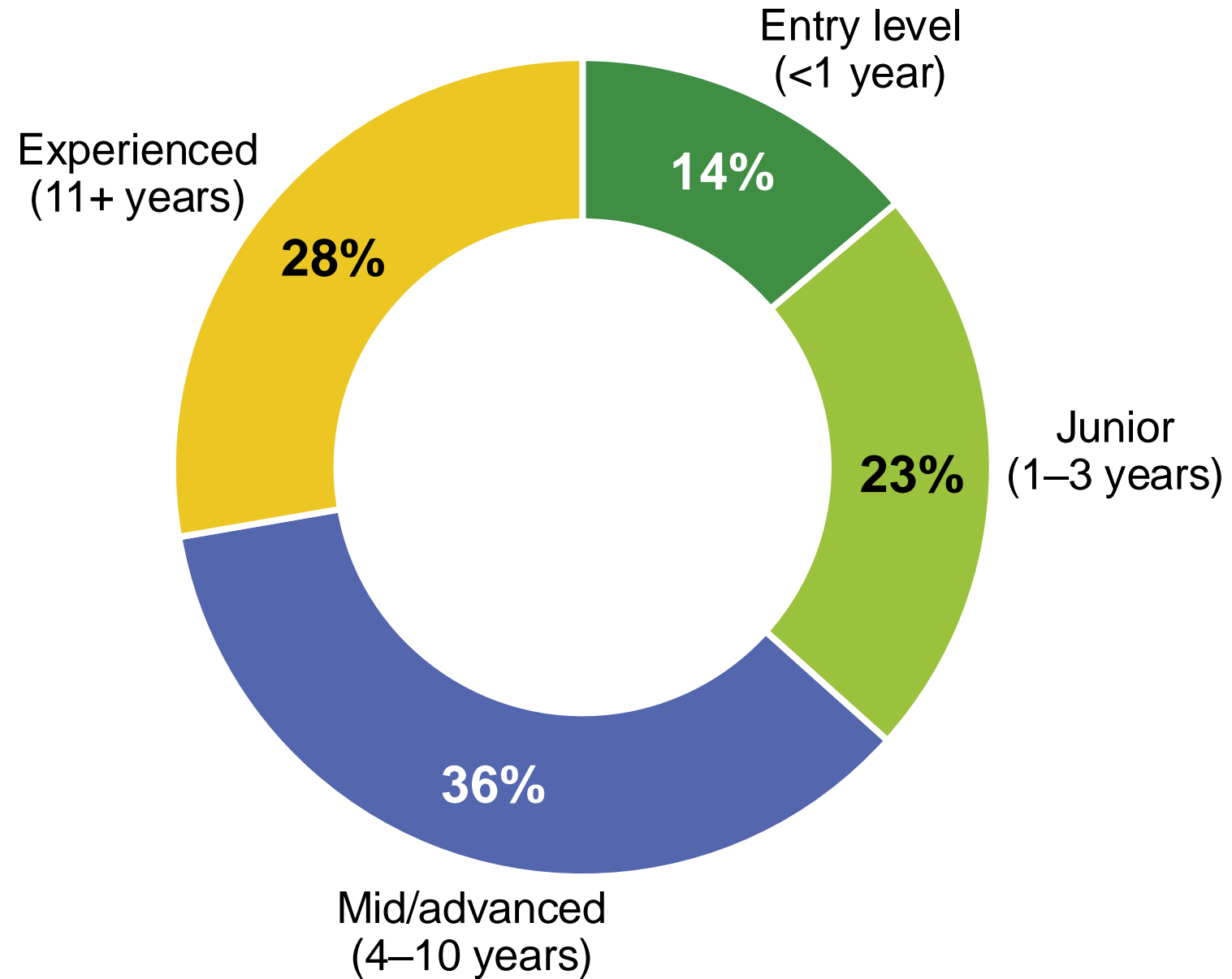ISC2™

Your Future. Secured.

First Look at the 2024 Cybersecurity Workforce Survey

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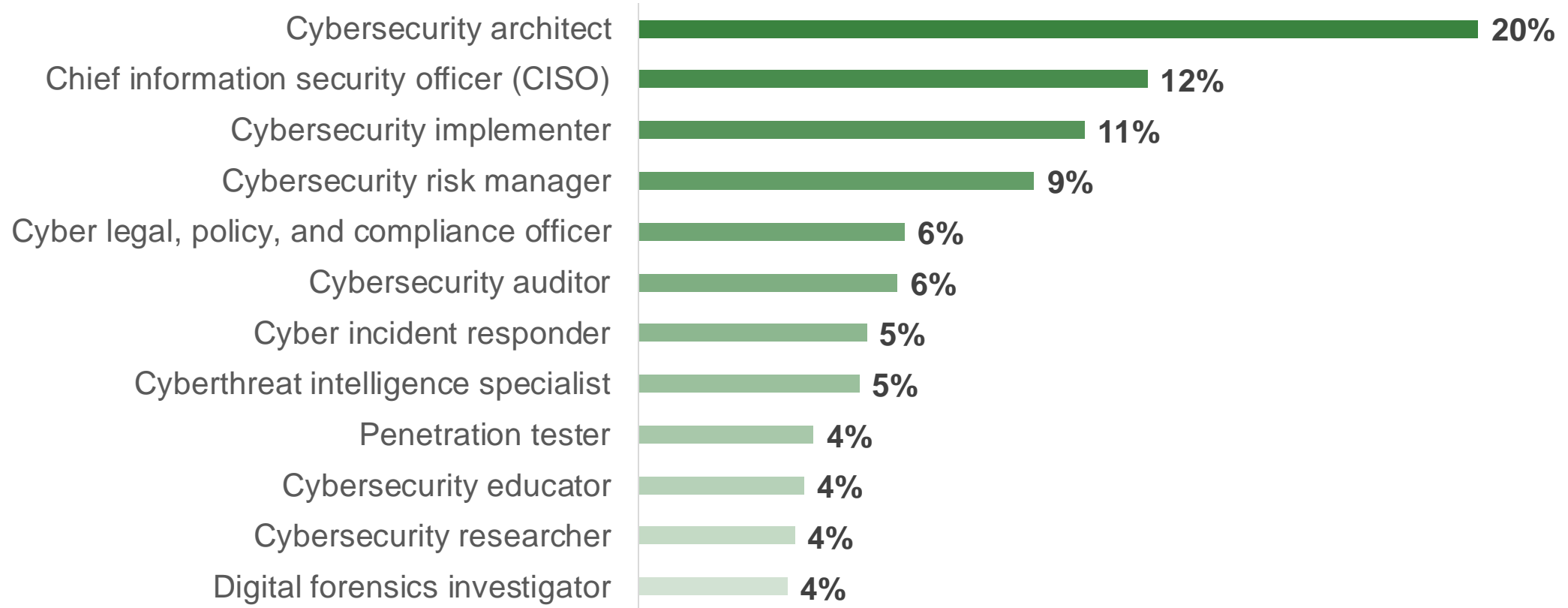
Average cybersecurity team composition in the E.U. by level/years of experience

Entry level (<1 year)
14%

Junior (1–3 years)
23%

Mid/advanced (4–10 years)
36%

Experienced (11+ years)
28%

Source: 2024 ISC2 Cybersecurity Workforce Study.

ISC2

E.U. Respondents' Profile as per ECSF

Profile	Percentage
Cybersecurity architect	20%
Chief information security officer (CISO)	12%
Cybersecurity implementer	11%
Cybersecurity risk manager	9%
Cyber legal, policy, and compliance officer	6%
Cybersecurity auditor	6%
Cyber incident responder	5%
Cyberthreat intelligence specialist	5%
Penetration tester	4%
Cybersecurity educator	4%
Cybersecurity researcher	4%
Digital forensics investigator	4%

ISC2

Threat Landscape

🇪🇺 In the European Union,

72%

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

🇪🇺 In the European Union,

42%

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

🇪🇺 In the European Union,

53%

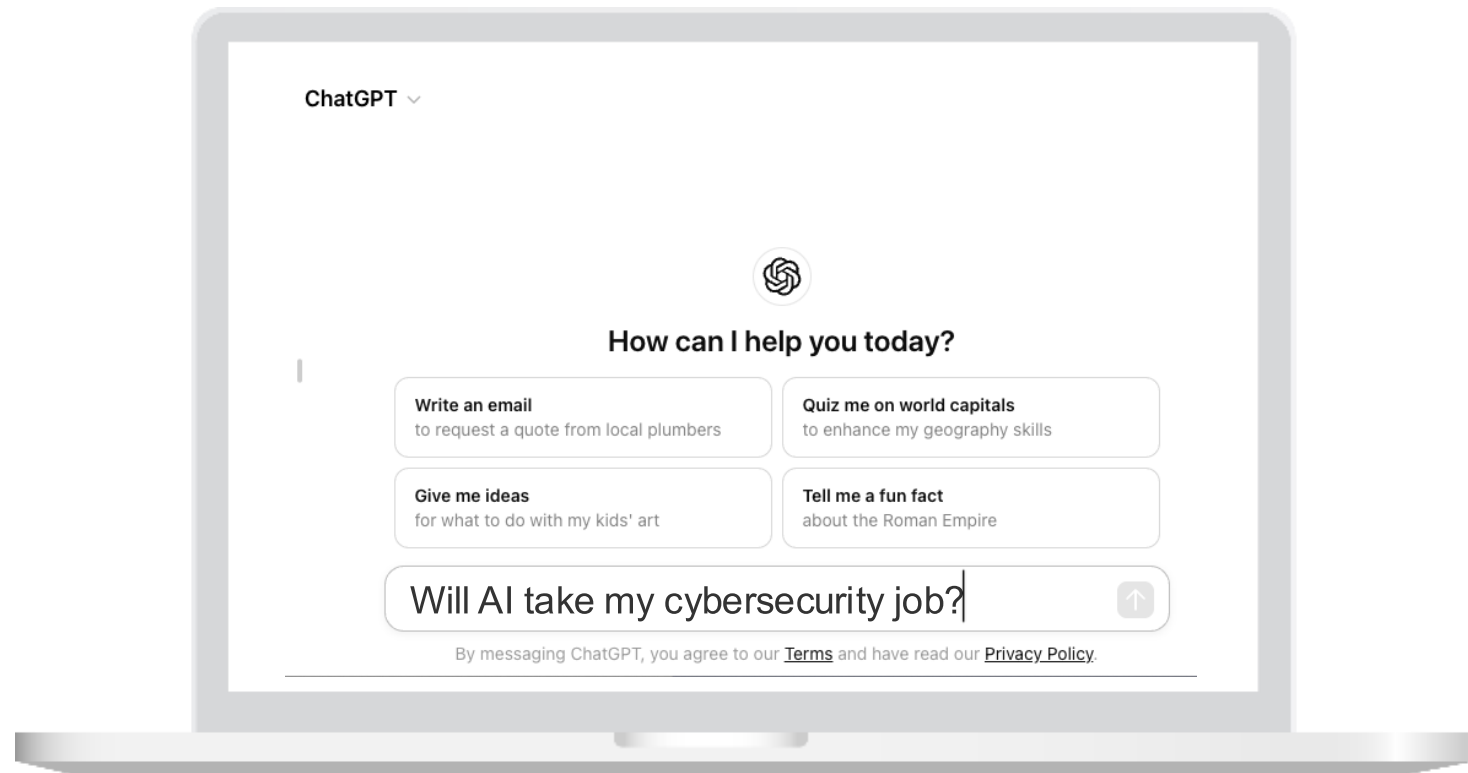anticipate a rise in malicious actors contacting cybersecurity professionals over the next year

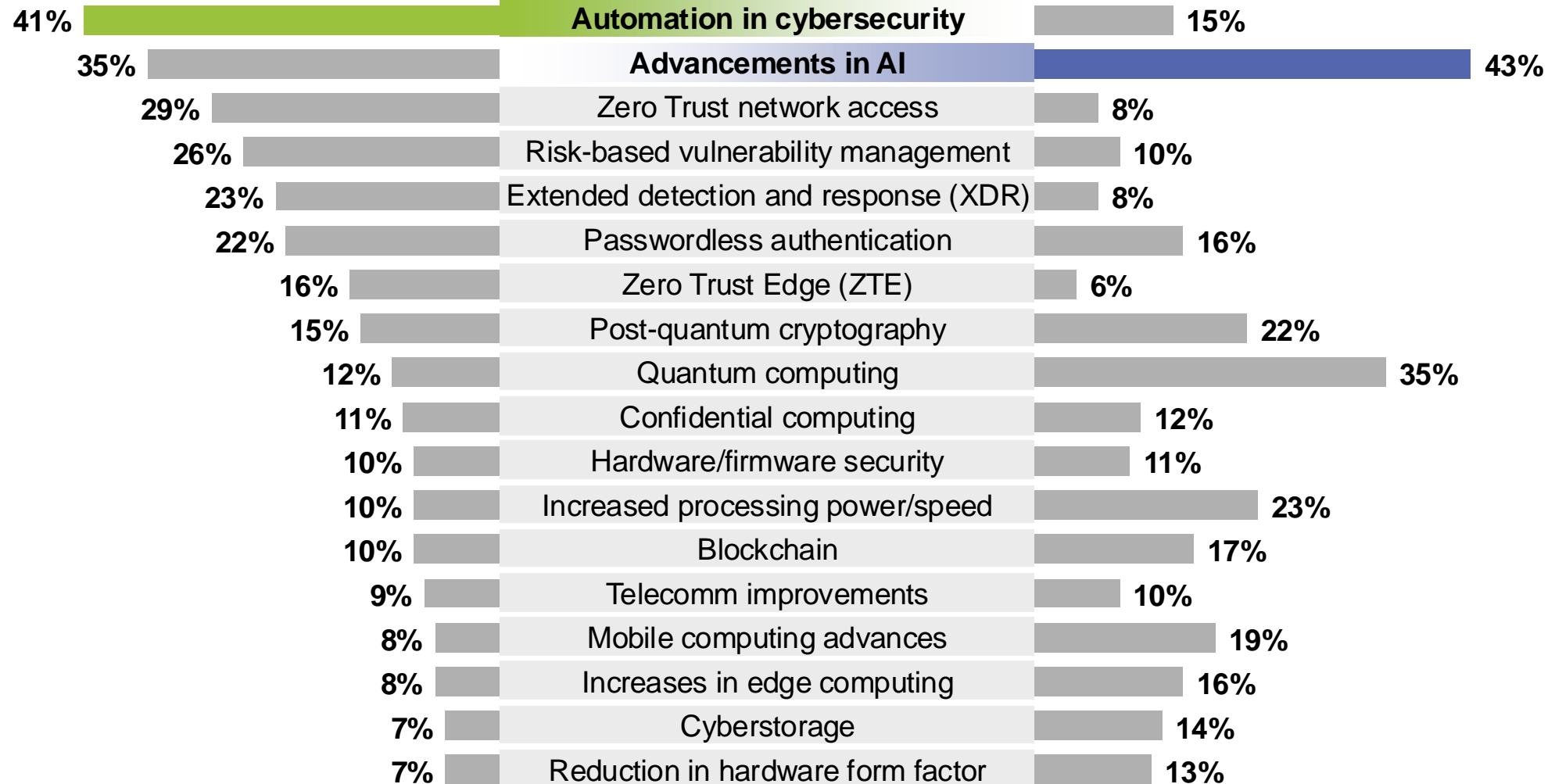🇪🇺 In the European Union,

48%

say the biggest challenge the industry faces will be emerging technologies

Source: 2024 ISC2 Cybersecurity Workforce Study.

ISC2

Tech with the greatest *positive* impact on organizational security in the E.U.

Tech with the greatest *negative* impact on organizational security in the E.U.

Positive	Technology	Negative
41%	**Automation in cybersecurity**	15%
35%	**Advancements in AI**	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%

ISC2

Workforce and Skills Gaps

Cybersecurity workforce size in the E.U. slowed while gap continues to increase
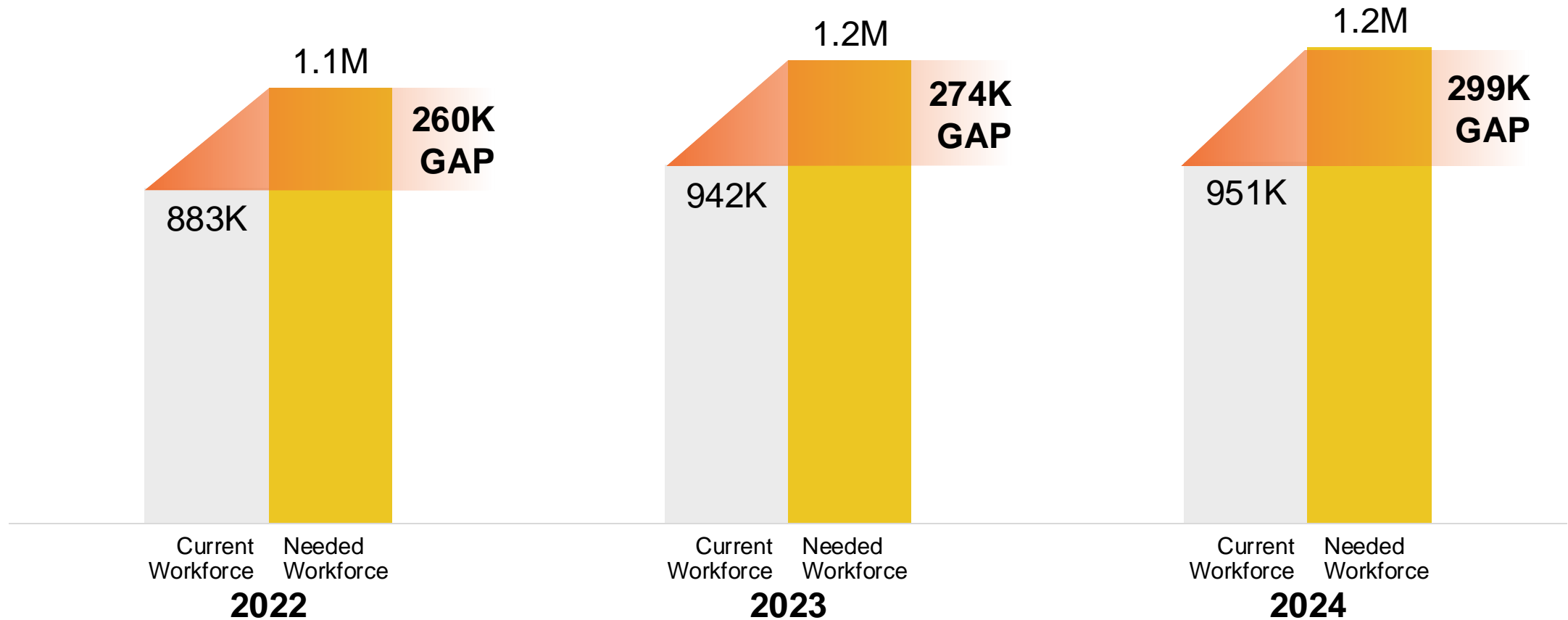
Source: 2022–2024 ISC2 Cybersecurity Workforce Studies. The ISC2 Cybersecurity Workforce Gap is an estimate of the number of people needed globally to adequately secure organisations. The Workforce Gap is not an estimate of open positions or cybersecurity jobs available.

🇪🇺 In the European Union,

55%

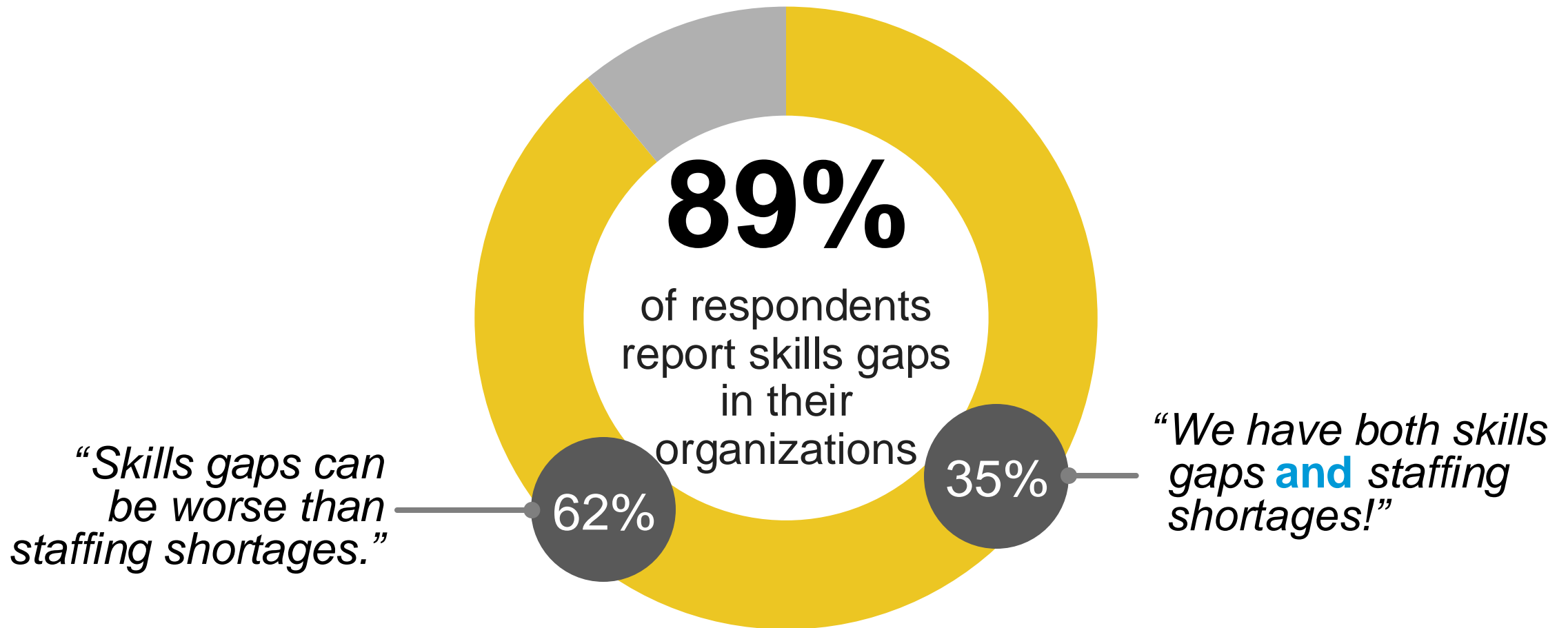say that staffing shortages put their organizations at significant risk

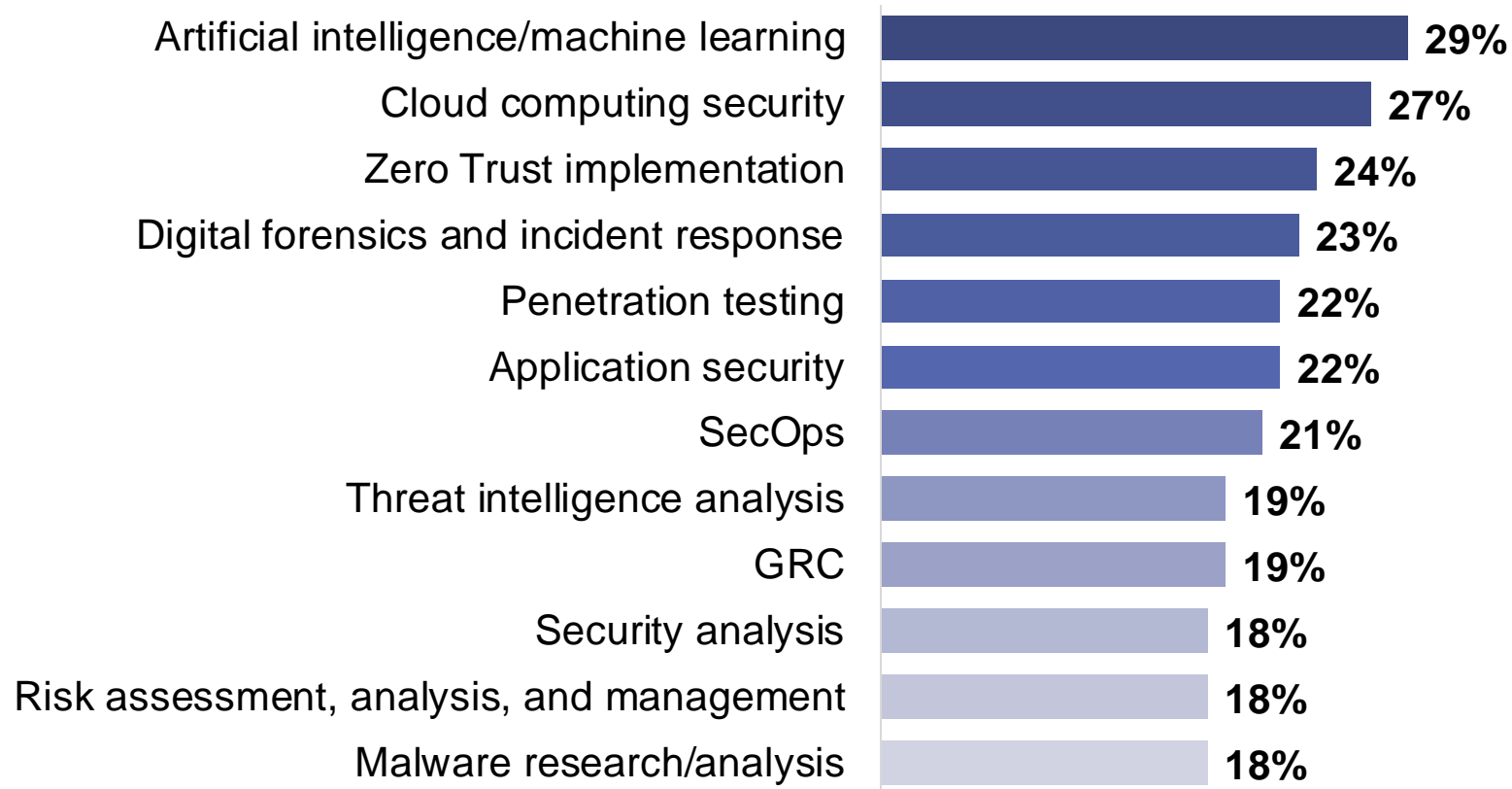# Reasons for cybersecurity staff shortages in the E.U.

Reason	Percentage
My organization can't find enough qualified talent	46%
My organization doesn't have the budget	27%
My organization doesn't pay a competitive wage	26%
Leadership misaligns staff resources	24%
My organization can't offer opportunities for growth/promotion for security staff	24%
My organization is struggling to keep up with turnover/attrition	21%
My organization doesn't put enough resources into training non-security IT staff to become security staff	21%
My organization doesn't prioritize security	19%
My organization has implemented new technologies that we don't have the skills to operate/optimize yet	18%
My organization has attempted to replace jobs with technology (other than genAI) that is not yet sufficient	10%
My organization has attempted to replace jobs with genAI technology that is not yet sufficient	7%
We have had cutbacks because of company performance	6%

Source: 2024 ISC2 Cybersecurity Workforce Study.

ISC2

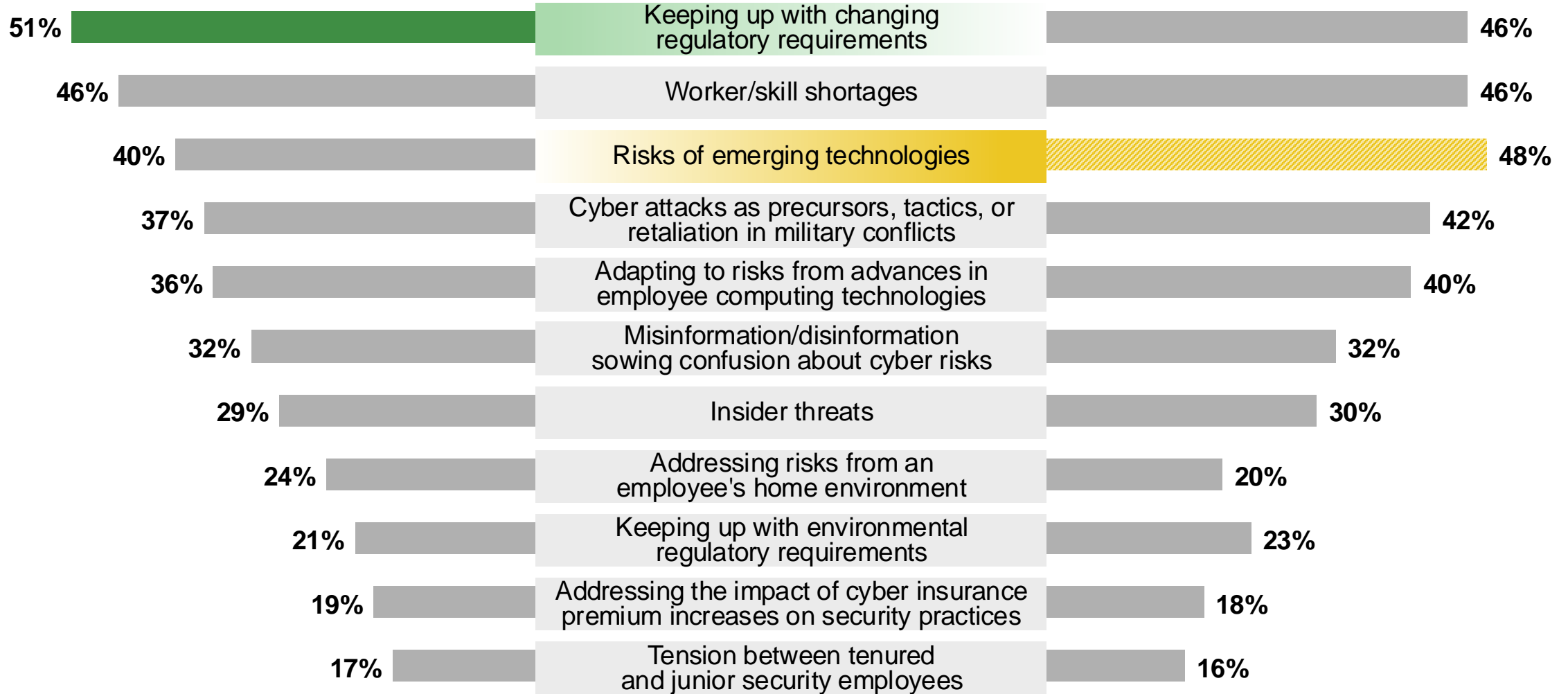# It's not only about people; the skills problem in the E.U. is quickly outpacing shortage concerns

89%

of respondents report skills gaps in their organizations

"Skills gaps can be worth than staffing shortages."

62%

35%

*"We have both skills gaps **and** staffing shortages!"*

ISC2

Where are the technical skills gaps on E.U. security teams?

Skill	Percentage
Artificial intelligence/machine learning	29%
Cloud computing security	27%
Zero Trust implementation	24%
Digital forensics and incident response	23%
Penetration testing	22%
Application security	22%
SecOps	21%
Threat intelligence analysis	19%
GRC	19%
Security analysis	18%
Risk assessment, analysis, and management	18%
Malware research/analysis	18%

Source: 2024 ISC2 Cybersecurity Workforce Study.

ISC2

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*

Challenge	Past 12 months	Next two years
Keeping up with changing regulatory requirements	51%	46%
Worker/skill shortages	46%	46%
Risks of emerging technologies	40%	48%
Cyber attacks as precursors, tactics, or retaliation in military conflicts	37%	42%
Adapting to risks from advances in employee computing technologies	36%	40%
Misinformation/disinformation sowing confusion about cyber risks	32%	32%
Insider threats	29%	30%
Addressing risks from an employee's home environment	24%	20%
Keeping up with environmental regulatory requirements	21%	23%
Addressing the impact of cyber insurance premium increases on security practices	19%	18%
Tension between tenured and junior security employees	17%	16%

Source: 2024 ISC2 Cybersecurity Workforce Study.

ISC2

Organizations in the E.U. have experienced cybersecurity cutbacks in the past 12 months

Layoffs
- 2023: 21%
- 2024: 20%
- Change: -1%

Budget cuts
- 2023: 28%
- 2024: 31%
- Change: 3%

Hiring freezes
- 2023: 29%
- 2024: 33%
- Change: 4%

Freezes on promotions
- 2023: 23%
- 2024: 29%
- Change: 6%

Source: 2024 ISC2 Cybersecurity Workforce Study.

ISC2

In the European Union,

32% expect cybersecurity cutbacks in 2025
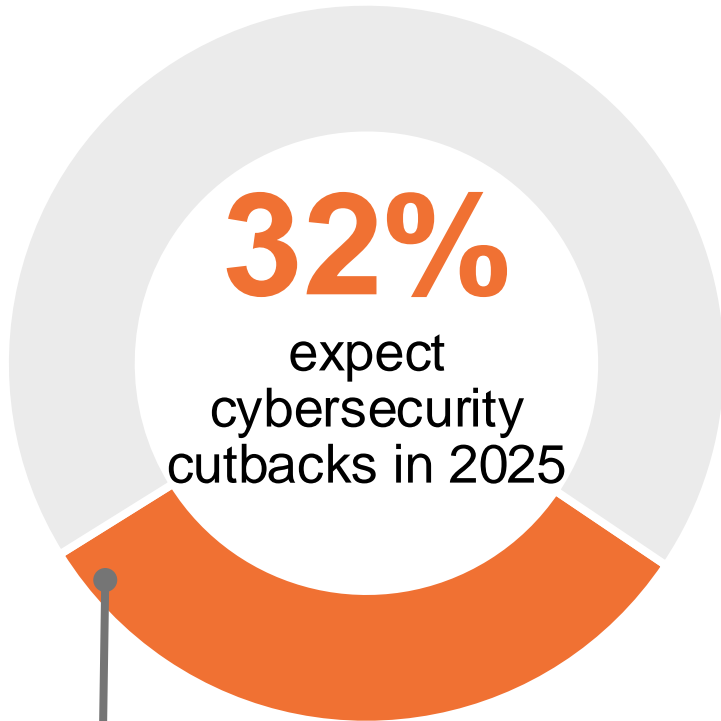
18% expect layoffs in 2025

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

Cybersecurity job satisfaction is declining in the E.U.

78%

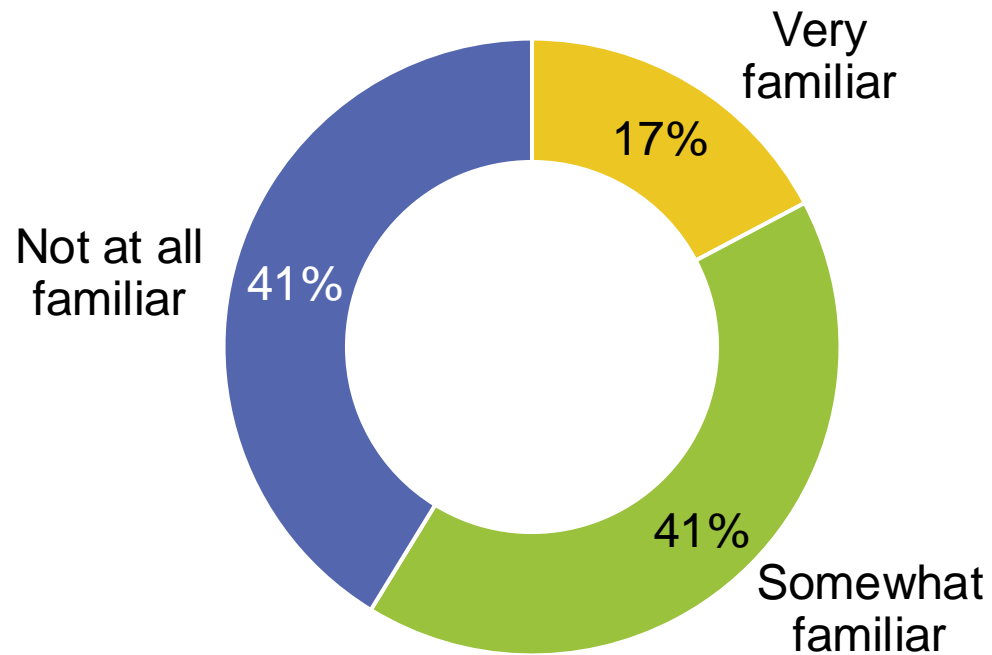**74%**

70%

2022

2023
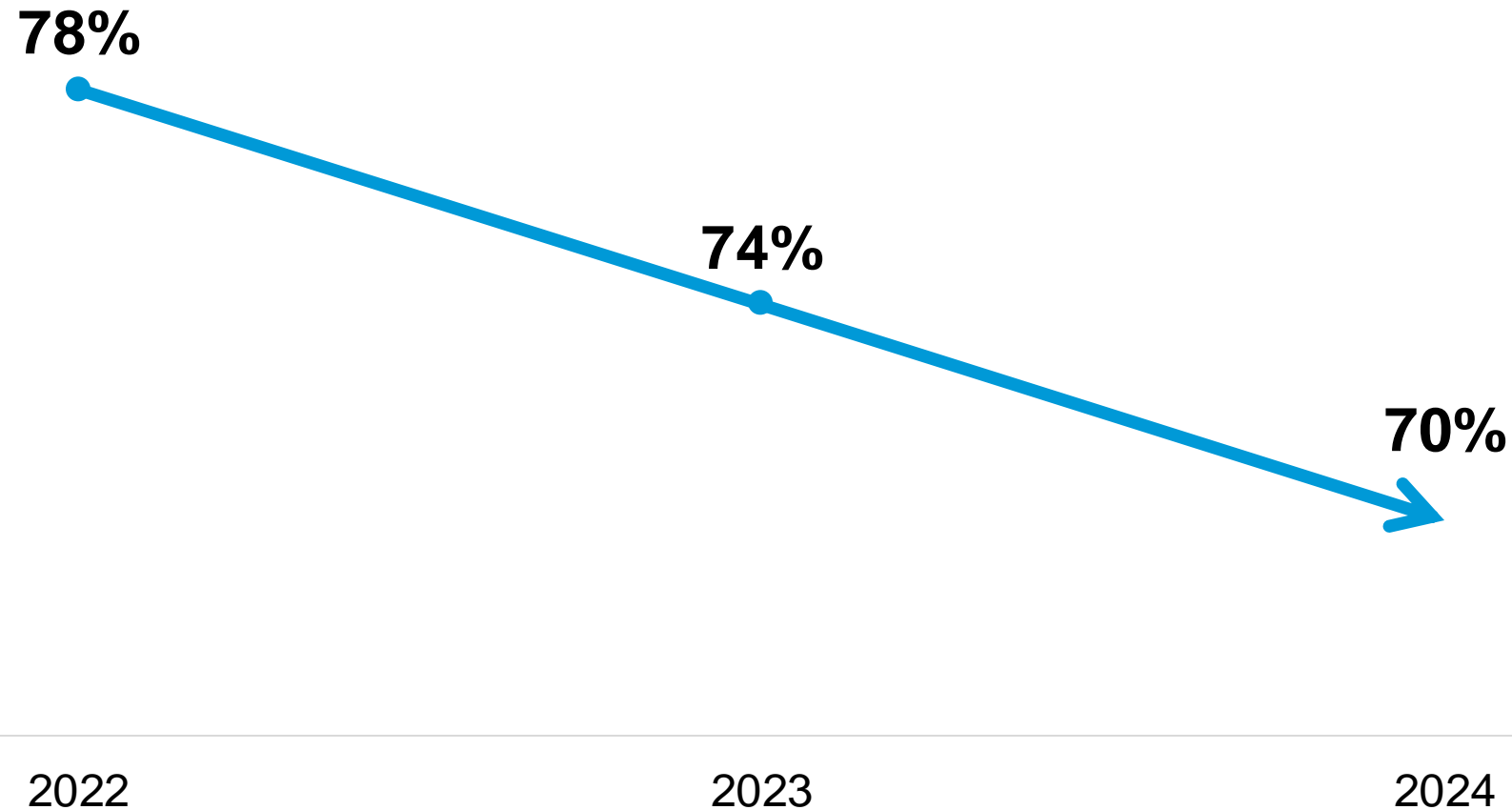
2024

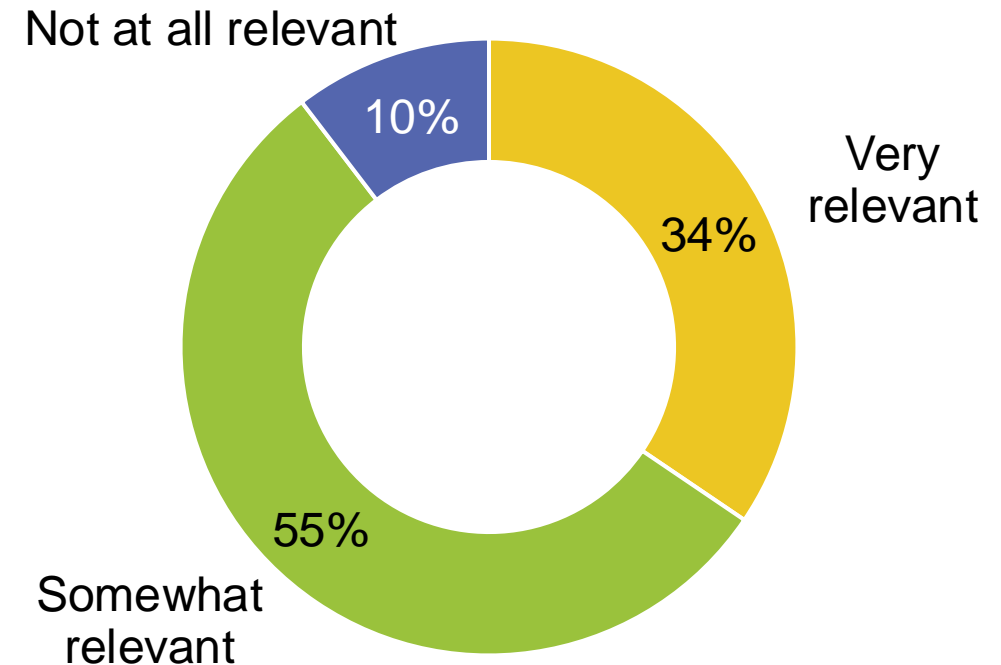Source: 2024 ISC2 Cybersecurity Workforce Study.

ISC2

The Regulatory Landscape

Familiarity with ECSF developed by ENISA not universal (59%), yet 90% think it is relevant

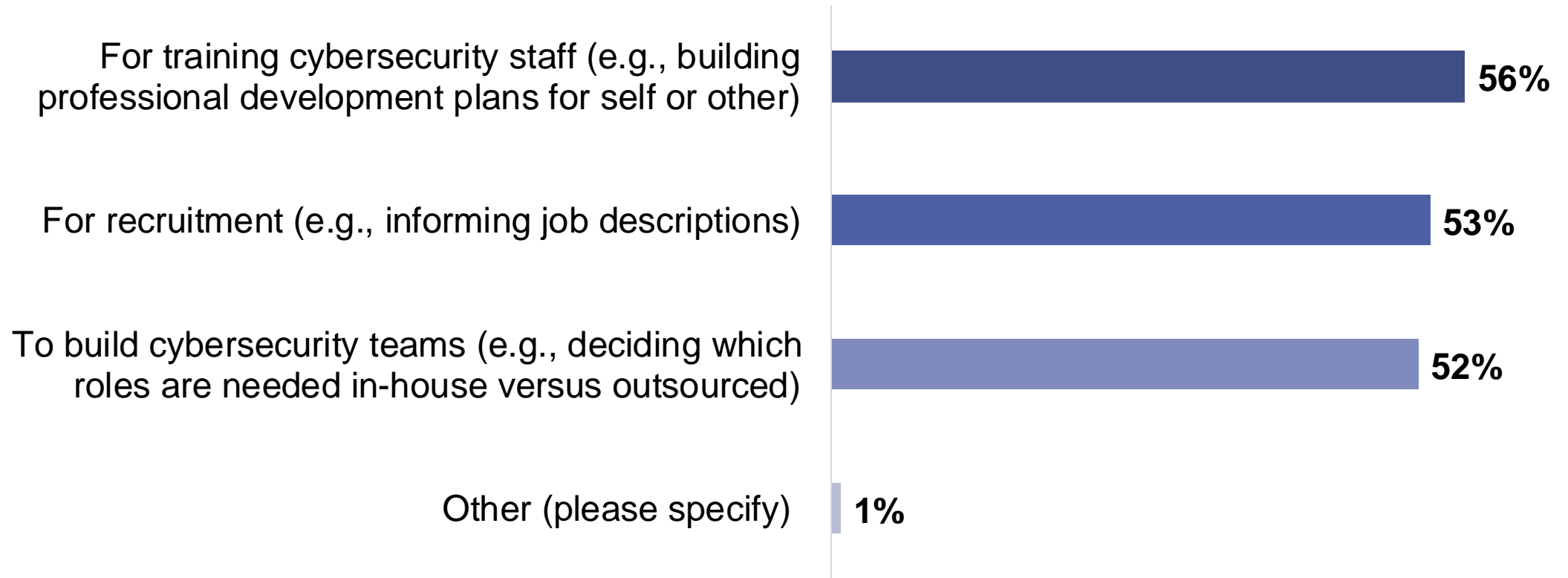## Please rate your level of familiarity with the ECSF

Very familiar 17%

Somewhat familiar 41%

Not at all familiar 41%

How relevant is the ECSF to the cybersecurity profession?

Not at all relevant 10%

Very relevant 34%

Somewhat relevant 55%

ISC2

ECSF useful for training, recruitment, and staffing

How do you or your organization plan to use the ECSF?

Category	Percentage
For training cybersecurity staff (e.g., building professional development plans for self or other)	56%
For recruitment (e.g., informing job descriptions)	53%
To build cybersecurity teams (e.g., deciding which roles are needed in-house versus outsourced)	52%
Other (please specify)	1%

Source: 2024 ISC2 Cybersecurity Workforce Study.

ISC2

54% are prepared to implement EU CRA; CISO, compliance, and architects needed

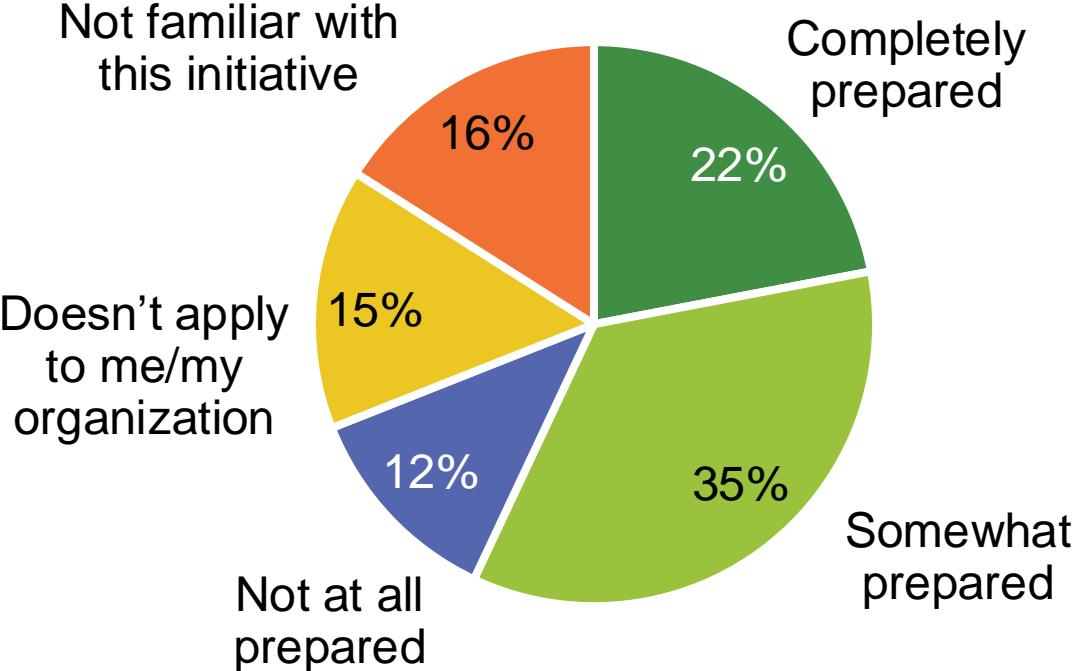## Level of preparedness to implement requirements of EU CRA

- Completely prepared 20%
- Somewhat prepared 34%
- Not at all prepared 10%
- Doesn't apply to me/my organization 18%
- Not familiar with this initiative 19%

Roles needed to implement CRA

Role	%
CISO	52%
Cyber legal, policy, and compliance officer	43%
Cybersecurity architect	35%
Cybersecurity risk manager	31%
Cybersecurity auditor	26%
Cybersecurity implementer	24%
Cyber incident responder	23%
Cyber threat intelligence specialist	18%
Cybersecurity educator	15%
Cybersecurity researcher	11%
Penetration tester	11%
Digital forensics investigator	11%

Source: 2024 ISC2 Cybersecurity Workforce Study.

ISC2

57% are prepared to implement EU NIS2; CISO, compliance, and risk managers needed

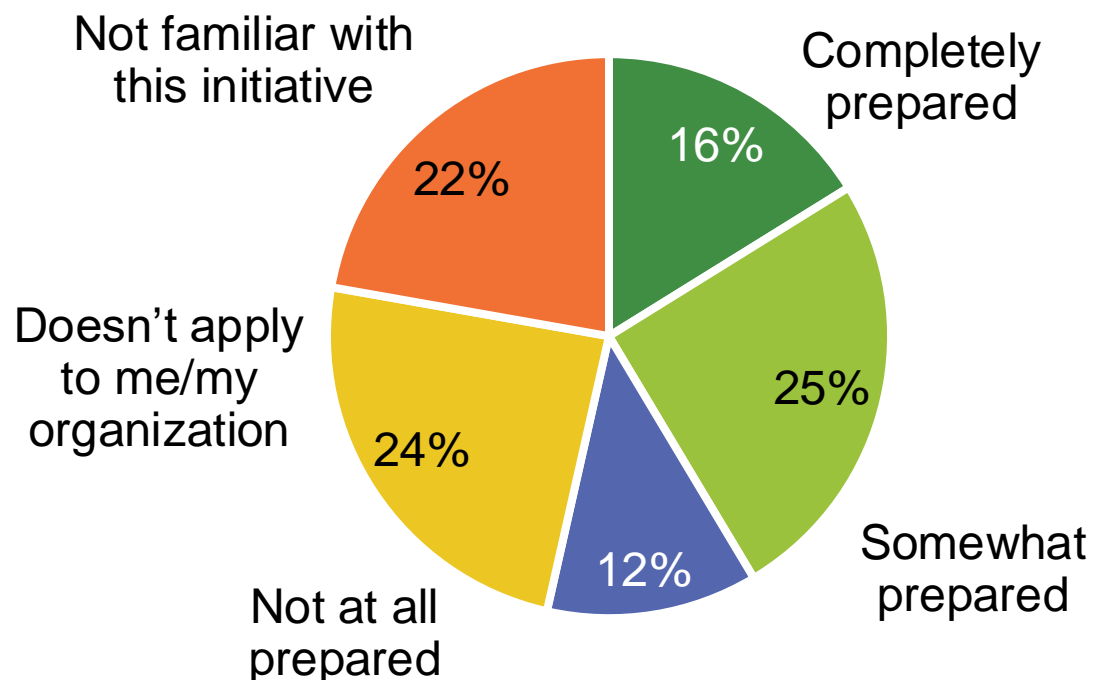## Level of preparedness to implement requirements of EU NIS2 directive

- Completely prepared: 22%
- Somewhat prepared: 35%
- Not at all prepared: 12%
- Doesn't apply to me/my organization: 15%
- Not familiar with this initiative: 16%

Roles needed to implement NIS2

Role	Percentage
CISO	52%
Cyber legal, policy, and compliance officer	42%
Cybersecurity risk manager	36%
Cybersecurity architect	31%
Cybersecurity auditor	25%
Cybersecurity implementer	25%
Cyber incident responder	21%
Penetration tester	15%
Cyber threat intelligence specialist	15%
Cybersecurity educator	14%
Cybersecurity researcher	13%
Digital forensics investigator	12%

Source: 2024 ISC2 Cybersecurity Workforce Study.

ISC2

41% are prepared to implement DORA; CISOs, compliance, and risk managers needed

Level of preparedness to implement requirements of DORA

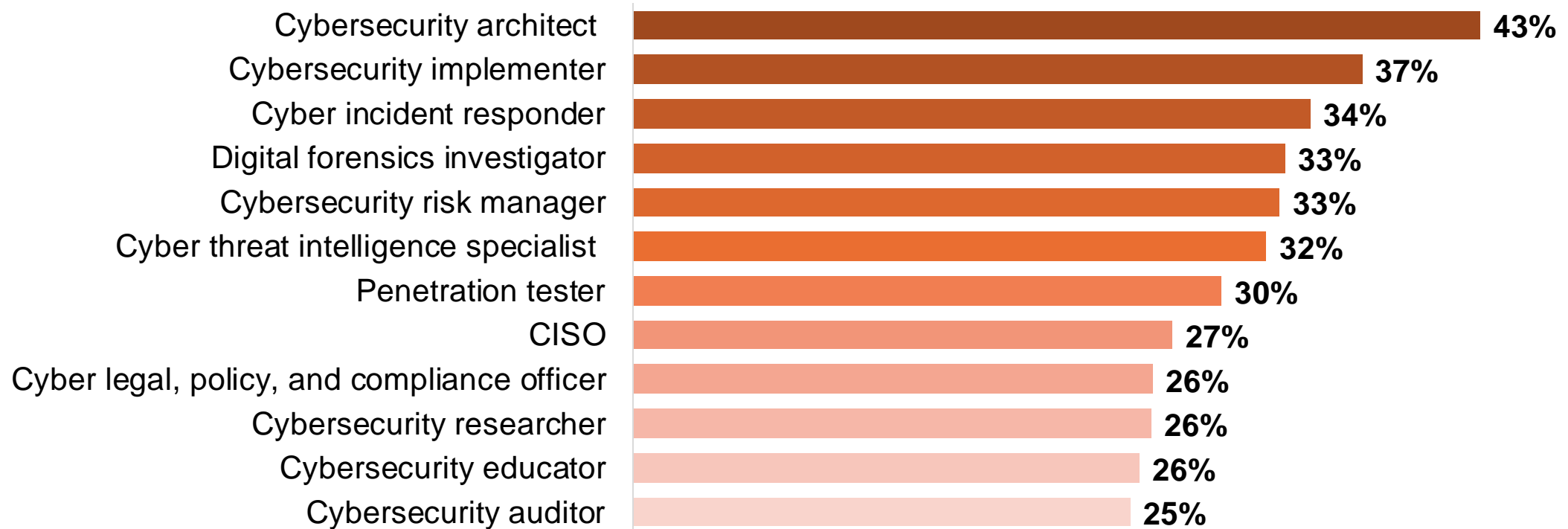- Completely prepared: 16%
- Somewhat prepared: 25%
- Not at all prepared: 12%
- Doesn't apply to me/my organization: 24%
- Not familiar with this initiative: 22%

Roles needed to implement DORA

Role	%
CISO	48%
Cyber legal, policy, and compliance officer	41%
Cybersecurity risk manager	32%
Cybersecurity architect	29%
Cybersecurity auditor	25%
Cybersecurity implementer	21%
Cyber incident responder	20%
Cyber threat intelligence specialist	18%
Penetration tester	17%
Digital forensics investigator	17%
Cybersecurity educator	16%
Cybersecurity researcher	15%

ISC2

E.U. organizations are most lacking architects (needed to implement CRA, NIS2, and DORA)

In which of the following areas/roles is your organization lacking cybersecurity talent?

Role	Percentage
Cybersecurity architect	43%
Cybersecurity implementer	37%
Cyber incident responder	34%
Digital forensics investigator	33%
Cybersecurity risk manager	33%
Cyber threat intelligence specialist	32%
Penetration tester	30%
CISO	27%
Cyber legal, policy, and compliance officer	26%
Cybersecurity researcher	26%
Cybersecurity educator	26%
Cybersecurity auditor	25%

Source: 2024 ISC2 Cybersecurity Workforce Study.

ISC2

Key takeaways

- The past year has been challenging for cybersecurity professionals.

- The threat landscape is the worst in five years.

- For the first time, growth in cyber workforce has slowed down with teams experiencing cutbacks.

- Regulatory and legislative requirements continue to place pressure on cybersecurity teams and impacting skills deficits.

- In this context, it remains vital for the new EU mandate to continue to prioritize investment in cybersecurity workforce and skills development.

Thank You!

ISC2™