

VOICE OF AN IN-HOUSE PENTESTER

2024 REPORT



Sprocket
Security

Voice of an In-House Pentester

News of massive data breaches fills the headlines each day. The frequency and severity of cyber attacks have only increased in recent years, and attackers are not only taking advantage of vulnerabilities in networks and systems, but also taking advantage of unaware employees through social engineering attacks. Security teams need all the help they can get in protecting their organization.

One of those tools is penetration testing, which looks for risks and security vulnerabilities utilized by real-world hackers against an attack surface. This helps organizations know where to take action to remediate vulnerabilities and increase their overall security awareness.

But are security teams today using penetration testing to their advantage and seeing positive results? Or are they missing out on the benefits because there are still areas for improvement?

To find out, we surveyed 200 in-house pentesters, individuals who perform penetration testing within their organizations. They shared their insights on why their penetration testing programs are successful, the challenges they encounter, the tools they find most effective, and their top priorities for the coming year.

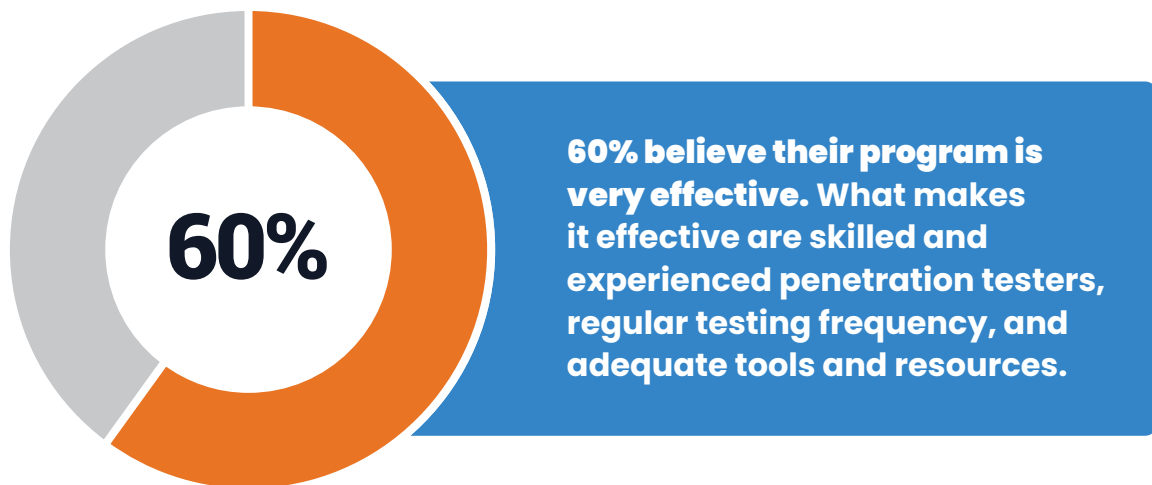
We hope these insights inspire you to enhance your own penetration testing efforts and strengthen your organization's defenses.

Casey Cammillerri
CEO and Founder, Sprocket



Key Findings

Here are seven findings from our respondents about their penetration testing program:



Identifying and prioritizing vulnerabilities is their top objective. They also use penetration testing to validate the effectiveness of security controls and to meet compliance requirements.

The limited scope of testing is their top challenge. Other challenges include keeping up with the rapidly evolving threat landscape and inadequate budgets for penetration testing.

The most common vulnerability they find is weak or default passwords. Other found vulnerabilities include outdated or unpatched software and sensitive data exposure.

The top capability they would add to their program is continuous testing and monitoring. They would also add more experienced penetration testers and threat intelligence integration.

The biggest sign of a successful penetration testing program is improved security awareness. Other signs of success include increased coverage of IT infrastructure and a reduction in the number of vulnerabilities found over time.

Expanding the scope of testing is their top priority for the next year. Other priorities include embracing continuous testing and hiring more skilled penetration testers.



Table of Contents

PART 1

State of Penetration Testing

PART 2

Penetration Testing Priorities and Plans

PART 3

Takeaways for Security Practitioners



PART 1

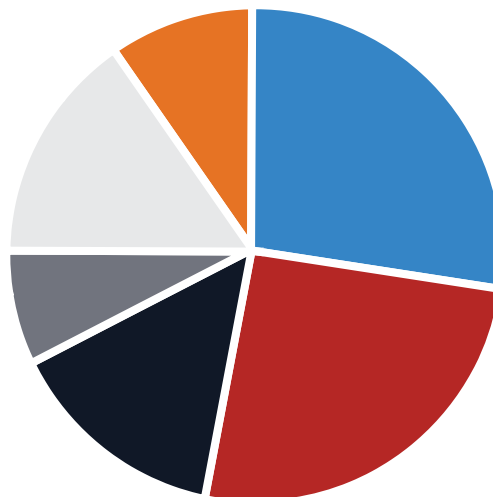
State of Penetration Testing







Penetration testing is a key part of keeping an organization safe. It helps security teams understand system vulnerabilities, uncover weaknesses, and know what steps they need to take next in their security approach. Here's how security teams are approaching their penetration testing, what they're doing to make their program more effective, and what challenges they face.

The majority of in-house testers conduct penetration testing monthly or quarterly

The largest segment (28%) says they conduct penetration testing monthly, while the second largest segment (26%) tests quarterly. 15% test bi-annually, 8% test annually, and 16% test as needed. Only 10% test continuously.

How often does your organization conduct penetration testing?

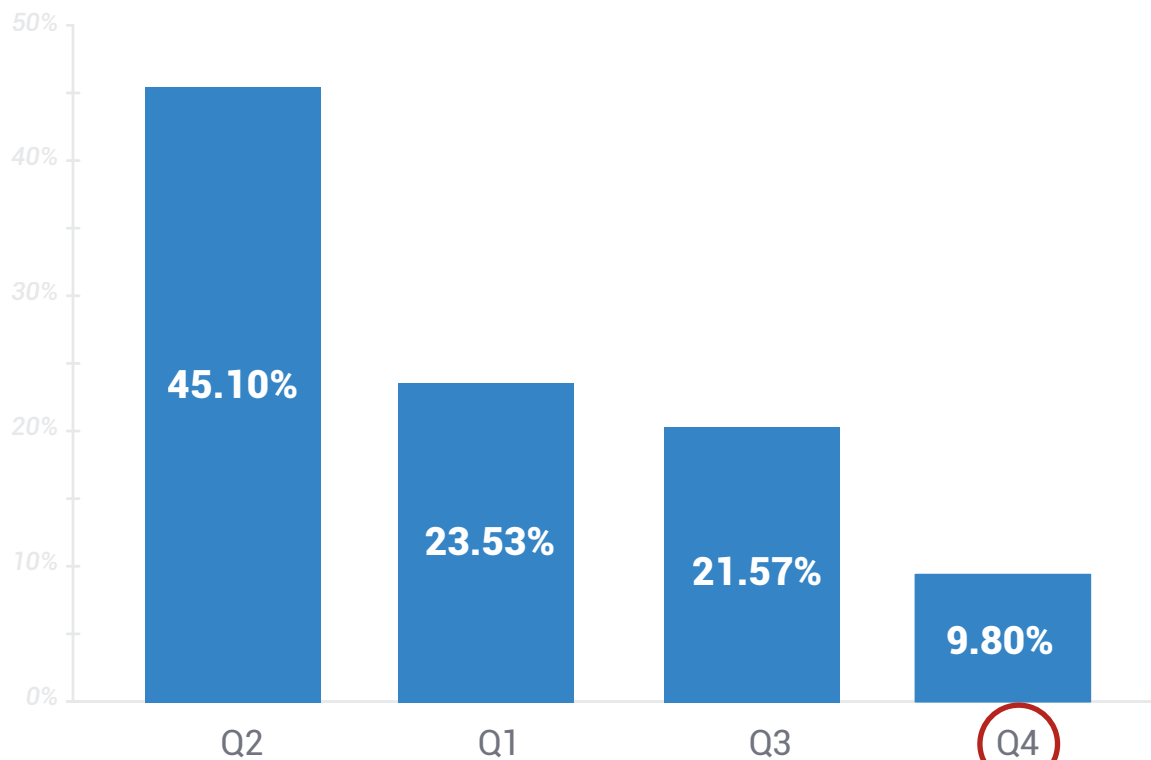


	As needed	15.50%
	Annually	7.50%
	Bi-annually	14.50%
	Monthly	27.50%
	Quarterly	25.50%
	Continuously	9.50%

Nearly half of in-house teams conduct their testing in Q2

The largest segment (45%) conducts their testing in Q2, while the second largest segment (24%) tests in Q1. 22% test in Q3 and 10% test in Q4.

Which quarter do you do your testing?

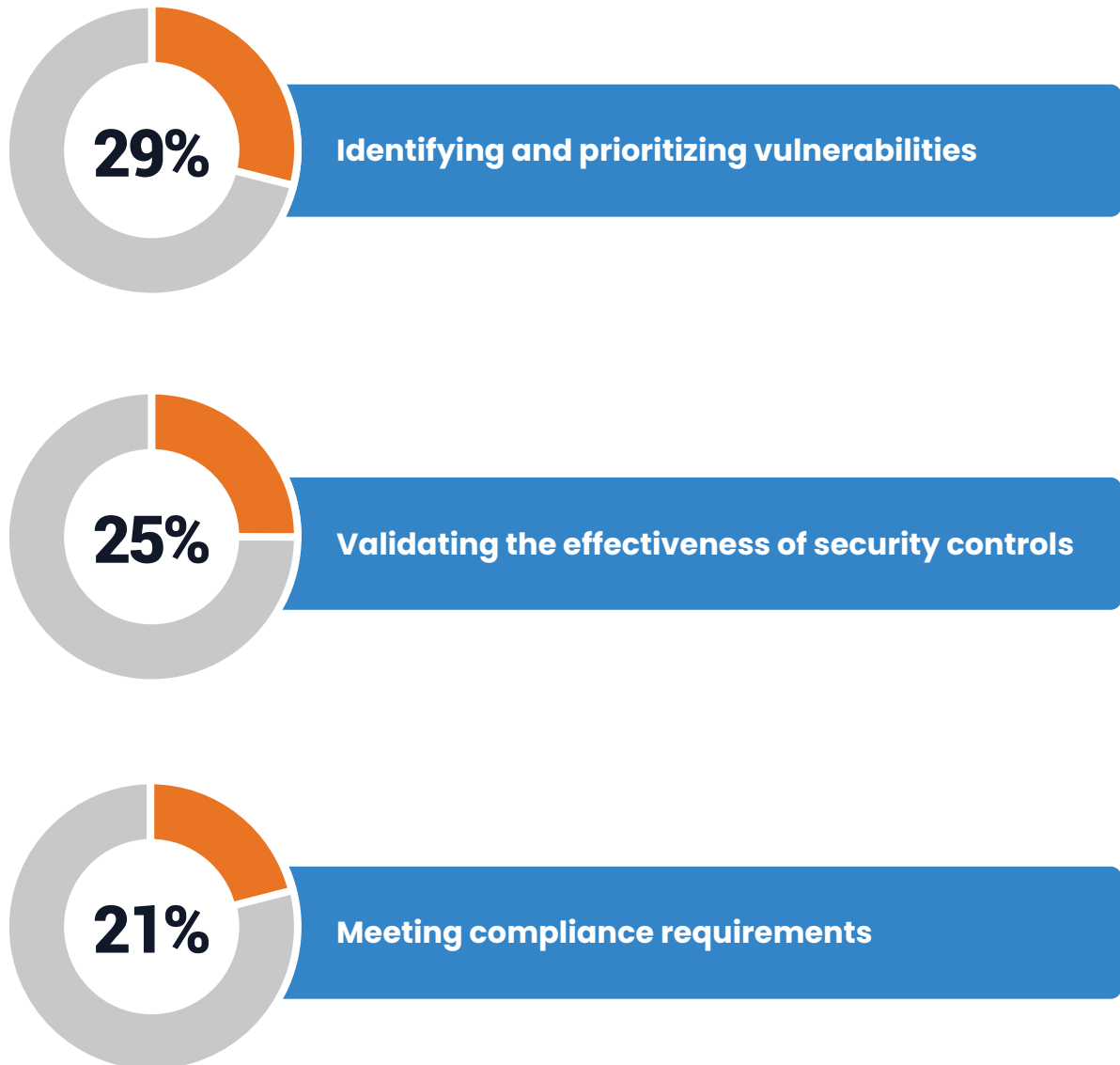


COMMENT FROM CASEY

In-house teams often conduct penetration tests throughout the year, ramping up in Q2. However, compliance pressures lead many organizations to hire third-party pentesters in Q4. The tendency toward periodic testing, whether in Q2 or Q4, can leave organizations vulnerable to emerging threats in between engagements. Continuous testing, on the other hand, ensures a constant watch over the attack surface, helping to identify and mitigate risks in real-time.

Identifying and prioritizing vulnerabilities is their top objective

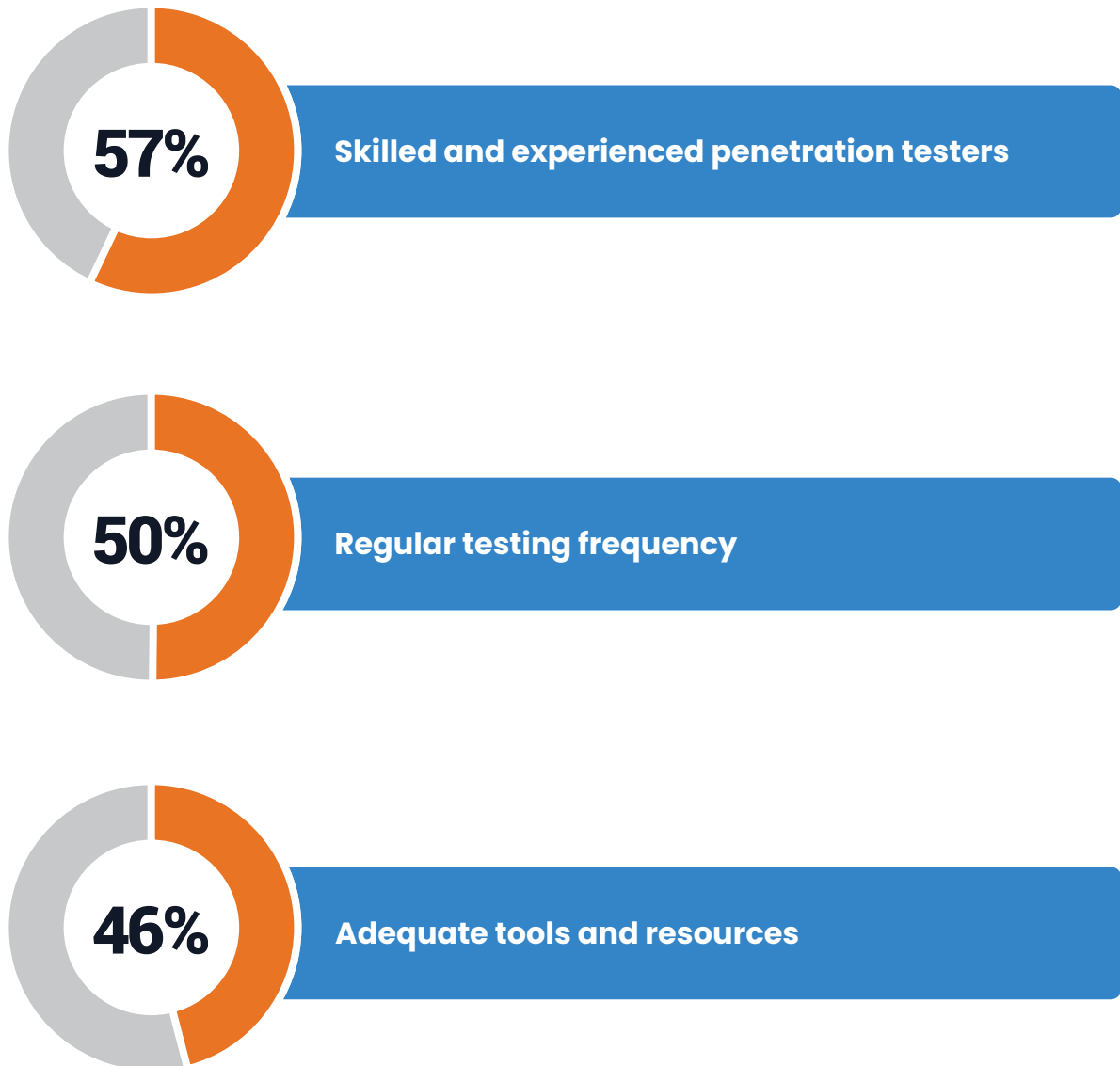
The top objectives they aim to achieve with their penetration testing program are:



Other objectives include improving incident response capabilities (14%) and enhancing security awareness among employees (12%).

Skilled penetration testers make their program effective

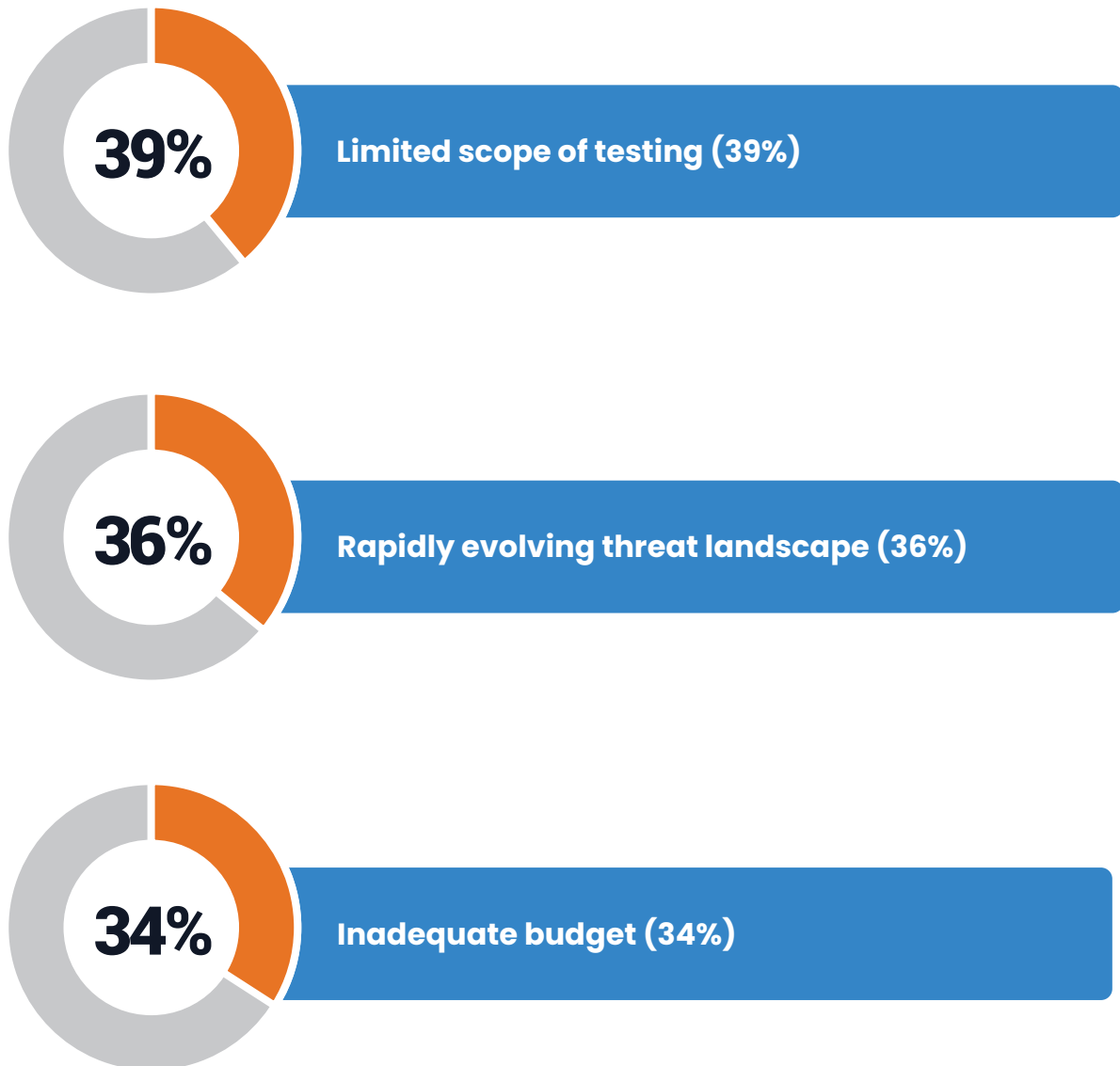
The top factors that make their penetration testing program so effective are:



Other factors include comprehensive testing methodology (41%), support from management (31%), and effective communication and collaboration with stakeholders (24%).

The limited scope of testing is top challenge for in-house teams

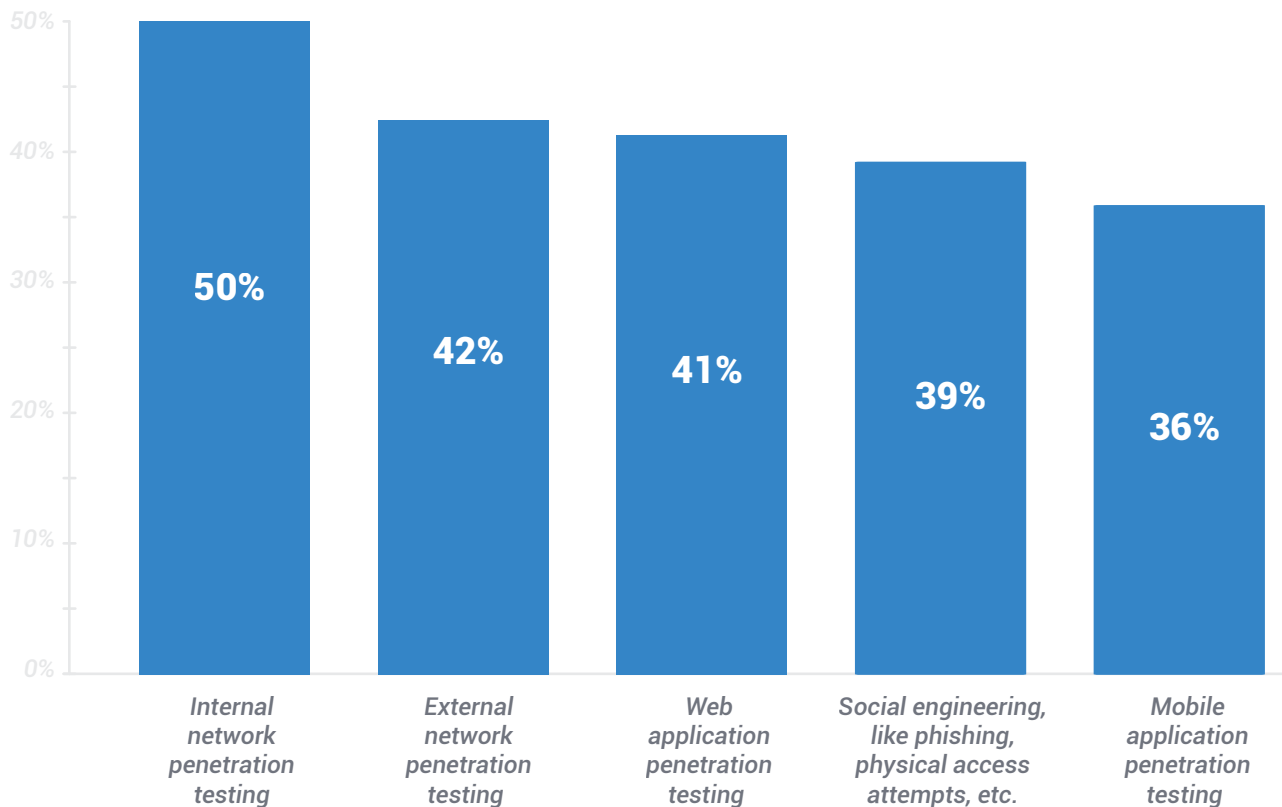
The top factors that make their penetration testing program challenging are:



Other challenges include a lack of skilled personnel (33%), difficulty in prioritizing remediation efforts (31%), a lack of management support (24%), and insufficient tools and resources (20%).

Internal network penetration testing is the most popular type

In-house teams perform the following types of penetration testing:



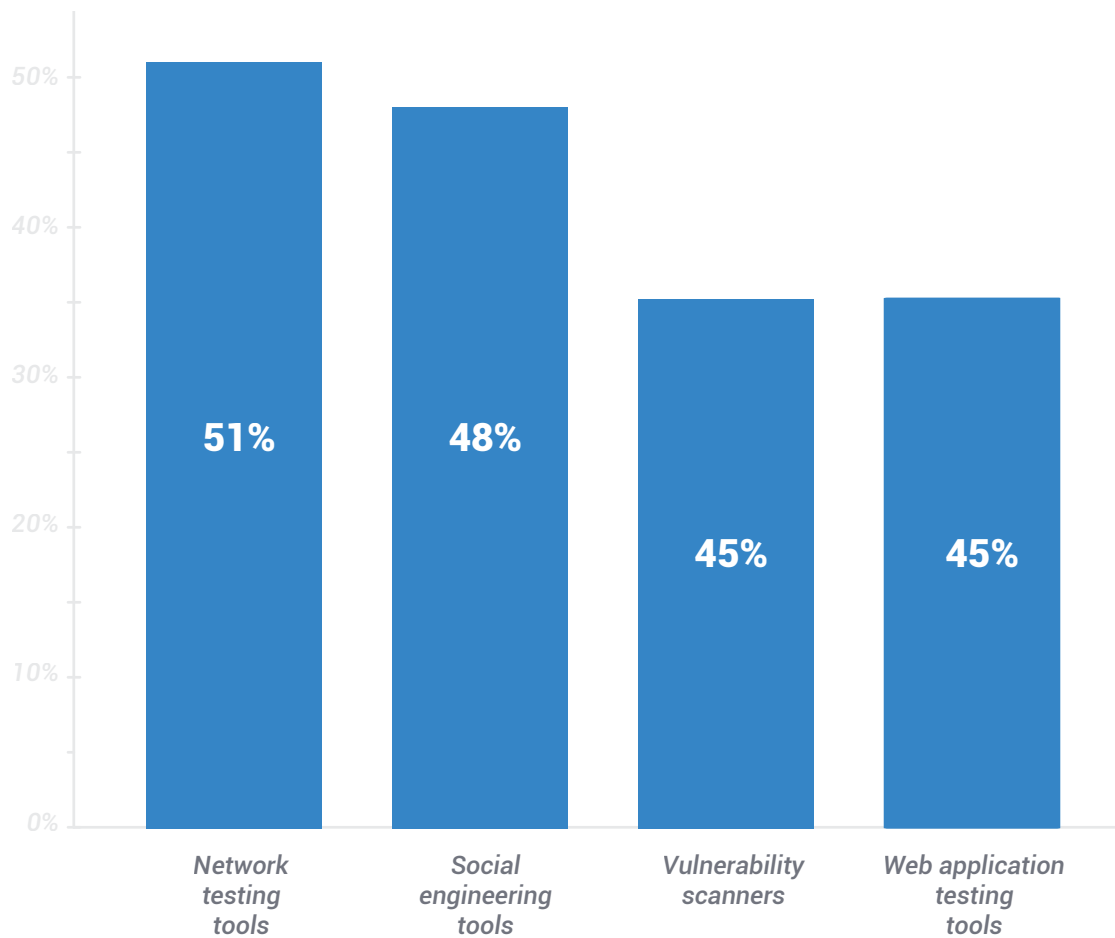
Other types include IoT/embedded systems penetration testing (34%), wireless network penetration testing (33%), cloud infrastructure penetration testing (32%), and red team engagements (16%).

COMMENT FROM CASEY

In-house teams typically focus on internal network testing to secure the organization's infrastructure, while third-party pentesters often handle external testing, simulating real-world attacks. Both are essential—internal testing protects sensitive systems, and external testing defends against common external threats. A comprehensive security program requires both approaches to ensure full protection.

Network testing tools are the most popular for in-house penetration testing teams

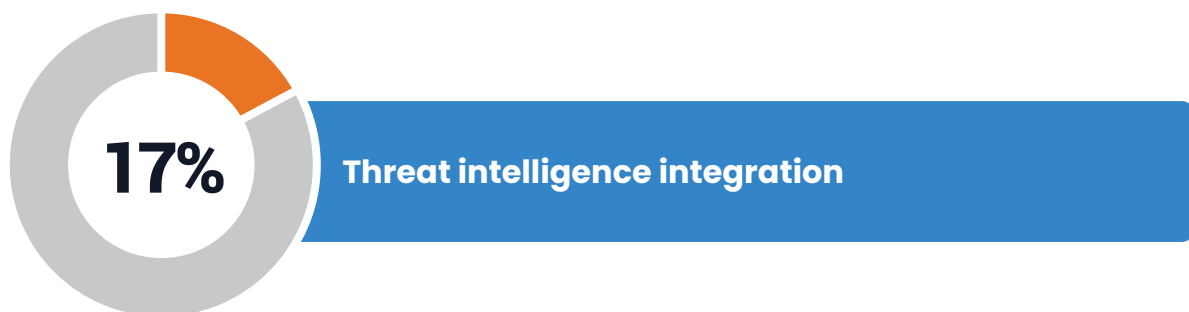
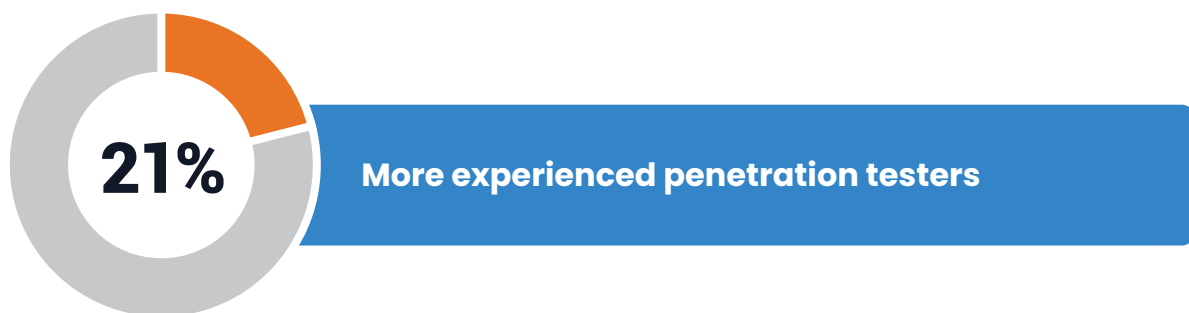
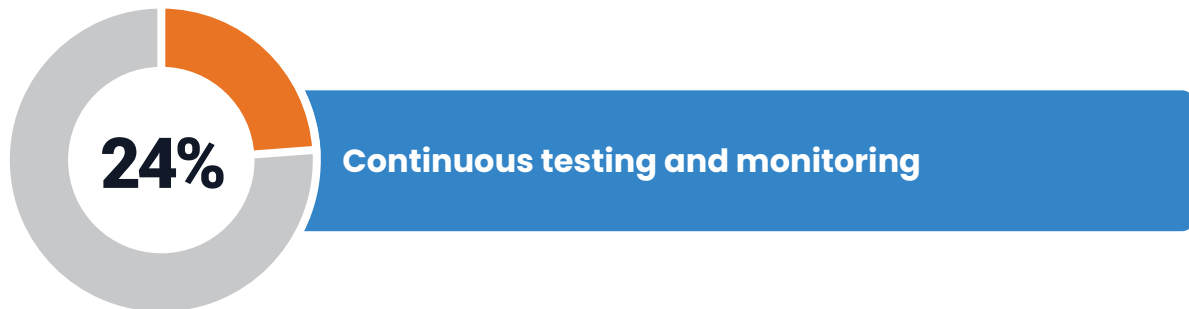
The most popular penetration testing tools and technologies are:



Other tools include wireless testing tools (40%), cloud security testing tools (38%), and exploitation frameworks (36%).

They would add continuous testing and monitoring to their program

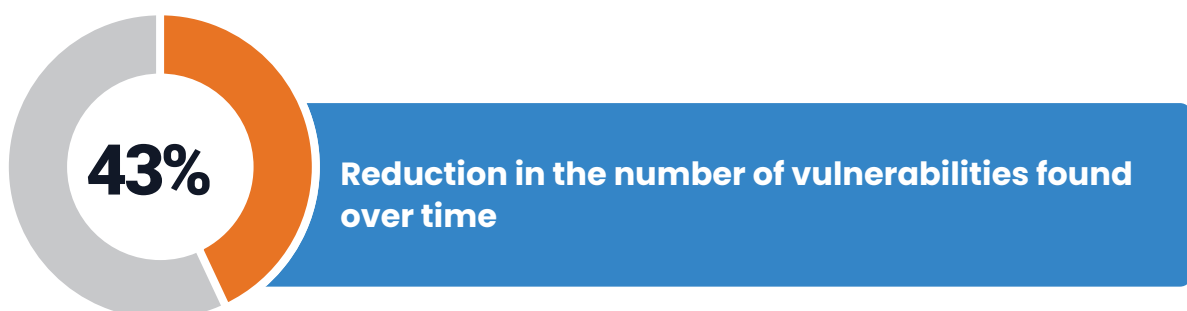
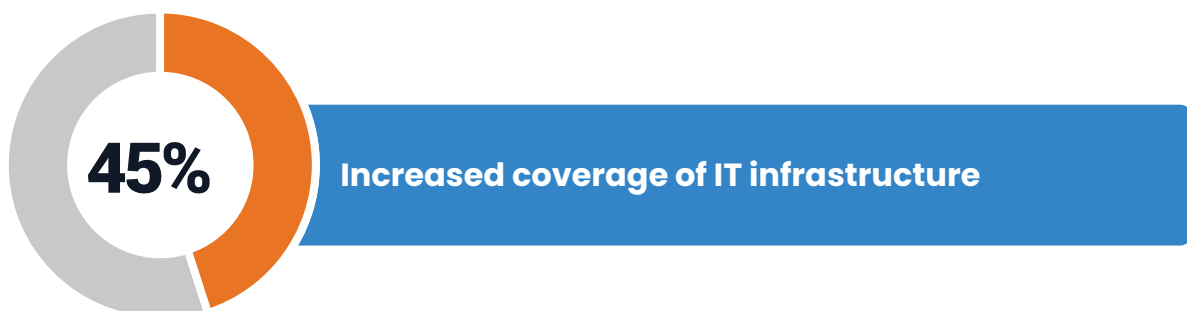
Respondents would like to add the following to their existing penetration testing program:



Other factors include an expanded scope of testing, including cloud, mobile, and IoT (15%), automation tools for vulnerability scanning and exploitation (14%), and improved reporting and communication (9%).

Improved security awareness is the top sign of success

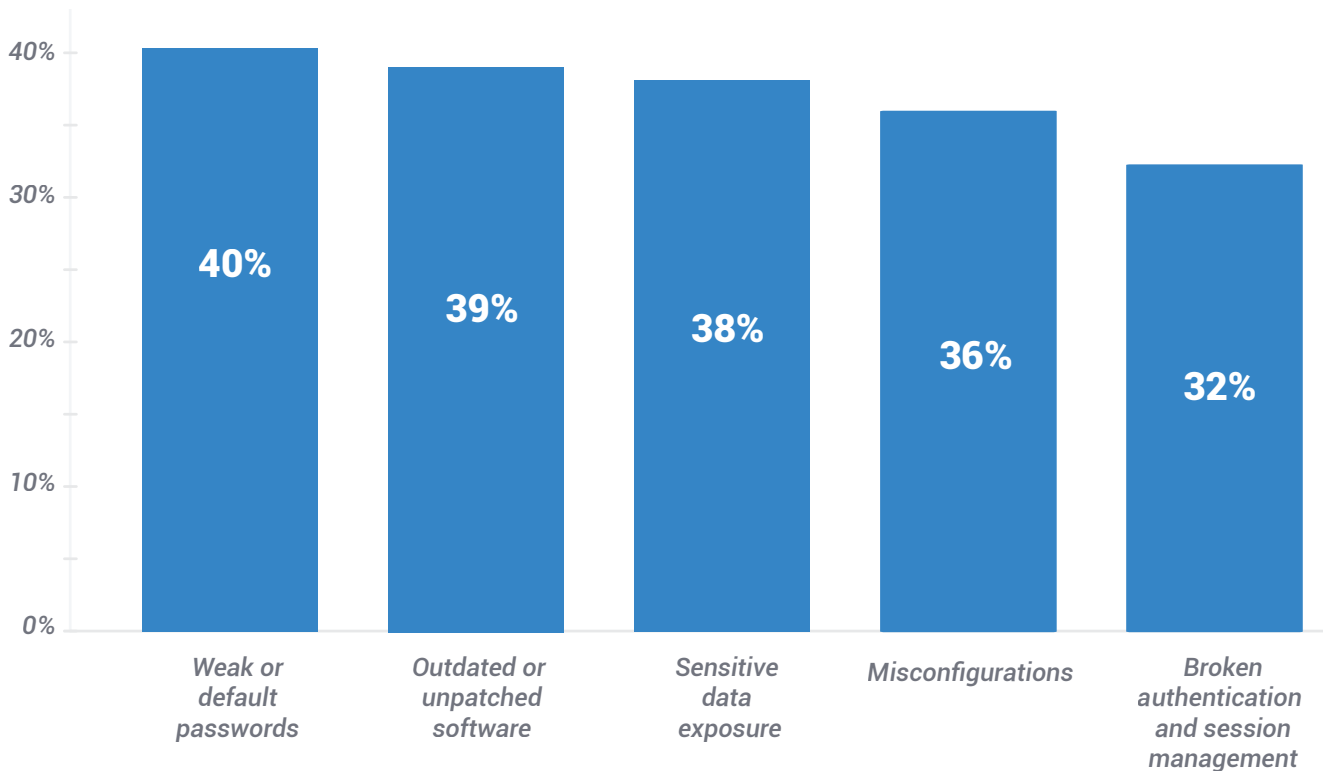
They measure the success of their penetration testing program in the following ways:



Other ways include faster remediation times (39%) and compliance with industry standards and regulations (25%).

Weak or default passwords are the most common vulnerability

The most common types of vulnerabilities they encounter during penetration testing are:



They also find injection flaws, like SQL injection and cross-site scripting (30% tie), insufficient logging and monitoring (30% tie), using components with known vulnerabilities (25%), and social engineering (24%).

COMMENT FROM CASEY

Weak or default passwords remain the most common vulnerability found during penetration tests, especially on internal networks. This highlights a persistent gap between security awareness and implementation. Both in-house teams and external pentesters encounter this issue frequently. Addressing it is essential for any security strategy, as prioritizing password hygiene is key to strengthening overall defenses.

Summary

Organizations know they need to use penetration testing as part of a robust security approach to keep them safe. The top objective for penetration testing is to identify and prioritize vulnerabilities so they can be remediated — and the most common vulnerabilities they find are weak or default passwords, outdated or unpatched software, and sensitive data exposure. Other objectives include using penetration testing to validate the effectiveness of security controls and to meet compliance requirements.

Overall, 60% believe their in-house testing program is very effective. They say what makes it effective is the skilled and experienced penetration testers they use, as well as having a regular testing frequency and adequate tools and resources — and the most effective tools they use are network testing tools and social engineering tools.

Despite many already having adequate tools and resources, respondents said if they could add anything to their penetration testing program, they would add continuous testing and monitoring so they always stay ahead of issues that could compromise their organization. They would also add more experienced penetration testers and threat intelligence integration.

Penetration testing isn't always seamless, and the biggest challenge they face is the limited scope of their testing that won't truly uncover everything they need to know. Other challenges include trying to keep up with the rapidly evolving threat landscape and lacking the budget for expanded penetration testing.

How are they measuring their penetration testing program's success? Respondents deem their penetration testing successful if it can improve security awareness among their employees. It's also successful if it's increased the coverage of their IT infrastructure or helped reduce the number of vulnerabilities found over time.

PART 2

Penetration Testing Priorities and Plans

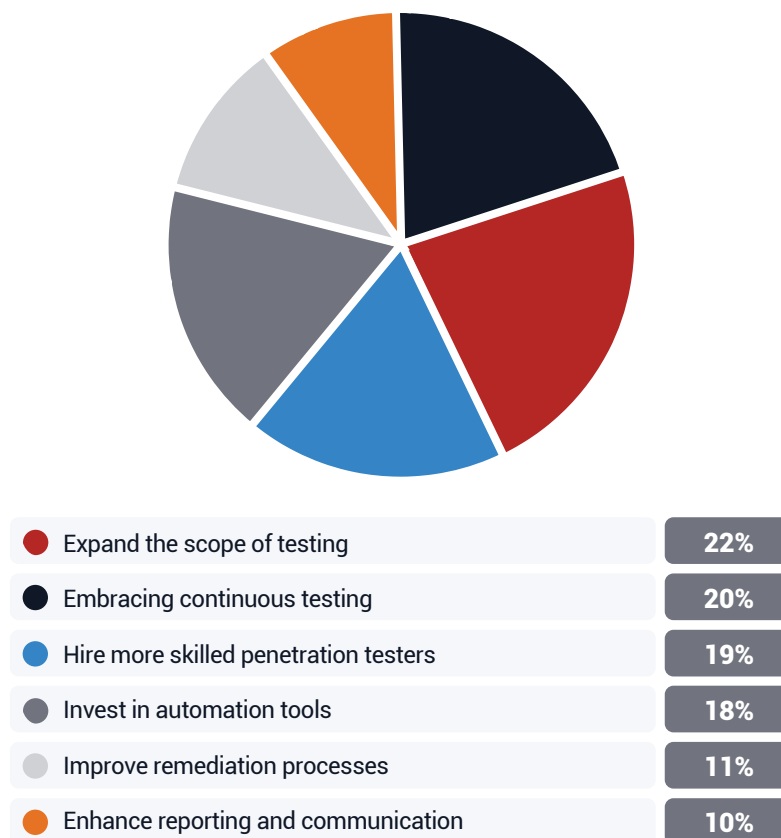
Not only do organizations need a robust penetration testing program, but they also need strategies to support that program into the future. In this section, respondents share about how they're allotting their budgets for penetration testing, what skills their team needs to be successful, and how they're preparing for the next twelve months.

Expanding the scope of their testing is their top priority

The top priority for their penetration testing program over the next year is:

1. Expand the scope of testing (22%)
2. Embrace continuous testing (20%)
3. Hire more skilled penetration testers (19%)

What would you say is your #1 priority for your Penetration Testing program over the next 12 months?

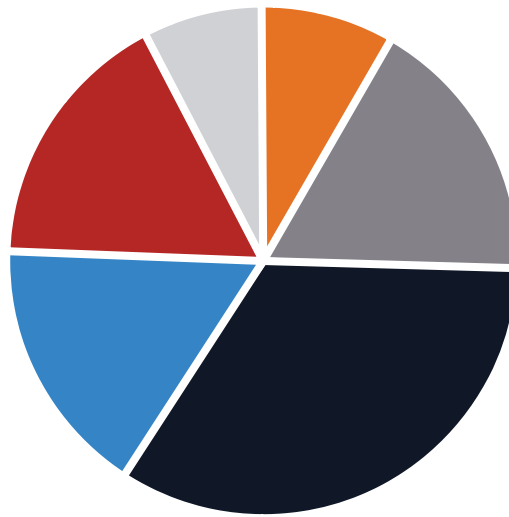


Other priorities include investing in automation tools (18%), improving remediation processes (12%), and enhancing reporting and communication (10%).

There are a variety of annual budgets specific to penetration testing

Annual budgets specific to penetration testing, including labor, tools, and contracts, are significantly distributed.

What is your annual budget specific to penetration testing (including labor, tools, and any contracts)?

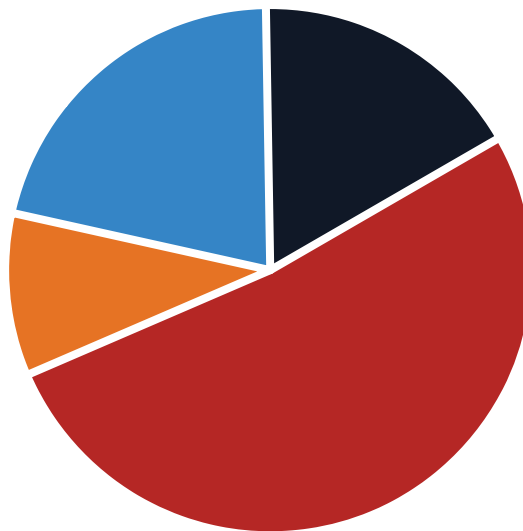


<input type="radio"/> I don't know	9%
<input type="radio"/> Less than \$20,000	17%
<input type="radio"/> \$20,000 - \$99,999	33%
<input type="radio"/> \$100,000 - \$149,999	16%
<input type="radio"/> \$150,000 - \$499,999	18%
<input type="radio"/> \$500,000 +	7%

Over half will see their penetration budget increase

52% say their budget for penetration testing is going to increase over the next year, while 23% say there will be no change. 9% say it will decrease, and 17% don't know how it will change.

How is your budget for Penetration Testing going to change over the next 12 months?



<div></div> Increase	52%
<div></div> No change	23%
<div></div> I don't know	16%
<div></div> Decrease	9%

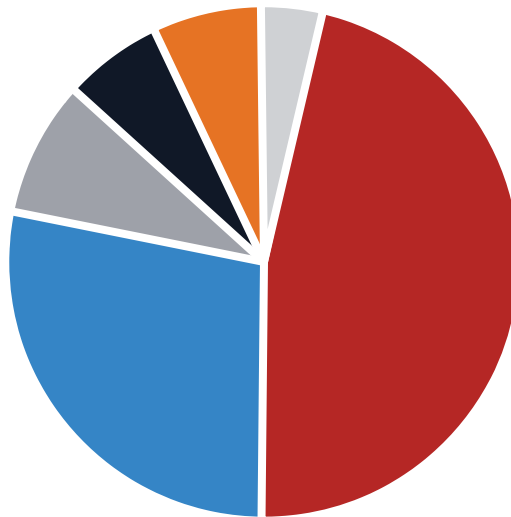
COMMENT FROM CASEY

Over half of respondents expecting a budget increase for penetration testing shows that offensive security is a growing priority. Organizations are recognizing the need for proactive measures to stay ahead of evolving threats. As investment in these programs grows, the value of identifying and addressing vulnerabilities before attackers exploit them is clear. Offensive testing, especially when combined with continuous strategies, is key to maintaining a strong security posture.

For those increasing their budgets, nearly half will increase by up to 25%

For those who say their budget will increase, 46% say it will increase by up to 25%, while 28% say it will increase between 26% and 50%. 9% say it will increase between 51% and 75%, and 7% say it will increase between 76% and 100%. 7% say it will increase more than 100%. 4% don't know how it will increase.

By what percentage will it increase?

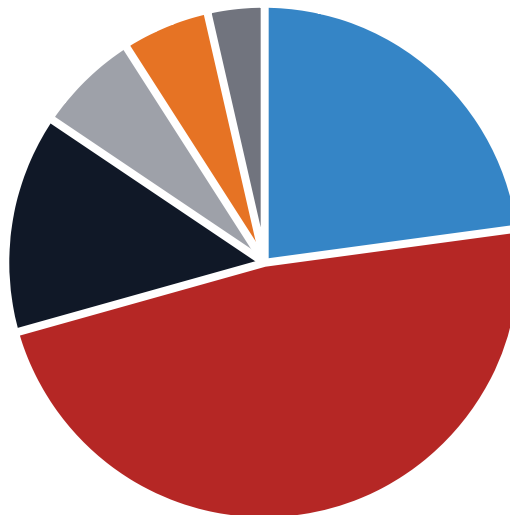






 I don't know	4%
 Less than 25%	46%
 26% - 50%	28%
 51% - 75%	8%
 76% - 100%	7%
 More than 100%	7%

For those decreasing their budgets, nearly half will decrease by 25% or less

For those who say their budget will decrease, 47% say it will decrease by 25% or less, while 15% say it will decrease between 26% and 50%. 7% say it will decrease between 51% and 75%, and 6% say it will decrease between 76% and 100%. 3% say it will decrease more than 100%. 23% don't know how it will decrease.

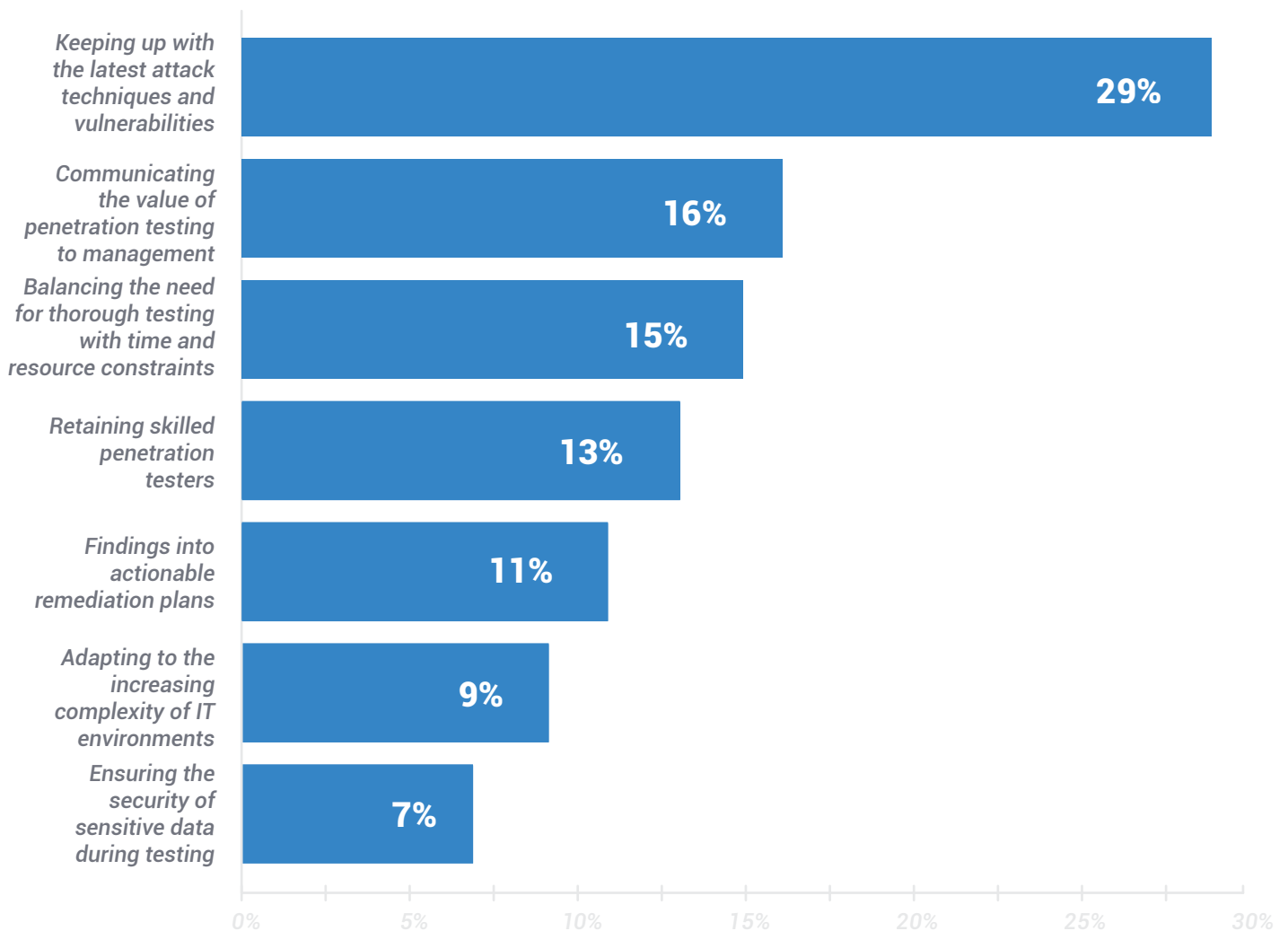
By what percentage will it decrease?



 I don't know	23%
 Less than 25%	47%
 26% - 50%	15%
 51% - 75%	6%
 76% - 100%	6%
 More than 100%	3%

They most worry about keeping up with the latest attack techniques

The challenges respondents most worry about with their penetration testing activities are:

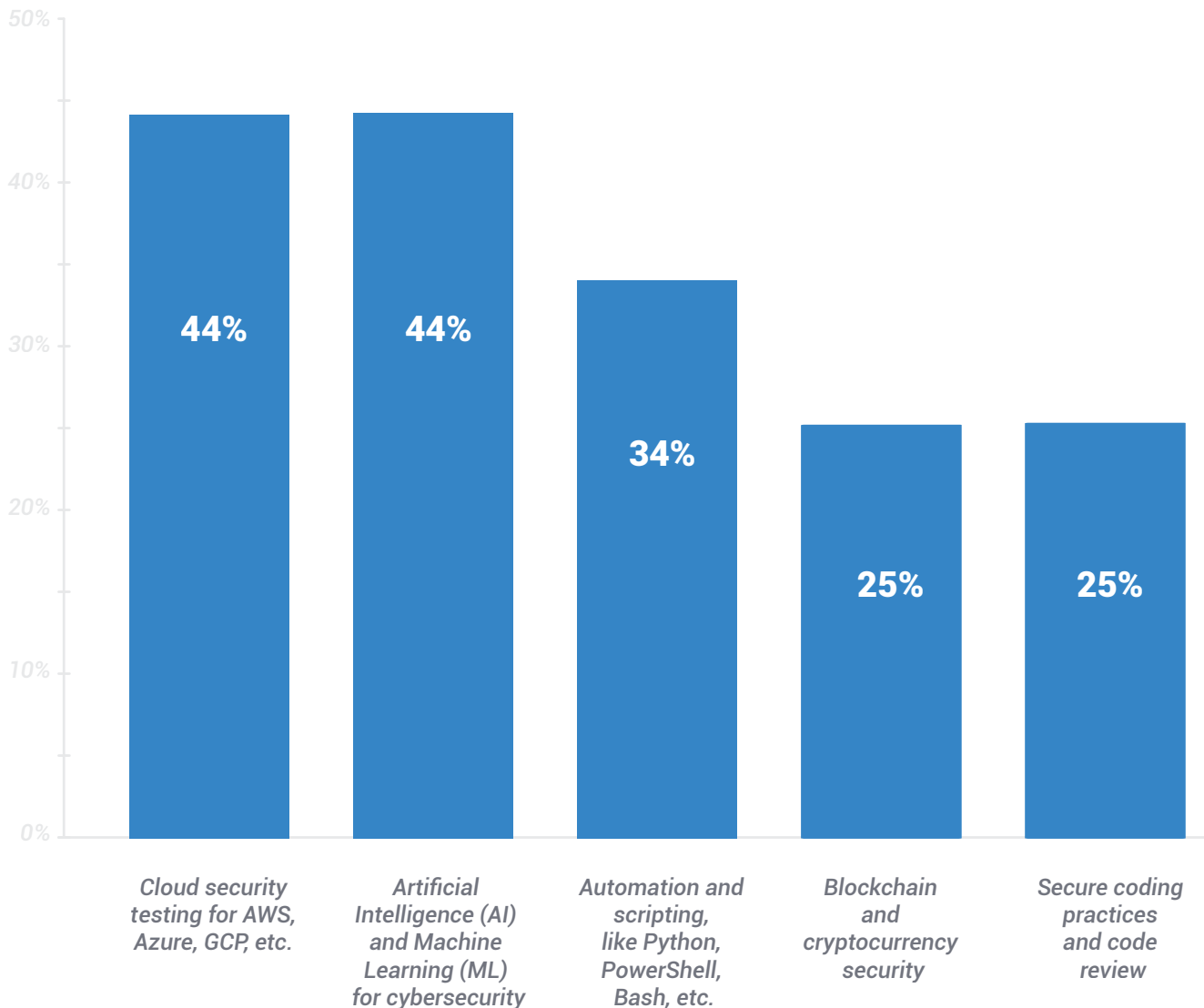


COMMENT FROM CASEY

With attack techniques evolving rapidly, security teams are focused on staying ahead of new threats. Bringing in external pentesters and adopting a continuous testing mindset are crucial. External teams, exposed to the latest attack vectors, offer fresh insights that internal teams might miss. Combining this expertise with continuous testing helps identify and address vulnerabilities in real time, keeping organizations protected from emerging threats.

Cloud security testing and AI are the top skills penetration testers need

The skills penetration testers should focus on developing to future-proof their careers are:



Other skills include threat hunting and advanced persistent threat (APT) detection (21%), social engineering and physical security testing (20%), IoT and embedded systems security testing (18%), incident response and forensics (14% tie), continuous integration and continuous deployment (CI/CD) security (14% tie), security architecture and design principles (13% tie), compliance and regulatory knowledge for GDPR, HIPAA, PCI-DSS, etc. (13% tie), soft skills, like communication, collaboration, critical thinking, etc. (11%), and DevSecOps practices and principles (8%).

Summary

Over the next year, their top priority for penetration testing programs will be to expand the scope of testing — their biggest challenge today. They also want to embrace continuous testing — the top thing they would add to their program if they could. They also plan to hire more skilled penetration testers, as skilled testers are what they say makes their penetration testing program most effective.

In thinking about hiring penetration testers, respondents say the top skills they need are cloud security testing and knowing how to use AI/ML for cybersecurity efforts. They also want penetration testers to be proficient in automation and scripting as well.

In terms of budgets for penetration testing, respondents have all different levels of budgets allotted. However, 52% say their budget for penetration testing is going to increase over the next year. Of those respondents, 46% say it will increase by up to 25%, while 28% say it will increase between 26% and 50%.

Finally, as cybersecurity attacks continue to increase in frequency and severity, their biggest worry is being able to keep up with the latest attack techniques and vulnerabilities. They're also worried about communicating the value of penetration testing to management — key for getting buy-in and budget commitment — and balancing the need for thorough testing with time and resource constraints.

PART 3

Takeaways for Security Practitioners

60% of the respondents find their in-house penetration testing program very effective – but that leaves 28% who say it's only somewhat effective, while 13% say it's not very effective at all. Penetration testing is a key tool for security teams to be able to identify how their systems would withstand an attack and where their weaknesses lie. What changes can security make so that their penetration testing program becomes a very effective one?

1. Adopt continuous testing

Those who said their program was very effective attribute that effectiveness to their regular testing frequency. Additionally, respondents said if they could add one thing to their program, it would be continuous testing.

Why should testing be continuous? Given the rapid internal activities and innovations at organizations that constantly change the attack surface, as well as rapidly evolving attacker techniques, it no longer makes sense to test once and then test again at some point in the future. That first test has likely already become obsolete, leaving an organization open to risk. Security teams can get started by working with partners that offer continuous testing, as well as visibility into their attack surface, risk assessments, and remediation plans.

2. Work with knowledgeable penetration testers

Respondents said that the top contributor to making their penetration testing program effective was having skilled and experienced penetration testers. Additionally, one of their top priorities for next year is to hire more skilled penetration testers, and the top skills they're looking for in a pentester include cloud security testing, AI and ML for cybersecurity, and automation and scripting.

The more skilled the penetration tester, the more like an adversary they can be in uncovering the vulnerabilities in an organization. Skilled penetration testers will also know how to perform a variety of tests that will provide a more comprehensive view of an organization's risk. The biggest challenge mentioned above is their limited scope of testing; by expanding that scope and using experienced penetration testers, organizations will increase their findings and significantly decrease their risk.

3. Use the right tools

Another key factor in having a very effective penetration testing program is having adequate tools and resources. These tools will help experienced pentesters uncover more vulnerabilities that, when remediated, will strengthen an organization's systems and networks. These tools and resources can help expand the scope of testing, which is respondents' biggest challenge.

What tools and resources should security teams have on hand? Respondents said that their most valuable penetration testing tools are network testing tools, social engineering tools, vulnerability scanners, and web application testing tools.

4. Communicate value to leadership for buy-in and budget

One of the biggest worries for respondents above is about their ability to communicate the value of penetration testing to management. This is important because to have a truly effective penetration testing program, security teams need leadership buy-in, which can directly result in budget allotment (and one of their biggest challenges is having an inadequate budget for their program).

Security teams can increase their effectiveness at communicating with leadership by tracking and articulating how their penetration testing program helps reduce overall risk in their company. Leadership isn't likely to be interested in the ins-and-outs of the different types of security testing, but will be interested in how penetration testing reduces their chances of a breach, how it's reducing risk, and how it's improving overall security. Once they see that it can reduce overall risk, making the case for an increased budget will be easier.

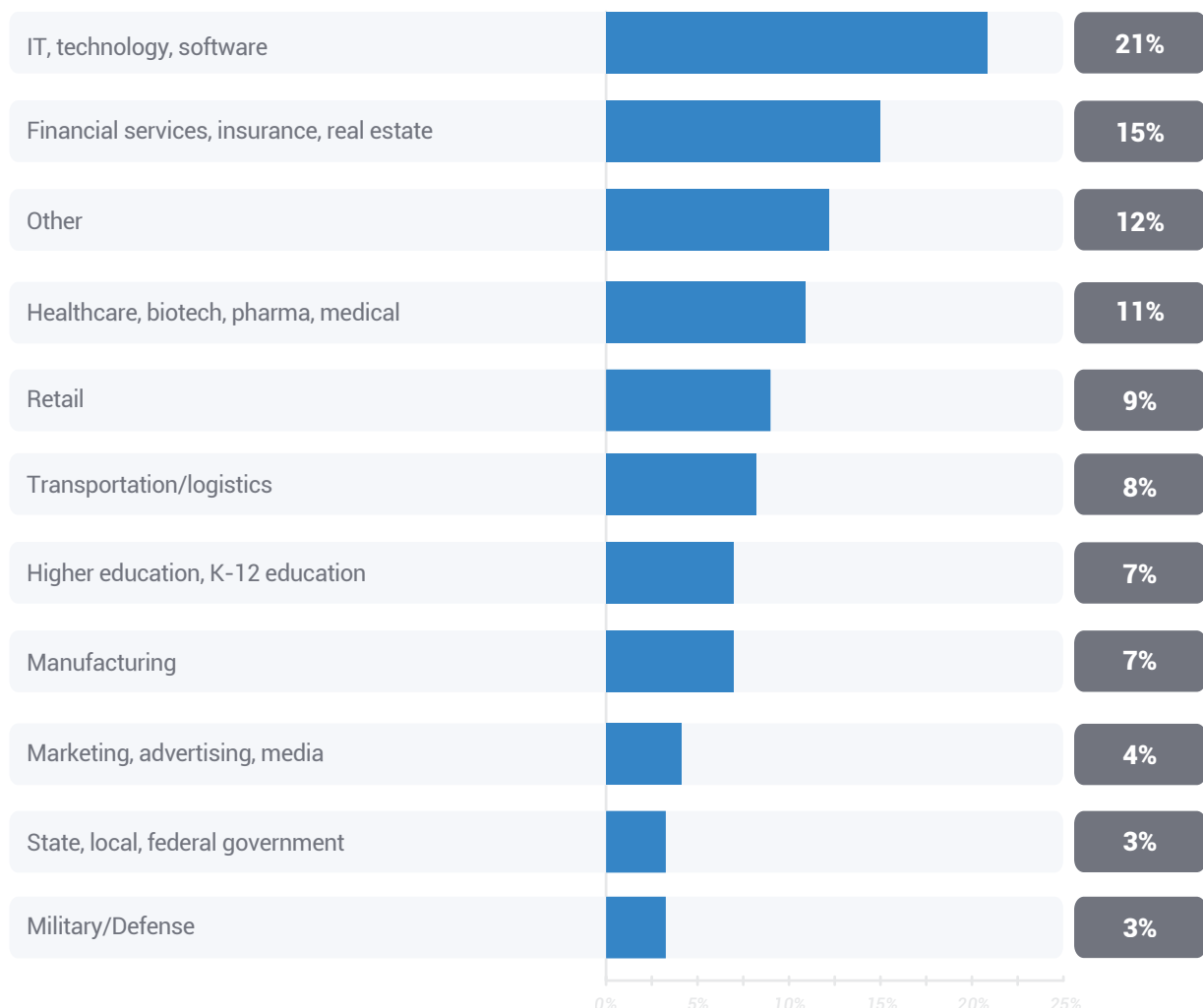
Conclusion

Cyber attacks and other threats to an organization's networks and systems are only going to increase. Now is the time for security teams to shore up their approach to penetration testing by expanding their scope, partnering with experienced pentesters and vendors, and adopting continuous testing so that they can always know the true state of their risk and take action before attackers do.

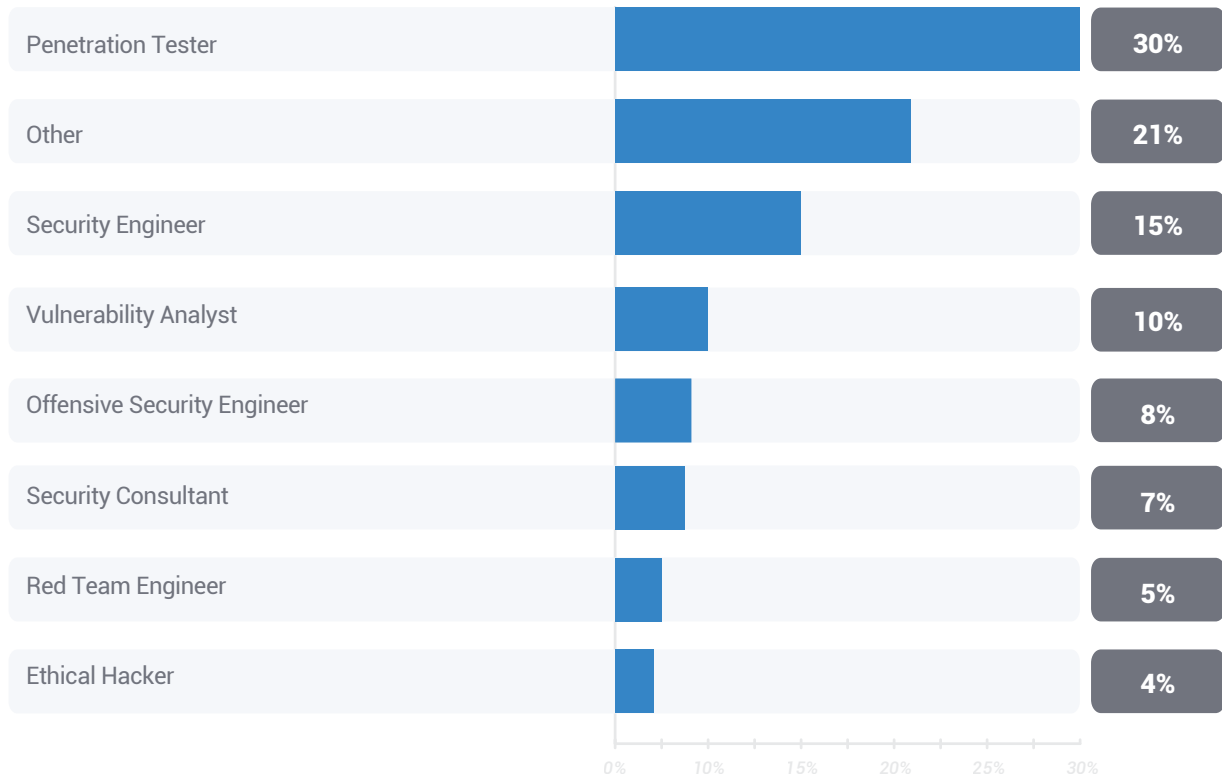
Profile of Who We Surveyed: Methodology and Participant Demographics

To provide greater context around these findings, here are more details on who we surveyed and the methodology used. Starting on July 15, 2024, we surveyed 200 in-house pentesters, individuals who perform penetration testing within their organizations. The survey was conducted online via Pollfish using organic sampling. Learn more about the Pollfish methodology [here](#).

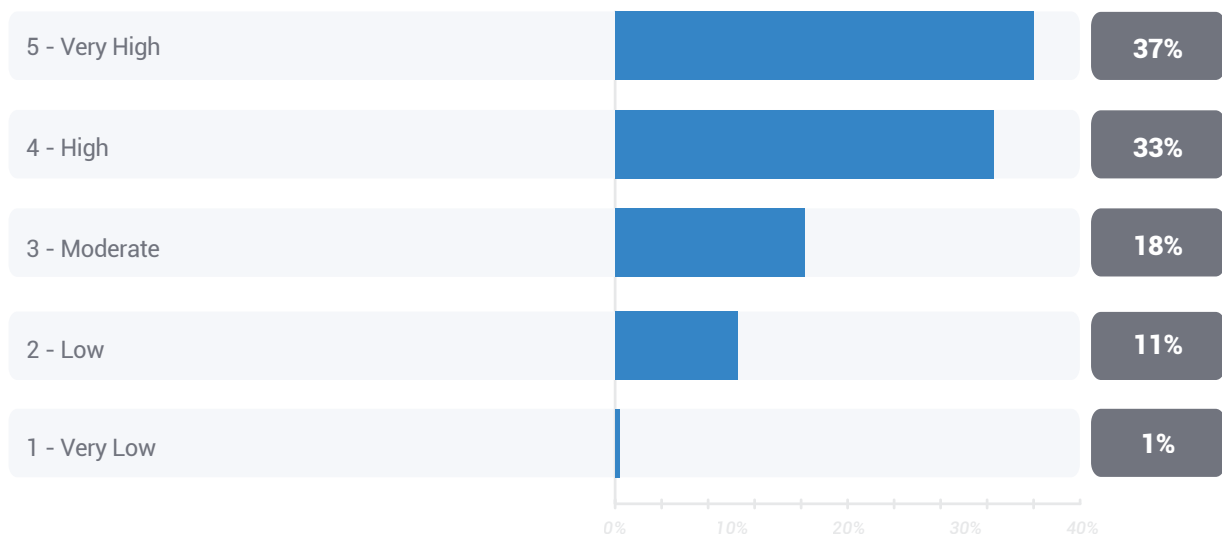
What industry does your organization primarily operate in?



What best describes your job title/role?



On a scale of 1-5, how would you rate your organization's overall cybersecurity maturity?





Sprocket
Security

Sprocket Security is an expert-driven offensive cybersecurity platform specializing in continuous penetration testing. From attack surface management to red and purple teaming exercises, Sprocket's platform is setting a new standard in offensive cybersecurity for enterprises across industries. To schedule a demo of Sprocket, please visit www.sprocketsecurity.com