SIRP

Security Analysts

Attitudes to automation

June/July 2020

Project overview and methodology

1. The survey was conducted among 250 security professionals who manage threat alerts in the UK working in companies of 500 employees or more.

2. At an overall level results are accurate to ± 6.2% at 95% confidence limits assuming a result of 50%.

3. The interviews were conducted online by Sapio Research in June 2020 using an email invitation and an online survey.

Key stats

Organisations receive an average of **840** security alerts a **day**

Security professionals spend **18%** of their day **managing alerts**

52% are at least **slightly frustrated** by the current process for investigating threats

Only **32%** of the alert triage and incident response is automated

76% feel good about having more process automation

Time spent on **mundane tasks that should be automated** is what **51%** dislike most about their job

Summary and Overview

1. **Security analysts are busy on a daily basis dealing with alerts –** Organisations receive an average of 840 security alerts a day, with security professionals spending 18% of their day managing these alerts. Organisations have an average of 12 security tools.

2. **Dealing with alerts is still not a perfect system –** Almost a third believe missed alerts due to high alert volumes is a significant problem. In addition to this, over a quarter of overall alerts turn out to be false positives. It's not surprising that over half are at least slightly frustrated by the current process for investigating threats.

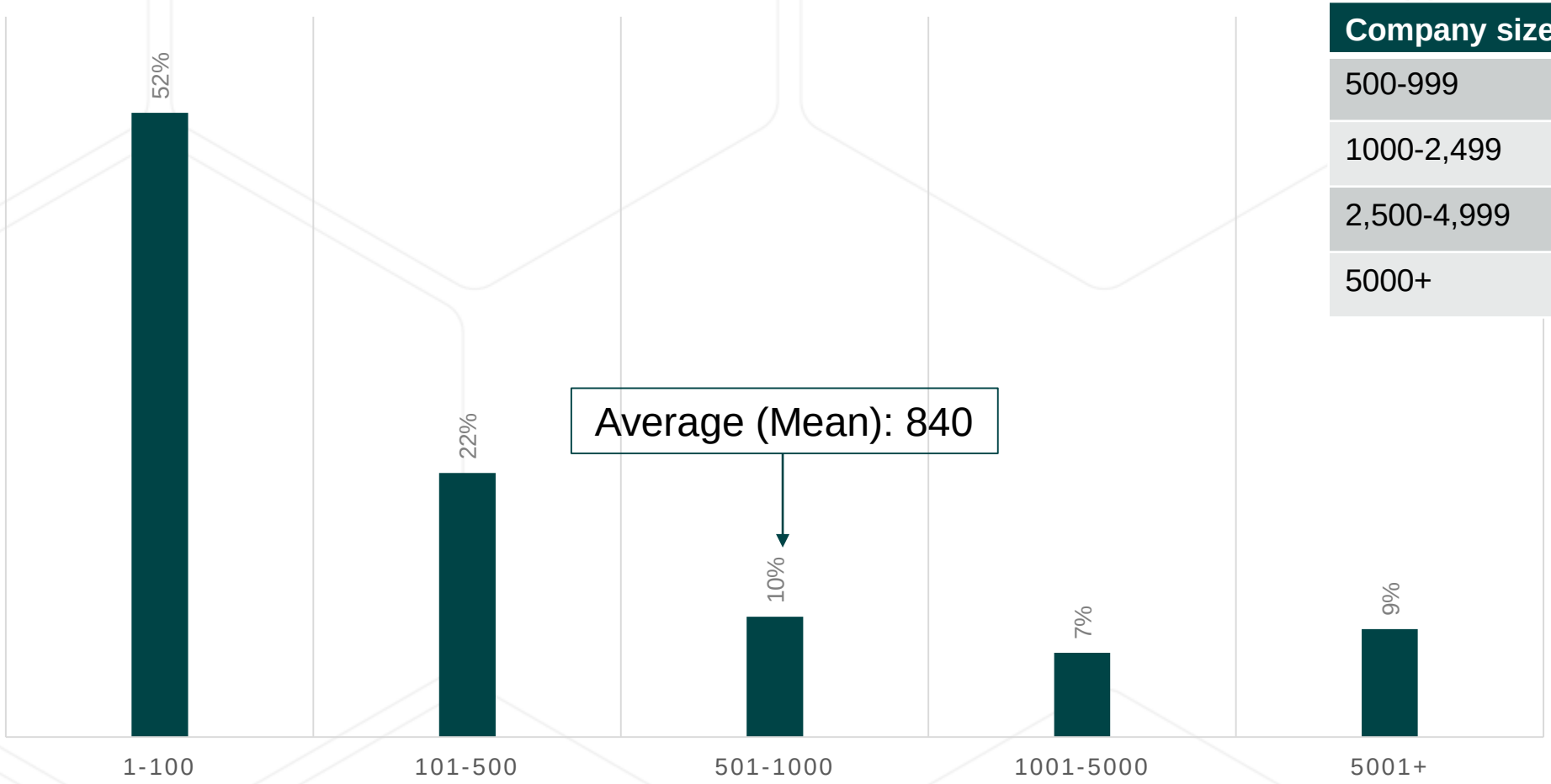
3. **The prospect of automation –** On average, under a third of the alert triage and incident response is automated. Although only 4% are unable to prioritise alerts based on risks to their organisation, over three quarters would still feel good about having more process automation.

4. **How automation could help job satisfaction –** The team spirit is what two thirds enjoy most about their job, followed by investigating alerts for over 2 in 5. Time spent on mundane tasks that should be automated is what half dislike most about their job. Perhaps automation could help, as currently almost half are considering leaving their role.

5. **The effects of Covid-19 –** The pandemic may have sped the journey towards automation, with almost half having experienced a reduced workforce as a result of it, and just over 2 in 5 spending more time on non-productive tasks and feeling pressure on the job.

Findings

Organisations receive an average of 840 security alerts a day

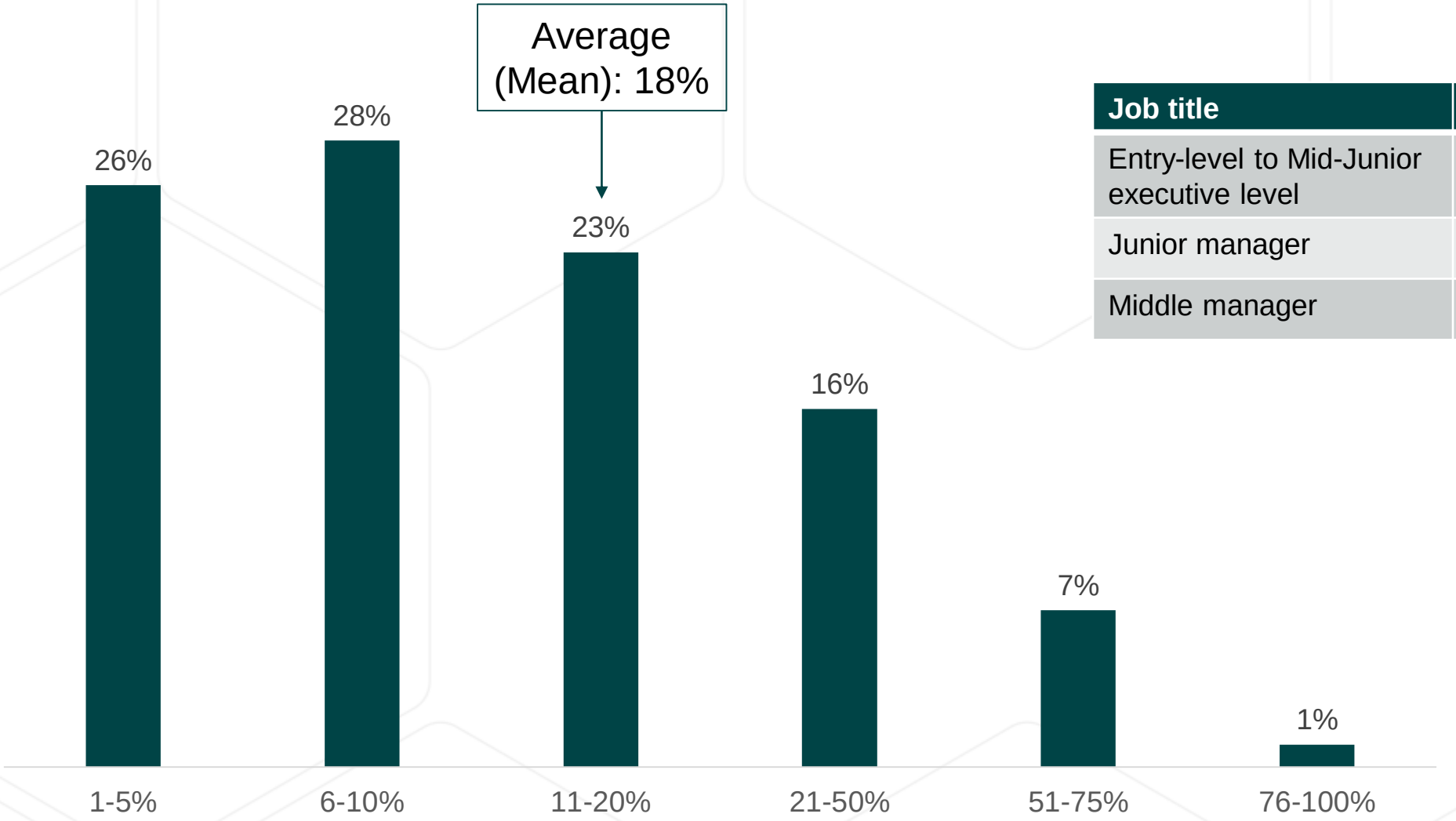


Company size	Average
500-999	175
1000-2,499	653
2,500-4,999	484
5000+	1520

Q1. On average how many security alerts does your organisation receive in a day? Select one

Base: 250

Security professionals spend 18% of their day managing alerts

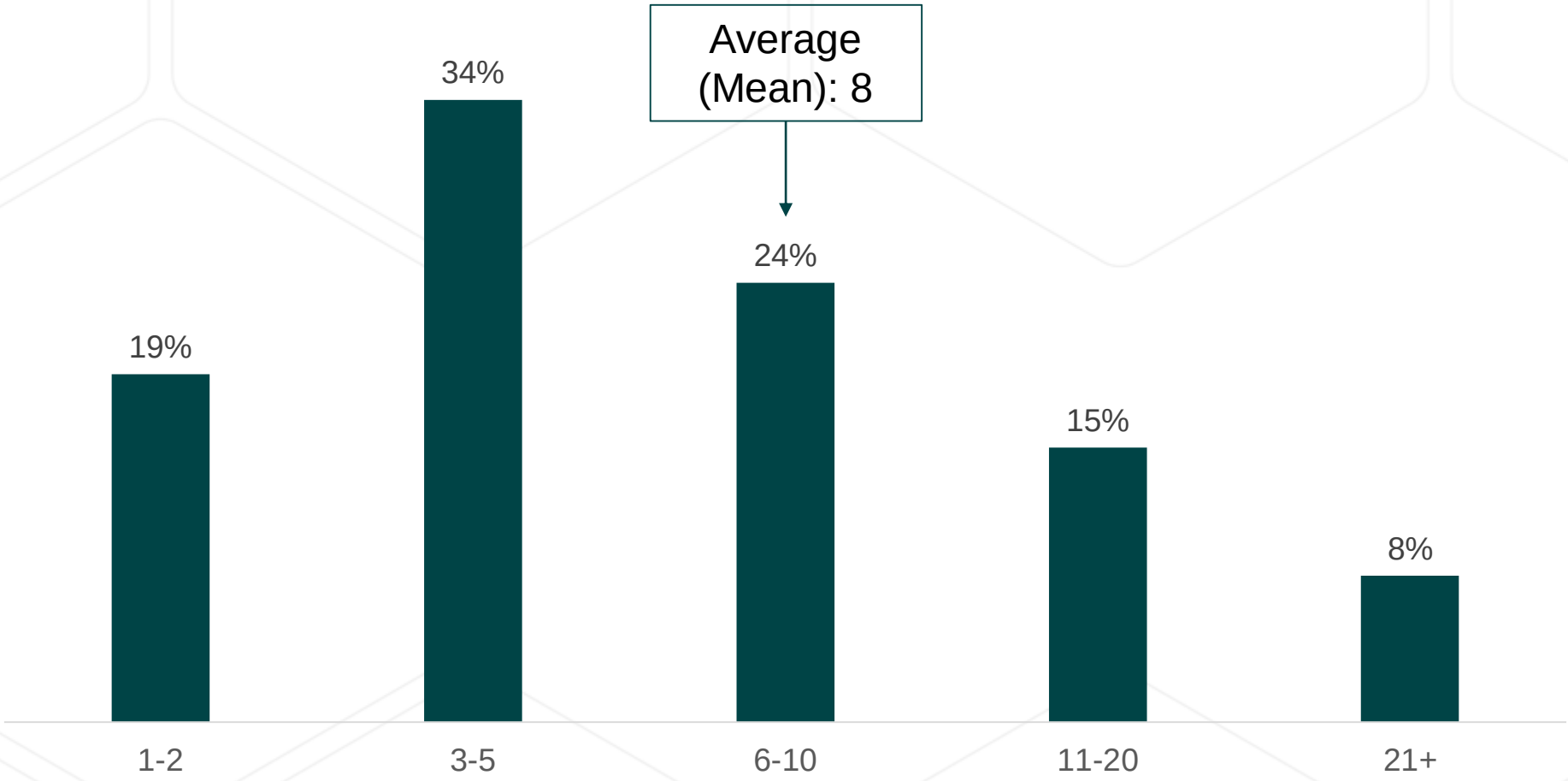


Job title	Average
Entry-level to Mid-Junior executive level	12%
Junior manager	15%
Middle manager	20%

Q2. What % of your day is spent managing alerts? Select one

Base: 250

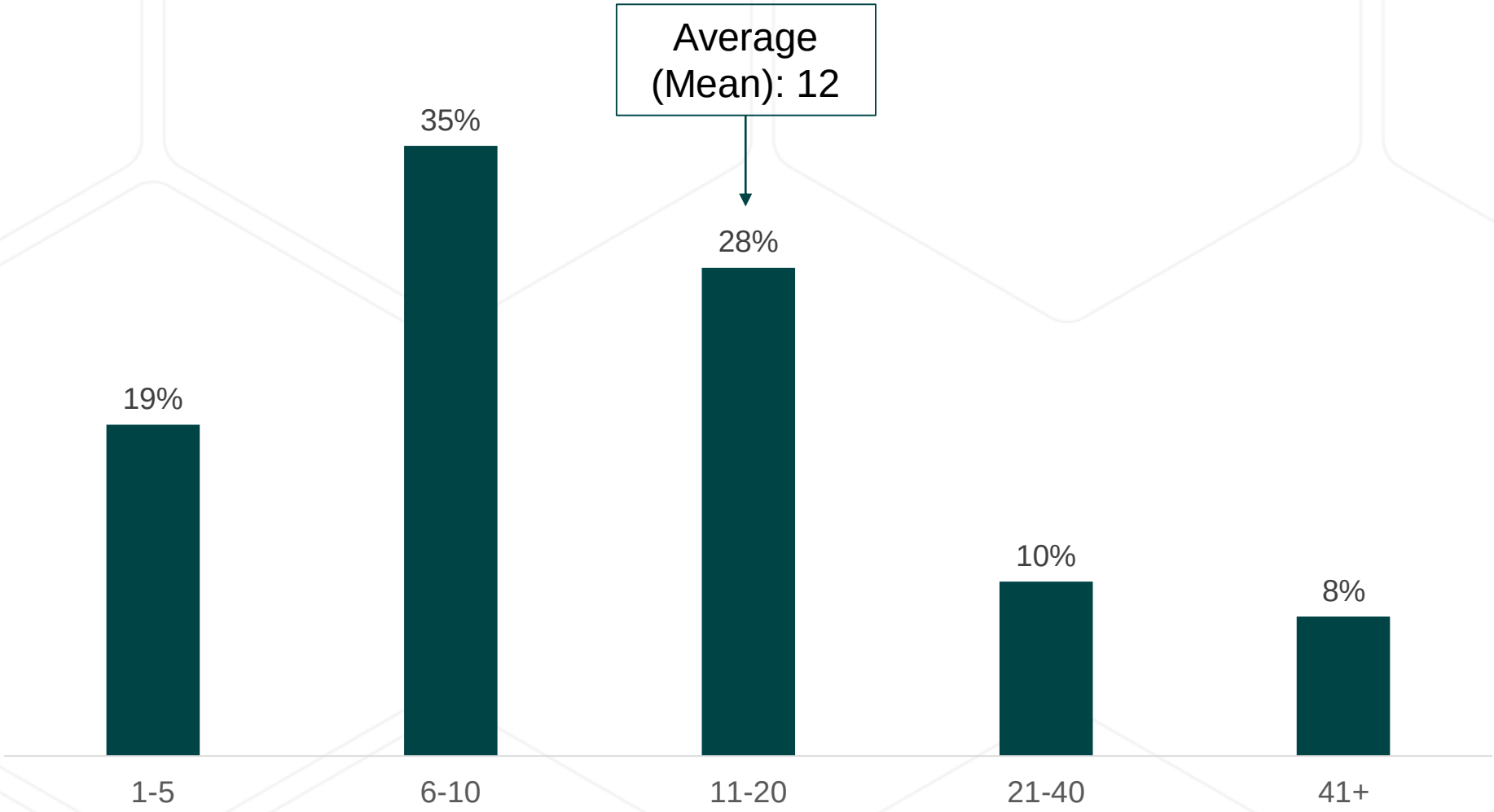
On average a team consists of 8 security analysts



Q3. How many security analysts work in your team? Select one

Base: 250

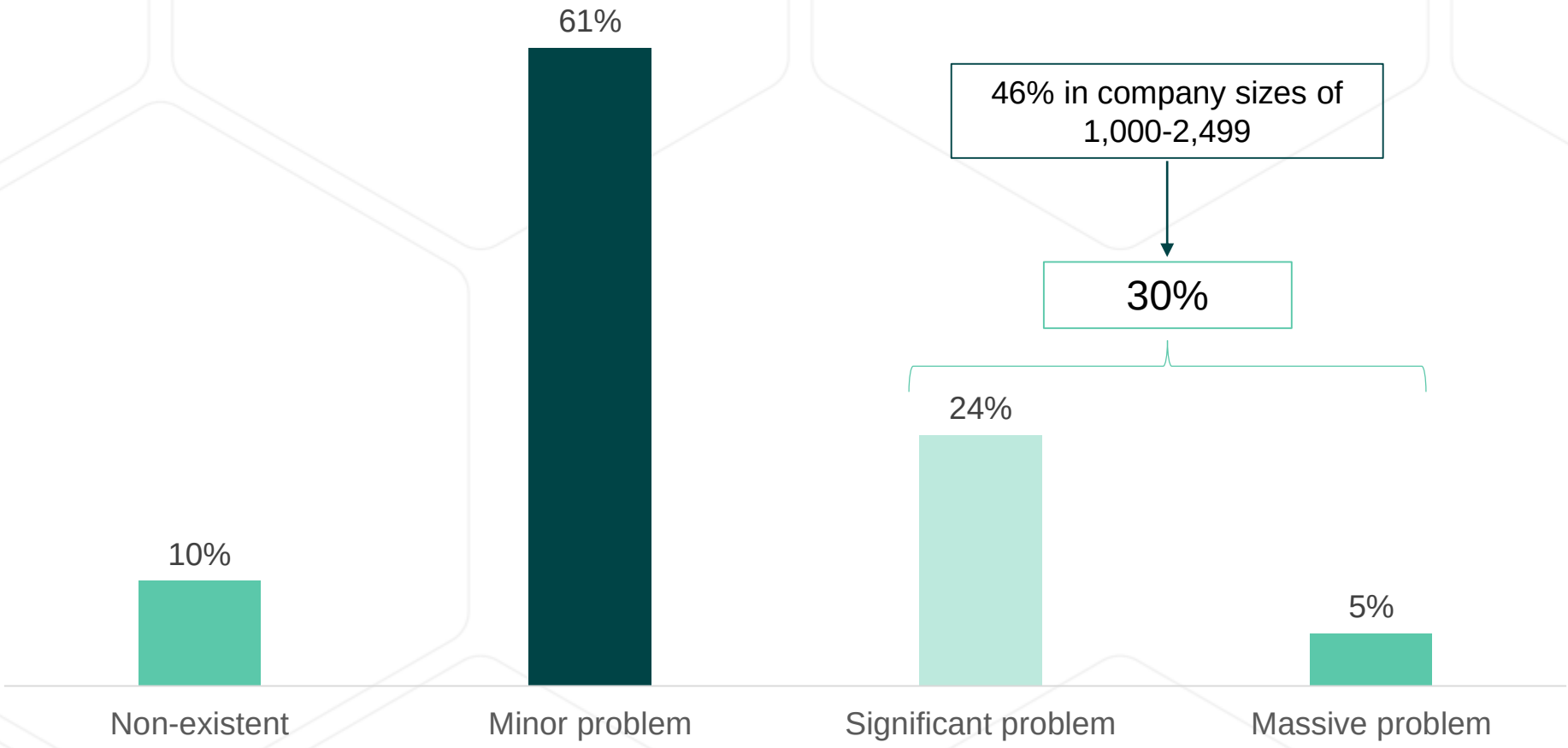
On average organisations have 12 security tools



Q4. How many security tools (e.g. SIEM, firewall, routers, antivirus, Active Directory, network intrusion detection, host intrusion prevention, deception technology) does your organisation have? Select one

Base: 250

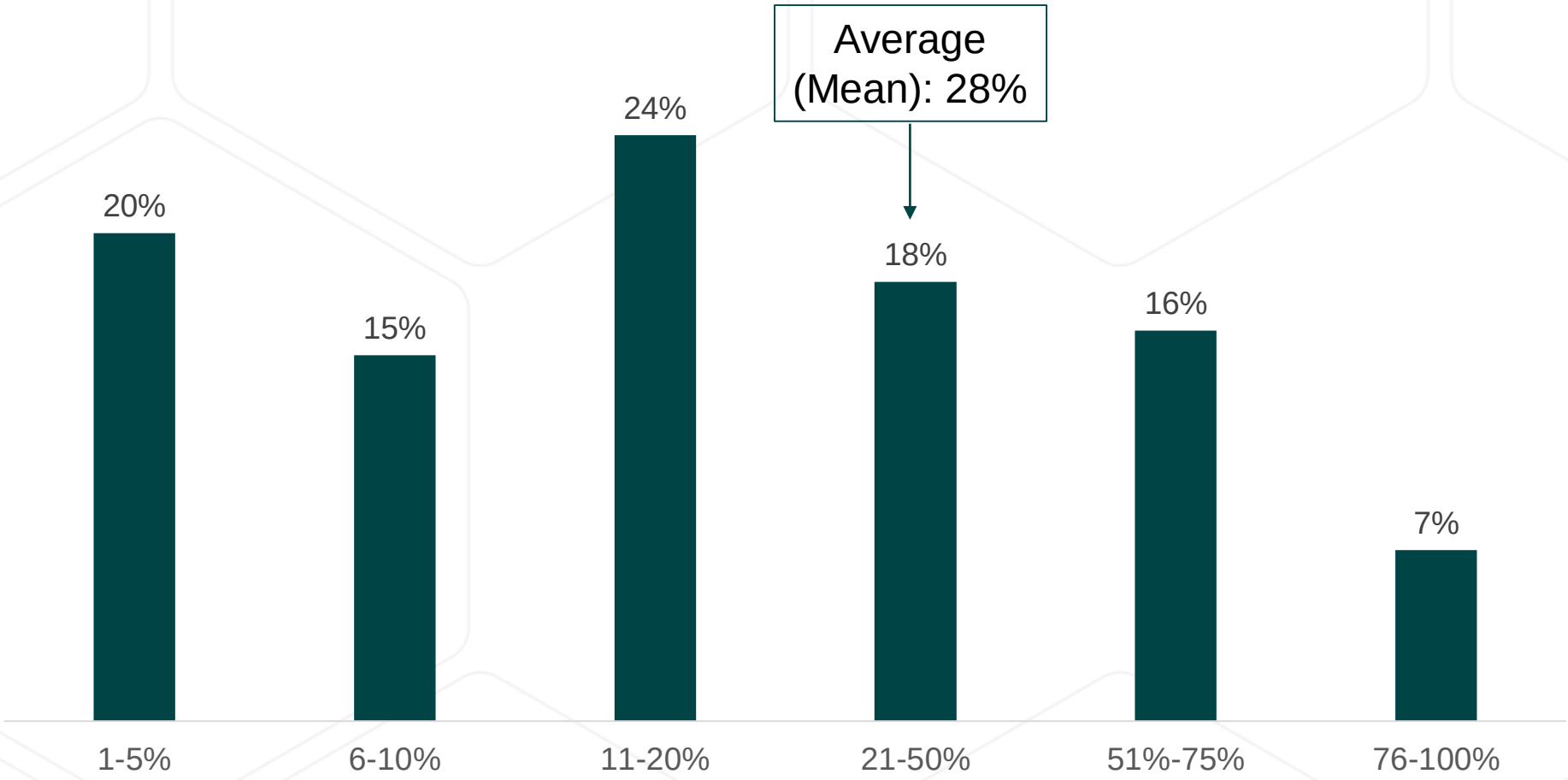
Almost a third (30%) believe missed alerts due to high alert volumes is a significant problem



Q5. How much of a problem is missed alerts due to high alert volumes? Select one

Base: 250

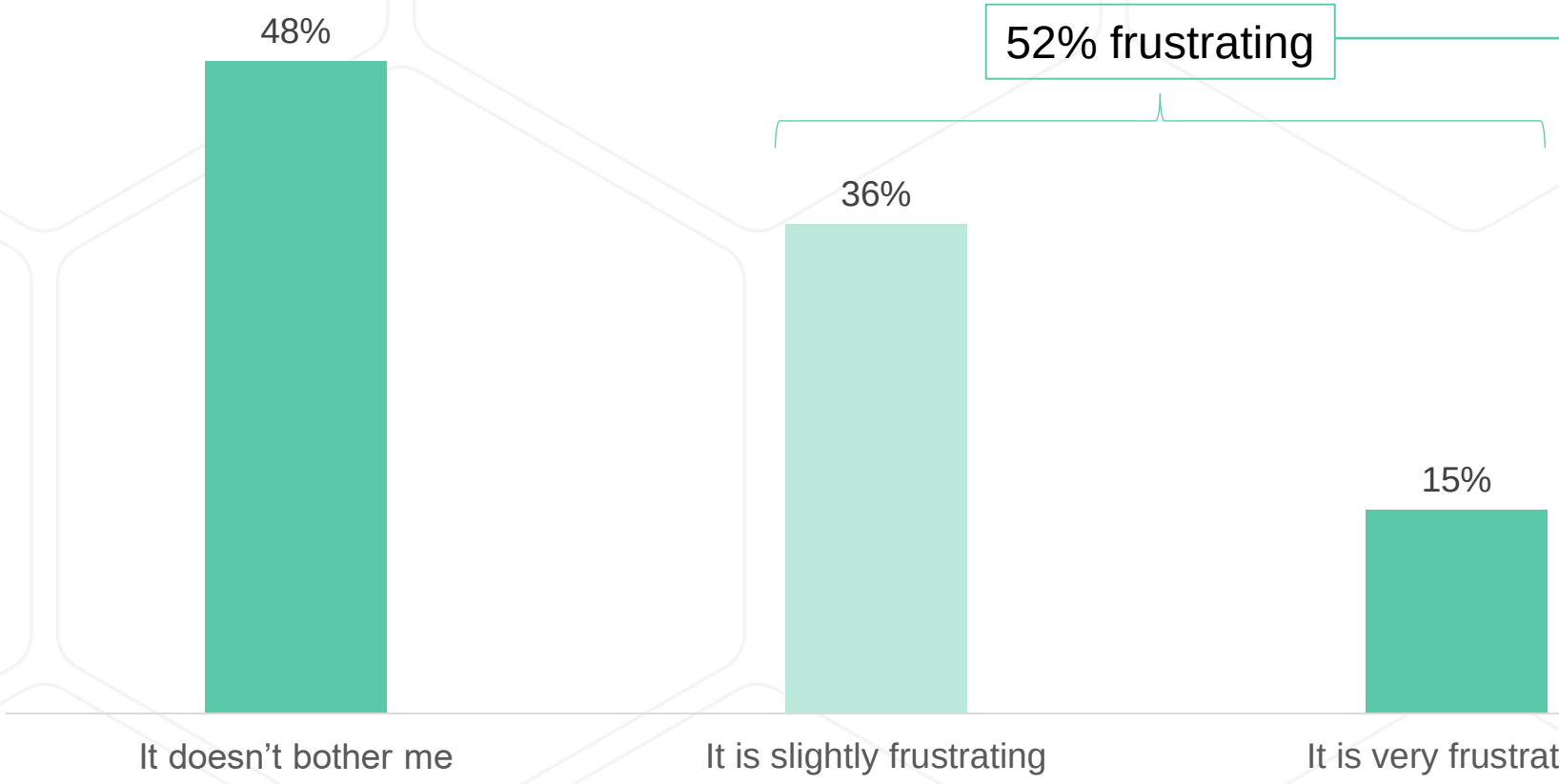
On average, 28% of overall alerts turn out to be false positives



Q6. On average what % of overall alerts turn out to be false positives? Select one

Base: 250

Over half are at least slightly frustrated by the current process for investigating threats (52%)

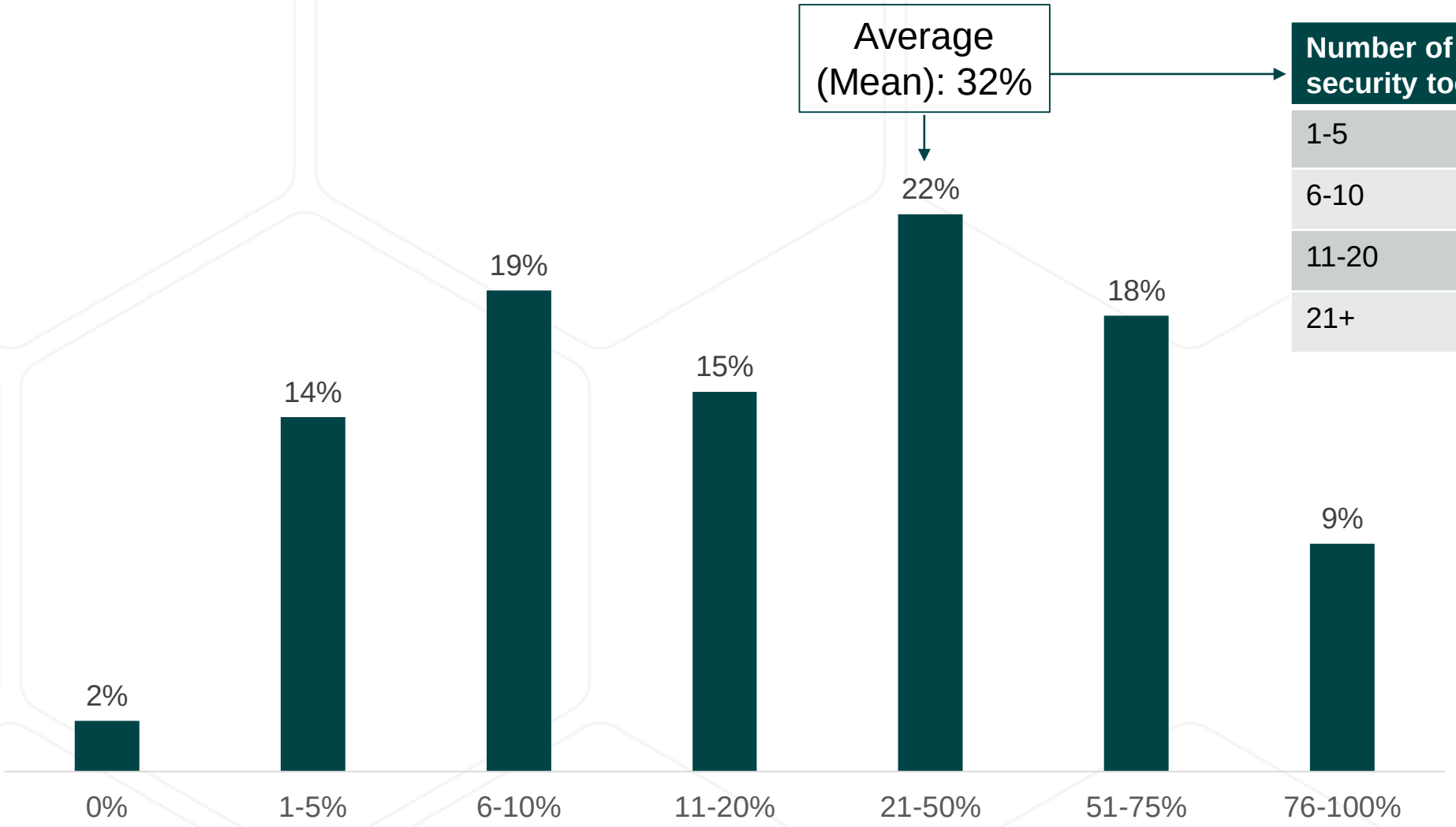


% of day spent managing alerts	% frustrating
1-5%	36%
6-10%	51%
11-20%	58%
21-50%	58%
51-75%	82% (low base number)

Q7. How does the current process for investigating threats make you feel? Select one

Base: 250

On average, under a third of the alert triage and incident response is automated (32%)

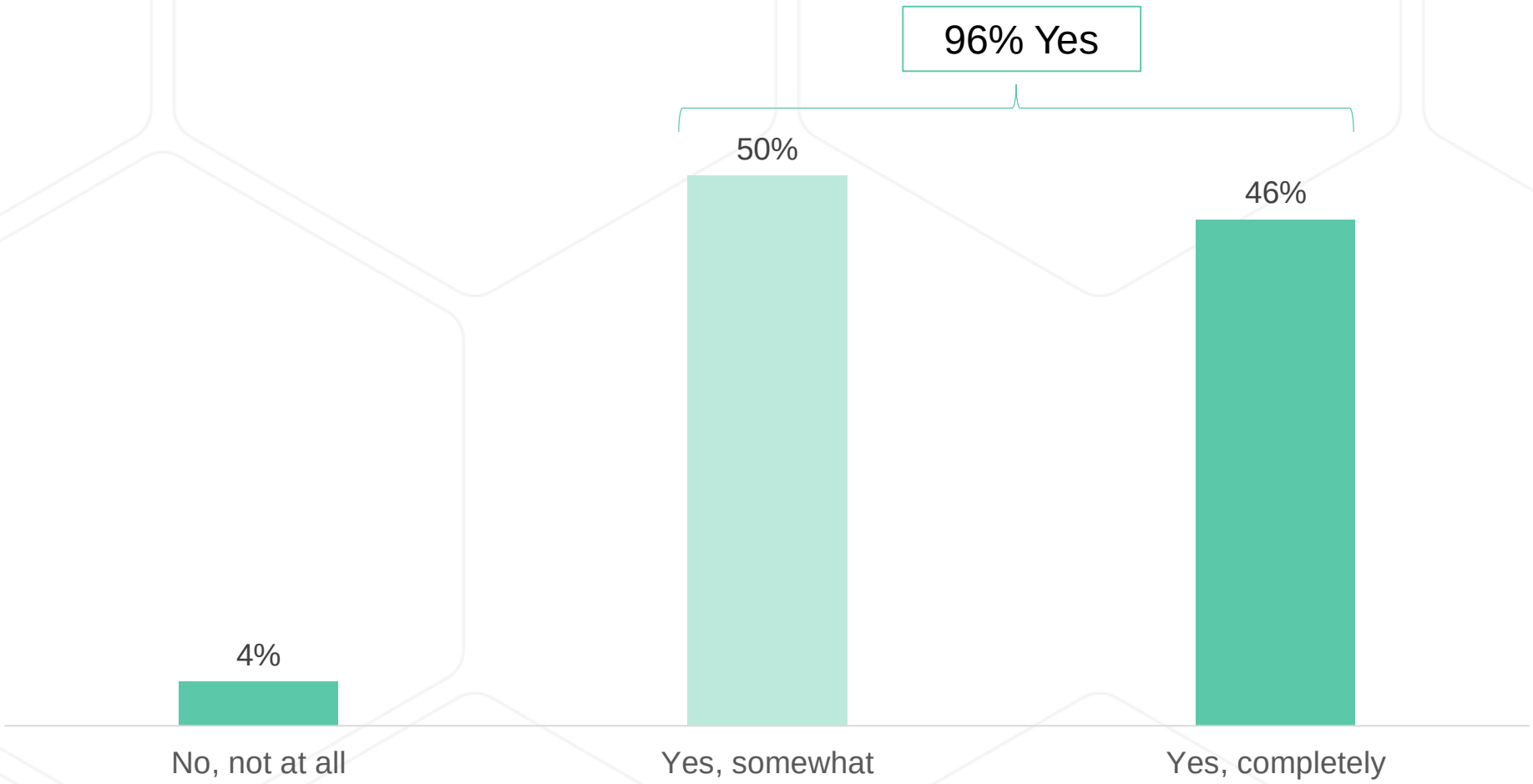


Number of security tools	% automated (average)
1-5	25%
6-10	29%
11-20	30%
21+	45%

Q8. How much of the alert triage & incident response process is automated? Select one

Base: 250

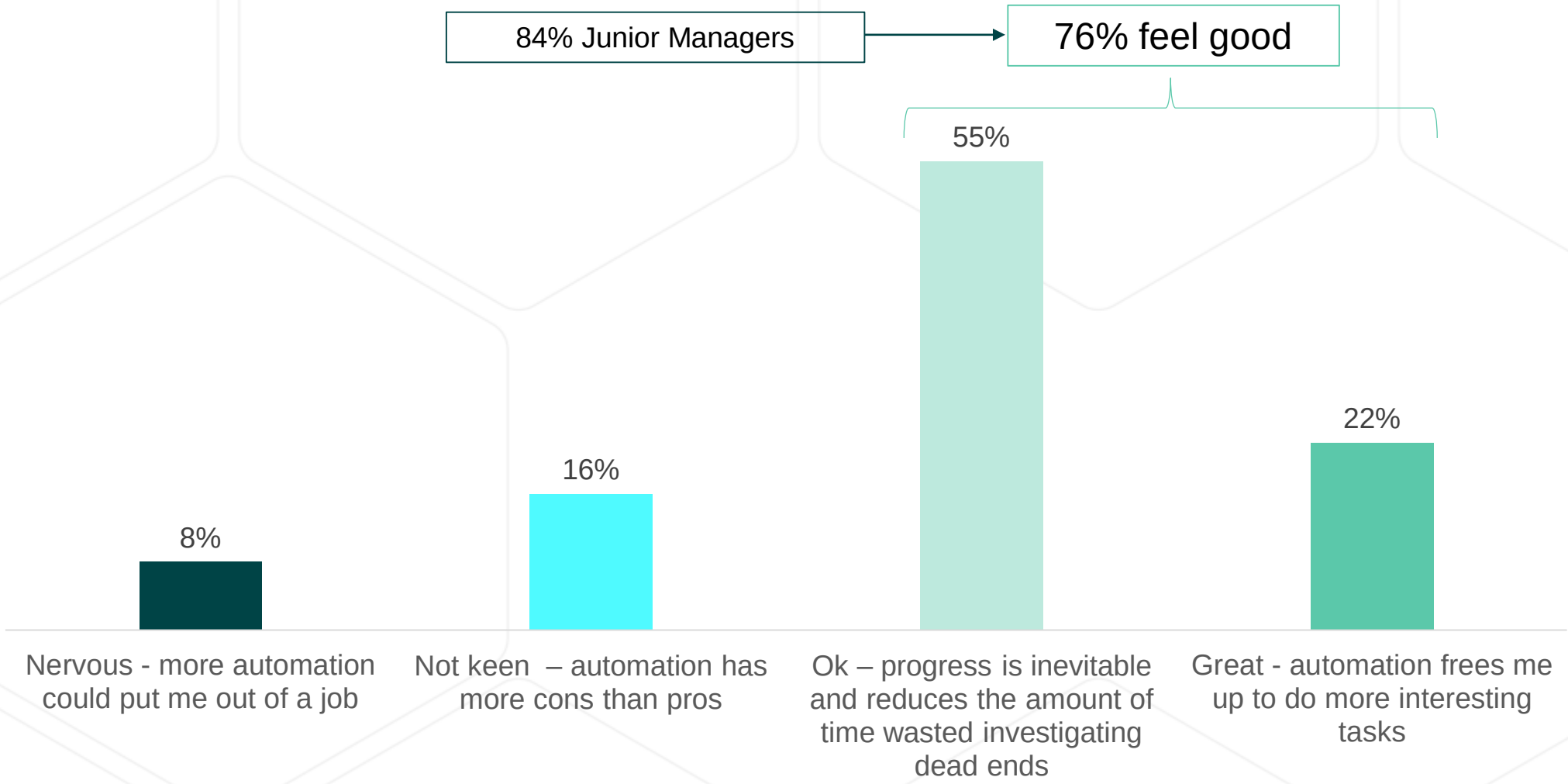
Only 4% are unable to prioritise alerts based on risks to their organisation



Q9. Are you able to prioritise alerts based on the risks to your organisation? Select one

Base: 250

Over three quarters feel good about having more process automation (76%)



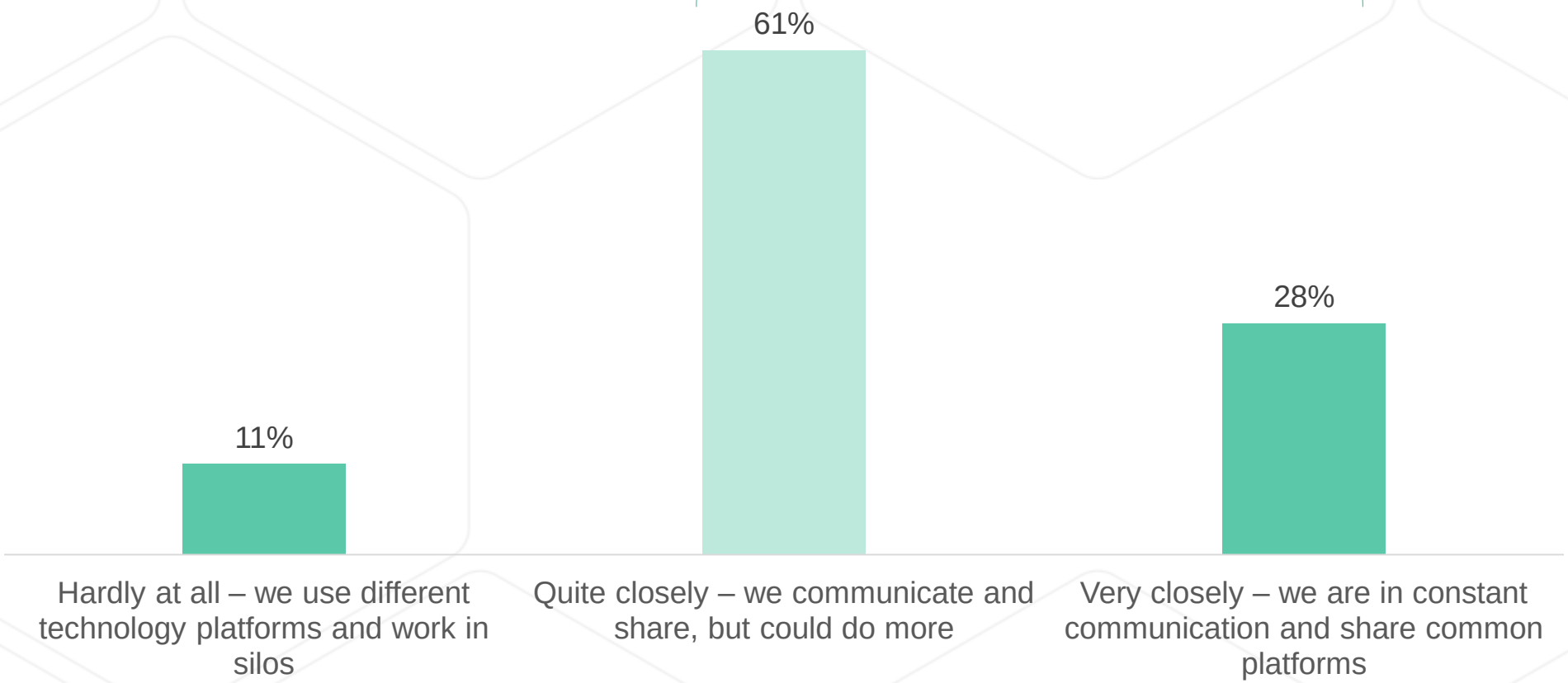
Q10. How does more process automation make you feel? Select one

Base: 250

89% work closely with other departments like GRC or vulnerability management

98% of those spending 21-50% of day managing alerts vs 80% spending 1-5%

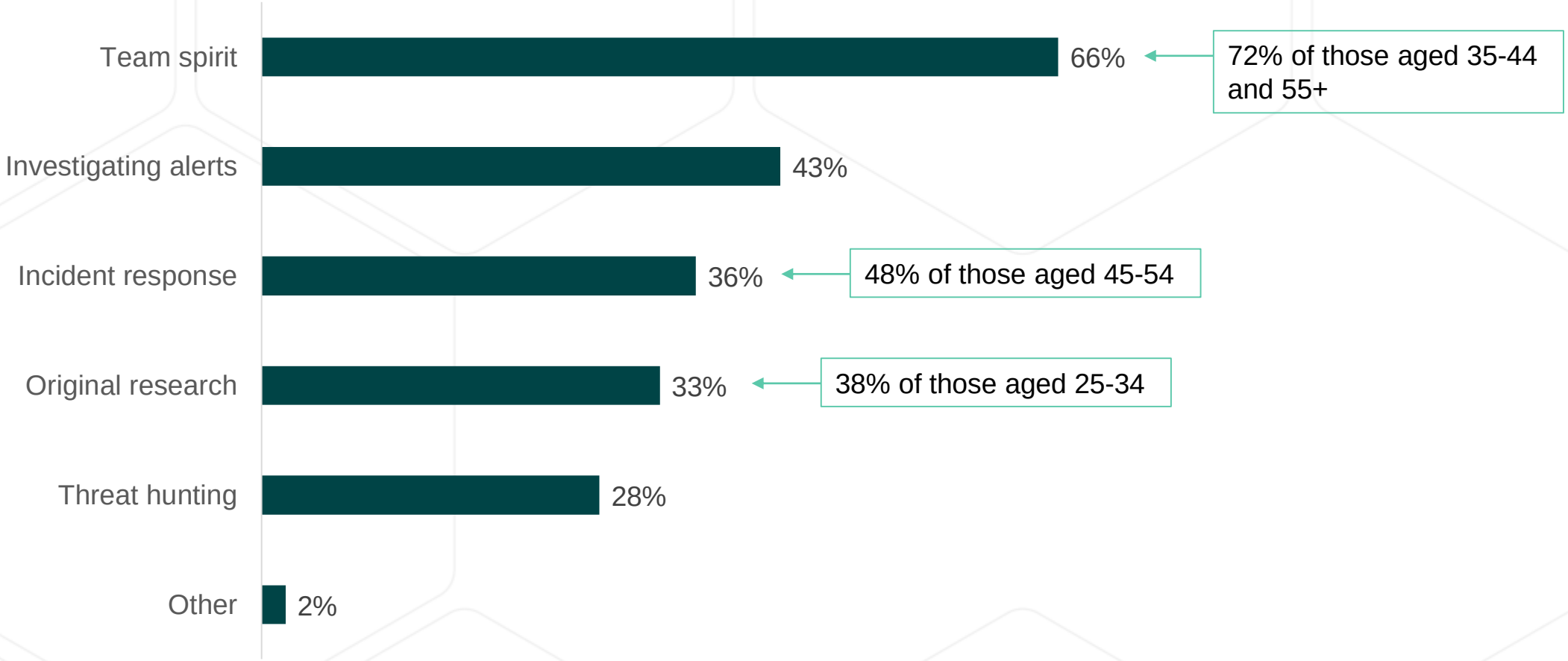
89% Closely



Q11. Which of the following best describes how closely you work with other departments like GRC or vulnerability management? Select one

Base: 250

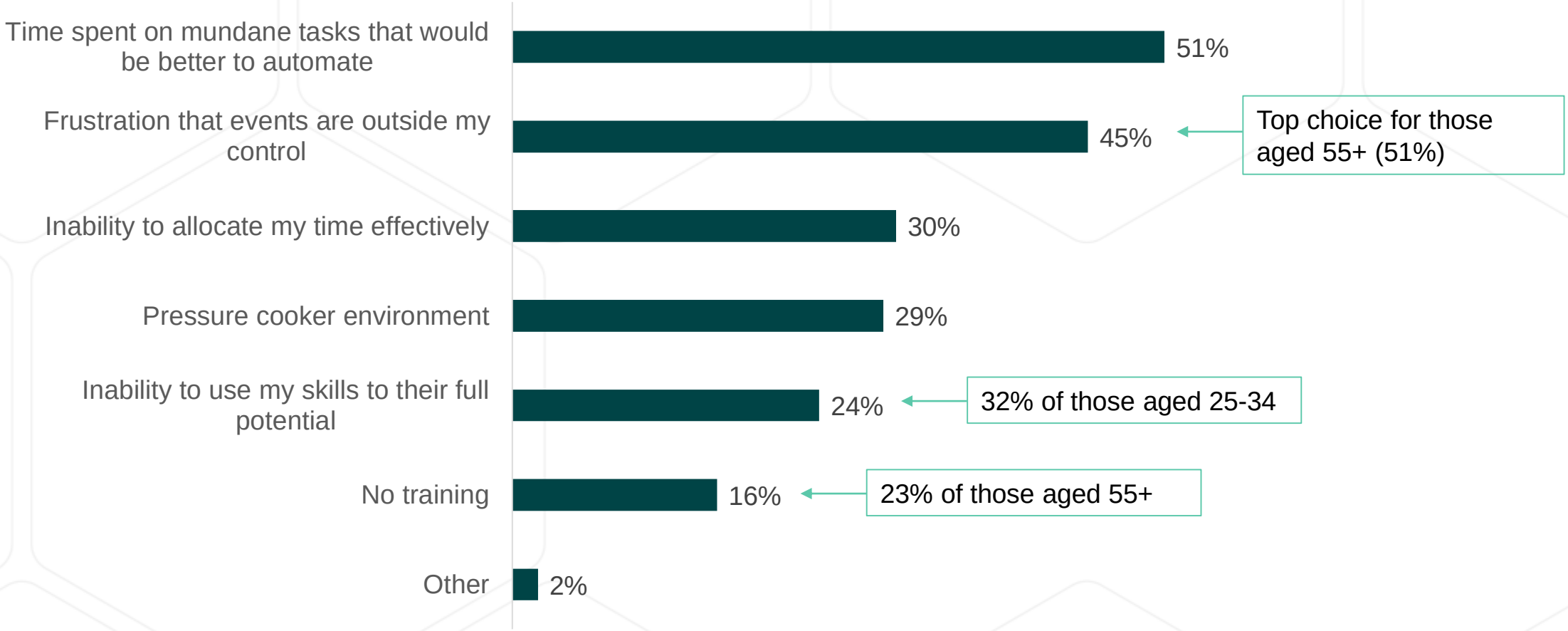
The team spirit is what two thirds enjoy the most about their job (66%)



Q12. What do you enjoy most about your job? Select up to three

Base: 250

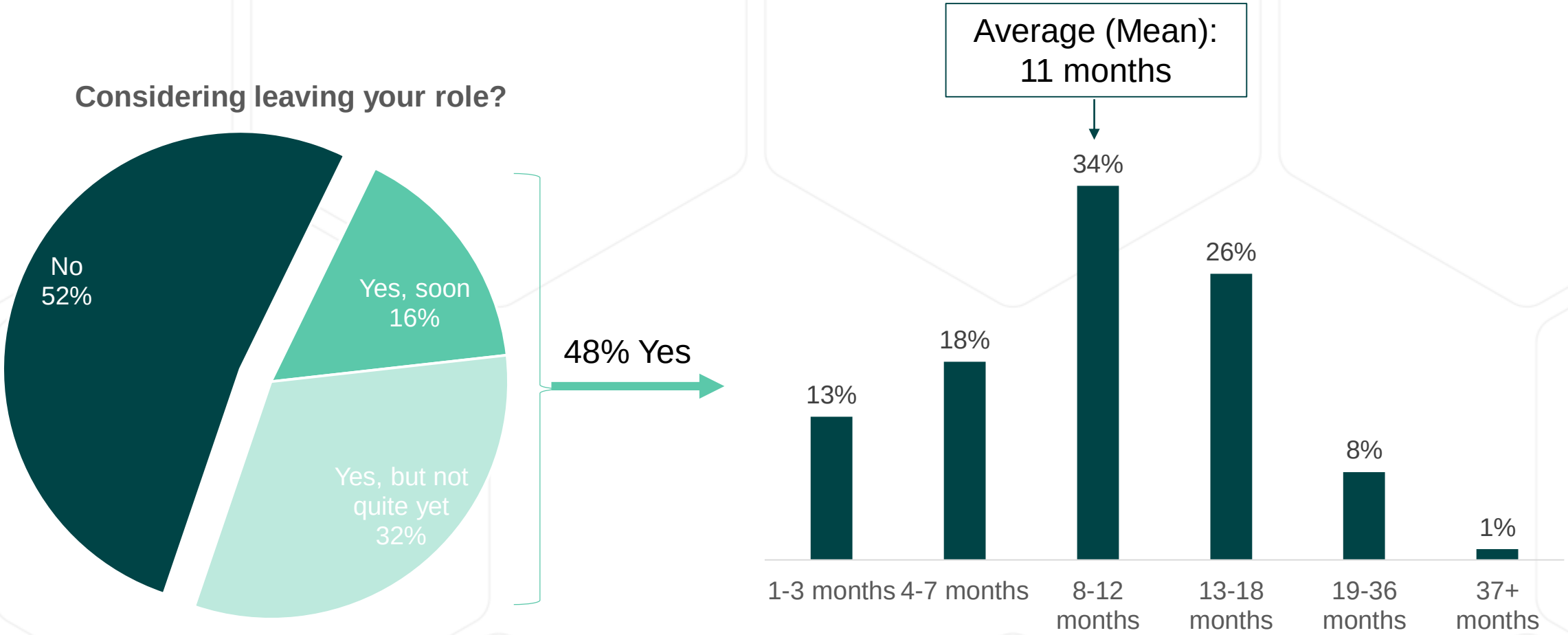
The time spent on mundane tasks that should be automated is what half dislike most about their job (51%)



Q13. What do you dislike most about your job? Select up to three

Base: 250

Almost half are considering leaving their role (48%), with an average time until leaving of 11 months



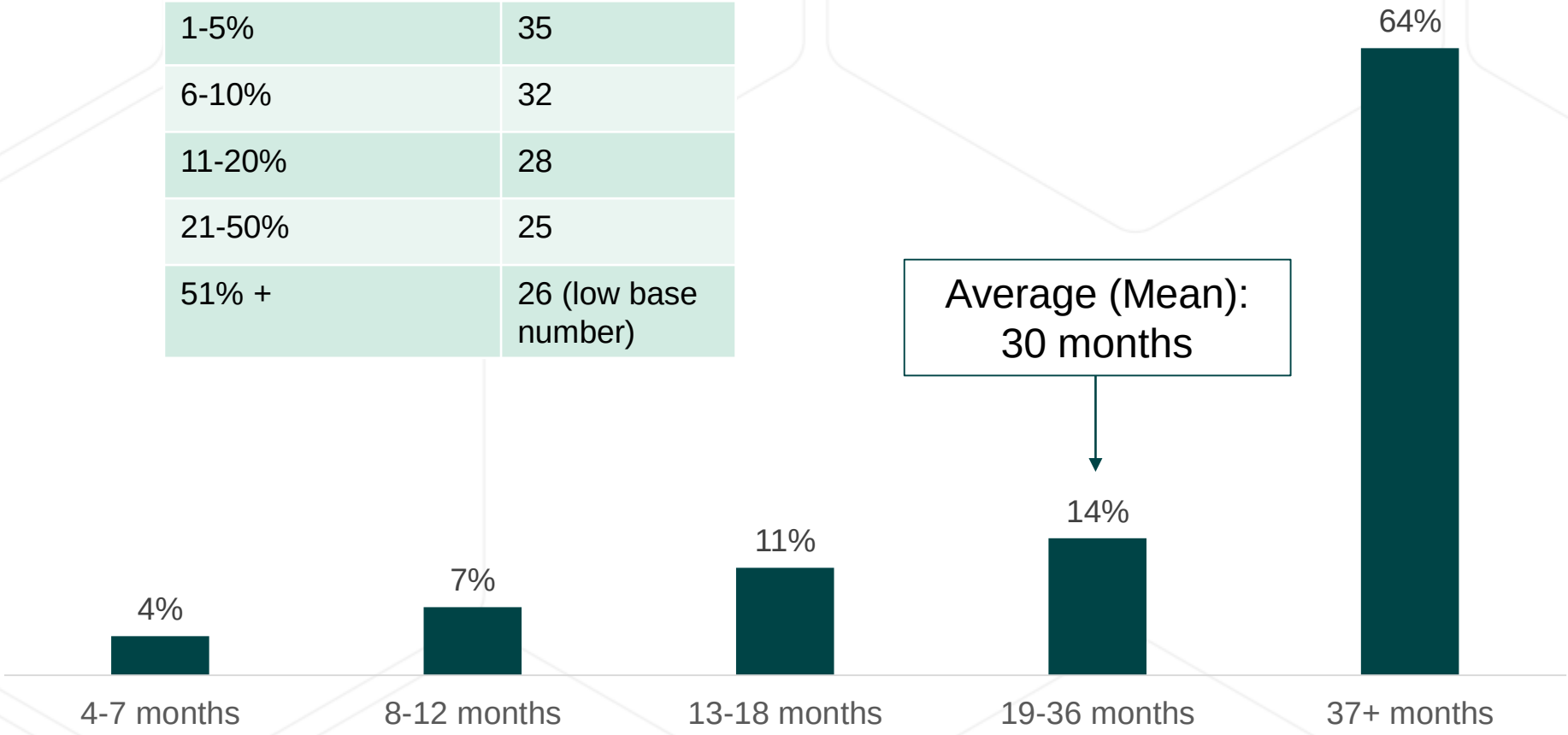
Only asked to those considering leaving

Q14. Are you considering leaving your role? Select one
Q15. At what point would you consider leaving? After: Select one

Base: 250 / 119

Just under two thirds stay for over 3 years at one company on average (64%)

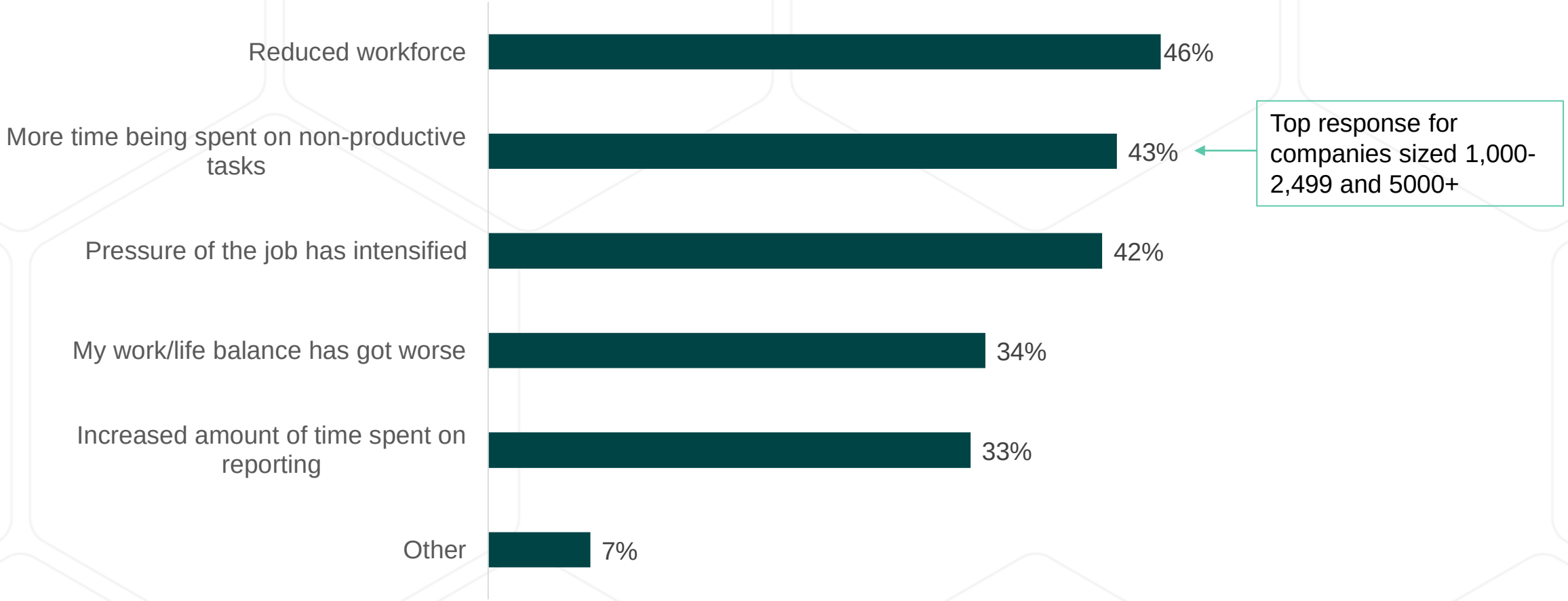
% of day spent managing alerts	Months (Mean)
1-5%	35
6-10%	32
11-20%	28
21-50%	25
51% +	26 (low base number)



Q16. What's the average amount of time you stay at one company? Select one

Base: 250

Almost half have experienced a reduced workforce as a result of the pandemic, followed by just over 2 in 5 spending more time on non-productive tasks (43%) and feeling pressure on the job (42%)

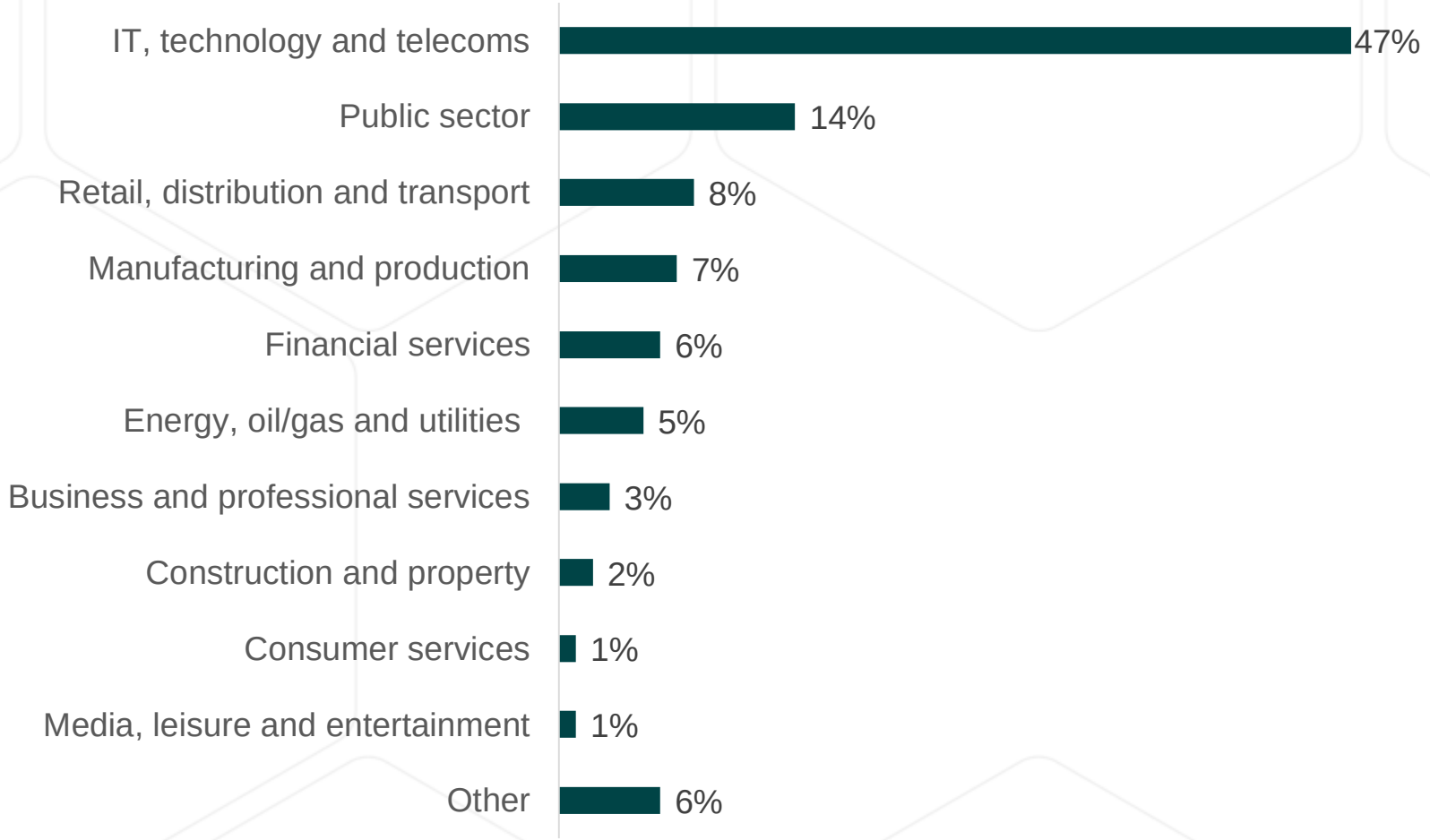


Q17. What are the top 3 biggest changes to your job caused by the pandemic? Select up to three

Base: 250

Demographics

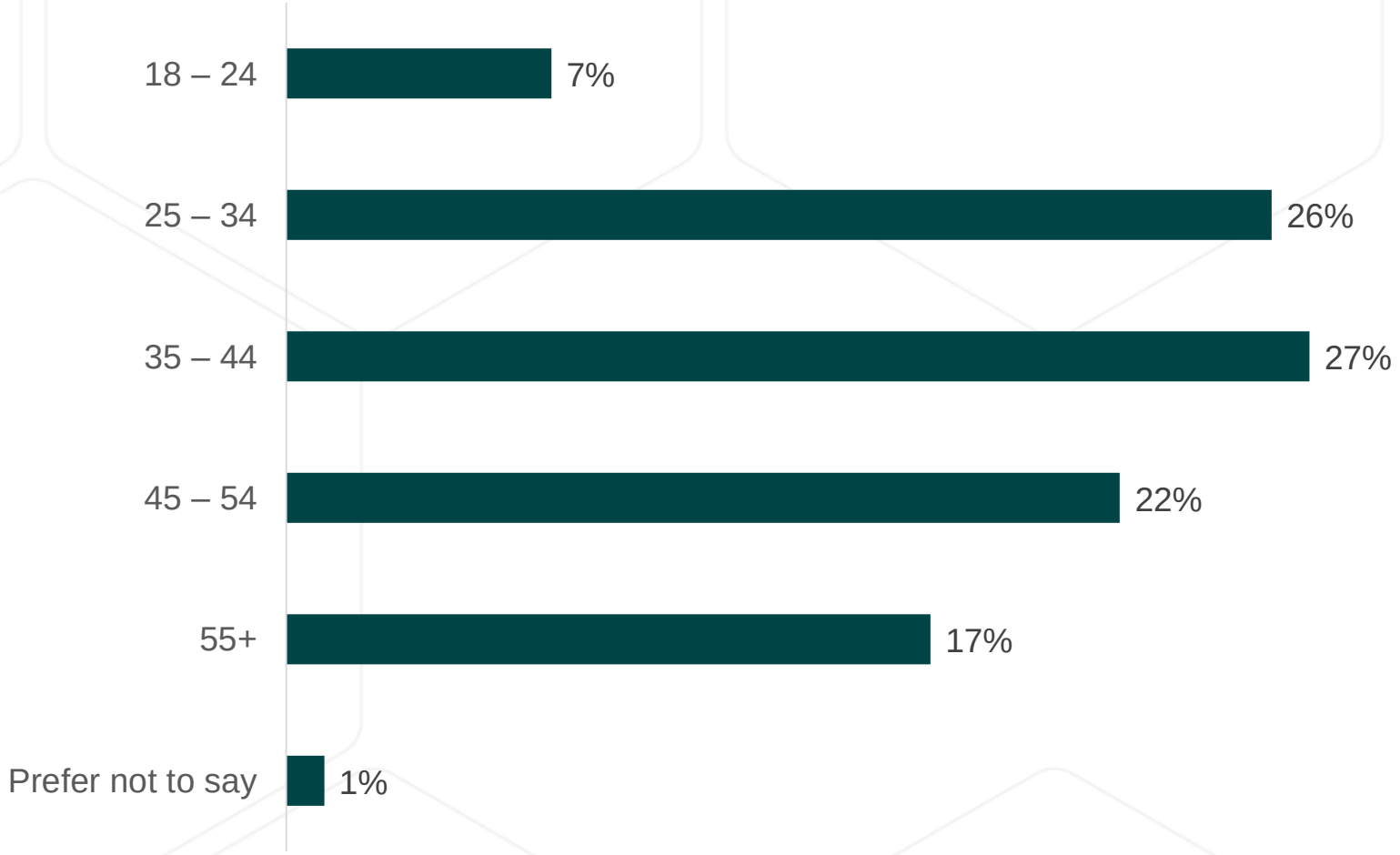
Industry



D1. Within which industry is your organisation? Select one

Base: 250

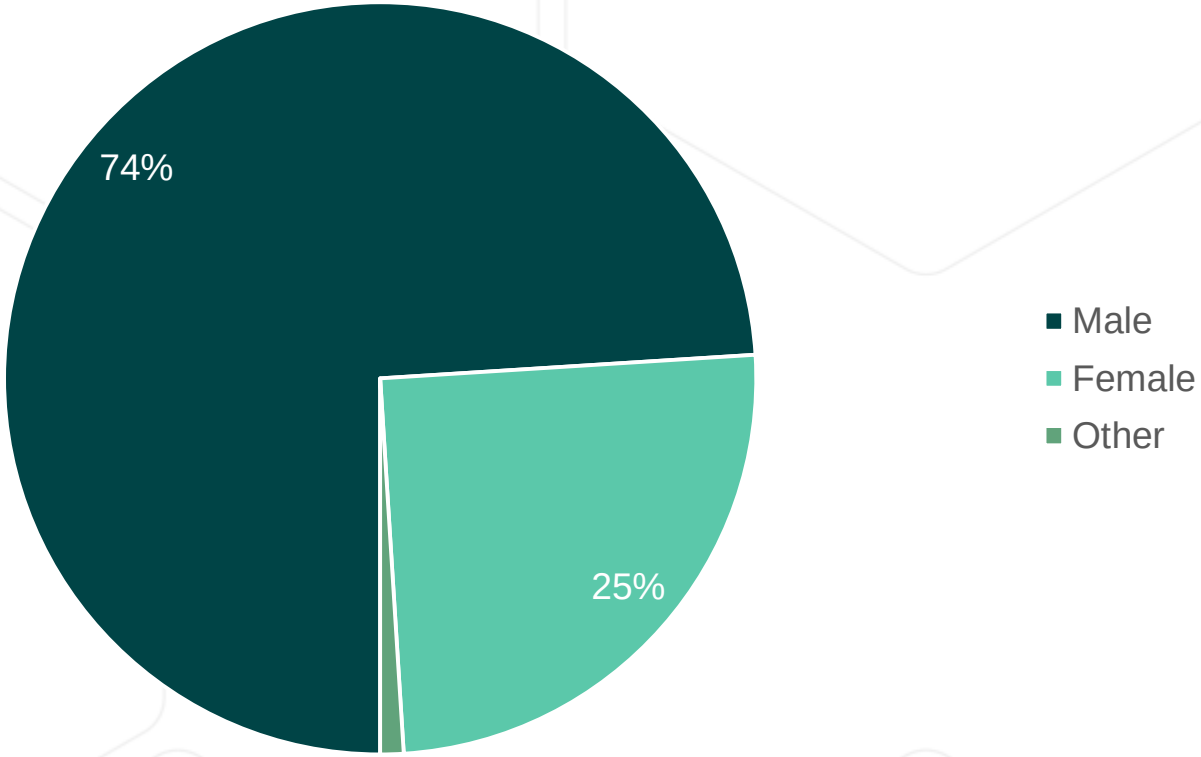
Age



D2. How old are you? Select one

Base: 250

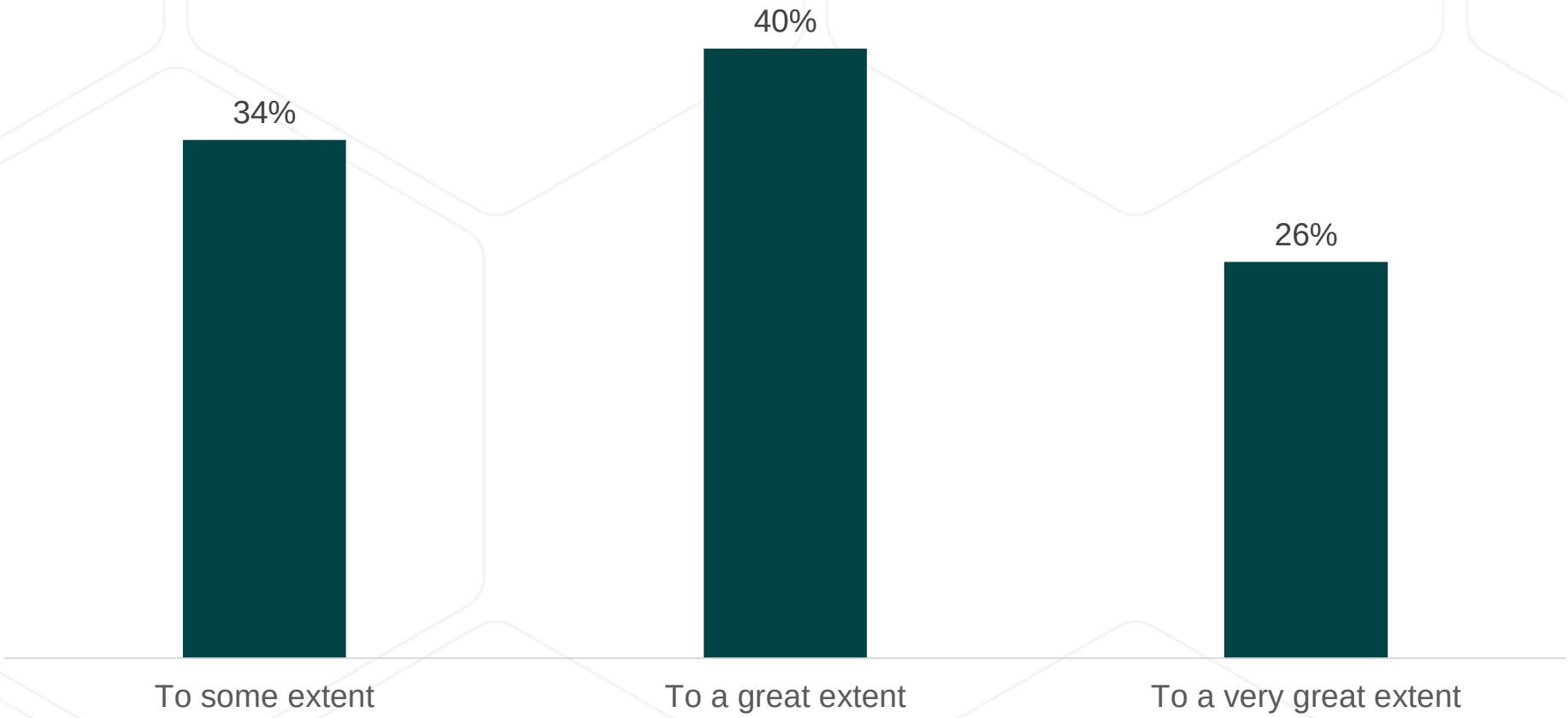
Gender



D3. What is your gender? Select one

Base: 250

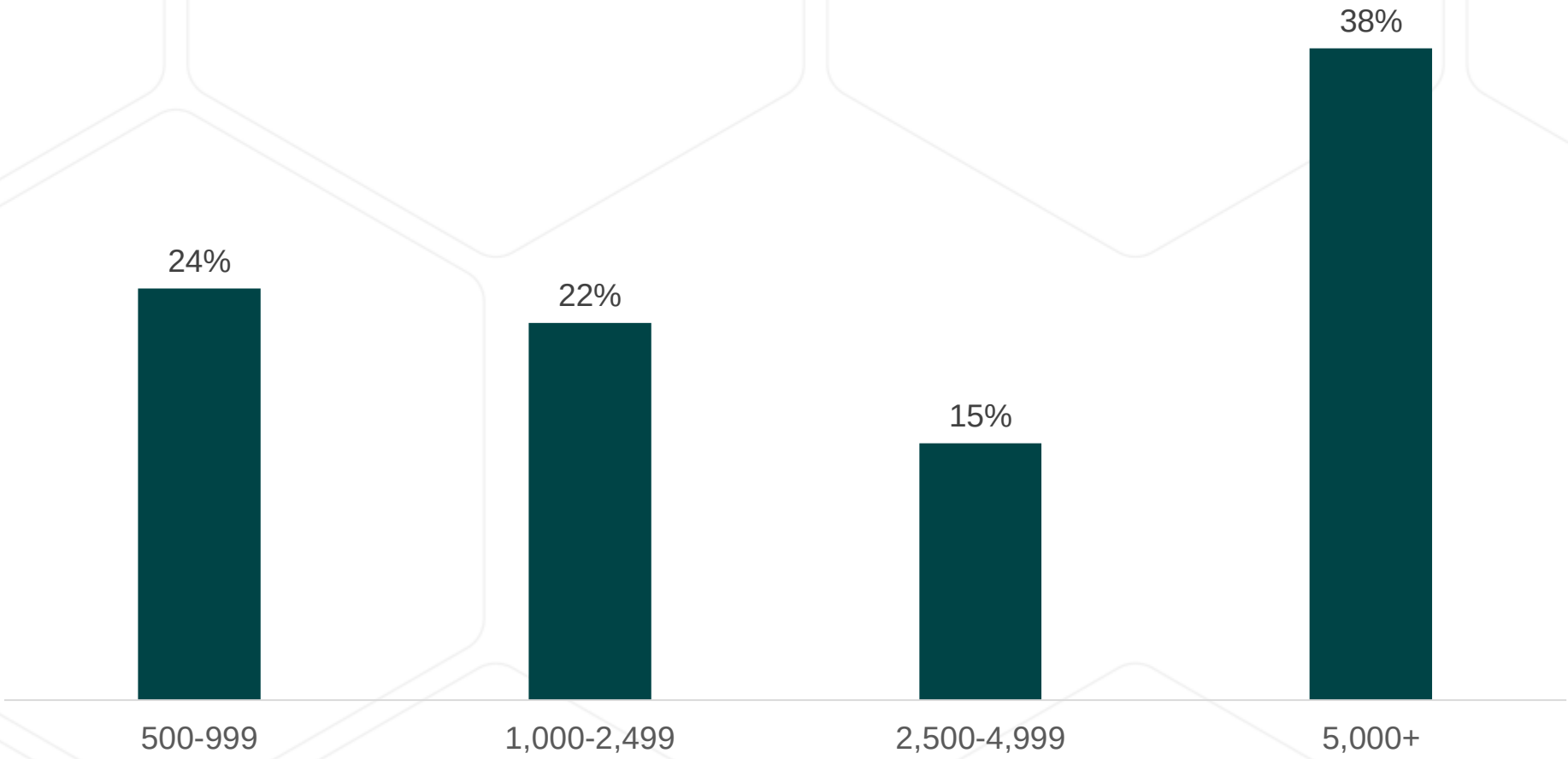
Extent of time spent managing threat alerts



S2. To what extent does your role include managing threat alerts in your organisation? Select one

Base: 250

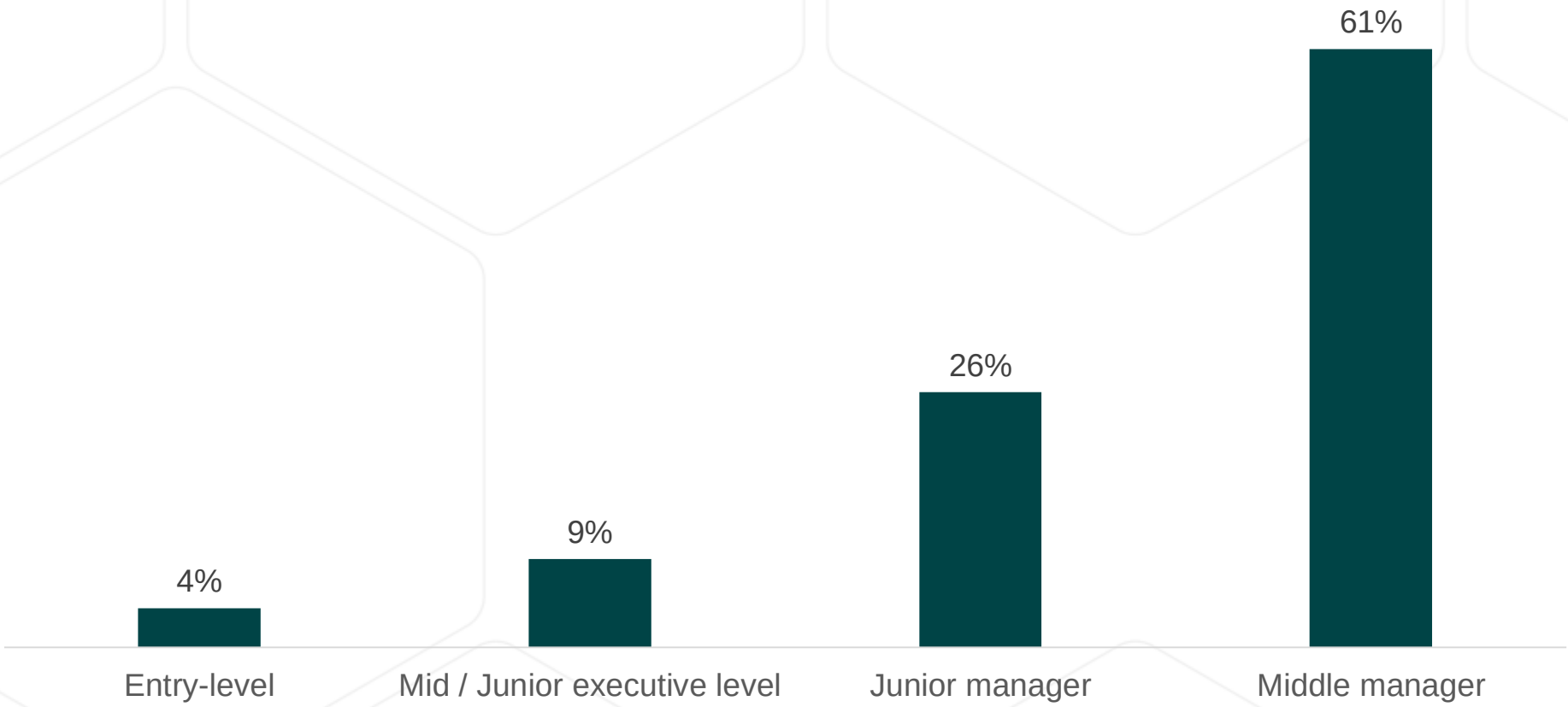
Employees



S3. How many employees work in your organisation across all locations? Select one

Base: 250

Job role



S4. Which of these best describes your job role? Select one

Base: 250

United Kingdom
53 London Road, London, SW17 9JR, United Kingdom.

North America
6510 Lincoln Ave, Lincolnwood, IL 60712.

Email: info@sirp.io
Web: www.sirp.io