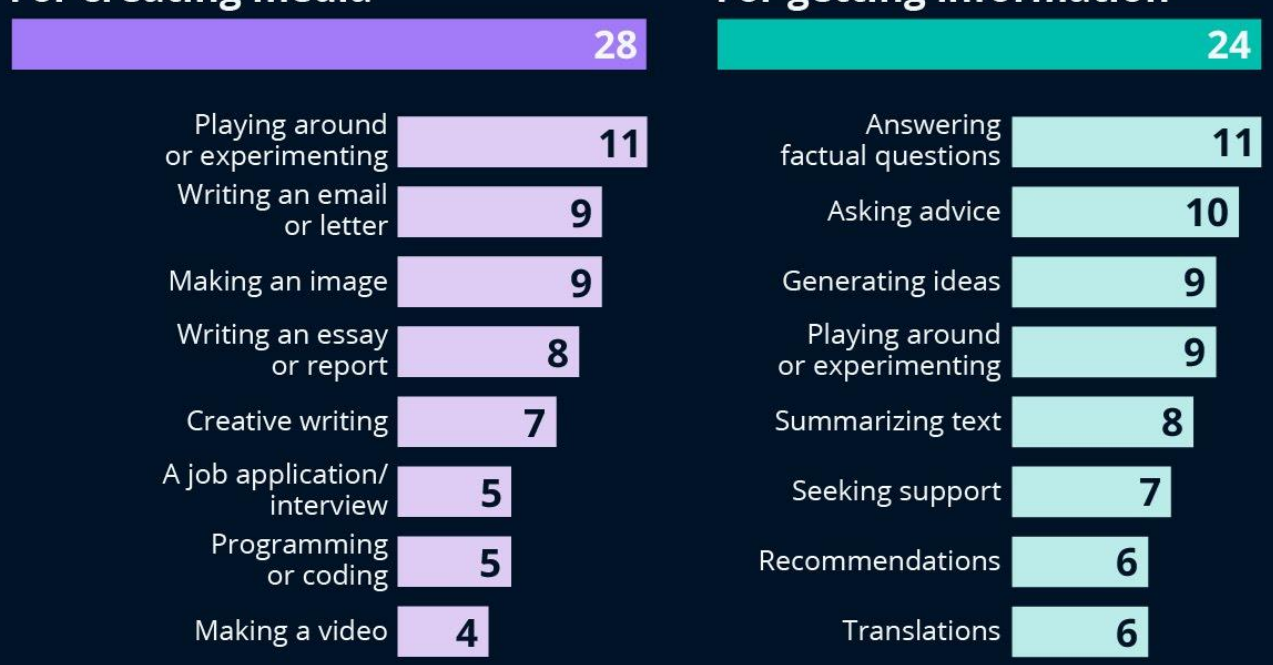
Source: RISJ | YouGov

statista

Sursa

Generative AI: A Jack of All Trades?

Share of respondents who have tried to use a generative AI tool (e.g. ChatGPT) for the following applications (in %)



12,217 adults surveyed in Argentina, Denmark, France, Japan, the UK and the US; Mar.-Apr. 2024

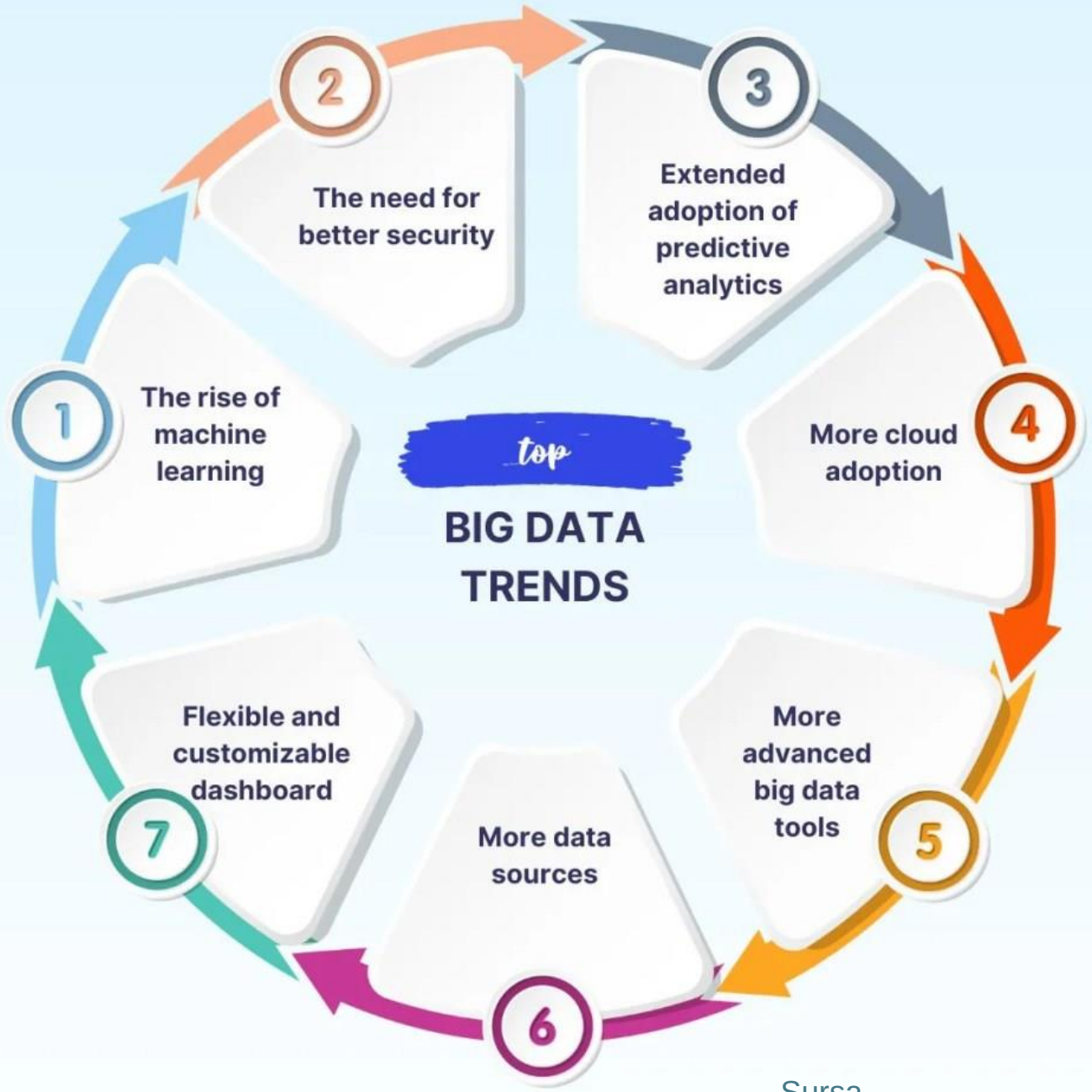
Source: Reuters Institute for the Study of Journalism

statista

Sursa

Tendințe și provocări | Big Data

- Creșterea volumului și complexității datelor
- Nevoia de securizare a datelor
- Oportunități prin ML
- Încorporarea Big Data în domenii diverse



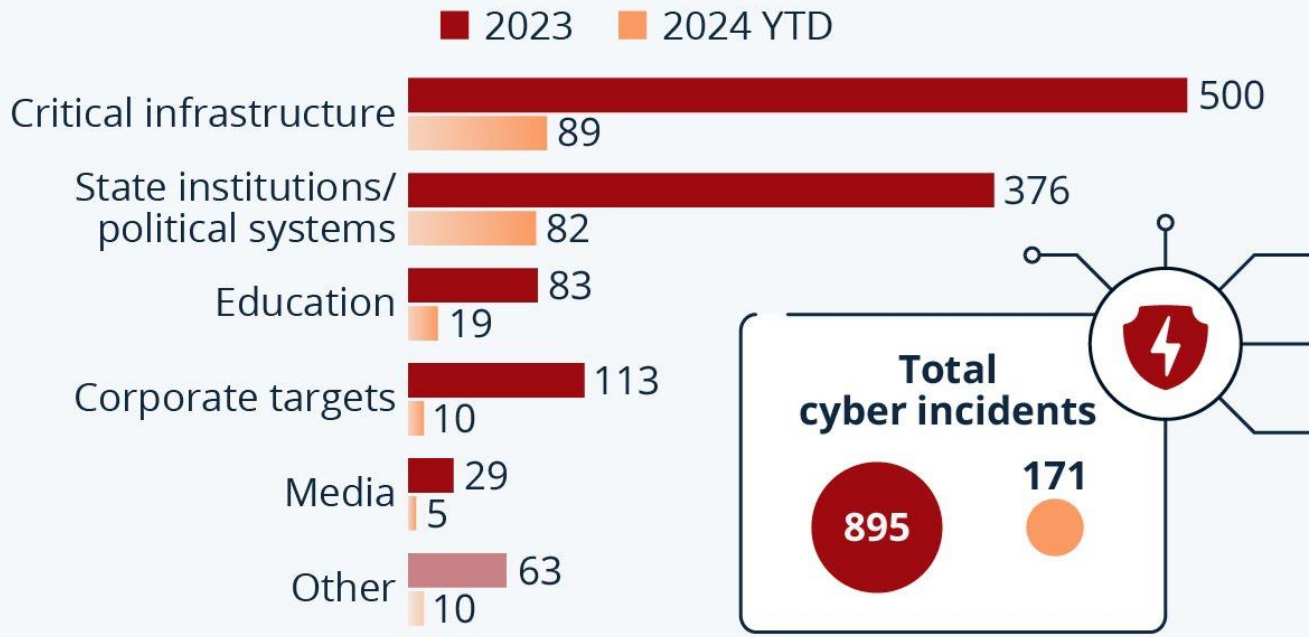
Sursa

Tendințe și provocări | Securitate

- Creșterea amenințărilor
- Necesitatea de a integra securitatea prin design
- Protejarea datelor sensibile și a proprietății intelectuale
- Oportunități: dezvoltarea AI
- Sporirea suprafeței de atac prin Generative AI

Cybercrime: Critical Infrastructure Is Top Target

Number of worldwide political cyber attacks aimed at the following sectors, by reported period*



As of Mar. 26, 2024

* One incident may target more than one sector. Initial access by malevolent actors may not always coincide with report period.

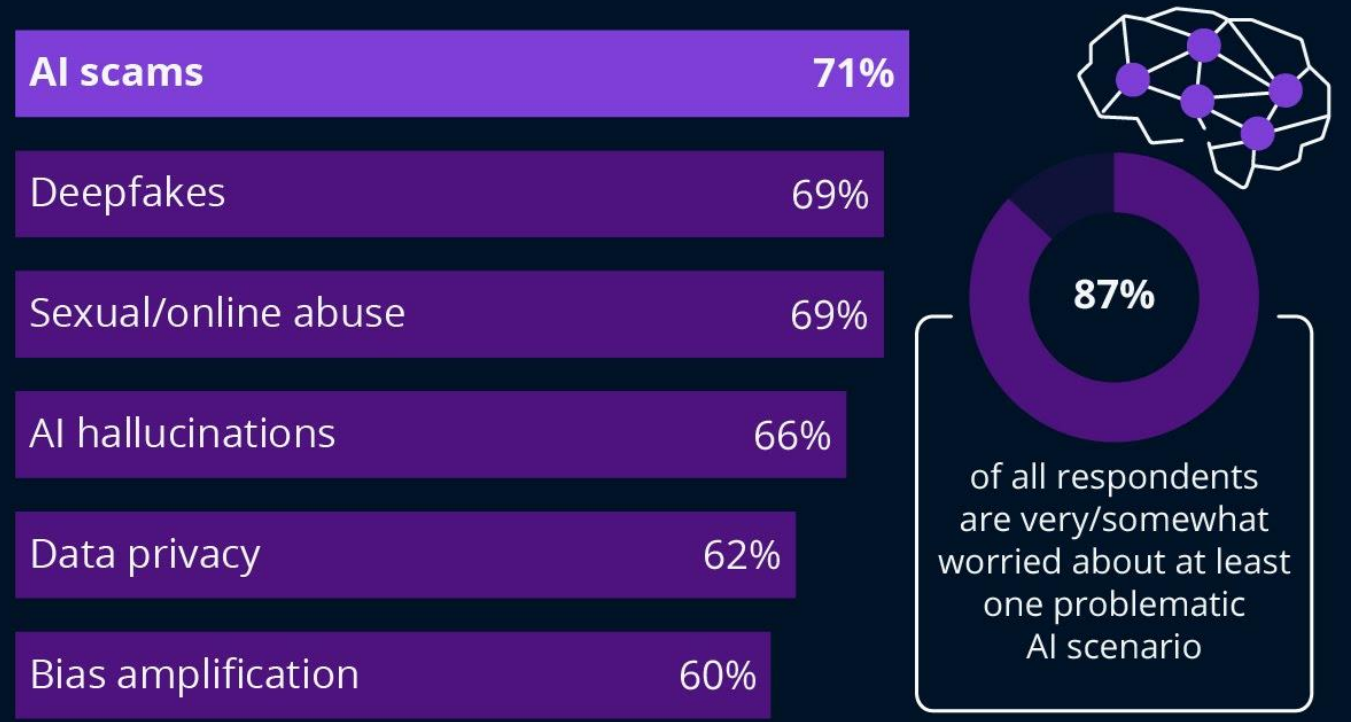
Source: European Repository of Cyber Incidents

statista

Sursa

Scams, Fakes, Abuse: The Dangers of Generative AI

Share of respondents being very/somewhat worried about the following potential problems caused by AI



16,795 respondents (13-64 y/o) in 17 countries surveyed online Jul.-Aug. 2023
Source: Microsoft Global Online Safety Survey 2024

statista

Sursa

The Cybersecurity Crisis of Artificial Intelligence: Unrestrained Adoption and Natural Language-Based Attacks

Andreas Tsamados[1], Luciano Floridi[2], Mariarosaria Taddeo[13]

[1]Oxford Internet Institute, University of Oxford, 1 St Giles', Oxford, OX1 3JS, UK

[2] Digital Ethics Center, Yale University, 85 Trumbull Street, New Haven, CT 06511, US

[3] The Alan Turing Institute, British Library, 96 Euston Rd, London NW1 2DB, UK

* Email of correspondence author: mariarosaria.taddeo@oii.ox.ac.uk

Abstract

The widespread integration of autoregressive-large language models (AR-LLMs), such as ChatGPT, across established applications, like search engines, has introduced critical vulnerabilities with uniquely scalable characteristics. In this commentary, we analyse these vulnerabilities, their dependence on natural language as a vector of attack, and their challenges to cybersecurity best practices. We offer recommendations designed to mitigate these challenges.

TikTag contra ARM

- Cercetătorii au vizat Memory Tagging Extension (MTE), în ARM arhitectura 8.5-A, care detectează coruperea memoriei. [Articol]
- Prin dispozitivele TikTag: executarea de cod arbitrar, escaladarea privilegiilor, scurgerea de date sau refuzul serviciului

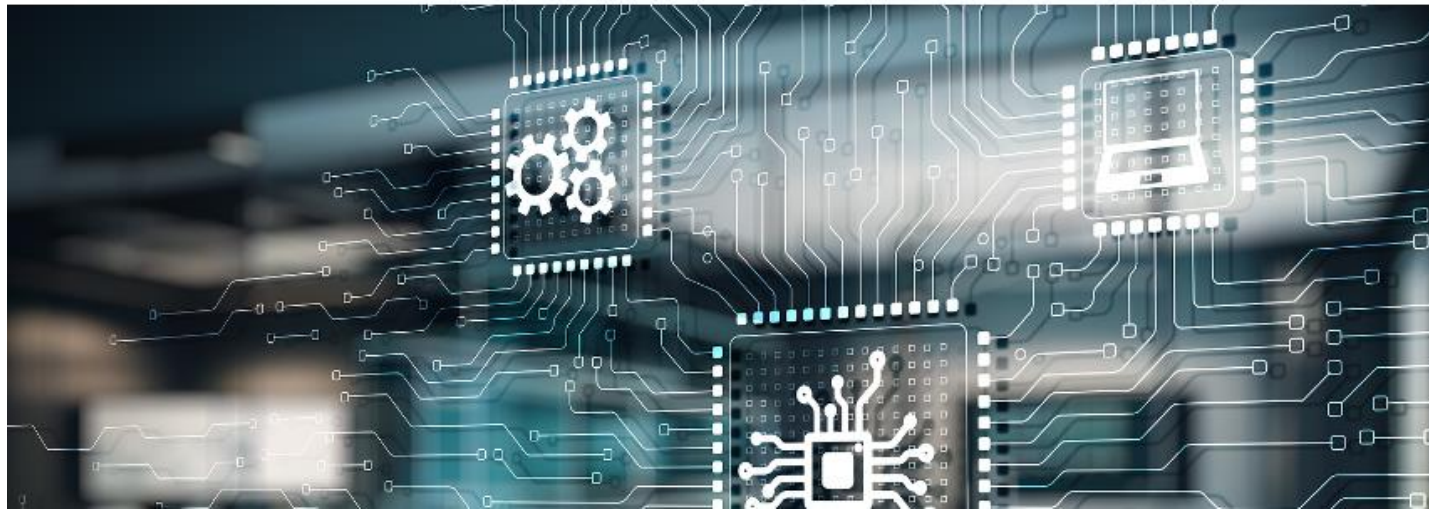
Sursa

ENDPOINT SECURITY

New TikTag Attack Targets Arm CPU Security Feature

Researchers have targeted the MTE security feature in Arm CPUs and showed how attackers could bypass protections.

By Eduard Kovacs
June 18, 2024



Criza Microsoft / Crowdstrike

- Cea mai mare „pană” digitală: 19 iulie 2024
- Riscurile monopolizării tehnologice
- Focalizare excesivă pe eficiență, cu costuri de reziliență

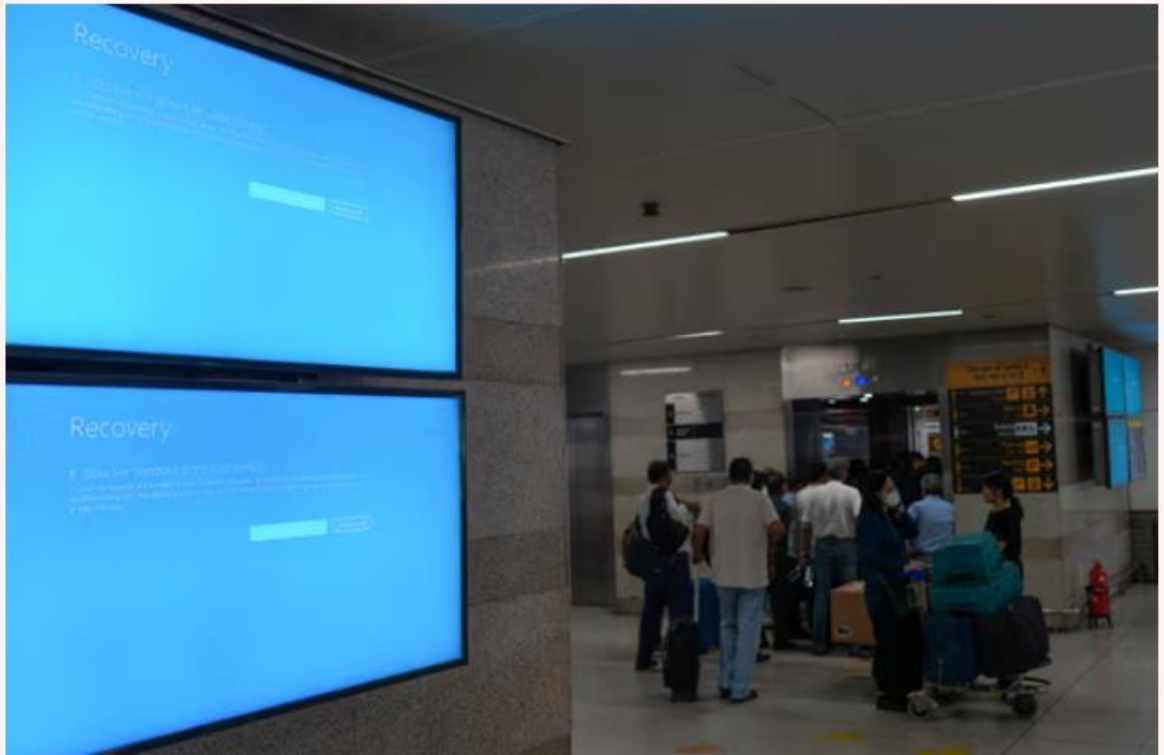
Sursă

Analysis

The Microsoft/CrowdStrike outage shows the danger of monopolization

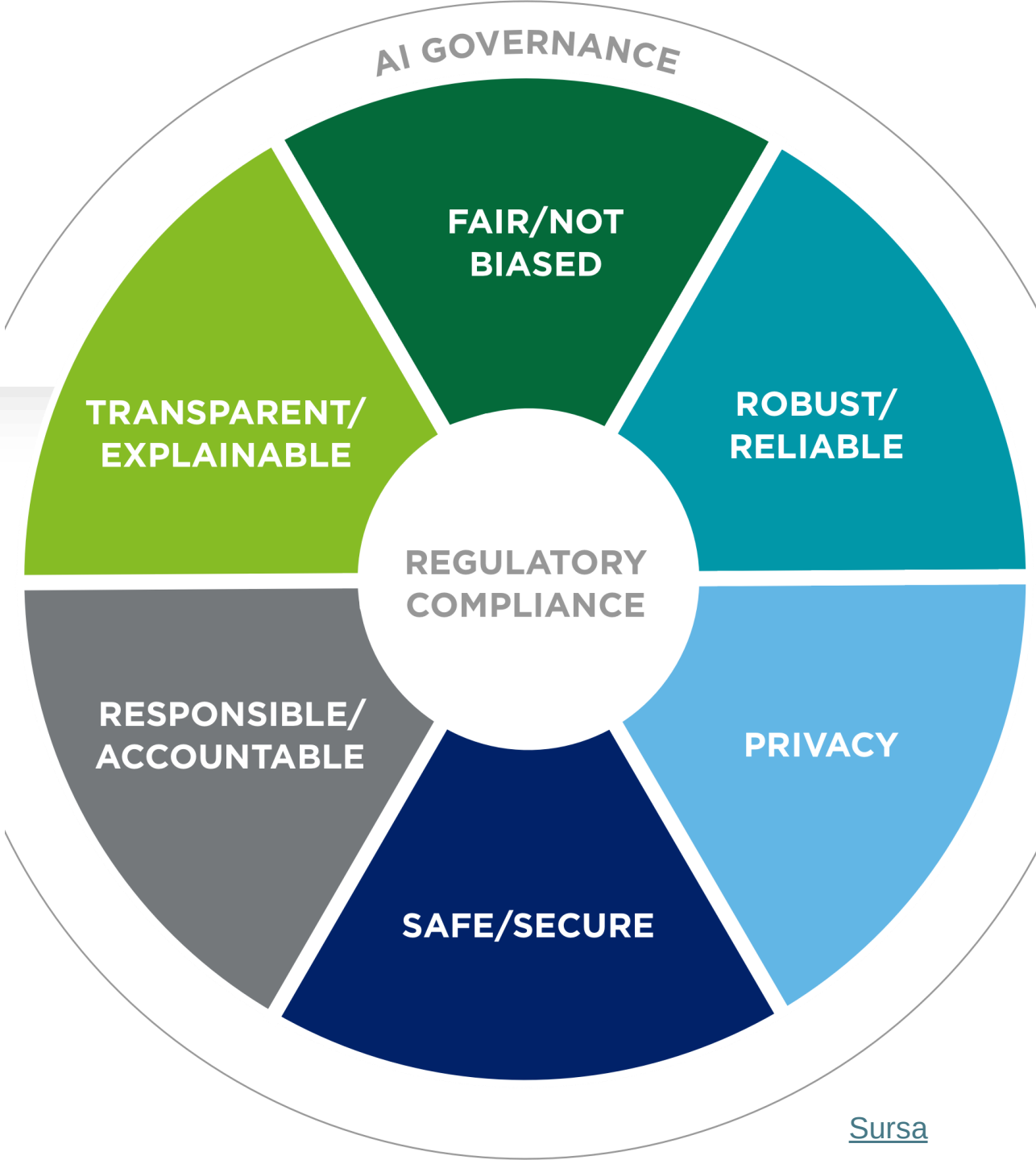
Edward Ongweso Jr

As the world recovers from the largest IT outage in history, it shows the danger of one point of failure in IT infrastructure



Tendințe și provocări | Etică & reglementări

- Creșterea reflecției publice privind etica tehnologiei
- Reglementări europene și globale; GDPR, DSA & DMA, AI Act
- Provocări etice ale AI
  - Explicabilitate
  - Părtinire
  - Încredere
  - Procurarea și utilizarea datelor
  - Securitate
  - Responsabilitatea deciziilor



Sursa

Tendințe și provocări | Personalizare

- Cererea crescută pentru soluții personalizate
- Oportunități prin AI
- Diversificarea surselor de date (Internet, IoT)
- Tensiunea personalizare / confidențialitate

Sursa

Analiza programelor de studii

Obiective actuale

- **Elaborarea noilor planuri de învățământ** pentru „Știința datelor” și „Securitate informațională”
  - Lista competențelor noi
  - Rezultate ale învățării
  - Matricea corelării rezultatelor învățării cu disciplinele de studii
  - Proiect plan de învățământ

- **Chestionarul de evaluare:**

https://forms.gle/Zvv3jU1fk4TrmsjL6

Programe analizate - Știința datelor

Universitate	Program
Harvard University	Master's in Data Science
Stanford University	Statistics & Data Science MS
New York University	Masters in Data Science
TU Delft	Data Science and Artificial Intelligence Technology (Master)
ETH Zurich	Master in Data Science
Universitatea din București FMI	Data science (Master)
Universitatea Babeș Bolyai – UBB Facultatea de Matematică și Informatică	Data Science for Industry and Society MA
Universitatea Babeș Bolyai – UBB Sociologie	Analiza datelor complexe (Master)

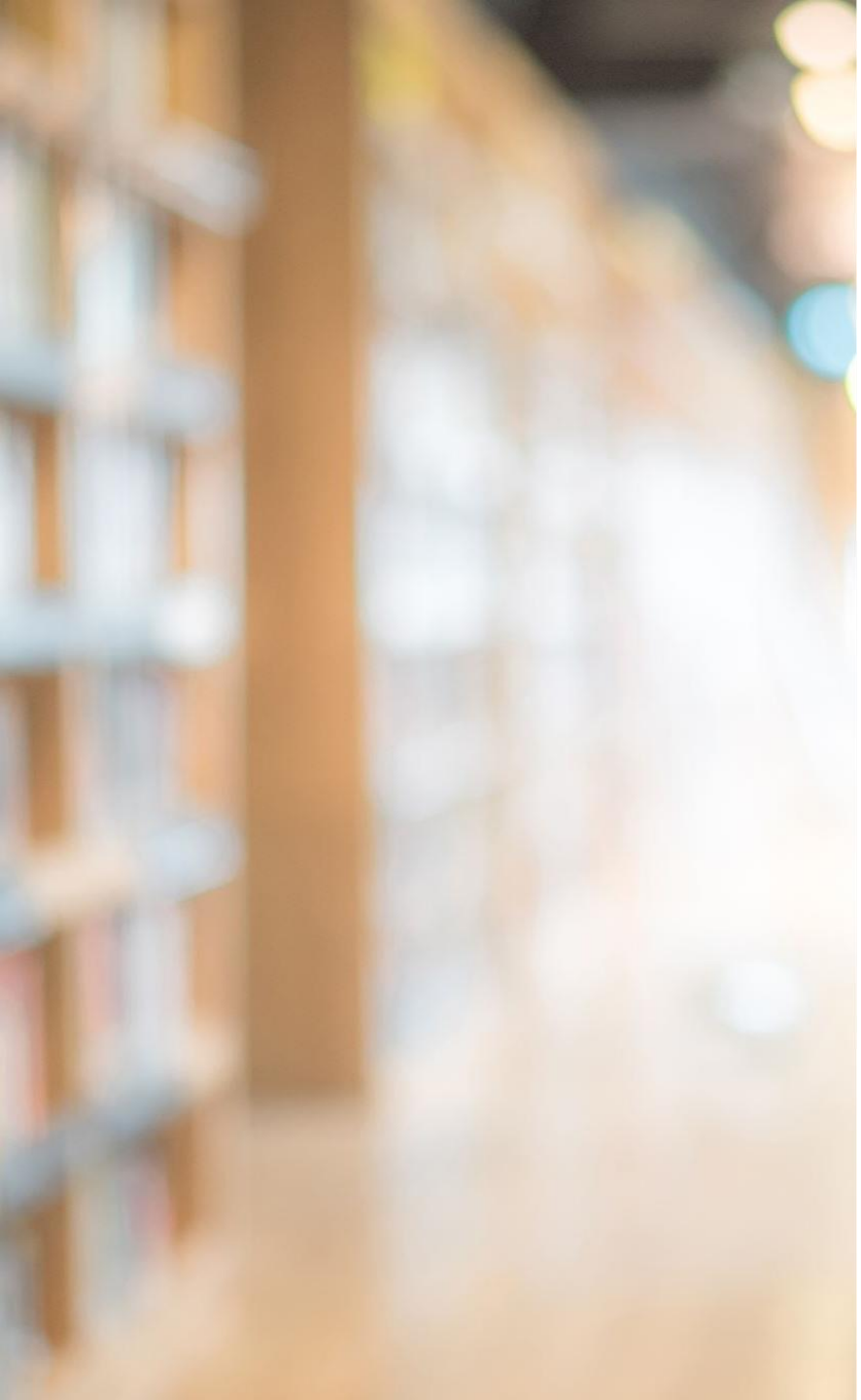
Programul UTM „Analiza datelor”

Contextul actual

- Program comprehensiv și bine articulat
- Acoperă competențele esențiale
- Nevoia de aprofundare în anumite domenii

Zone de aprofundare

- Evoluții în **înțelegerea și utilizarea datelor în societate**
- Provocări de **confidențialitate și securitate** în fluxuri informaționale
- **Impactul AI** asupra securității datelor



Tematica propusă

- **Înțelegerea datelor în societate**
  - Aspecte economice, psihologice și sociologice ale datelor masive
  - Impactul asupra pieței libere și modelelor de afaceri
  - Utilizarea datelor în diverse contexte sociale
- **Confidențialitate și securitate**
  - Provocări în fluxurile informaționale
  - Perspective ale decidenților, experților și utilizatorilor
  - Modele de reglementare globale (UE, SUA, China)
  - Strategii de asigurare a confidențialității datelor
- **AI și securitatea datelor**
  - Impactul AI asupra securității cibernetice
  - Riscuri asociate tehnologiilor emergente
  - Pregătirea pentru abordarea provocărilor în evoluție

Programe analizate – Securitate informațională

Universitate	Program
Harvard University Extension School	Cybersecurity Masters
Stanford University	Cybersecurity Graduate Certificate
Stanford University	Advanced Cybersecurity Program
MIT Professional Education Division	Applied Cybersecurity
European Institute of Technology – EIT Digital Eötvös Loránd University (ELTE) Universitatea Babeș Bolyai – UBB University of Rennes University of Trento (UniTN) University of Turku (UTU) University of Twente (UT)	CyberSecurity
New York University	Cybersecurity Master
TU Delft	Cybersecurity Master
ETH Zurich	Master in Cybersecurity
Universitatea Națională de Știință și Tehnologie POLITEHNICA București - UNSTPB	Securitatea Reţelelor Informatice Complexe
Universitatea Tehnică „Gheorghe Asachi” din Iași	Securitatea Spațiului Cibernetic (Master)
Universitatea Tehnică din Cluj-Napoca UTCN	Ingineria Securității Cibernetice / Cybersecurity Engineering (EN) (CE)
Universitatea din București FMI	Securitate și Logică Aplicată
Universitatea Babeș Bolyai – UBB Facultatea de Matematică și Informatică	Securitate Cibernetică

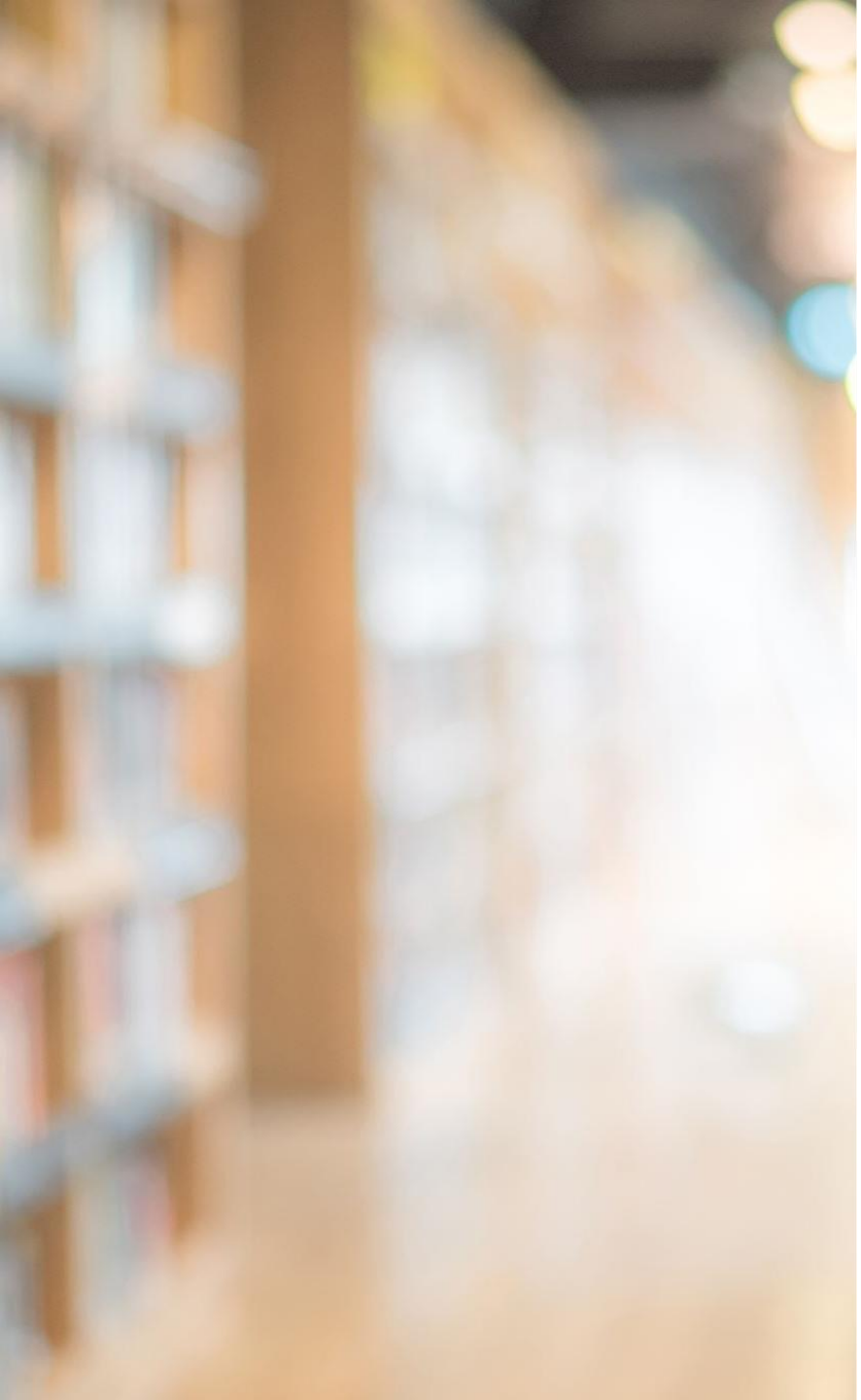
Programul UTM „Securitate informațională”

Contextul actual

- Program comprehensiv și bine articulat
- Acoperă competențele esențiale
- Nevoia de aprofundare în anumite domenii

Zone de aprofundare

- Analiza datelor și detecția erorilor
- Securitatea și confidențialitatea datelor vaste
- AI și securitatea cibernetică
- Securitatea IoT
- Blockchain și aplicațiile sale



Tematica propusă

- **Analiza datelor și detecția erorilor**
  - Măsurarea fenomenelor și erori de măsurare
  - Coincidențe, corelații și cauzalitate
  - Extragerea informației prin tehnici de analiză a datelor
- **AI și securitatea cibernetică**
  - Provocările AI pentru securitatea cibernetică
  - Atacurile specifice modelelor ML/AI
- **Securitatea IoT și Blockchain**
  - Securizarea Internetului Lucrurilor (IoT)
  - Blockchain și aplicațiile sale

Agenda propusă a instruirii

Argumente bazate pe dovezi: analiza datelor în societate

- Coincidențe, corelații și cauzalitate
- Măsurarea fenomenelor și erori de măsurare
- Eșantionarea și modelarea; erori specifice
- Extragerea informației prin tehnici de analiză a datelor

Datele masive în societate

- Dimensiunea economică: datele și piața liberă, modele de afaceri
- Dimensiunea psihologică și sociologică

Confidențialitatea și securitatea datelor

- Decidenți: Modele de reglementare în EU, SUA și China
- Experți și utilizatori: Strategii de asigurare a confidențialității

AI și securitatea cibernetică

- Provocările AI pentru securitatea cibernetică
- Atacurile specifice modelelor ML / AI

Opțional - Teme aprofundate

- Blockchain și aplicațiile sale
- Securizarea Internetului Lucrurilor (IoT)

Tendințe și provocări | IoT și dezvoltare durabilă

IoT și sisteme conectate

- Proliferarea dispozitivelor conectate
- Provocări legate de interoperabilitate și standard
- Gestionarea și securizarea rețelelor complexe de dispozitive

Dezvoltarea durabilă și ingineria verde

- Presiunea de a crea soluții sustenabile
- Integrarea principiilor de durabilitate în proiectare și producție
- Abordarea provocărilor legate de schimbările climatice