FORTRA

2022 Penetration Testing Report

Introduction

As the number of successful cyber-attacks continues to increase at a frightening pace, many organizations are embracing holistic security strategies that incorporate ways to detect and minimize the impact of a breach, as well as methods to preempt such attacks by uncovering and closing security gaps. Penetration testing is a key component of this proactive approach by identifying and exploiting security weaknesses, safely demonstrating the potential impact. Such efforts lay out paths to remediation and help prioritize threats based on the specific level of risk they pose to the organization, allowing security professionals to act well before an attacker can.

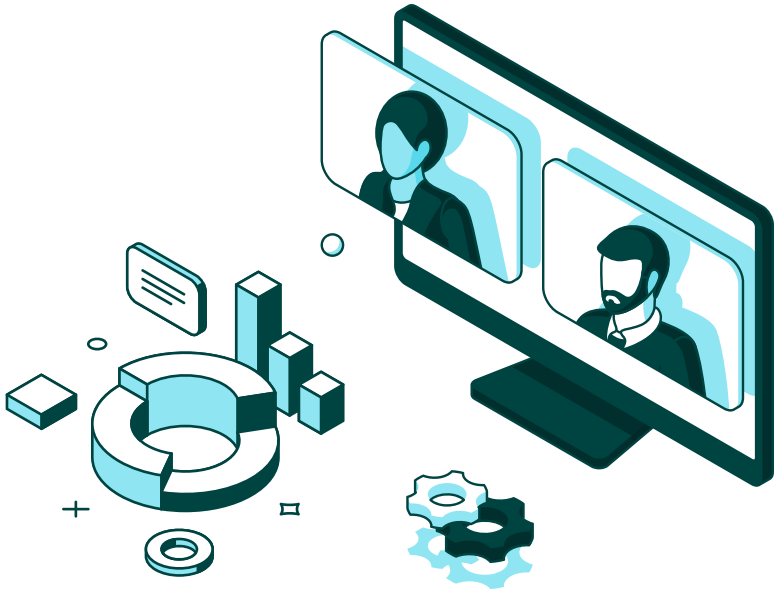
Penetration testing encompasses a great variety of security assessments, tools, and services. Three years ago, Core Security, by HelpSystems launched its first penetration testing survey in order to get a better picture of how cybersecurity professionals are using penetration testing in the field, providing a detailed picture of pen testing strategies and the resources required to deploy a successful pen testing program.

After this inaugural survey established a strong baseline of data, we decided to build upon it by conducting it annually, tracking year over year changes, trends, challenges, and areas of improvement. In this third annual global survey, we continued to discover slight shifts in the role penetration testing plays in the cybersecurity landscape.

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 2021 survey and also uncover new insights, analyzing the general evolution and advancement of the penetration testing field.



Reasons for Pen Testing

Organizations continue to pen test for multiple reasons, with 75% reporting they perform pen tests for compliance, 75% for measuring security posture, and 57% for vulnerability management program support (Figure 1). The 5% increase in compliance from the 2021 survey may reflect the increasing number of organizations that have to adhere to specific industry standards or regulations. Those needing to prove compliance to standards that don't specifically mandate penetration testing may be taking advantage of the fact that pen testing is one of the most efficient ways to both fulfill and prove adherence.

While the decrease in use as a support for vulnerability management programs could be concerning, it may also reflect the current security climate of rapidly increasing risk. Many organizations have become so overwhelmed that they currently rely on having more of an ad hoc security approach. Others are perhaps beginning to incorporate more sophisticated cybersecurity practices in direct response to an attack. 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 maximal coverage and impact.

Reasons for Pen Testing

Why does your organization perform penetration tests?

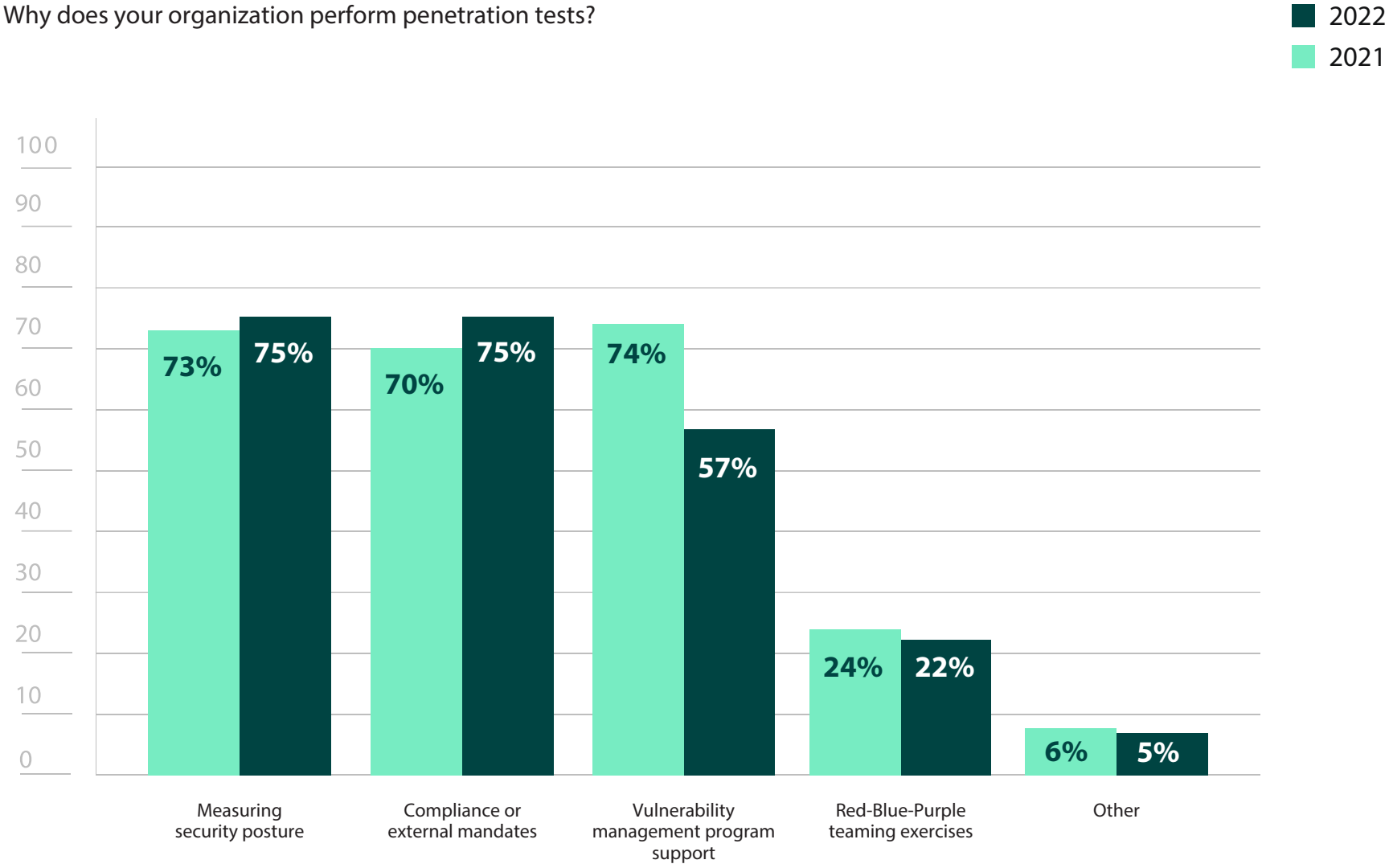


Figure 1: Reasons for performing penetration tests

Common Security Concerns

Respondents reported phishing (80%), ransomware (68%), and misconfigurations (57%) as top concerns, which aligns with what cyber attackers are commonly targeting and deploying (Figure 2).

The rising concern over phishing and poor passwords (55%) illustrates the inescapable threat that employees inadvertently pose to organizations, either by carelessly opening an email or choosing a password that is both easy to remember and simple to guess. According to PhishLabs, phishing attacks grew by 28% in 2021. Regular social engineering penetration tests are one of the best ways to reduce the risk of successful phishing attacks, as they can both flag vulnerable employees and also help to keep such attacks top of mind, helping to ensure employees think twice before clicking anything.

The concern over ransomware is also well justified and connected to phishing. According to the 2021 Malware Report, the number one way previous ransomware breaches had entered organizations was through phishing emails (70%). The rapid increase in ransomware attacks is alarming, with a consistent growth rate of well over 100% year over year. The cost of ransomware attacks has also become overwhelming. The average ransom demand in 2021 was a staggering $220,298–and this number only tells half the story. The average recovery cost for data recovery, ransomware removal, etc. is $1.85m.

Lastly, concern over misconfigurations is also understandable, as IT infrastructures become ever more complex, with even small organizations having multi-faceted environments with multiple tools and systems that consistently need updating and other maintenance that can be hard to keep up with. For example, security vulnerabilities have become an endemic part of technology that every organization must constantly be vigilant for, patching or executing workarounds as necessary. According to the National Vulnerability Database (NVD), over 19,000 vulnerabilities were discovered in 2020, and over 20,000 were found in 2021. Penetration testing can be an invaluable tool for both uncovering vulnerabilities and ensuring that such fixes are properly implemented.

Common Security Concerns

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

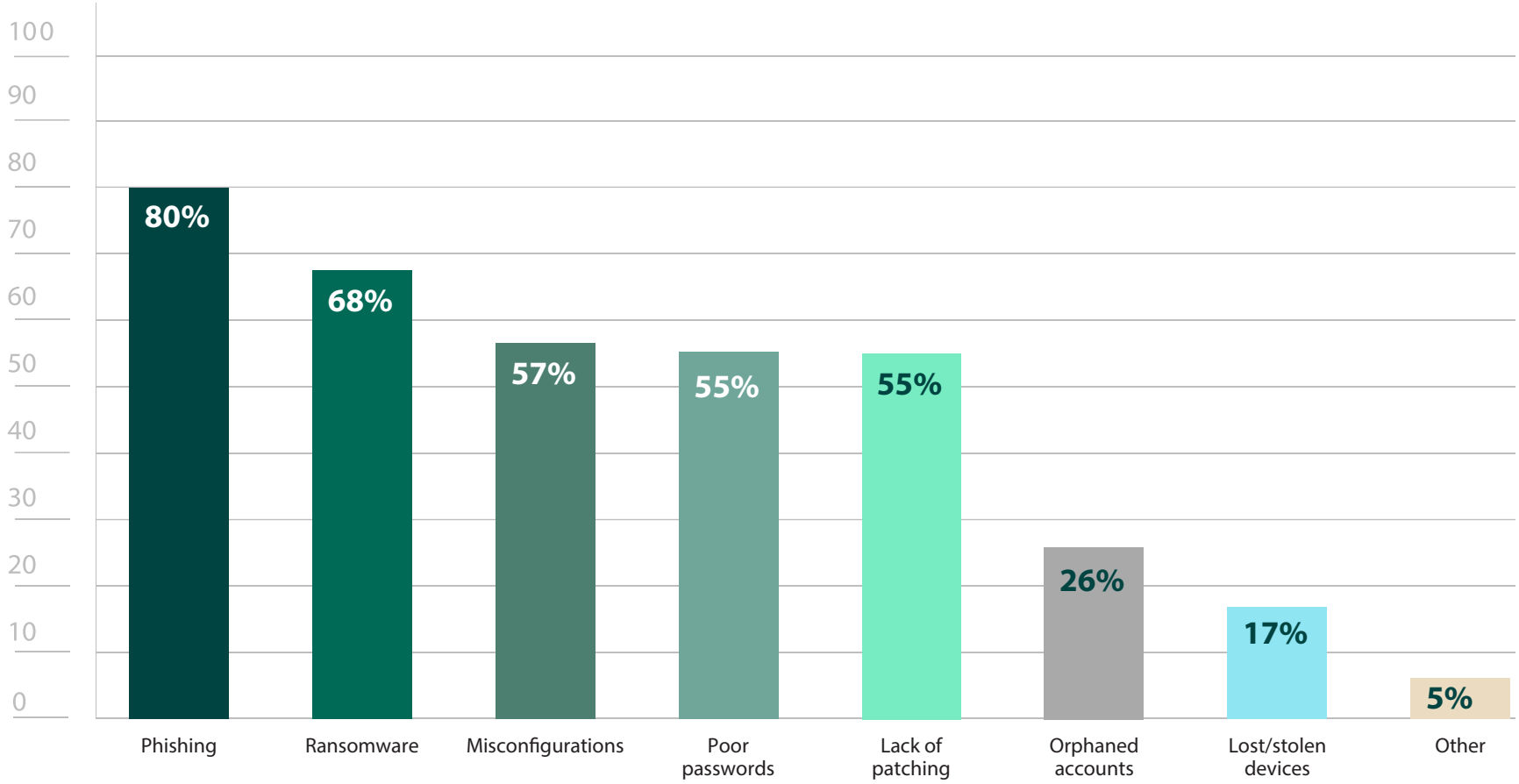
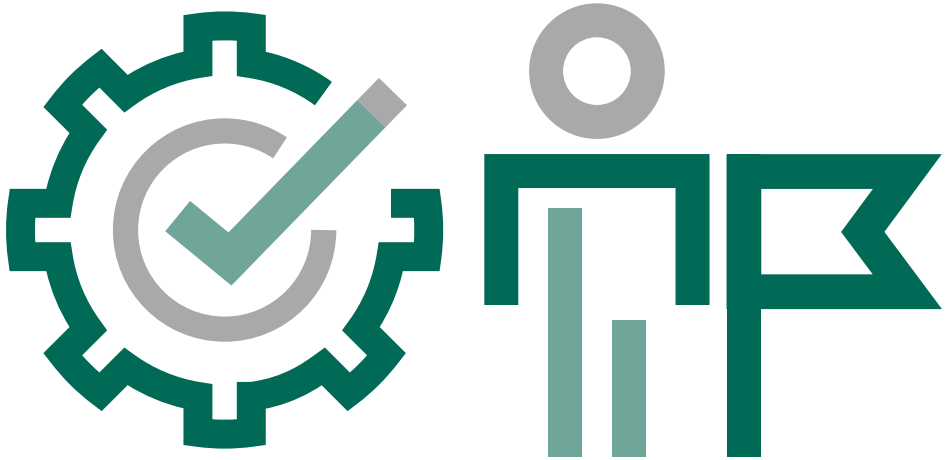


Figure 2: Common security concerns

General Penetration Testing Challenges

The value of pen testing is acknowledged by cybersecurity professionals—94% of respondents noted that penetration testing is at least somewhat important to their security (Figure 4). There was even a small increase of 3% from last year's results. However, perhaps the strongest indicator of an increased backing of pen testing efforts is the reduction in respondents experiencing challenges. For example, hiring enough skilled personnel is down 12% (Figure 3). While there is certainly still a cybersecurity skills shortage, this decrease may indicate that organizations have been given sufficient budgets to hire such highly desired professionals. This is supported by the 7% decrease in the challenge to get executive sponsorship and funding for such programs. Additionally, the 15% decrease for those having issues getting others to act on the findings indicates both that programs are better funded, and that cybersecurity threats have become a higher priority than ever before. While the struggle to find third-party penetration testers remains steady at 45%, this most likely means that third-parties are consistently booked.

It is worth acknowledging that the confidence level may still be a bit too high, with a 9% jump from last year (Figure 5). While additional investment is certainly something to be proud of, the security climate is so precarious that even the smallest amount of overconfidence can lead to disaster. Though it's important not to become pessimistic about cybersecurity, it is equally critical not to rest on our laurels, continuing to shift and evolve alongside of, and hopefully ahead of, attackers.



General Penetration Testing Challenges

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

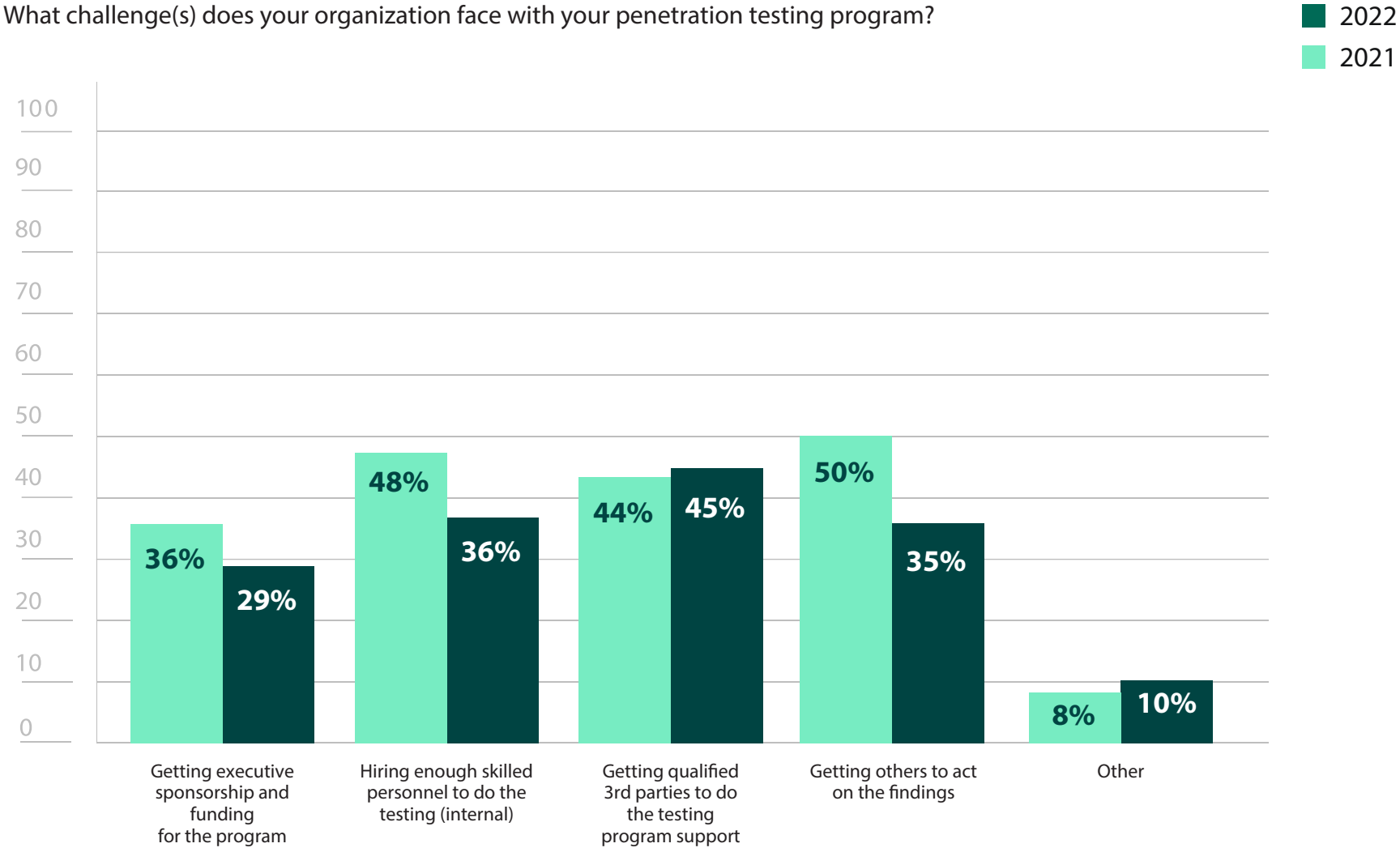


Figure 3: Pen testing challenges

General Penetration Testing Challenges

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

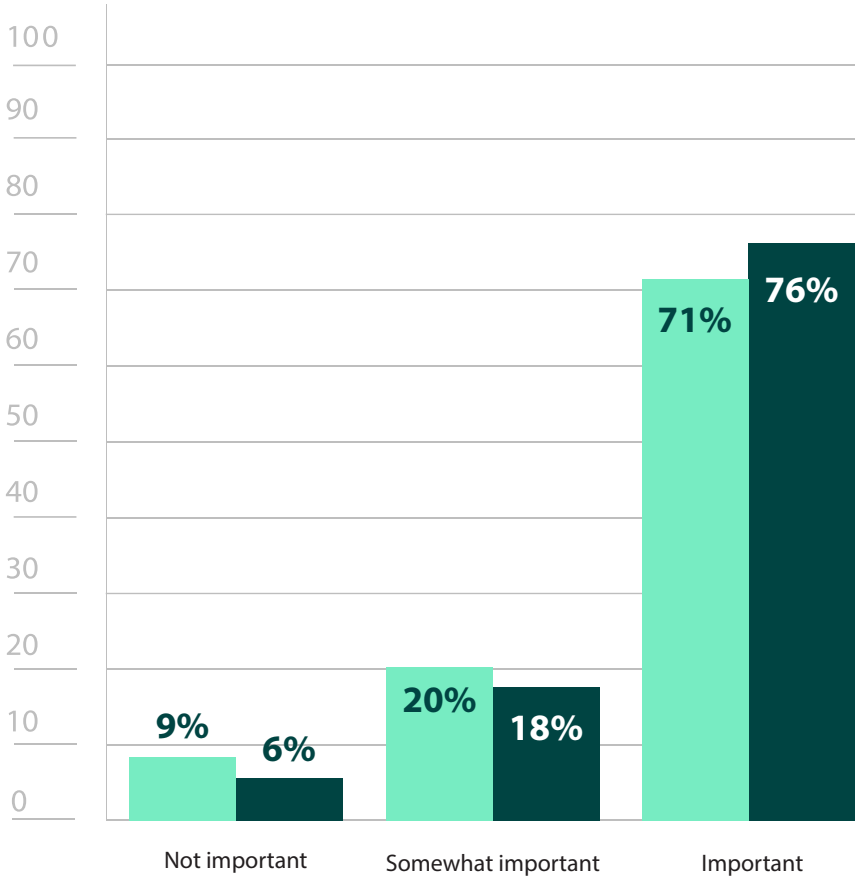


Figure 4: Importance of penetration testing

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

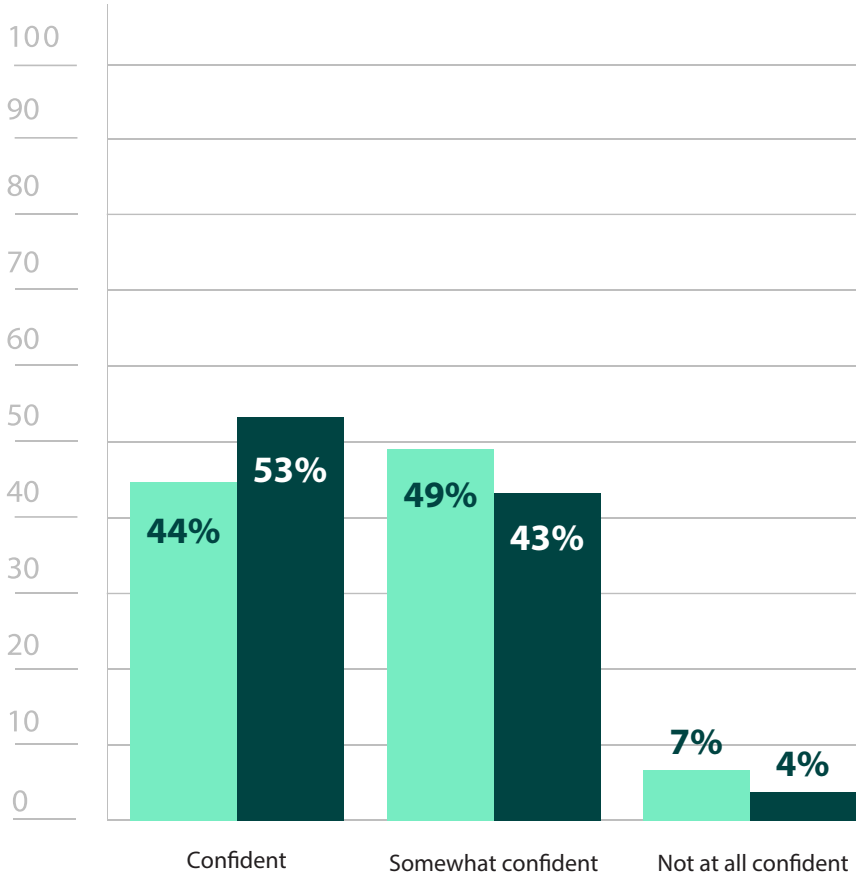


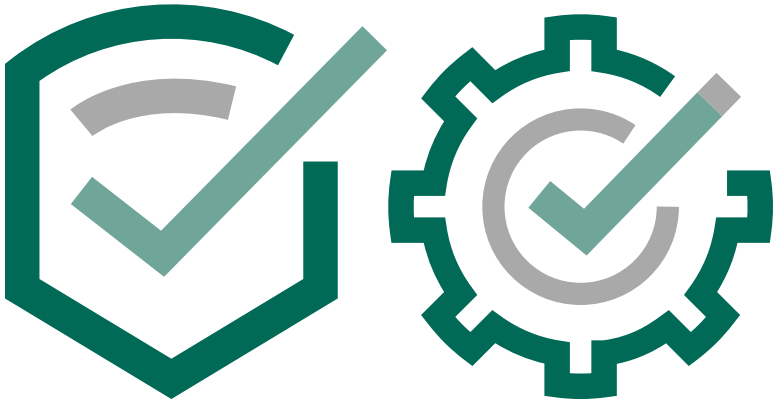
Figure 5: Confidence in security posture

Compliance and Pen Testing

As seen in Figure 1, compliance to external mandates was one of the primary reasons respondents conducted penetration tests. In fact, 96% of respondents reported pen testing was at least somewhat important for their compliance initiatives (Figure 6).

Typically, 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 testing can provide insight on potential security weaknesses, showing how an attacker could gain access to these different types of data. Organizations can use such test findings to prioritize anything endangering sensitive data, even running retests to confirm appropriate remediation.

In order to ensure organizations are obeying these requirements, such regulations require proof of compliance. Pen tests are not only a way to evaluate an organization's security posture, but they can also help verify adherence, proving to auditors or other authorities that mandated security measures are in place or working properly. Pen testing is even mandated to comply with Payment Card Industry Data Security Standard (PCI DSS) in requirement 11.3, which states that a comprehensive pen testing program must be implemented. As some of these other regulations are revisited and revised, it wouldn't be surprising to see penetration testing become an explicit component in the future.



Compliance and Pen Testing

How important is penetration testing to your compliance initiatives?

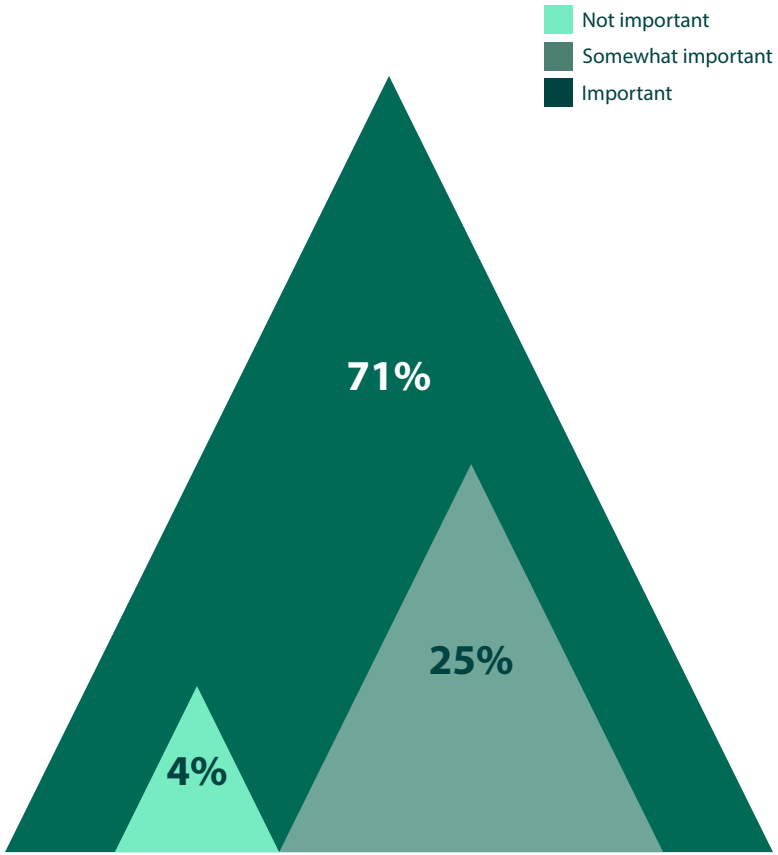


Figure 6: Importance of penetration testing for compliance

Phishing

Phishing remains a pervasive threat, with 80% of respondents listing it as a top security concern. Though the technique of phishing is decades old, attackers continue to refine their methods. For example, according to PhishLabs, vishing threats grew by 554% in 2021. Such attacks involve emails that are concerningly realistic, so much so that they convince victims to call a phone number. From there, attackers continue the ruse and solicit sensitive information to a fake representative. A well-crafted phish can be easy for anyone to fall for, especially if they aren't looking for the signs.

Given the risk that such attacks pose, it was encouraging to see a 4% increase in ongoing testing this year (Figure 7). However, a slight increase in those that responded that they never conduct phishing simulations was discouraging. It's hard to think that it's a matter of a lack of awareness considering its continued coverage in the news. Considering only 30% of respondents use third-party testing services for social engineering tests, it may be due to a lack of resources (Figure 19).

Given the numerous other priorities, it's understandable that phishing assessments would be outside the scope of engagements. However, organizations may want to consider a phishing campaign tool to run their own tests, which can be straightforward and run routinely. In fact, 48% of respondents felt that phishing capabilities were a crucial feature in pen testing tools (Figure 22). These tests not only reveal who is susceptible to such attacks in your organization, they can serve as a reminder to employees to be mindful of what's in their inbox. The results of these tests also provide a starting point when crafting employee education efforts.

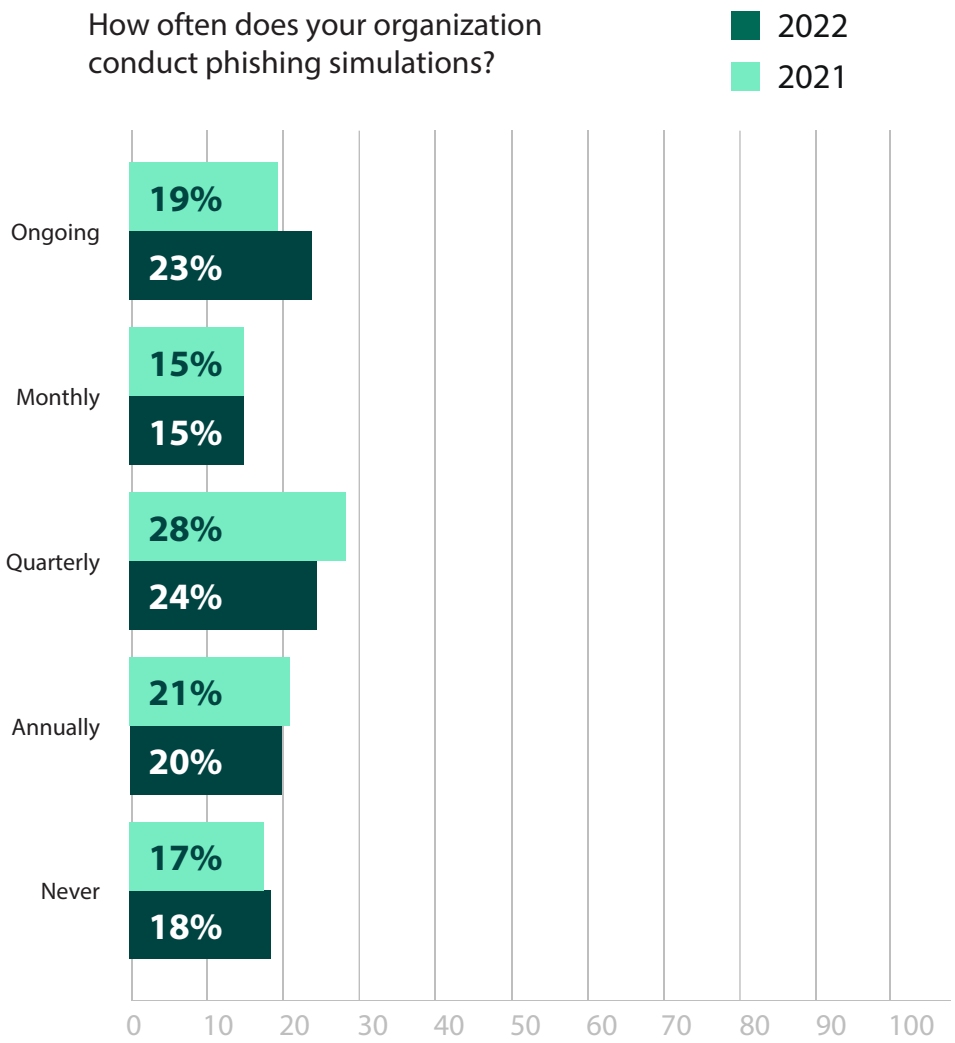


Figure 7: Frequency of phishing simulations

Penetration Testing Frequency

This year's results are quite similar to 2021. There is only a slight drop in the number of people who never pen test and a minor rise in those who pen test annually (Figure 8). Though small, it may indicate some progress towards incorporating a proactive security strategy in addition to other more reactive efforts like antivirus and breach detection. At the very least, it suggests the stability of penetration testing once it's introduced into an organization's strategy.

With the majority of respondents still only testing one or two times a year, retesting needs to be given more priority. An initial test helps to determine a prioritized list of security weaknesses so organizations know what remediations are most urgent. But how can you be sure that problems have been properly fixed? Retesting against the baseline of an initial test confirms whether improvements have been successfully implemented and security holes are closed.

Additionally, an annual test may be scoped to focus on only the most critical systems. However, as infrastructures grow, even the most critical systems may be too broad of a scope. It could help to incorporate automated penetration testing tools, which can streamline the process and enable those with less experience to run more frequent, routine tests.

17% of respondents reported pen testing daily or weekly, which is likely a result of confusion around the difference between vulnerability scans and a full pen test (Figure 8). Vulnerability scanners have a broad focus and can be run more frequently, detecting known security weaknesses and prioritizing them based on external threat intelligence. Penetration testing focuses on the exploitation of these weaknesses to see if and how easily an attacker may be able to breach an environment. Since both tools are essential, it's important that organizations can distinguish between the two, ensuring they have both layers of proactive security.

Penetration Testing Frequency

How often does your organization pen test?

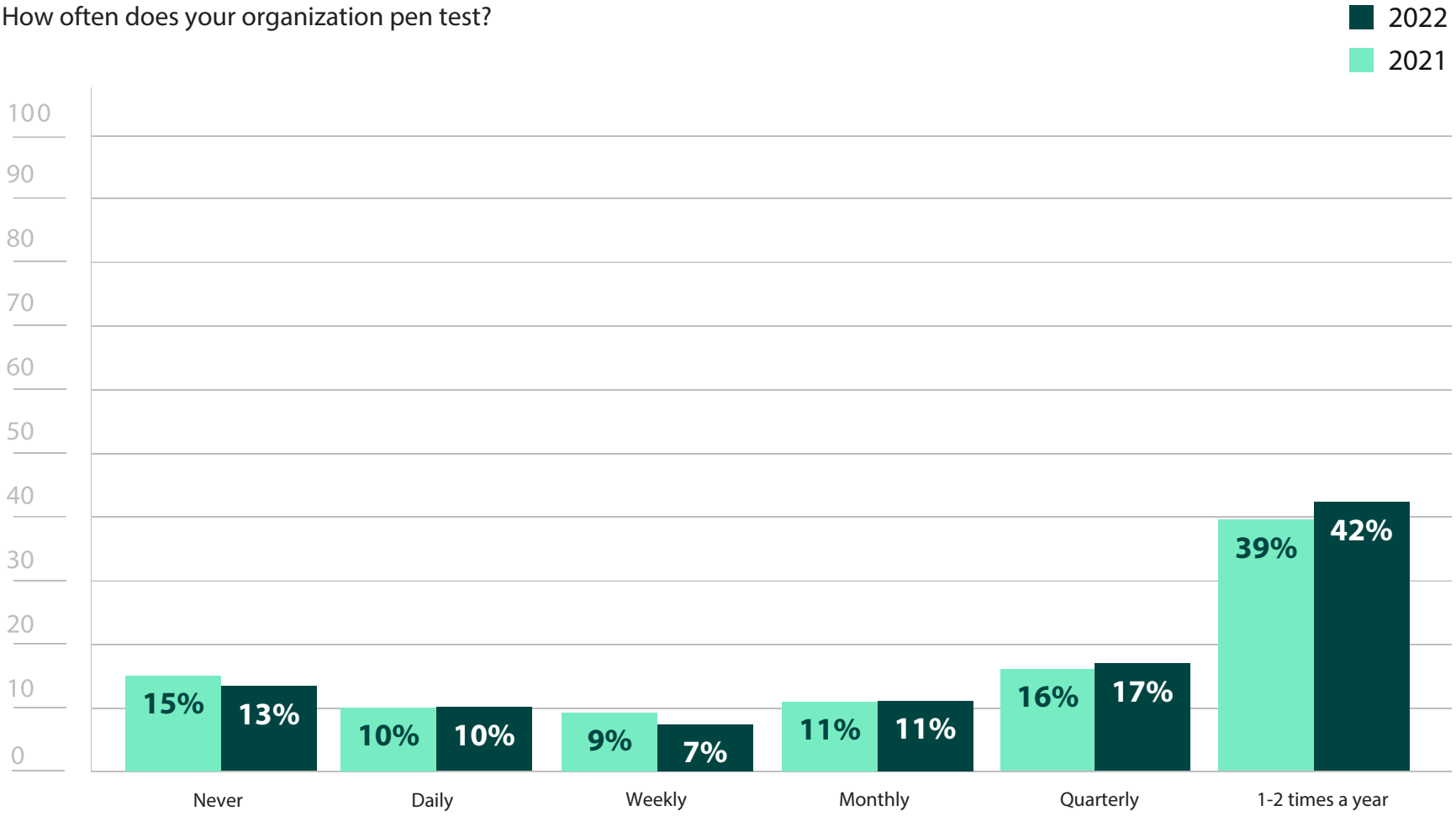


Figure 8: Frequency of penetration testing

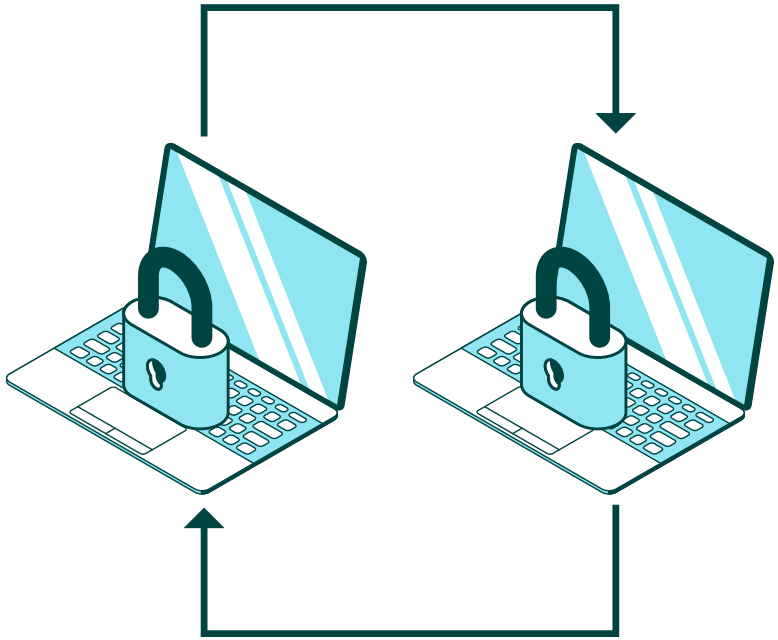
In-House Penetration Testing Efforts

There is a significant decrease in the number of respondents who have an internal pen testing team at their organization (41%), with a 15% decrease from last year's survey (Figure 9). Interestingly, there is also a 10% increase in the number of respondents who have had an in-house team in the past. This may be explained by the 11% increase in people not having an internal team because they felt they didn't need one full time (Figure 12).

However, this does not appear to mean that penetration testing has decreased as a priority, as there is a 7% increase in those who use third-party testing exclusively (Figure 12). Additionally, there is a dramatic 24% decrease in those that list funding as a reason they do not have an in-house penetration testing team, so there does not appear to be an issue with resources, either. As the economy recovers from the pandemic, organizations may simply be finding a balance in what security processes work best.

This decrease in the number of in-house teams may also indicate that security teams are instead being given the additional task of running basic penetration tests, which are now easier to do with penetration testing tools. In fact, 54% of respondents who did not have internal teams noted that pen testing technology influenced their decision on whether to have an in-house pen testing team (Figure 13).

It is worth noting that organizations that did have teams do seem to have grown both in size and experience. There was a 10% increase in those that have 6-10 team members, and a 5% increase in those that have more than 11 members (Figure 10). Additionally, there was a 26% increase in team members with 6 or more years of experience (Figure 11). This could also be reflective of the seeming increase in budgets, as organizations may be able to hire advanced penetration testers.



In-House Penetration Testing Efforts

Do you have an in-house penetration testing team?

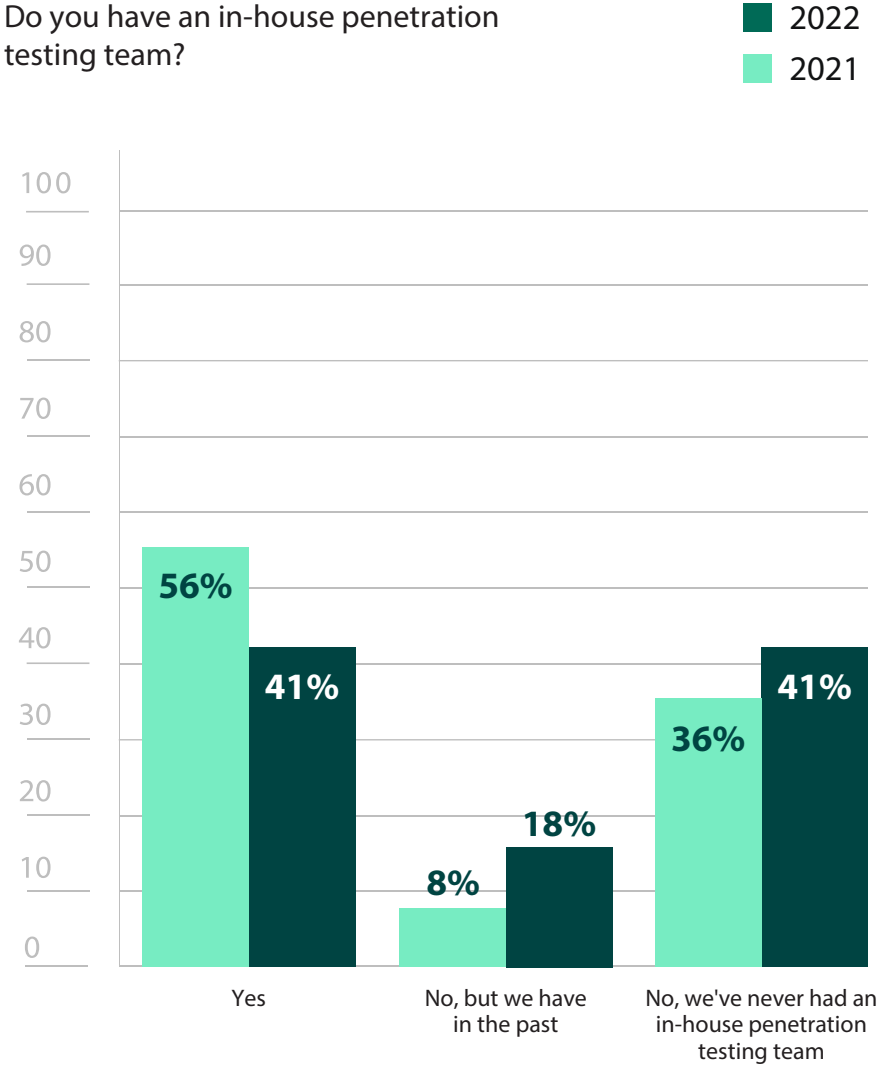


Figure 9: In-house penetration testing

In-House Penetration Testing Efforts

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

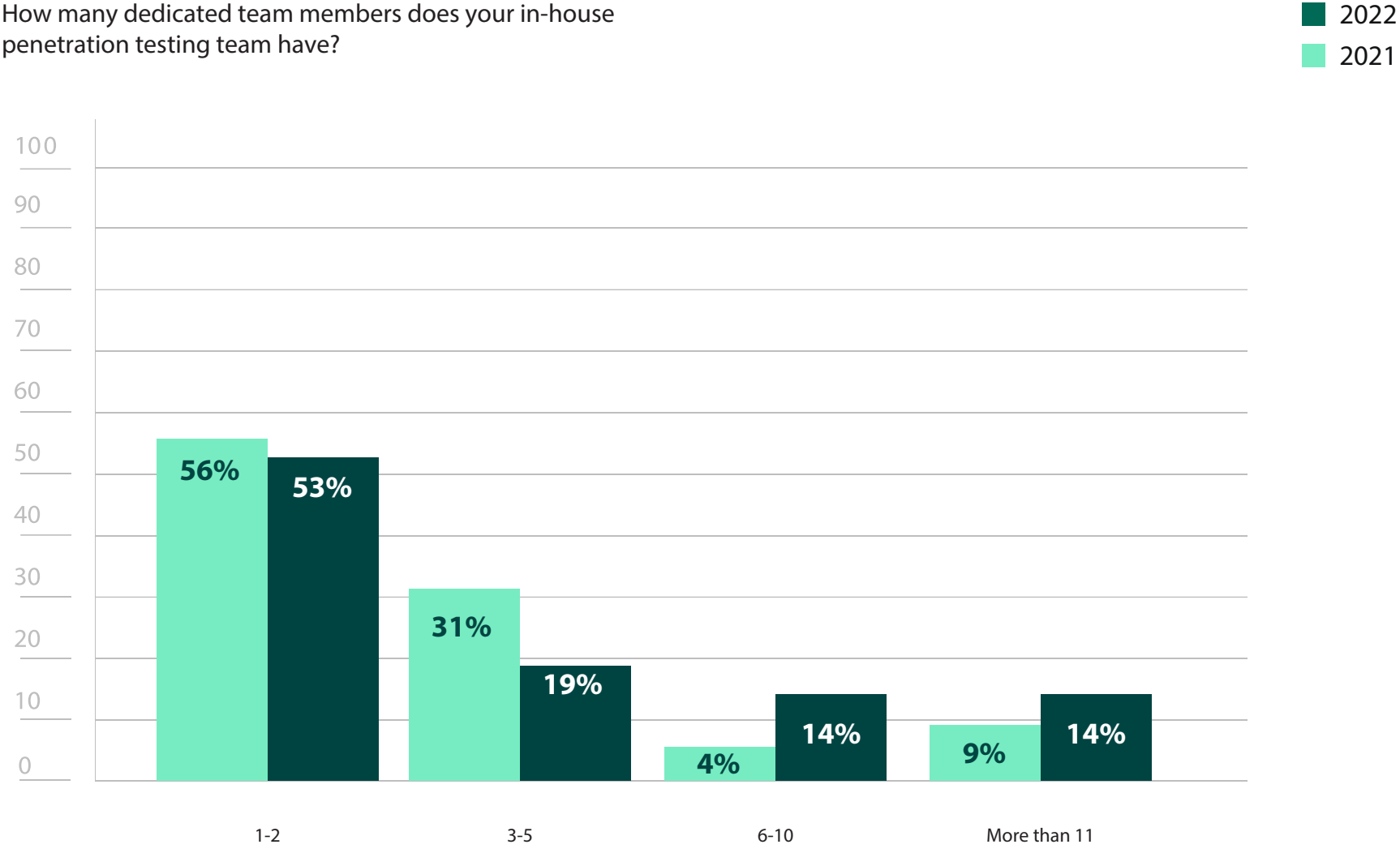


Figure 10: In-house pen testing team size

In-House Penetration Testing Staffing Challenges

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

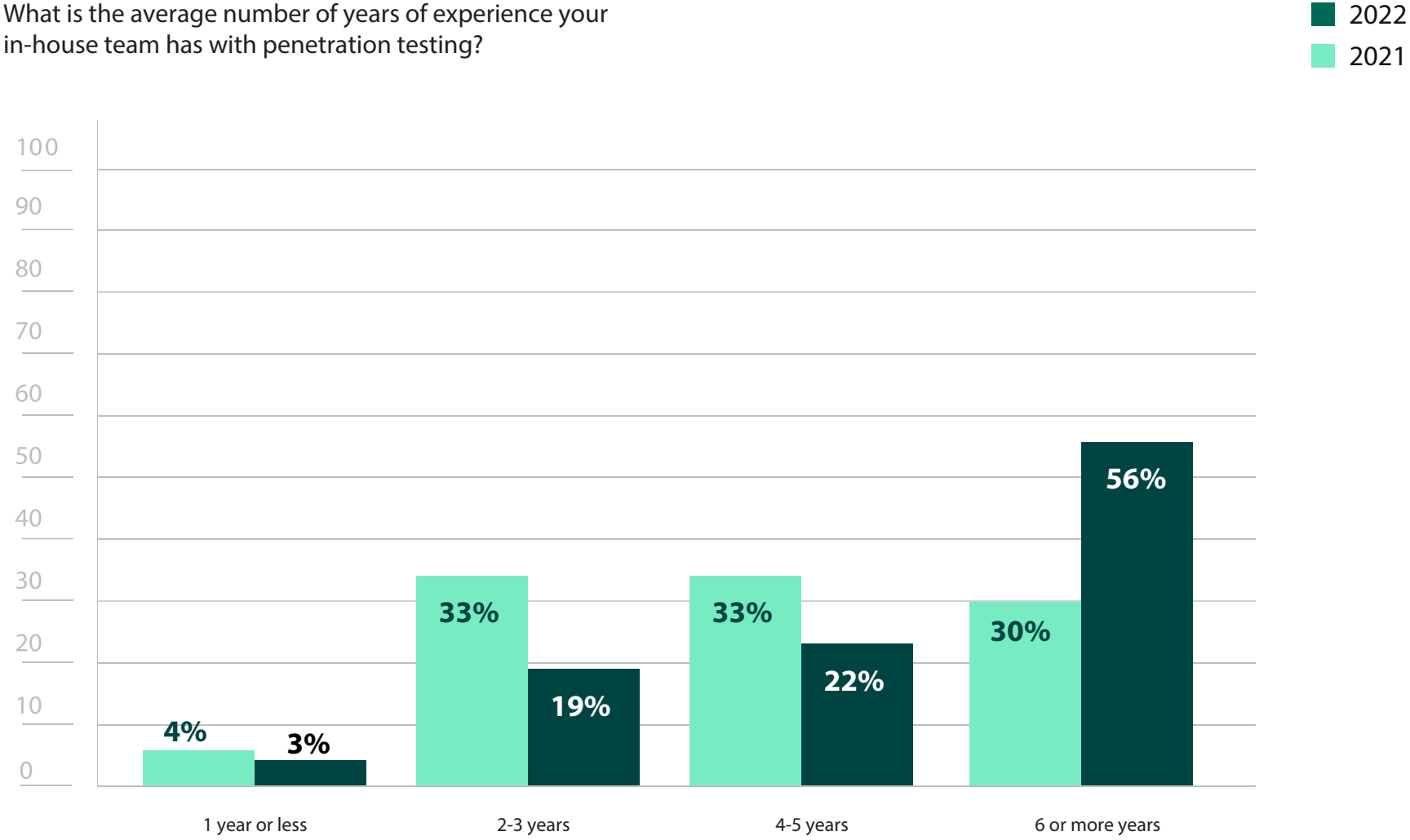


Figure 11: Years of experience of in-house pen testing team

In-House Penetration Testing Staffing Challenges

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

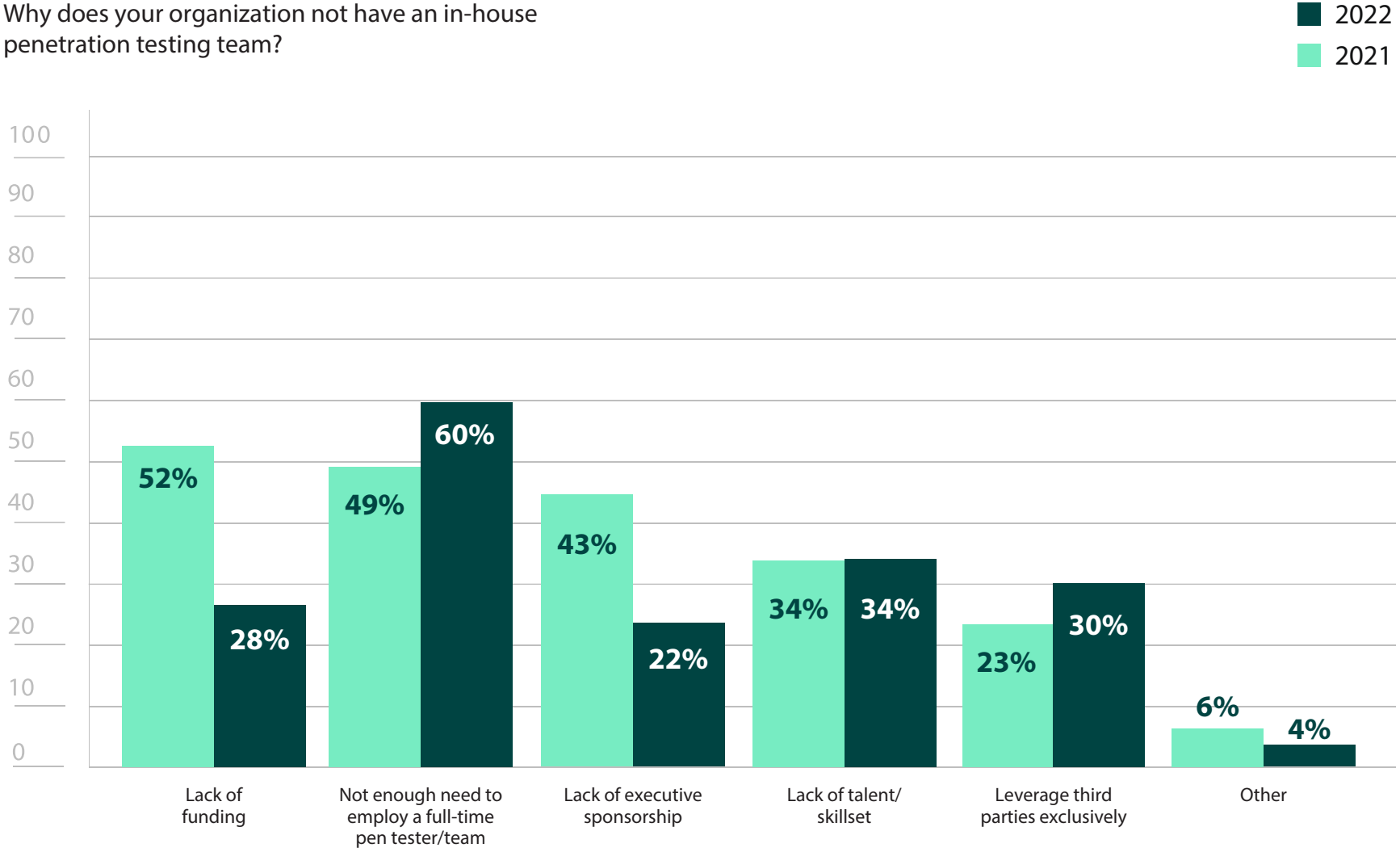


Figure 12: Reasons for not having an in-house pen testing team

In-House Penetration Testing Staffing Challenges

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

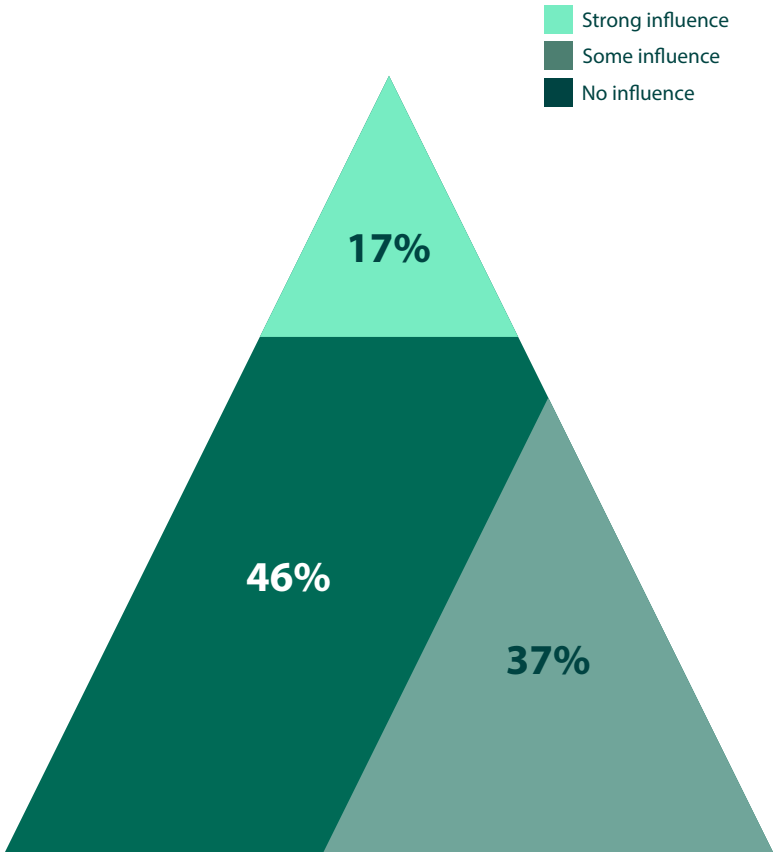


Figure 13: Influence of pen testing technology

Remote Work

The COVID-19 pandemic has made a lasting impact on the workforce, with many companies declaring their employees will now be permanently remote or hybrid. Security teams will have to continue to adapt to the challenges that such an infrastructure poses, shifting priorities as needed.

The top three changes are the same as last year, with network (38%) and web application tests (35%) being given more emphasis and the scope of pen tests being broadened (35%). The numbers are generally down from last year, which may reflect those strategies had already been revised sufficiently in 2020 (Figure 14). The 8% increase for those that have had no impact on their pen testing priorities is somewhat surprising given how much remote work increases the attack surface. For example, security teams can't verify how employees are managing their home networks, potentially adding multiple new attack vectors. Running more network security tests will help to identify new vulnerabilities that result from a newly remote workforce.

Remote Work

How has the increased emphasis on remote work altered your pen testing strategy or priorities?

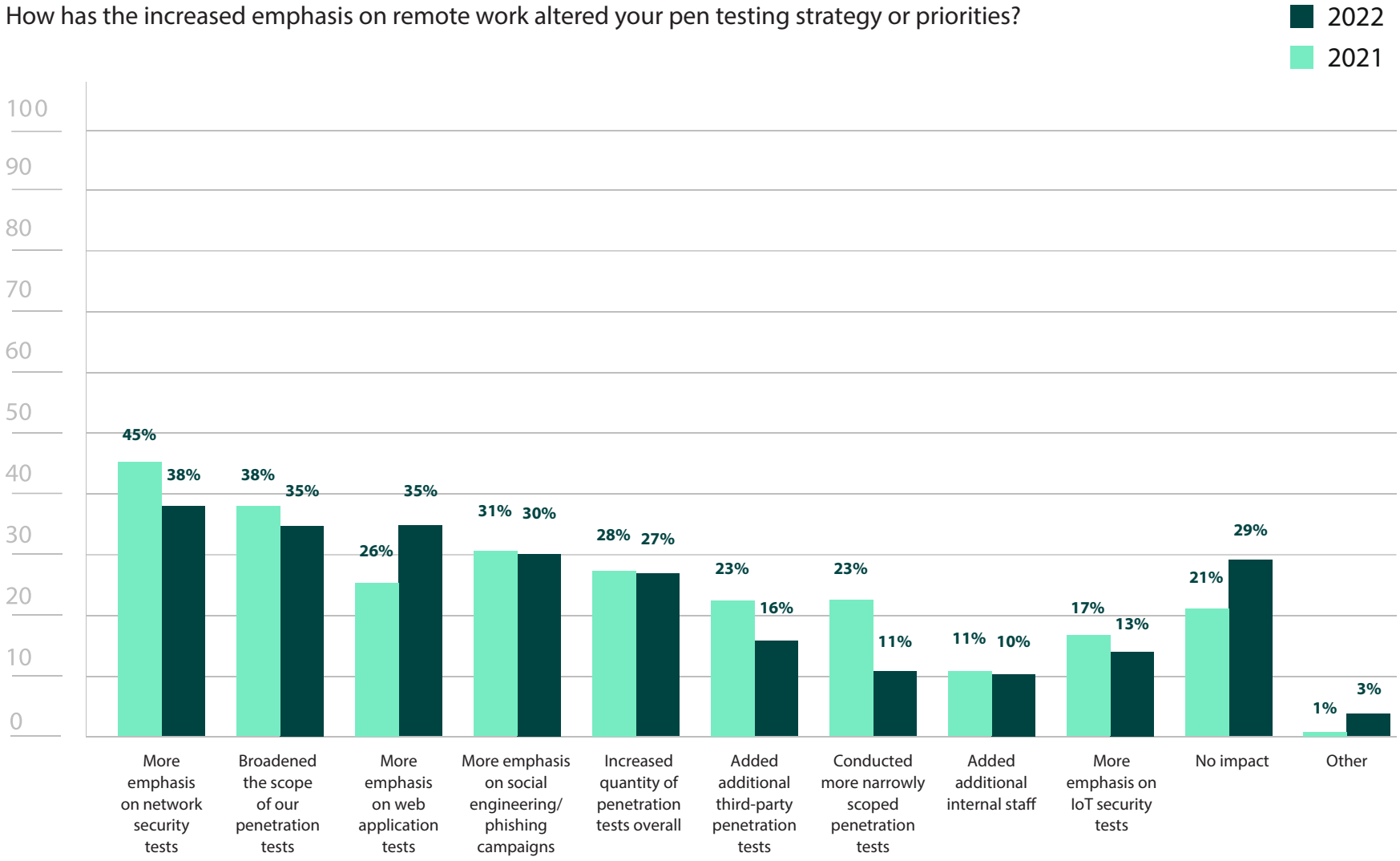


Figure 14: Effect of remote work on pen testing strategies and priorities

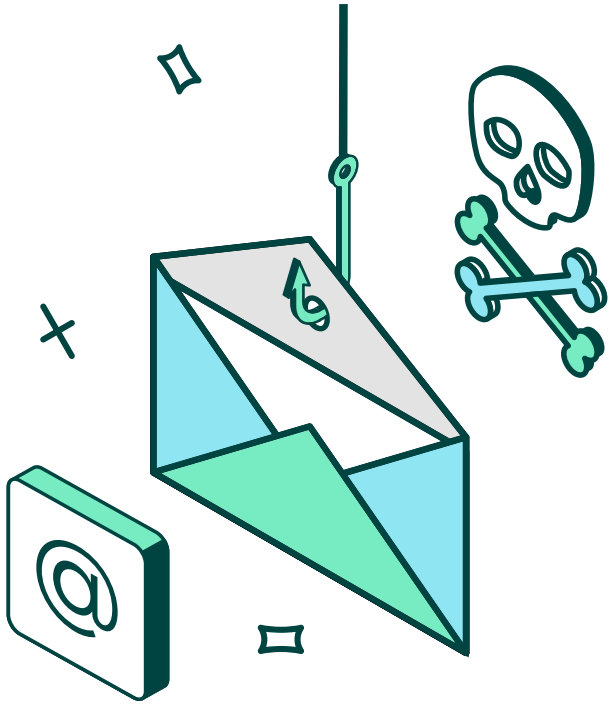
Third-Party Services

Third-party pen testing teams remain a popular resource, with 83% of respondents leveraging third party teams in some capacity (Figure 18). For organizations that don't have any tests conducted in-house, third-party pen testing teams may be the only way an organization can find out the state of their security. While not as large of an issue as it was in last year's survey, 32% of respondents listed a lack of personnel to conduct such tests, emphasizing the importance of having pen testing services available (Figure 15).

Even when organizations have security teams that can conduct penetration tests, they may not be dedicating 100% of their time to it. Third-party teams are fully immersed specialists that can stay up to date on the latest trends. They can be an invaluable way to bring different skillsets to the organization, not to mention a fresh perspective. This external viewpoint (63%) and fresh skillset (56%) were top reasons respondents listed for why organizations use third-party teams (Figure 15).

Wanting an impartial assessment from someone who is unfamiliar with their particular environment may also be a reason for why 79% of organizations tend to change services at least every 2-3 years (Figure 17). Alternatively, while it is not mandated by any specific compliance requirement, rotating between at least two firms is typically considered an industry best practice. Given how many respondents cited compliance (58%) as a reason for using thirdparty teams, this may also be part of why changing providers is so common (Figure 15).

Though many assume an in-house team is meant as a replacement for third-party services, organizations should ideally use both. IT environments are constantly changing, and small mistakes could easily open up new attack vectors. While third-party services bring an objective outlook and diverse skillsets, internal pen testing team can provide regular, standardized testing. With 63% of respondent using both types of services in some capacity, it appears that a balance between internal and external pen testing is regularly being followed (Figure 18).



Third-Party Services

Why does your organization utilize third-party penetration testers?

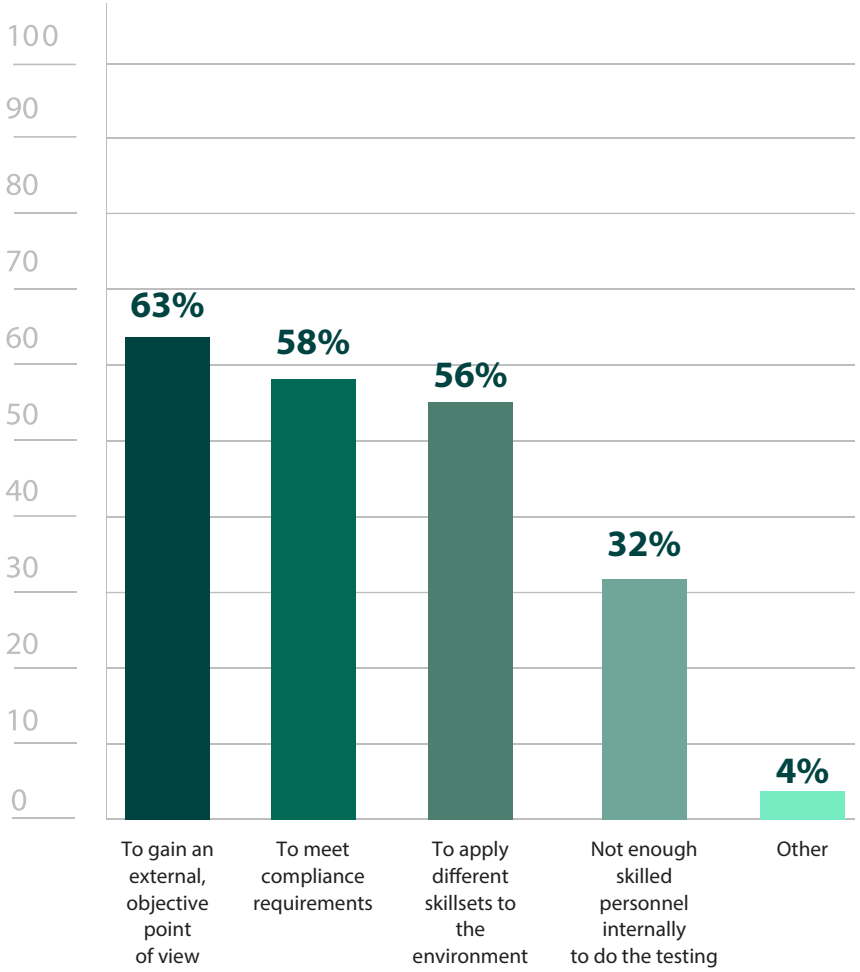


Figure 15: Reasons for utilizing third-party pen testing services

How often do you conduct third-party penetration tests?

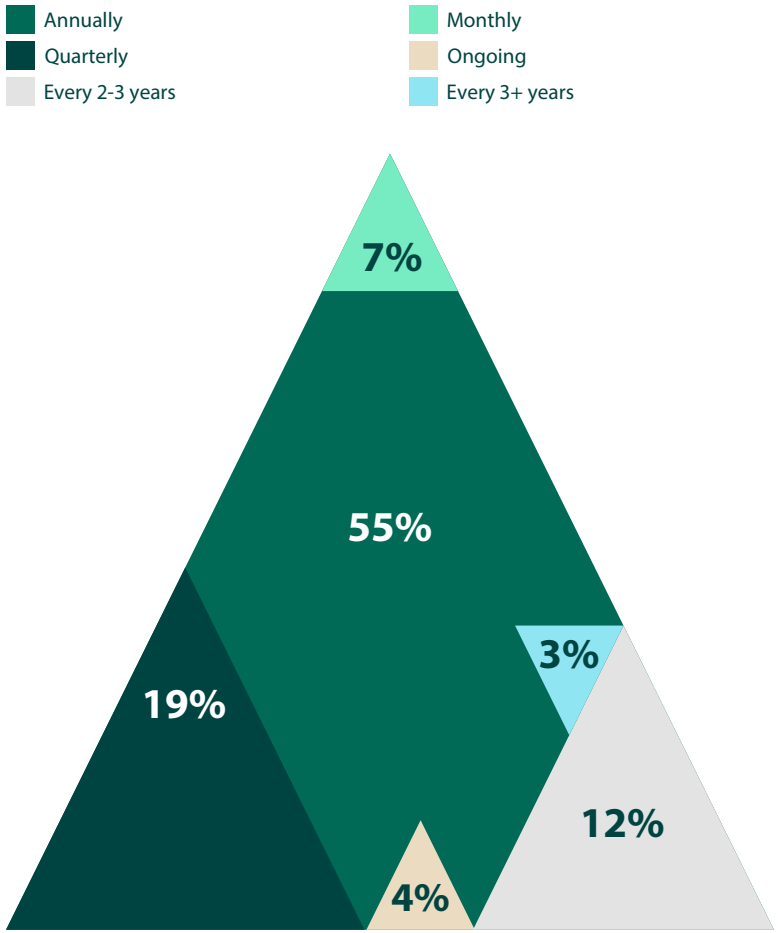


Figure 16: Frequency of third-party pen tests

Third-Party Services

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

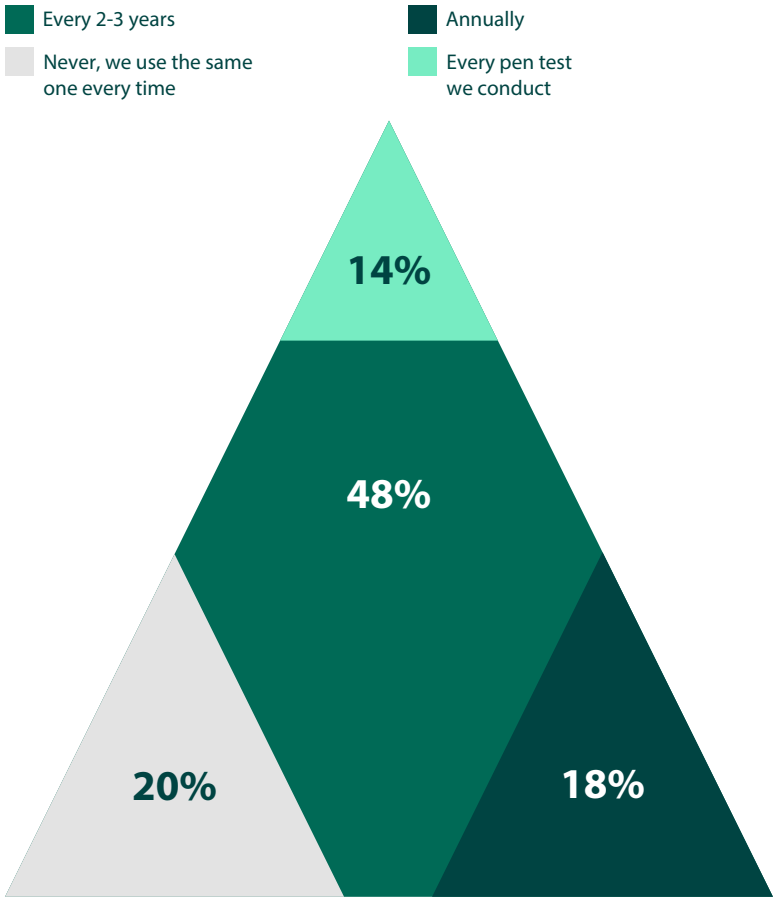


Figure 17: Rotation frequency of third-party pen testing services

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

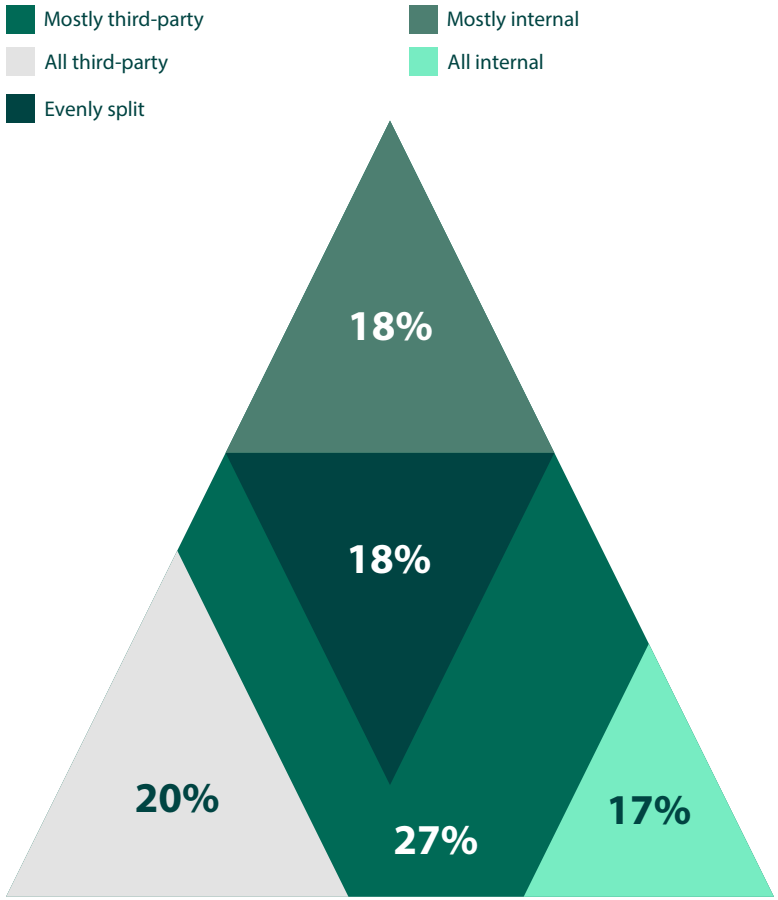


Figure 18: Split between internal and third-party pen testing resources

Third-Party Services

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

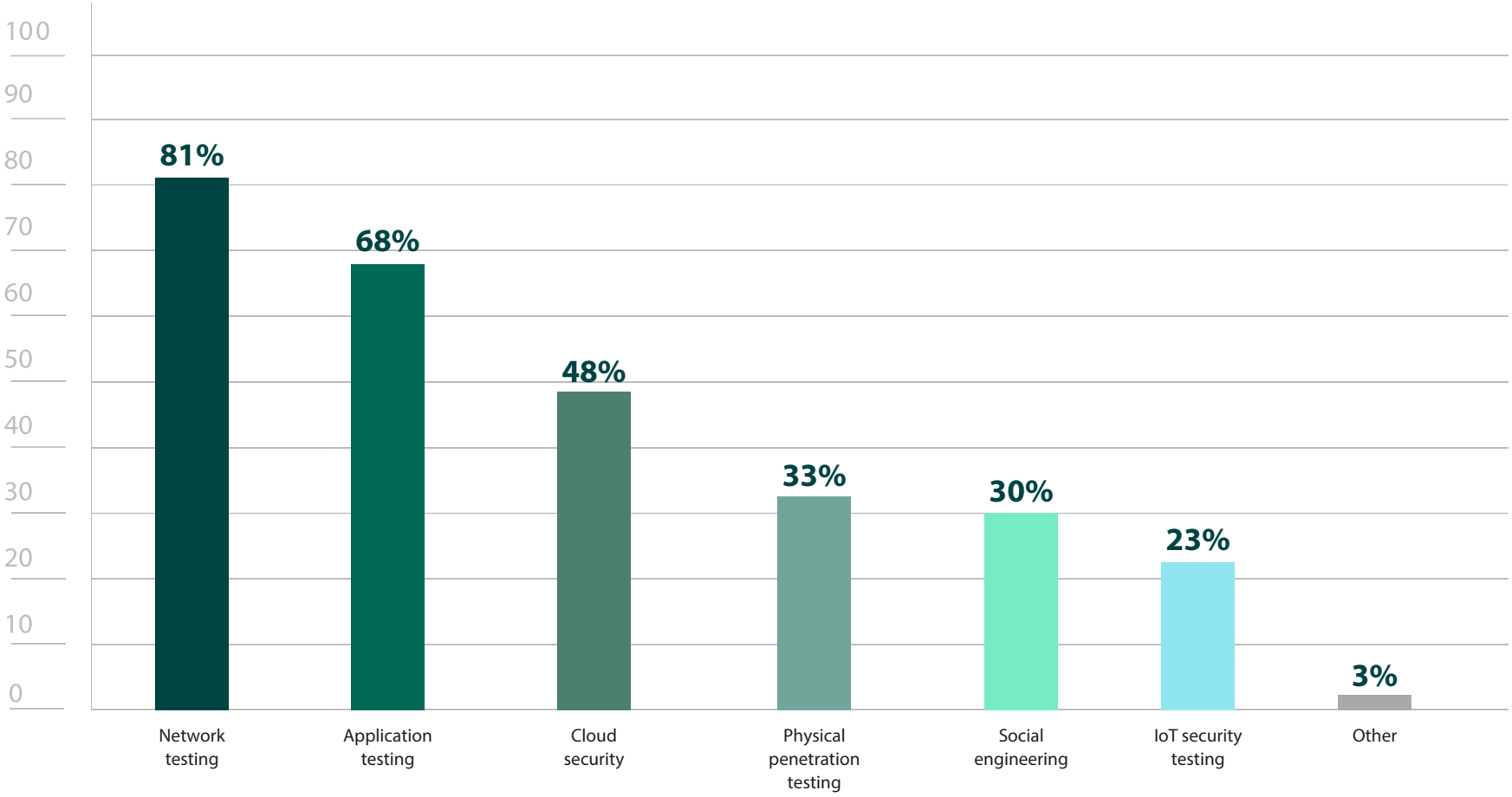


Figure 19: Types of pen tests third-party testers are requested to perform

Penetration Testing Tools

Respondents universally use at least one pen testing tool of some kind, illustrating how integral they are to the penetration testing process (Figure 20). 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. Consequently, most penetration testers use a variety of tools during engagements, either commercial, open-source, or a combination of the two. There was a 12% increase from last year for those using both commercial and open-source tools, potentially illustrating how some toolsets have been expanded (Figure 20). Interestingly, there was a 13% decrease in those solely using free/open-source tools, so perhaps organizations have gotten the budget to add one or more commercial tools to their library.

Available features and functionality are top of mind when in the market for a paid pen testing tool, with 94% of respondents listing it as an important evaluation criterion (Figure 21). In terms of the features that they're looking for, reporting remained the most sought after capability in paid penetration testing tools, with 77% of respondents listing it as an important feature (Figure 22). This corresponds with the high number of people who use pen testing for compliance— automated reporting functionality maintains consistency and produces reports that can be used for regulatory auditors.

At 67%, having an extensive threat library is the second most sought after feature (Figure 22). Since exploit writing takes time and expertise, finding reliable, expertly tested exploit libraries that are regularly updated can make testing efforts significantly more efficient.

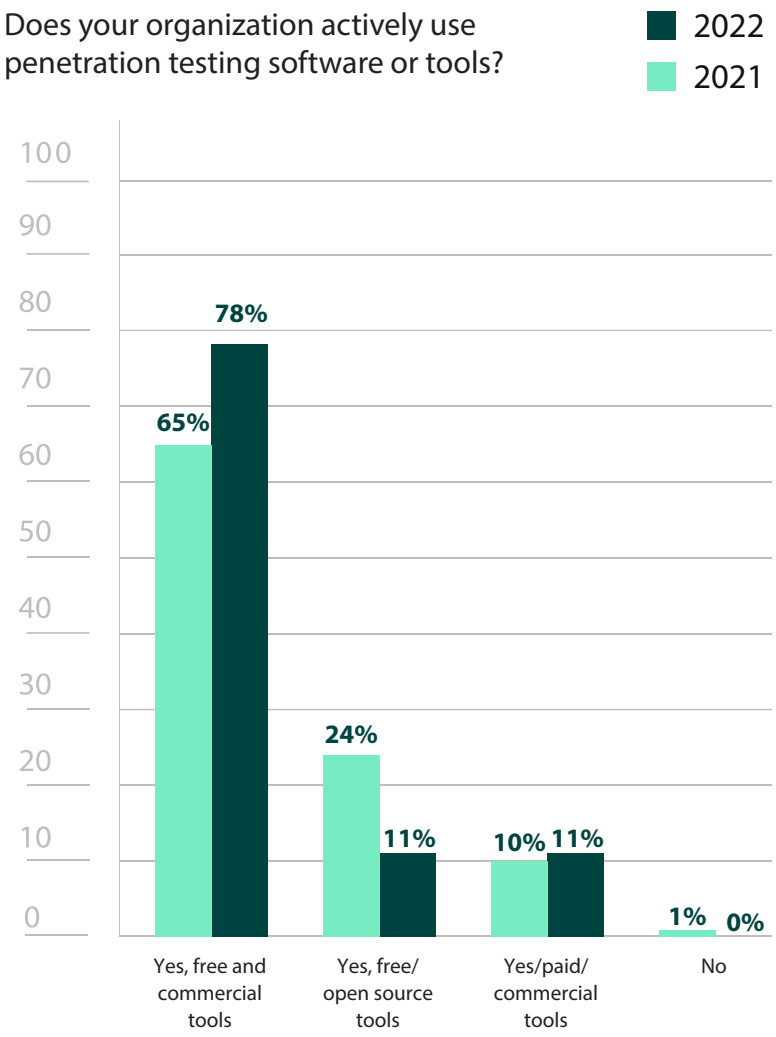


Figure 20: Active use of penetration testing software

Penetration Testing Tools

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

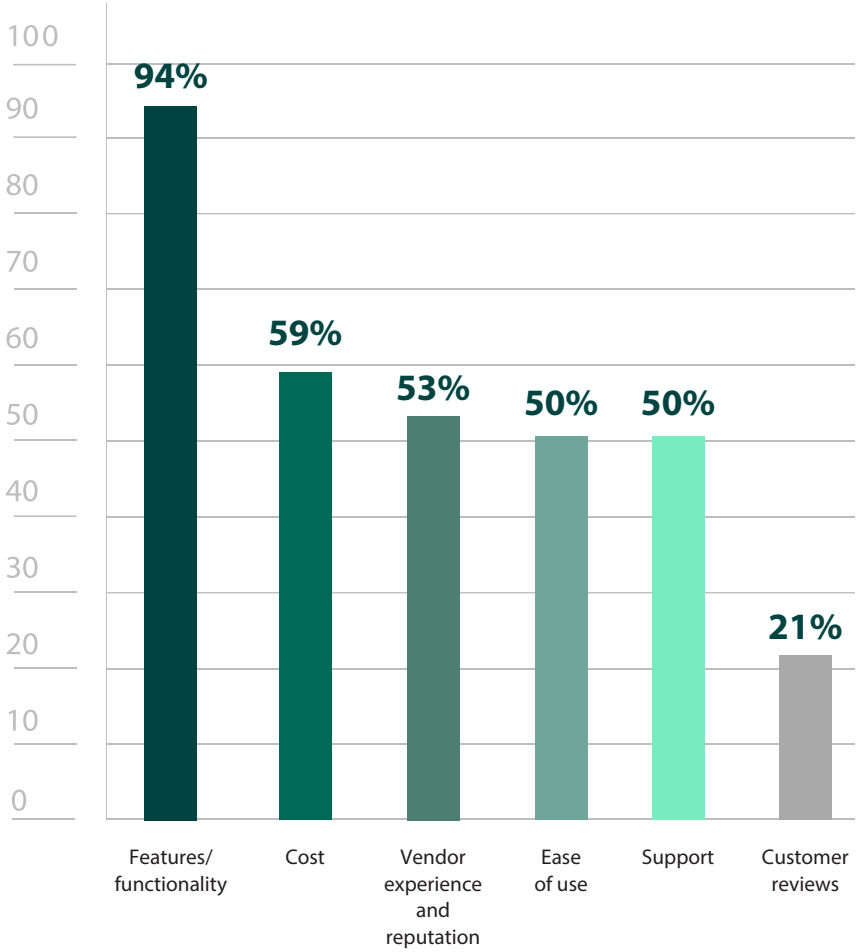


Figure 21: Most important criteria for evaluating pen testing software

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

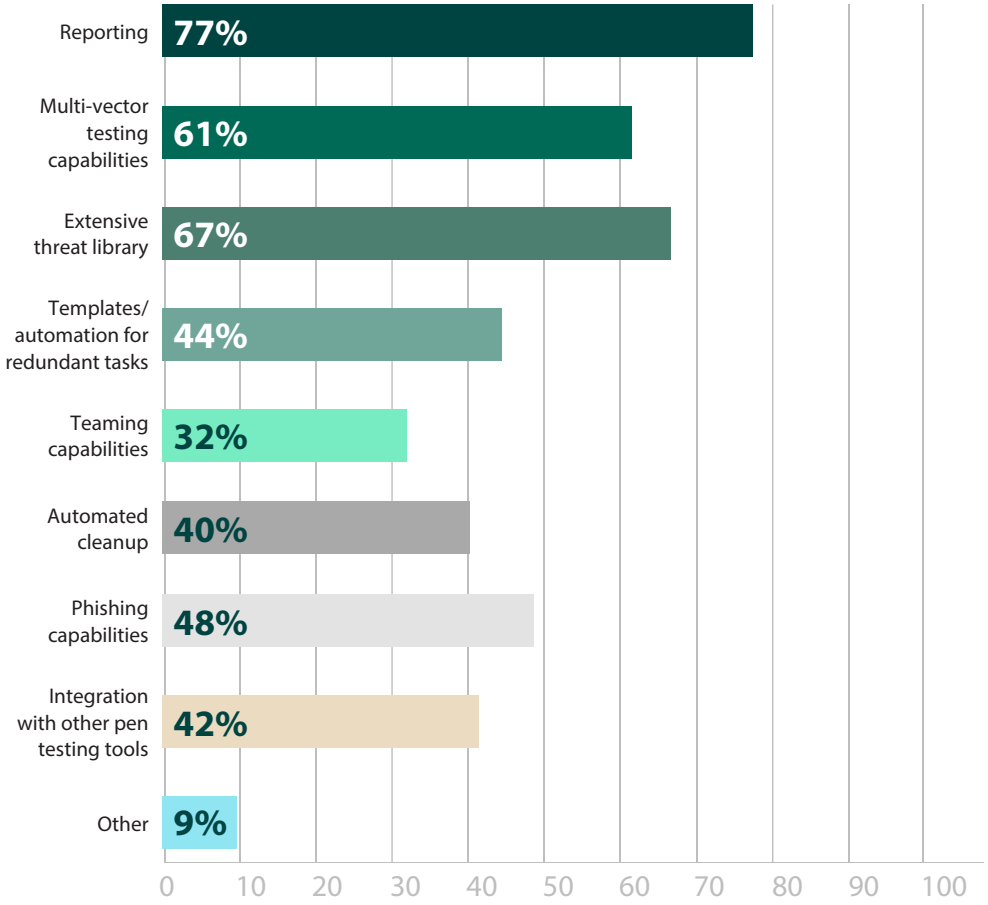


Figure 22: Most important features in pen testing software

Other Security Assessment Solutions

As mentioned earlier, penetration testing is an important component in a proactive security strategy. Other tools that security professionals are using are indicative of where organizations are in their vulnerability management journey (Figure 23). Vulnerability scanners (87%), for example, are usually the first step, staying a bit higher level and having a broad scope, often covering large portions or the entirety of a security environment. Post-exploitation and threat emulation, on the other hand, are commonly used in Red Teaming efforts, which are typically only used by those who have a fairly well-established program in place.

Though integration wasn't the most sought-after feature in pen testing tools (42%), it experienced a small growth from last year, and may continue to do so as organizations expand their security portfolio and want to centralize as many tools as possible (Figure 22). Comprehensive penetration testing tools can be the ideal point of unification, as many can already integrate or incorporate with other common security assessment tools respondents are using, like vulnerability scanners (87%) (Figure 23).

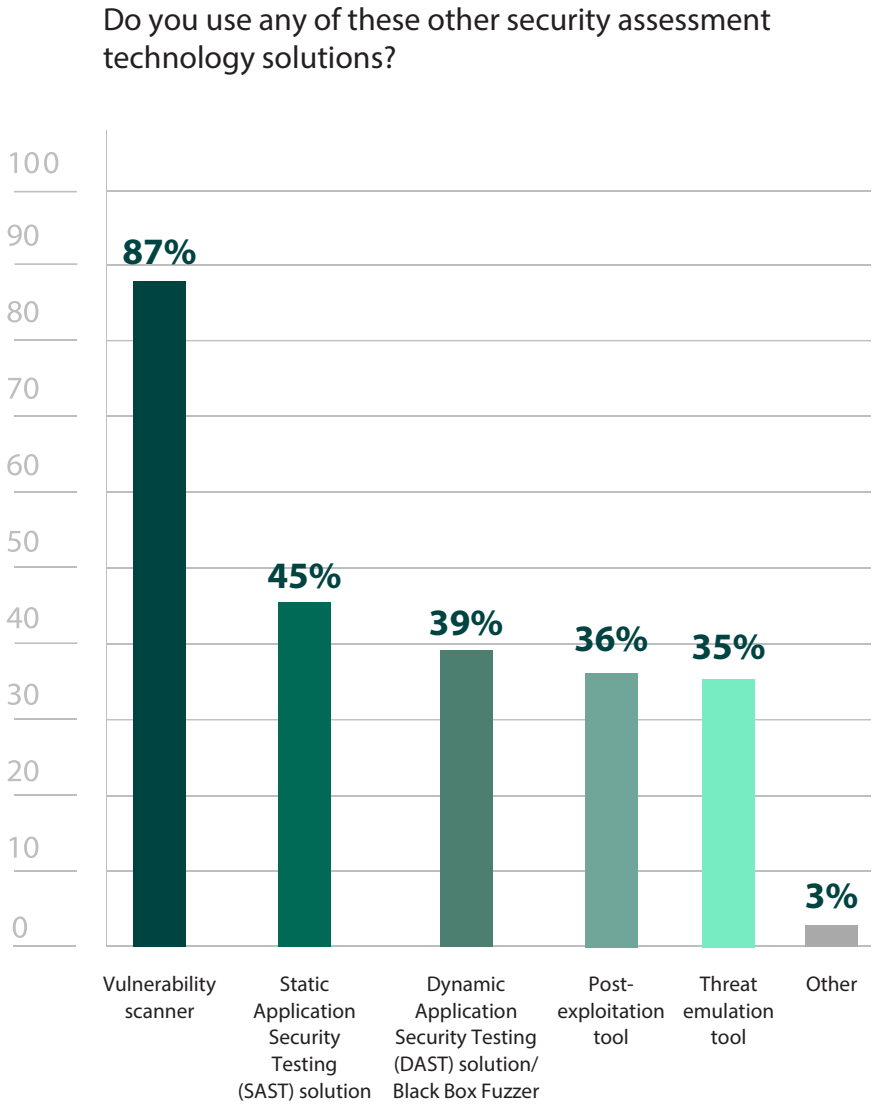


Figure 23: Other security assessment tools used

Pen Testing in Different Environments

As the most common operating system, it's not surprising that Windows (87%) was the most common area respondents were most concerned about testing (Figure 24). However, it's clear that there is some level of concern about every type of environment. It was promising to see Linux have such a high level of concern (61%), considering how many used to believe Linux was innately secure and relatively immune to malware.

However, it is somewhat troubling to see both IoT (20%) and SCADA (8%) on the low end of the spectrum. Looking at respondents solely from the manufacturing industry, where SCADA is most common, only 20% of respondents are concerned about pen testing this environment. Many SCADA and IoT devices don't have the more defensive measures in place. For example, there is no real antivirus for an MRI machine. Additionally, certain IoT devices and SCADA systems are essential to the primary function of an organization, so taking control of these devices or simply disabling them can completely cripple a business. Previous large scale attacks have even affected the functionality of cities or countries.

Similarly, while it was promising to see both external (86%) and internal (72%) infrastructures have high pen testing numbers, cloud infrastructures (46%) were significantly less commonly tested (Figure 25). Cloud environment usage is still growing at a steady pace, and the myth persists on who is responsible for their security. The cloud provider is not solely in charge of ensuring that a cloud environment is protected. Depending on which environment an organization uses (IaaS, PaaS, or SaaS), responsibilities will vary, but it is always a shared endeavor. Ideally, cloud environments should be pen tested just as often as internal and external environments.

Pen Testing in Different Environments

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

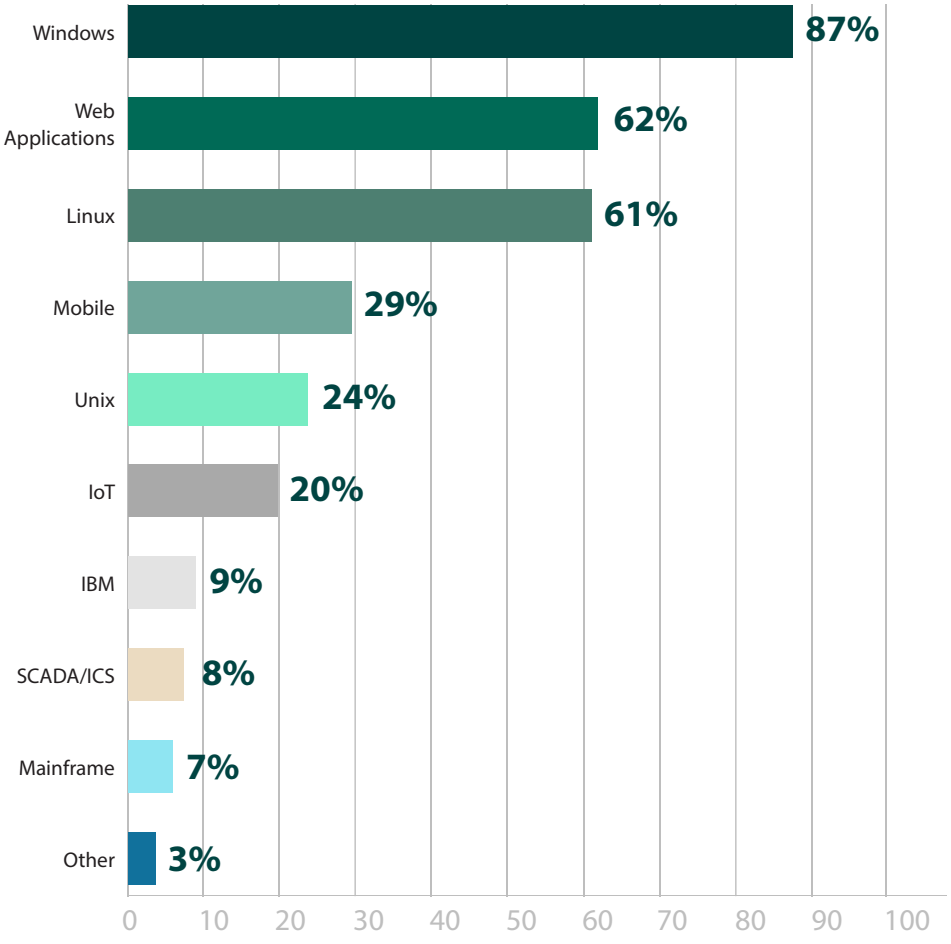


Figure 24: Environments in need of pen testing

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

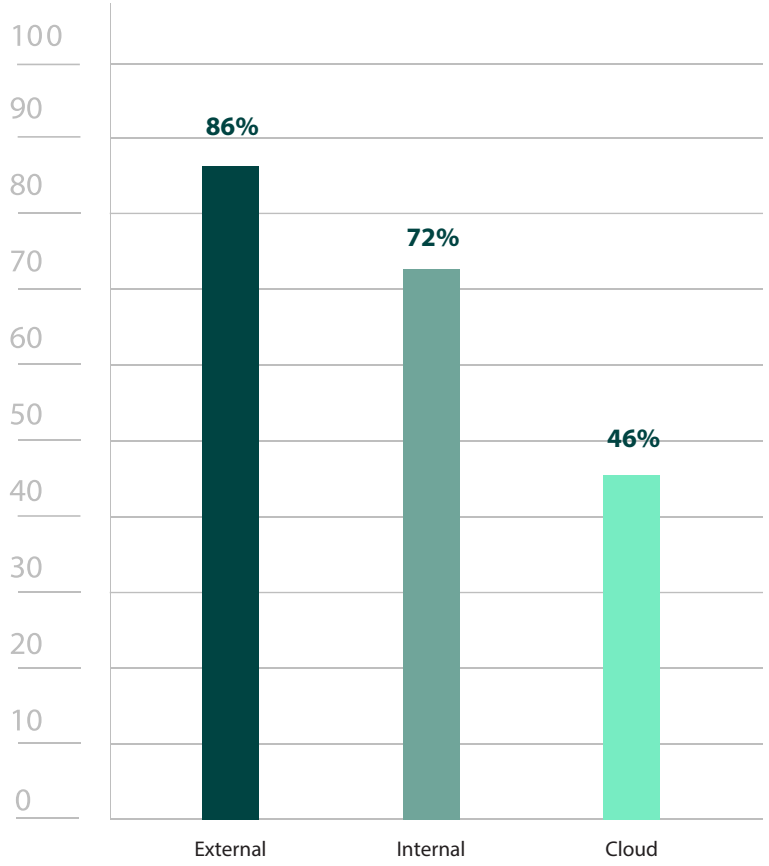


Figure 25: Infrastructures regularly pen tested

Demographics

Which region is your organization headquartered?

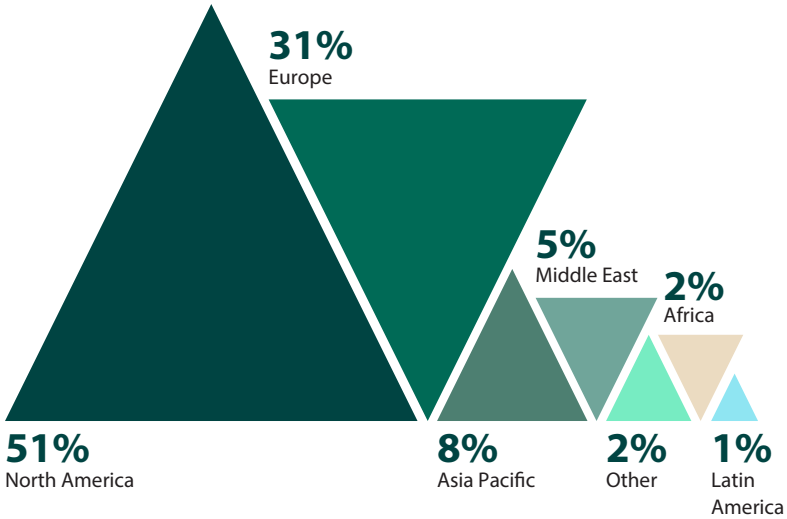


Figure 26: Regions surveyed

What is your primary industry?

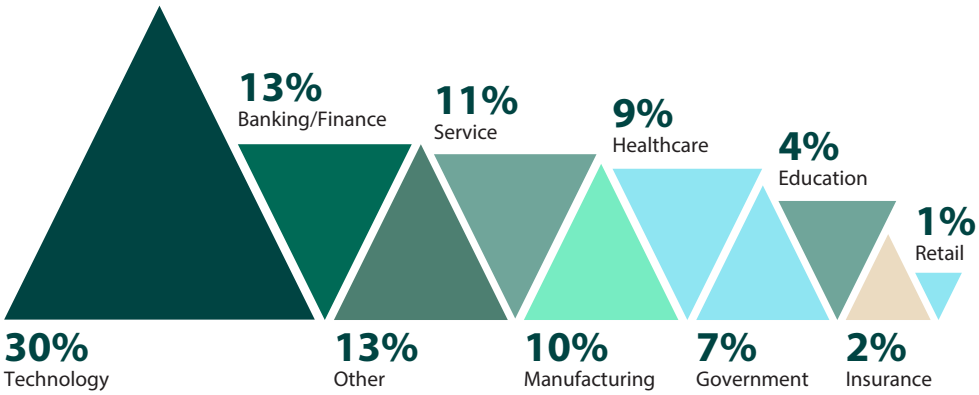


Figure 27: Industries surveyed

This report is based on the results of a comprehensive survey of cybersecurity professionals around the globe with the aim of presenting an accurate picture of how penetration testing is utilized by different organizations and to provide insights about the effectiveness of ethical hacking strategies. The respondents represent a diverse cross-section of industries, company size, job level, and region.

Demographics

What is your job level?

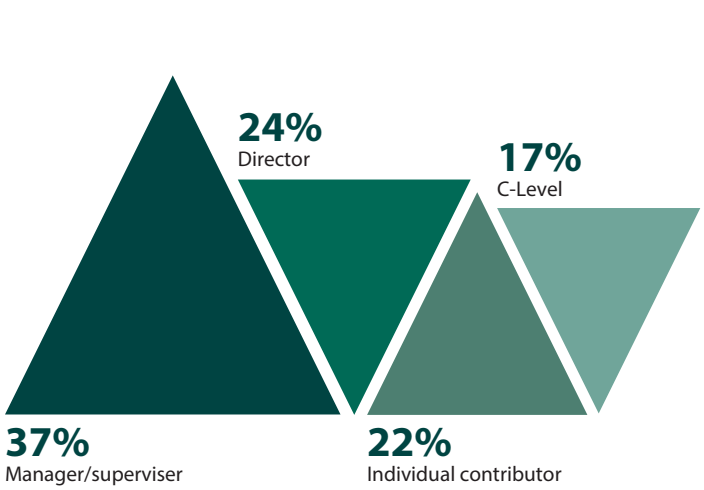


Figure 28: Job levels surveyed

How many employees does your organization have?

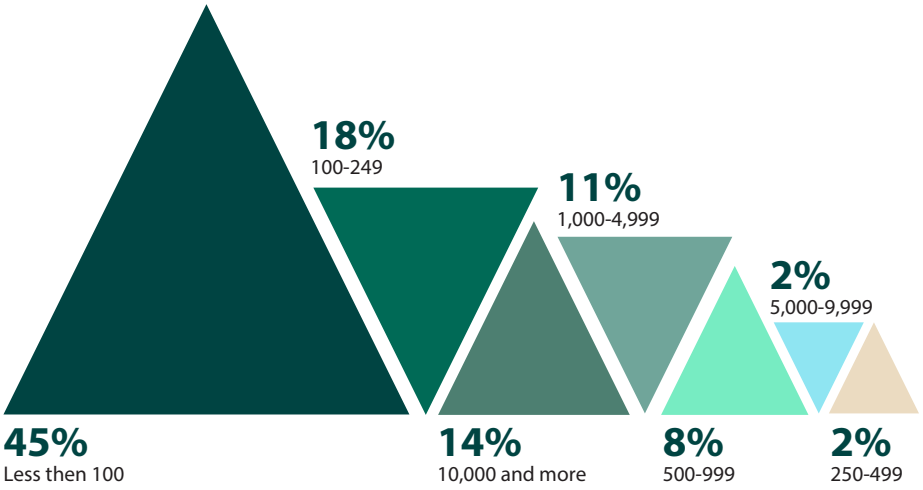


Figure 29: Size of organizations surveyed

Conclusion

The goal of this survey was to provide continued visibility into how cybersecurity professionals are utilizing pen testing. The results revealed the broad range of ways organizations pen test and gives every sign that penetration testing will remain a crucial practice for years to come. The flexibility in its implementation is key to ensuring these tests are routinely conducted—organizations have the option to use in-house teams or third-party services and open-source or commercial tools. This is a positive indication that any organization can tailor a program to suit their needs and available resources.

While funding obstacles from last year appear to have been reduced, the continued challenges of phishing, ransomware, and inattention to specific environments prove more concerning long term, particularly given the prevalence of overconfidence in existing cybersecurity strategies. Putting your organization to the test on a regular basis is still the best way to ensure you're continuously reducing your cyber risk exposure. The goal of pen testing shouldn't simply be to check it off the to-do list.

Penetration testing not only provides short term value by finding and prioritizing the security weaknesses that currently pose the highest risk, it can also provide long term value as part of a comprehensive security portfolio that is designed to adapt to both the new and persisting challenges of cybersecurity. By continuing to focus on building a comprehensive strategy, with proactive processes like penetration testing being prioritized as much as the traditionally defensive measures, organizations will deserve to feel confident in their security posture.

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-0223-r2-vm)