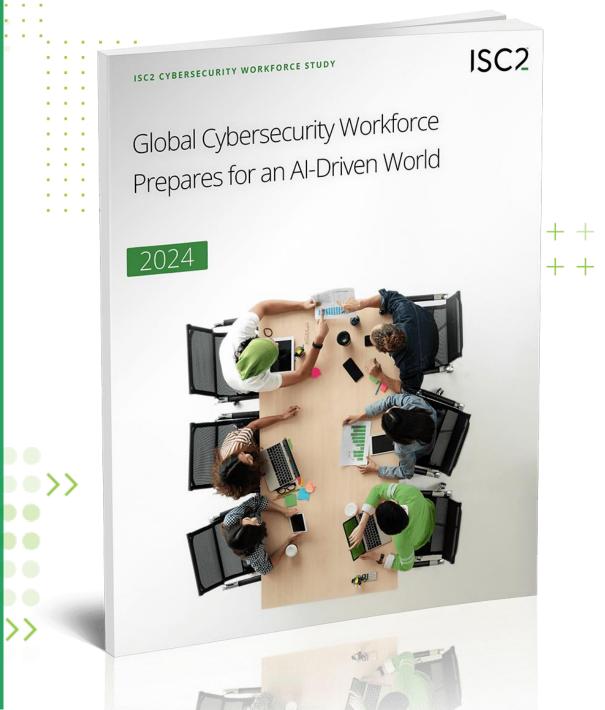
JSC2[®] Your Future. Secured.

2024 Cybersecurity Workforce Survey Focus on the E.U.



In 2024, pressures on the cybersecurity workforce increased.

Gen Al delivers some benefits

2024 ISC2 Cybersecurity Workforce Study Focus on the E.U.











The Threat Landscape

es traubl e di in a new fraihinti; \r\nVersion* + AppVersion + "\r\nAuthor: * + AppAuthor

mainte ik a feaiktt.getüefauttfootkitt); anning (crean = 16.gatScreenSize()) ifem auf printiniscreen.galdigth() + * --- * + screen.getHeight());

nutrin intelle vald manetering() args) throws Exception (// nume runk manipulscation logic horo

mateun sulfannerF = false;

(salealt prefs"; CESS DENIED

Compiling Nodes

sor.dir" ssorsvor

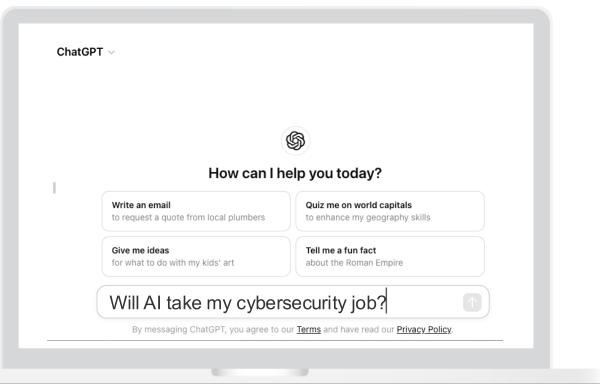
of cybersecurity professionals say the threat landscape is the worst they've seen in 5 years



of E.U. cybersecurity professionals have been approached by a malicious actor wanting them to act as a malicious insider

anticipate a rise in malicious actors contacting cybersecurity professionals over the next year

say the biggest challenge the industry faces will be emerging technologies



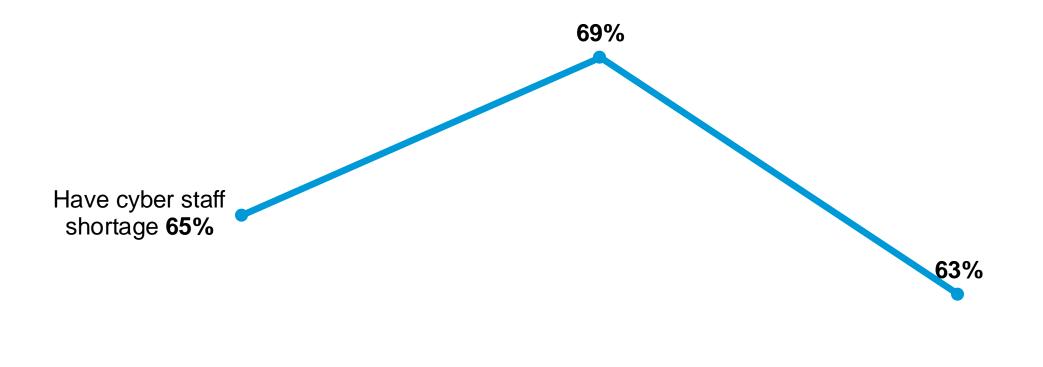


Emerging tech with the greatest positive impact or organisational security)	Emerging tech v greatest <i>negati</i> organisational s	ve impact on
41%	Automation in cybersecurity	15%	
35%	Advancements in Al		43%
29%	Zero Trust network access	8%	
26%	Risk-based vulnerability management	10%	
23%	Extended detection and response (XDR)	8%	
22%	Passwordless authentication	16%	
16%	Zero Trust Edge (ZTE)	6%	
15%	Post-quantum cryptography	22%	
12%	Quantum computing		35%
11%	Confidential computing	12%	
10%	Hardware/firmware security	11%	
10%	Increased processing power/speed	23%	
10%	Blockchain	17%	
9%	Telecomm improvements	10%	
8%	Mobile computing advances	19%	
8%	Increases in edge computing	16%	
7%	Cyberstorage	14%	
7%	Reduction in hardware form factor	13%	



State of the Cybersecurity Workforce

Cybersecurity staffing shortages are a persistent issue for organizations in the E.U.







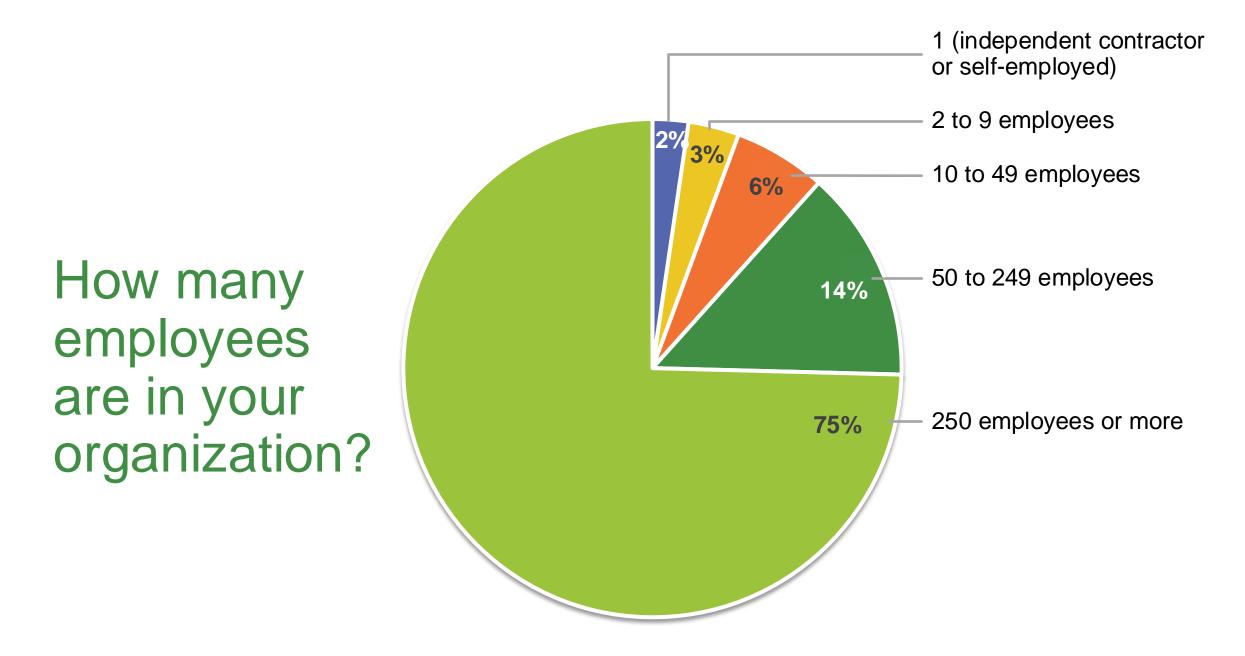


Which of the following best describes your role/title (in relation to ECSF)?

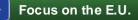
Cybersecurity architect Chief Information Security Officer (CISO) 12% 11% Cybersecurity implementer 9% Cybersecurity risk manager Cyber legal, policy, and compliance officer **6%** Cybersecurity auditor **6%** 5% Cyber incident responder Cyberthreat intelligence specialist 5% Penetration tester 4% 4% Cybersecurity educator 4% Cybersecurity researcher Digital forensics investigator 4% Other 10%



20%







Level within organisation

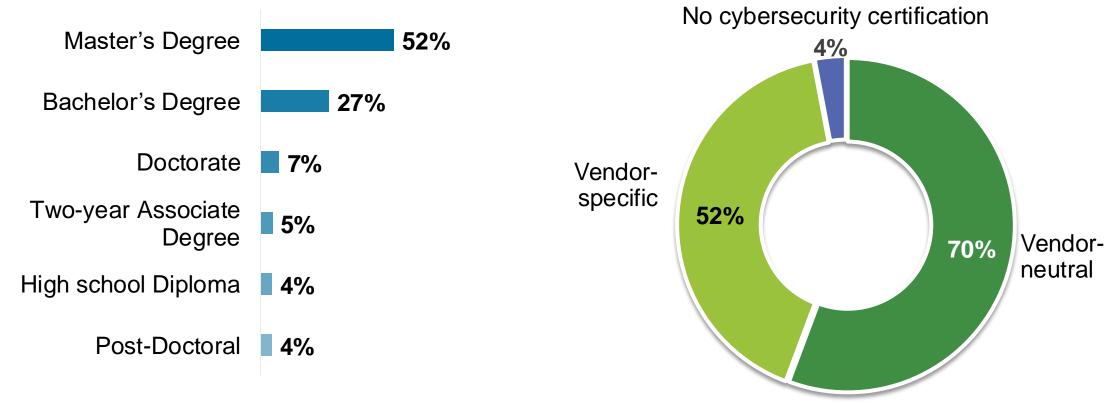




Vendor-neutral cybersecurity certifications are the standard choice among professionals

Highest level of education completed

Cybersecurity certification currently held





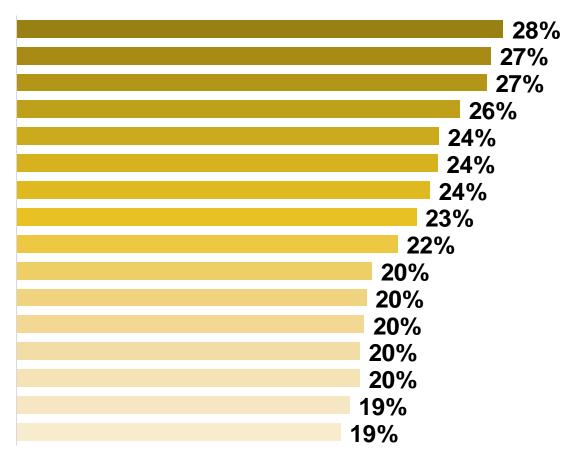
Which of the following best describes the industry your organization is in?

IT services	
Financial services	11%
Consulting	8%
Government	5%
Telecommunications	5%
Other	4%
Automotive	4%
Manufacturing	4%
Retail/Wholesale	4%
Security Software/Hardware Development	3%
Transportation	3%
Engineering	3%
Energy/Power/Utilities	3%
Military/military contractor	3%
Healthcare	2%
Education	2%
Insurance	2%
Non-Security Software/Hardware Development	2%
Construction	2%
Food/Beverage/Hospitality/Travel	1%
Entertainment/Media	1%
Hosted/cloud services	1%
Aerospace	1%
Real estate	1%
Nonprofit	1%
Legal	1%



24%

In which areas/roles is your organisation lacking cybersecurity talent?

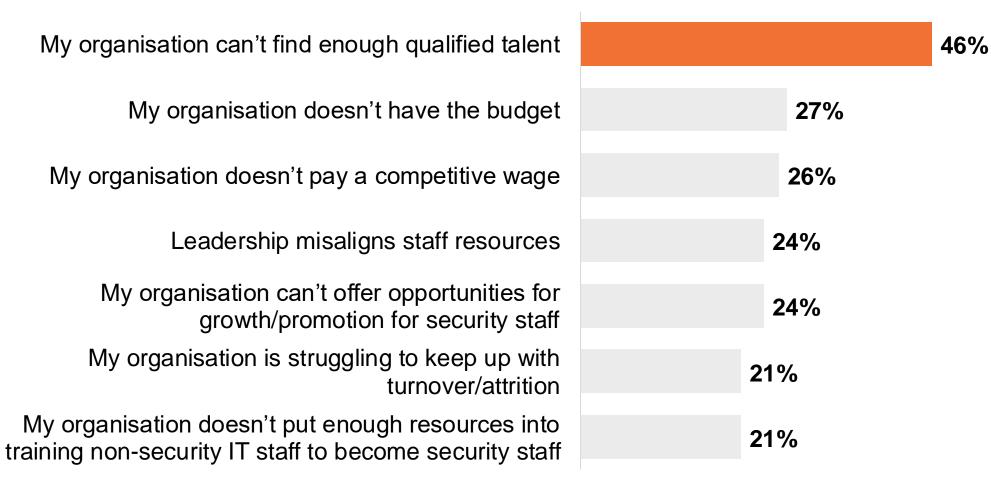


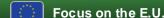
Cyberthreat intelligence **Digital forensics** Secure system architecture and design Security testing Secure system development Cybersecurity audit and assurance Cybersecurity governance and risk management Cybersecurity generalist Cybersecurity management Data protection and privacy Secure operations Incident response Cryptography and communications security Network monitoring and intrusion detection Vulnerability management Identity and access management



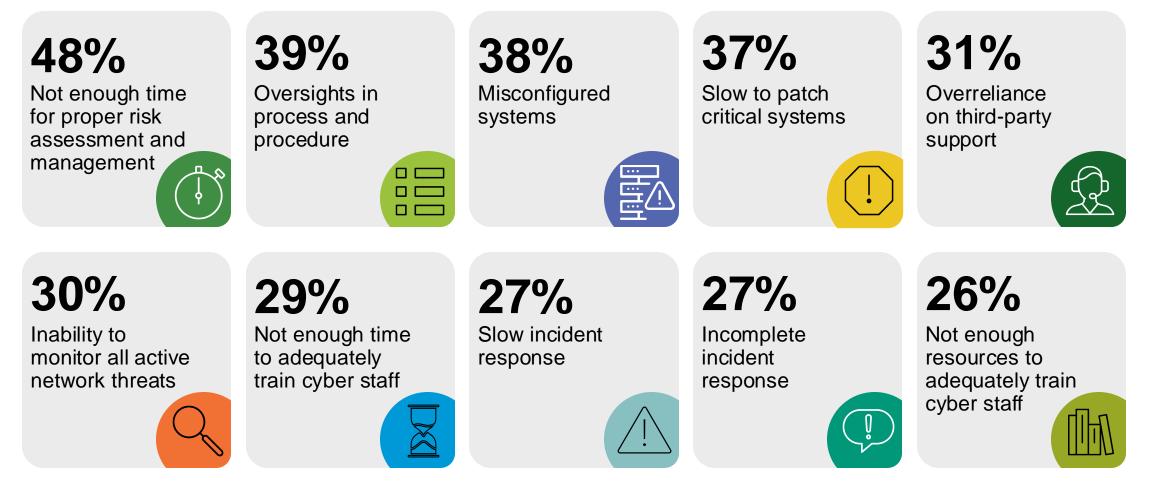
say that staffing shortages put their organisations at significant risk of cyber attacks

Reasons for cybersecurity staff shortages



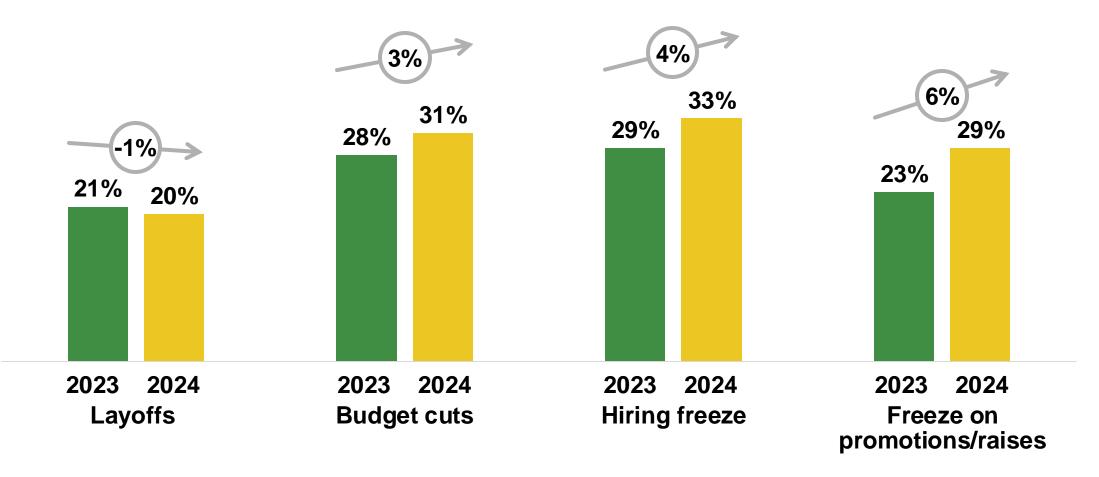


Impact of staffing shortages





Organisations have experienced cybersecurity cutbacks in the past 12 months

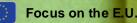


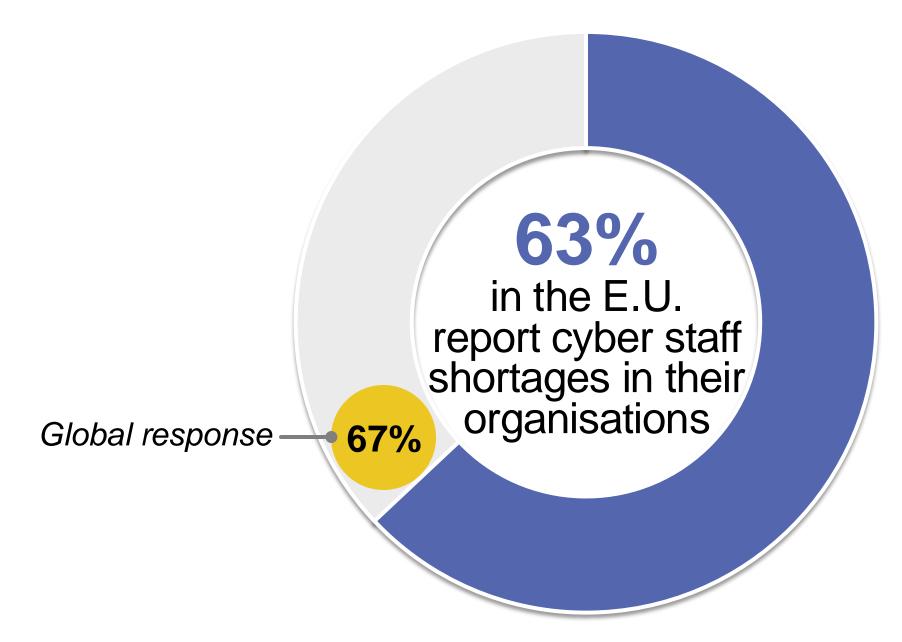




expect cybersecurity cutbacks in 2025

18% expect layoffs in 2025
25% predicted layoffs in 2024, lower than what they reported (20%)

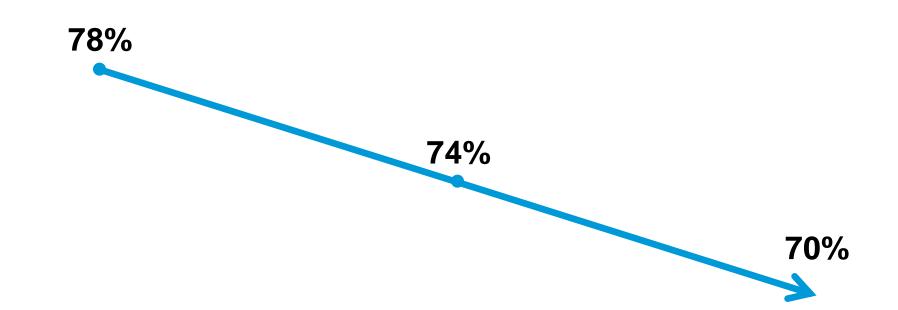








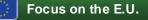
Cybersecurity job satisfaction is declining in the E.U.



2022







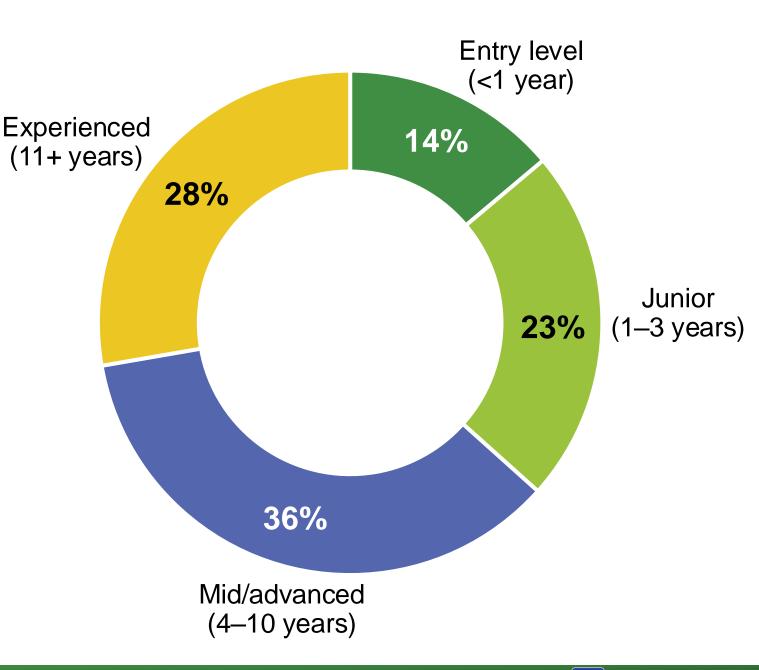
Biggest challenges faced in the E.U. over the *past 12 months*

Biggest challenges to come in the E.U. in the *next two years*

51%	Keeping up with changing regulatory requirements	46%
46%	Worker/skill shortages	46%
40%	Risks of emerging technologies	48%
37%	Cyber attacks as precursors, tactics, or retaliation in military conflicts	42%
36%	Adapting to risks from advances in employee computing technologies	40%
32%	Misinformation/disinformation sowing confusion about cyber risks	32%
29%	Insider threats	30%
24%	Addressing risks from an employee's home environment	20%
21%	Keeping up with environmental regulatory requirements	23%
19%	Addressing the impact of cyber insurance premium increases on security practices	18%
17%	Tension between tenured and junior security employees	16%

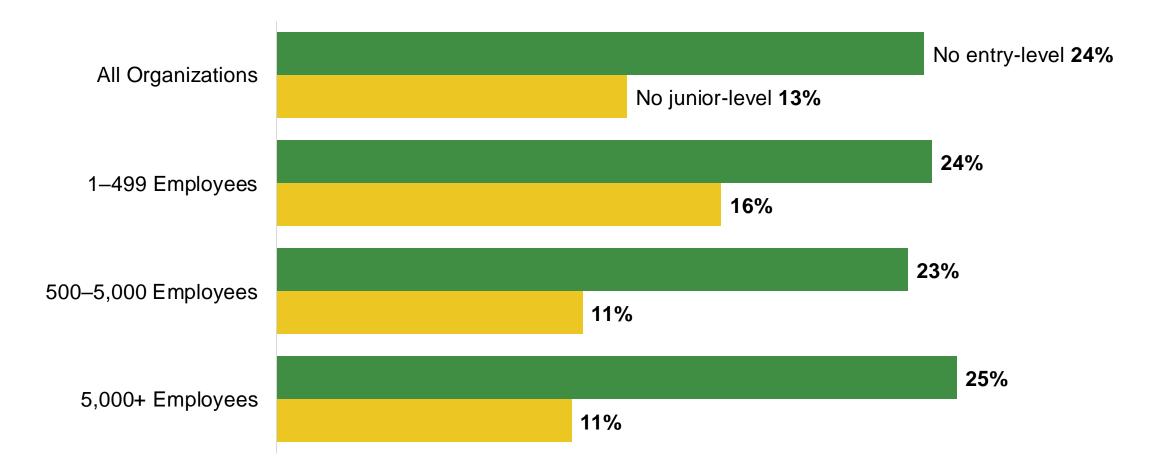


Average cybersecurity team composition in the E.U. by level/years of experience





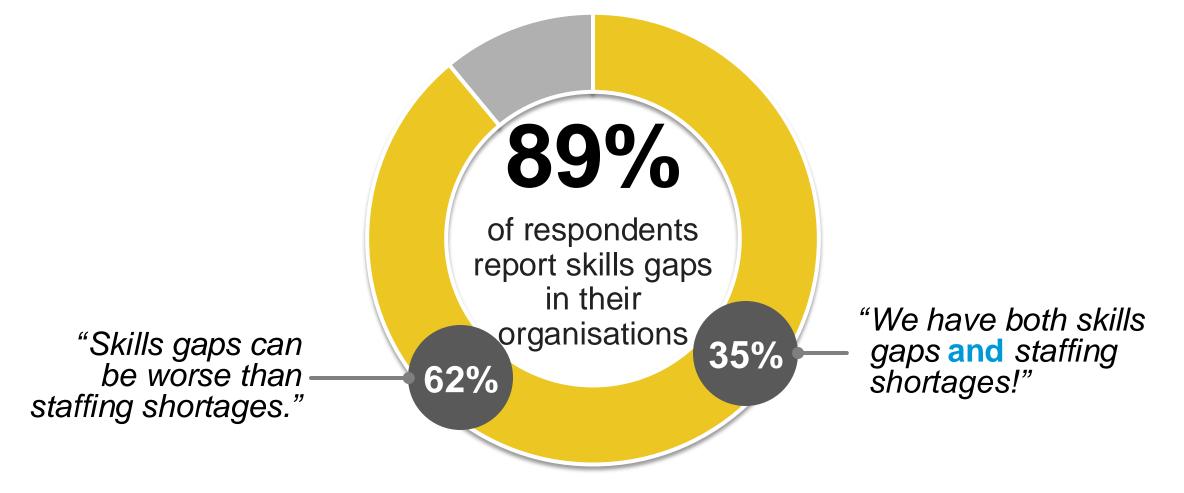
Organizations in the E.U. with no entry- or junior-level professionals on security teams





Skills Gaps Are a Growing Problem

It's not only about people; the skills problem is quickly outpacing shortage concerns



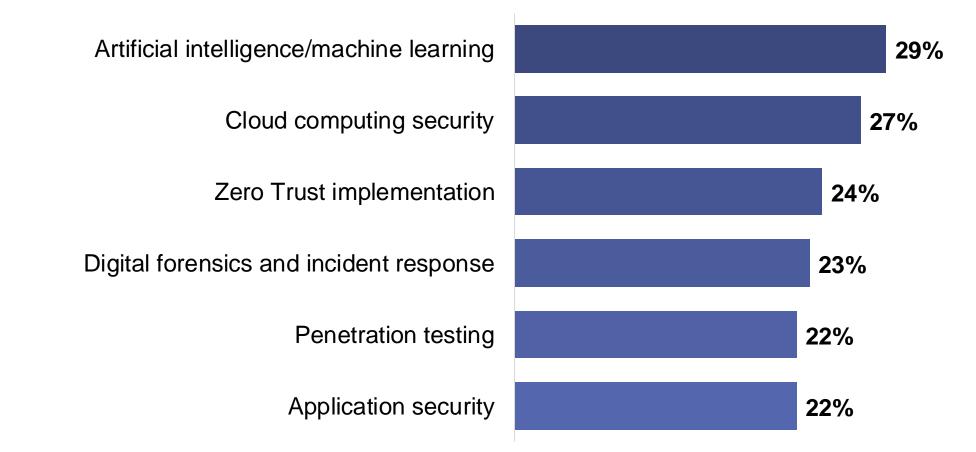




	CRITICAL skills gaps		
		reported	skills gaps reported
	Education	18%	96%
	Construction	20%	94%
	Healthcare	20%	94%
	Real estate	15%	93%
	Nonprofit	16%	92%
	Aerospace	19%	92%
	Telecommunications	19%	92%
Clobal akilla	Non-Security Software/Hardware Development	15%	92%
Global skills	Food/Beverage/Hospitality/Travel	16%	92%
gaps by industry	Government	20%	92%
	Manufacturing	17%	91%
	Energy/Power/Utilities	14%	91%
	Insurance	12%	91%
muustry	Military/military contractor	19%	90%
	IT services	17%	90%
	Transportation	17%	90%
	Financial services	13%	88%
	Hosted/cloud services	12%	88%
	Automotive	14%	88%
	Retail/Wholesale	17%	87%
	Entertainment/Media	17%	87%
	Consulting	12%	87%
	Engineering	15%	87%
	Security Software/Hardware Development	13%	84%
Source: 2024 ISC2 Cybersecurity Workforce Stu	dy. Legal	11%	83%

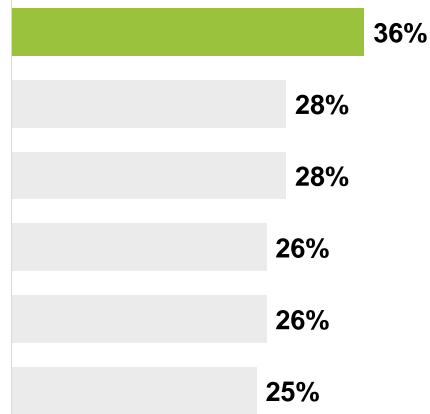


Where are the technical skills gaps on security teams?





Lack of qualified talent top reason for cybersecurity skills gaps in 2024



My organisation can't find people to hire with the skills we need My organisation doesn't have the budget to hire enough people IT often introduces new tech but doesn't have the expertise to secure it In general, we struggle to keep people with in-demand skills My organisation is growing faster than our team can keep up Leadership misaligns staff resources





Organisations are		
addressing skills gaps		
with training		

37% 37% 34% 31% 30% 28% 24% 24%

Implementing/improving online training platforms

Promoting free training and educational content from our security vendors

Outsourcing

Implementing/improving in-person training courses

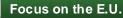
Cross-training employees from outside of cybersecurity on cybersecurity skills

Investing in security team attendance at industry conferences

Investing in more/new technology

Increasing certification reimbursements/requirements





The skills cybersecurity hiring managers are *looking for when hiring*

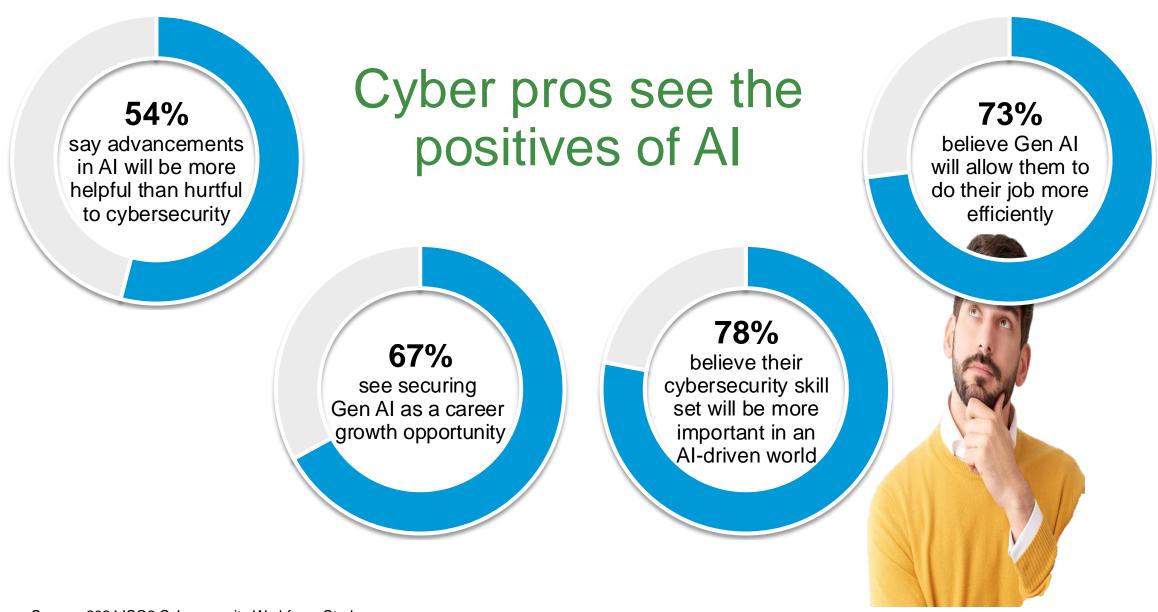
The skills cybersecurity professionals *think are in demand*

26%	Curious/eager to learn	21%	These nontechnical
25%	Teamwork and collaboration skills	22%	skills rank higher
21%	Strong problem-solving abilities	24%	
19%	Strong communication skills	27%	than technical skills
17%	Cloud computing security	26%	
15%	Strong strategic thinking skills	16%	
14%	Security engineering	12%	
13%	Strong project management skills	9%	
12%	Risk assessment, analysis & mgmt	16%	
12%	Security analysis	10%	
11%	Application security	11%	
11%	AI/ML	18%	
11%	GRC	18%	
11%	Time management and organisation	7%	
9%	Emotional intelligence	7%	
9%	Security administration	7%	
9%	Network monitoring	5%	
8%	Leadership abilities	9%	
8%	Identity and access management	9%	
7%	Threat intelligence analysis	9%	
7%	Operation technology security (ISC)	6%	
7%	Conflict resolution skills	7%	



Gen AI and the Cyber Profession

00



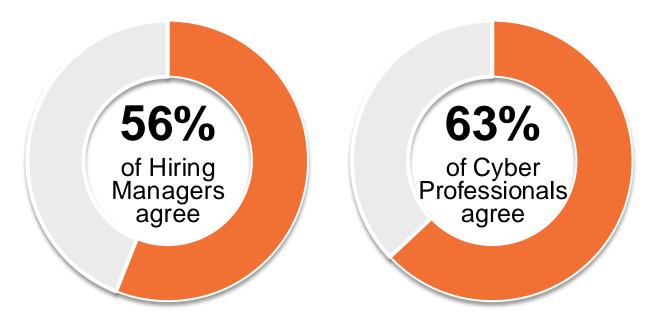
Source: 2024 ISC2 Cybersecurity Workforce Study.





Skills needed for AI/ML are somewhat unclear

"I don't know enough about Gen AI to identify the skills I'll need to succeed in an AI-driven world."







Source: 2024 ISC2 Cybersecurity Workforce Study.

57%

of respondents agree that nontechnical skills will be more important for cybersecurity professionals in an Al-driven world

Focus on the E.U.

	Building my cybersecurity skills/knowledge base	72%	
Cyber pros are future- proofing their skills for Al About half (53%) believe their skills will be complemented, not threatened, by Al	Learning more about Al and/or building AI-related skills	55%	
	Trying to become more of a strategic contributor and less of tactical one	47%	
	Obtaining certifications not related to AI	43%	
	Learning about possible vulnerabilities and exploits in AI solutions	42%	
	Obtaining new Al-related certifications	25%	
	Obtaining a new degree	23%	
	Considering changing careers	18%	
	Attempting to move into a managerial role	13%	

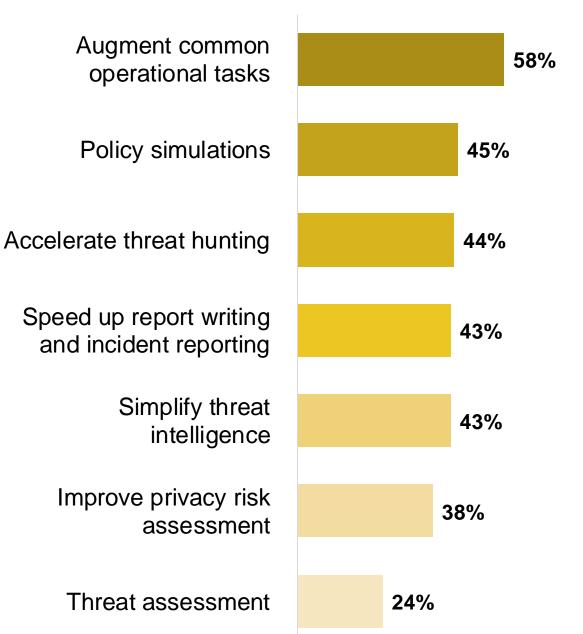


ISC₂

How Gen AI is being used now

61% feel confident in their ability to utilize Gen AI in their roles today

And **71%** feel they will be able to effectively use Gen AI within their role in the next 2 years





Gen AI is being integrated into organisations; most have use policies

52% of pros say Gen AI is built into the cybersecurity tools they use

72% say their organisations have implemented Gen AI in other parts of the organisation



Organisations face Gen AI adoption barriers

Lack of expertise	56%	
Data privacy & security concerns	49%	
Lack of a clear Gen AI strategy	38%	
Lack of training	34%	
Lack of staff	32%	
Lack of understanding where to apply Gen AI	25%	
Lack of employee readiness	25%	
Lack of budget	24%	
Lack of executive support	23%	
Issues integrating with existing infrastructure	21%	
Issues with data infrastructure	20%	
Reconciling Gen AI recommendations that conflict with legacy practices	14%	



Organisations are already seeing Gen Al benefits and expect more in the future

		See this benefit nov	v Totals
Reduced time spent on tedious tasks	43%		<mark>51%</mark> 94%
Improved threat detection		<mark>57%</mark>	<mark>36%</mark> 93%
Easier access to information	41%		51% 92%
Improved ability to make decisions		<mark>57%</mark>	30% 87%
Improved decision-making capabilities	5	<mark>4%</mark>	<mark>32%</mark> 86%
Reduced costs for my organisation/team	52	<mark>2%</mark> 29	<mark>9%</mark> 81%
Reduction in/easing of the effects of skills gaps at my organisation	51	<mark>% 27</mark> 9	<mark>%</mark> 78%
Reduction in/easing of the effects of staffing shortages at my organisation	48%	<mark>% 22%</mark>	70%

Source: 2024 ISC2 Cybersecurity Workforce Study.



2024 ISC2 Cybersecurity Workforce Study Focus on the E.U.

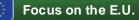












ISC 2

2024 ISC2 Cybersecurity Workforce Study

ISC2.org/research

ISC2 CYBERSECURITY WORKFORCE STUDY



Global Cybersecurity Workforce Prepares for an Al-Driven World









The past year has been challenging for cybersecurity professionals. If you have been feeling higher levels of stress in your roles, you are not alone.

Focus on learning skills, both technical and nontechnical, that are in demand.

Consider hiring entry- or junior-level professionals for your team. Hire for nontechnical attributes, train for technical skills.

Conversation starters

Why are cybersecurity teams seem as expendable despite increasing threats?

How do you keep your team focused on skill building, especially when budgets tighten?

How do you maintain team resilience when you're understaffed?

How involved is your team in securing AI and setting the rules for its use in your organisation?



Thank You!

ISC2

© ISC2. All rights reserved. This presentation's images are subject to copyright protection and used under license from third parties. Do not use images from this presentation in other presentations or documents without first consulting with the creative team. The use of copyrighted images outside the licensed scope constitutes copyright infringement and subjects the user to monetary damages and other penalties.