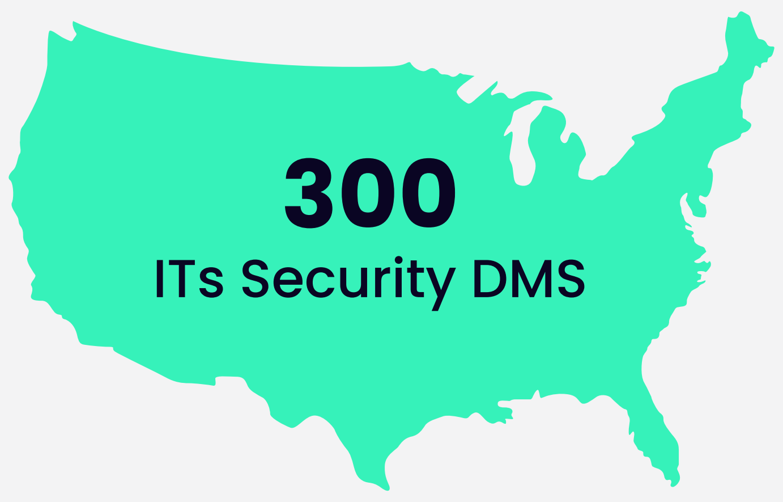
seemplicity

The 2025 Remediation Operations Report

GUIDE

The **2025 Remediation Operations Report** explores the evolving state of vulnerability management and security operations, based on insights from 300 IT and Security Decision Makers. Through this research, we uncover the key risk management challenges organizations face, the trends shaping their security strategies, and the technologies driving efficiency in vulnerability remediation. From security budgets to automation and AI adoption, this report provides a data-driven look at how organizations are tackling the growing complexity of vulnerability management and remediation operations.

Country of Residence



Annual Revenue

$	**15%**	Less than $50m
$$	**53%**	$50.1m to $500m
$$$	**32%**	More than $500m

Level of Influence

10%	have some influence on purchase decisions
29%	have a lot of influence on purchase decisions
61%	make cybersecurity purchase decisions alone

Business Size

# of Employees	501 to 1,000	1,001 to 5,000	5,001 to 10,000	10,000+
% of Respondents	**24%**	**47%**	**14%**	**15%**

Top 3 Business Industry

#1	**19%**	Software Technology
#2	**17%**	Manufacturing
#3	**12%**	Finance/Insurance/Accounting

Executive Summary

IT and Security Decision Makers report that their organizations are increasing their security investments, but financial constraints persist, forcing teams to allocate their spending strategically. The findings reveal a growing shift toward risk-based vulnerability management and AI-driven remediation, yet many organizations still struggle with making security findings actionable, prioritizing effectively, and addressing inefficiencies in their remediation processes.

The research shows that automation and structured collaboration have a strong, positive influence on the efficiency of vulnerability management. However, manual processes, unstructured workflows, and excessive noise from vulnerability scanning tools continue to slow remediation efforts, leading to delays and security risks. Despite advancements in automation, a significant portion of vulnerability management remains manual, increasing operational inefficiencies and contributing to alert fatigue.

Collaboration plays a critical role in improving remediation speed and decision-making. While many organizations perceive their collaboration as strong, the data reveals that poor communication and fragmented workflows persist, reinforcing the need for structured processes and centralized collaboration. Strengthening cross-team coordination can significantly reduce inefficiencies, ensuring that security and development teams are aligned in prioritization and remediation efforts.

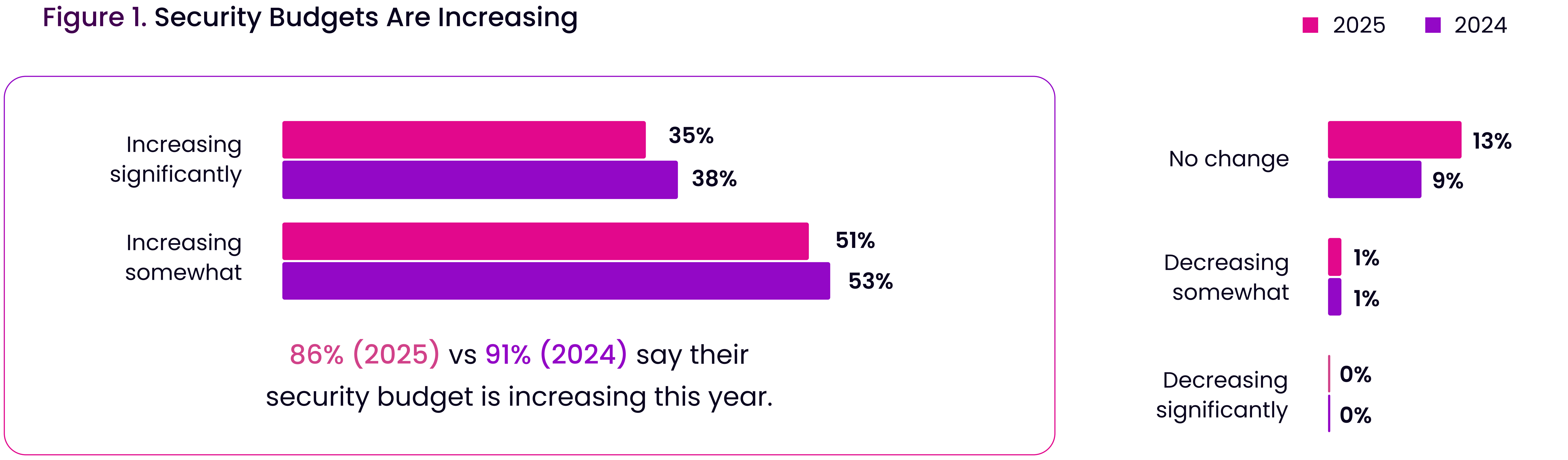
To close these gaps, organizations must adopt structured risk-based prioritization models, enhance collaboration through centralized workflows, and scale automation to reduce manual inefficiencies. By optimizing these areas, security teams can accelerate remediation efforts, reduce exposure time, and enhance overall resilience against evolving threats.

KEY FINDINGS

Security Budgets

Organizations are adjusting their security budgets to keep pace with growing risks. Most organizations are increasing their security spending in 2025 (86%), though this marks a slight decline from 2024, when 91% reported budget increases (Figure 1).

Figure 1. Security Budgets Are Increasing



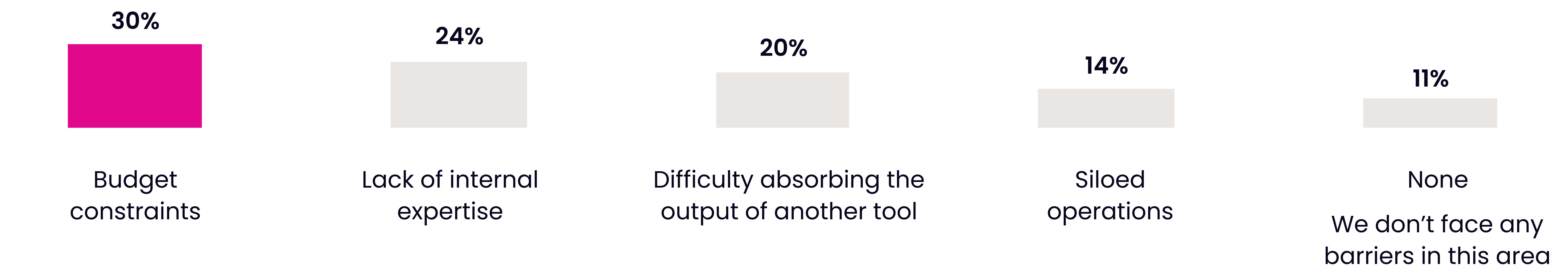
86% (2025) vs 91% (2024) say their security budget is increasing this year.

How, if at all, is your total security budget changing this year? Select one

Base: 300

Despite this ongoing investment, budget constraints remain a hurdle for some. In fact, 30% of organizations cite budget limitations as the biggest barrier to adopting new vulnerability management tools (Figure 2). This suggests that while security teams are securing more funding, financial flexibility remains limited, forcing them to carefully prioritize their investments.

Figure 2. Budgets Are Still A Limit For Some



What is the biggest barrier to adopting new tools or technologies for vulnerabilities management? Select one

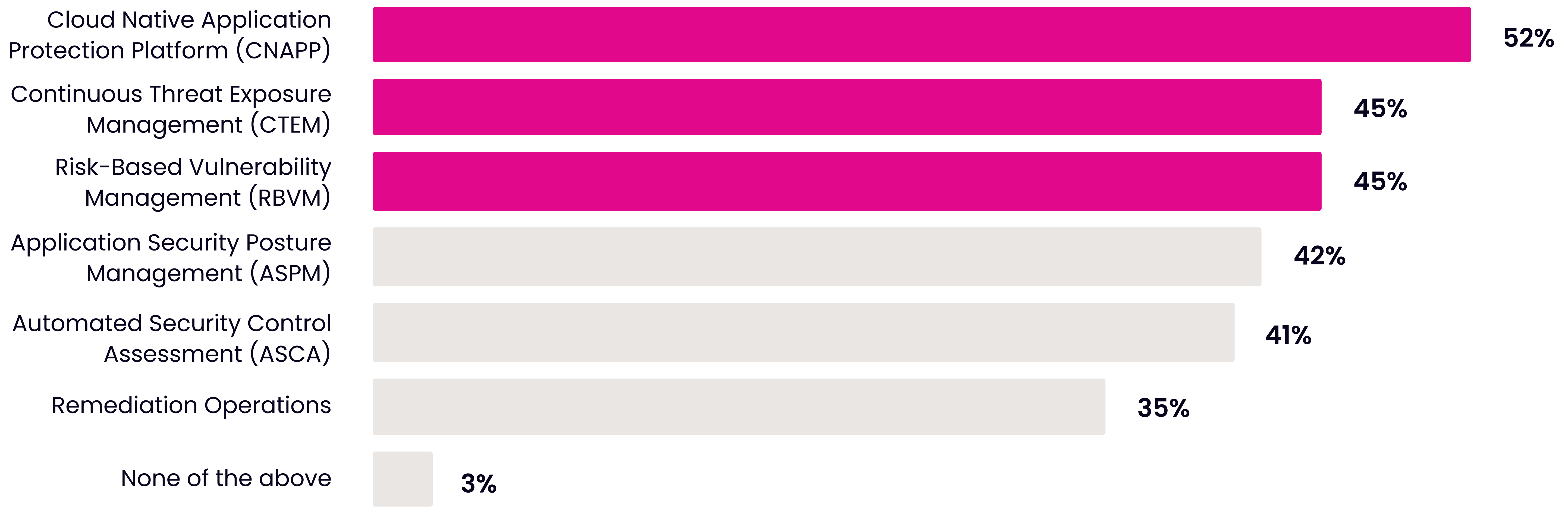
Base: 300

However, even with budget constraints, most organizations recognize the need for continued improvement and have allocated funds for security enhancements, budgeting for an average of three new vulnerability and exposure management tools in 2025 (Figure 3). This indicates that security leaders are committed to a multi-layered defense strategy, even when resources are tight.

Among the most prioritized investments, Cloud-Native Application Protection Platforms (CNAPP) leads the list, with 52% of organizations budgeting for it, followed closely by Continuous Threat Exposure Management (CTEM) and Risk-Based Vulnerability Management (RBVM), both at 45%. This shift suggests a growing preference for consolidated security architectures and continuous assessment capabilities, indicating that organizations are becoming more focused on long-term security strategies rather than short-term fixes.

Figure 3. Priority Investments Are CNAPP, CTEM & RBVM

Mean number of categories budgeted for: **3**



Which categories has your organization budgeted for, if any, in the next 12 months to improve vulnerability management? Select all that apply

Base: 300

Vulnerability Management Practices and Trends

MEASURING SUCCESS

When evaluating the success of their vulnerability management programs, 61% of organizations rely on the number of vulnerabilities resolved as their primary metric (Figure 4). While this provides a tangible measure of activity, it does not necessarily equate to reduced risk. However, the data also reveals that organizations do not rely on a single metric alone – on average, they use three different measures of success.

Fewer breaches (54%) and mean time to remediation (49%) rank as the second and third most common metrics, respectively. This reflects a growing recognition that vulnerability management is not just about volume but also about long-term risk reduction and operational efficiency. The inclusion of breach reduction and remediation speed as key metrics highlights an increasing focus on the effectiveness and timeliness of security efforts, rather than just the quantity of issues addressed.

Figure 4. Many Focus On Quantity Over Quality

Mean number of measures used: 3

Number of vulnerabilities resolved	Fewer Breaches	Mean time to remeadiation	SLA compliance rates	Cross-team aligment
61%	54%	49%	47%	40%

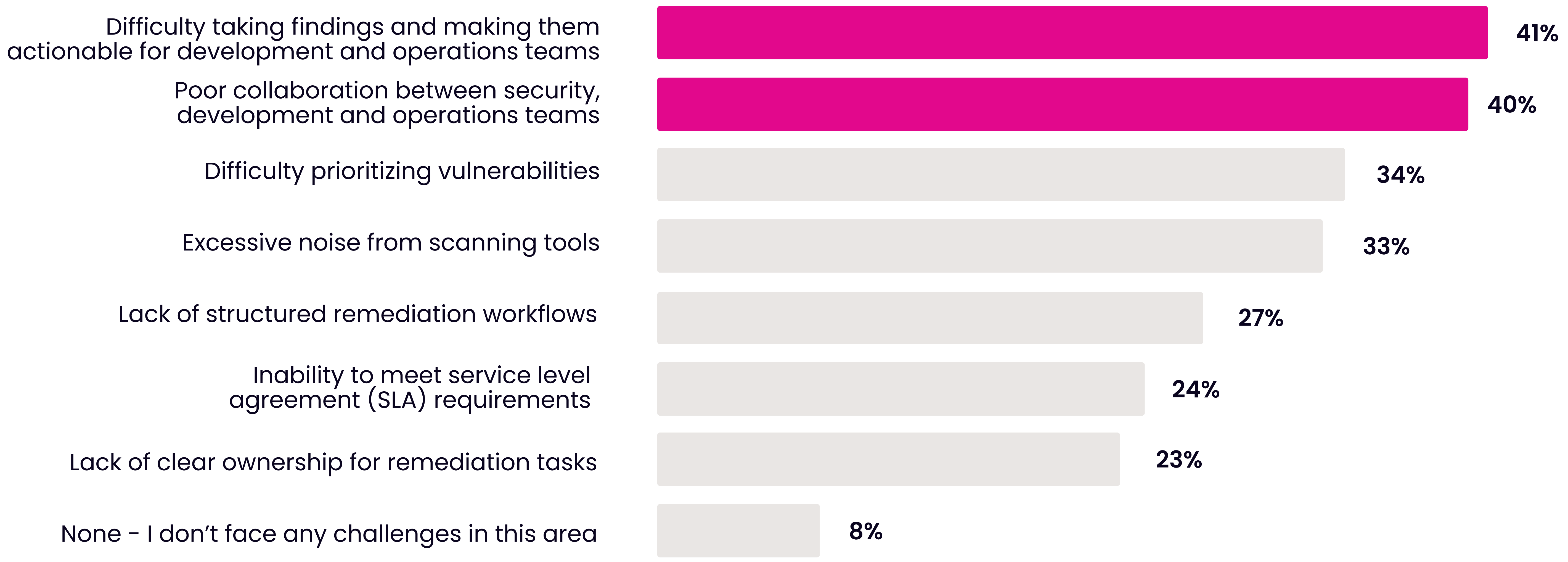
How do you measure the success of your vulnerability management program? Select all that apply

Base: 300

CHALLENGES IN MANAGING VULNERABILITIES

When it comes to managing vulnerabilities, organizations continue to struggle with making security findings actionable. The biggest challenge is translating findings into clear, actionable steps for development and operations teams (41%), closely followed by poor collaboration between security and development teams (40%) (Figure 5). The near-equal ranking of these challenges reinforces their correlation: when security and development teams are not aligned, vulnerability findings may lack the clarity needed for prompt action, while ineffective remediation workflows further strain collaboration. This cycle underscores the critical need for stronger cross-functional processes, ensuring security teams provide developers with clear, prioritized guidance that accelerates remediation rather than hindering it.

Figure 5. Key Challenges: Actionability, Collaboration, Prioritization

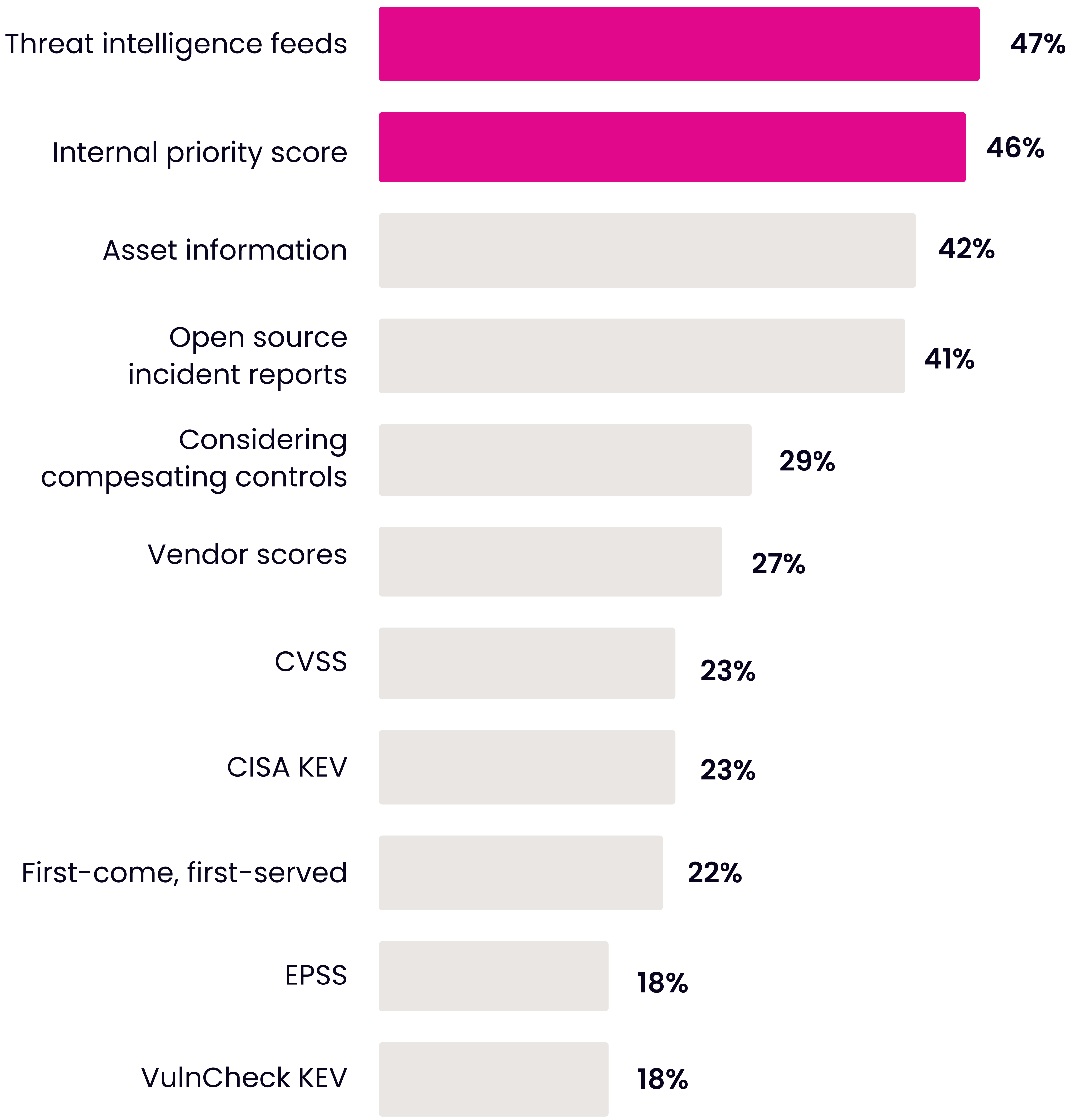


What are your biggest challenges in managing vulnerabilities today? Select up to three

Base: 300

PRIORITIZING VULNERABILITIES

Figure 6. TI & Internal Scores Drive Priority



How does your organization prioritize vulnerabilities for remediation? Select all that apply

Base: 300

Figure 7. Structured Models Most Effective

	% Effective
VulnCheck KEV	98%
EPSS	96%
CISA KEV	96%
Threat intelligence feeds	96%
Asset information	95%
Considering compesating controls	95%
Vendor scores	94%
Open source incident reports	93%
Internal priority score	93%
CVSS	91%
First-come, first-served	85%

How effective are your methods of priorization?

Base: varies* (55-142)

**Asked to those who selected each option at Q4*

When prioritizing vulnerabilities, threat intelligence feeds (47%) and internal priority scores (46%) are the most commonly used methods (Figure 6). However, when organizations assess the effectiveness of different prioritization approaches, structured models such as VulnCheck KEV, EPSS, and CISA KEV rank the highest (98%, 96%, and 96%, respectively) (Figure 7). Despite their superior effectiveness, these structured approaches remain underutilized, with EPSS and VulnCheck KEV being used by only 18% of respondents. This disconnect between commonly used methods and their perceived effectiveness suggests a gap in adoption of data-driven, risk-based prioritization strategies. This could be due to implementation challenges, lack of awareness or expertise, or a belief that these methods are not applicable to their specific environment.

A concerning finding is that 22% of organizations still rely on a first come, first served approach. While relatively low on the list, this random and unstructured method is ranked as the least effective, yet is almost as commonly used as CISA KEV (23%) – a trusted industry database that provides high-confidence intelligence on vulnerabilities actively exploited in attacks. The fact that an arbitrary method like “first come, first served” is used nearly as often as a proven, risk-based approach highlights a fundamental misalignment in prioritization strategies, and the need for greater education about best-in-class prioritization approaches.

This data also provides important context for broader vulnerability management challenges. The third biggest challenge in managing vulnerabilities is difficulty prioritizing vulnerabilities (see Figure 5), which aligns with the low adoption of structured prioritization models and the continued reliance on unstructured methods. The lack of a fully risk-based approach contributes to inconsistencies in prioritization, making it harder for security teams to provide clear direction on remediation. This, in turn, could explain why organizations struggle to make findings actionable and why cross-team collaboration remains a significant pain point.

The misalignment between prioritization method usage and effectiveness presents an opportunity for security teams. By shifting toward structured, data-driven approaches that have been proven to improve remediation outcomes, organizations can streamline their vulnerability management processes, enhance risk-based decision-making, and accelerate remediation efforts.

Challenges & Efficiency

LEVEL OF NOISE IN VULNERABILITY SCANNING

Figure 8. Noise Remains A Problem

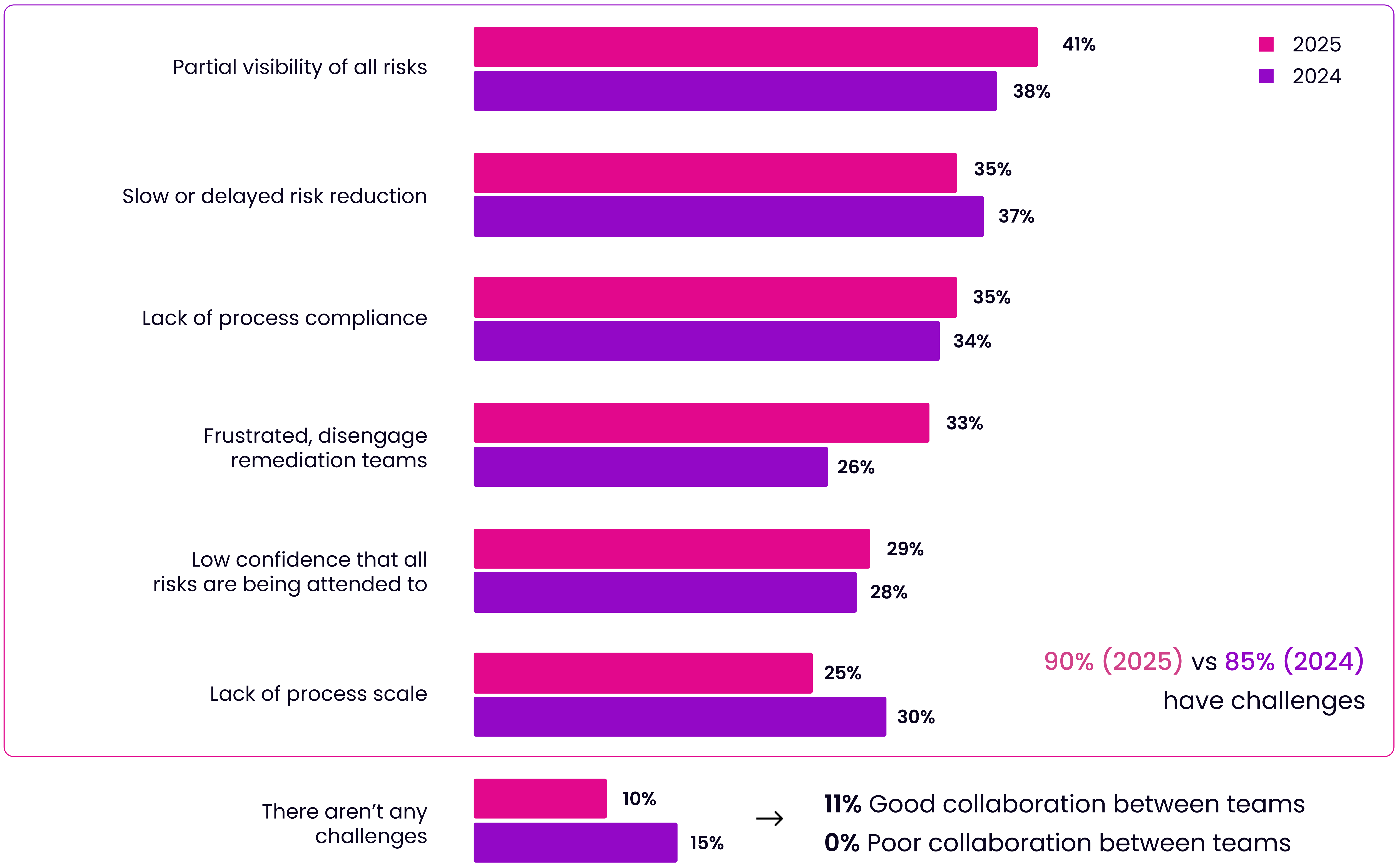
	Very High	High	Moderate	Low	Very Low
2025	**15%**	**35%**	**39%**	**9%**	**2%**
2024	**23%**	**28%**	**38%**	**10%**	**1%**

50% (2025) vs 51% (2024) High

How would you rate the level of noise generated by your current risk and vulnerability scanning tools? Base: 300

Excessive noise from vulnerability scanning tools remains a persistent challenge for security teams. Although fewer report very high levels of noise in 2025 compared to 2024 (15% vs 23%), overall, 50% of IT security decision-makers report high levels of noise – a figure nearly unchanged from 2024's 51% (Figure 8). This consistency suggests that, despite some advancements, more can be done to reduce alert fatigue and improve signal-to-noise ratios.

Figure 9. Noise Has Consequences



90% (2025) vs 85% (2024) have challenges

11% Good collaboration between teams

0% Poor collaboration between teams

Are there any challenges in managing the noise generated by vulnerability scanning tools? Select up to three

Base: 300

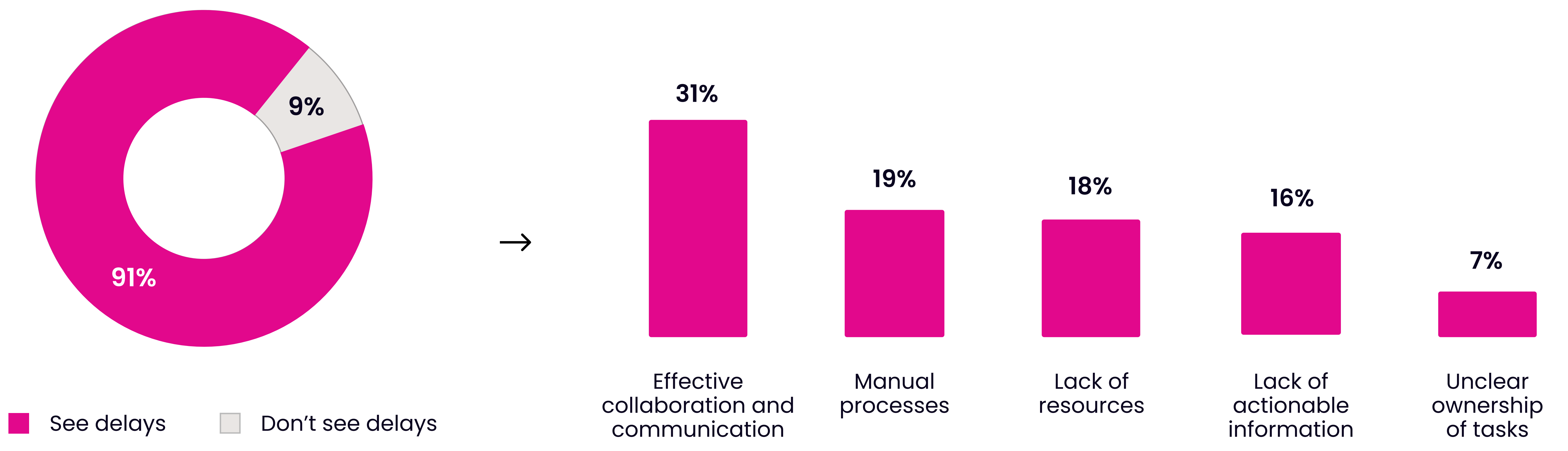
The issue is further underscored by the fact that 90% of organizations report challenges in managing noise, an increase of 5% from 2024 (Figure 9). This rise suggests that existing filtering and prioritization methods are not keeping pace with the ever-growing volume of security findings, reinforcing earlier data that highlight prioritization as a major vulnerability management challenge. Partial visibility of risks (41%), along with slow risk reduction and lack of process compliance (both 35%), were cited as the top three consequences of excessive noise. This data highlights that noise isn't just an inconvenience; it's a direct barrier to effective decision-making and timely and reliable remediation. These impacts likely explain why excessive noise ranks as the fourth biggest challenge in vulnerability management (see Figure 5).

Interestingly, organizations with strong cross-team collaboration are less likely to struggle with noise-related issues. An 11% of organizations with good collaboration report no noise-related challenges, whereas none (0%) of those with poor collaboration were free of noise challenges. This correlation reinforces the idea that effective teamwork and streamlined communication help teams respond to alerts more efficiently.

The data in Figures 8 and 9 point to the need for security teams to implement stronger noise-filtering mechanisms, improve collaboration across functions, and develop clearer workflows for prioritizing alerts. Without these improvements, organizations will continue to struggle with alert fatigue, slowing down vulnerability management efforts and increasing security risks.

VULNERABILITY REMEDIATION EFFICIENCY

Figure 10. Collaboration & Communication Are Critical



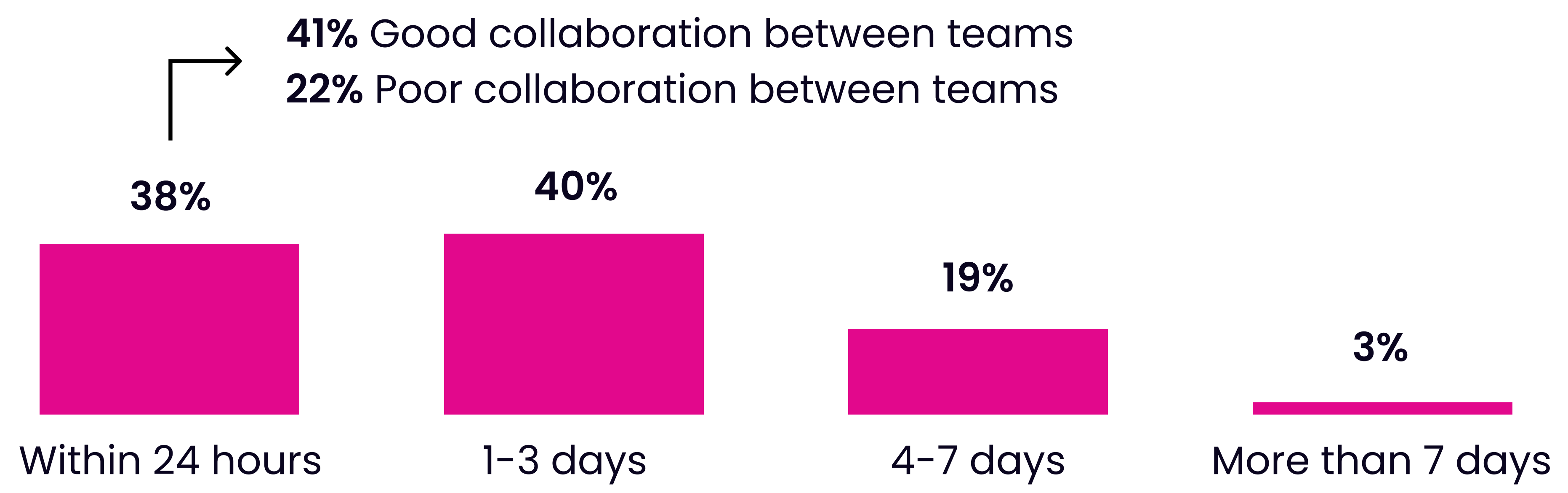
What is the primary cause of delays in vulnerability remediation in your organization? Select one

Base: 300

Delays in remediation remain a widespread issue, with 91% of organizations experiencing setbacks in addressing vulnerabilities (Figure 10). This indicates a significant gap in operational efficiency, as teams struggle to coordinate and execute remediation efforts effectively; the leading cause of these delays is collaboration and communication challenges (31%), highlighting the direct impact of poor cross-team coordination on remediation efficiency. Without clear communication and structured workflows, confusion over ownership, slow decision-making, and prolonged security exposure become inevitable. Given that poor collaboration is also identified as one of the top challenges in vulnerability management (see Figure 5), it's clear that breakdowns in communication have a considerable effect on the entire vulnerability management lifecycle.

Beyond collaboration issues, manual processes (19%) and lack of resources (18%) were cited as the second and third biggest causes of remediation delays. These findings suggest that delays could be improved through automation and better resource allocation.

Figure 11. To Remediate Faster, Collaborate



Noise generated	Mean
High	3 days
Moderate	2 days
Low	1 day

Overall mean: **2 days**

What do you believe is the actual average response time for addressing critical vulnerabilities? Select one

Base: 300

Figure 11 reveals that organizations report that critical vulnerabilities take an average of two days to remediate, but for 1 in 5 organizations, it takes four or more days. These prolonged timelines are a direct consequence of the inefficiencies outlined in Figure 10.

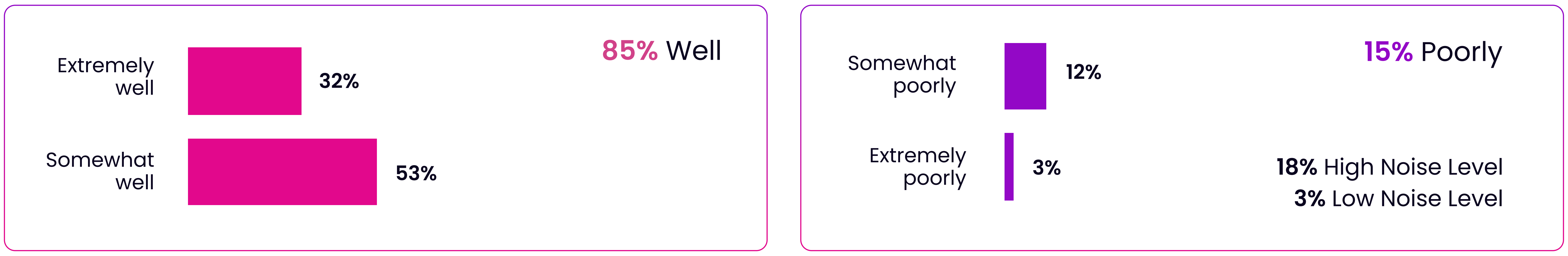
Supporting the idea that collaboration efficacy correlates with remediation speed, Figure 11 highlights that those with good cross-team collaboration are significantly more likely to respond to critical vulnerabilities within 24 hours (41%) than those with poor cross-team collaboration (11%). Another key factor affecting remediation speed is noise from scanning tools. Organizations that experience high levels of noise take an average of two additional days to remediate critical vulnerabilities compared to those with low noise levels. This reinforces the findings in Figure 9 that show that excessive noise is not just an issue of alert fatigue – it has a measurable impact on remediation speed. Without improvements in noise management, remediation workflows will remain slow, leaving organizations exposed to threats for longer periods and increasing the risk of exploitation.

Together, the findings in Figures 10 and 11 emphasize that remediation efficiency requires improvements in communication, automation, and prioritization. Organizations that fail to address these operational inefficiencies will continue to struggle with delays, exposing themselves to prolonged security risks.

Cross-Team Collaboration

THE STATE OF COLLABORATION

Figure 12. Reduce Noise To Collaborate Better



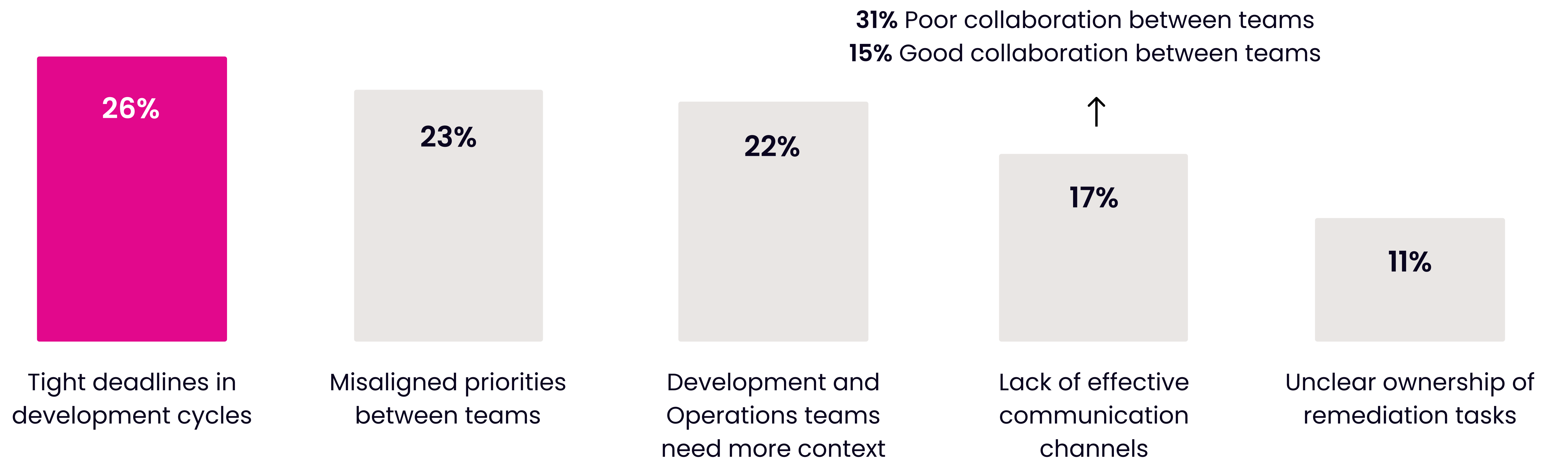
On a scale from extremely poorly to extremely well, how well does your security team collaborate with development and operations teams on remediation? Select one

Base: 300

Most organizations perceive their collaboration between security, development, and operations teams as strong, with 85% stating they collaborate well on remediation (Figure 12). However, Figure 10 suggests that collaboration breakdowns remain a top cause of remediation delays. This indicates that while organizations may rate their collaboration positively, inefficiencies still persist, affecting their ability to execute remediation effectively and at speed.

Organizations with high noise levels are significantly more likely to rate their collaboration as poor (18%) compared to those with low noise levels (3%), underscoring the impact of noise-related challenges.

Figure 13. Tight Deadlines Increase Friction



What is the most significant barrier to effective collaboration between security, development, and operations teams? Select one

Base: 300

When examining barriers to collaboration, the top-ranked challenges reveal long-standing friction points between security and engineering teams. Tight development deadlines and misaligned priorities were cited as the biggest obstacles (Figure 13), highlighting the ongoing tension between speed and security. Closely following these challenges is the lack of sufficient security context for development and operations teams, making it difficult for them to determine which vulnerabilities require immediate attention. This finding aligns with Figure 5, where the number one challenge in vulnerability management was making security findings actionable.

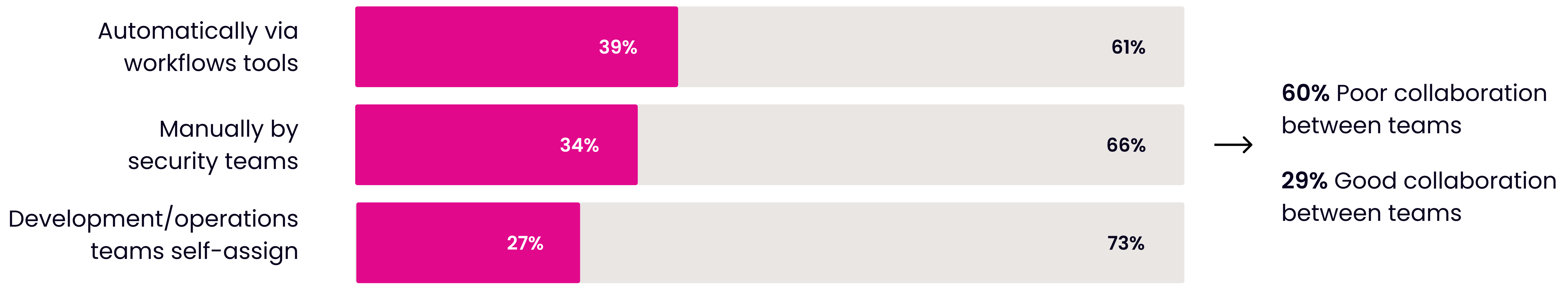
Another critical factor is communication – 17% of organizations cite ineffective communication channels as their biggest barrier to collaboration, but this number rises to 31% among organizations that already struggle with collaboration. Conversely, for those with strong collaboration, only 15% see a lack of effective communication channels as a major barrier.

> This implied link between the presence of effective communication channels and the strength of collaboration reinforces the need for dedicated and structured communication channels rather than ad hoc or fragmented discussions.

Ultimately, collaboration challenges stem largely from structural and workflow misalignment, as well as a lack of actionable security context. To improve collaboration, organizations need to bridge the gap between security and development priorities, provide development teams with clearer security insights, and establish structured communication channels that foster alignment and efficiency.

WORKFLOW GAPS

Figure 14. Manual Workflows Bad For Collaboration

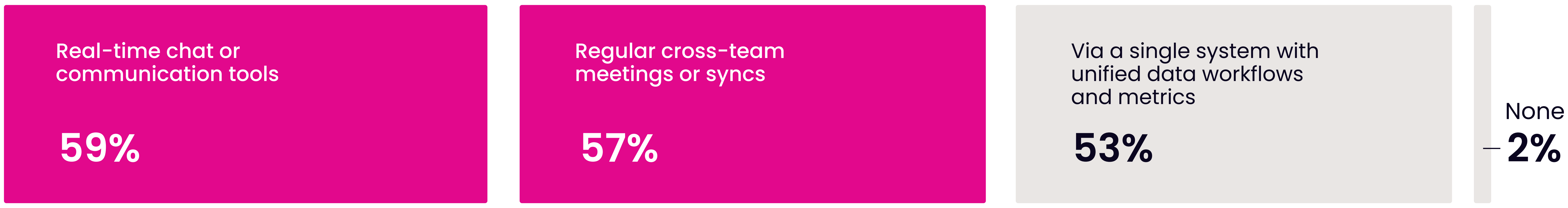


How are remediation tasks typically assigned to development or operations teams? Select one — Base: 300

A key aspect of collaboration is how remediation tasks are assigned within organizations. Responses were fairly evenly distributed, with the most common method reported being automated assignment via workflow tools (39%). However, 34% of organizations still rely on manual task assignment, while 27% leave it to development and operations teams to self-assign (Figure 14). This means that despite automation being the most common approach, the majority of organizations (61%) still depend on inefficient and unstructured workflows, which could explain why misaligned priorities and lack of security context were ranked as major collaboration barriers (see Figure 13). Given that manual processes were ranked among the top causes of remediation delays (see Figure 10), the fact that over a third of organizations still manually assign remediation tasks indicates a major operational gap that slows remediation efforts and reduces accountability. Additionally, self-assignment suggests a lack of alignment and unclear ownership, leading to inconsistencies in remediation and inefficient cross-team collaboration.

The link between manual processes and poor collaboration is particularly evident; for organizations with poor collaboration, manual task assignment jumps to 60%, reinforcing the connection between collaboration and operational efficiency.

Figure 15. Ad-Hoc Communications Dominate

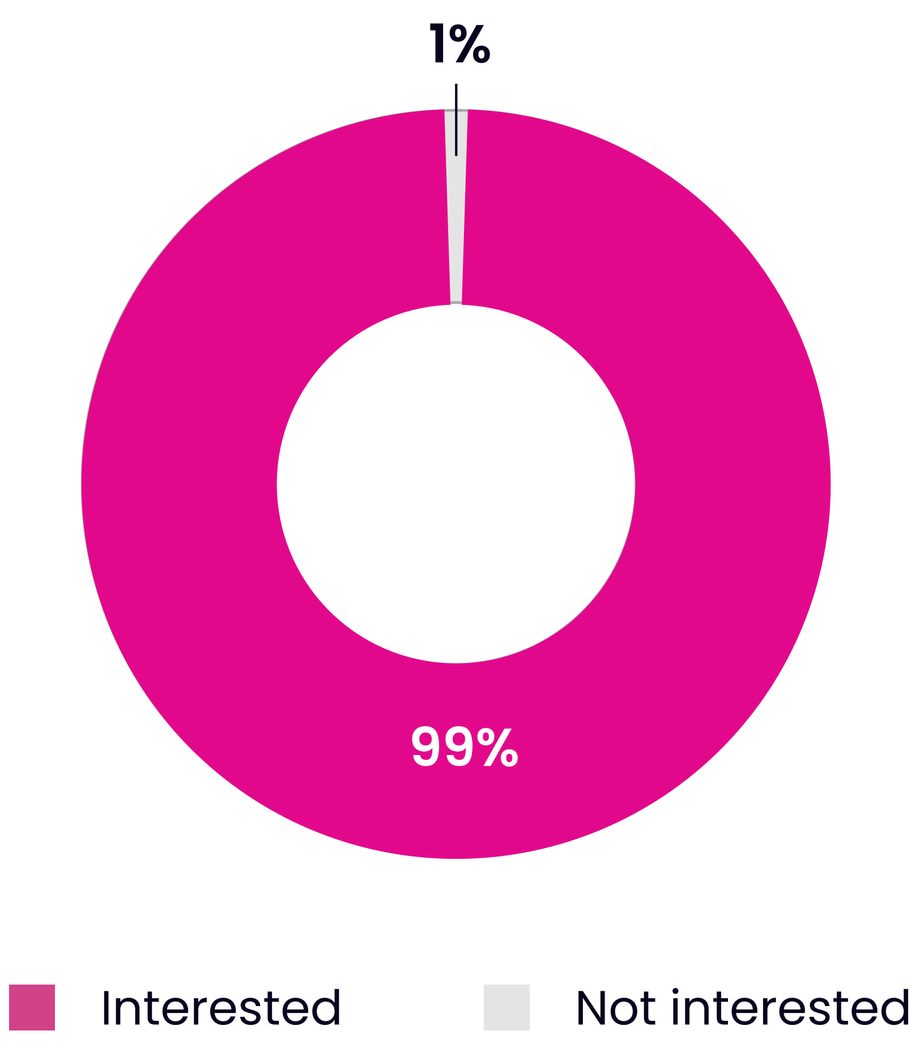


How does your organization facilitate collaboration on remediation tasks? Select all that apply — Base: 300

When examining how organizations facilitate collaboration on remediation tasks, real-time chat (59%) and regular meetings (57%) were the most common methods (Figure 15). However, while these ad-hoc approaches support communication, they lack the structure and clarity needed for efficient remediation. And, despite the adoption of unified systems that provide structured workflows, nearly half of organizations still lack one, meaning their remediation efforts are likely fragmented across multiple tools and communication channels.

Encouragingly, there is strong interest in adopting centralized collaboration solutions. Among organizations that do not currently use a single system for remediation collaboration, 99% expressed interest in implementing one (Figure 16). This overwhelming demand suggests that organizations recognize the inefficiencies in their current methods and see value in a structured, centralized approach. A unified system could help align priorities, reduce miscommunication, and streamline remediation workflows, ultimately improving both collaboration and remediation efficiency.

Figure 16. Unified Platforms Wanted



To what extent would you be interested in a single system with unified data, workflows and metric? Select one — Base: 300

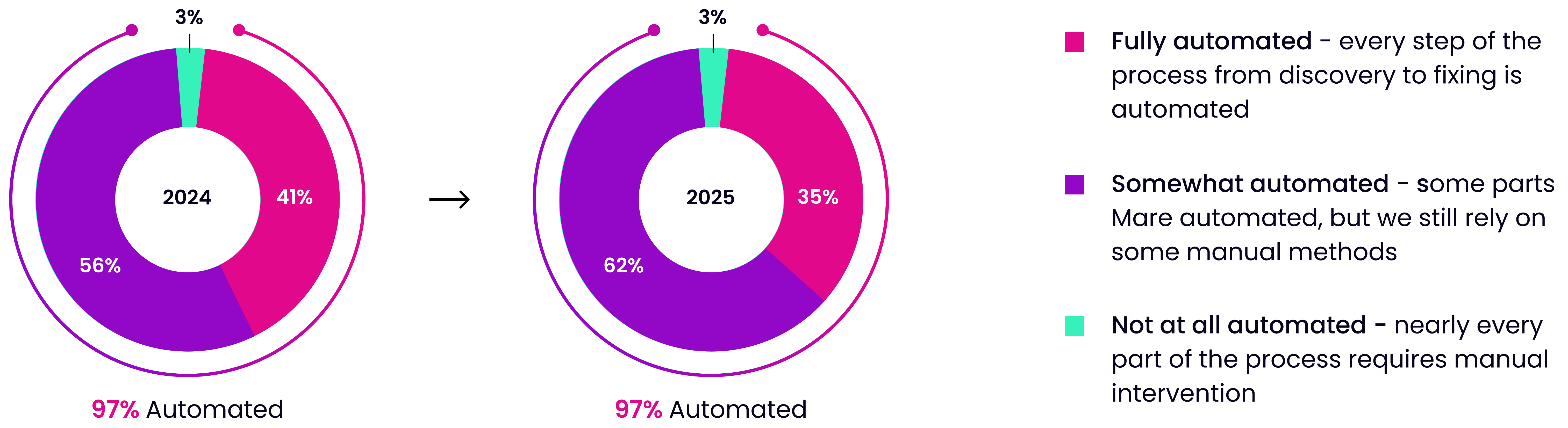
**Asked only to those who did not choose 'via a single system with unified data, workflows and metrics' at Q17*

Automation and AI Adoption

AUTOMATION IN VULNERABILITY MANAGEMENT

Automation is now a standard part of vulnerability management, with 97% of organizations reporting some level of automation in their processes (Figure 17). However, despite this widespread adoption, fewer organizations report having fully automated processes - dropping from 41% in 2024 to 35% in 2025. This decline suggests that while automation remains integral, many organizations struggle to sustain fully automated workflows, possibly due to integration challenges, limitations in automation tools, or the increasing complexity of security environments that require human oversight.

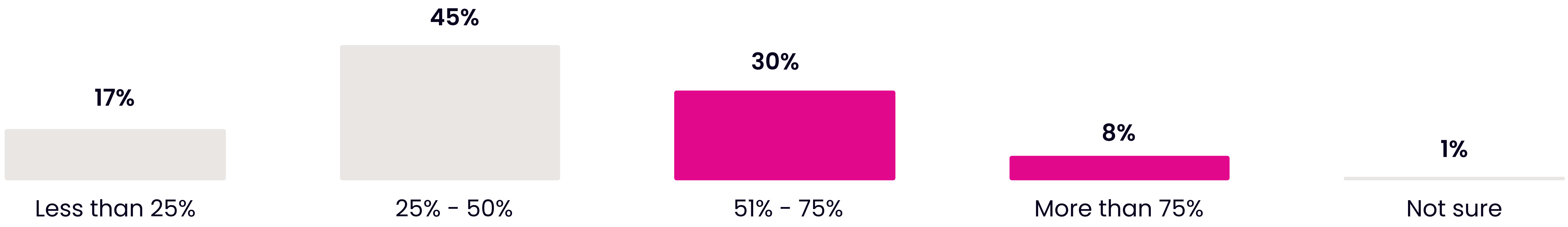
Figure 17. Full Workflow Automation Is Elusive



To what extent is your vulnerability management process automated? Select one — Base: 300

However, even with high adoption rates, manual intervention remains a significant factor in vulnerability management. Alarmingly, nearly 40% say more than half of their vulnerability management process is manual (Figure 18). Given that manual processes are a leading cause of remediation delays (see Figure 10), organizations need to move beyond basic automation adoption and focus on optimizing and expanding automation to eliminate inefficiencies, reduce bottlenecks, and accelerate remediation speed.

Figure 18. Manual Burden Remains High



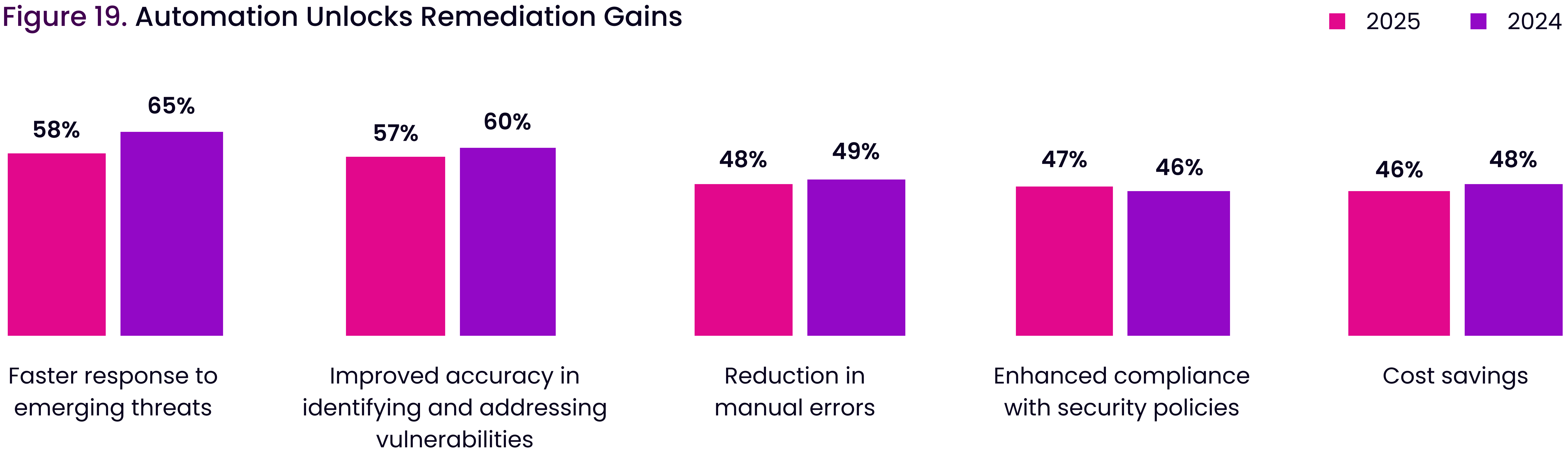
What percentage of your vulnerability management process is spent on manual tasks? Select one

Base: 300

BENEFITS OF AUTOMATION IN VULNERABILITY MANAGEMENT

The benefits of automation in vulnerability management are clear, with faster response times being the most commonly cited advantage (Figure 19). This reinforces a correlation between automation and improved remediation efficiency. Alongside speed, improved accuracy (57%) and reduction in manual errors (48%) are also reported as key benefits, highlighting automation's role in enhancing consistency and reliability in security operations. Not only does automation help organizations move faster, but it also helps them work smarter, minimizing the inconsistencies and risks that come with manual workflows.

Figure 19. Automation Unlocks Remediation Gains



What benefits, out of the following, have you observed from the automation of vulnerability management tasks? Select all that apply

Base: 292* / 291*

Asked to those who have automated vulnerability management processes

However, despite these advantages, manual intervention remains prevalent (see Figure 18), preventing organizations from fully realizing automation's potential. If organizations were to expand their automation efforts, they would likely see even greater efficiency gains and risk reduction in their remediation processes. The gap between automation adoption and full automation maturity suggests that organizations still have work to do in maximizing the impact of their automation investments.

FUTURE OF AI IN VULNERABILITY MANAGEMENT

Figure 20. Optimism for Automated Remediation

	Automated remediation	Vulnerability assessment	Vulnerability prioritization	Remediation planning
2025	**30%**	**28%**	**26%**	**16%**
2024	**22%**	**38%**	**30%**	**10%**

What aspect of vulnerability management do you think would most benefit from AI integration? Select one

Base: 300

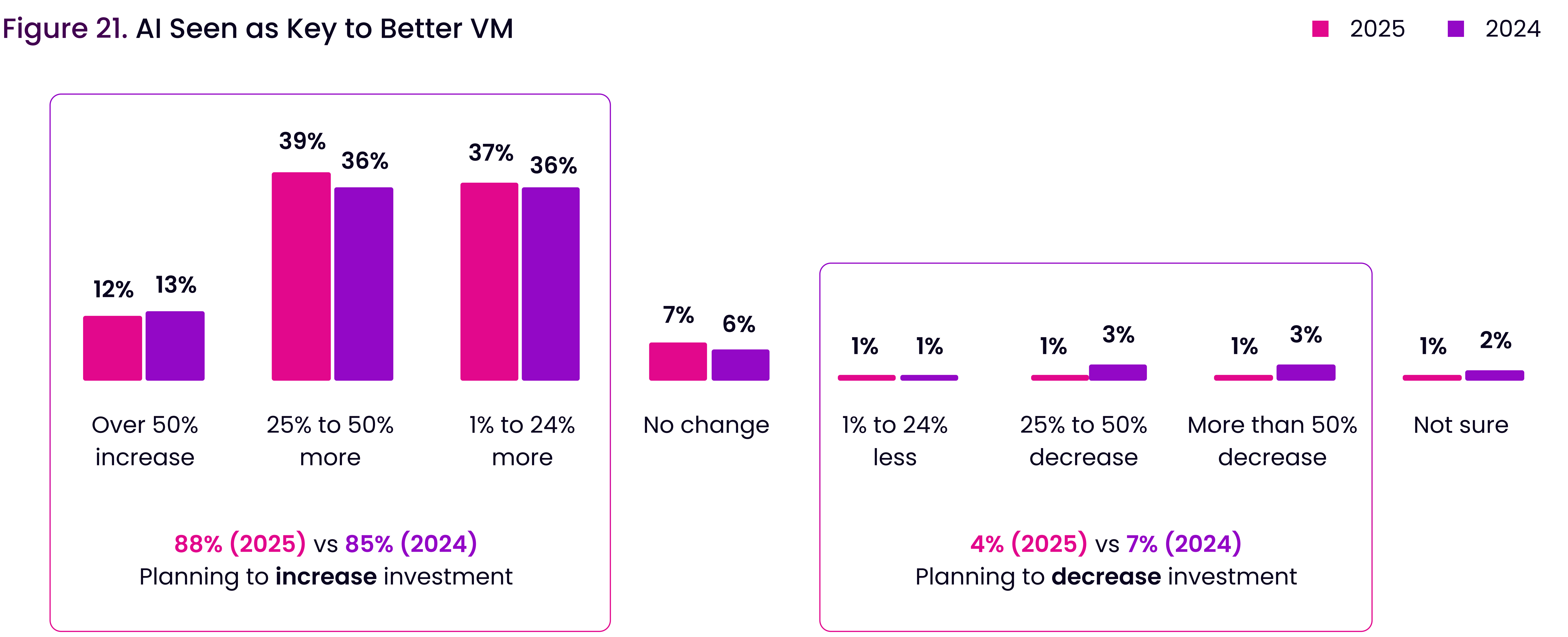
When asked which aspect of vulnerability management would most benefit from AI integration, 30% of organizations pointed to automated remediation, making it the top-ranked use case – up from third place in 2024 (Figure 20). The increase from 22% to 30% year-over-year signals a growing recognition that AI can help move beyond just identifying vulnerabilities to actually improving remediation workflows and execution. This aligns with earlier findings that highlight operational inefficiencies in remediation, suggesting that organizations acknowledge the efficiency gap and see AI as a key solution.

While vulnerability assessment remains the second most common AI use case, it has seen a notable decline since 2024. This shift suggests that organizations may have already made progress in automating assessments or that they recognize greater challenges elsewhere, such as remediation execution. It also indicates a potential realization that AI-driven vulnerability assessment alone does not necessarily translate into improved remediation outcomes.

Another area gaining traction is AI-powered remediation planning, which has increased from 10% in 2024 to 16% in 2025. This suggests that organizations are increasingly recognizing the need for structured, efficient remediation processes.

Ultimately, this year's data reflects a fundamental shift in how organizations view AI's role in vulnerability management. Instead of solely focusing on detection and assessment, they are increasingly looking to AI to streamline remediation workflows. This shift aligns with previously discussed findings that highlight inefficiencies in vulnerability management and remediation, reinforcing the strong correlation between where organizations struggle and where they see AI as having the most potential to drive improvements.

Figure 21. AI Seen as Key to Better VM



How much is your organization planning to increase or decrease investment in AI technologies in the next 5 years? Select one

Base: 300

Looking ahead, 88% of organizations plan to increase their AI investments over the next five years, up from 85% in 2024 (Figure 21). While this year-over-year increase is not drastic, it reflects growing confidence in AI's value in addressing persistent security challenges. Overall, the fact that a majority of organizations are planning to increase their AI investments indicates widespread recognition that automation and intelligent systems are essential for improving vulnerability management and are willing to expand their investments accordingly.

Conclusion and Next Steps

The data highlights a pressing need for more efficient, structured, and data-driven approaches to vulnerability management. To improve remediation speed and reduce security risk, organizations should consider the following next steps:

ADOPT RISK-BASED PRIORITIZATION MODELS

Move away from reactive approaches and combine proven, structured frameworks like EPSS and CISA KEV with organization-specific business context to prioritize vulnerabilities effectively.

REDUCE NOISE AND ALERT FATIGUE

Implement smarter filtering mechanisms to focus on high-risk vulnerabilities and avoid overwhelming security teams.

STRENGTHEN CROSS-TEAM COLLABORATION

Establish clear workflows, ownership structures, and dedicated communication channels to improve alignment between security and development teams.

SCALE AUTOMATION EFFORTS

Expand automation beyond basic tasks to eliminate bottlenecks, improve efficiency, and reduce manual workload in remediation.

INVEST IN AI-DRIVEN REMEDIATION SUPPORT

As teams shift from identification to execution, AI-powered remediation tools can help streamline workflows and improve response times.

As organizations scale security efforts in 2025, those that embrace automation, collaboration, and structured risk-based approaches will be better positioned to manage vulnerabilities efficiently, reduce exposure time, and enhance overall security resilience.

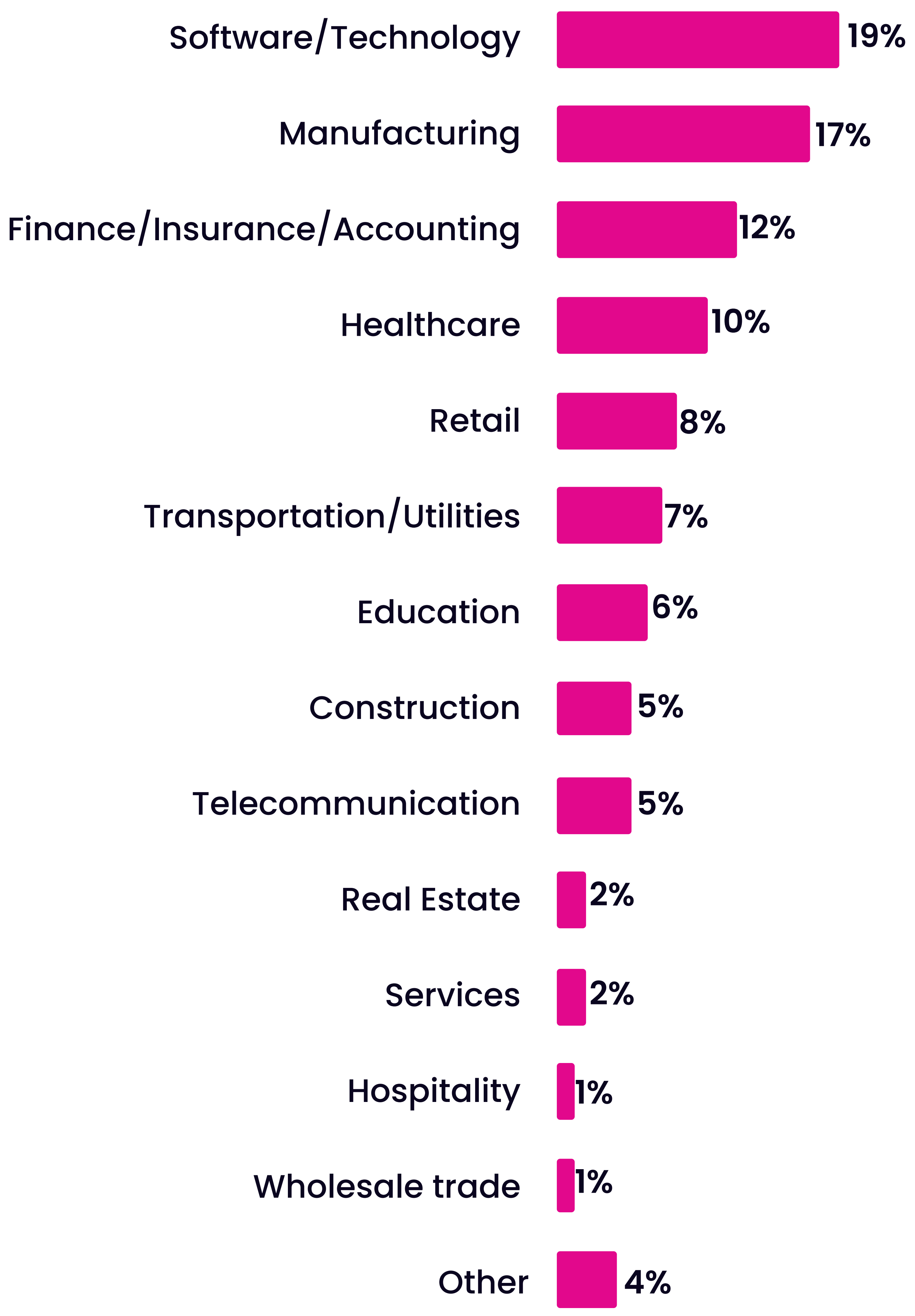
Methodology and Respondents

This research was a joint effort between Seemplicity and Sapio Research. Seemplicity revolutionizes vulnerability and exposure management with its AI-powered Remediation Operations (RemOps) platform. By automating and streamlining remediation processes, Seemplicity consolidates findings, accelerates risk reduction, and delivers tailored remediation plans for security, IT, and DevOps teams. Trusted by Fortune 500 companies, the platform enables organizations to enhance operational resilience and build scalable security programs. Sapio Research is a full-service research agency based in the UK that specializes in B2B and Technology market research.

The survey was created by Seemplicity, with Sapio Research consulting on its development. Sapio Research carried out the survey online, recruiting a select group from their qualified database. 300 responses were collected from IT and Security decision makers of midsize and large US-based organizations across various industries.

Sapio Reseach was responsible for all survey administration and data collection; Seemplicity was responsible for data analysis.

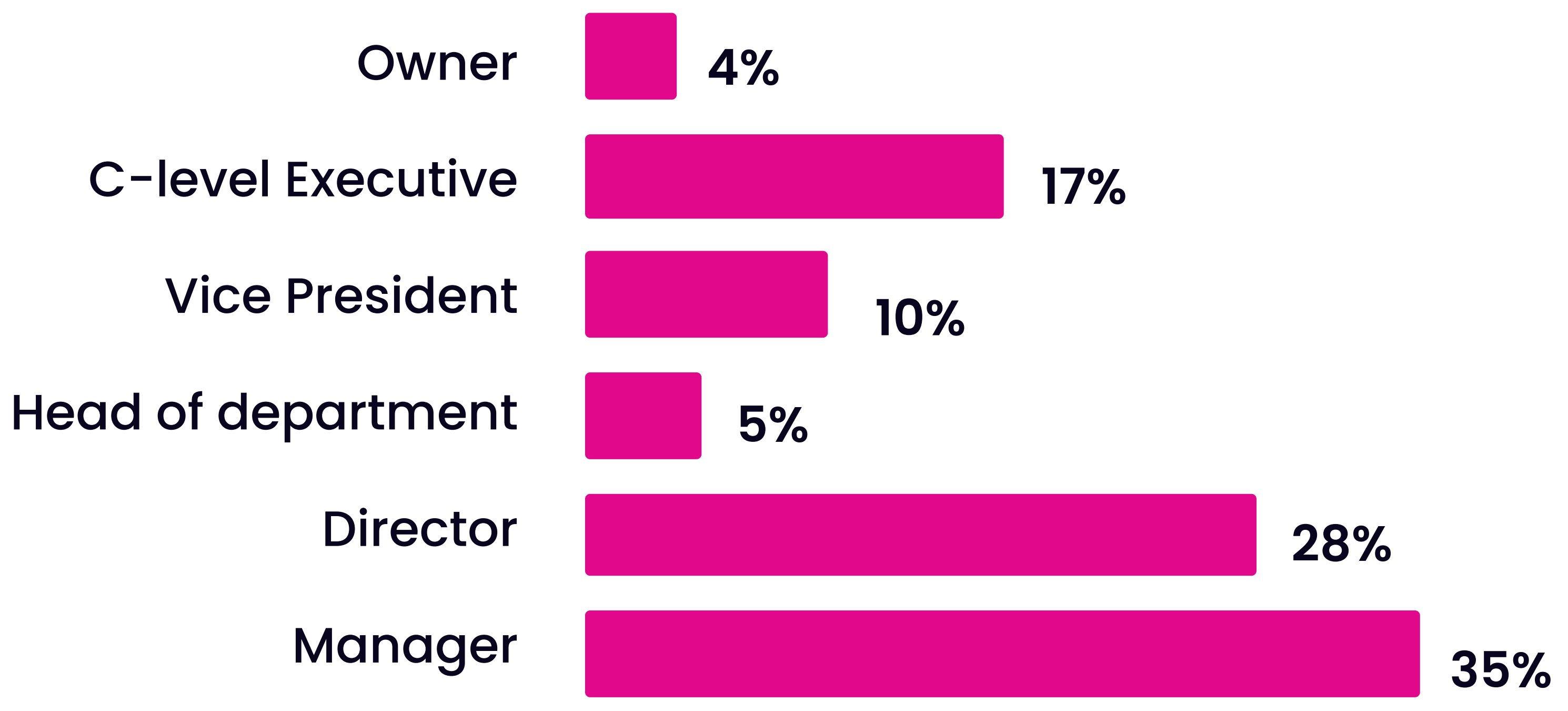
Industry



S2. Which of the following categories best describes the industry you work for? Select one

Base: 300

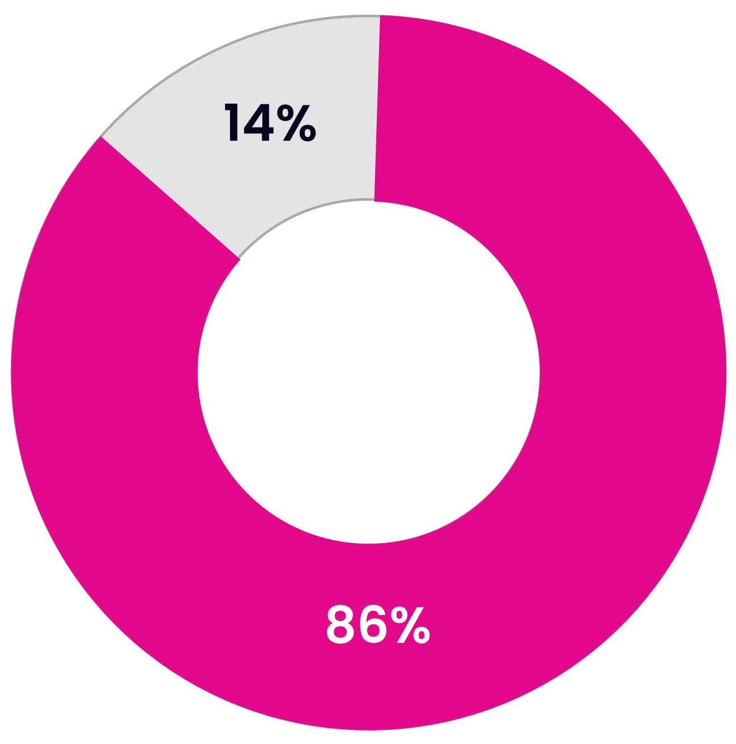
Job Role



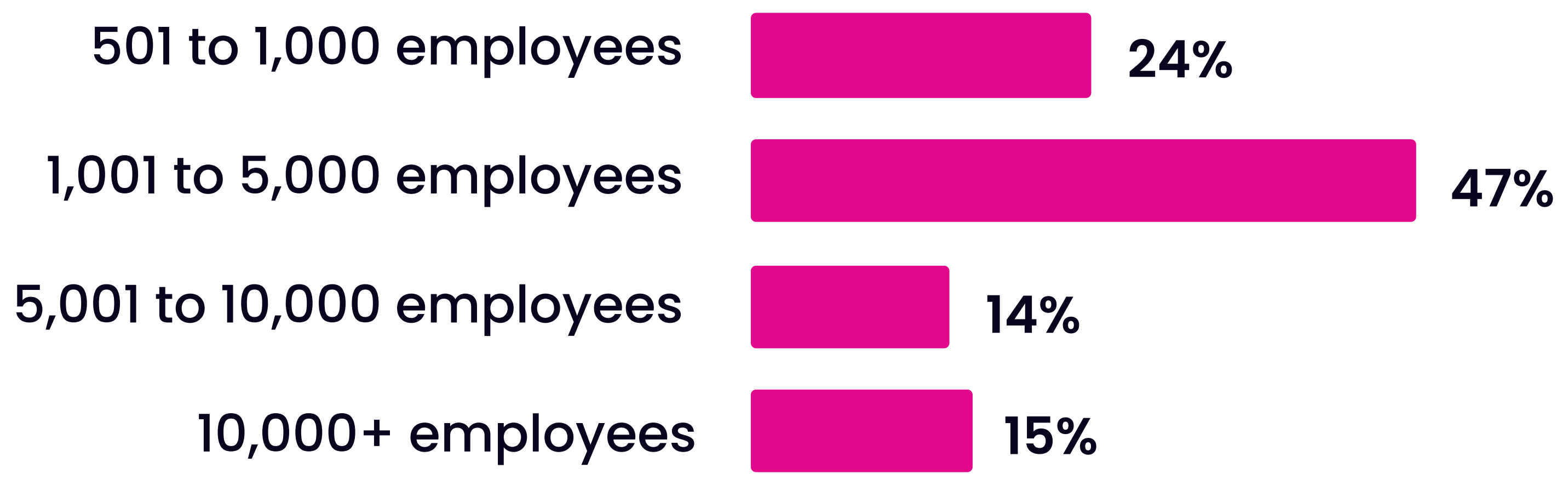
Job Function

■ IT

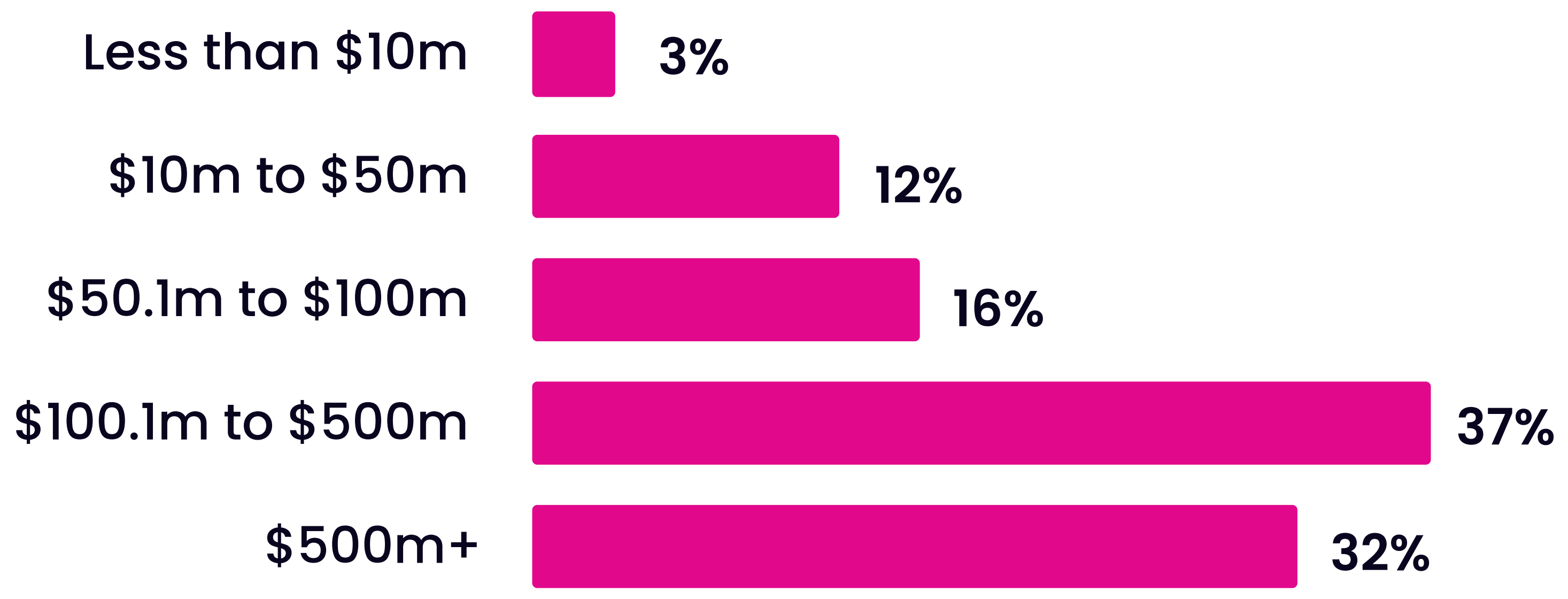
□ Cybersecurity



Company Size



Annual Revenue



Influence Over Cybersecurity Purchases

■ I alone make the cybersecurity purchase decisions

■ I have a lot of influence on the cybersecurity purchase decisions

□ I have some influence on the cybersecurity purchase decisions