seemplicity

RESEARCH REPORT

The 2024 Remediation Operations Report

The 2024 Remediation Operations Report offers insights into the evolving realm of remediation operations in 2024. In an era where digital threats and organizational vulnerabilities loom large, understanding the trends, challenges, and best practices in cybersecurity is paramount.

The purpose of this research is to build an understanding of IT and Security Decision Maker perceptions around cybersecurity, automation and Artificial Intelligence (AI) involvement. This report covers various aspects of cybersecurity and vulnerability management, providing a comprehensive overview of key trends and strategies shaping these domains today. From the exponential growth in security budgets to the transformative potential of automation and AI, **The 2024 Remediation Operations Report** aims to equip organizations with the knowledge and insights needed to fortify their defenses and stay ahead of emerging threats.

Demographic Snapshot

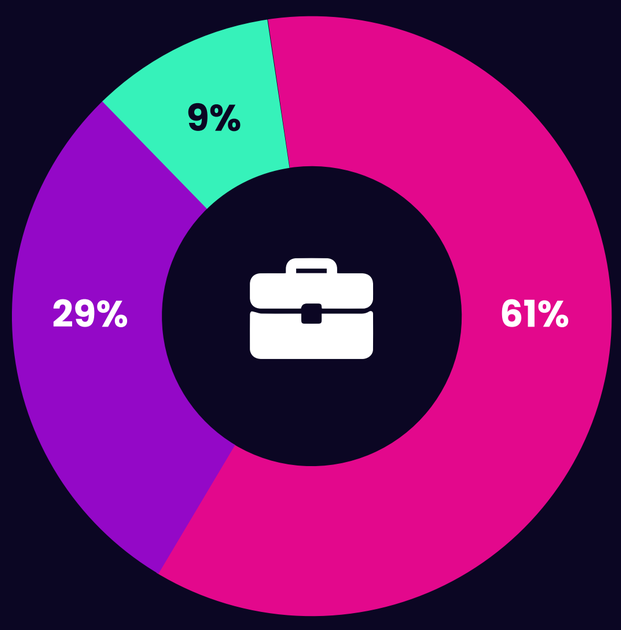
Country of Residence

Annual Revenue

$	**21%**	Less than $50m
$$	**44%**	$50.1m to $500m
$$$	**34%**	More than $500m

Level of Influence

- **9%** 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	% of Respondents
501 to 1,000	**23%**
1,001 to 5,000	**50%**
5,001 to 10,000	**16%**
10,000+	**11%**

Top 3 Business Industry

#1	**19%**	Software Technology
#2	**15%**	Manufacturing
#3	**13%**	Finance Insurance Accounting

Key Findings

Security Investments

As cyber threats become more sophisticated, investing in security is vital to stay ahead. The report's findings indicate organizations recognize that enhanced cybersecurity budgets are essential to safeguard assets and maintain stakeholder trust.

Change in security budget this year

In 2024, the **total security budget is increasing** for most companies.

ALMOST ALL

91%

say their security budget is increasing this year

Q4. How, if at all, is your total security budget changing this year? Select one

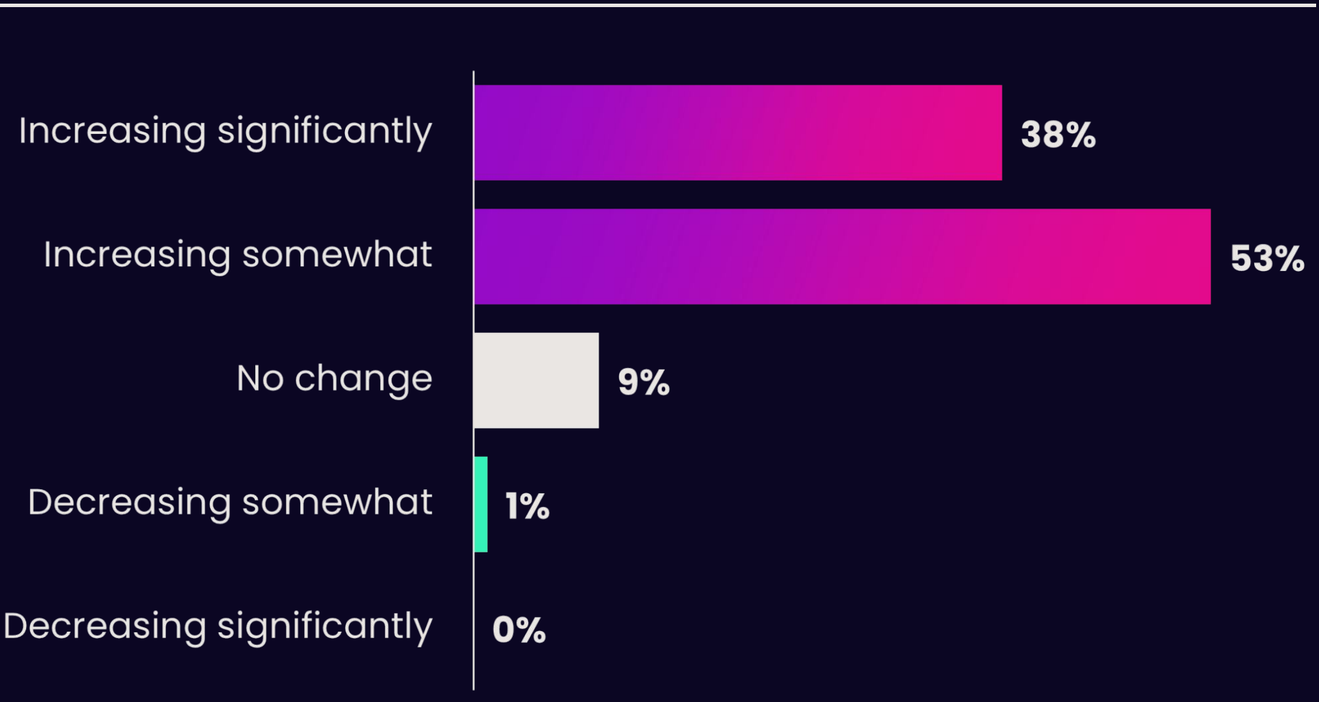


Figure 1

91% of respondents say their security budget is increasing this year, demonstrating a growing recognition of the importance of cybersecurity within organizations. This finding suggests that security is becoming an organization-wide initiative, enforced from the top down, rather than solely the security team.

Change in security products budget

On average, budget for security products **has grown by 22% in the past year**, with only **3%** saying the budget **hasn't grown at all.**

Q3. By how much, if at all, did your security products budget grow in the last 12 months? Select one

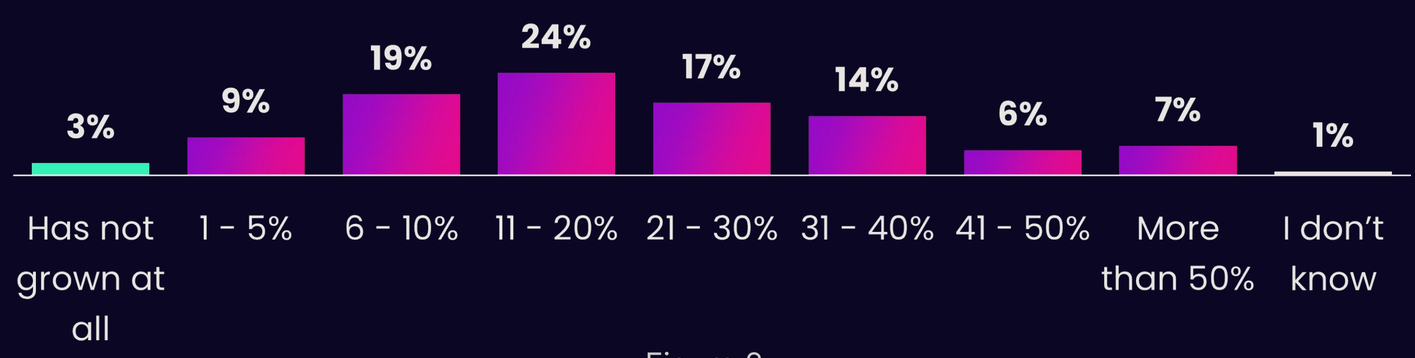


Figure 2

96% of respondents say their budget for security products grew in the last year. This surge in investment in security products underscores the urgency organizations feel to bolster their defenses against evolving threats. The average growth rate of 22% suggests that companies are not only investing more in security but are doing so at a significant pace. These numbers indicate that the current tech stack, even with an average of 38 vendors (see fig.3), is still not a sufficient defense mechanism.

These trends suggest a heightened awareness of the evolving threat landscape, regulatory requirements and high-profile security breaches - and the imperative for robust defense measures. The landmark verdict in the SolarWinds case saw the SEC charge SolarWinds' CISO with fraud and internal control failures. The case set a precedent, with organizations recognizing the need to invest more resources into cybersecurity solutions to safeguard their assets and maintain trust with stakeholders.

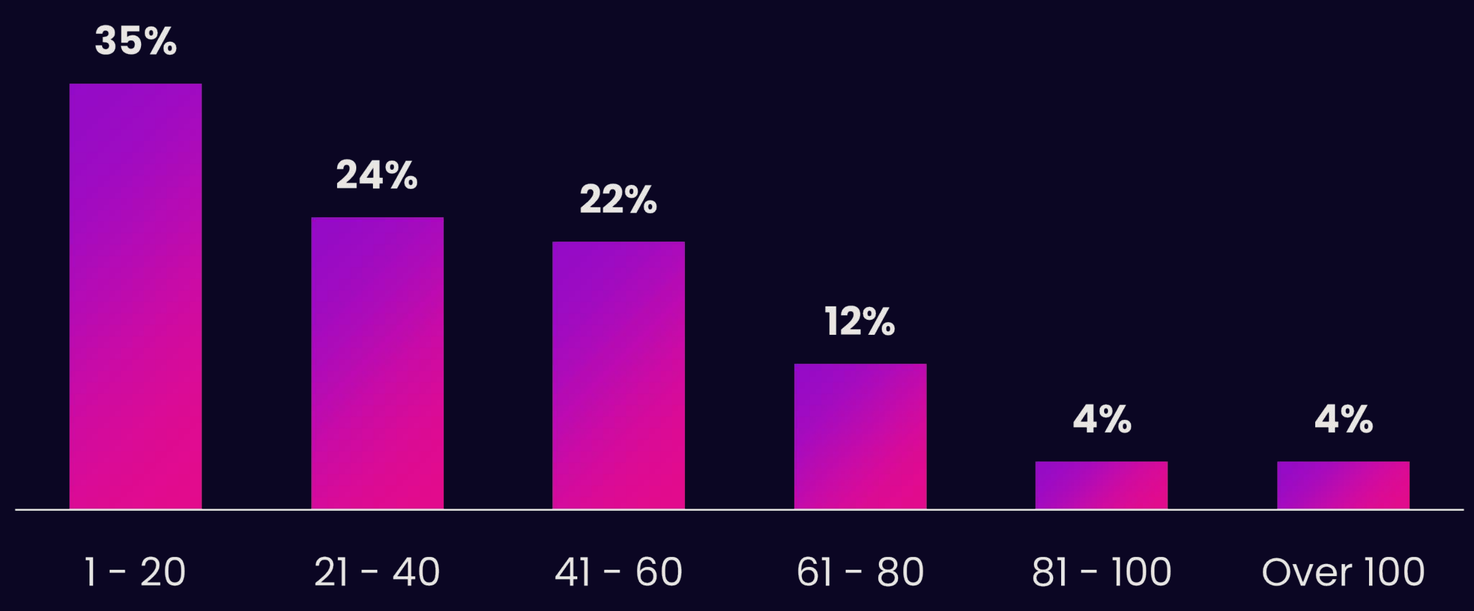
Vulnerability Management

Tools and Vendors

Effective vulnerability management relies on an assortment of tools, each addressing different security needs.

Number of security product vendors

On average, organizations are using **38 different security product vendors.**



Q2. How many different security product vendors do you use in your organization? Select one

Figure 3

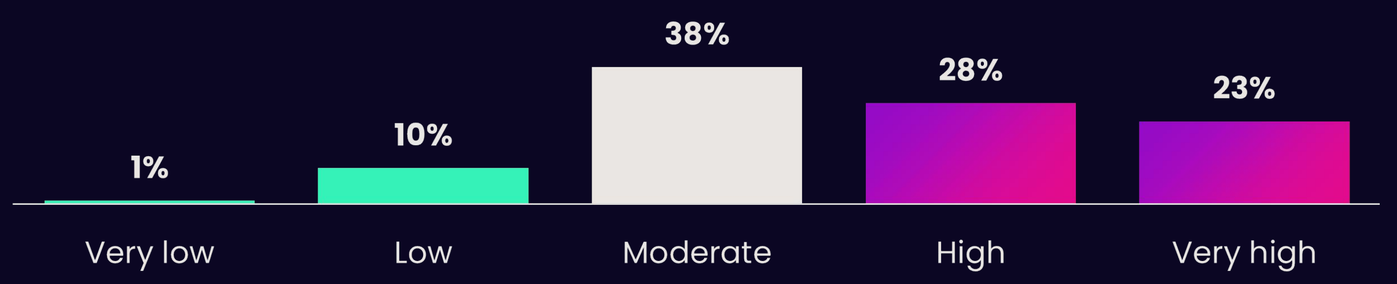
However, the fact that organizations are utilizing an average of 38 different security product vendors indicates complexity and fragmentation. It suggests that organizations adopt a multi-faceted approach to security, leveraging a diverse set of tools and solutions from various vendors to address different aspects of their security needs. Managing such a large number of vendors can pose challenges in terms of integration, interoperability, and overall efficacy of the security infrastructure.

Noise

With a multitude of security tool vendors, organizations face the challenge of managing excessive noise, which can hinder the efficiency of vulnerability management efforts.

Level of noise generated by risk and vulnerability scanning tools

More than half (51%) say the level of noise generated by scanning tools is **high**, with only **11%** saying it's **low**.



Q6. How would you rate the level of noise generated by your current risk and vulnerability scanning tools? Select one

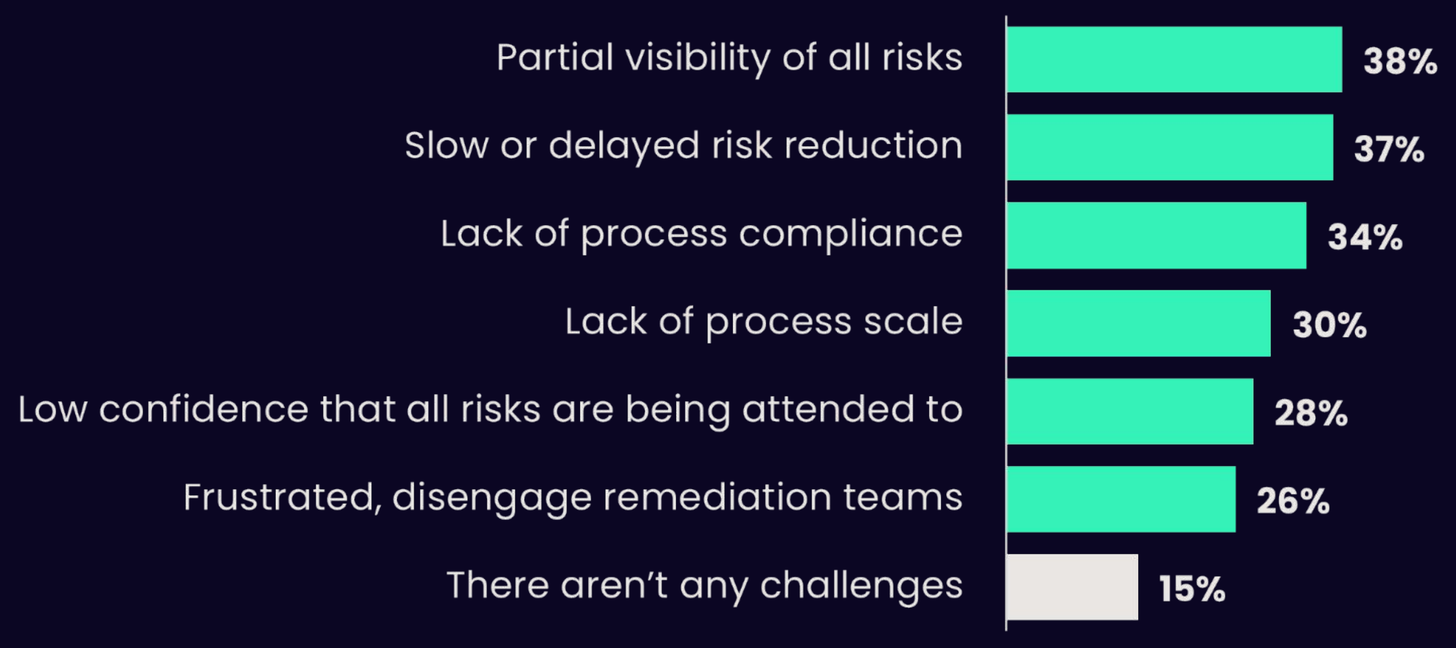
Figure 4

51% of respondents say their tools generate a high to very high level of noise, indicating that a majority of organizations are inundated with a large volume of alerts, notifications, and findings from various tools in their tech stack, of which not all are information signals. High noise levels can overwhelm and distract security teams, making it difficult for them to discern and prioritize genuine risks from false positives or less critical issues.

When looking back at the data in fig.3, we can deduce that, despite best intentions, more is not better - it's the opposite. The very tools organizations purchase to help strengthen their cybersecurity posture are creating more work for security teams and more gaps in their attack surfaces.

Challenges in managing noise generated by risk and vulnerability scanning tools

85% have challenges in managing noise generated by scanning tools.



Q8. Are there any other challenges in managing the noise generated by vulnerability scanning tools? Select up to three

Figure 5

Top challenge

85% have challenges in managing noise generated by scanning tools, with the top challenge being **slow or delayed risk reduction (25%)**.

Q9. Out of the challenges your organization faces, which is the top one? Select one

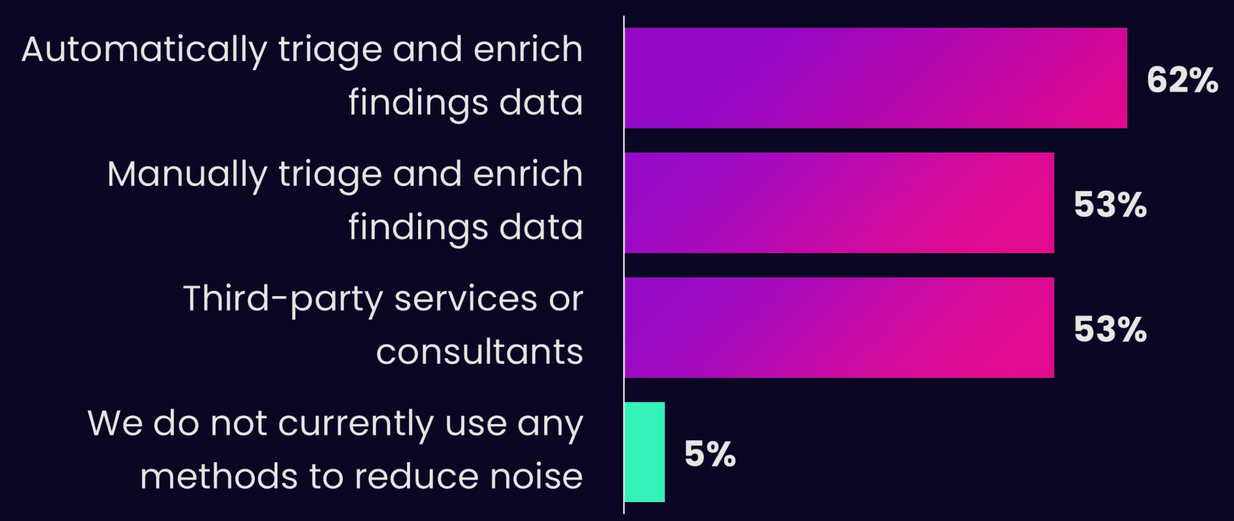
**Asked to those who experience challenges in managing noise*

Figure 6

With 85% of respondents finding it challenging to manage the noise, it is clearly a widespread struggle within the industry and significantly impactful. The top challenge being slow or delayed risk reduction emphasizes the severity of the issue, indicating that the overwhelming noise impedes efficient vulnerability identification and prioritization, thus slowing down the response to risks.

Methods used to reduce noise of vulnerability scanning tools

62% currently use **automatically triage and enrich findings data** to reduce the noise of scanning tools, with only **5%** saying **they have no methods**.



Q10. What methods does your organization currently use to reduce the noise of vulnerability scanning tools? Select all that apply

Figure 7

The fact that a significant majority of respondents (95%) are leveraging at least one method to try and reduce noise indicates acknowledgement of the problem and the urgent need to address it. There is clear demand for solutions that help organizations effectively manage the noise, further supporting the fact that this is an urgent issue.

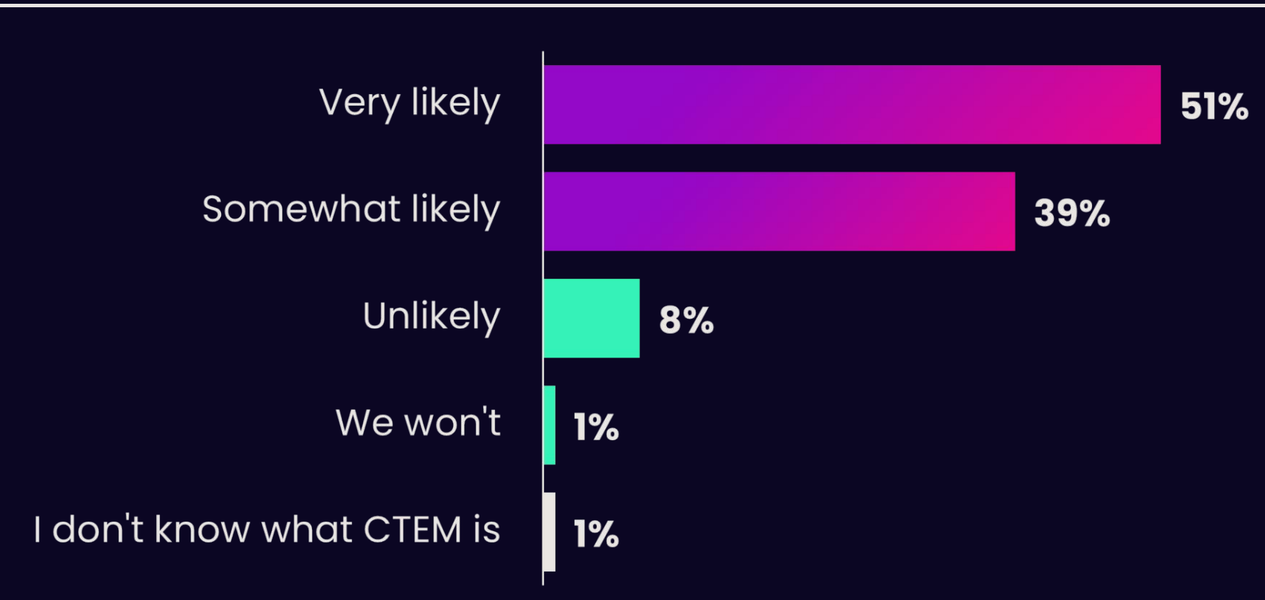
And with a majority of organizations automatically triaging and enriching data findings (62%), there is growing recognition of automation's importance in vulnerability management. This trend towards automation aligns with broader industry shifts towards leveraging technology to enhance cybersecurity resilience (see Automation). However, clearly these efforts are limited in their success, per the findings above.

CTEM

The Continuous Threat Exposure Management (CTEM) framework represents a proactive approach to vulnerability management. By continuously monitoring IT infrastructure for vulnerabilities, CTEM enables organizations to stay ahead of threats and enhance their overall security posture, moving beyond traditional periodic assessments.

Adoption of CTEM program in the next 12 months

90% say it's **likely they'll adopt** a CTEM program in the next 12 months.



Q12. What's the likelihood you'll adopt a Continuous Threat Exposure Management (CTEM) program in the next 12 months? Select one

Figure 8

The high percentage of respondents (90%) indicating their likelihood to adopt CTEM programs indicates industry-wide acknowledgement of the value of the CTEM framework and signals a shift towards proactive risk management strategies over reactive incident response. Organizations want to be able to continuously monitor their IT infrastructure for vulnerabilities, rather than relying solely on periodic assessments.

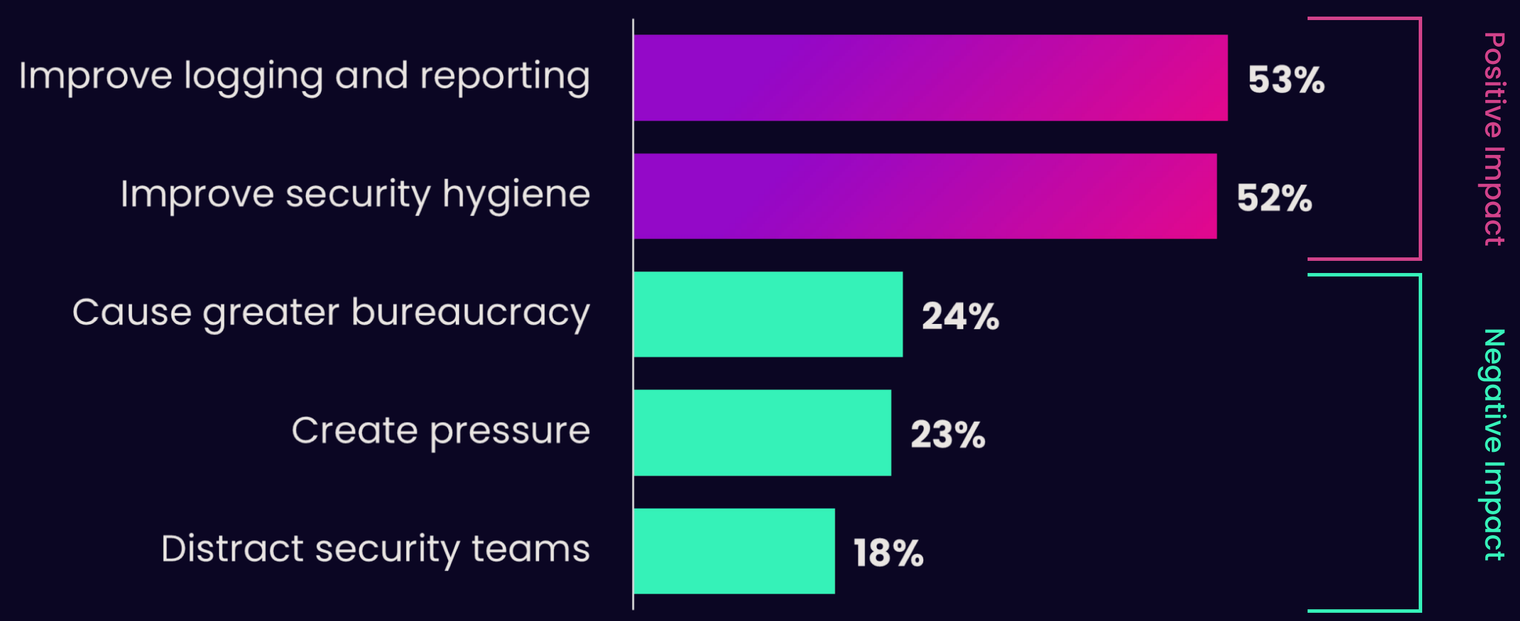
Considering the adoption of CTEM involves investments in advanced security technologies and platforms, this finding suggests that organizations are willing to spend on solutions that provide real-time insights into their security posture and facilitate proactive risk reduction.

SEC Cybersecurity Disclosure Requirements

The SEC's cybersecurity disclosure requirements mandate timely reporting of material cybersecurity incidents and annual disclosures on cybersecurity risk management and governance. This regulation signifies a critical industry shift towards greater transparency and accountability in cybersecurity practices.

Impact of SEC disclosure requirements

Half think the new SEC disclosure requirements will **improve logging and reporting (53%)** and **improve security hygiene (52%)**.



Q11. How do you think the new Securities and Exchange Commision (SEC) disclosure requirements will impact your organization's vulnerability management practices? Select up to two

Figure 9

More than half of the surveyed organizations perceive regulatory compliance as an opportunity to enhance their vulnerability management practices rather than merely a regulatory burden.

These findings suggest that organizations recognize the need for improved vulnerability management practices, such as enhanced visibility and transparency into their cybersecurity posture and robust security hygiene, in order to more effectively reduce the attack surface and mitigate security risks.

However, the perceived negative impacts of the SEC requirements reflect apprehensions about increased bureaucracy. This tends to bring about resource allocation challenges in the form of administrative burdens, which take people, time and attention away from other cybersecurity objectives. This ties in with the anticipation that the regulatory requirements will distract security teams. These findings underscore the importance of effective resource allocation, clear communication, and strategic planning to ensure that compliance efforts do not compromise the organization's overall security posture. Organizations may need to invest in streamlining processes and implementing efficient workflows to mitigate the negative impact of increased bureaucracy.

The perception of increased pressure indicates some organizations expect heightened expectations and scrutiny regarding their cybersecurity efforts, particularly in relation to vulnerability management, and is likely part of the reason behind why we are seeing increased security investments (figs.1&2). Such findings emphasize the importance of effective vulnerability management practices in mitigating risks and demonstrating regulatory compliance.

Automation

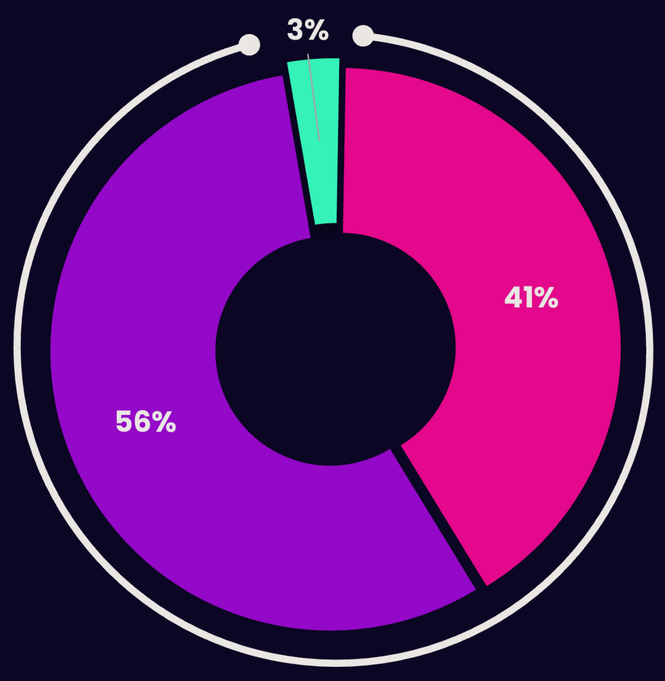
As cyber threats become more sophisticated, investing in security is vital to stay ahead. The report's findings indicate organizations recognize that enhanced cybersecurity budgets are essential to safeguard assets and maintain stakeholder trust.

Automation of vulnerability management process

Only 3% say their vulnerability management process is **not automated at all**.

97%

Automated



- **Fully automated** - every step of the process from discovery to fixing is automated
- **Somewhat automated** - some parts are automated, but we still rely on some manual methods
- **Not at all automated** - nearly every part of the process requires manual intervention

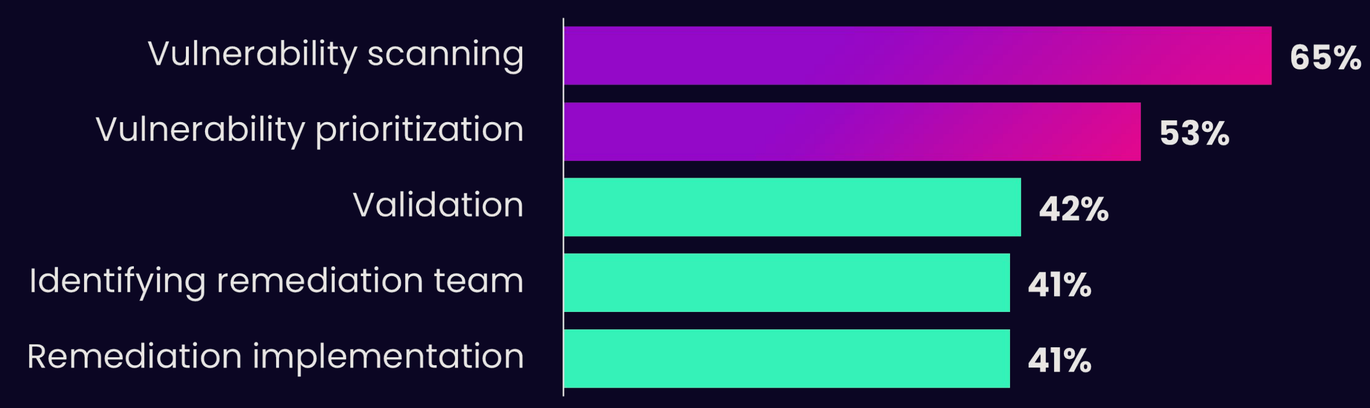
Q13. To what extent is your vulnerability management process automated? Select one

Figure 10

The high percentage of respondents (97%) indicating some level of automation suggests a growing recognition of the benefits of automation in vulnerability management. However, the fact that a sizable portion still relies on manual methods in *some* capacity (**somewhat automated**, 56%; **not at all automated**, 3%) indicates that there may be barriers to full automation.

Vulnerability management automation

Vulnerability scanning (65%) and **vulnerability prioritization (53%)** are **currently automated** within the organization.



Q15. Which specific tasks in vulnerability management are currently automated in your organization? Select all that apply

**Asked to those who have automated vulnerability management processes*

Figure 11

Automation is predominantly applied to the foundational steps in vulnerability management (**vulnerability scanning**, 65%; and **vulnerability prioritization**, 53%). But, there is also a notable level of automation in the remediation process (**identifying remediation team** and **remediation implementation**, both 41%), indicating a comprehensive approach to automating key stages of vulnerability management, further supporting the idea that organizations are recognizing the value of automation.

Vulnerability management task automation and its benefits

89%

say that automation has **improved vulnerability management efficiency**

Q16. How has automation impacted vulnerability management efficiency? Select one

**Asked to those who have automated vulnerability management processes*

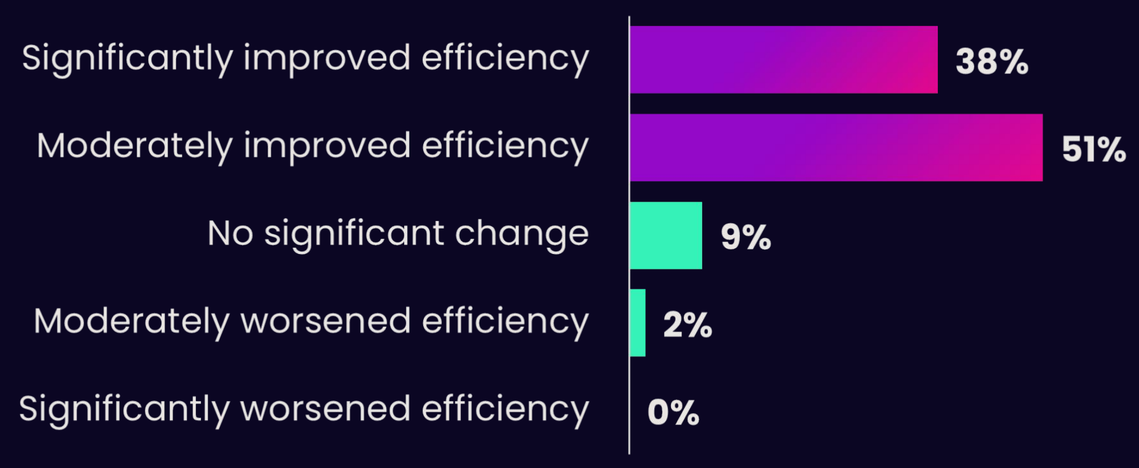


Figure 12

89% of respondents say automation has improved vulnerability management efficiency, with the top benefit being **faster response to emerging threats** (65%). The overwhelmingly positive response regarding the impact of automation on efficiency underscores its value in streamlining vulnerability management processes. As a result of the improved efficiency, automation has enabled organizations to respond more swiftly to threats, highlighting its transformative impact on vulnerability management practices.

Benefits of automating vulnerability management tasks

Faster response (65%) and **improved accuracy (60%)** are the **top benefits** of vulnerability management task automation

Q17. What benefits, out of the following, have you observed from the automation of vulnerability management tasks? Select all that apply

**Asked to those who have automated vulnerability management processes*

Figure 13

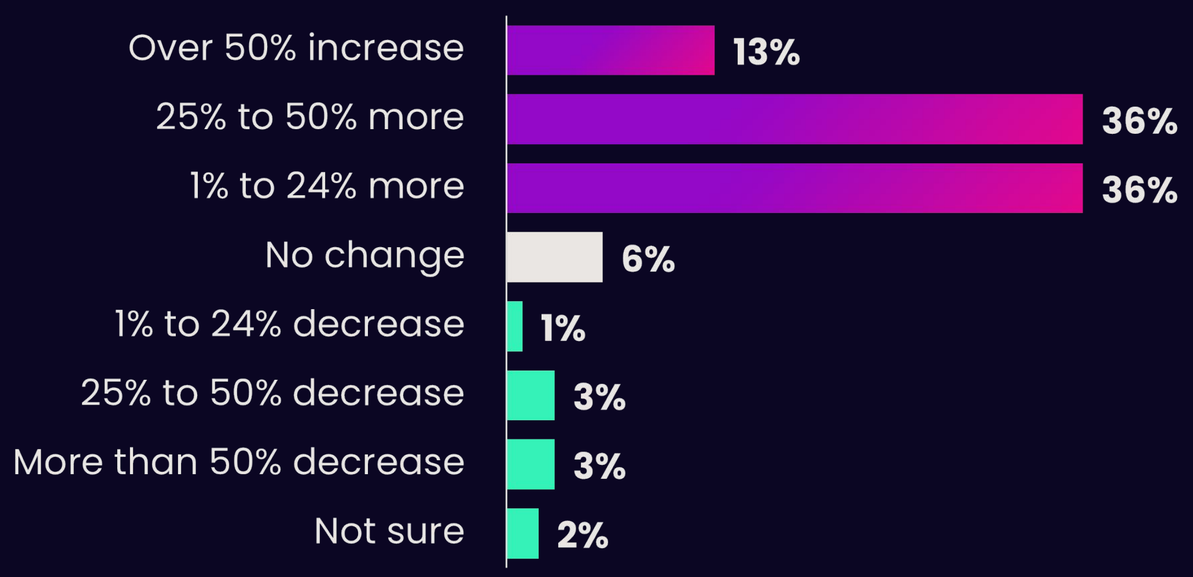
Overall, the findings collectively indicate a significant adoption and positive perception of automation in vulnerability management. This signifies a shift towards more automated and proactive approaches (tying in with the significant likelihood of adopting a CTEM framework), with organizations that embrace automation standing to gain a competitive advantage in managing risks effectively. Nonetheless, there are still areas where manual methods persist, such as in some parts of the remediation process. This suggests that automation here is still in its early stages, with few tools on the market providing such capabilities.

Artificial Intelligence

Artificial Intelligence (AI) is increasingly recognized as a crucial tool in cybersecurity, enhancing the accuracy of risk detection and streamlining vulnerability management processes. Organizations are investing heavily in AI to address evolving cyber threats, reflecting its growing importance in the industry. However, there is still some hesitation around AI's potential and the extent to which it should be used within cybersecurity - at least for now - due to its infancy.

Change in AI investments in the next 5 years

Majority (85%) of companies are **planning to increase its investment in AI in the next 5 years**.



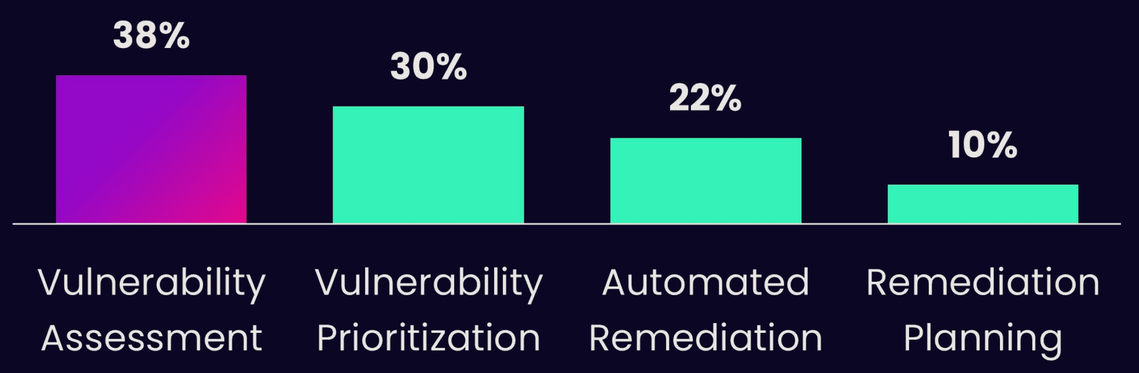
Q24. How much is your organization planning to increase or decrease investment in AI technologies in the next 5 years? Select one

Figure 14

The majority of companies (85%) are planning to increase AI investment in the next 5 years. The high level of planned investment in AI technologies underscores the perceived importance of AI in addressing cybersecurity challenges. Organizations recognize the potential benefits of AI and are willing to allocate resources to harness its capabilities.

AI and vulnerability management

38% say **vulnerability assessment would benefit the most** from AI integration.



Q18. What aspect of vulnerability management do you think would most benefit from AI integration? Select one

Figure 15

Respondents believe AI will have the most significant impact on the initial stages of vulnerability management (**vulnerability assessment**, 38%; and **vulnerability prioritization**, 30%). By leveraging AI in these areas, organizations can streamline their vulnerability management processes and focus their efforts on addressing the most critical security risks.

Impact of AI in cybersecurity

Almost two thirds (64%) perceive the role of AI in cybersecurity as **a weapon against bad actors**.

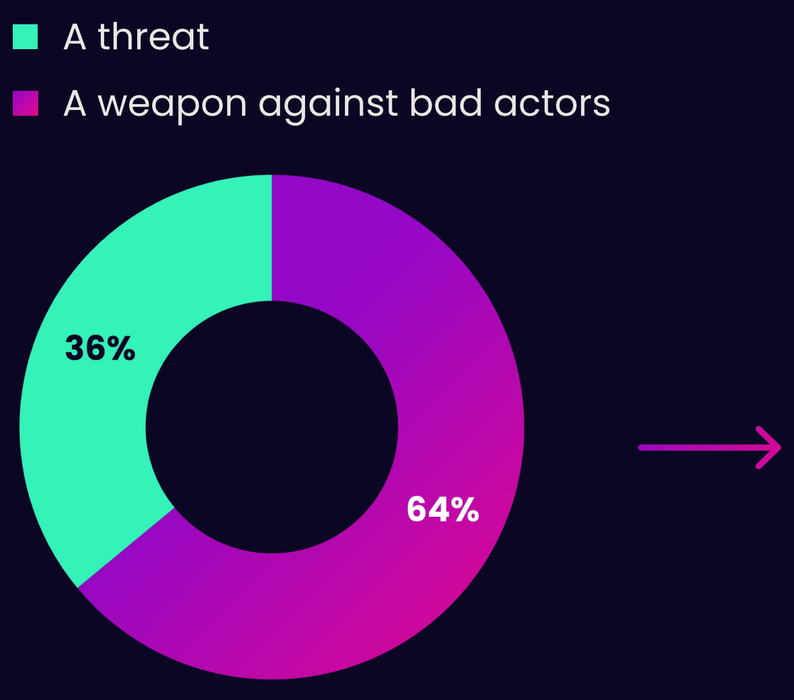


Figure 16

Q20. Which of the following best describes how you perceive the role of AI in the overall context of cybersecurity? Select one

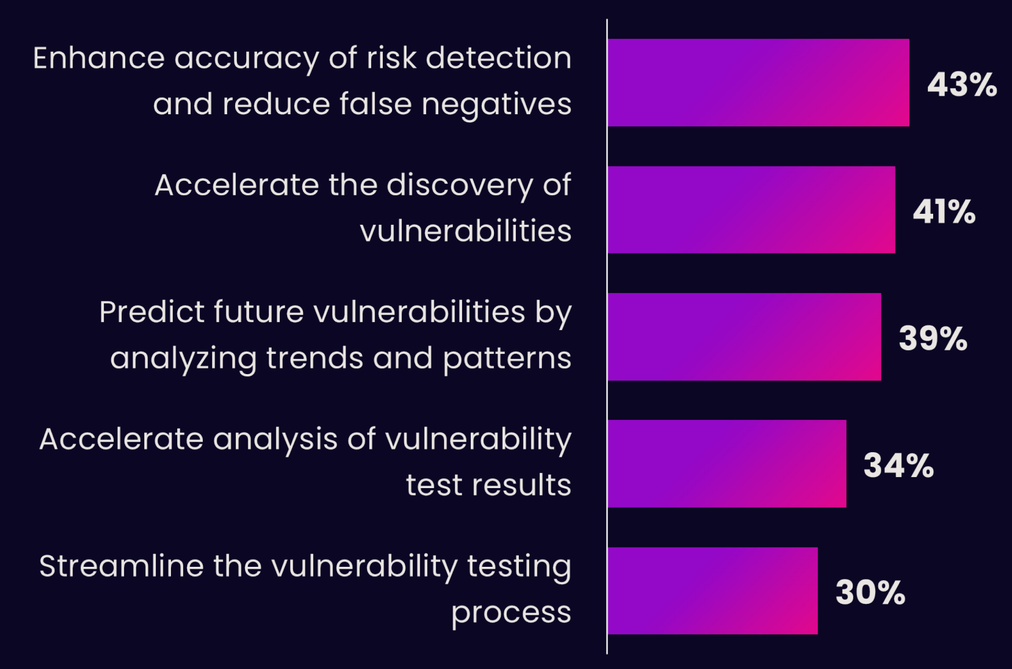


Figure 17

Q22. Which cybersecurity areas do you feel AI will most positively impact? Select up to two

The predominant perception (64%) of AI as a weapon against bad actors reflects optimism about its potential to bolster cybersecurity capabilities. The top positive impact being **enhanced accuracy of risk detection and reduced false negatives** (43%) shows the value of AI as a strategic asset in combating one of the most widespread challenges in the industry - noise (see Noise).

AI and vulnerability management

68% are concerned vulnerability management **will become more difficult** with AI integrated into software development.

Q19. How concerned are you that vulnerability management will become more difficult with AI integrated into software development? Select one

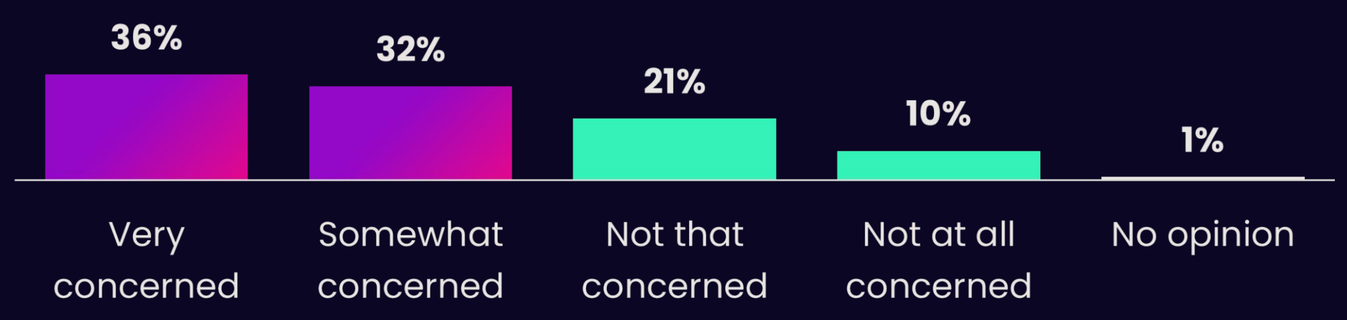


Figure 18

There is significant concern (68%) regarding the impact on vulnerability management that the integration of AI in software development will have. AI will rapidly speed up code development at a pace that security teams cannot keep up with, making effective vulnerability management a challenge.

Cybersecurity risk management and AI

Half (50%) agree that AI could **complement** human decision making in cybersecurity risk management but **not fully replace it**.

Q23. To what extent do you believe AI could eventually replace human decision-making in cybersecurity risk management? Select one

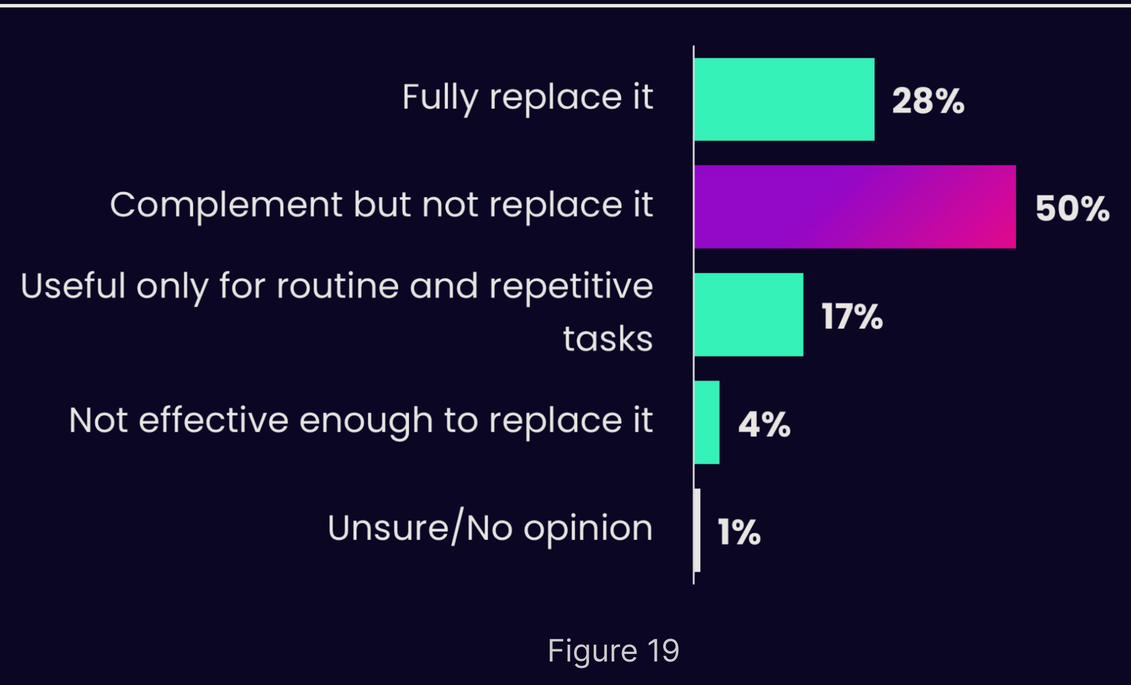


Figure 19

The mixed views on the potential for AI to replace human decision-making in cybersecurity risk management reflect the complexity of this topic. While AI has the potential to automate routine tasks and enhance decision-making processes, human expertise and judgment remain critical in addressing complex and evolving cyber threats. At this stage, respondents are not convinced that AI will ever be capable of fully mimicking these human factors.

Next Steps

The 2024 Remediation Operations Report uncovers the dynamics of cybersecurity in 2024, revealing key trends and insights that have significant implications for organizations worldwide. The exponential growth in security budgets underscores the increasing recognition of cybersecurity as a top priority, while the proliferation of diverse security tools and vendors highlights the complexity and fragmentation within the industry.

The challenge of managing tool noise and the significant interest in CTEM underscore the need for proactive and streamlined vulnerability management strategies. Automation and artificial intelligence emerge as powerful allies in this endeavor, promising to enhance efficiency and accuracy in identifying and mitigating security risks. Nonetheless, artificial intelligence is still met with some reservation and skepticism due to its infancy and its risks have not gone unnoticed.

Going forward, organizations must embrace a holistic approach to cybersecurity, leveraging a variety of tools, techniques and technologies to fortify their defenses against evolving threats. By staying ahead of emerging trends and adopting innovative strategies, organizations can navigate the complexities of the cybersecurity landscape with confidence and resilience.

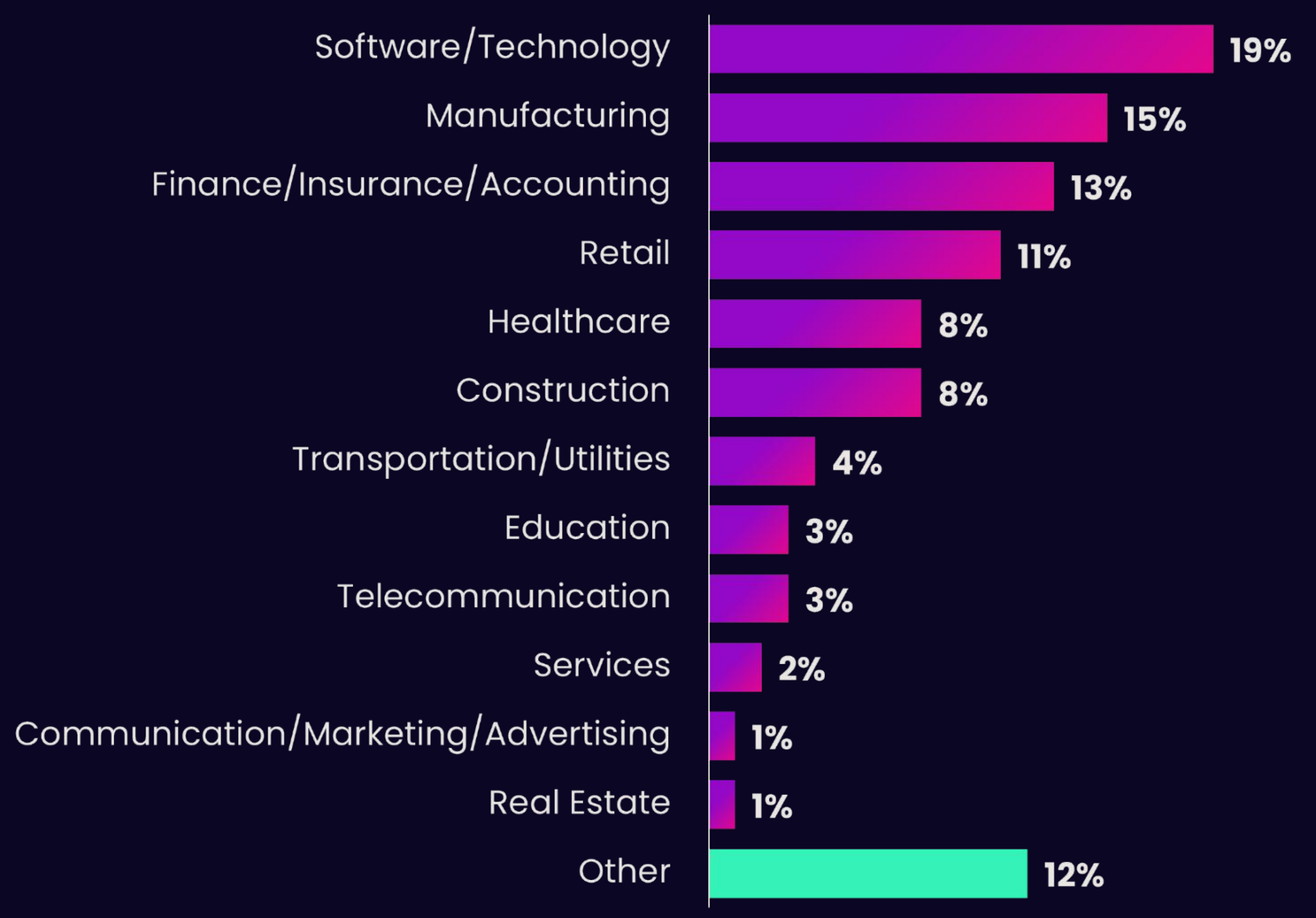
Methodology and Respondents

This research was a joint effort between Seemplicity and Sapio Research. Seemplicity's leading Remediation Operations platform revolutionizes the way security teams drive and scale risk reduction efforts across organizations by orchestrating, automating, and consolidating all remediation activities into one workspace. 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.

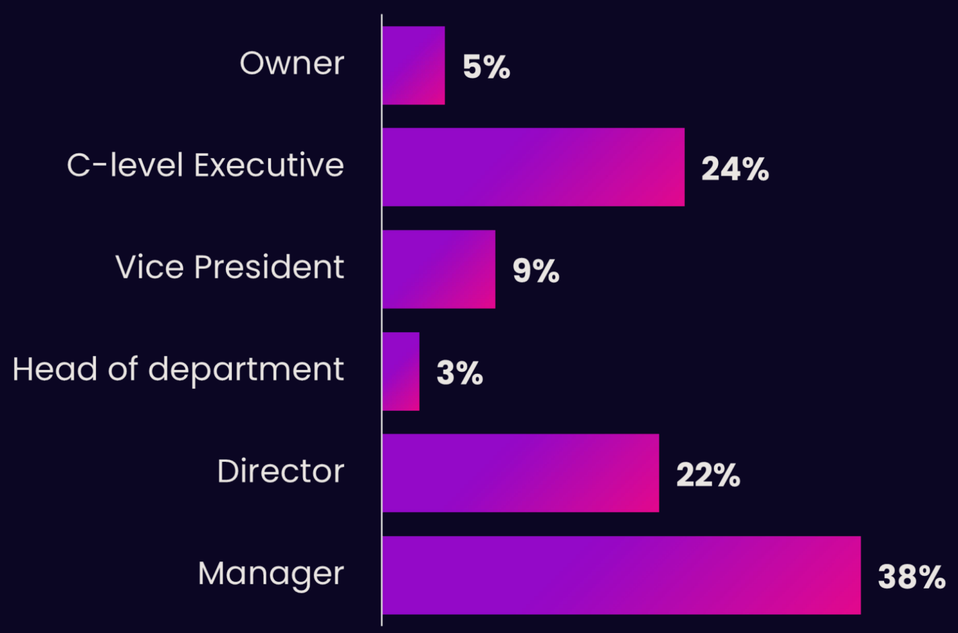
Industry



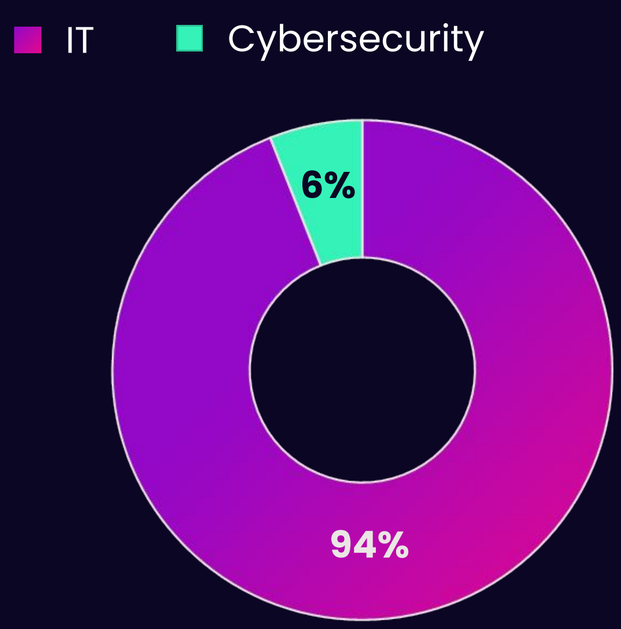
S2. Which of the following categories best describes the industry you work for? Select one

Figure 20

Job Role

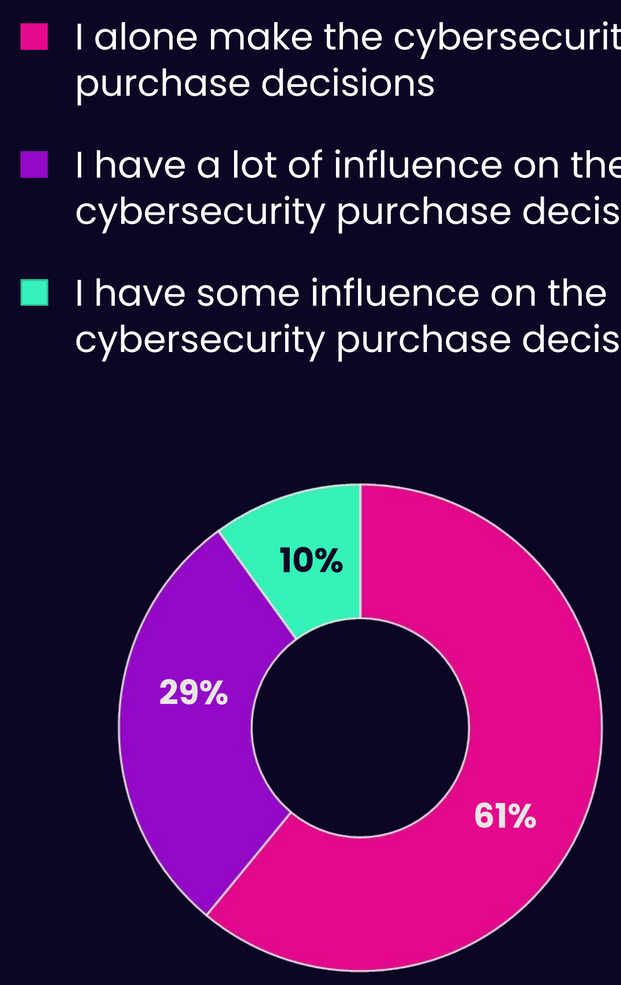


Job Function



Company Size

Influence Over Cybersecurity Purchases



Annual Revenue