KPMG Cybersecurity Survey

SECURITY OPERATIONS CENTER (SOC) LEADERS PERSPECTIVE

Results

May 2024

Objectives & Methodology

Objectives

To understand Security Operation Center (SOC) leaders' perspectives on security practices, cyber threats, perceived effectiveness of security operations, goals and challenges, threat preparedness, and opportunities for generative AI.

The survey looked ahead to understand future perspectives (2 years out) and how SOCs are evolving in the allocation of resources, solution usage, and AI adoption.

Survey Methodology

- **A 15-minute, online survey** among **C-Suite security leaders** in the US and was fielded April 12-19, 2024.
- The sample includes **200 'security leaders'** meeting the following criteria:
  - Role in the **IT, Security, and Technology** business function
  - Job titles including **Chief Information Security Officer (CISO), Chief Security Officer, and AI Security Officer**
  - Large enterprise with **at least 500 employees** and an **annual revenue of at least $1B**
  - Organizations from a mix of industries

Activities and Timing

Activity	Timing
Approve survey	April 5
Program and test survey; soft launch data collection	April 8 – April 12
Survey fielding; process data	April 15 – April 19
Detailed analysis and (PPT) reporting	April 22 – May 1 (deliver report end of day)
Partner readout	May 3
Embargo Outreach	May 6 – May 10
Launch in Media	May 13

Key Takeaways: Summary

C-Suite security leaders are optimistic about the effectiveness of their security operations:

- They are confident about their SOC's visibility and readiness to deal with security threats. Seven in ten (69%) say they have a 'solid understanding' of their SOC's vulnerabilities.
- A majority (85%) of security leaders believe their SOC is well poised to prevent increasingly sophisticated cyber attacks. And nearly all (91%) claim full visibility across their organization's risk areas.
- Two-thirds (64%) are satisfied with the time it takes to remediate their vulnerabilities (however, they may not have an accurate picture of the timing because just a third (32%) are regularly using mean time to respond metrics).
- Most are focused on goals of increasing digital trust through proactive identification, and remediation of threats, and enabling the business to innovate faster through new product and service offerings.
- Nearly three-quarters are taking an innovator/first to adopt approach when it comes to using new cybersecurity solutions and services. It's likely that this 'first adopter' mentality is being fueled by AI, especially as leaders are looking to AI to help them stay ahead of new and emerging threats and drive agility and responsiveness in their SOCs.

But 4 in 10 leaders have also experience a Cyber attack in the last year:

- Despite a high degree of confidence, a sizeable proportion (40%) have experienced a cyberattack in the last year that resulted in a breach.
- There is also significant concern (76%) about the growing sophistication of new cyber threats, especially with Malware.
- Leaders are most concerned about organized cyber-crime groups, insider threats (employees and contractors), and individual hackers.

Key Takeaways: Summary

Security leaders see AI as a "game changer" for the SOC effectiveness:

- Two-thirds (66%) of security leaders consider AI-based automation very important, now and in the future, for staying ahead of new threats and increasing the agility and responsiveness of their SOCs.
- At least six in ten view AI as a "game changer" across all security functions, including identity management, monitoring, predicative analytics, identifying anomalies, etc.
- While AI-based automation has many benefits, the reliability of AI recommendations is a top concern for leaders. Additional AI concerns focus on employee backlash, culture change, security, lacking a long-term AI strategy and the significant effort that is required to set up and train AI solutions.

Challenges remain, but Cyber leaders expect to increase their budget and resources:

- Security data quality issues, alert fatigue, and determining the true severity of threats are bogging down SOC efforts.
- About half of security leaders also say they have 'major issues' with retention (47%) and maintaining up-to-date knowledge (46%), skills and expertise (45%) to identify, analyze, and remediate emerging threats.
- However, in facing these challenges, more than two-thirds expect future headcount (74%) and budget (68%) to increase.
- There is also also a move to simplify through consolidation of security solutions; likely due to current, top challenges experienced with complex security environments and a lack of integration between security solutions.
- They also feel like they are spending the right amount on vendor tooling (Solutions & Services) and log management.
- Training for more sophisticated threats is currently underway among two-thirds (67%). And collaborating with other organizations is common for about 6 in 10 SOCs.

Key Takeaways: Summary

Cyber leaders have a limited picture of emerging threats and SOC performance:

- Most are only utilizing a few metrics to understand the performance of their SOCs – and at least four in ten say they struggle with assessing their SOC's performance, most often when it comes to analysis and identifying improvement areas.
- Lacking tools and solutions, incomplete data for analysis, and the expertise needed for evaluation are the biggest barriers to measuring SOC performance.

Key Takeaways: Top Challenges

Security leaders point to challenges across operations, performance evaluation, and staffing. Looking ahead, they raise concern about trusting AI-based solutions and their impact on company/employee culture.

Top Challenges for Security Leaders and their Organization's SOC

Operational Pain Points	• Issues with security data quality and completeness (30%, percentages for top ranked) • Fatigue in navigating low fidelity alerts vs. real threats (30%) • Monitoring perimeters (25%) and delays in threat detection/remediation (24%)
Identifying & Remediating Threats	• Determining the severity of cyber threats and vulnerabilities (32%) • Contributing to this: complexity of IT environment (29%), lack of integration across solutions (29%), lack of skills or expertise among SOC staff (29%)
Evaluating SOC Performance	• Measuring SOC performance – collecting relevant data (50%) • Analyzing – interpreting, finding insights, identifying issues/opportunities (45%) • Reporting – detailed reporting, scoring/metrics (41%)
Talent for SOC	• Attracting and retaining talent (47%) • Staying current with training security staff (46%) • Lacking specialized expertise for evolving threats (45%)
AI-based Automation for SOC	• Trusting the accuracy and reliability of AI recommendations (38%) • Impact on company culture (30%) and employee backlash over potential job loss (30%)

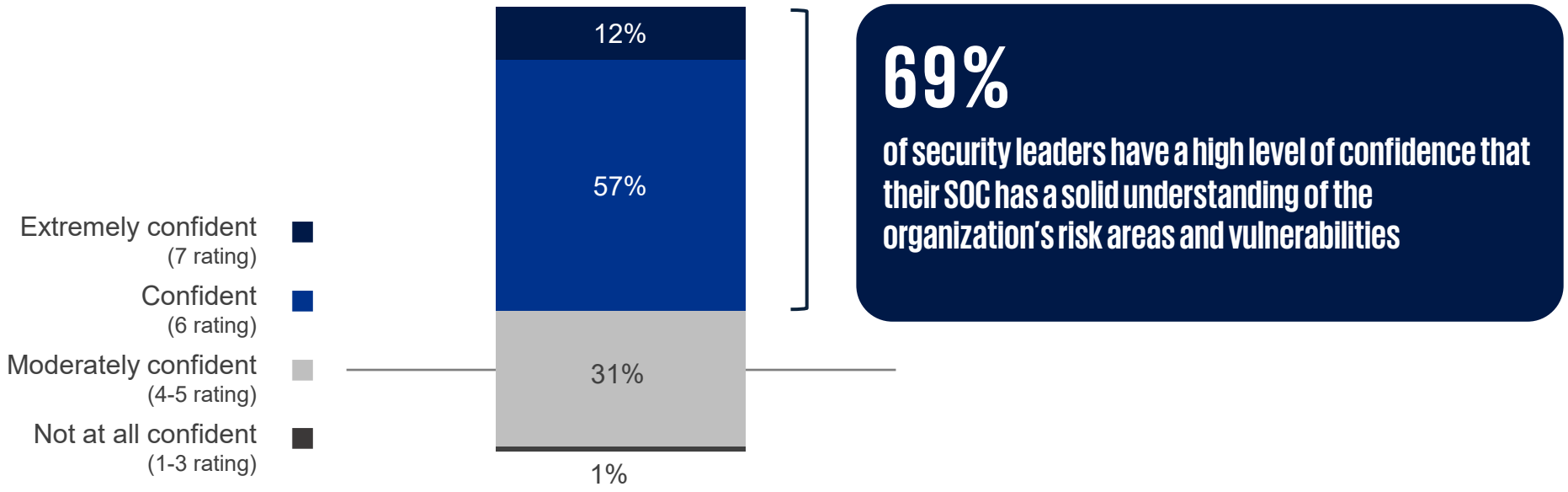
DETAILED FINDINGS

Cyber Leader Optimism

Seven in ten security leaders are confident in their SOC's understanding of the organization's vulnerabilities.

Majorities of security leaders from both medium- and large-sized organizations feel assured in this area.

Confidence that SOC has a Solid Understanding of the Organization's Risk Areas and Vulnerabilities



69%

of security leaders have a high level of confidence that their SOC has a solid understanding of the organization's risk areas and vulnerabilities

Q16. To what degree are you confident that your security operations center (SOC) has a solid understanding of your organization's risk areas/vulnerabilities? (Base: Total security leaders, n=200)

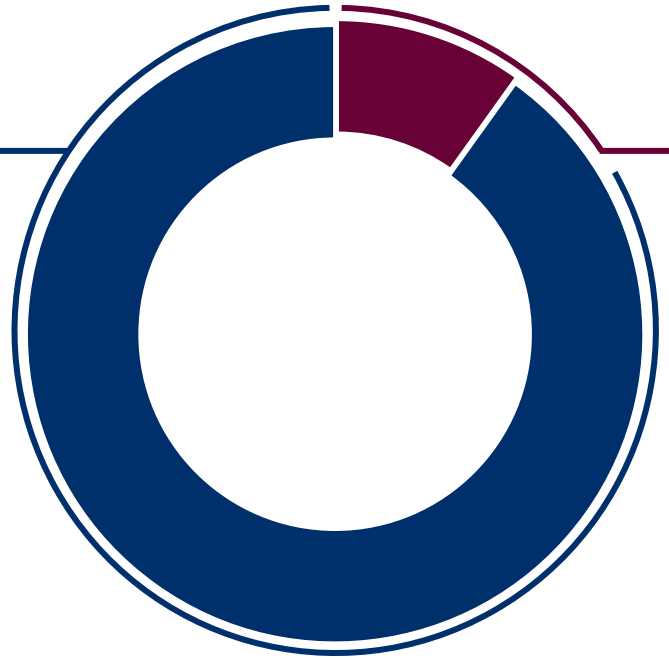
Nearly all security leaders claim full visibility across their organization's risk areas and vulnerabilities.

Even among the minority that say they have less than 100% visibility (10%), most say they have at least 75% visibility.

Self-Assessment: Level of SOC's Visibility Across All of the Organization's Risk Areas and Vulnerabilities

91%

of security leaders say their SOC has **full visibility across their organization's risk areas and vulnerabilities**



10%

of security leaders say their SOC has **less than full visibility across their organization's risk areas and vulnerabilities**

% Visibility (for those less than full)

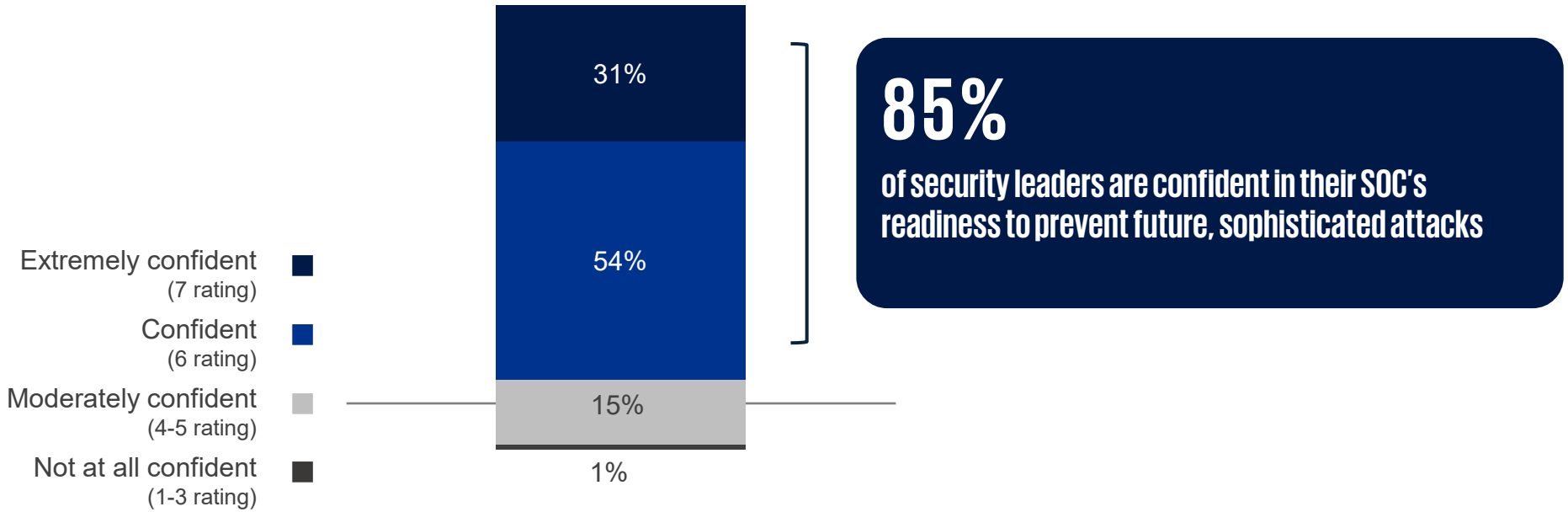
68%	**75% or more**
26%	50% to less than 75%
5%	Less than 50%

Q17. To what extent does your security operations center (SOC) have full visibility across all your organization's risk areas/vulnerabilities? (Base: Total security leaders, n=200) | Q17b. What percent visibility of your organization's risk areas/vulnerabilities do you have? (Base: Security leaders indicating they have less than 100% visibility, n=19)

The vast majority believe their SOC is poised to prevent increasingly sophisticated cyber attacks.

More than eight in ten leaders across medium- and large-sized companies claim this level of preparedness.

Self-Assessment: Preparedness for Increasingly Sophisticated Cyber Threats and Attacks



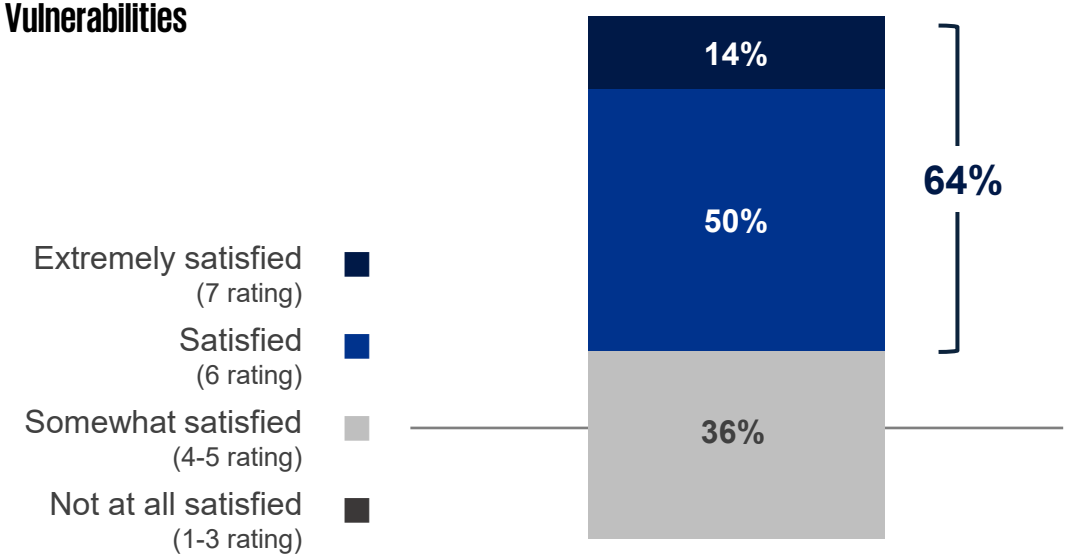
Q30. How confident are you in your security operations center's (SOC) readiness to prevent future, sophisticated attacks? (Base: Total security leaders, n=200)

On average security leaders report it takes about 15 days for their SOC to remediate a vulnerability and most are satisfied with this timing.

Time to remediate is significantly shorter among those satisfied with the time (9 days) compared to those not satisfied (25 days).

Satisfaction with SOC's Time Required to Address and Remediate Vulnerabilities

Satisfaction with Time to Remediate Vulnerabilities



Average Time to Remediate Vulnerabilities

14.7 days

average # of days for the organization's SOC to respond to and remediate a vulnerability (total security leaders)

9.2 days Among those satisfied with time

vs.

24.5 days Among those NOT satisfied with time

Specific Responses:

92%	<75 days
4%	75 days - <150 days
5%	150 days - <250 days
1%	250 days+

Q18. How satisfied are you with the time it takes your security operations center (SOC) to address and remediate a vulnerability? | Q19. On average, how many days does it take your security operations center (SOC) to respond to, and remediate a vulnerability? Your best estimate is fine. (Base: Total security leaders, n=200)

A majority claim "first adopter" status and identify their SOC's approach as innovative.

These Cyber leaders tend to be from larger, higher-revenue organizations, and are especially prevalent among technology companies.

Approach of Organization's Security Operations Center

LAGGING → INNOVATIVE

2% Laggard

*We have **difficulty implementing new solutions and approaches** even when they are well-established.*

13% Late Adopter

*We generally look for solutions and approaches with **well-established use cases**.*

14% Early Adopter

*Not the first to adopt new solutions and try new approaches, but we are usually **next in line after use cases are established**.*

72% Innovator

*Tend to be **first to adopt new solutions** and try new approaches even when they do not have existing use cases.*

Self-identified INNOVATORS tend to be:

- From **very large enterprise** (5,000+ employees, 75%) ($5B+ revenue, 54%)
- Most are from **tech companies** (22%), followed by healthcare (13%) and automotive (13%).

Q1. Which of the following best describes your security operations center (SOC) in terms of how it views innovation and evolving its approach? (Base: Total security leaders, n=200)

Yet, four in ten security leaders indicate their SOC has suffered a recent cyber attack that caused a security breach.

The most common breaches were the result of malware attacks, among others.

Experience with and Type of Attacks Resulting in Security Breaches in the Last Year

40%

of security leaders indicate their **SOC has suffered an attack(s) that resulted in a security breach in the last year**

Number of Cyber Attacks
(Past Year)

60%	*No attacks*
38%	*1-3 attacks*
2%	*4 or more*

TYPE OF ATTACK(S)
(Shown among all security leaders)

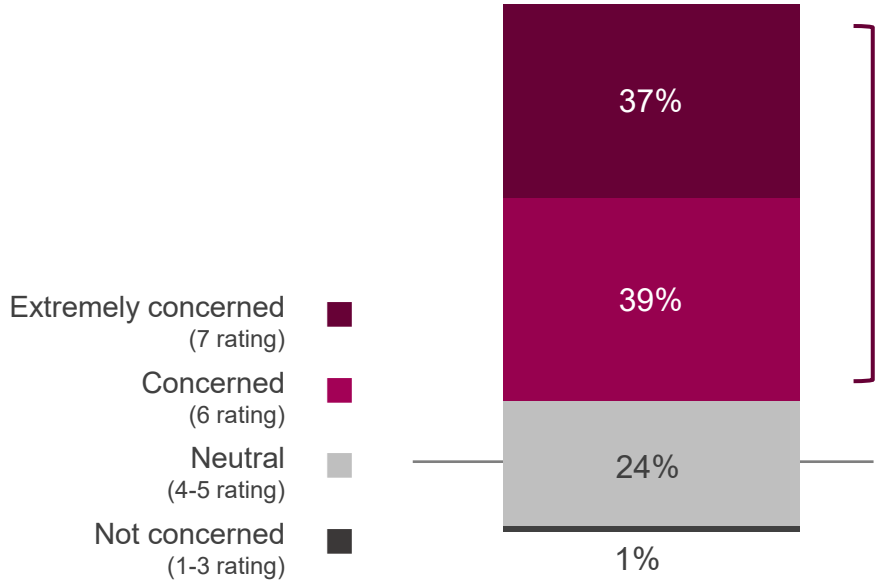
19%	**Malware attack**
11%	Password attack
10%	Ransomware attack
10%	Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS)
10%	Internet of Things (IoT) attack
10%	Insider threats/tricking users into breaking security procedures
7%	Phishing attack
7%	SQL injection attacks
6%	Man-in-the-Middle attacks
5%	Spoofing attack
60%	Have NOT suffered an attack in the last year

Q14. In the last in the last year, has your security operations center (SOC) suffered an attack(s) that resulted in a security breach? (Base: Total security leaders, n=200) | Q15. What type of security attack(s) was it? Select all the apply. (Base: Total security leaders in organizations that suffered an attack resulting in a security breach, n=81; Not shown above, "other," %)

Looking ahead, most are concerned about the increasing sophistication of new cyber threats.

Concern peaks among those who have had recent experience with a cyber attack that resulted in a security breach in the past year.

Concern about Increasingly Sophisticated Cyber Threats/Attacks and Source



76%

of security leaders are concerned about the increasing sophistication of new cyber threats and attacks

Concern especially common among…

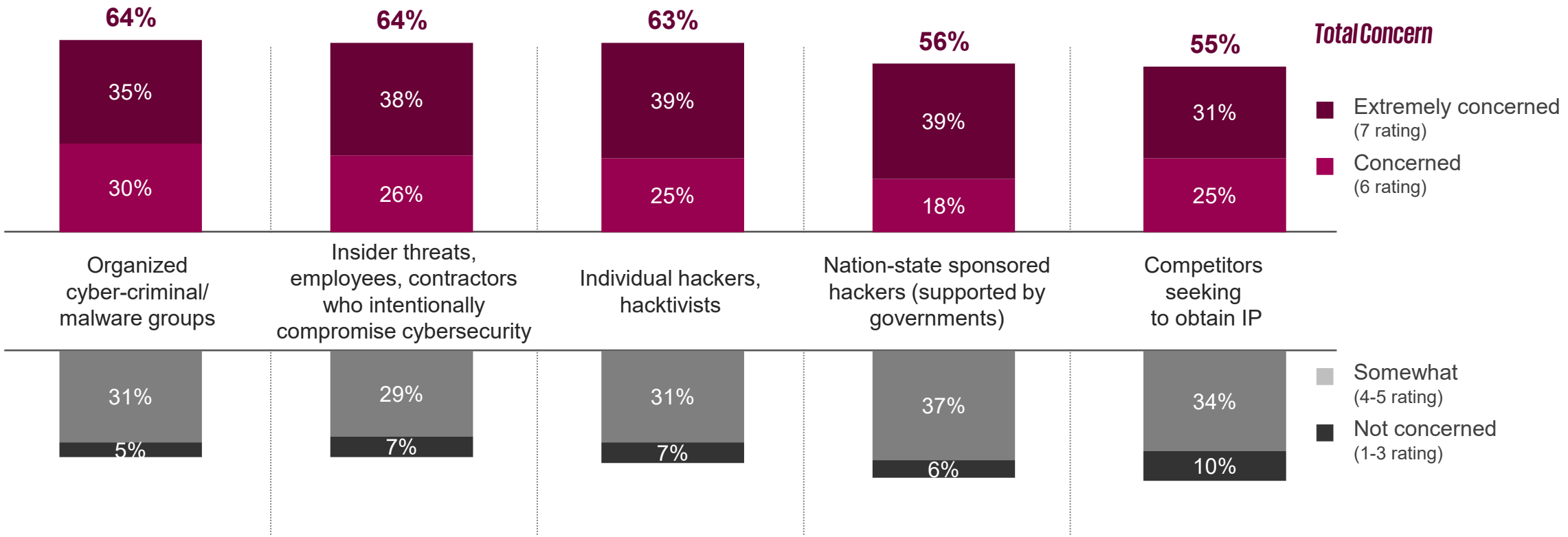
81% **Large-sized companies** (5K+ employees) **vs.** **64%** **Medium-sized companies** (<5K employees)

85% Leaders that **experienced a cyber attack** **vs.** **69%** Leaders that have **NOT experienced a cyber attack**

Q29. Please rate your level of concern about the increasing sophistication of new cyber threats and attacks. (Base: Total security leaders, n=200)

Leaders are most concerned about organized cyber-crime groups, insider threats (employees and contractors), and individual hackers.

Concern about Cyber Threats/Attacks from Specific Groups



Q31. Please rate how concerned you are about being the target of sophisticated attacks from the following groups. (Base: Total security leaders, n=200)

Security leaders that have experienced a recent cyber attack are still confident about their SOC's oversight of risk areas and threat readiness.

Attitudes among Security Leaders Experiencing Cyber Attacks

Preparedness for Increasingly Sophisticated Cyber Threats and Attacks

% Confidence in understanding risk areas

73%	vs.	66%
Security Leaders – **Recent** Cyber Attack		Security Leaders – **No Recent** Cyber Attack

Visibility Across the Organization's Risk Areas/Vulnerabilities

% Full visibility across risk areas

90%	vs.	91%
Security Leaders – **Recent** Cyber Attack		Security Leaders – **No Recent** Cyber Attack

Confidence in SOC's Readiness to Prevent Future Cyber Attacks

% Confidence in readiness of SOC

86%	vs.	83%
Security Leaders – **Recent** Cyber Attack		Security Leaders – **No Recent** Cyber Attack

Expected Change to SOC Budget (Next 2 Years)

% Increasing SOC Budget

78%	vs.	71%
Security Leaders – **Recent** Cyber Attack		Security Leaders – **No Recent** Cyber Attack

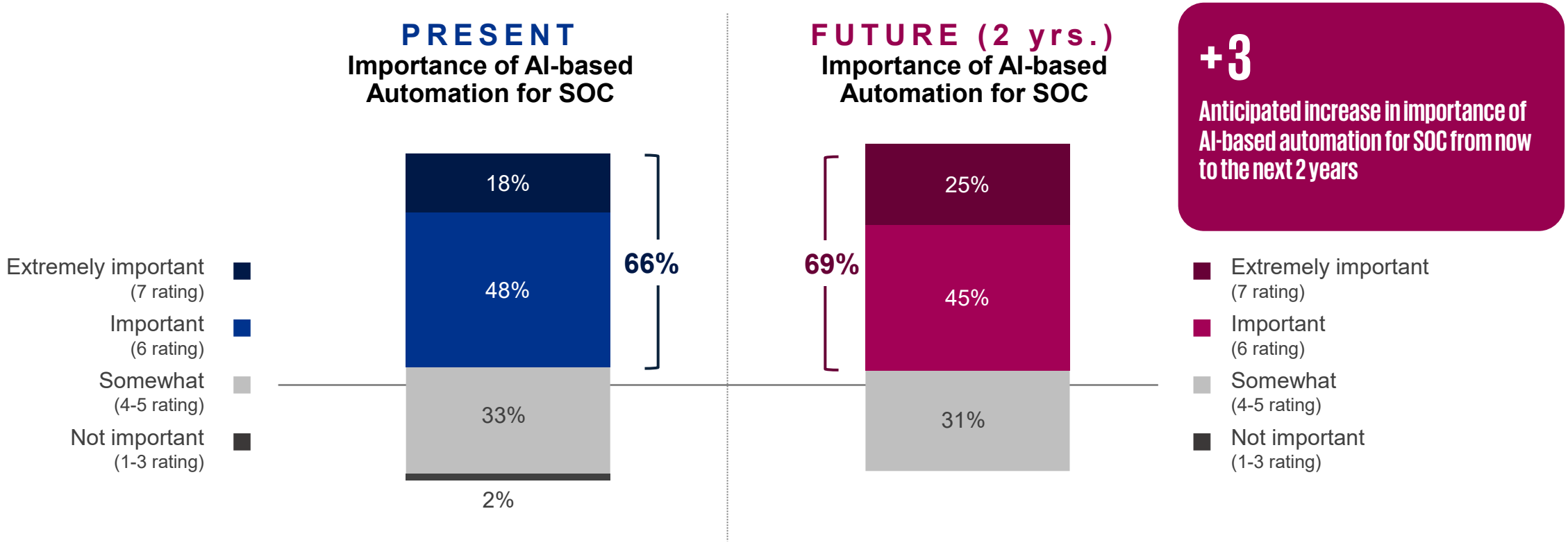
Q16. To what degree are you confident that your security operations center (SOC) has a solid understanding of your organization's risk areas/vulnerabilities? | Q17. To what extent does your security operations center (SOC) have full visibility across all your organization's risk areas/vulnerabilities? | Q30. How confident are you in your security operations center's (SOC) readiness to prevent future, sophisticated attacks? | Q6. Are you expecting your security operations center (SOC) budget to increase, stay the same or decrease over the next two years? (Base: Total security leaders, n=200)

DETAILED FINDINGS

AI as a “Game Changer”

Two-thirds of security leaders believe AI-based automation for their SOC is important now and will remain so for the next two years.

Importance of AI-based Automation for SOC: Present and Future State



Q21. How important is automation delivered through AI (Generative AI, machine learning) to your security operations center (SOC) right now? | Q22. How important will automation delivered through AI (Generative AI, machine learning) be over the next 2 years? (Base: Total security leaders, n=200)

Leaders are looking to AI-based automation to stay ahead of new and emerging threats and to increase SOC agility and response.

SOC measurement and reporting, and the availability of resources through increased productivity resulting from AI-based automation are also highly desired. Security leaders from medium- and large-sized companies are similar in their preferred uses of AI.

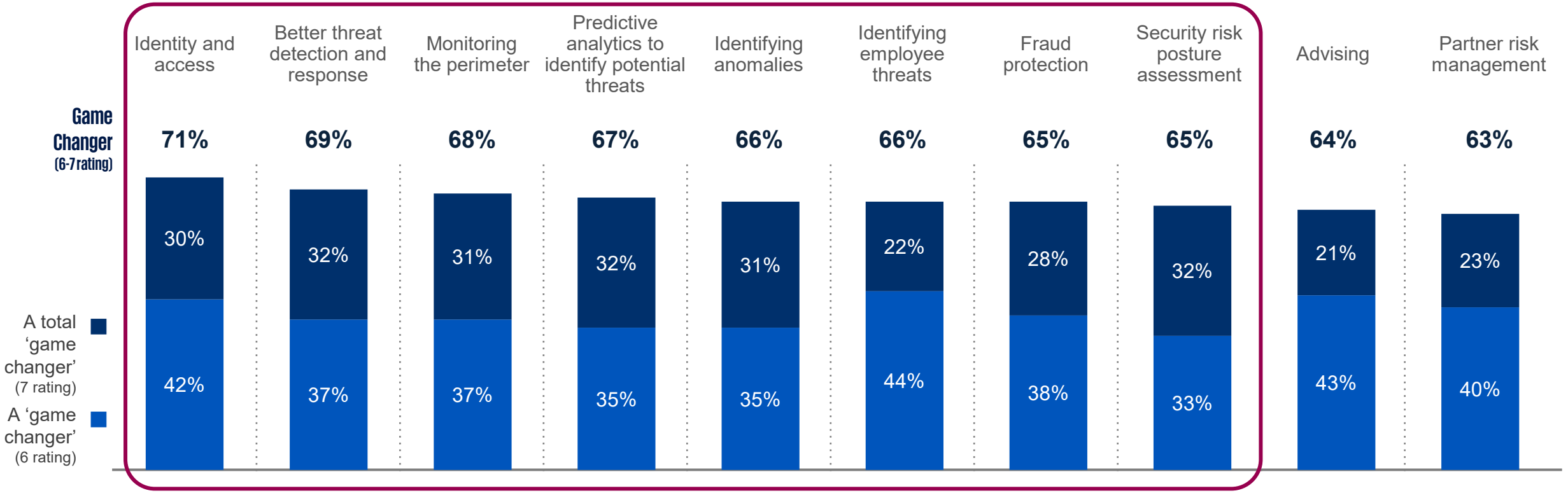
Desired Benefits of AI-based Automation for SOC (up to three responses allowed)

Q23. What benefits do you want automation through AI (Generative AI, machine learning) to generate for your security operations center (SOC)? Select up to 3.
(Base: Total security leaders, n=200)

At least six in ten security leaders believe AI will be a "game changer" across all security functions.

Security leaders most commonly identify AI as transformative in identity access.

Areas in Which AI Will be a 'Game Changer' in Identifying and Remediating Threats/Vulnerabilities

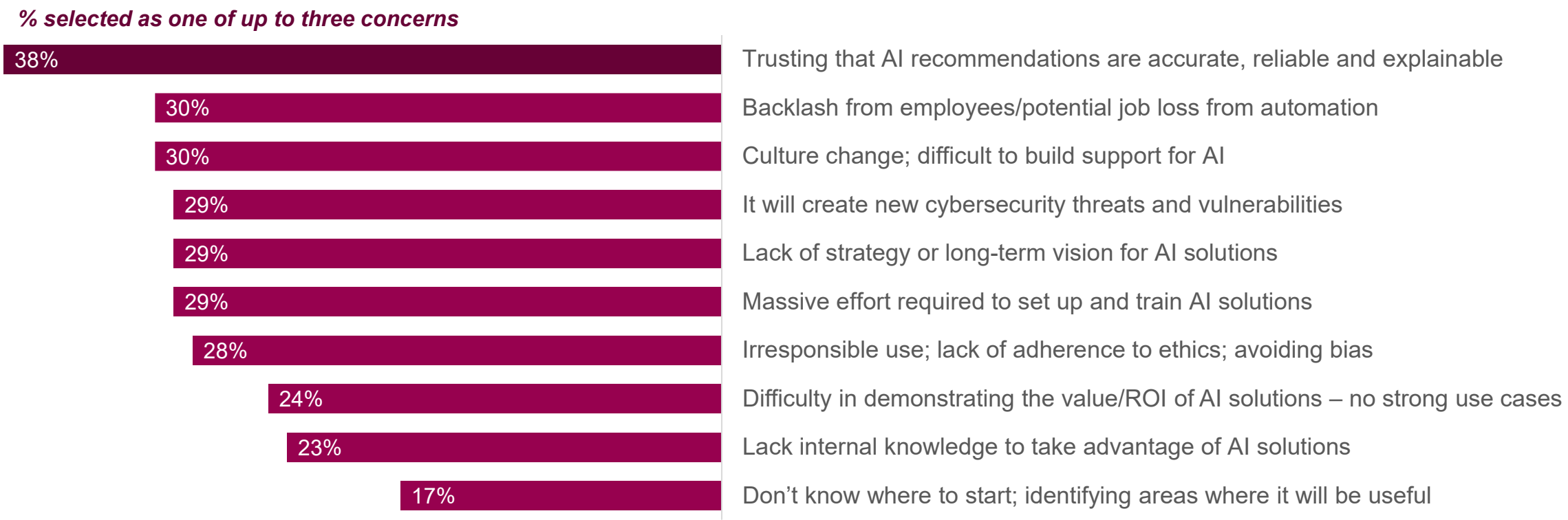


Q24. Over the next 2 years, where do expect AI (Generative AI, machine learning) will be a 'game changer' in identifying and remediating threats and vulnerabilities? (Base: Total security leaders, n=200; see appendix for full descriptions provided to survey respondents as part of the answer text.)

While AI-based automation has many benefits, the reliability of AI recommendations is a top concern for leaders.

Additional concerns focus on employee backlash, culture change, security, lacking a long-term AI strategy and the significant efforts required to set up and train AI solutions.

Challenges: Concerns about AI-based Automation for SOC (up to three responses allowed)



Q25. What are your biggest concerns about adopting AI (Generative AI, machine learning) in your security operations center (SOC)? Select up to 3.
(Base: Total security leaders, n=200; Not shown above: "other")

DETAILED FINDINGS

SOC Resources, Budget & Solutions

Improving trust in their organization's SOC is a top goal for nearly half of security leaders.

Supporting new business cases is also a priority among more than a third of security leaders looking ahead.

Priorities: for the Organization's SOC over Next Two Years

% selected as one of up to three priorities

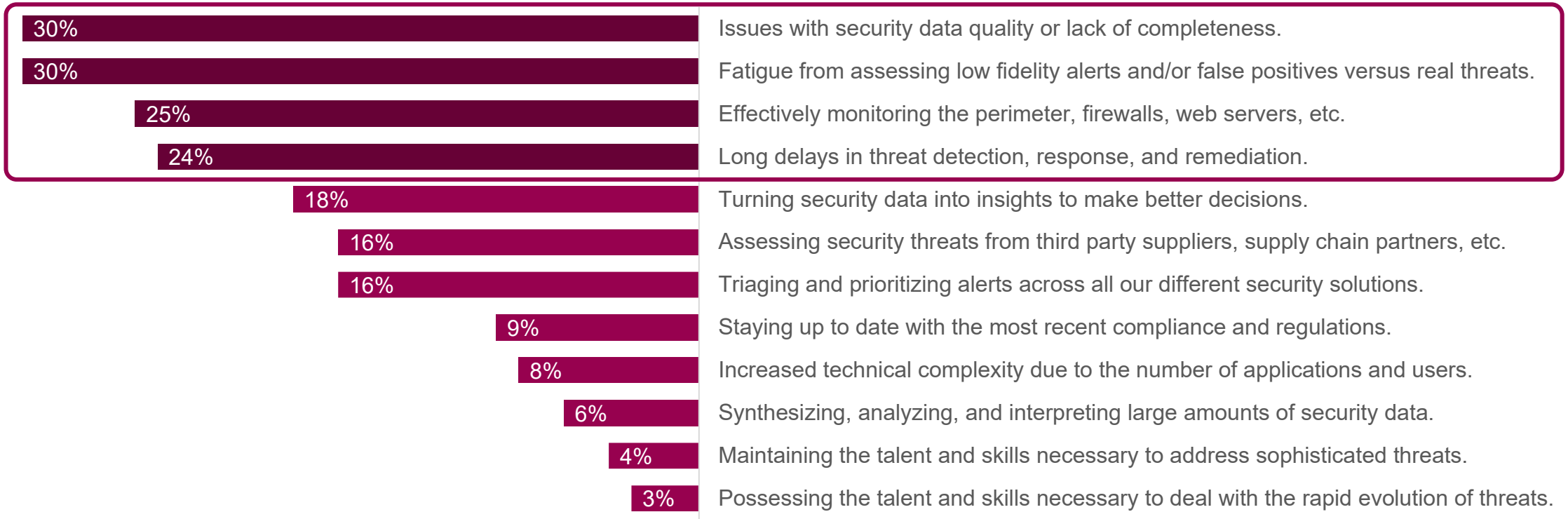
Q2. Please select the TOP 3 priorities for your security operations center (SOC) over the next 2 years. Select up to 3. (Base: Total security leaders, n=200)

Top pain points for security leaders include navigating security data quality and the prioritization of various levels of threats.

Monitoring perimeters effectively and detecting and responding to threats in a timely manner are a challenge for about one in four security leaders.

Challenges: Overall SOC Pain Points

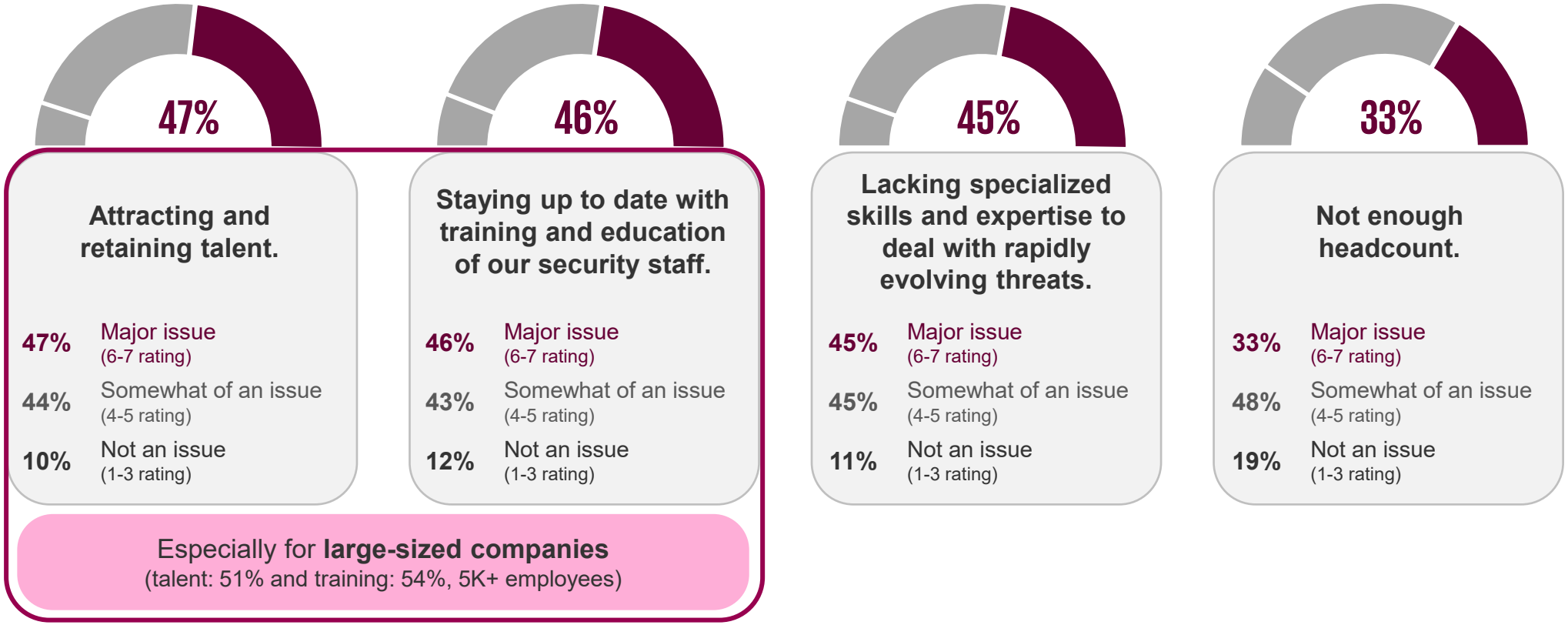
% ranked #1-2 as "most painful"



Q13. How would you rank your TOP 3 from the following where "1" the most painful, "2" the second most painful and so forth. (Base: Total security leaders, n=)

Half of security leaders also face challenges of retaining talent and maintaining training and expertise to deal with sophisticated threats.

Challenges: Talent Issues in the Organization's SOC



Q5. To what extent are you facing the following talent issues in your security operations center (SOC)? (Base: Total security leaders, n=200)

Nearly a third of security leaders indicate their SOC has difficulty determining the severity of cyber threats and vulnerabilities.

The complexity of the IT environment, lack of integration across solutions, and a lack of expertise among SOC staff are factors likely contributing to this challenge as they are experienced by more than one in four security leaders .

Challenges: SOC's Barriers to Identifying and Remediating Threats and Vulnerabilities

Q20. What are the biggest barriers to identifying and remediating threats and vulnerabilities? Select up to 3.
(Base: Total security leaders, n=200; Not shown above: "none of these are challenges," 1%)

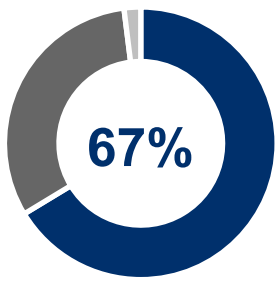
Just half of security leaders say their SOCs are taking proactive steps (threat hunting and prediction) to address threats.

Training for more sophisticated threats is most mentioned as currently underway, among two-thirds of security leaders. Collaborating with other organizations is common for about 6 in 10 SOCs.

Current or Planned Actions to Address Sophisticated Future Cyber Attacks and Threats

Increasing Cybersecurity Expertise

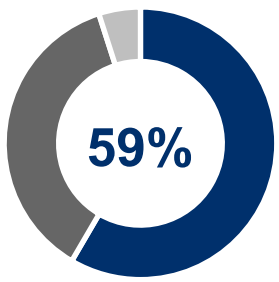
Training to handle more sophisticated threats.



Already doing this | 67%
Planning, next 12 mo. | 32%
No plans | 2%

Sharing And Collaborating

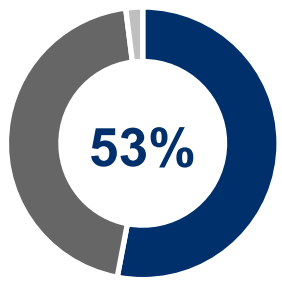
Sharing and receiving threat intelligence with other organizations.



Already doing this | 59%
Planning, next 12 mo. | 37%
No plans | 5%

Threat Hunting

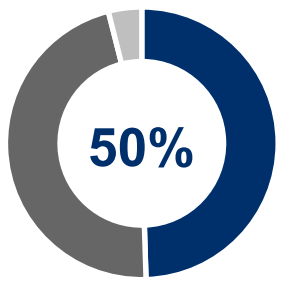
Rather than waiting for threats, proactive threat hunting.



Already doing this | 53%
Planning, next 12 mo. | 45%
No plans | 2%

Predictive Threat Intelligence

Using AI and advanced analytics to predict potential threats.



Already doing this | 50%
Planning, next 12 mo. | 47%
No plans | 4%

% Already Doing this Action

Q32. Are you already doing now, planning to do, or have no immediate plans to do the following to address sophisticated, future attacks and threats? (Base: Total security leaders, n=200)

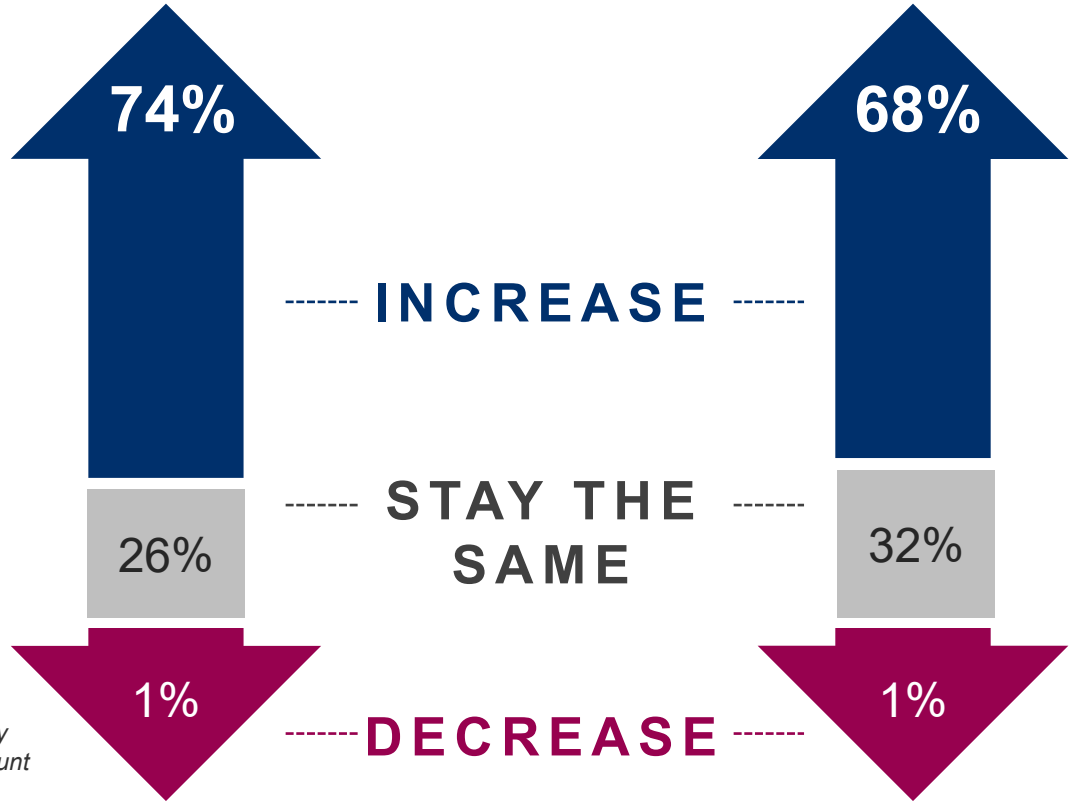
Faced with these priorities and challenges, leaders are expecting to increase SOC headcount and budget over the next two years.

The majority (87%) say their SOC budget and headcount will increase by under 20%.

Expected Change to SOC Headcount and Budget (Next Two Years)

SOC Headcount

% Increase	
Less than 10%	**46%**
10% to <20%	**41%**
20% or more	**13%**



SOC Budget

% Increase	
46%	Less than 10%
41%	10% to <20%
13%	20% or more

Q4a. Are you expecting headcount within your security operations center (SOC) to increase, stay the same or decrease over the next two years? (Base: Total security leaders, n=200) | Q4b. By what percent is your headcount increasing? (Base: Security leaders indicating their headcount is increasing, n=147)

Q6. Are you expecting your security operations center (SOC) budget to increase, stay the same or decrease over the next two years? (Base: Total security leaders, n=200) | Q7. By what percent is your security operations center (SOC) budget increasing? (Base: Security leaders indicating their SOC budget is increasing, n=135)

Current annual SOC budget averages $14.6M with most (37%) going to prevention and detection.

Log management and reporting accounts for 15% of the SOC budget, on average.

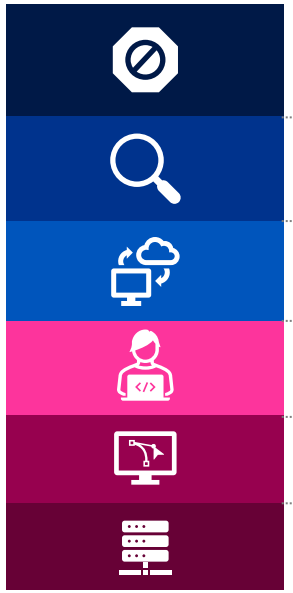
Annual Overall SOC Budget and Distribution Across Expenses

$14.6 M
Average Annual SOC Budget

Annual Budget Breakout:

22%	Less than $2M
38%	$2M to less than $10M
39%	$10M or more

Average Distribution of SOC Budget Across Expenses



19%	**Prevention** (vulnerability, threat intelligence)
18%	**Detection** (Intrusion, endpoints, network traffic)
17%	**Maintaining Infrastructure** (i.e., hardware, cloud, storage, network)
16%	**Response and Remediation**
15%	**AI, Machine Learning**
15%	**Log Management and Reporting**

Q8. Approximately, what is the annual overall budget for your security operations center (SOC)? Use your best estimate. | Q9. Adding to 100%, how is your security operations center (SOC) budget allocated across the following expenses? Please consider budget for staffing and solutions/tools. For answer choices where no budget is allocated input "0."
(Base: Total security leaders, n=200)

Most security leaders believe they are spending the right amount on vendor tooling and log management.

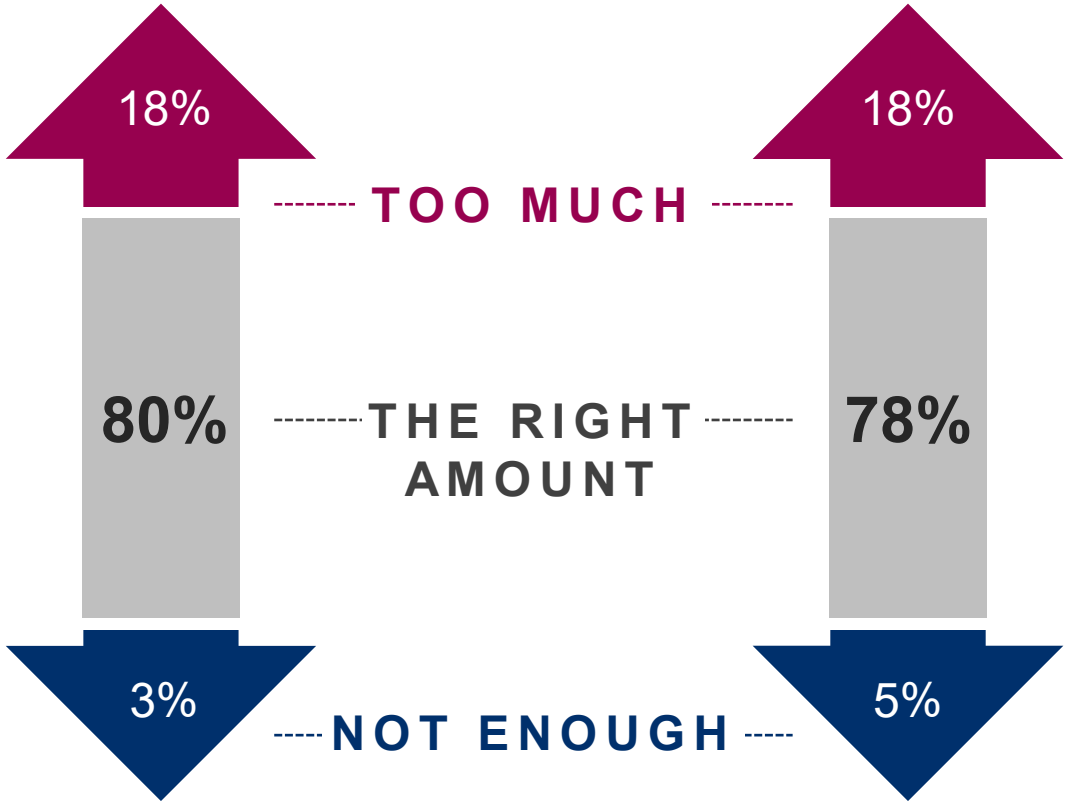
About one in five report they are spending too much on these budget areas.

Perception of SOC Spending on Vendor Tooling and Log Management

Spending on Vendor Tooling (Solutions & Services)

% Spending Too Much

Less than 10%	**33%**
10% to <20%	**28%**
20% or more	**39%**



Spending on Log Management

% Spending Too Much

26%	Less than 10%
40%	10% to <20%
34%	20% or more

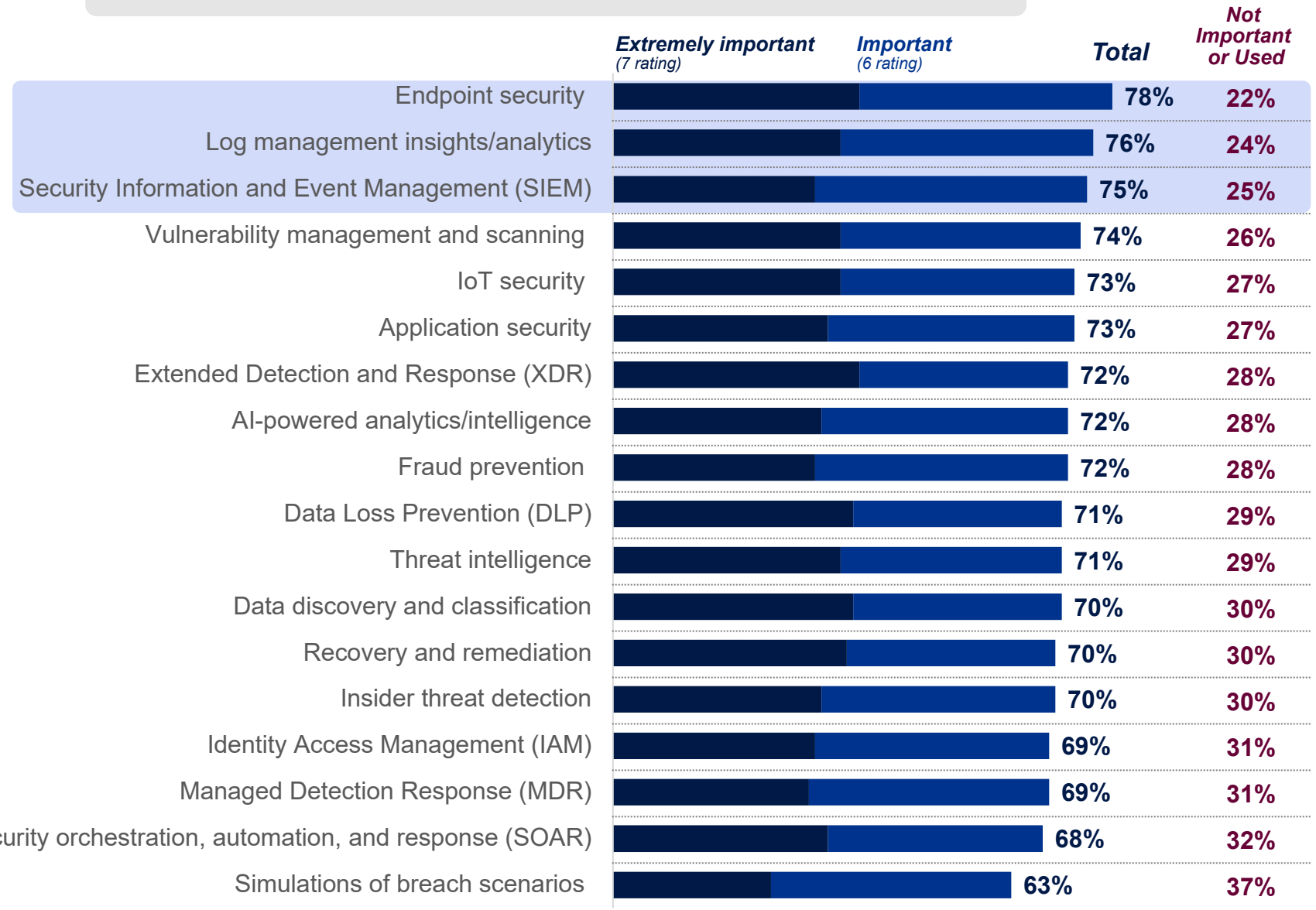
Q10a. Which best describes your feelings about how much your security operations center (SOC) is spending on its vendor tooling (solutions and services)? (Base: Total security leaders, n=200) | Q10b. By what percent is your security operations center (SOC) spending too much on vendor tooling (solutions and services)? (Base: Security leaders indicating their SOC is spending too much, n=36)

Q11a. Which best describes your feelings about how much your security operations center (SOC) is spending on log management and storage? (Base: Total security leaders, n=200) | Q11b. By what percent is your security operations center (SOC) spending too much on log management? (Base: Security leaders indicating their SOC is spending too much, n=35 or not enough)

Security leaders indicate a myriad of important current solutions for their SOC.

Services that reach utilization among 3 in 4 SOCs include endpoint security, log management analytics, and SIEM.

Most Important Services and Solutions for the Organization's SOC



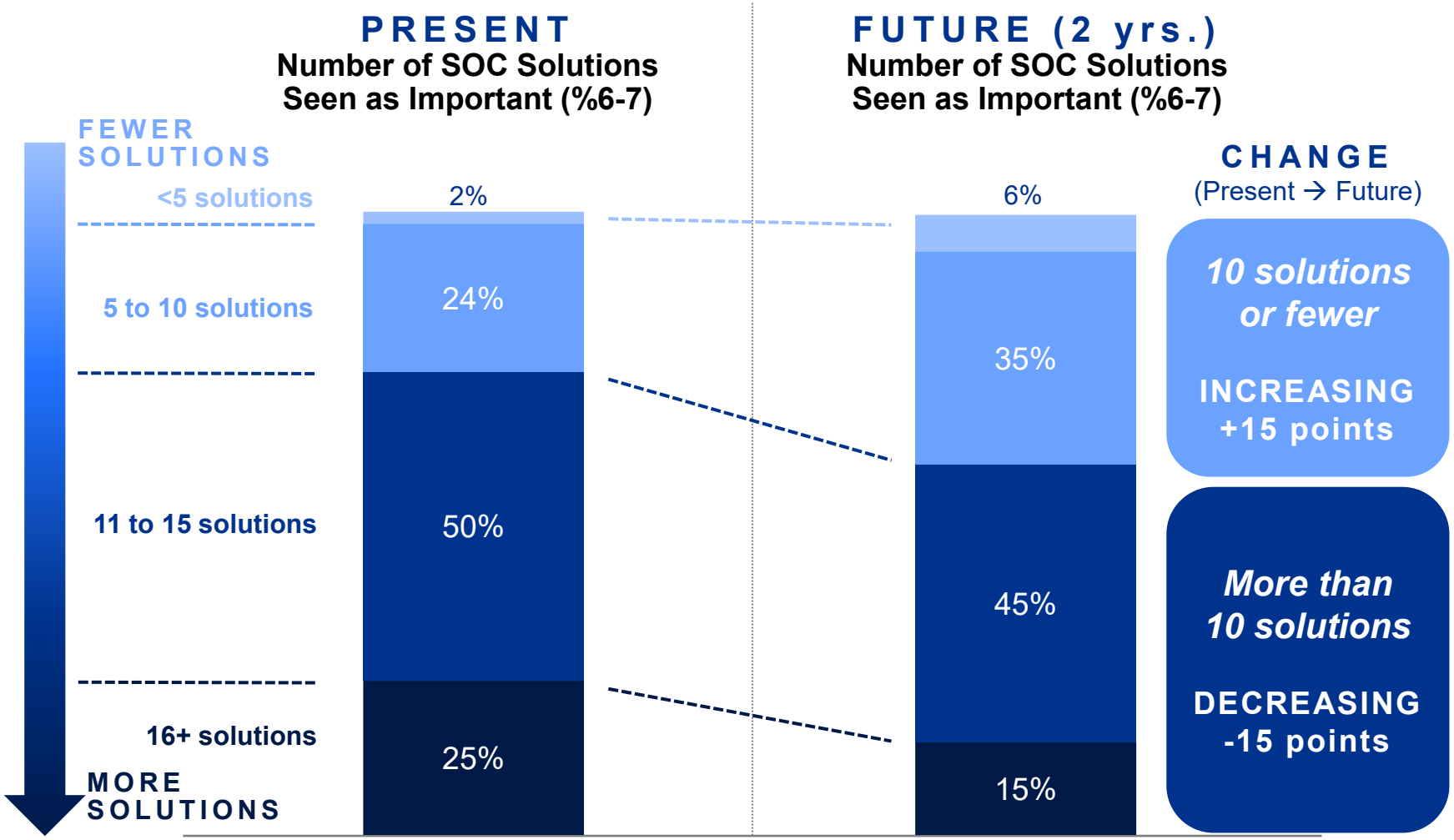
Q3A. How important are the following services and solutions to your security operations center (SOC)? | Q3B. How important will these services and solutions be to your security operations center (SOC) over the next 2 years? (Base: Total security leaders, n=200)

But, looking ahead for the next two years, security leaders say that fewer services and solutions will be as important.

This suggests more prioritization and consolidation of solutions in the future. It also reflects the challenges experienced with complex security environments and lack of integration that security leaders cite as top challenges.

Q3A. How important are the following services and solutions to your security operations center (SOC)? | Q3B. How important will these services and solutions be to your security operations center (SOC) over the next 2 years? (Base: Total security leaders, n=200)

Most Important Services and Solutions for the Organization's SOC: Present and Future (Next Two Years)



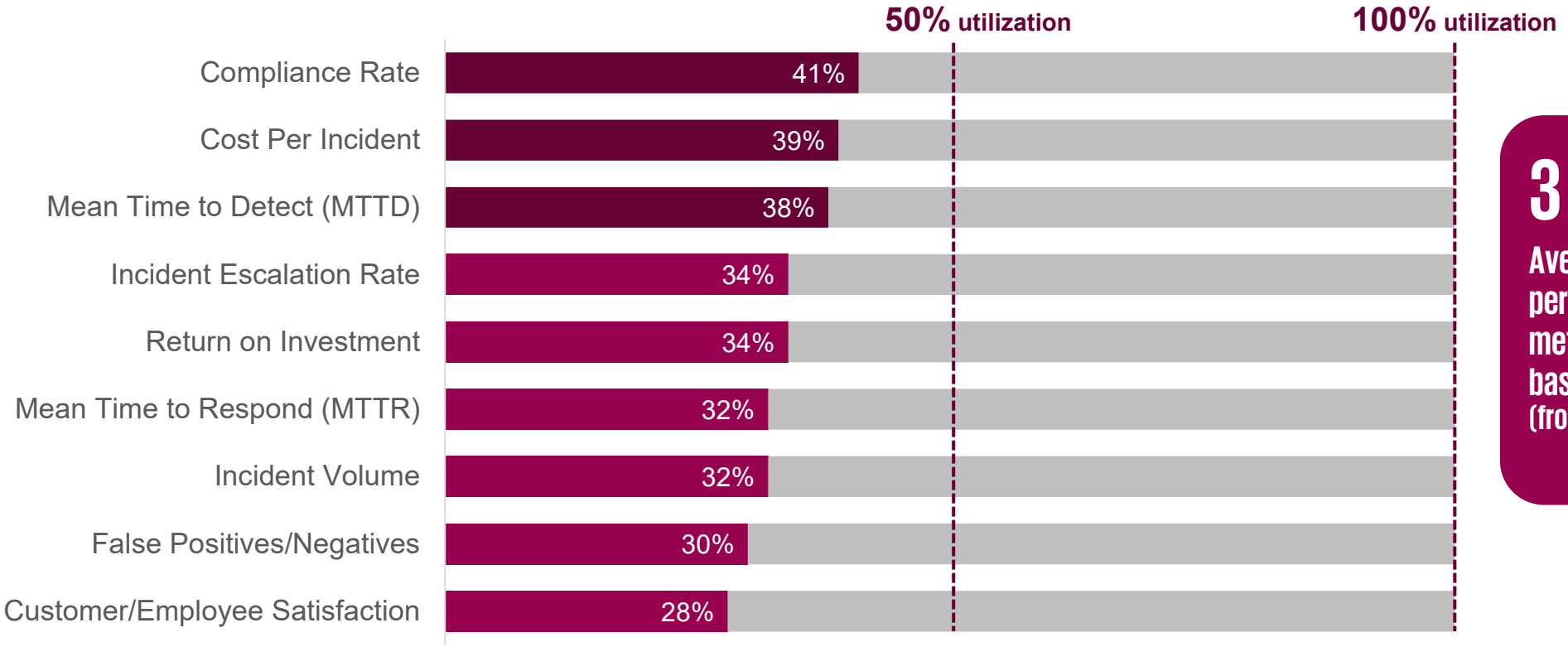
DETAILED FINDINGS

SOC PERFORMANCE

On average, security leaders say they are using three SOC performance measurement metrics on a regular basis.

Taken individually, no SOC performance measurement metric reaches utilization among 50% of organizations.

SOC Performance Measurement Metrics Utilized (Multiple responses allowed)



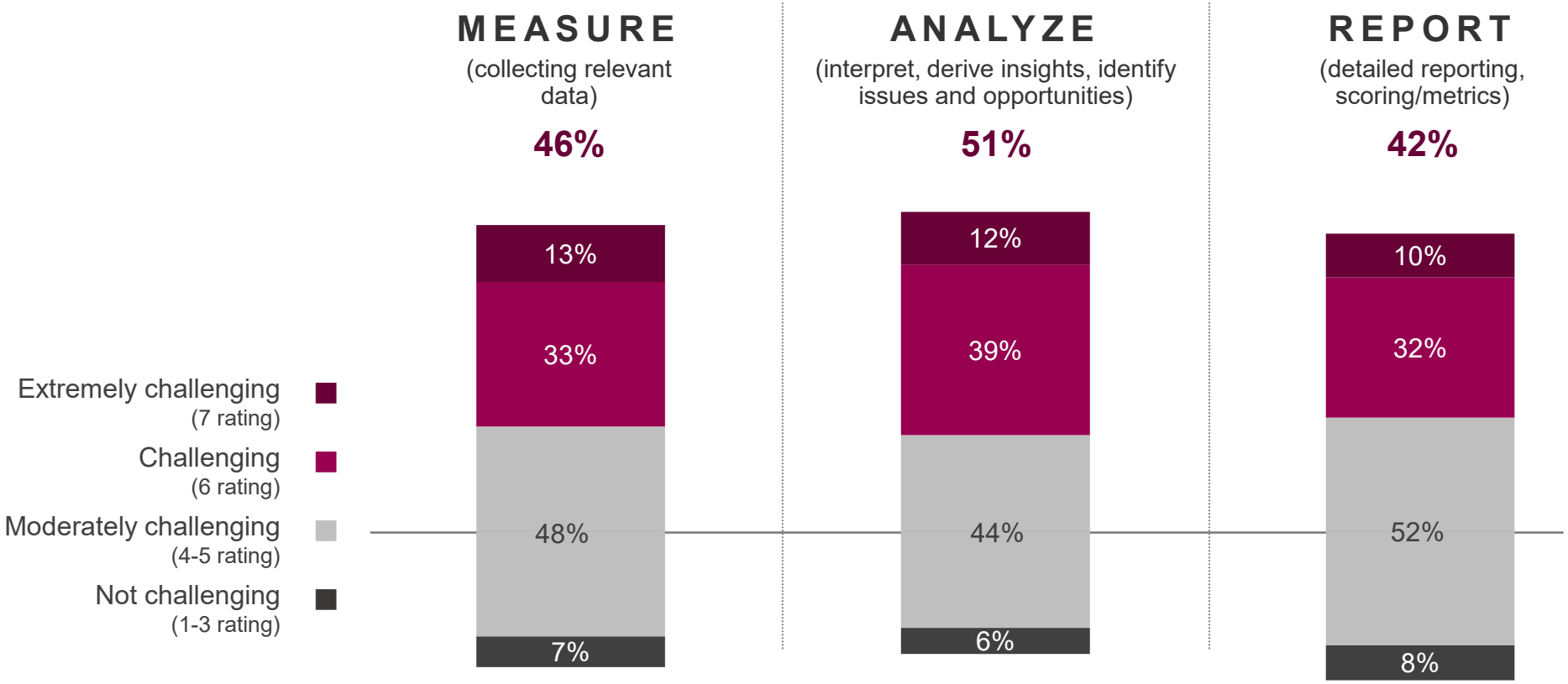
3.1

Average number of SOC performance measurement metrics used on a regular basis (from this survey list)

Q28. What metrics does your security operations center (SOC) use on a regular basis to measure its performance? Select all that apply.
(Base: Total security leaders, n=200; see appendix for full descriptions provided to survey respondents as part of the answer text; Not shown above: "none of these," 1%)

At least four in ten security leaders struggle with assessing their SOC's performance – most prevalently in analyzing relevant data.

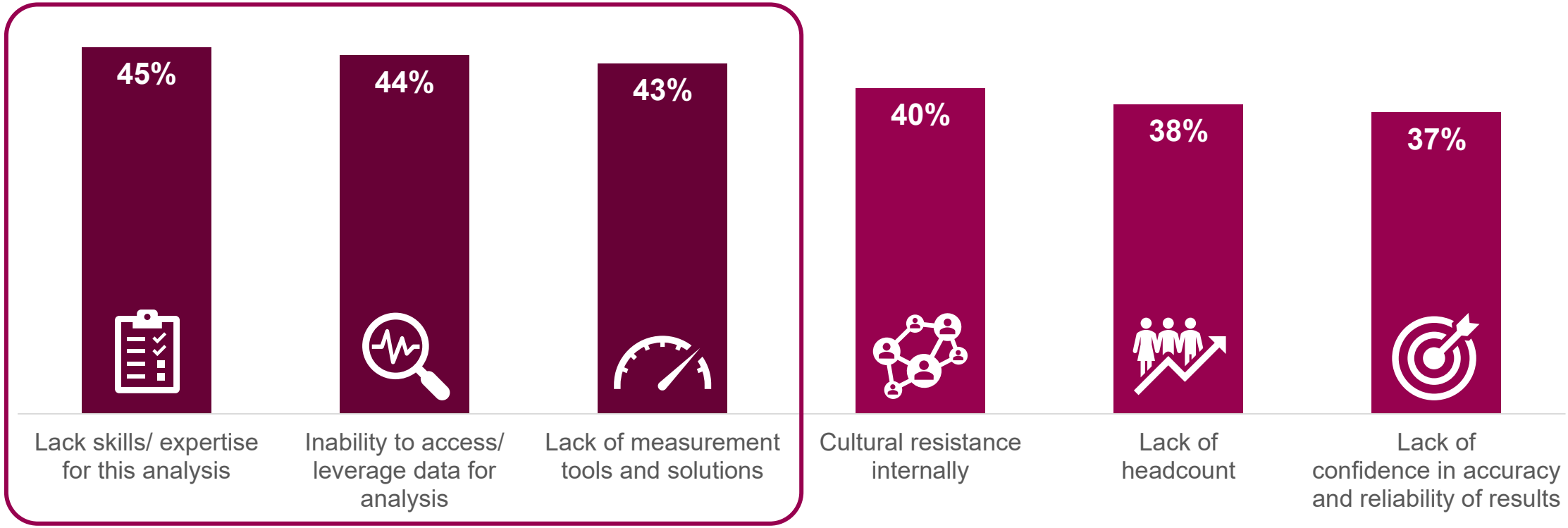
Challenges: Measuring, Analyzing and Reporting on SOC Performance



Q26. To what degree is it a challenge to measure, analyze and report on the performance of your security operations center (SOC)? (Base: Total security leaders, n=200)

At least four in ten security leaders cite specific challenges in lacking measurement tools, comprehensive data for analysis, and the expertise needed for evaluation.

Challenges: Measuring, Analyzing, and Reporting on SOC Performance (Multiple responses allowed)



Q27. What are the most significant challenges for you to measure, analyze and report on the performance of your security operations center (SOC)? Select all that apply. (Base: Total security leaders, n=200; Not shown above: "No challenges," 2%)

APPENDIX

- Respondent profile
- Full survey descriptions
- Additional detailed findings

Respondent Profile

PRIMARY FUNCTION

100%

IT, Security or Technology

JOB TITLE

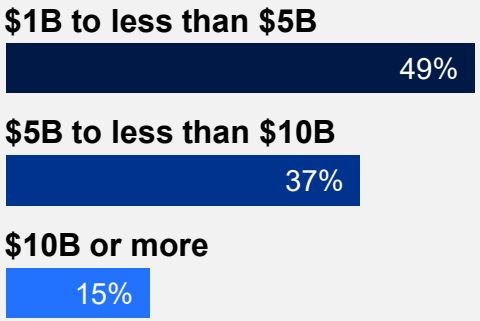
INDUSTRY

Consumer & Retail	27%
Industrials/Manufacturing	22%
Healthcare & Life Sciences	18%
Technology	18%
Energy, Natural Resources & Chemicals	13%
Telecommunications & Media	7%
Financial Services – Banking	3%
Financial Services – Insurance	1%
Other	1%

COMPANY SIZE

500 – 999	7%	33%
1,000 – 4,999	27%	
5,000 – 9,999	42%	67%
10,000 – 19,999	15%	
20,000+	10%	

ANNUAL REVENUE



QTS2. What best describes your primary business function? | QS3. Which of the following best describes your title? | QS4. Approximately how many individuals does your company employ across all locations? | QS5. What was the annual revenue for your company in its last fiscal year? | QS1. What industry do you work in? Select all that apply.

Areas in Which AI Will Be a "Game Changer"

Full Descriptions Provided to the Survey Respondent

Q24. Over the next 2 years, where do expect AI (Generative AI, machine learning) will be a 'game changer' in identifying and remediating threats and vulnerabilities? (Rated on scale of 1 – "Not at all a 'game changer'" to 7 – "A total 'game changer.'")

- **Better threat detection and response** (reduces alert 'noise' and identify genuine threats).
- **Fraud prevention** (enhancing detection).
- **Identifying employee threats** (unintentional or intentional).
- **Identifying anomalies** (detecting deviations from normal behaviors/patterns)
- **Advising** (how to respond and remediate an issue).
- **Monitoring the perimeter** (constant monitoring to identify potential threats).
- **Security risk posture assessment** (show performance, provide scores, and benchmarks)
- **Identity and access** (ensuring the right identity access privileges)
- **Partner risk management** (protecting organization from third party security risks).
- **Predictive analytics to identify potential threats** (keeping up with changing threat landscape).

Security Operation Center Measurement Metrics

Full Descriptions Provided to the Survey Respondent

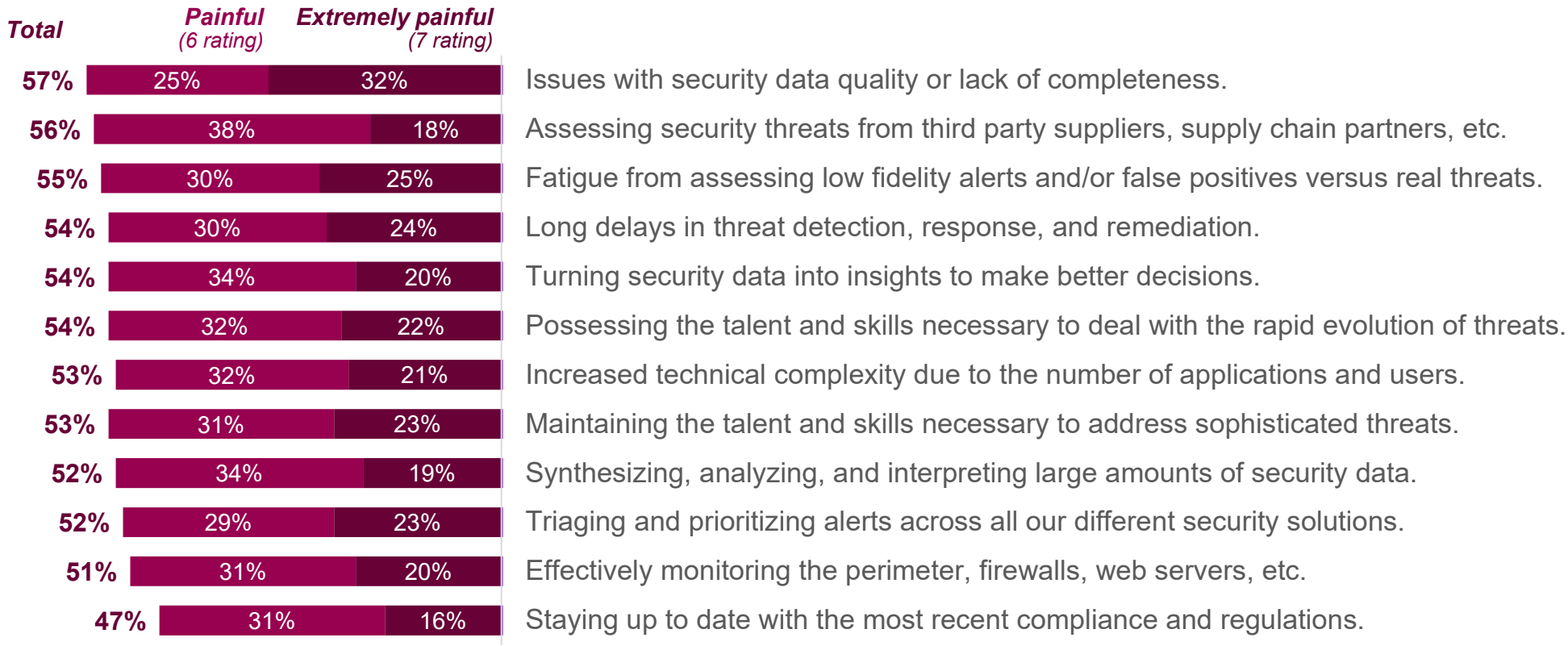
Q28. What metrics does your security operations center (SOC) use on a regular basis to measure its performance? Select all that apply.

- **Mean Time to Detect (MTTD)** – time to detect a threat.
- **Mean Time to Respond (MTTR)** – time it takes to respond to a threat.
- **Incident Volume** – tracks the number of security incidents handled over a given period.
- **Incident Escalation Rate** – how many incidents require escalation.
- **Compliance Rate** – how well we meet compliance obligations (regulatory, industry standards or internal policies).
- **Customer/Employee Satisfaction** – among external customers and/or internal employees.
- **Return on investment** for security tools and solutions.
- **False Positives/Negatives** – percentage of alerts that are false positives or actual threats missed.
- **Cost Per Incident** – cost associated with handling a security event.
- **None of these;** we do not measure our performance.

About half or more security leaders identify with each of the varied challenges for their organization's SOC services and operations.

About a third of security leaders say issues with security data quality and completeness are "extremely painful" for their SOC, the top challenge cited overall.

Challenges: Overall SOC Pain Points



Q12. Please rate the degree to which the following are causing pain in your security operations center (SOC)? (Base: Total security leaders, n=200)