FORTRA™

2023 Penetration Testing Report

Introduction

Since penetration testing encompasses a great variety of security assessments, tools, and services, there is no set formula for the creation and maintenance of a pen testing strategy. For those wanting to successfully incorporate pen testing into their own cybersecurity program, this can present a challenge, with no clear place to look to as a guiding example.

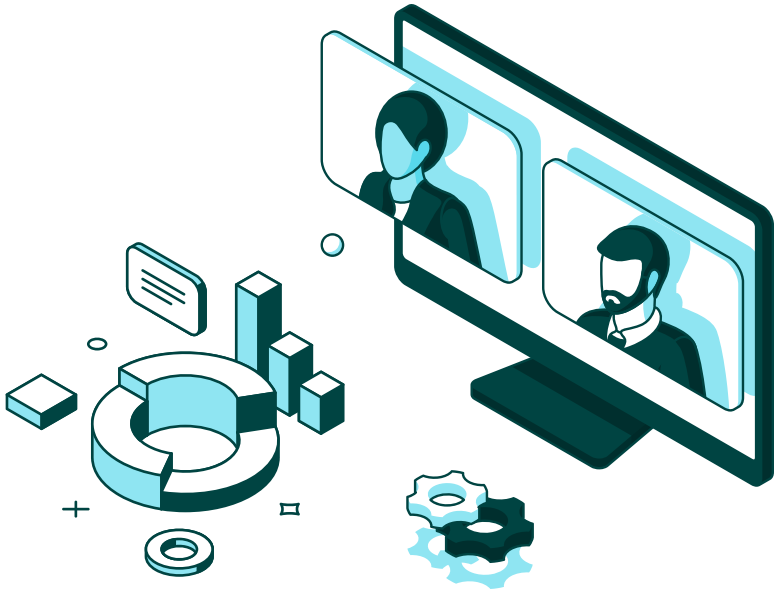
In general, cybersecurity has become tied to an organization's reputation, with a breach having the potential to severely damage their standing. Unfortunately, this can create an environment in which everyone is reticent to share any aspect of their security journey. However, knowledge sharing and analysis is a critical part of defining best practices and presenting a united front against threat actors. With over a decade of specialized experience, Fortra's Core Security developed a penetration testing survey in order to get a better picture of how cybersecurity professionals are using penetration testing in the field, including pen testing strategies and the resources required to deploy a successful pen testing program.

Now in its fourth year, this survey continues to track year-over-year changes, trends, challenges, and areas of improvement. The data collected provides visibility into the full spectrum of pen testing's role, helping to determine how these services, tools, and skills must evolve. This year, we continue to see slight shifts in the role penetration testing plays in the cybersecurity landscape and identify how broader trends, like the global economy, can influence its role.

The results are explored in detail in this report, providing valuable data on the following key issues related to pen testing:

- Top security concerns like ransomware, phishing, and misconfigurations
- Testing frequency and remediation
- Compliance concerns
- Pen testing in different environments
- In-house pen testing team efforts and challenges
- Using and selecting third-party teams
- Evaluating pen testing toolsets
- Integrating pen testing with other security assessment tools

We'll show a comparison to the results of the 2022 survey and uncover new insights, analyzing the general evolution and advancement of the penetration testing field.



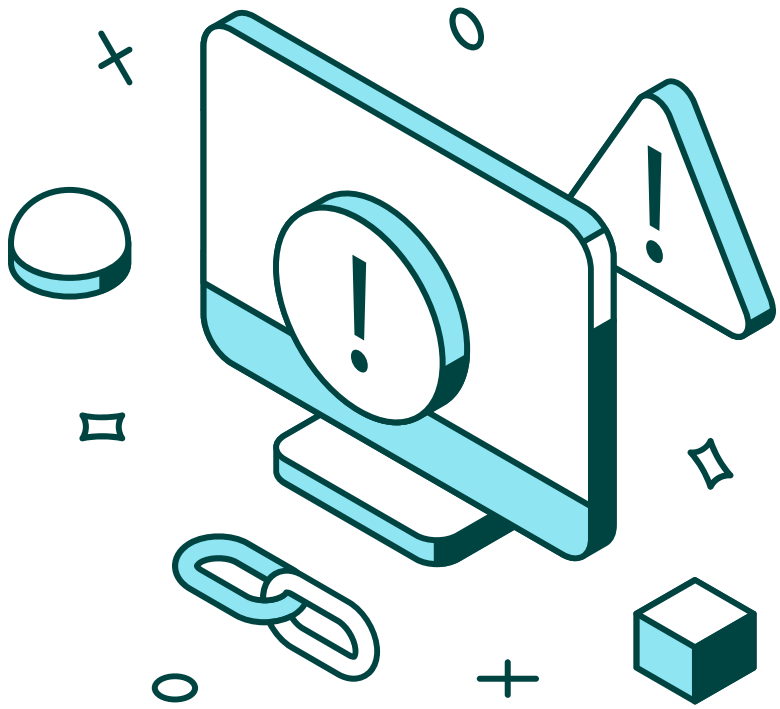
Reasons for Pen Testing

Organizations pen test for multiple reasons, with 69% reporting they perform pen tests for risk assessment and remediation prioritization, 62% for vulnerability management program support, 58% for compliance and external mandates, and 40% for internal or company specific mandates (Figure 1).

Risk assessment and remediation prioritization are foundational offensive security practices, helping identify security weaknesses in an IT environment and determining which have the most potential for harm. This provides guidance for organizations on where to allocate resources for mitigation. Those respondents who reported solely using pen testing for risk assessment and remediation prioritization may be relying on a more ad hoc security approach.

However, risk assessment is a key component of any vulnerability management program, which is an established strategy of identifying, classifying, prioritizing, and remediating weaknesses in an IT environment. While a penetration test will always provide helpful insights, organizations can achieve more with a formalized program, in which tools can work in tandem to provide maximum coverage and impact.

External and internal mandates are also related to one another, in that they both set cybersecurity standards to which organizations must adhere. The key difference is that external mandates are set by regulatory bodies, government agencies, or some other entity while internal mandates are company specific. Because external mandates are enforceable by law and can impose fines or other consequences, they are typically given priority over internal mandates, which the data seems to suggest. However, it is still worth having internal mandates, as they are written with the specific needs of the organization in mind and often go beyond the baseline of cybersecurity that is set by external regulations.



Reasons for Pen Testing

Why does your organization perform penetration tests?

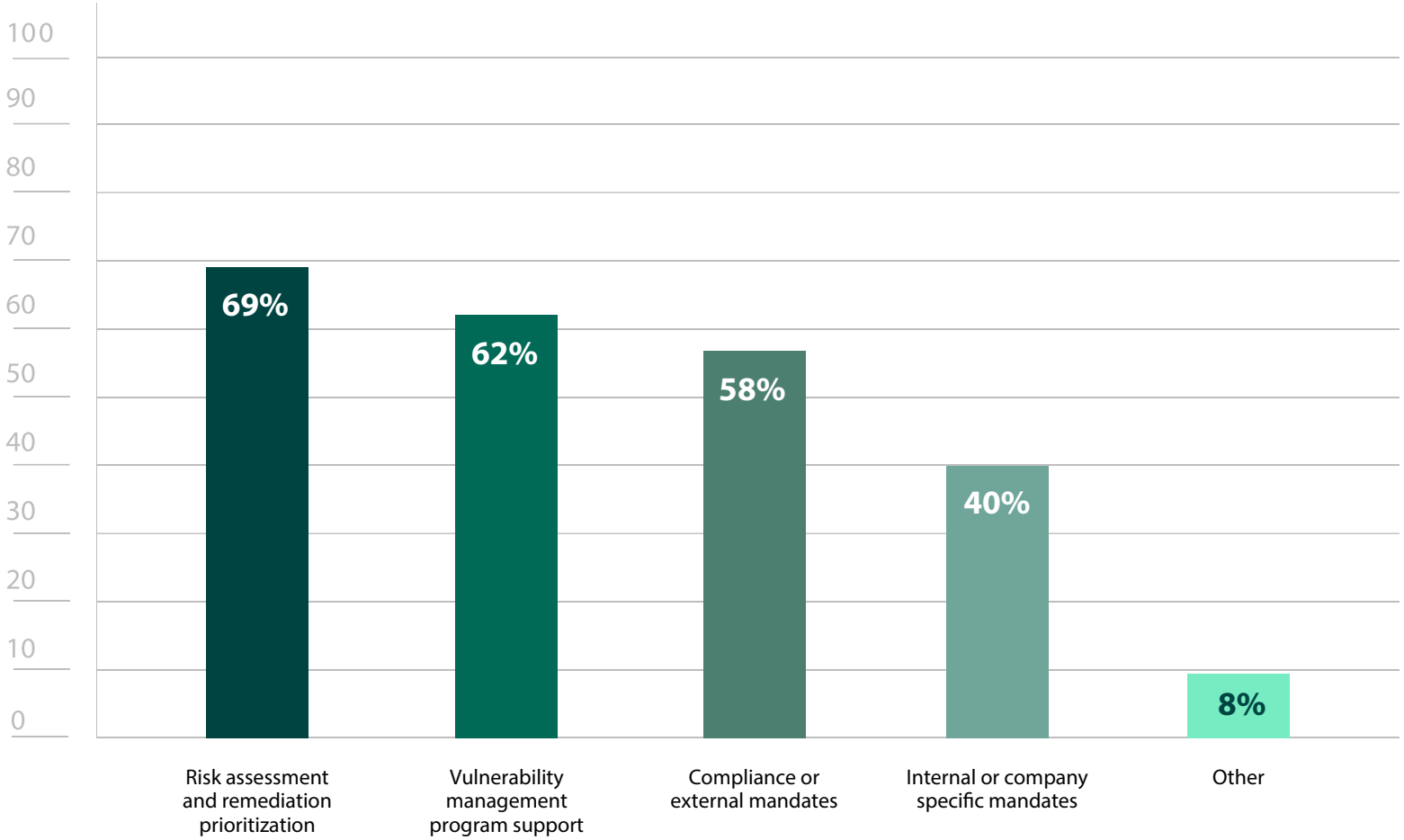


Figure 1: Reasons for performing penetration tests

Common Security Concerns

Ransomware (72%), phishing (70%), and misconfigurations (58%) were once again the top security concerns (Figure 2) for survey respondents. According to Verizon's *2022 Data Breach Investigations Report*, there was a 13% increase in ransomware breaches, accounting for 25% of all breaches. With ransomware on a seemingly endless upward trajectory, it's unsurprising that it is the most common concern this year. Ransomware is also closely linked with phishing, with phishing emails serving as the number one delivery method for ransomware payloads.

Additionally, unintentional internal threats (54%) were the fourth top concern (Figure 2). This is a large category of threats that consist of any actions from employees, contractors, or third-party vendors that inadvertently result in security incidents. This may include misconfigurations, failure to follow security policies (i.e. strong passwords, ignoring software updates, etc.), or even losing one's employee ID card.

Though part of the broader category of unintentional internal threats, misconfigurations were actually a slightly bigger concern for respondents. This may be due to how widespread they've become. As IT infrastructures continue to grow in complexity, there is that much more potential for errors and oversights in the configuration of hardware, software, or network settings. Unfortunately, misconfigurations throw the door for attackers wide open, and were ultimately responsible for 14% of all breaches in 2022.

Supply chain attacks (44%), in which a malicious actor compromises an outside partner or supplier to conduct attacks against the supplier's customers, can also occur as a result of unintentional internal threats. This strategy is increasingly popular amongst attackers. In fact, the Verizon report stated that 61% of system intrusion incidents were supply chain attacks. Unsurprisingly, ransomware is often used in supply chain attacks, making the concern around it all the more justified.

All of these concerns share one thing in common: the inescapable threat that employees inadvertently pose to organizations.

Common Security Concerns

What common security risks/entry points are you most concerned about?

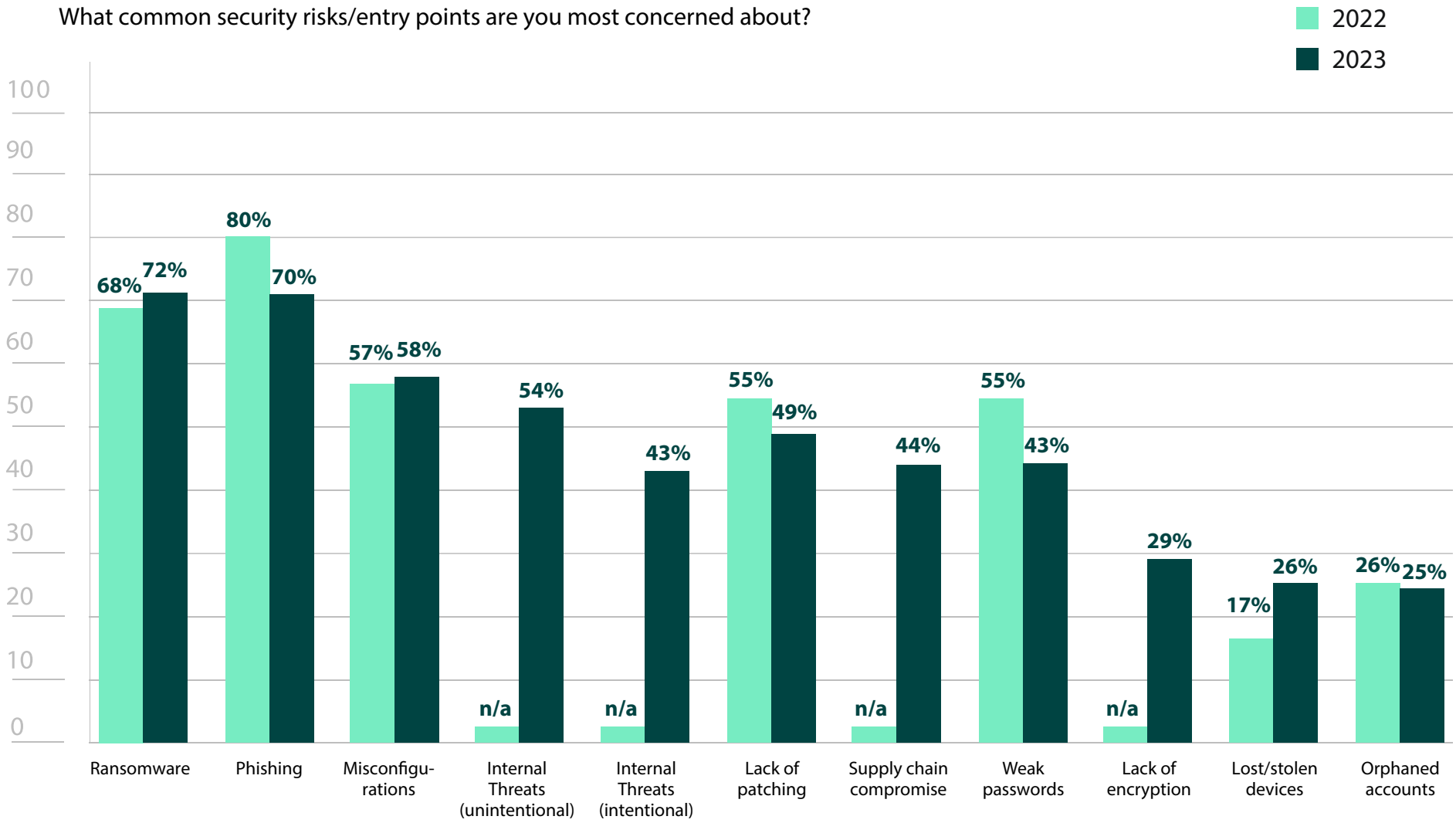


Figure 2: Common security concerns

General Pen Testing Challenges

Feelings on the value of penetration testing remain the same, with 94% of respondents once again noting that penetration testing is at least somewhat important to their security (Figure 4).

While the view on the import of pen testing remained steady, there were some changes in the challenges that are being encountered in pen testing. First, trouble getting a qualified third-party is notably reduced, down 15% from 2022 (Figure 3). Pen testing is a rapidly growing market, with research predicting to see a market growth of $2.6 billion by 2030. This means more third-party service offerings to choose from every year. However, such growth makes it worth exercising extreme caution when choosing a service provider, as the quality will vary greatly. Many focus on basic, routine tests that are performed with a pen testing tool, packaging it as a custom service. It's critical to find a partner with experts that can tailor their tests for your needs and goals, and even advise you on the different testing options.

There was also a concerning increase in the lack of resources to act on the findings of a pen test, up 23% from last year (Figure 3). While pen testing is an effective means of determining the quality of an organization's security and flagging which weaknesses are putting you most at risk, the only way to improve your security posture is to follow through with actions that close those security gaps, such as patching, reconfiguration, or implementing new policies. Penetration testing should not be seen as a box to check, but rather a map that needs to be followed. Equally important is repeating pen tests after the remediation process to validate that fixes were properly implemented.

Lastly, while the 15% drop in security posture confidence (Figure 3) may appear concerning at first glance, it is actually best to err on the side of caution when it comes to cybersecurity. Overconfidence often translates into stagnation and rigidity, feeling no need to reevaluate if all appears well. However, cybersecurity requires constant appraisal and flexibility, readjusting and pivoting as attackers find new techniques, tactics, and vulnerabilities. This 15% drop could reflect that the reality of the current threat landscape is setting in.

General Pen Testing Challenges

What challenge(s) does your organization face with your penetration testing program?

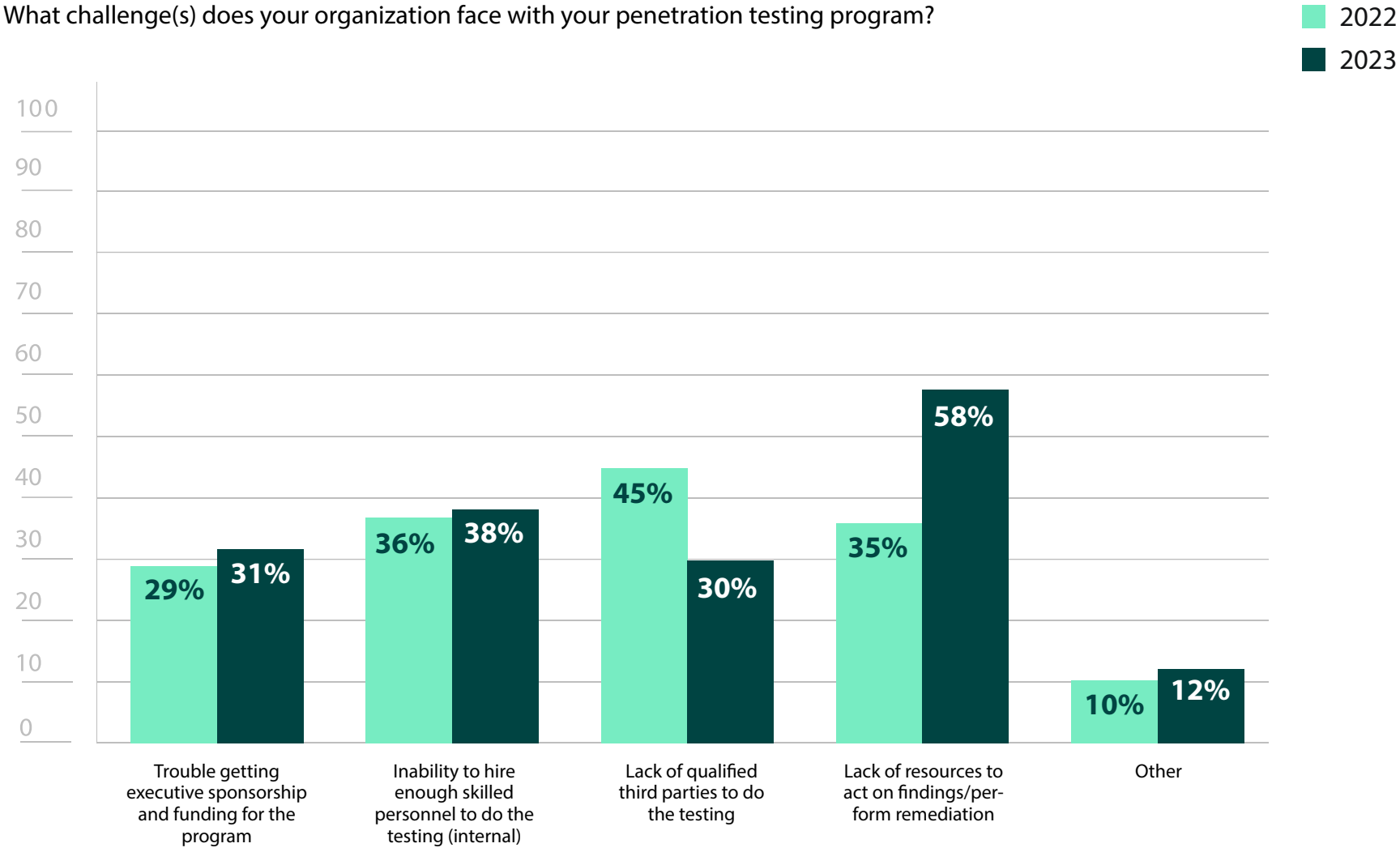


Figure 3: Pen testing challenges

General Pen Testing Challenges

How important is penetration testing to your organization's security posture?

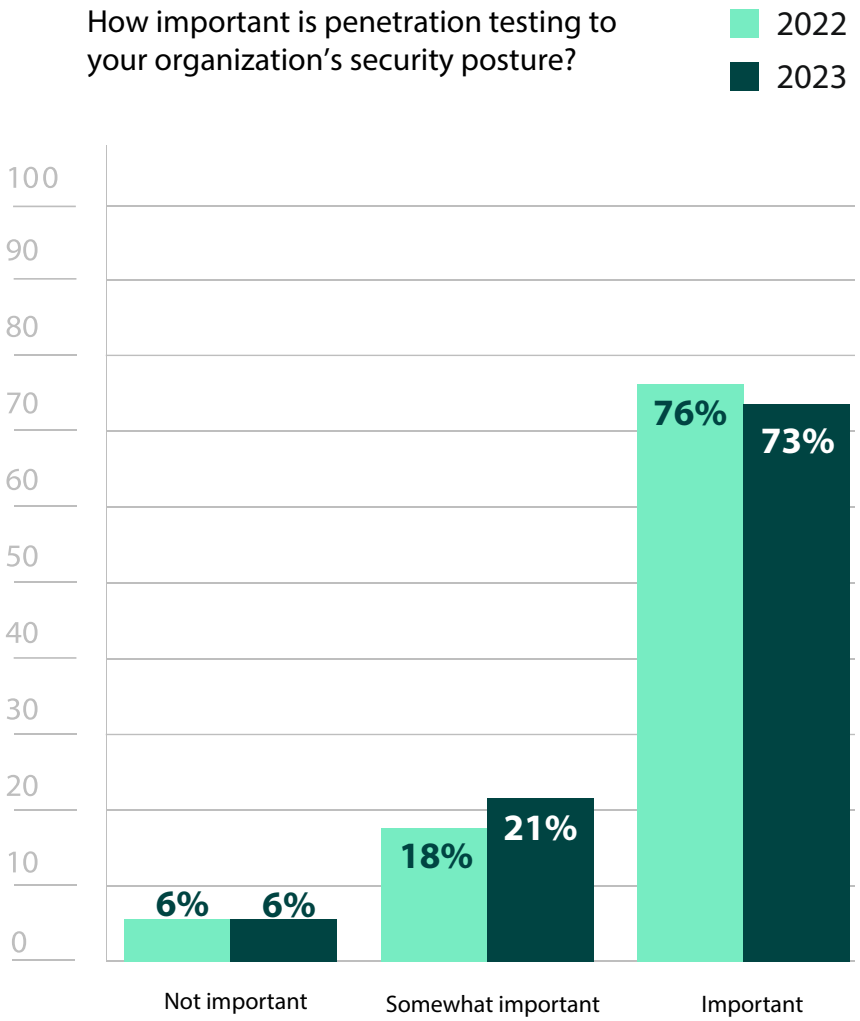


Figure 4: Importance of penetration testing

How confident are you in your organization's security posture?

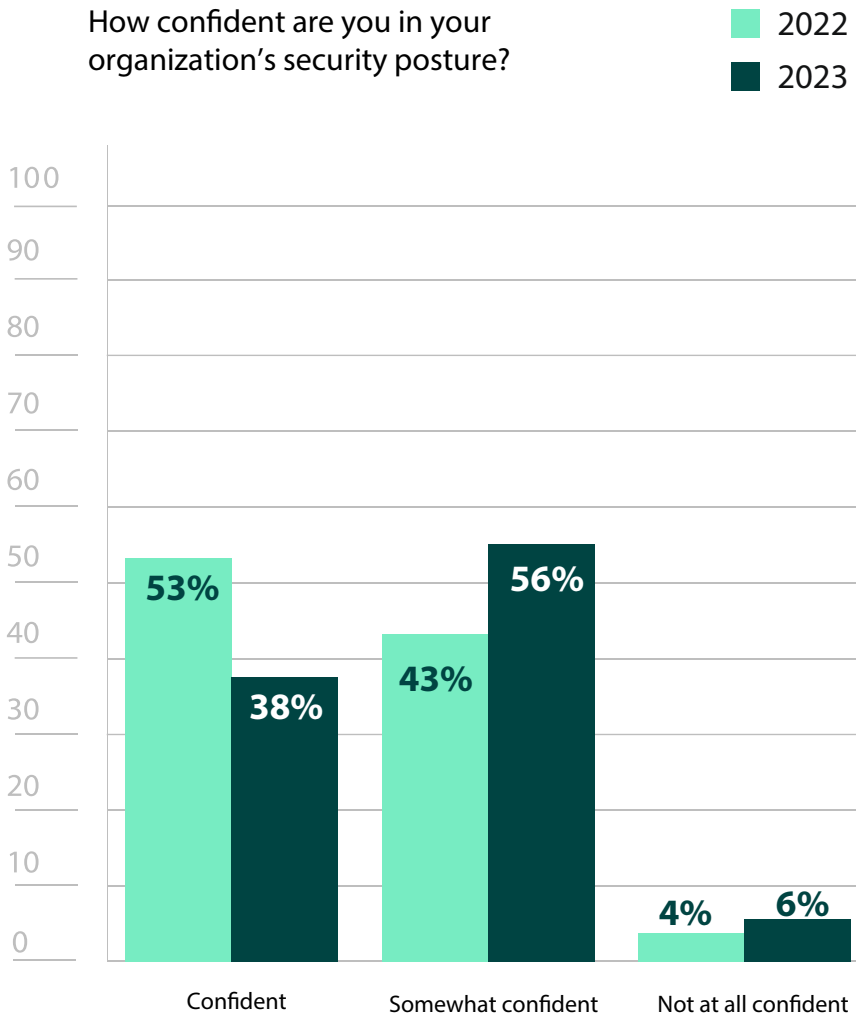


Figure 5: Confidence in security posture

Compliance and Pen Testing

Regulations like HIPAA, PCI DSS, SOX, GDPR, or the CMMC mandate appropriate protection of highly sensitive data, like credit card numbers, social security numbers, and other personally identifying information. Pen tests are not only a way to evaluate an organization's security posture, but they can also help verify adherence to these regulations, proving to auditors or other authorities that mandated security measures are in place or working properly.

Though there was a decline from last year, pen testing was still at least somewhat important to compliance initiatives for 93% of respondents (Figure 6). Interestingly, with an increase in the number of data protection and security laws and regulations, pen test needs surrounding compliance only seem to be growing. 41% of respondents have increased the number of overall pen tests in response to these mandates (Figure 7).

Compliance initiatives show no signs of slowing, either. The European Commission is revising the GDPR in 2023 to streamline cross-border instances of data protection enforcement. Not only are existing regulations being continually updated to incorporate new measures, new laws and regulations are also emerging. For example, in 2022, nearly every US state put forth cybersecurity bills. Additionally, the 2023 National Cybersecurity Strategy includes a proposal to expand requirements for all operators of critical infrastructure. According to Gartner, three quarters of the world's population will be under privacy regulations in 2023.

While some had to increase the number of pen tests in response to compliance initiatives, others had to shift their strategies in some other way, whether it was expanding the scope of their tests (29%), adding more internal staff (23%), or placing more emphasis on certain types of tests, like web application (35%) or social engineering (36%) (Figure 7). Only 16% of respondents reported that there was no impact to their pen testing strategies as a result of compliance needs, illustrating the influence compliance continues to have on pen testing approaches.

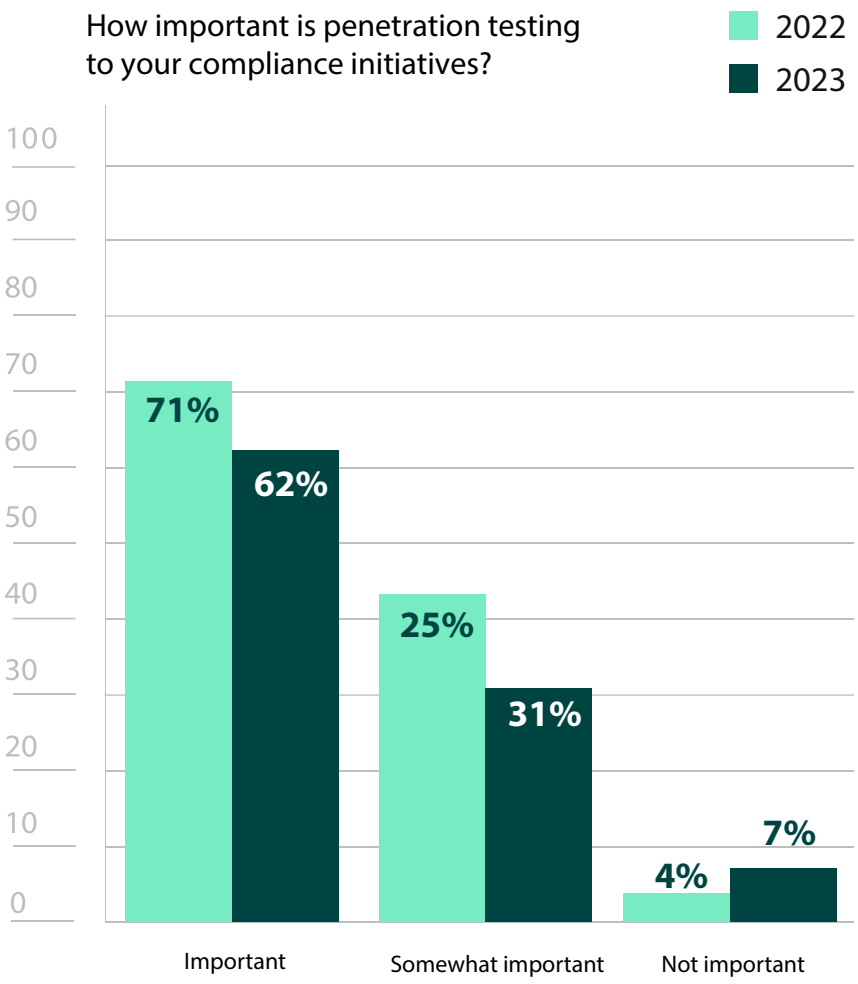


Figure 6: Importance of penetration testing for compliance

Compliance and Pen Testing

How has the increase in compliance regulation/mandates affected your pen testing strategy or priorities?

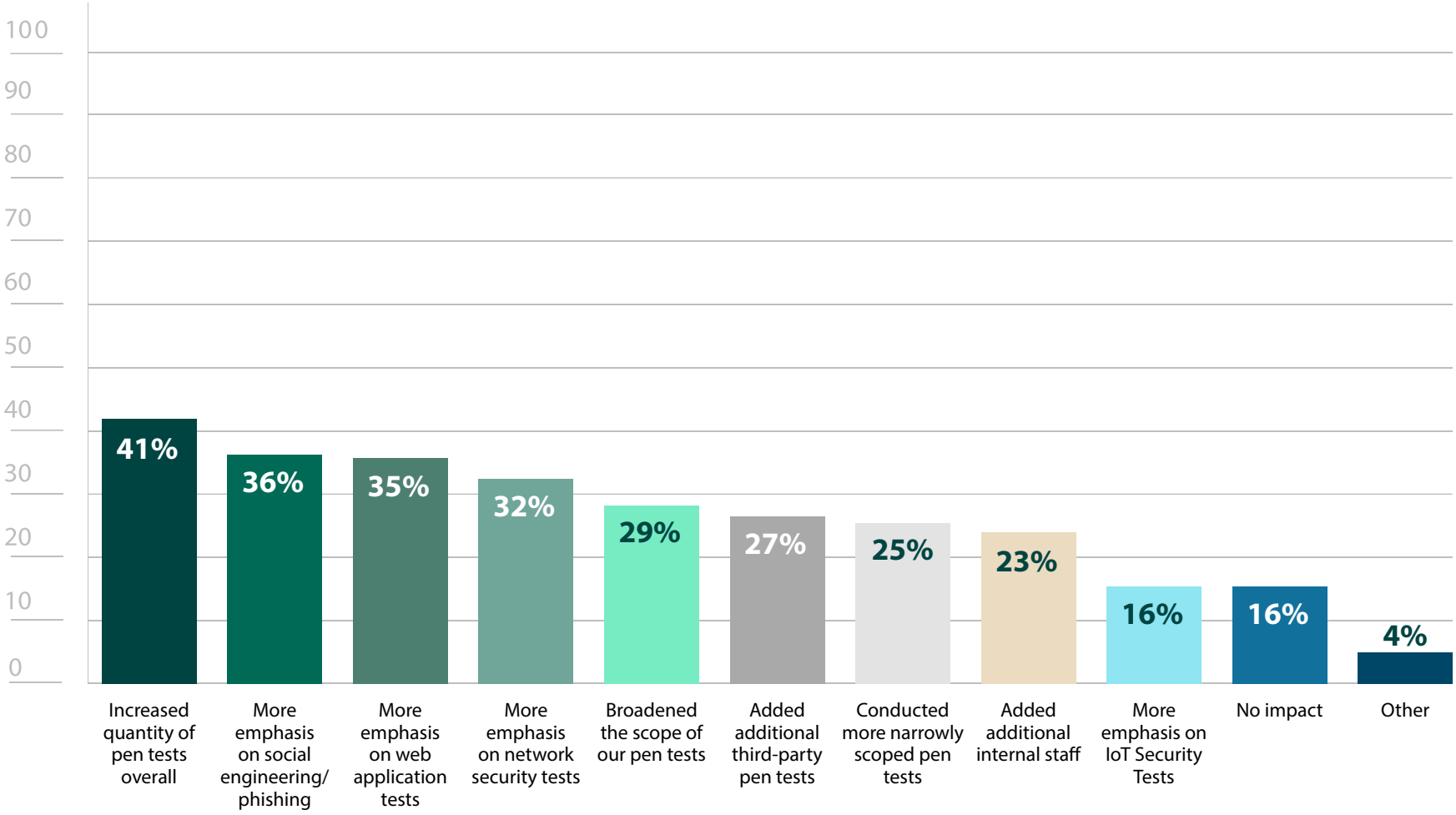


Figure 7: Impact of compliance mandates on pen testing strategies

Phishing

With the Anti-Phishing Working Group observing a record 1,270,883 total phishing attacks in Q3 of 2022 alone, it's unsurprising that phishing is a top security concern of respondents (70%) (Figure 2).

Since phishing is one of the oldest attack tactics around, how has it remained so pervasive? Ultimately, it's the human element of phishing that has kept it remarkably effective. People receive so many messages and emails that it's easy to become careless, clicking on links while your mind is elsewhere. Others overly rely on spam filters, which attackers have become adept at evading. Spear phishing techniques have also improved, with everything seemingly personalized and appearing so authentic that even a cybersecurity pro could be fooled.

Though phishing attacks will persevere, one of the best defenses is to keep people on their toes. Running regular phishing simulation exercises can help serve as a regular initiative to keep users vigilant and train them to exercise more precaution.

With this in mind, it was encouraging to see an 8% increase in monthly phishing simulations (Figure 8), which is a good cadence to promote ongoing awareness. New and existing regulations have also underscored the threat phishing poses, with 36% of respondents noting that compliance initiatives have placed an increased emphasis on social engineering tests (Figure 7). This may also be reflected in the 16% increase in the usage of third-party testing services for social engineering tests (Figure 19).

With generative AI making sophisticated phishing emails and texts the norm, easy ways to spot attacks like spelling and grammar errors may soon become a thing of the past. Instead, users need to question the intent of the email and whether the request makes sense. Do you often receive emails from this person? Is this how an application allows asks you to authenticate your credentials? By running routine phishing simulation campaigns with follow up reports and trainings, organizations can foster a culture of healthy skepticism.

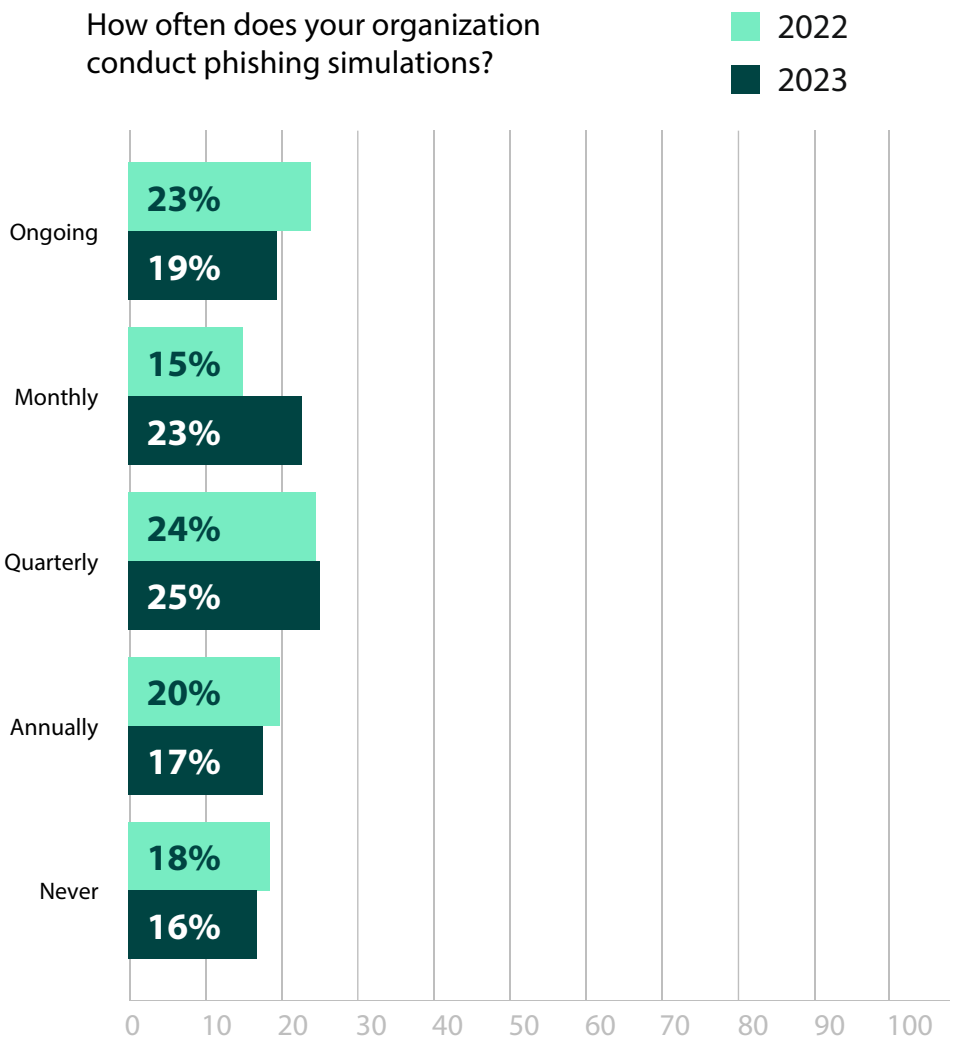


Figure 8: Frequency of phishing simulations

Penetration Testing Frequency

Results for pen testing frequency have remained consistent. As in 2022, the majority of respondents are, at most, pen testing only a few times a year. While running one to two pen tests (38%) is far better than nothing (14%) (Figure 9), it does raise concerns about retesting. An initial test provides guidance on remediation, but a retest is critical for ensuring these vulnerabilities have been successfully mitigated. Improperly applying a patch may not just leave the vulnerability intact, it can also open new security gaps. Remediation validation should not just be left for the next year's round of testing. However, when resources are limited, making a business case for retesting may prove difficult. This aligns with the finding of respondents encountering challenges with the lack of follow up (58%) from pen tests (Figure 3).

Running too few tests isn't ideal, but running daily or even weekly pen tests may be impractical, since they do require the already scarce resources of time, budget, and talent. In order to run daily pen tests, you would need to have a large pen testing team. Even then, they would likely only be able to run smaller pen tests on different parts of the infrastructure—running a large scope pen test every single day would be a difficult challenge. However, though 8% of respondents reported daily pen testing (Figure 9), just 50% of those respondents had internal teams of more than five team members. For the other 50%, it may be that they are instead referring to the frequency with which vulnerability scans are being run. Vulnerability management solutions are typically highly automated and can easily be scheduled to run on a daily basis, while pen testing requires more advanced planning.

Those running monthly (12%) or even quarterly (20%) tests (Figure 9) are more likely to have achieved a balance, having the means for testing and retesting without placing a strain on resources. However, penetration testing frequency is a perfect example of where best practices collide with real world practicalities. Every security team will have to determine their needs while keeping resources and budgets in mind.

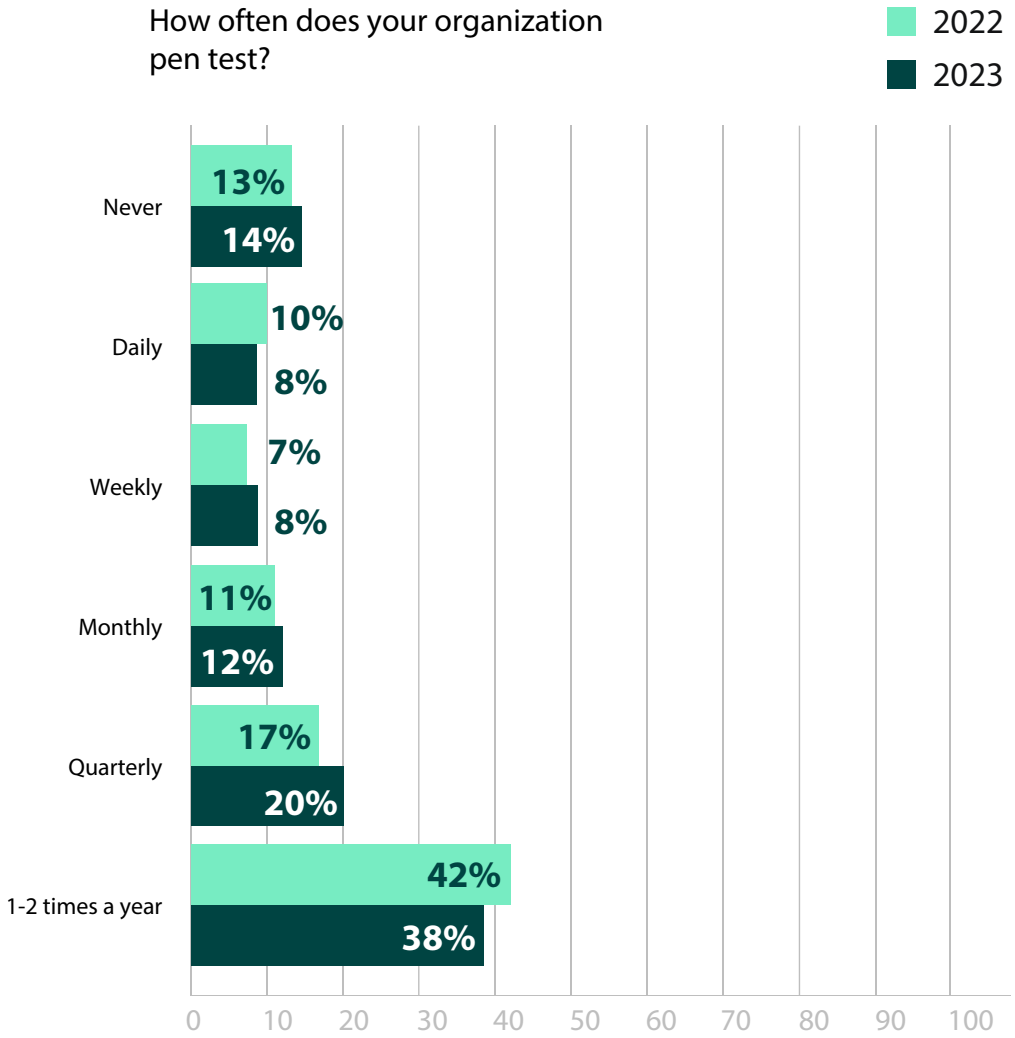


Figure 9: Frequency of penetration testing

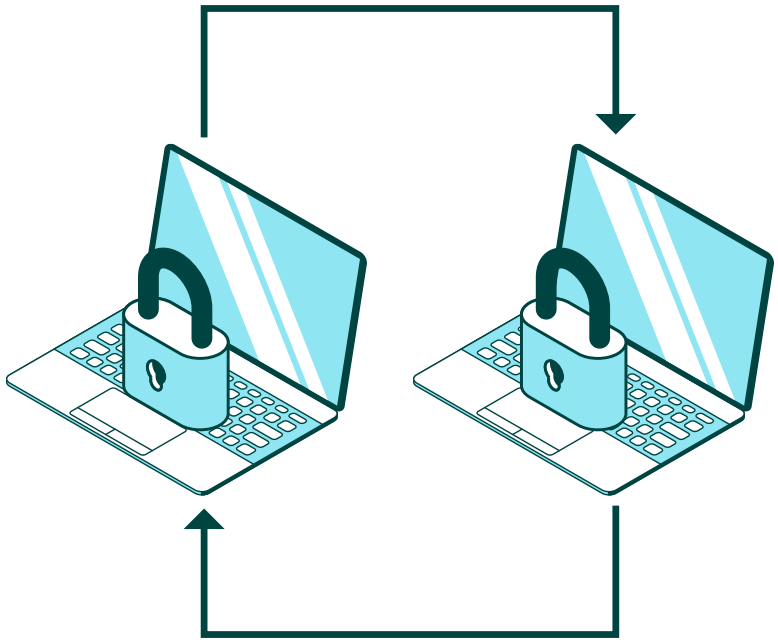
In-House Penetration Testing Efforts

Having pen testing capabilities in-house can quickly expand pen testing efforts, allowing for more frequent tests and coverage of a wider scope of the IT infrastructure. It also ensures that changes to the infrastructure are more efficiently assessed to ensure new security gaps aren't opened. This year shows a small amount growth of in-house pen testing efforts, with a 7% increase from last year in the number of respondents who have an internal pen testing team at their organization (Figure 10).

Curiously, the size of pen testing teams seems to be fluctuating, with teams both growing and shrinking. While there is a 21% increase in the number of teams with 3-5 members, there is an 11% decrease in the number of teams with 1-2 members and 10% decrease in teams of 6 or more (Figure 11).

The decrease in larger teams may be illustrative of the cybersecurity skills gap, which continues to persist. In fact, according to (ISC)²'s *2022 Cybersecurity Workforce Study*, the cybersecurity workforce gap has grown more than twice as much as the workforce with a 26.2% year-over-year increase. In a field with so many job openings, it wouldn't be uncommon for there to be more turnover and instability in team size. Pen testing tools may be helping offset the skills gap, with a 14% increase in the number of respondents who cited that pen testing technology has at least some influence on an organization's decision on having an in-house team (Figure 14).

While there was an increase in the number of respondents with in-house pen testing teams, there were still more respondents who either had lost their in-house team or never had one to begin with. Reasons for the lack of an in-house team vary, with top reasons being insufficient need (48%), lack of talent (36%), and lack of funding (28%) (Figure 13). Interestingly, there is a 12% decrease in respondents citing insufficient need for a full-time pen testing team. This may reflect a growing acknowledgement of the usefulness of in-house pen testing teams, or even pen testing in general.



In-House Penetration Testing Efforts

Do you have an in-house penetration testing team?

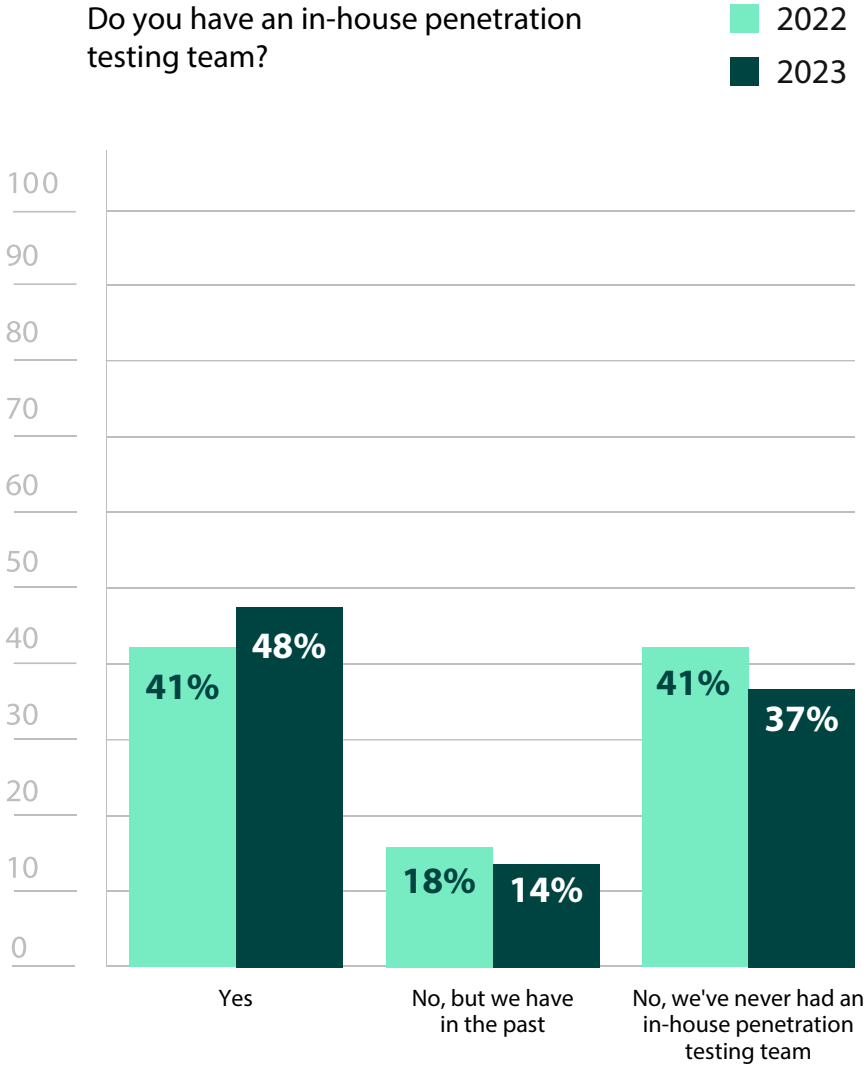


Figure 10: In-house penetration testing

How many dedicated team members does your in-house penetration testing team have?

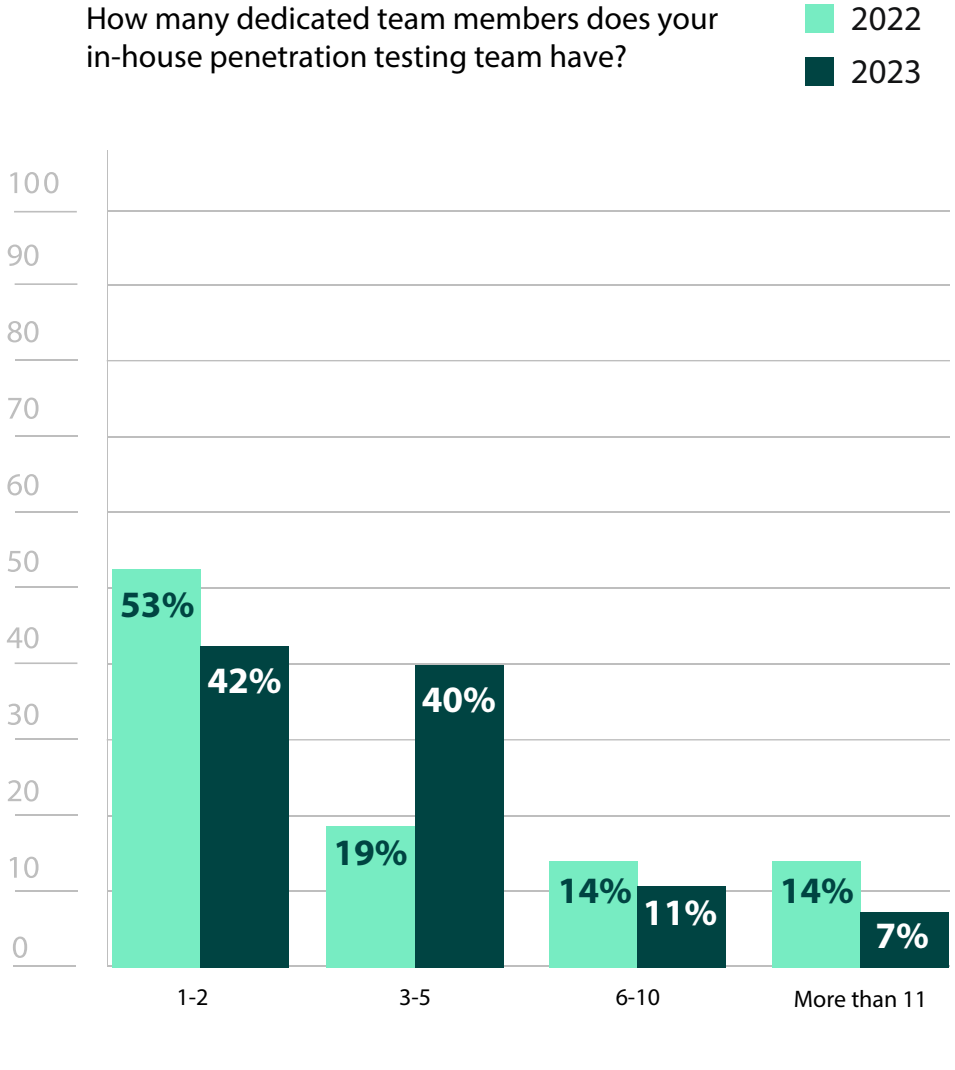


Figure 11: In-house pen testing team size

In-House Penetration Testing Efforts

What is the average number of years of experience your in-house team has with penetration testing?

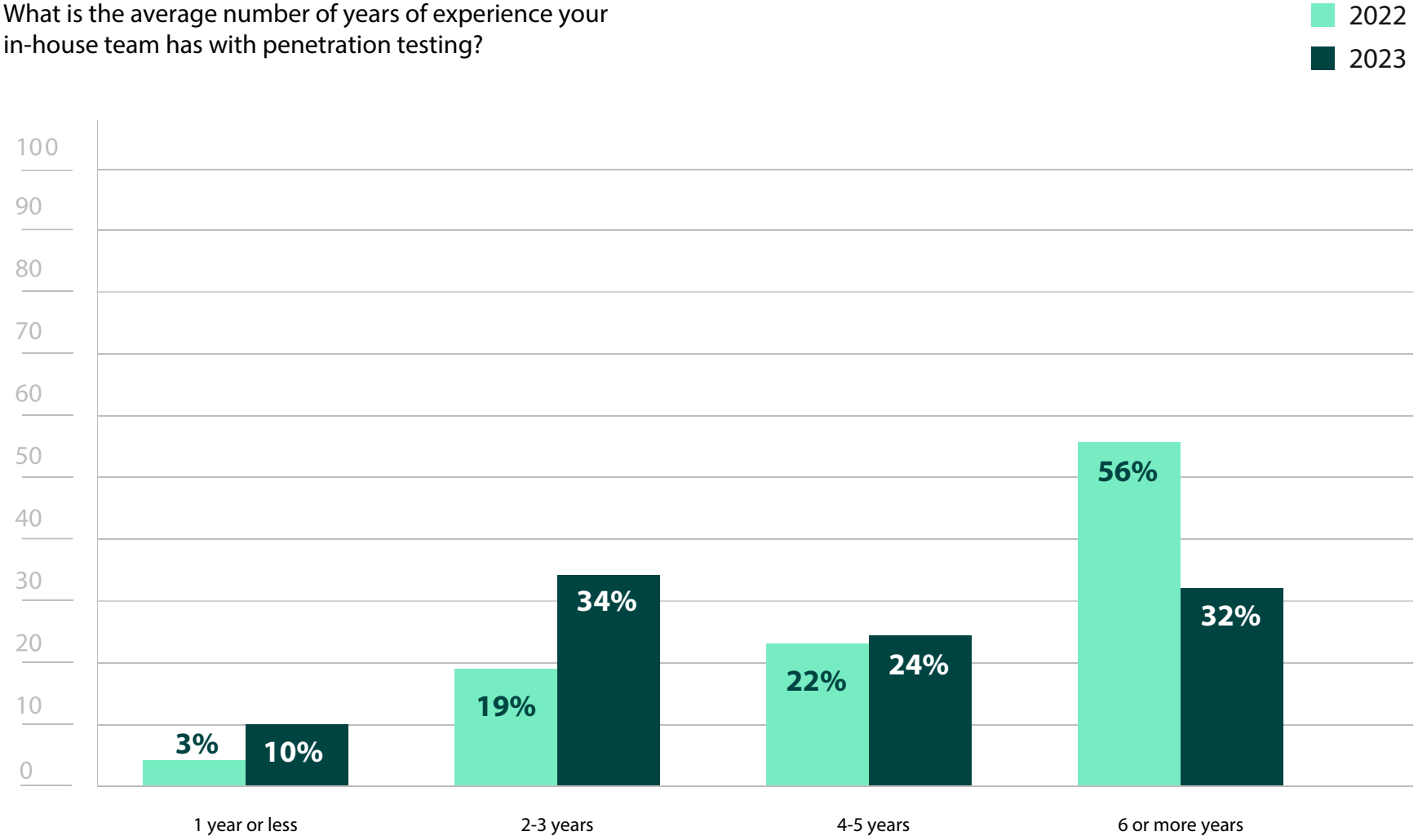


Figure 12: Years of experience of in-house pen testing team

In-House Penetration Testing Efforts

Why does your organization not have an in-house penetration testing team?

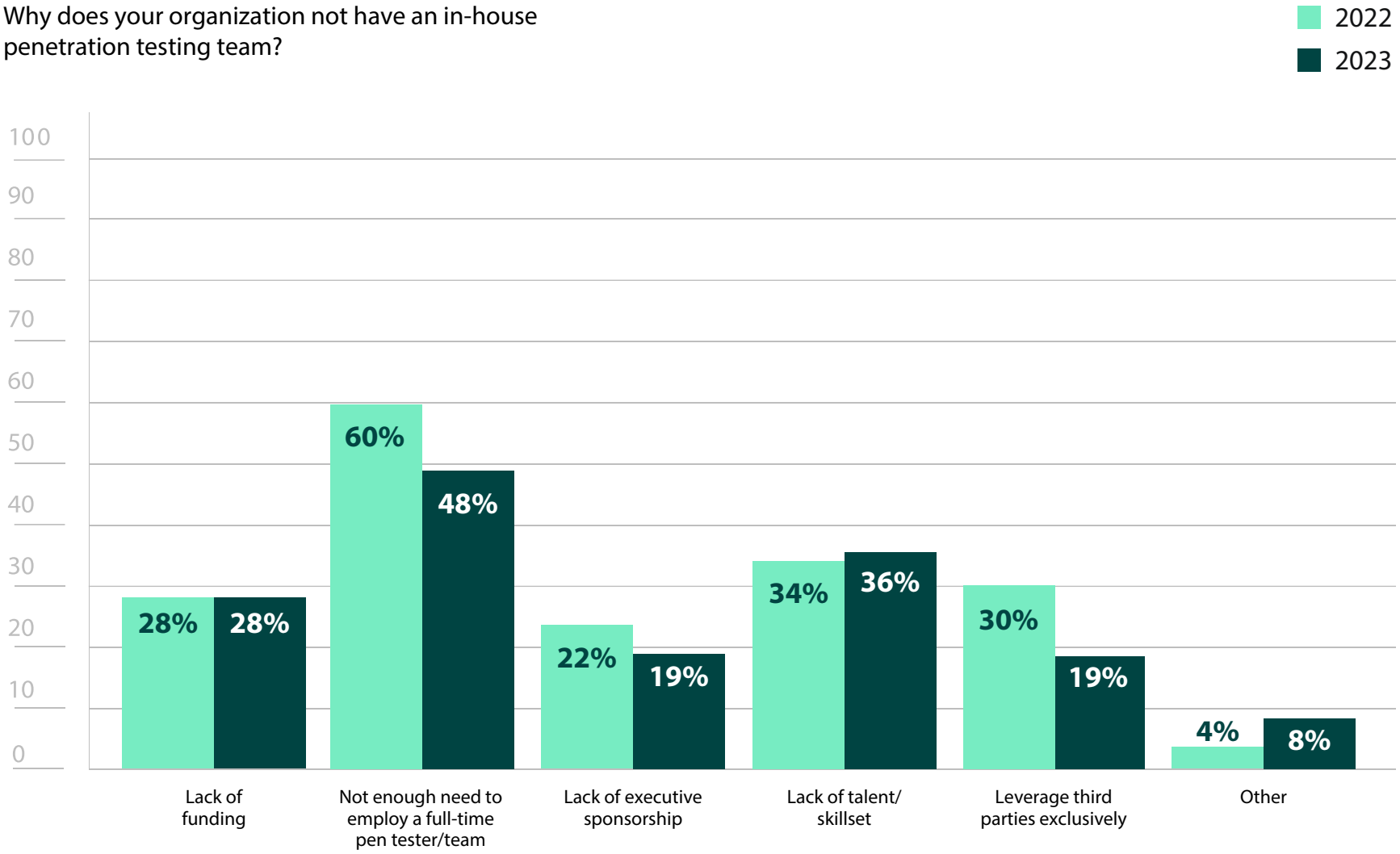


Figure 13: Reasons for not having an in-house pen testing team

In-House Penetration Testing Efforts

How does penetration testing technology influence your organization's decision to have or not have an in-house penetration testing function?

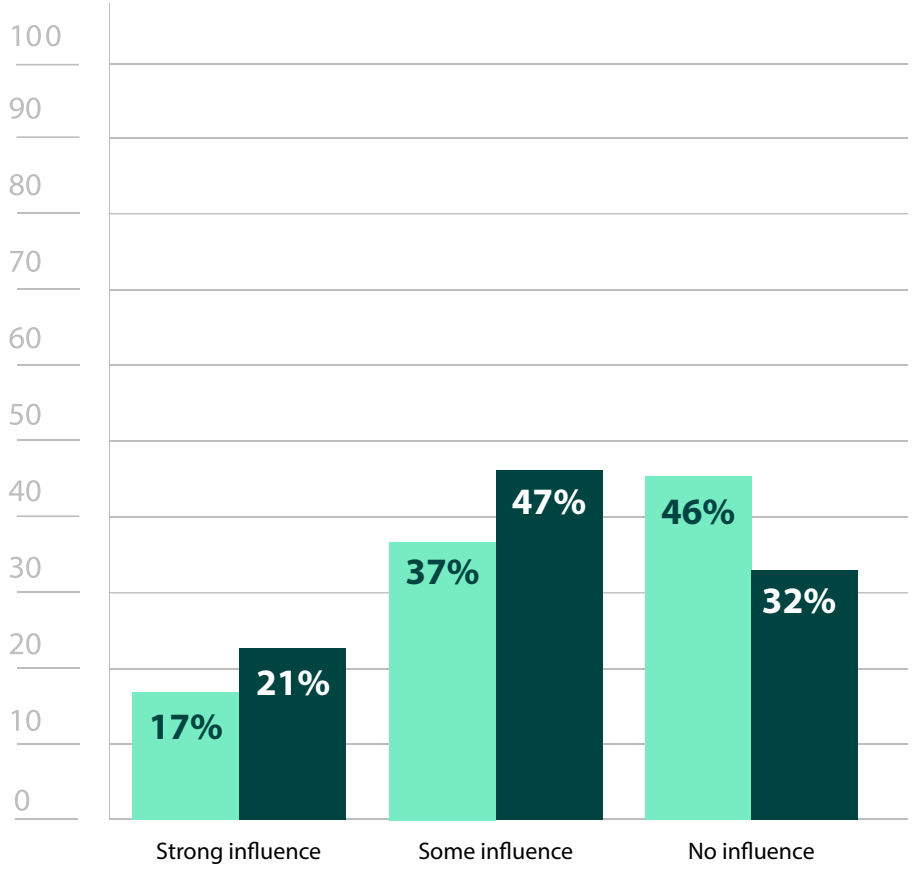


Figure 14: Influence of pen testing technology

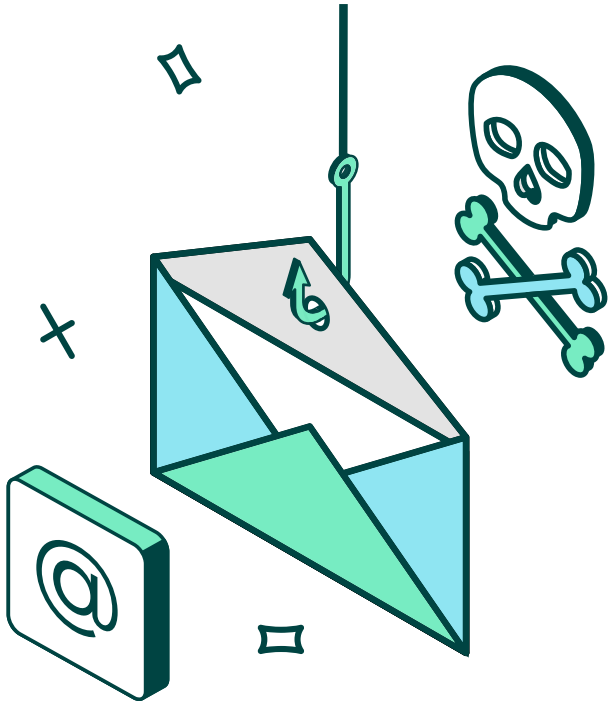
Third-Party Services

Third-party pen testing teams remain a popular resource, with 78% of respondents leveraging third-party teams in some capacity (Figure 18). However, there was a noteworthy shift indicating an increased preference for in-house testing, with a 16% drop in those who used mostly or exclusively third-party services and a 13% increase in those who use all or mostly in-house testing (Figure 18). Though many assume an in-house team is meant as a replacement for third-party services, organizations should ideally use both, so it was promising to see even a modest 5% increase in those who have an even split between in-house and third-party.

What makes an even split ideal? While an internal pen testing team can provide regular, standardized testing, they also become quite familiar with the environment that they're assessing. The top reason third-party services are solicited is because of their external, objective point of view (58%) (Figure 15). Additionally, since third-party teams are fully immersed specialists that can stay up to date on the latest trends and techniques, they are also frequently utilized to apply different skillsets (50%). Wanting an impartial assessment and a diversity of skills may also be a reason for why 76% of organizations tend to change services at least every 2-3 years (Figure 17).

There was a 13% drop in the use of third-party services for compliance. As mentioned earlier, compliance regulations are expanding in number and complexity, so this may be more of a reflection of teams managing their compliance needs internally rather than outsourcing. Many falsely assume that in order to meet compliance needs, third-party testing is required. However, this typically is not the case. In fact, PCI DSS, which has some of the most explicit requirements for pen testing, does not state that a third-party test is necessary. Some organizations find third-party services ideal for determining compliance needs and obtaining strategic support with initial tests. They then use pen testing tools to maintain compliance.

Lastly, though they are used most often for network (81%) and application (65%) testing, it is worth pointing out that third-parties are utilized by 36% of respondents for physical pen tests (Figure 19). These tests involve attempting to gain entry to a physical facility, system, or network through the exploitation of weaknesses like doors, locks, cameras, or other access controls. Such assessments can only be completed by third-parties, further highlighting the unique services they can provide.



Third-Party Services

Why does your organization utilize third-party penetration testers?

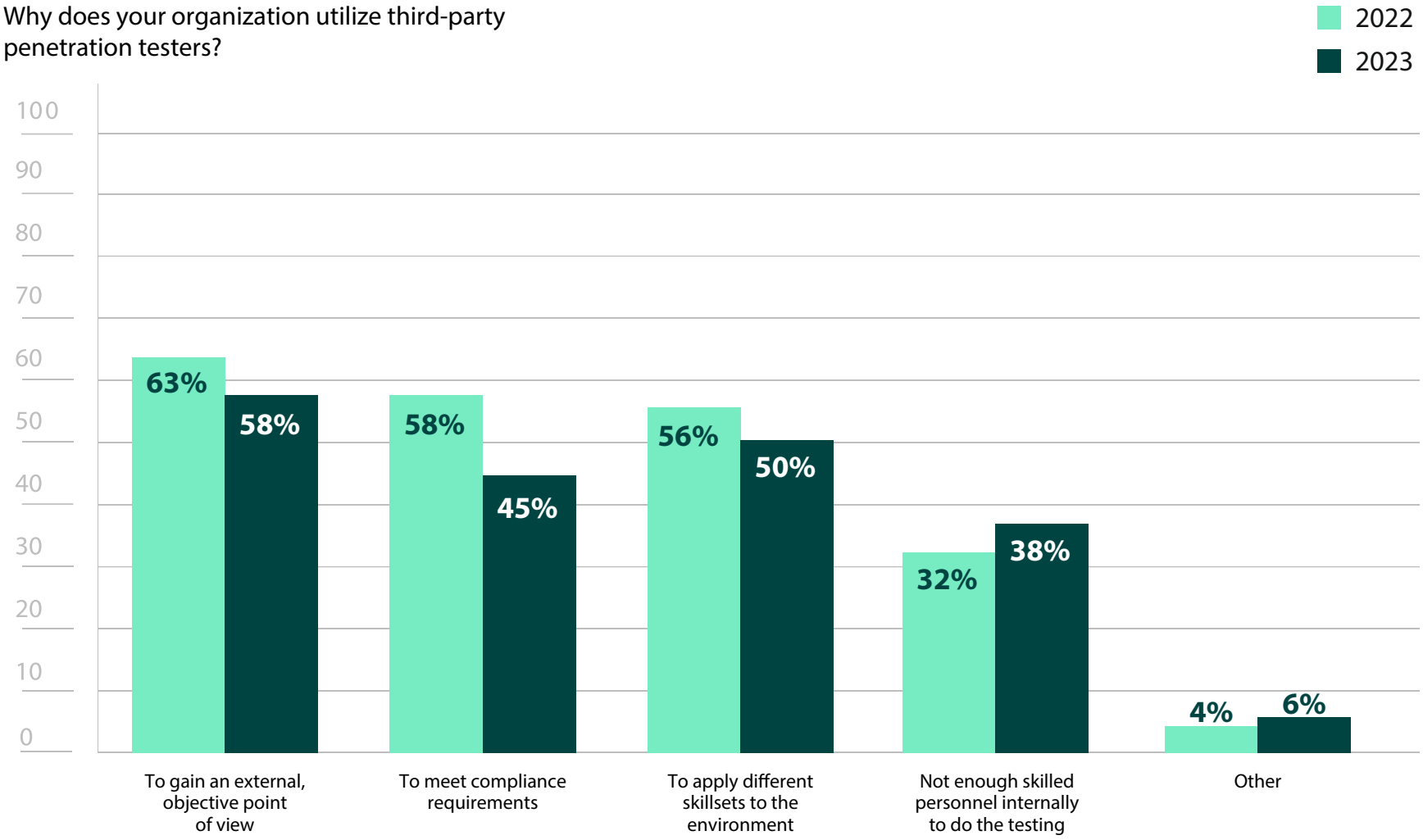


Figure 15: Reasons for utilizing third-party pen testing services

Third-Party Services

How often do you conduct third-party penetration tests?

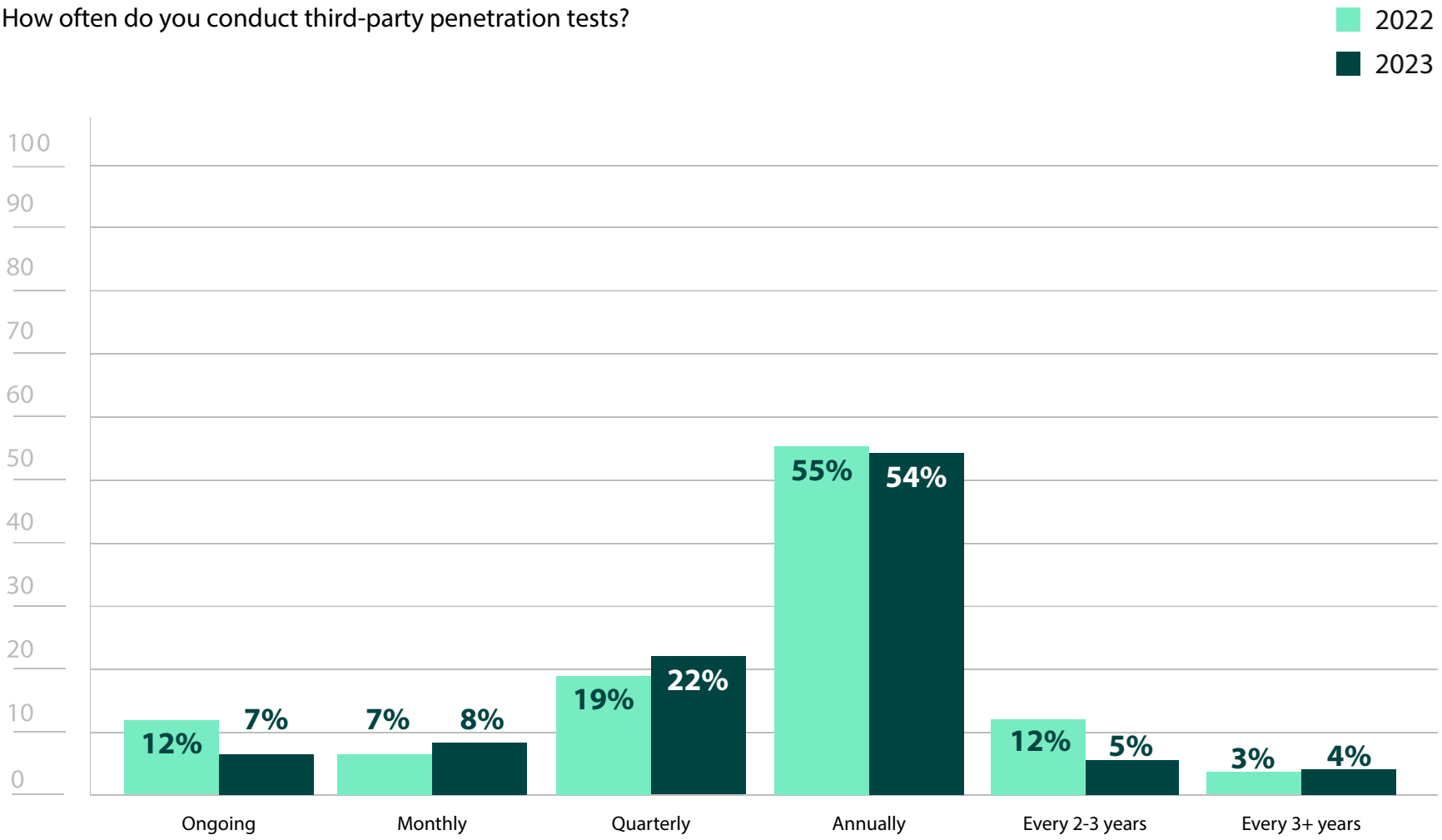


Figure 16: Frequency of third-party pen tests

Third-Party Services

How often do you change which third-party pen testing service you work with?

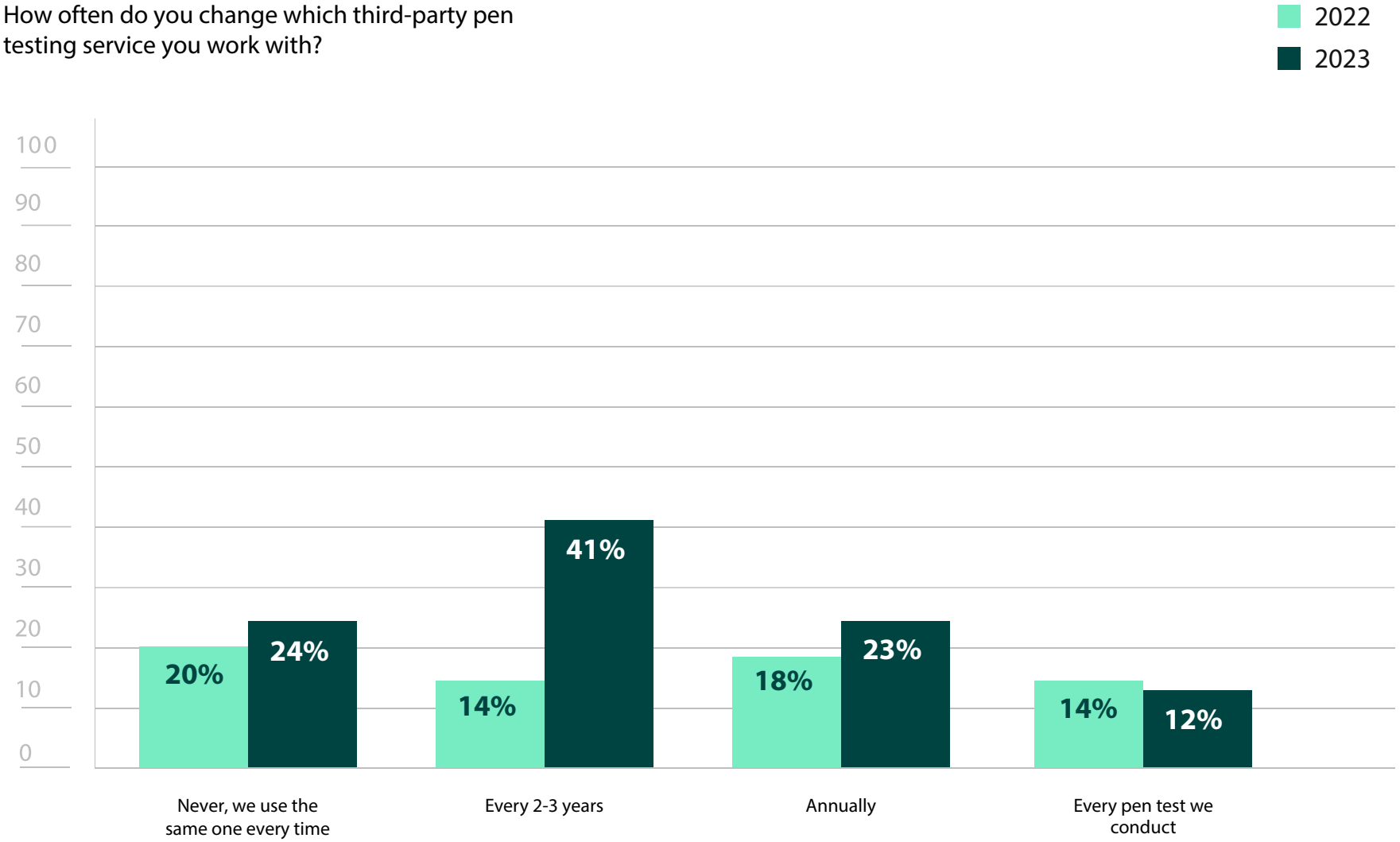


Figure 17: Rotation frequency of third-party pen testing services

Third-Party Services

What is the current split between using internal and third-party pen testing resources?

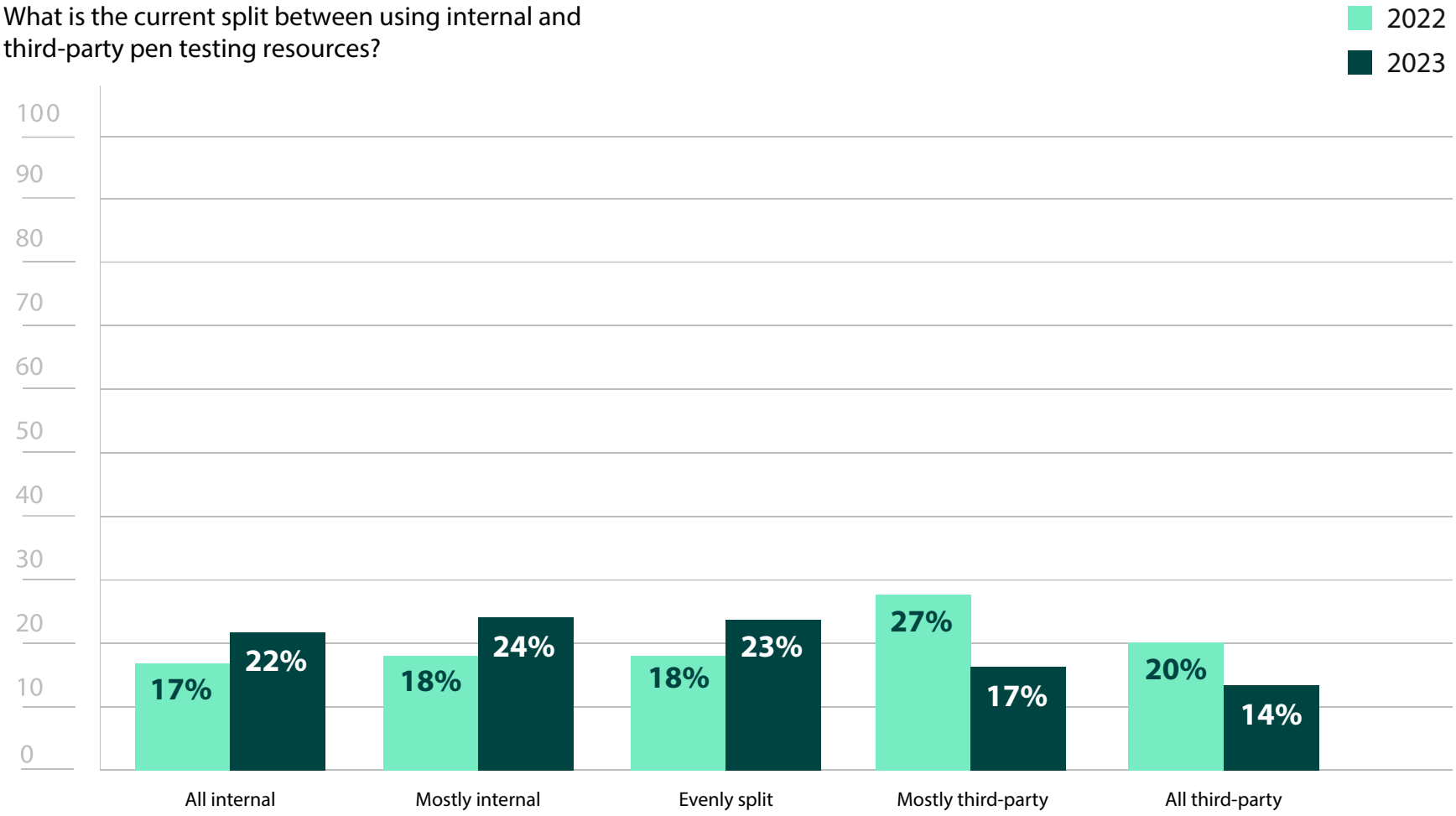


Figure 18: Split between internal and third-party pen testing services

Third-Party Services

Whch types of penetration tests do you utilize third-party testers for?

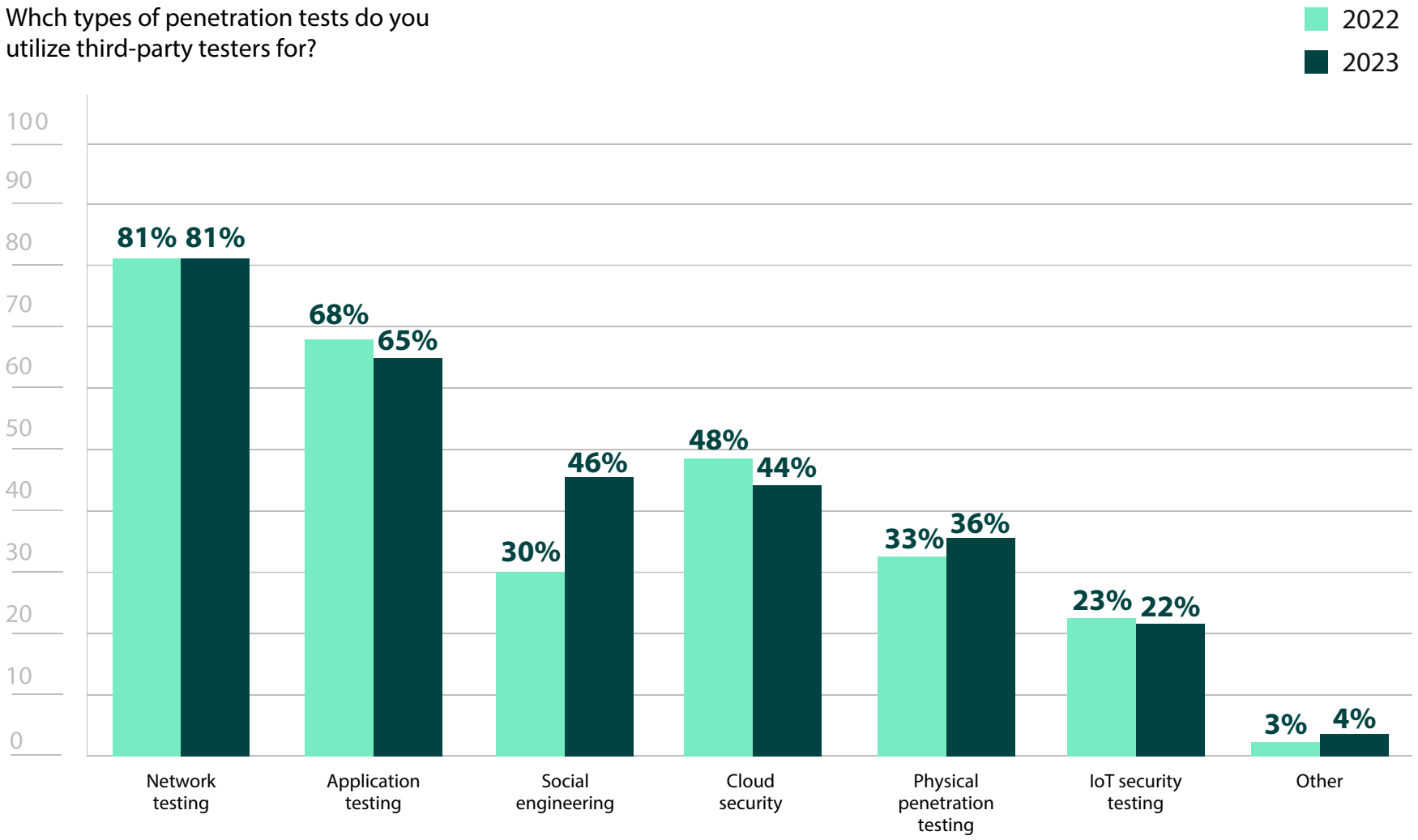


Figure 19: Types of pen tests third-party testers are requested to perform

Other Security Assessment Services

Just as organizations may have complementary solutions in their offensive security tool kit, they may also have offensive security services in addition to pen testing. The use of third-party security awareness training (52%) appears to be the most commonly deployed (Figure 20). Awareness trainings have become a standard practice, with almost all regulations mandating some sort of security awareness program. Aside from being a compliance requirement, training programs are also frequently used as a follow-up to phishing simulations to improve vigilance.

Red teaming is also common, with 38% of respondents reporting that they use this service (Figure 20). Red teaming is often the next offensive security layer added after solidifying a pen testing program. These engagements emulate a real-world scenario, taking on the offensive role of an attacker who will have to evade detection and beat security controls, including the organization's own security team. While the goal of a penetration test is demonstrating the potential of vulnerability exploitation, the goal of a Red Team exercise is testing an organization's ability to successfully detect and respond to attacks, so that security teams can learn and improve from the exercise.

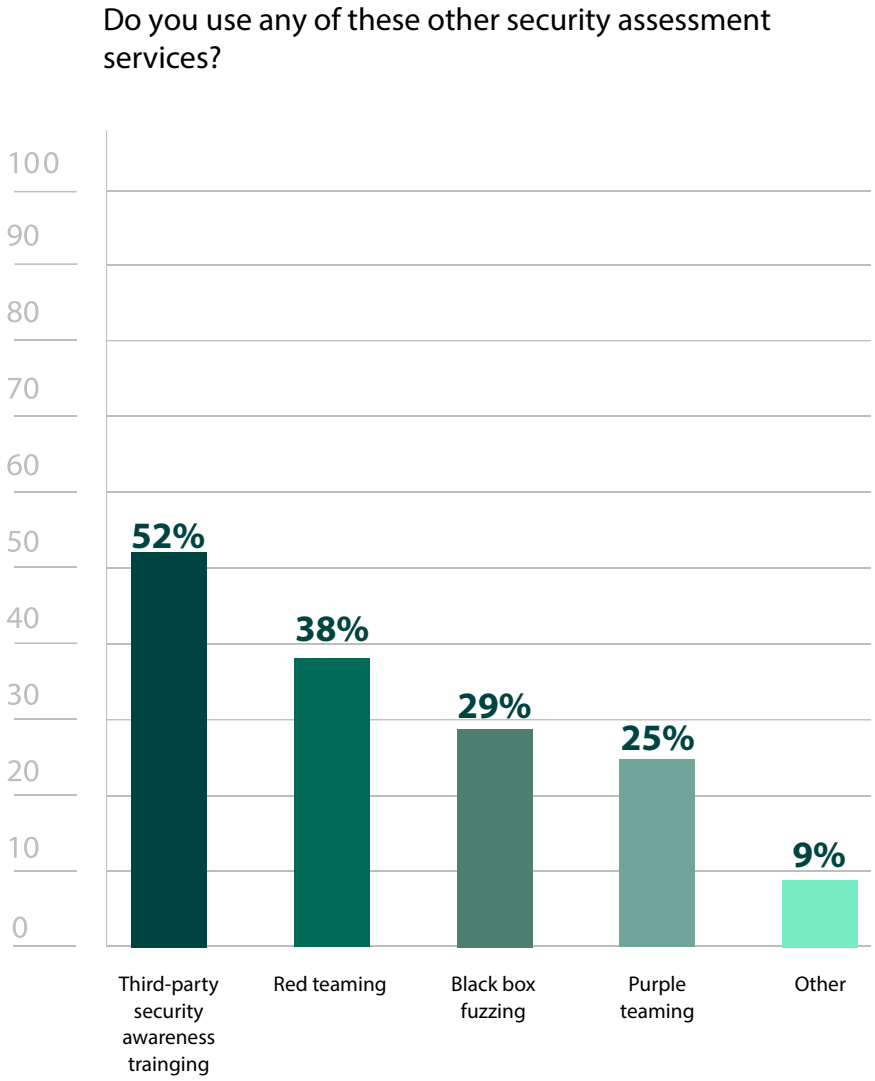


Figure 20: Other security assessment services used

Pen Testing Tools

Penetration testing tools are a broad category and can include specialized tools like port scanners, password crackers, or SQL injection tools, as well as more comprehensive tools that offer multiple features to centralize the testing process. Respondents still almost universally use at least one pen testing tool of some kind, but there were some interesting changes in the usage of free vs commercial tools. The use of both open source and commercial tools was down 21%. Meanwhile, usage of solely open source tools was up 15% and the usage of solely commercial tools was up 5% (Figure 21).

This year's numbers are actually more similar to those from the 2021 report. The 2022 report speculated that the increase in those using both commercial and open-source tools and the decrease in those solely using free/open-source tools may have reflected the economic recovery after the downturn of previous years, enabling them to add one or more commercial tools to their library. This year's data may be showing the effects of inflation, which was shown to have impacted cybersecurity budgets. This seems reinforced by the 9% increase in cost as a consideration when evaluating paid pen testing tools (Figure 22).

Though down from last year, features and functionality still remain the top consideration when searching for a paid pen testing tool, with 81% of respondents listing it as an important evaluation criterion (Figure 22). In terms of the features that they're looking for, reporting (71%), multi-vector testing capabilities (66%), and having an extensive threat library (65%) remained the top three sought after capabilities in paid penetration testing tools (Figure 23).

Interestingly, templates/automation capabilities saw a 13% increase from last year (Figure 23). Automation capabilities not only allow advanced testers to spend their time diving deep into more dynamic problems, they also help new testers get up to speed by aiding in the completion of routine pen tests. As mentioned earlier, many organizations are only running one or two tests annually, which may be insufficient. Pen testing automation allows organizations to run tests more frequently while still maintaining efficiency, and without having to dramatically increase headcount.

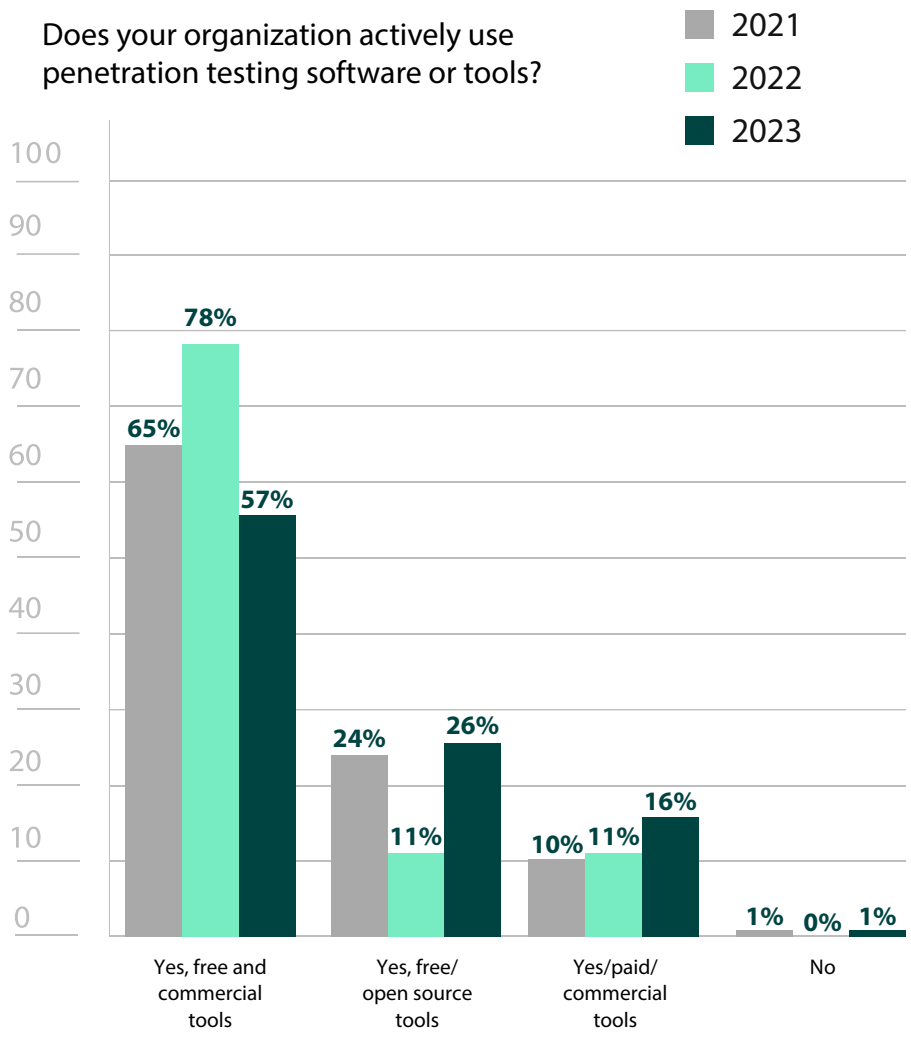


Figure 21: Active use of penetration testing software

Pen Testing Tools

What criteria do you consider most important when evaluating penetration testing software?

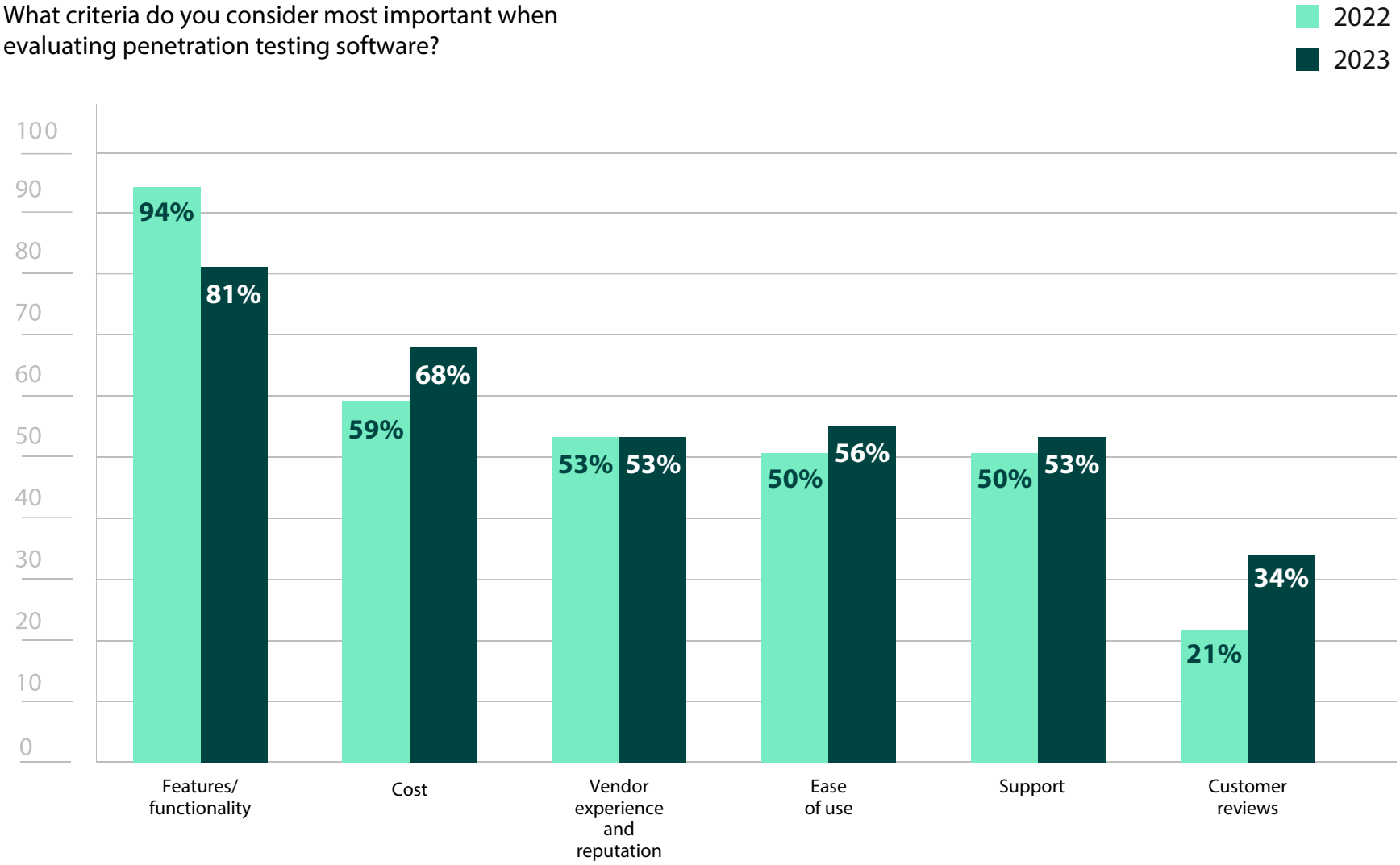


Figure 22: Most important criteria for evaluating pen testing software

Pen Testing Tools

What features are most important in paid/commercial penetration testing software/tools?

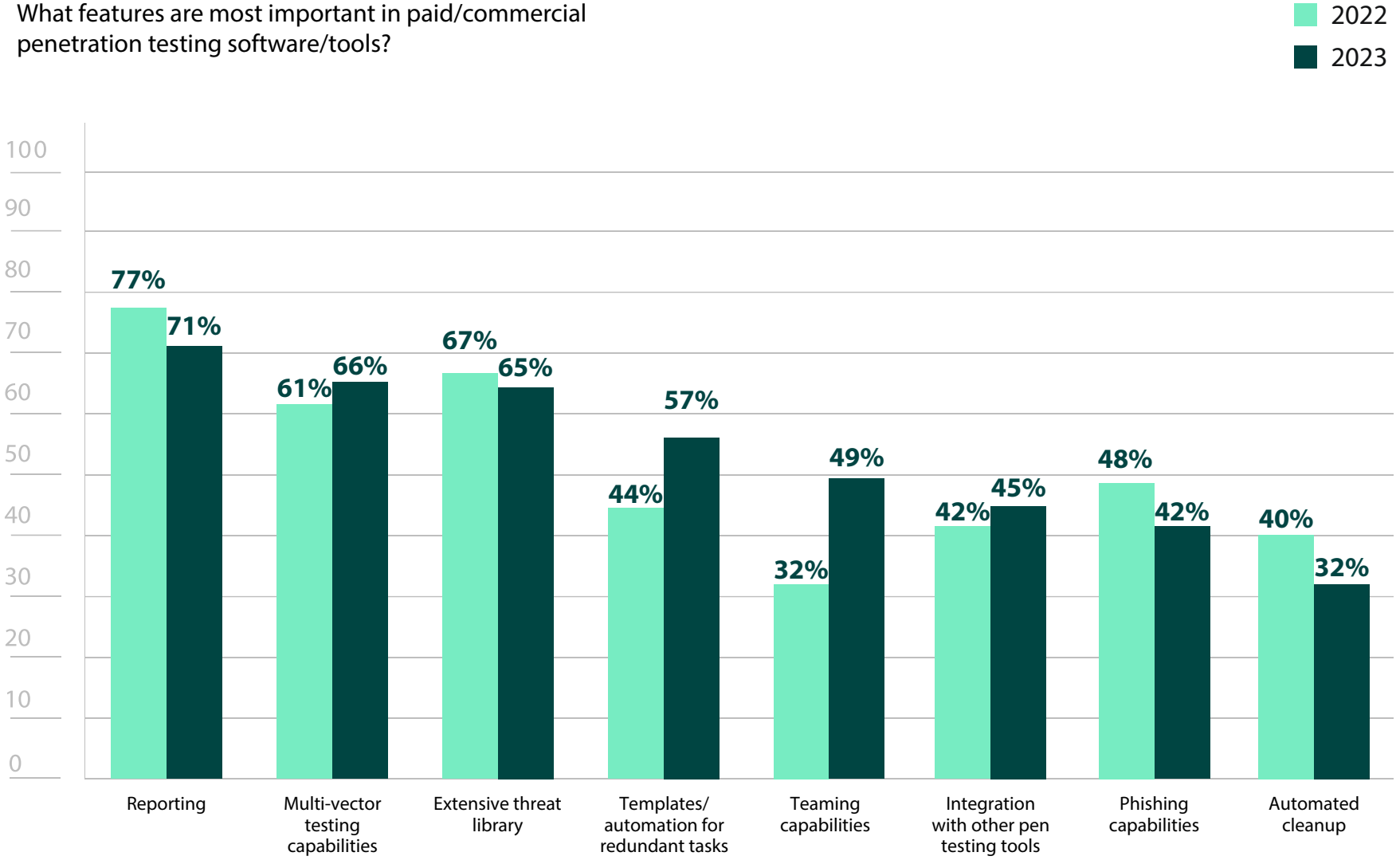


Figure 23: Most important features in pen testing software

Other Security Assessment Solutions

When taking an offensive security approach, new solutions will be added as your strategy matures. One foundational piece of effective offensive security is a vulnerability scanner, as they are a fundamental part of vulnerability management. These assessments provide visibility into the state of an organization's security on a regular basis. Routine, automated scans of networks and web applications identify and prioritize security weaknesses using external intelligence. Penetration testing is seen as the next step in vulnerability management journey, since the data vulnerability scans provide can augment penetration tests, providing insights into which weaknesses warrant additional investigation. Since respondents have already incorporated pen testing into their strategies, it's unsurprising that the majority of respondents (86%) already have vulnerability scanners (Figure 24).

Just as in 2022, post-exploitation (32%) and adversary simulation (27%) are significantly less common tools. These solutions are typically only used by those who have a more mature program that can deploy red team engagements. Many businesses, particularly SMBs, don't have a large enough security team to do so and may instead rely on third-party services. As seen in Figure 13, staffing challenges may prevent a larger organization from building an in-house pen testing team, let alone a red team. Other organizations may simply not be at this stage in their security journey, as full offensive security maturity cannot be achieved overnight.

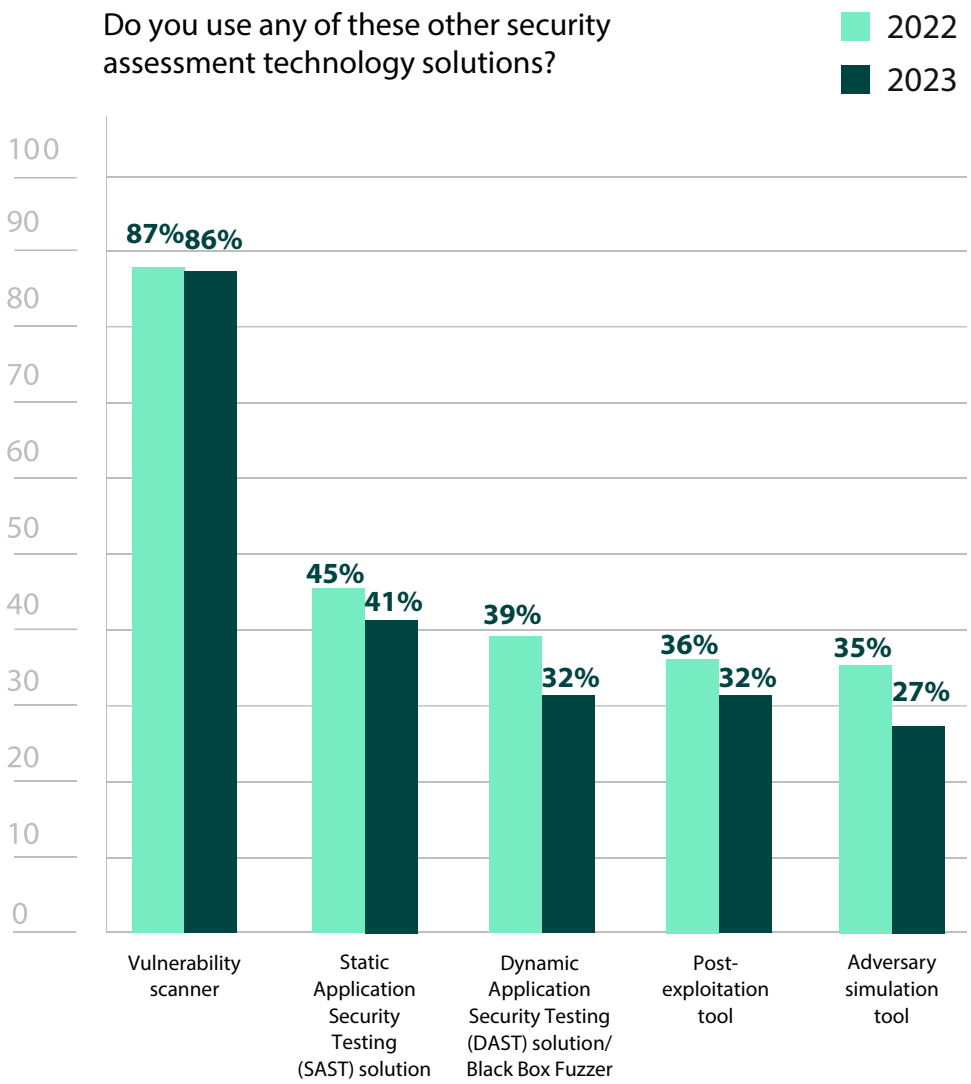


Figure 24: Other security assessment tools used

Vendor Consolidation

IT infrastructures are continuing to expand both in size and sophistication, with organizations finding themselves needing more assets and applications than ever before to effectively run day-to-day operations. The number of vendors an organization has to deal with can not only be overwhelming to manage, it can also become a cybersecurity risk. More vendors that have access to your environment can mean more potential attack vectors. By consolidating vendors, organizations can streamline operations and limit complexity, which reduces the attack surface and simplifies risk management.

Vendor consolidation has become an increasingly popular strategy, even for cybersecurity solutions, with most respondents considering it either somewhat important (37%) or important (43%) to consolidate security vendors (Figure 25). With the necessity of a layered security approach, it makes sense to choose solutions from a single vendor, especially those that can offer platform centralization, integration or interoperability features, unified support, cost savings, and more.

How important it is to consolidate vendors for your security solutions?

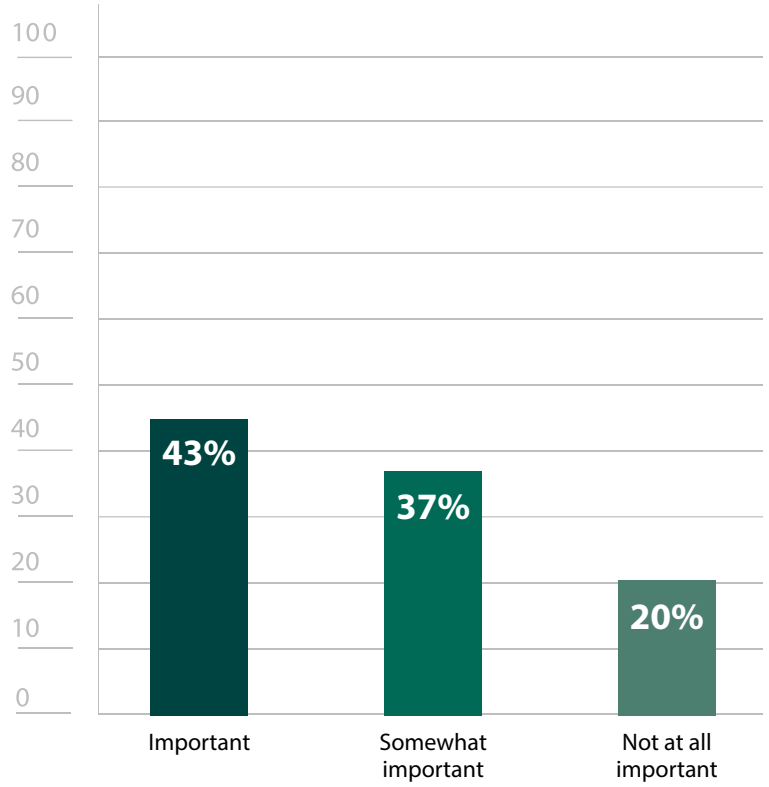


Figure 25: Importance of vendor consolidation

Pen Testing in Different Environments

As the most universal operating system, it is not surprising to see that Windows is once again the most common area (82%) respondents were concerned about testing (Figure 26). Windows can be run throughout an organization, including workstations, servers, and other assets. Additionally, Windows Active Directory is the heart of most organizational infrastructures, as it facilitates and centralizes network management and serves as a database, storing usernames, passwords, permissions, and more. Unfortunately, this makes it a prime target for attackers, as anyone who has domain admin rights to Active Directory has the ability to access, create, or modify any of the main accounts.

Though Windows is the most common, it's clear there is some level of concern about other operating systems, like Linux (54%), Unix (18%), and IBM (12%) (Figure 26), which are typically only used on application or database servers. While access to these servers is more limited and operating systems have long held a reputation of being secure, they are by no means immune to an attack. Storing critical and sensitive data also makes them a target, so it's wise for organizations to include them in the pen testing scope.

One noteworthy change from last year is an 11% uptick in mobile pen testing (Figure 26). 2022 saw a record number of attacks on smartphones, which may have prompted more organizations to determine the state of their own mobile security. Mobile environments are particularly vulnerable, as they are susceptible to multiple types of phishing attacks, including vishing (voice phishing), smishing (SMS phishing), and quishing (QR code phishing) attacks. Additionally, as MFA becomes more universal, phones are increasingly used as a means of authentication. Attackers are now using "SIM swapping" attacks to temporarily gain access to a phone in order to access or divert messages with authentication passcodes. With attack methods such as these, organizations are right to incorporate mobile pen testing, particularly phishing campaigns.

Cloud infrastructures experienced a similar spike in attacks in 2022, with nearly double the number from 2021. Unfortunately, cloud infrastructures (47%) remained significantly less commonly tested than internal and external infrastructures (Figure 27). As more resources and services become cloud based, organizations may need to reconsider their testing strategies to incorporate more assessments of cloud security.

Pen Testing in Different Environments

Which environments or operating systems are you most concerned about pen testing?

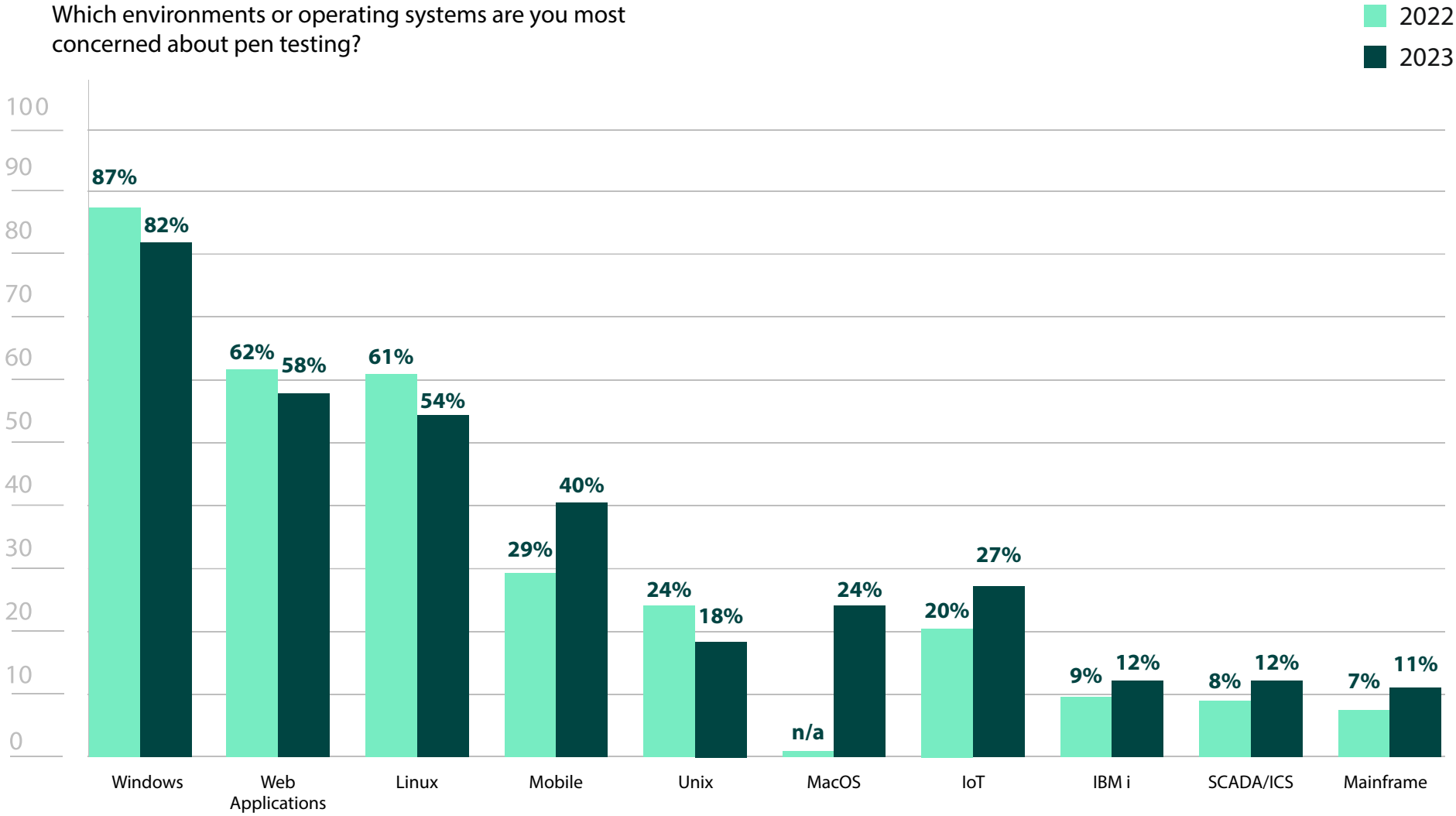
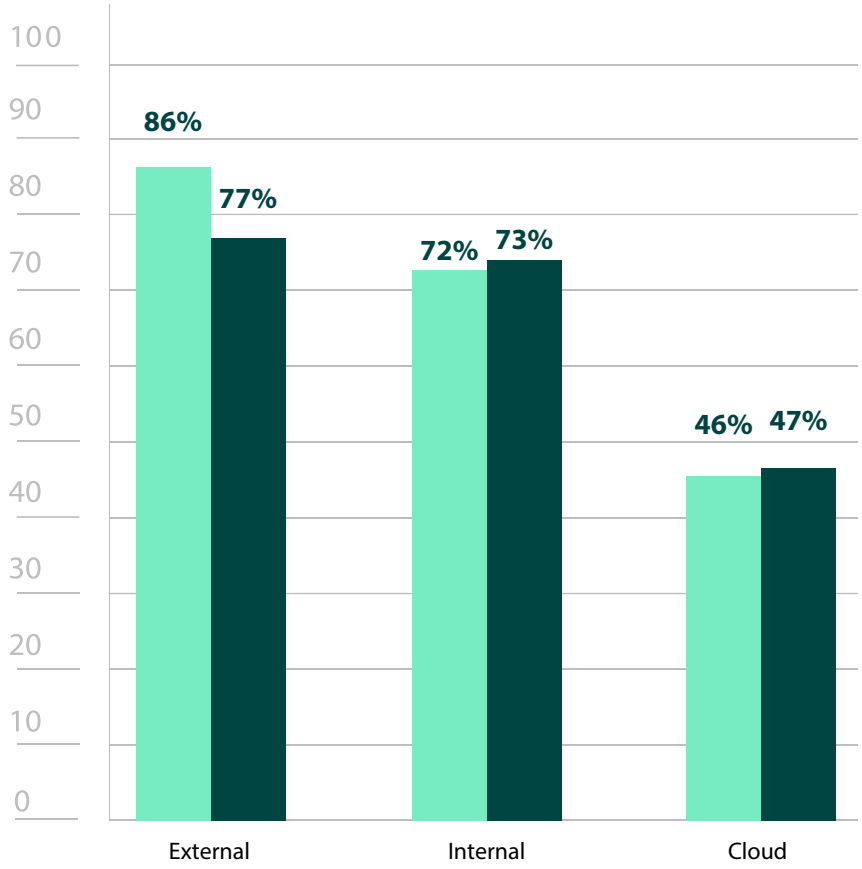


Figure 26: Environments in need of pen testing

Pen Testing in Different Environments

Against what infrastructure do you regularly (at least on an annual basis) conduct penetration testing?



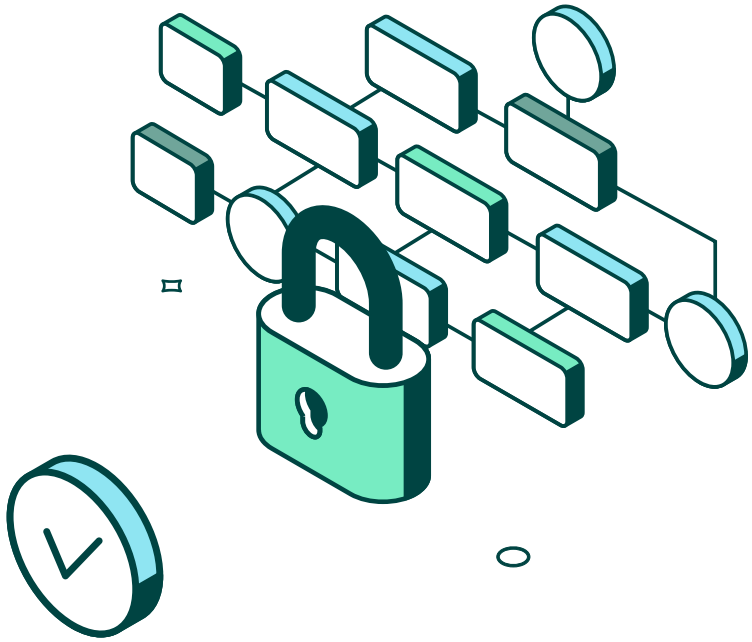


Figure 27: Infrastructures regularly pen tested

Demographics

In which region is your organization headquartered?

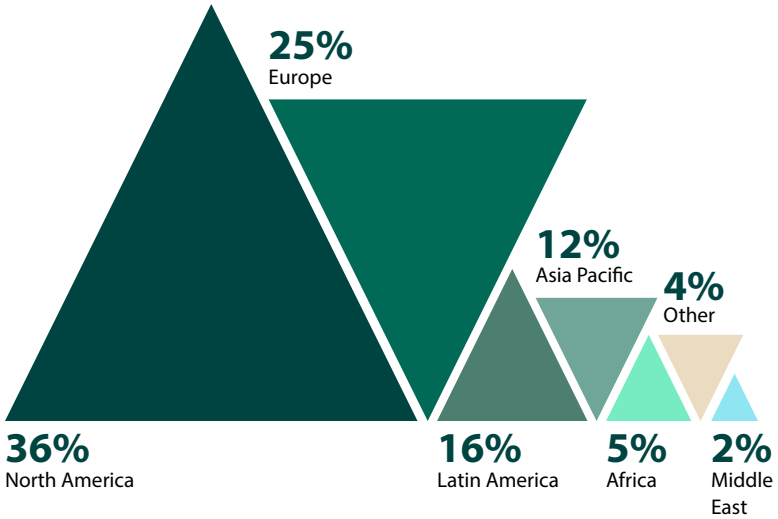


Figure 28: Regions surveyed

What is your primary industry?

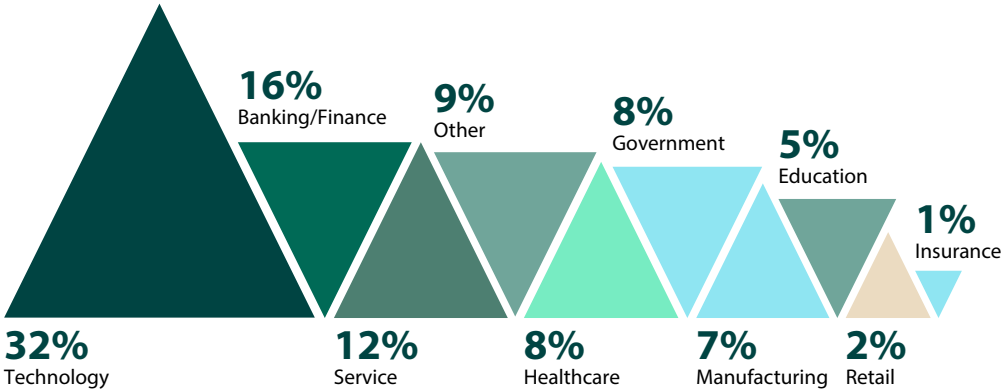


Figure 29: Industries surveyed

This report is based on the results of a survey focused on presenting an accurate picture of the cybersecurity concerns penetration testing addresses, how it is deployed by different organizations, and the challenges in creating and managing a penetration testing program. Cybersecurity professionals around the globe participated, with respondents representing a diverse cross-section of industries, company size, job level, and region.

Demographics

What is your job level?

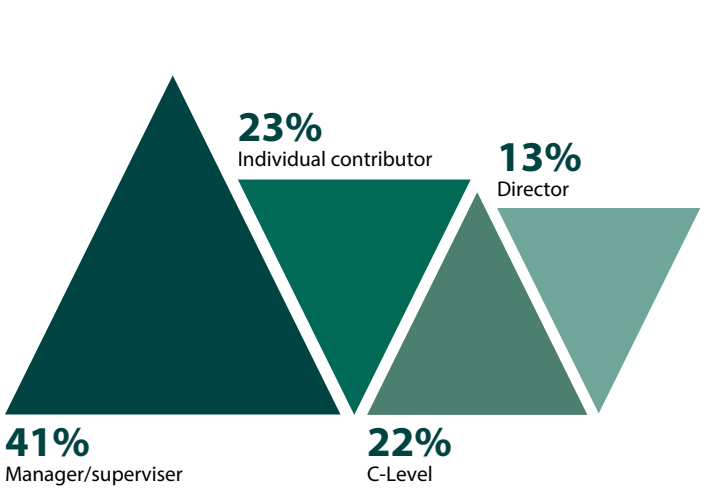


Figure 30: Job levels surveyed

How many employees does your organization have?

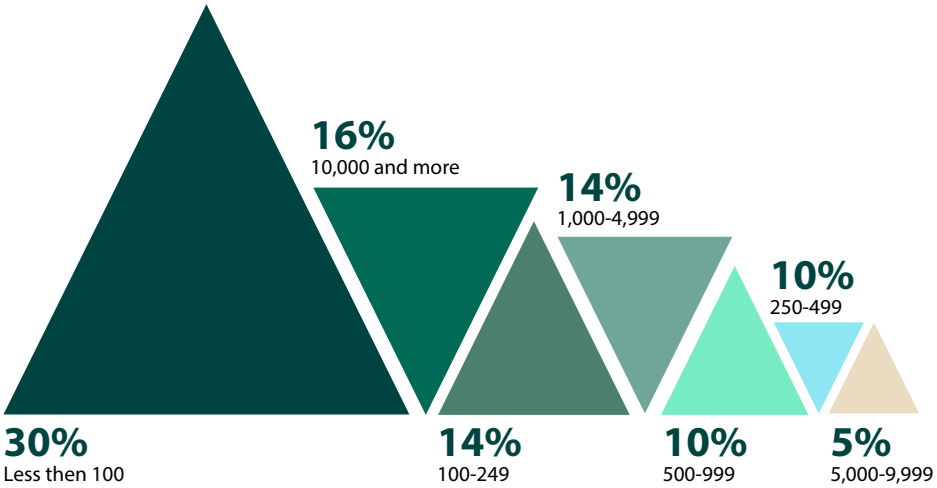


Figure 31: Size of organizations surveyed

Conclusion

The goal of this survey was to provide visibility into how cybersecurity professionals are utilizing pen testing. The results revealed the wide range of ways that people pen test and the elements shaping how they pen test. Organizations have many options to choose from when putting together a pen testing approach, which may seem daunting. Careful evaluation is needed when determining which tests to run, how often to run them, and whether they should be conducted in-house or by a third party. Fortunately, the variety of options is also what enables organizations of all different sizes and industries to tailor a strategy to suit their needs and resources.

Despite the acknowledgment of the importance of pen testing, the challenge of limited resources continues to endure. Though innovative tools can help with resource limitations and the skills gap, organizations will also have to make difficult decisions about which parts of their environment are most in need of assessment.

Pen testing programs are not without their obstacles, but the benefits of incorporating this proactive security practice demonstrate that they are well worth it. From vulnerability management to regulations requirements, pen testing helps reduce risk and continually elevate the security of an IT environment by providing guidance on how to close security gaps or stay compliant. Most importantly, penetration testing helps reduce the risk of incidents that put organizations' finances, efficiency, and trustworthiness at stake.

FORTRA™

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

(fta-cs-gd-0323-r1-db)