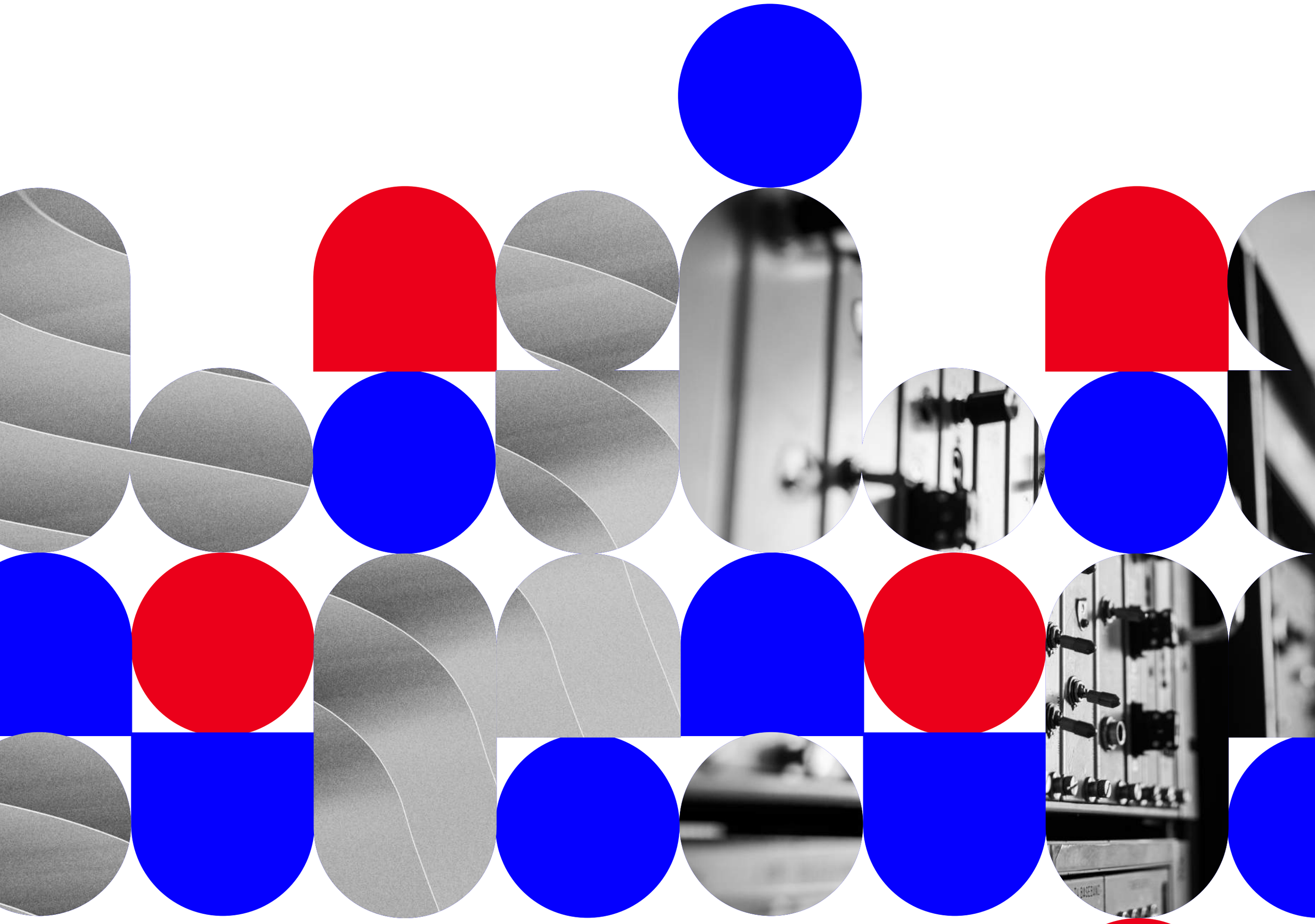
Recorded Future®

RESEARCH CONTENT 2025



2025 State of Threat Intelligence

Contents

Introduction.

Every year, enterprise organizations increasingly rely on threat intelligence to build proactive defenses against emerging cyberthreats. In 2025, this trend reaches new heights as state-sponsored threats, cybercrime, and geopolitical issues escalate, creating more substantial opportunities for business disruption.

Additionally, AI has lowered the barrier to entry for threat actors, enabling more bad actors to scale attacks in terms of both volume and sophistication. To stay ahead of these issues and prevent their security teams from burning out, organizations need the ability to find the signal in the noise.

As a force multiplier, threat intelligence enhances existing security tools, informs strategic planning, and mitigates risk to the business's assets and reputation. Threat intelligence is top of mind for many enterprise security teams as they work to advance their organization's threat intelligence maturity, consider vendor investments and consolidations, and plan how to allocate their cybersecurity budgets.

This report aims to uncover the current state of threat intelligence. Incorporating data from 615 cybersecurity executives, managers, and practitioners, this report reveals enterprise organizations' use cases, challenges, and future investment plans.

The data is clear. Over the past year, threat intelligence has become more critical for enterprise cybersecurity. In 2025, organizations are more likely to have dedicated threat intelligence teams, allocate a larger percentage of their cybersecurity budget to threat intelligence, and consider their threat intelligence maturity level advanced.

> Enterprises are increasing threat intelligence spend as security shifts **from reactive defense to a holistic, intelligence-driven strategy.** Modern intelligence helps detect attacks sooner, prioritize critical risks, and respond faster—strengthening vulnerability management, incident response, and board-level risk decisions.
>
> *Rich LaTulip, North America Field CISO, Recorded Future*

Key Insights.

01.

76% of enterprise organizations invest $250,000 or more per year in threat intelligence. In 2026, 91% of organizations plan to increase this investment.

02.

68% use threat intelligence to enhance existing security tools and 43% use it to guide strategic security investments.

03.

65% of enterprise organizations say threat intelligence supports security technology purchasing decisions. 58% say it guides business risk assessment.

04.

Enterprise organizations' biggest challenges with threat intelligence are **determining credibility, setting up integrations, and managing information overload.**

05.

Half (51%) consider themselves less than advanced in terms of threat intelligence maturity. Yet 87% expect improved maturity in the next two years.

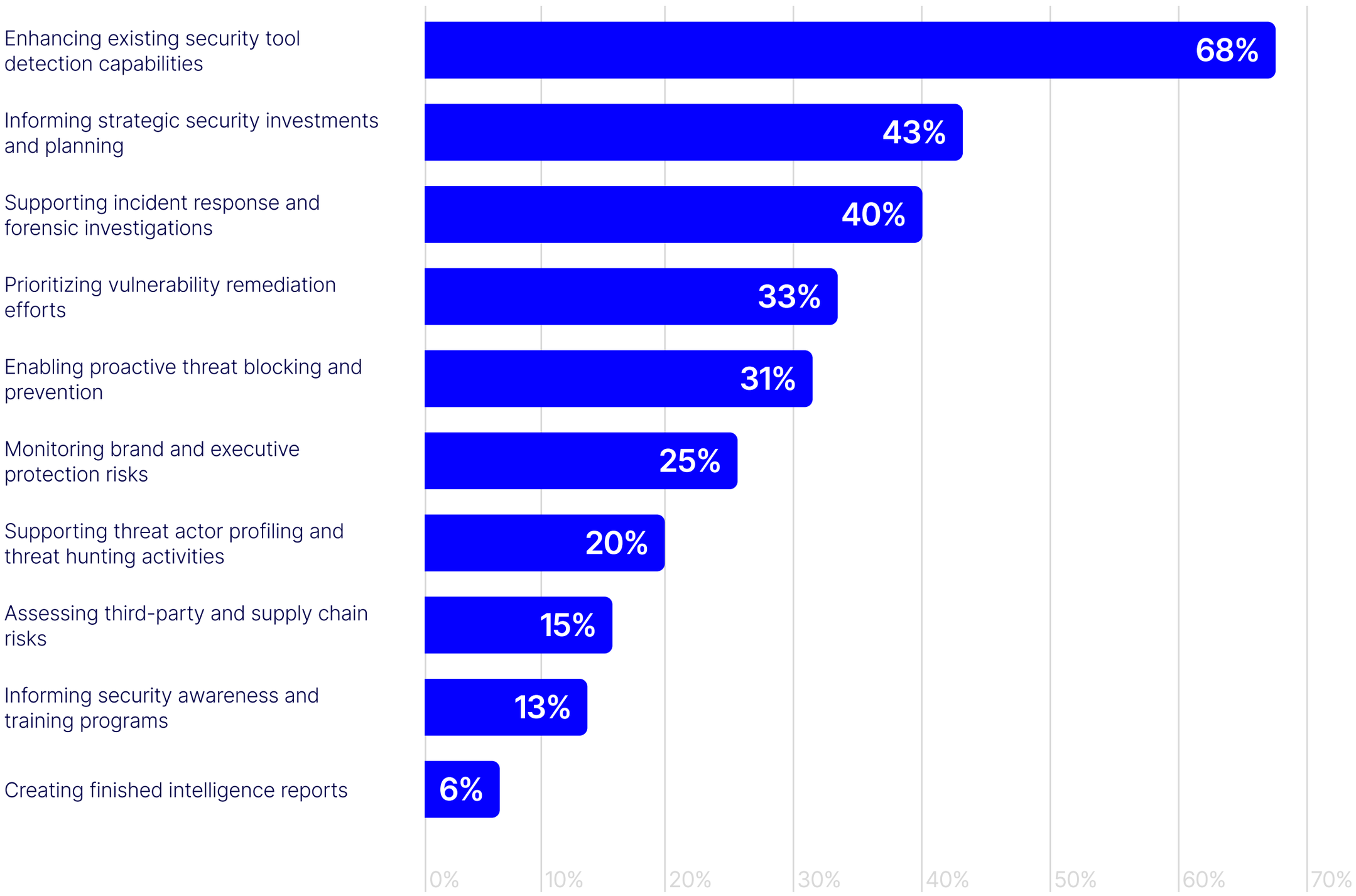
Threat intelligence usage and adoption

01

In 2025, strategic planning and investment has become one of the most common threat intelligence use cases for enterprise organizations. Forty-three percent of surveyed security professionals rely on this technology to inform strategic security investments and planning—a use case that wasn't previously on security teams' radar.

While most enterprise organizations report multiple use cases for threat intelligence, they primarily use it to enhance existing security tool detection capabilities (68%) and support incident response and forensic investigations (40%).

Which of the following best describes how your organization primarily uses threat intelligence?



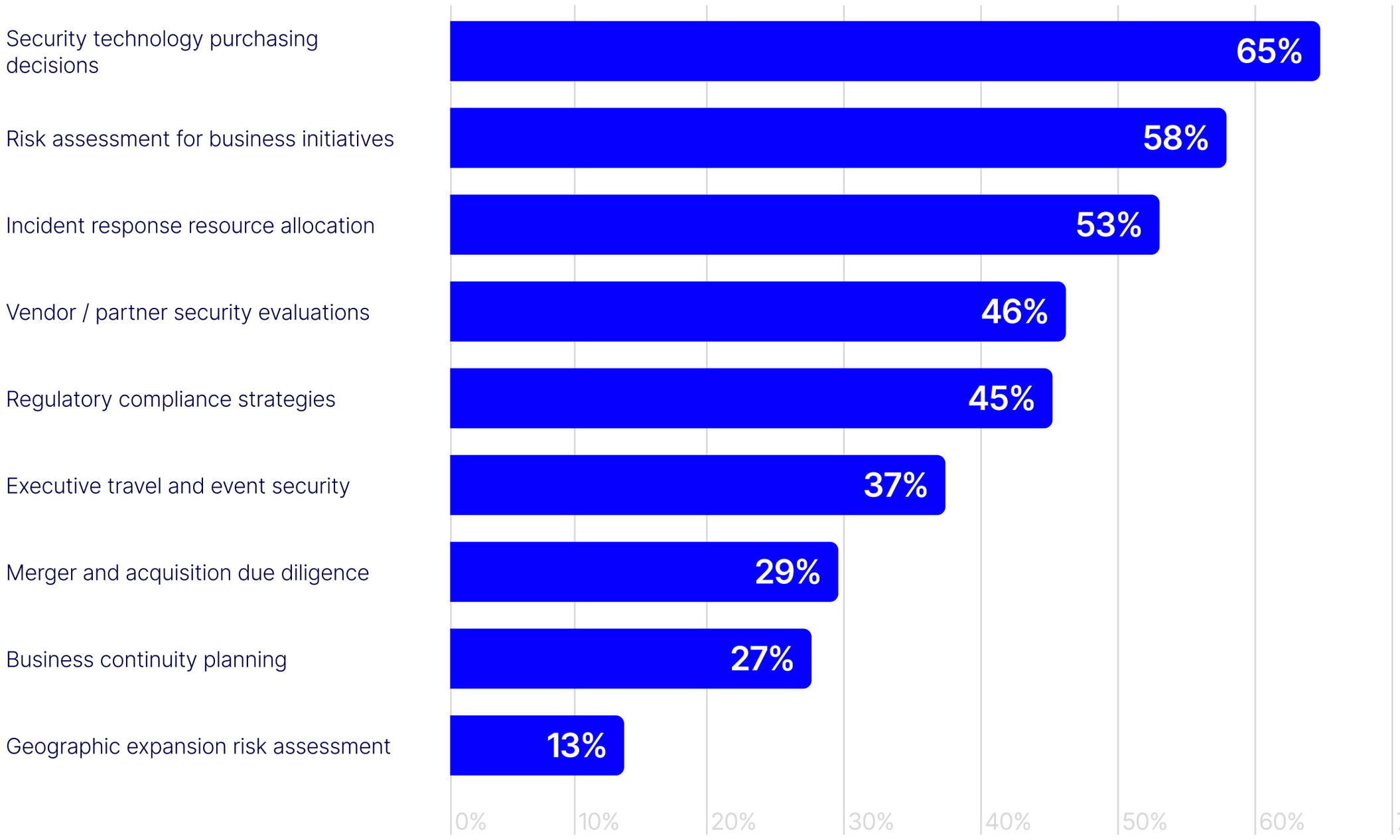
01

Recorded Future enabled our team to proactively identify and mitigate threats before the incidents occur. Leveraging its threat intelligence feed, we blocked potential phishing domains before they impacted our network, cutting down phishing incidents by 25% in one quarter.

Head of Threat Intelligence and Threat Hunting,
Large Enterprise Company

Most organizations use threat intelligence to guide business decisions related to purchasing, risk assessment, and resource allocation. Nearly two-thirds (65%) of surveyed security professionals say threat intelligence directly supports security technology purchasing decisions. Fifty-eight percent say it guides risk assessment for business initiatives, and 53% say it supports incident response resource allocation.

What business decisions has threat intelligence directly supported in your organization?



01

This indicates that threat intelligence has become a strategic component of cybersecurity rather than just a tactical tool. As a key part of so many critical business decisions, threat intelligence clearly garners substantial credibility and trust from executive leadership and finance teams.

> **When threat intelligence is part of board level conversations, it trickles down into many strategic decisions—where to invest, which risks to accept, and how to respond to regulation.**
>
> *Dan Elliott, Field CISO for APJ, Recorded Future*

As a result, nearly all enterprise organizations consider threat intelligence a critical investment. In fact, only 7% of surveyed security professionals have no threat intelligence team, which echoes findings from the 2024 State of Threat Intelligence report.

In 2025, more than three-quarters (83%) of surveyed security professionals report having a full-time team dedicated to threat intelligence, while 9% consider it a part-time responsibility. An additional 1% rely on an outsourced team for threat intelligence.

This reflects a slight shift toward dedicated full-time threat intelligence teams when compared to findings in the 2024 State of Threat Intelligence Report. In 2024, 80% of respondents had a full-time team, while 12% treated threat intelligence as a part-time responsibility.

01

Do you have a dedicated threat intelligence team?

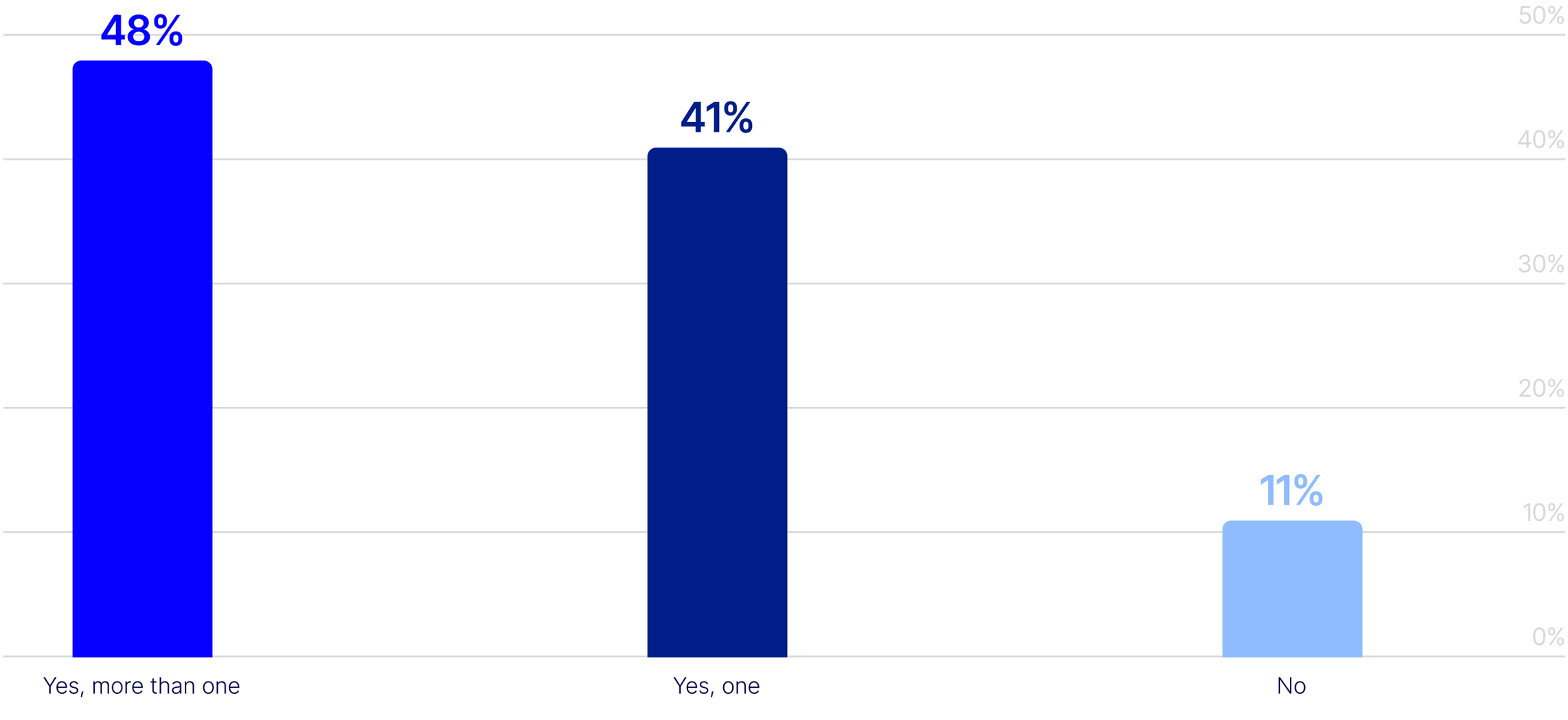
2025		2024	
83%	Yes	80%	Yes
7%	No	7%	No
9%	Part-time responsibility	12%	Part-time responsibility
1%	Outsourced	1%	Outsourced

It’s telling both that 83% of respondents now have a dedicated threat intelligence team and that this already high figure has increased year over year. Together, these takeaways indicate that more enterprise organizations are prioritizing cyber threat intelligence and allocating relevant resources.

Altogether, 89% of security professionals are currently paying for a threat intelligence vendor in 2025. Nearly half (48%) are paying for more than one vendor, while 41% are paying for only one.

01

Is your organization currently paying for a threat intelligence vendor?

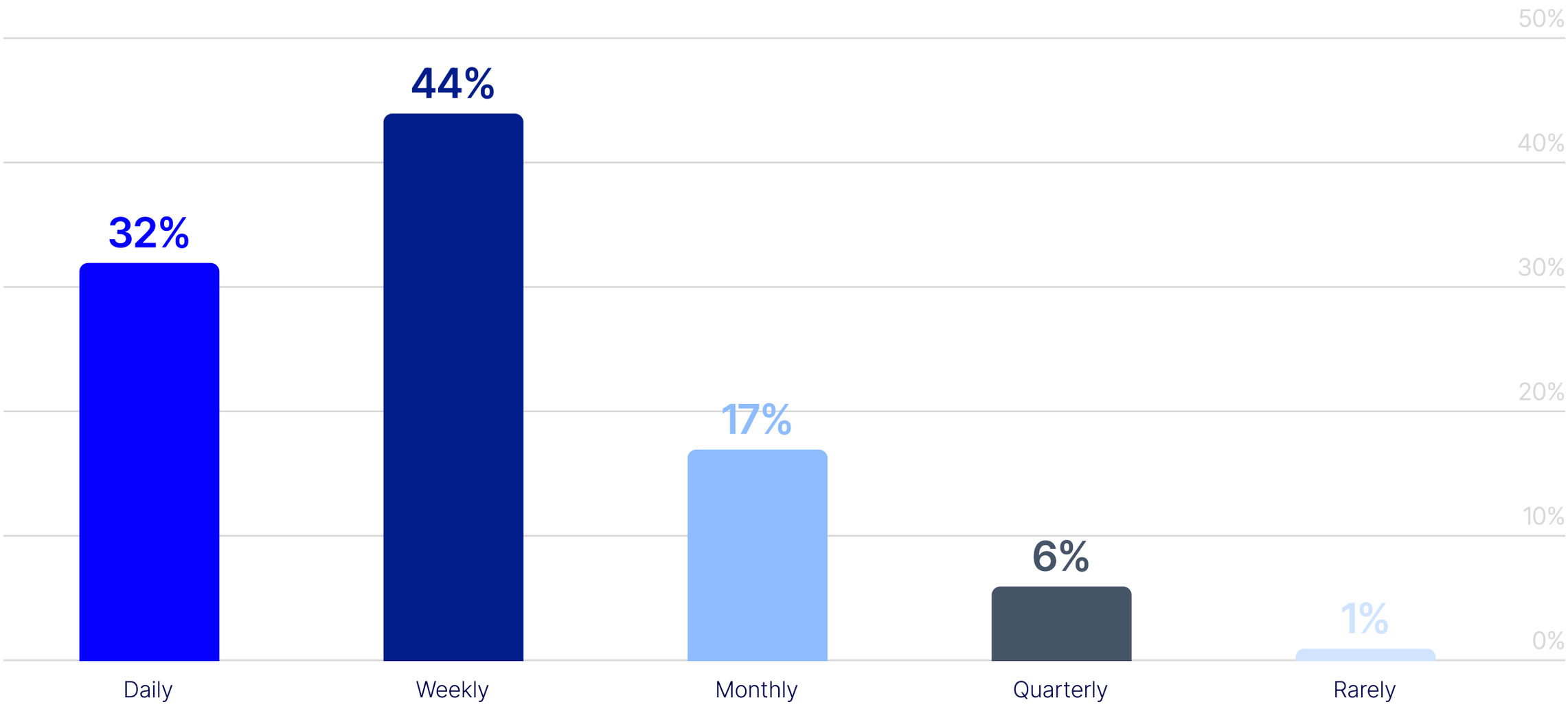


The fact that the majority have invested in at least one vendor and nearly half pay for more than one underlines the value that enterprise organizations place on threat intelligence. While investing in multiple vendors may present an opportunity for consolidation, the right approach when faced with greater budget or ROI scrutiny is a threat intelligence product with multiple data sources and integrations with other best-of-breed security solutions.

01

Most enterprise organizations frequently rely on threat intelligence, which reinforces the value it provides. Threat intelligence directly influences security decisions at least weekly for more than three-quarters (76%) of surveyed security professionals, with 32% saying it influences decisions daily. Just 1% say threat intelligence rarely influences these decisions.

How often does threat intelligence directly influence your security decisions?



Recorded Future helped our team cut down manual research with real-time threat intelligence. This helped in saving time connecting the dots, reduced dwell time, and helped us focus on high-risk alerts, risk scoring and prioritization, and better user experience.

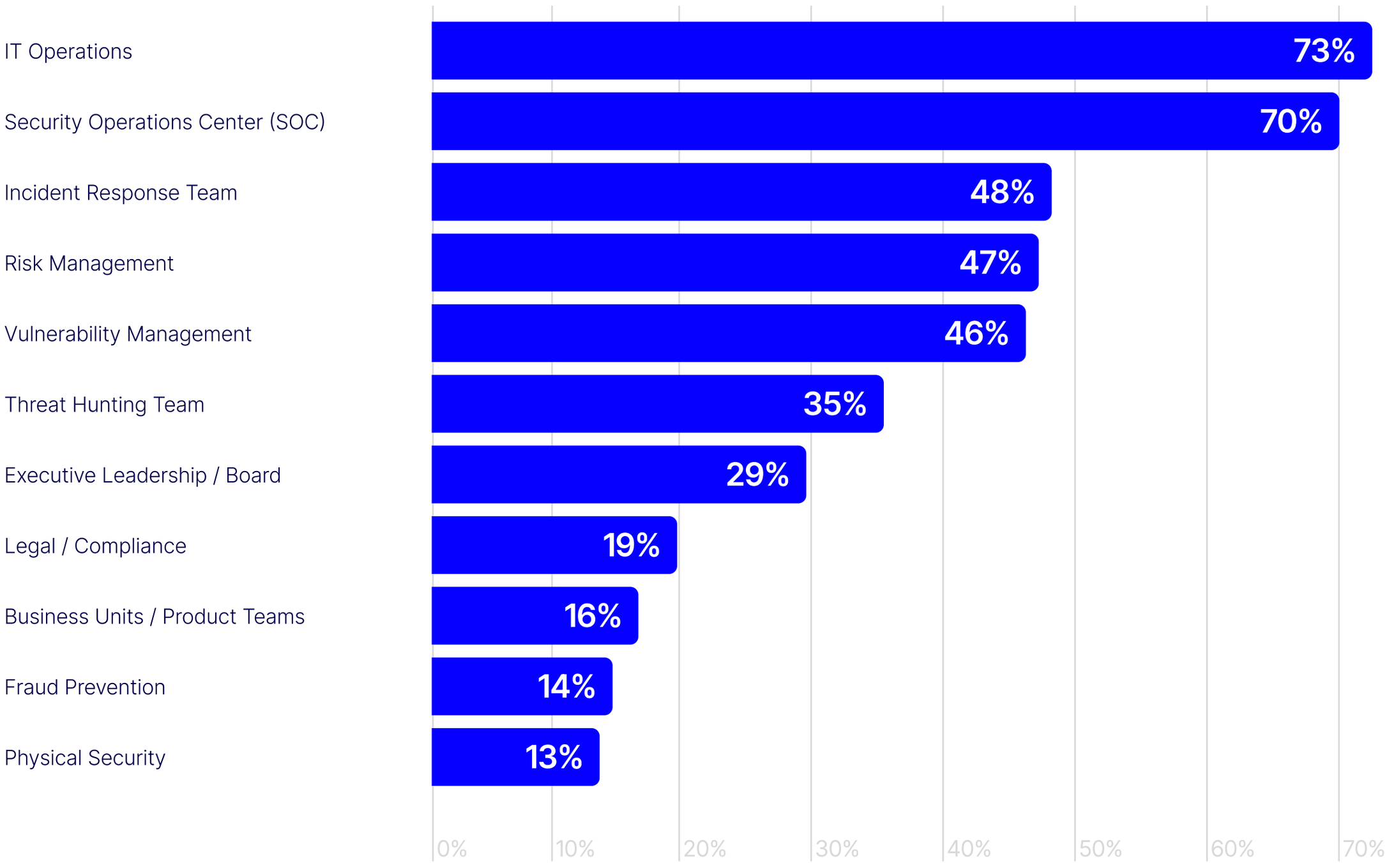
Dhanush K N, Security Engineer, Empower

01

In most enterprise organizations, multiple teams rely on threat intelligence. Three-quarters (73%) of surveyed security professionals say IT operations uses threat intelligence, and 70% say SOC actively consumes threat intelligence. Incident response teams (48%), risk management (47%), and vulnerability management (46%) also actively use threat intelligence.

In contrast, physical security (13%), fraud prevention (14%), business units and product teams (16%), and legal and compliance (19%) are least likely to actively consume threat intelligence.

Which teams in your organization actively consume threat intelligence?



I recommend aligning threat intelligence teams with risk teams and other business units. Once intelligence is embedded in regular decision-making, it's used to enrich organizational outcomes.

Dan Elliott, Field CISO for APJ, Recorded Future

Threat intelligence spending and success metrics

02

Most enterprise organizations allocate substantial cybersecurity budgets to threat intelligence—often with the goal of mitigating increasingly sophisticated attacks from a wider range of sources.

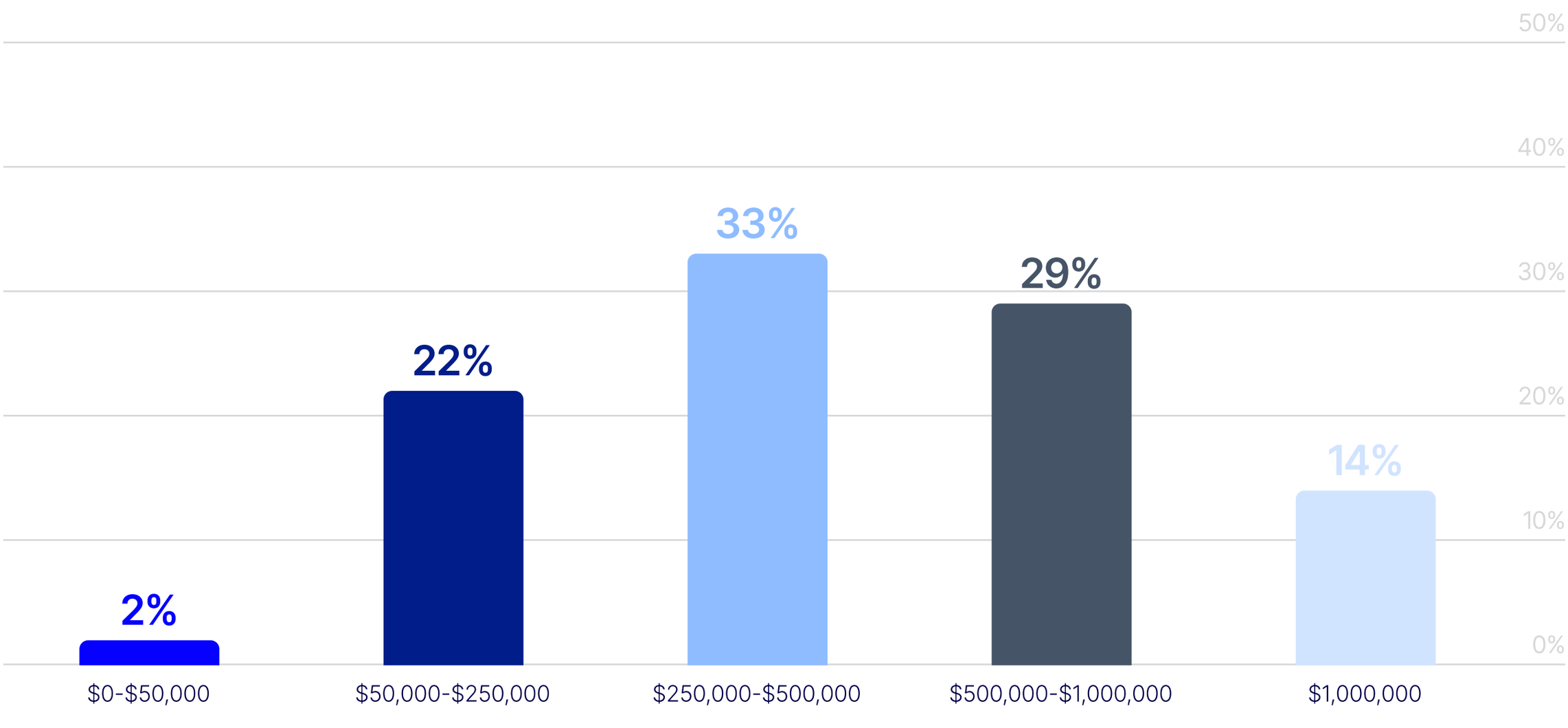
In 2025, data breaches involving a third party doubled compared to the previous year, and exploitation of vulnerabilities as an initial access vector increased 34%, according to the Verizon 2025 Data Breach Investigations Report.

> **Adversaries are moving faster and regulators have begun expecting more from leadership as far as preparation and resilience. Good intelligence helps you stay ahead of the curve and act rather than react.**
>
> *Dan Elliott, Field CISO for APJ, Recorded Future*

In concrete terms, most (76%) security professionals say their organization invests $250,000 or more per year in external threat intelligence products (excluding services). 33% spend $250,000 to $500,000, 29% spend $500,000 to $1 million, and 14% spend more than $1 million per year.

02

What is your annual investment in external threat intelligence products?



While these numbers are sizable, a year-over-year comparison shows a slight decrease in overall spending on external threat intelligence tools. In 2024, 79% reported spending at least $250,000 per year on threat intelligence products from external vendors, while 17% reported spending at least $1 million per year (17%).

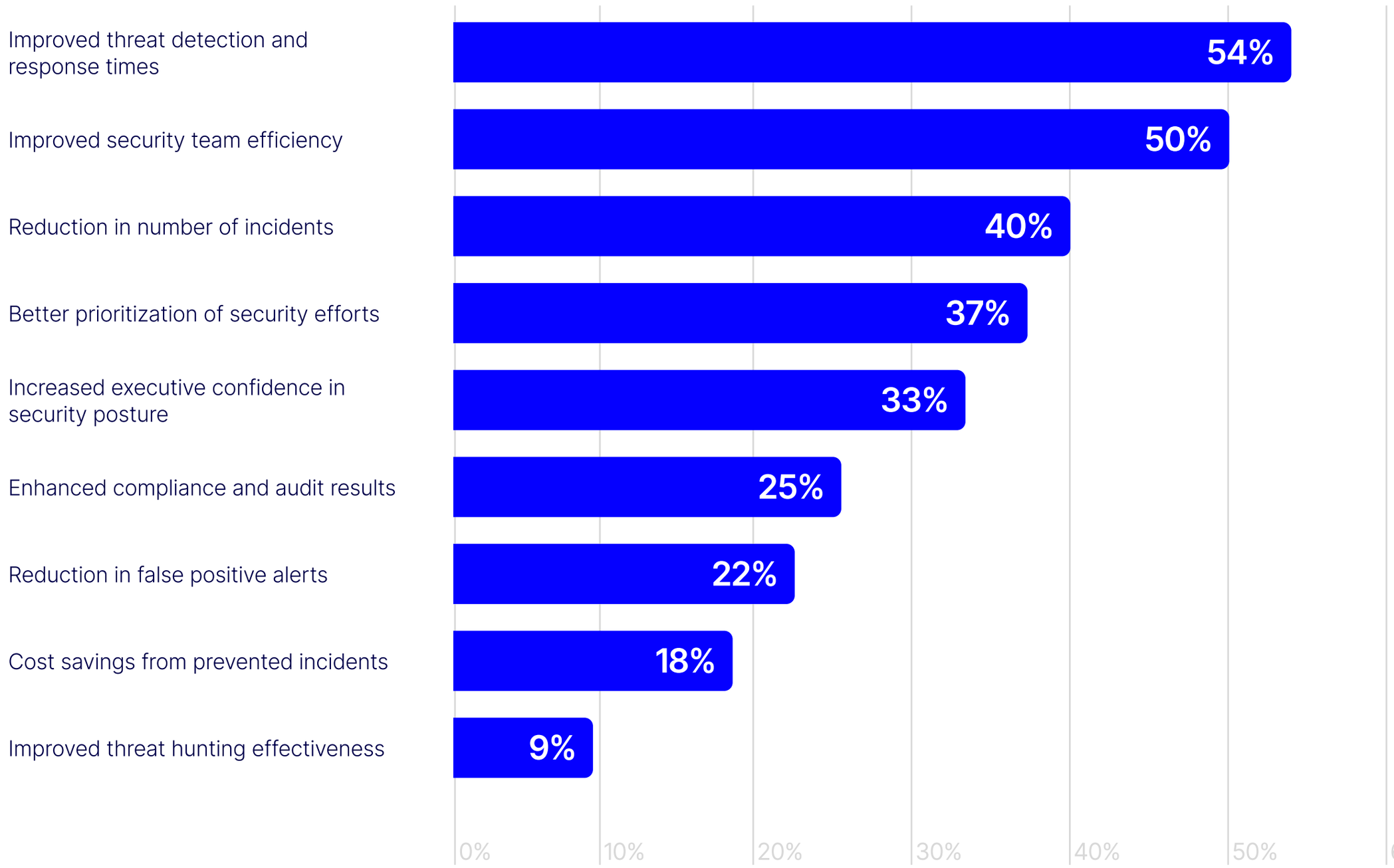
However, as Section 4 of this report reveals, any decrease in budget allocation for threat intelligence isn't likely to persist. In the next 12 months, nearly all enterprise organizations expect to spend *more* on threat intelligence.

02

When measuring the success of their threat intelligence programs, most organizations focus on speed and efficiency. Fifty-four percent of security professionals measure improved threat detection and response times, while 50% consider improved security team efficiency. Forty percent measure reduction in the number of incidents, and 37% consider prioritization of security efforts.

In contrast, few organizations use metrics like improved threat hunting effectiveness (9%) and cost savings from prevented incidents (18%) to measure threat intelligence success.

How do you measure the success of your threat intelligence program?



02

> “Recorded Future is the gold standard for threat intelligence. It has saved at least 50% of time for threat hunting, vulnerability management, incident triage, phishing emails, and anything else a SOC looks for!
>
> *Joshua C., Hospital and Health Care Company*

Explore how Recorded Future drives ROI for cybersecurity teams

Challenges with threat intelligence maturity

03

Threat intelligence maturity is improving year over year. Yet more than half of enterprise organizations consider theirs less than advanced.

Altogether, 49% of surveyed security professionals say their maturity level is advanced. This means they have tools that combine outputs from multiple threat intelligence sources, a dedicated threat intelligence team, and automated workflows that integrate threat intelligence with most security activities including business risk assessment.

Forty-four percent consider their threat intelligence maturity to be intermediate. In other words, they use multiple independent threat intelligence sources, have threat intelligence specialists integrated into different security teams, and have structured workflows that integrate threat intelligence with a few key security activities.

The remaining 6% rate their maturity level as basic or beginner. Five percent say they're at a basic level, meaning they use a few threat data feeds or threat intelligence analysts wear many hats—and they mostly react to alerts. The remaining 1% consider themselves beginners, meaning they primarily consume threat intelligence via their detection tools or free threat data feeds.

Overall, threat intelligence maturity has advanced compared to 2024. As the 2024 State of Threat Intelligence report shows, 45% of respondents considered their maturity level advanced, 40% considered themselves to be at an intermediate level, and 15% said they were at a basic or beginner level.

03

What is the maturity level of your threat intelligence?

2025		2024	
49%	Advanced	45%	Advanced
44%	Intermediate	40%	Intermediate
5%	Basic	10%	Basic
1%	Beginner	5%	Beginner

This progression in maturity year over year suggests that organizations are increasing investments in comprehensive threat intelligence products, dedicated teams, and automated workflows.

As these investments increase, enterprise organizations can experience a range of issues with threat intelligence vendors. Credibility, integrations, and information overload stand out as the leading difficulties.

Security professionals are looking two years down their roadmap. When new tools appear, it's important that your vendor can move and grow with you. During the POC/POV ask the tough questions and consider where they'll be to assist you in years two and three.

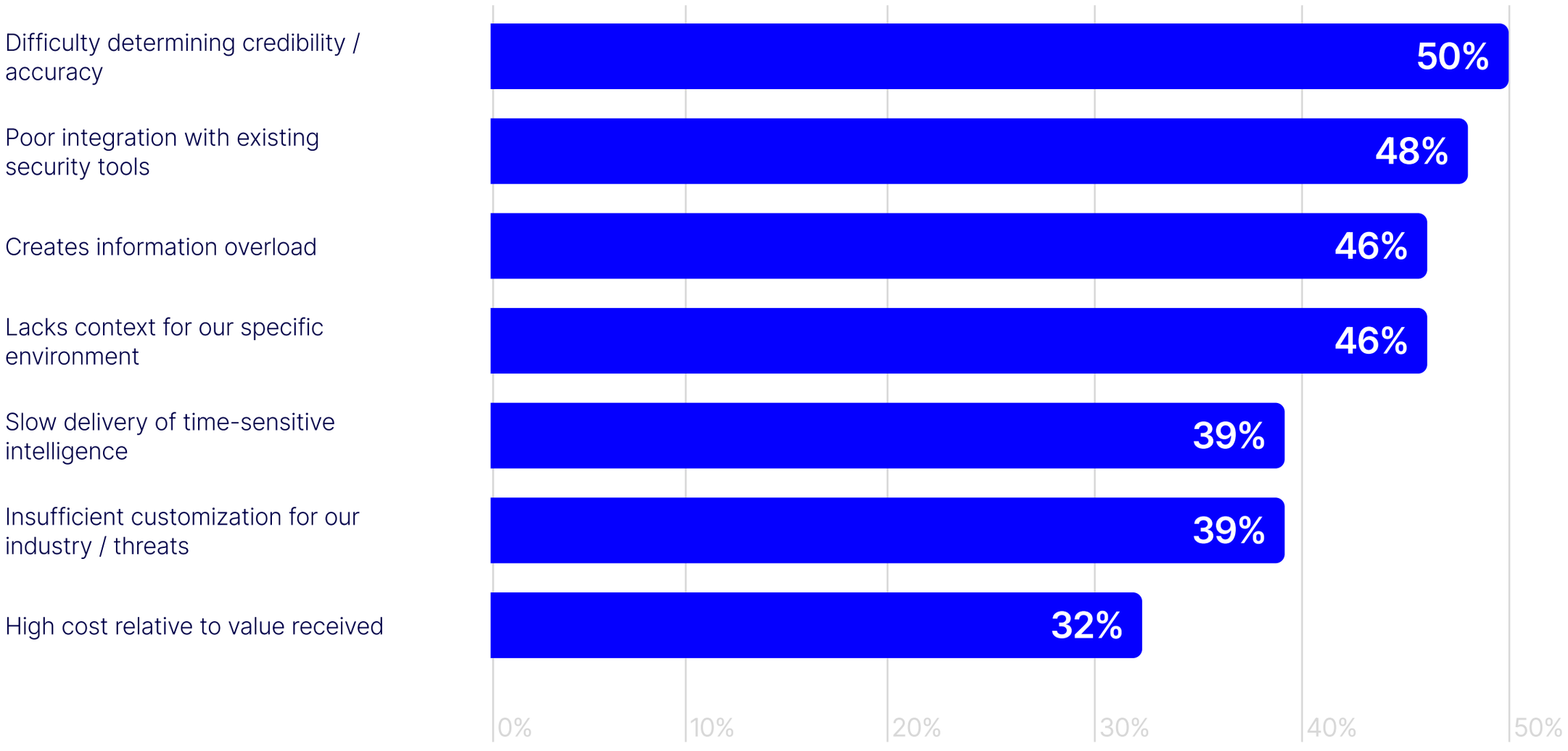
Dan Elliott, Field CISO for APJ, Recorded Future

03

In fact, 16% of respondents rank poor integration with existing security tools as their number one challenge with their current threat intelligence vendor. Another 16% rank difficulty determining credibility and accuracy their top concern.

Altogether, half of surveyed security professionals say difficulty determining credibility and accuracy is one of the top three issues with their current threat intelligence vendor. Rounding out these top three challenges are poor integration with existing security tools (48%), information overload (46%), and a lack of context for their specific environment (46%).

What are your biggest challenges with your current threat intelligence vendors?



This suggests security professionals are seeking a threat intelligence solution that they can seamlessly integrate into their security tools and workflows and that provides reliable, actionable intelligence with relevant context. This type of solution would ultimately improve signal-to-noise ratio.

03

> **[With Recorded Future] we are now actively able to detect threats and reduce risks that are relevant to our business rather than just read unspecific reports on threats targeting others.**
>
> *Head Cyber Threat Intelligence, Fortune 500 Construction and Engineering Company*

In contrast, high cost relative to value received (32%) is the least cited challenge, signaling that security professionals largely consider the cost of their threat intelligence vendors reasonable given the value they create.

However, the biggest challenges don't exactly align with the areas where enterprise organizations say their threat intelligence vendor needs the most improvement. A third of surveyed security professionals say speed of intelligence delivery is the area where their vendor needs the most improvement. One in five (22%) mention integration issues with security tools, and 21% cite in-depth analysis and context as their biggest vendor-related pain points.

In which area do you feel your threat intelligence vendor needs the most improvement?

33% Speed of intelligence delivery

22% Integration with our security tools

21% In-depth analysis and context

16% Relevance to our specific threats

6% Coverage of more use cases

3% ROI measurement

03

While enterprise organizations don’t cite speed as a challenge, they’re indeed seeking faster threat intelligence delivery. It also indicates that deeper integrations with security tools and more comprehensive analysis capabilities are table stakes for threat intelligence solutions.

> “Our team faced challenges in proactively identifying and mitigating threats targeting our organization. After integrating Recorded Future into our Cyber Threat Intelligence (CTI) workflow, we achieved a significant breakthrough in operational efficiency and threat visibility. We reduced detection time by 40%, from an average of 48 hours to 28 hours.
>
> *Cyber Threat Intelligence Specialist,*
> *Large Enterprise Professional Services Company*

While only a third of security teams say high cost is a challenge with their current threat intelligence vendors, cost effectiveness is a key factor for new investments. When evaluating a threat intelligence vendor, 34% of respondents say cost effectiveness is the number one factor. 20% say integration capabilities is the top factor, and 14% prioritize depth and actionability of analysis when choosing a threat intelligence vendor.

03

Rank these factors in terms of what's most important when choosing a threat intelligence vendor.

1. Speed of intelligence delivery
2. Cost-effectiveness
3. Timeliness of threat data
4. Depth and actionability of analysis
5. Coverage across numerous use cases
6. Customer support
7. Reputation in the industry
8. UI / UX and customization capabilities

These results reinforce the importance of security integrations for threat intelligence vendors. They also introduce cost and value as important decision-making factors and downplay aspects like UI/UX customization capabilities and customer support, which are two of the least-cited factors.

Security professionals should be considering: How actionable is the intelligence that the vendor is providing? This will involve strategic questions around which adversaries to focus on and why and how to address the possible threat intelligence program gaps to reduce risk. It will also involve tactical questions around speeding up and improving decision-making in the SOC.

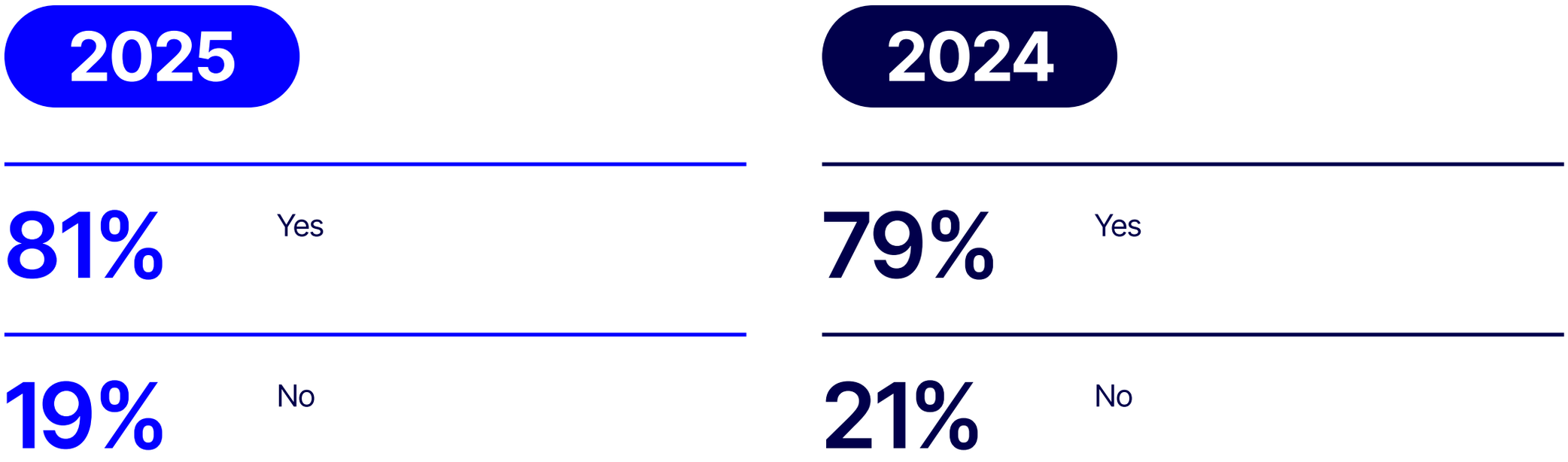
Jason Steer, CISO, Recorded Future

Future plans to strengthen threat intelligence

04

Vendor consolidation is a key goal for most enterprise organizations, with 81% of respondents indicating they intend to consolidate threat intelligence vendors.

Is your organization planning to consolidate threat intelligence vendors?



These consolidation plans aren't surprising given that nearly half of organizations pay for more than one threat intelligence vendor and even more may have multiple products in place. This shows a consistent preference to focus on one or two of the most useful threat intelligence vendors rather than monitoring separate feeds or adding complexity to already burdened security teams.

But it's important to note that these consolidation plans are not cost-cutting measures. Instead, organizations intend to spend more on threat intelligence in the coming year. Most (91%) respondents say their organization plans to invest more in threat intelligence in 2026.

The 2024 State of Threat Intelligence report reveals almost identical results. In 2024, 90% of respondents said their organization planned to invest more in 2025. This ongoing intention to increase investments reflects a continued confirmation of the importance of threat intelligence.

04

Does your organization have plans to invest more in threat intelligence in the next year?

2025		2024	
91%	Yes	90%	Yes
9%	No	10%	No

As security teams strive to consolidate solutions, they'll likely want to prioritize vendors that address critical capabilities. The data shows that security teams' threat intelligence work is almost evenly divided between five areas.

Surveyed security professionals spend 22% of their threat intelligence work on analyzing and contextualizing threats to their organization and 19% on threat hunting and proactive detection activities. They spend 18% on supporting incident response and investigations, 18% on vulnerability research and prioritization, and 17% on strategic threat landscape analysis and reporting.

What percentage of your threat intelligence work is spent on these tasks?

22% Analyzing and contextualizing threats to your organization

19% Threat hunting and proactive detection activities

18% Supporting incident response and investigations

18% Vulnerability research and prioritization

17% Strategic threat landscape analysis and reporting

04

This relatively even split shows the importance of each of these capabilities. Organizations should look for vendors who can provide threat intelligence capabilities across a number of use cases. At the same time, threat intelligence vendors have an opportunity to give security teams time back in certain areas so they can prioritize analysis and other human-dependent work.

> Threat Intelligence module is essential for our needs, seamlessly integrating to optimize our defense strategy. By using the platform alongside our in-house systems, we achieve faster and more precise results. This efficiency and the platform's steadfast reliability make it indispensable for our operations.
>
> *Ashraf G., Senior Principal / Enterprise Cloud Architect*

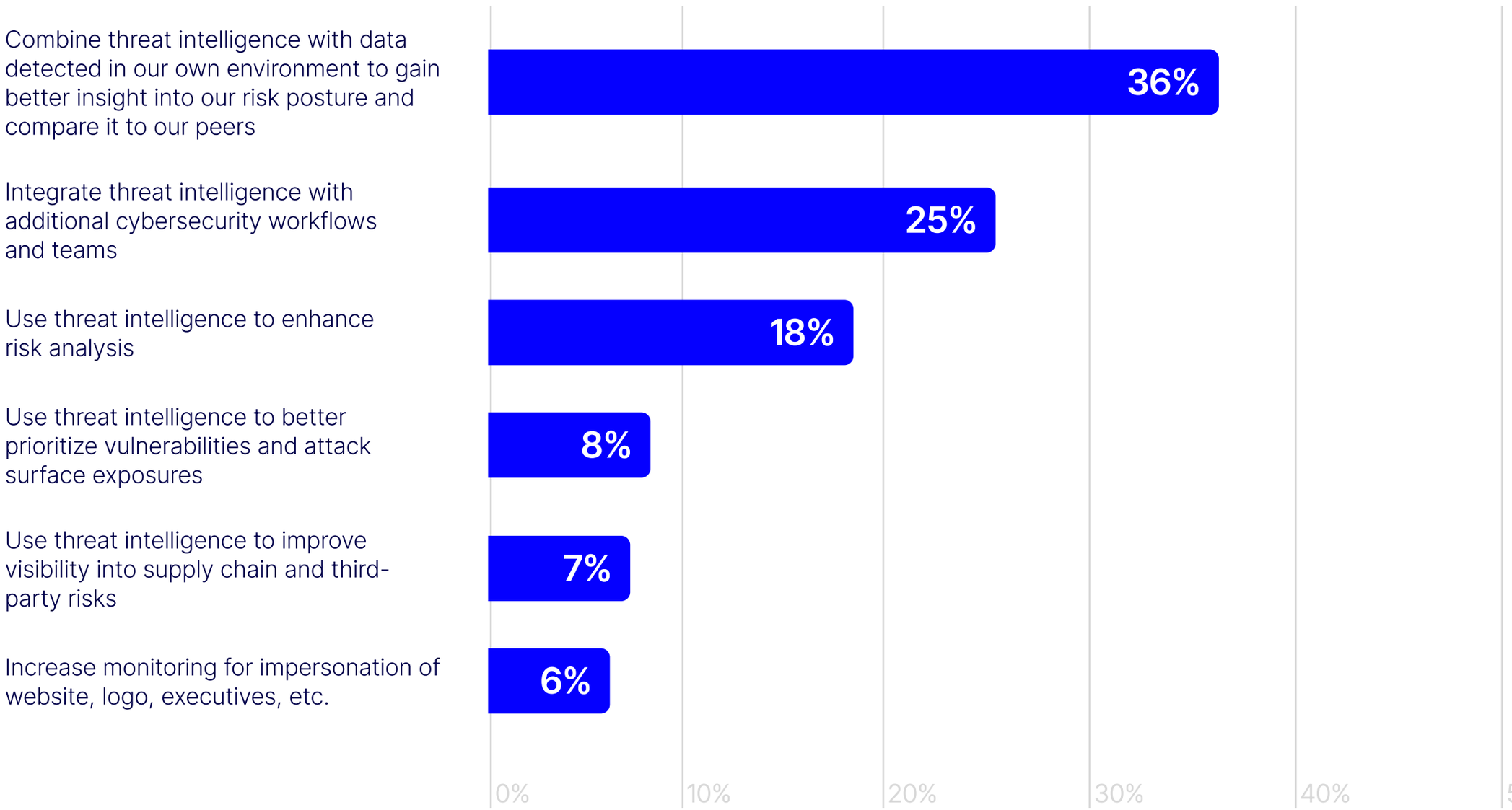
Learn how to develop an effective cyber threat intelligence program

04

Enterprise organizations intend to make a few key changes to improve how they use threat intelligence in the next two years. Over a third (36%) of surveyed security professionals say they plan to combine threat intelligence with data detected in their own environment to gain better insight into their risk posture and compare it to their peers.

A quarter (25%) say they plan to integrate threat intelligence with additional cybersecurity workflows and teams—focusing on identity access management, fraud, and GRC. An additional 18% say they aim to enhance risk analysis.

How does your organization plan to improve threat intelligence use in the next two years?



As the 2024 State of Threat Intelligence report shows, integrating threat intelligence with cybersecurity workflows and teams was also top of mind for 66% of respondents. In 2024, organizations also planned to better prioritize vulnerabilities (59%) and combine with internal data to improve risk posture (57%).

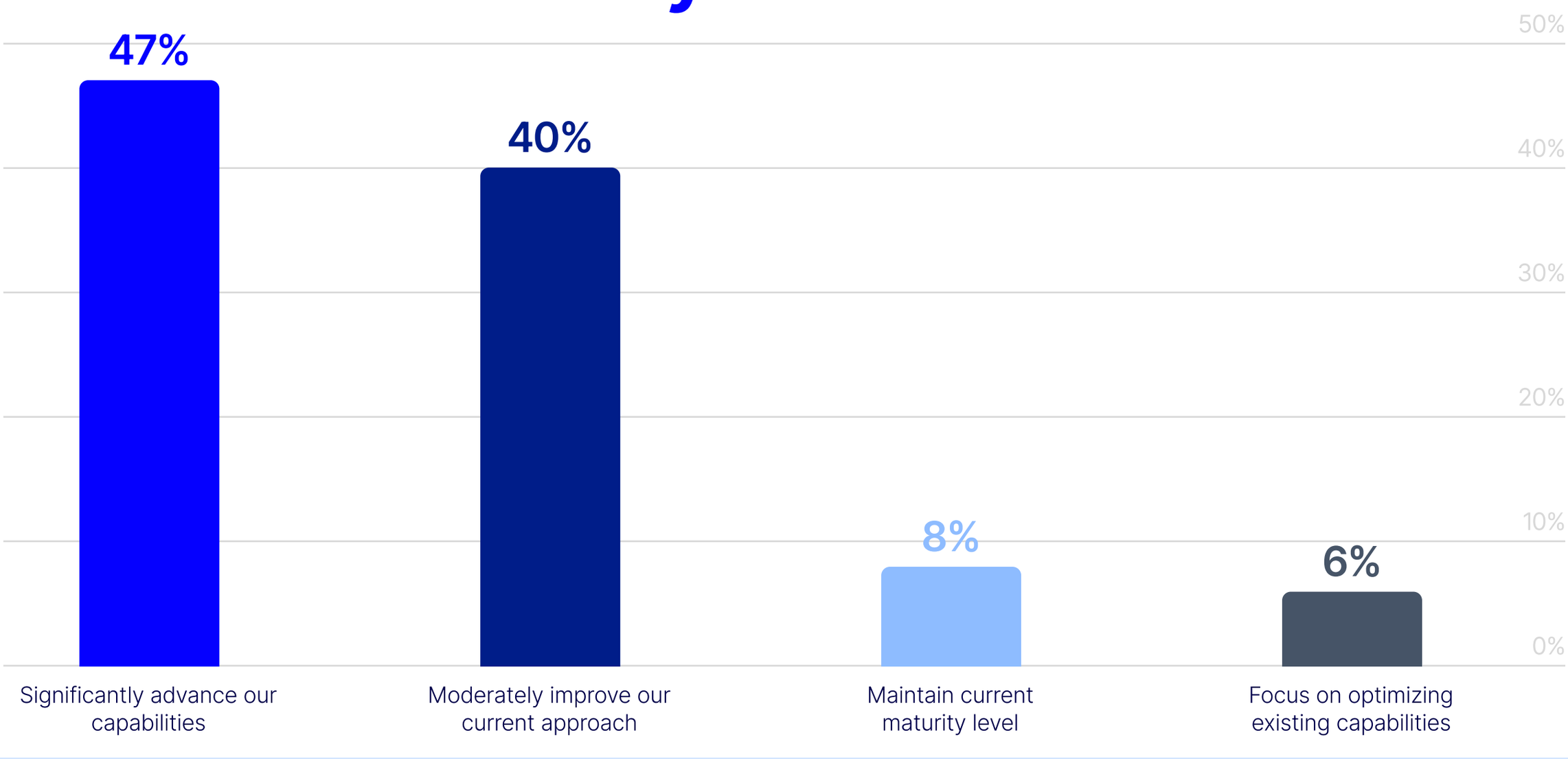
04

These year-over-year shifts echo other 2025 survey findings, which indicate that enterprise organizations primarily use threat intelligence to enhance existing detection capabilities. They also reinforce the importance of choosing a threat intelligence vendor that integrates with a wide range of cybersecurity solutions.

> Recorded Future acts on anywhere from several hundred to several thousands of IOCs per day and does not only save time, but provides unique value that cannot only be justified with time savings—the information may otherwise have been inaccessible.
>
> *Information Security Specialist, Diversified Financial Services Company*

As they improve how they use threat intelligence in the next two years, 87% of survey respondents expect a moderate to significant evolution in their threat intelligence maturity.

How do you expect your organization's threat intelligence maturity to evolve over the next two years?



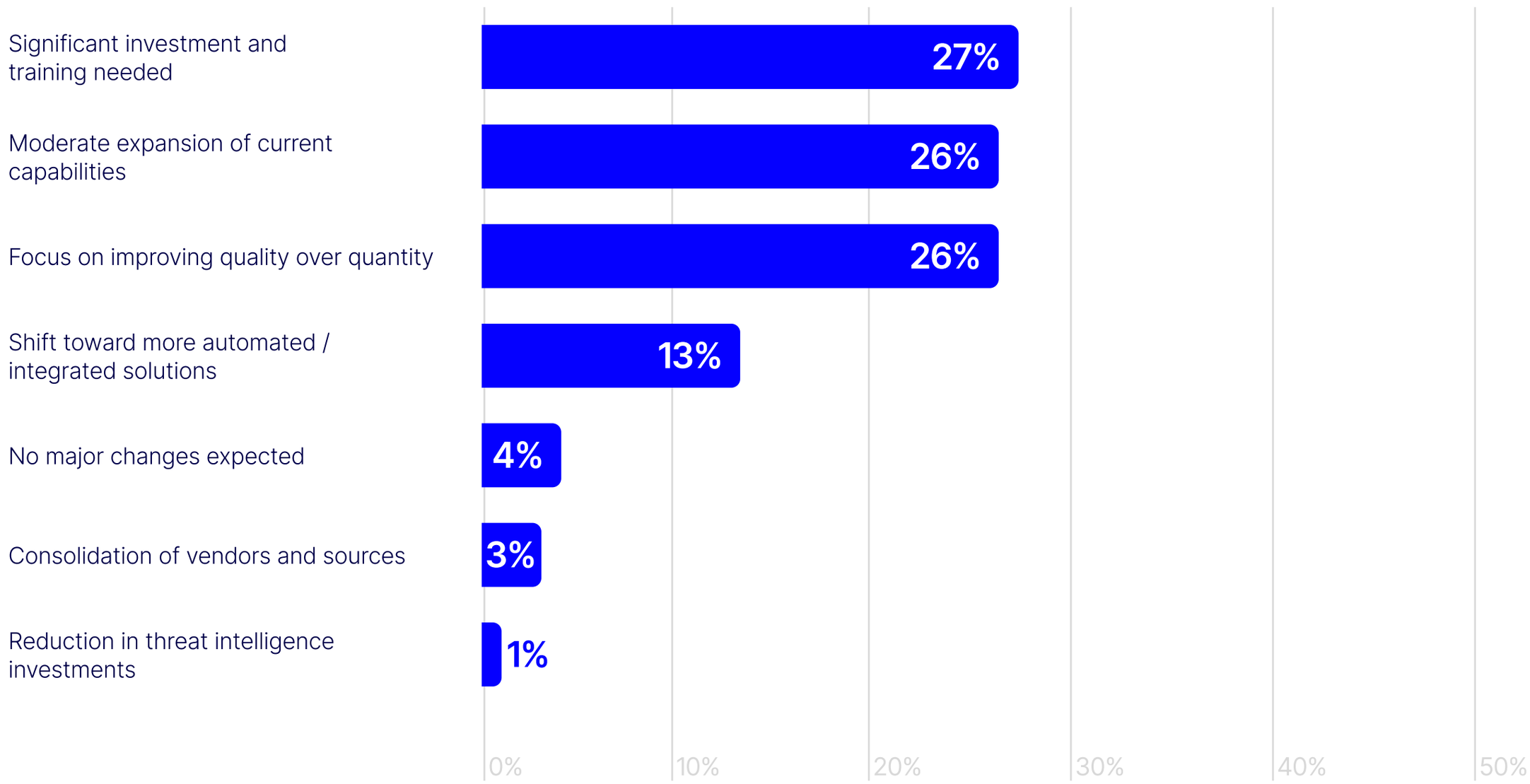
04

Just 8% expect to maintain their current maturity level over the next two years. This aligns with other survey findings, which reflect a gradual improvement in threat intelligence maturity and plans to increase threat intelligence spending.

To reach these maturity goals and keep pace with the changing cybersecurity landscape, most enterprise organizations anticipate needing moderate to significant threat intelligence improvements.

More than half of survey respondents (53%) expect moderate to significant changes to threat intelligence needs in the next 12 months. A quarter (27%) anticipate needing significant threat intelligence investments and training, and 26% expect a moderate expansion of current capabilities. An additional 26% predict shifting focus to quality over quantity.

How do you expect your threat intelligence needs to change in the next 12 months?



These findings acknowledge that most enterprise organizations need to make major strides to bring their threat intelligence capabilities and maturity to an acceptable level. The data also reflects clear intentions to increase investments in threat intelligence.

Conclusion.

Threat intelligence is an essential tool for enterprise organizations, particularly against the backdrop of state-sponsored threats, cybercrime, and geopolitical issues that continue to plague businesses in 2025. Most enterprises now have dedicated threat intelligence teams and use threat intelligence to guide daily or weekly decisions. Many use it to inform strategic planning, risk assessment, and incident response.

While nearly half of surveyed security professionals consider their threat intelligence maturity level advanced, an almost equal percentage expect to significantly evolve their threat intelligence capabilities in the next two years.

How does your organization's threat intelligence maturity compare? Get a clear answer and suggestions for next steps with Recorded Future's Maturity Assessment tool.

> **Enterprises can advance threat intelligence maturity by making it a core business strategy. They should embed threat insights into risk decisions, align security and operational teams, automate analysis and response, and continuously measure impact on decision quality and risk reduction to drive ongoing improvement.**
>
> *Rich LaTulip, North America Field CISO, Recorded Future*

To see more threats, identify them faster, and take action to remediate attacks, look to the most comprehensive and independent threat intelligence company.

Explore Recorded Future

Methodology.

Recorded Future partnered with third-party researcher UserEvidence to survey 615 cybersecurity executives, managers, and practitioners in August 2025.

All respondents represented companies with more than 1,000 employees. Over half (56%) were from organizations with 1,001-5,000 employees, while 44% were from organizations with more than 5,000 employees.

Most respondents held leadership roles in cybersecurity, including cybersecurity managers or directors (62%) and cybersecurity VPs or executives (21%). The remaining respondents were security practitioners.

All respondents were acquainted with their company's threat intelligence tools and policies. 81% reported being very familiar, and 19% were moderately familiar.

Respondents were from the United States (52%), the United Kingdom (17%), Canada (16%), and Australia (16%).

About Recorded Future.

Recorded Future is the world's largest intelligence company. The Recorded Future platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining Intelligence Graph®-powered AI with the world's largest collection of specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact business.

Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

Learn more

About UserEvidence.

UserEvidence is a software company and independent research partner that helps B2B technology companies produce original research content from practitioners in their industry. All research completed by UserEvidence is verified and authentic according to their research principles: Identity verification, significance and representation, quality and independence, and transparency. All UserEvidence research is based on real user feedback without interference, bias, or spin from our clients.

UserEvidence Research Principles

These principles guide all research efforts at UserEvidence—whether working with a vendor's users for our Customer Evidence offering, or industry practitioners in a specific field for our Research Content offering. The goal of these principles is to give buyers trust and confidence that you are viewing authentic and verified research based on real user feedback, without interference, bias, and spin from the vendor.

1. Identity Verification

In every study we conduct, UserEvidence independently verifies that a participant in our research study is a real user of a vendor (in the case of Customer Evidence) or an industry practitioner (in the case of Research Content). We use a variety of human and algorithmic verification mechanisms, including corporate email domain verification (i.e., so a vendor can't just create 17 Gmail addresses that all give positive reviews), and pattern-based bot and AI deflection.

2. Significance and Representation

UserEvidence believes trust is built by showing an honest and complete representation of the success (or lack thereof) of users. We pursue statistical significance in our research, and substantiate our findings with a large and representative set of user responses to create more confidence in our analysis. We aim to canvas a diverse swatch of users across industries, seniorities, personas—to provide the whole picture of usage, and allow buyers to find relevant data from other users in their segment, not just a handful of vendor-curated happy customers.

3. Quality and Independence

UserEvidence is committed to producing quality and independent research at all times. This starts at the beginning of the research process with survey and questionnaire design to drive accurate and substantive responses. We aim to reduce bias in our study design, and use large sample sizes of respondents where possible. While UserEvidence is compensated by the vendor for conducting the research, trust is our business and our priority, and we do not allow vendors to change, influence, or misrepresent the results (even if they are unfavorable) at any time.

4. Transparency

We believe research should not be done in a black box. For transparency, all UserEvidence research includes the statistical N (number of respondents), and buyers can explore the underlying blinded (de-identified) raw data and responses associated with any statistic, chart, or study. UserEvidence provides clear citation guidelines for clients when leveraging research that includes guidelines on sharing research methodology and sample size.