REPORT

Ponemon INSTITUTE

2023 • THE STATE OF OFFENSIVE SECURITY

Creating a Blueprint for Success

Sponsored by: BISHOPFOX

Table of Contents

Introduction

Sponsored by Bishop Fox, the purpose of this research is to learn important information about how organizations with mature security programs are deploying offensive security practices to achieve a strong cybersecurity posture. An offensive strategy is focused on proactive identification of security processes and controls that prevent a successful attack. In contrast, the objective of reactive measures, such as managed detection and response, is to minimize attacker dwell time once prevention fails. A balanced strategy between offensive and reactive approaches can result in a strong state of cybersecurity resilience.

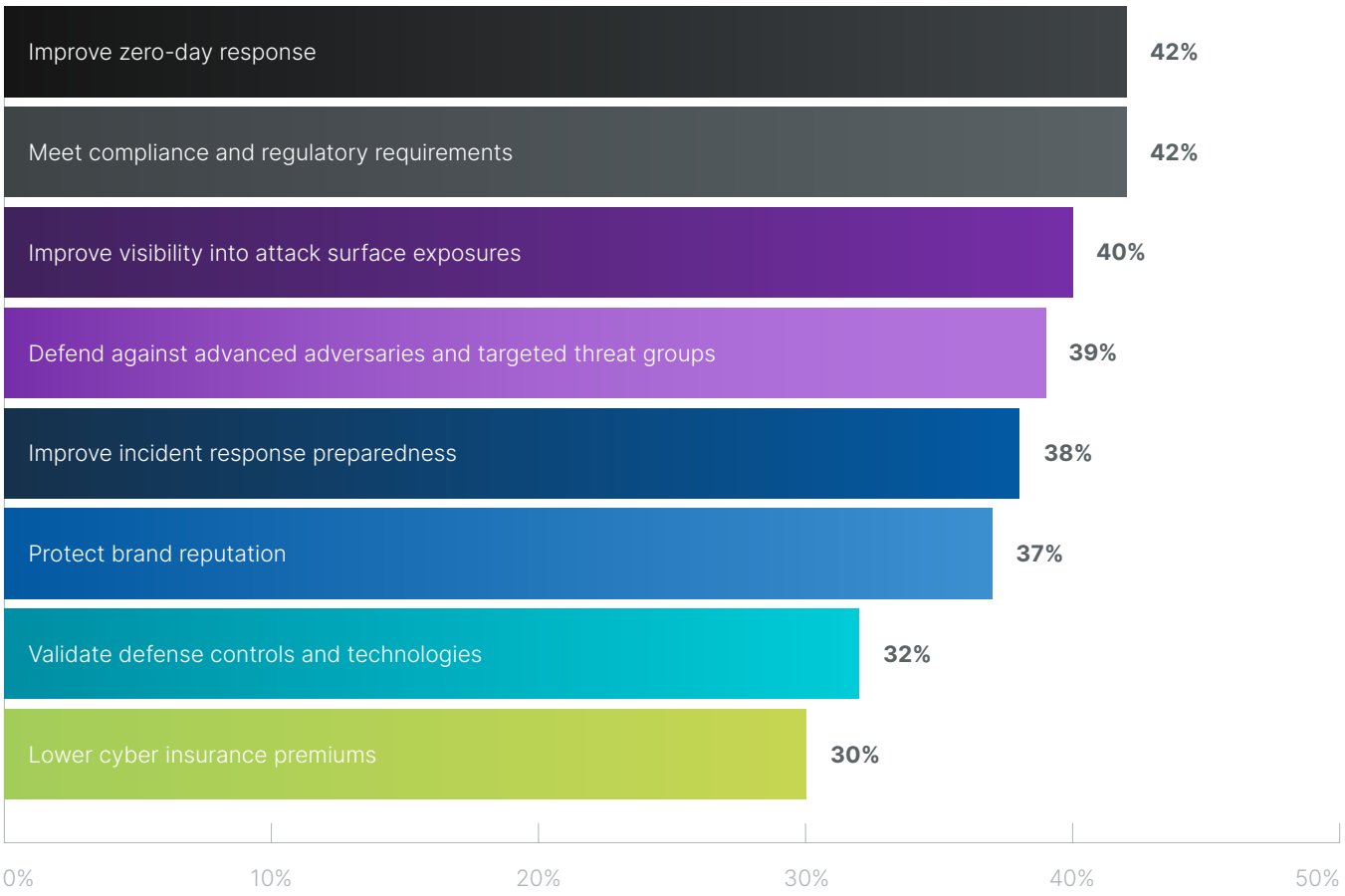
Ponemon Institute surveyed 664 IT and security practitioners in organizations that perform offensive security testing. Organizations represented in this research have a fully mature (39 percent of respondents), a very mature (29 percent), or a mature security strategy (32 percent). Maturity is determined by the level of an organization's deployment of security activities and technologies – fully deployed, mostly deployed, or many deployed.

According to the research, 64 percent of respondents say their organizations have benefited from offensive security testing and achieved security and governance goals. As shown in Figure 1, the objectives most often achieved are improving zero-day response (42 percent), meeting compliance and regulatory requirements (42 percent), and improving visibility into attack surface exposures (40 percent).

FIGURE 1

Which of the following goals or objectives did offensive security testing help your organization achieve?

Three choices permitted.



According to the research, offensive security helps organizations monitor cyber threats, build response times, strengthen network security and protect critical data. The following are the most salient findings from this research.

- **Organizations use third parties for offensive security testing because of their effectiveness, customization of engagements, and quality of deliverables.** Sixty-eight percent of respondents say their organization uses third-party offensive security service providers. Twenty-seven percent rely on external providers alone, while 41% use a combination of both internal and third-party testing.

  The three most important criteria when engaging offensive security vendors are effectiveness of services (48 percent of respondents), ability to customize engagements based on the needs of the organization (43 percent), and quality of deliverables, including reports (34 percent).

- **Changes in organizations' technological advancements and business operations influence adoption of offensive security testing.** The three top reasons influencing investment in offensive security testing are adoption of new technologies (44 percent of respondents), migration to the cloud (41 percent), and the release of new applications (40 percent).

- **Vulnerability scanners and attack surface management are the technologies most frequently purchased to support offensive security initiatives.** According to the research, vulnerability scanners are the most popular tools used to discover exposures and/or facilitate offensive security testing (50 percent of respondents). Vulnerability scans identify potential flaws in the system and rank them in order of severity depending on various factors. Almost half (48 percent) say their organizations use attack surface management technologies and digital risk protection services (46 percent).

More than half of respondents (52 percent) say offensive security testing helps their organization harden defenses against cyber threats. Of the cyber threats about which organizations are most concerned, ransomware drives the most offensive security investment (41 percent). This is closely followed by social engineering (40 percent) and cloud vulnerabilities (39 percent).

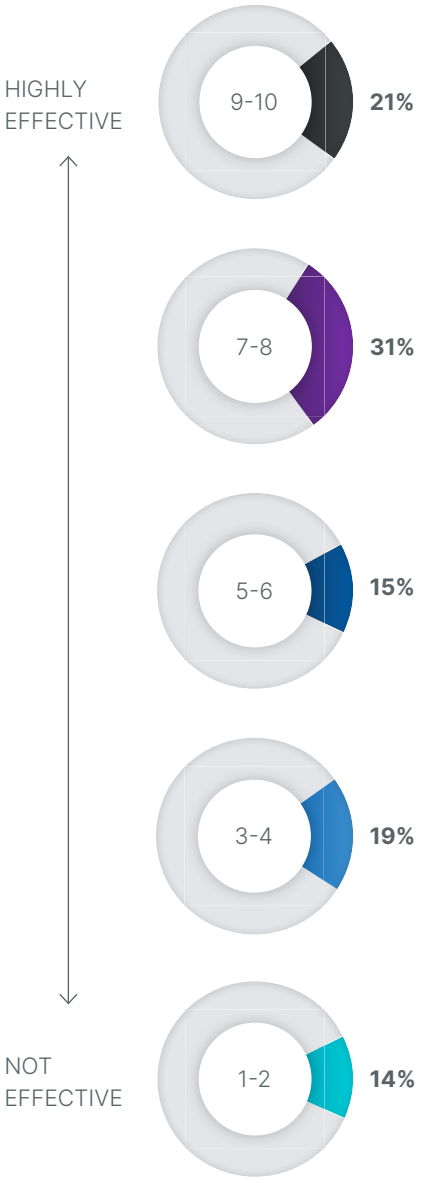
The following section applies to respondents who stated they implement red teaming, application security testing, IoT testing, internal and external network testing, and/or cloud security testing in their offensive security strategy.

- **Most organizations include red teaming in their offensive security testing strategy.** Red teaming is the practice of rigorously challenging an organization's ability to identify and mitigate tactics, techniques, and procedures designed to evade advanced security controls. Sixty-four percent of respondents say their offensive security strategies include red teaming. Other prevalent offensive security testing strategies include: application security testing (54 percent), testing IoT devices (49 percent), testing internal and external networks (47 percent), and cloud security testing (43 percent).
- **Offensive security testing in the cloud produces the greatest advancements in improving security posture.** Respondents cite cloud security testing as most effective in improving their organization's offensive security posture (57 percent of respondents), followed by red teaming (47 percent). Forty-three percent say offensive security testing is highly effective in improving the security of IoT devices, and 42 percent say application security testing is highly effective.

FIGURE 2

How effective has offensive security testing been in helping your organization harden its defenses against your top three threats?

Scale from 1 = not effective to 10 = highly effective.



- **Organizations recognize the value of offensive security testing and plan to increase their investments.** Investments in all areas of offensive security testing are projected to either significantly or moderately increase in the next one to two years. IoT device security (62 percent of respondents), cloud security (60 percent), red teaming (56 percent), application security (56 percent), internal network testing (55 percent), and external network testing/attack surface management (50 percent).

- **Continuous testing is important in identifying dangerous vulnerabilities targeted by attackers.** Continuous offensive security solutions combine the right mix of technology, automation, and human testing to prevent attacks before they can occur. While some organizations only test annually, bi-annually, quarterly, or monthly; more organizations in this study conduct continuous testing. According to the research, continuous testing is most often done in internal networks (31 percent of respondents), followed by external networks/attack surface (29 percent), applications (28 percent), and in red teaming (26 percent).

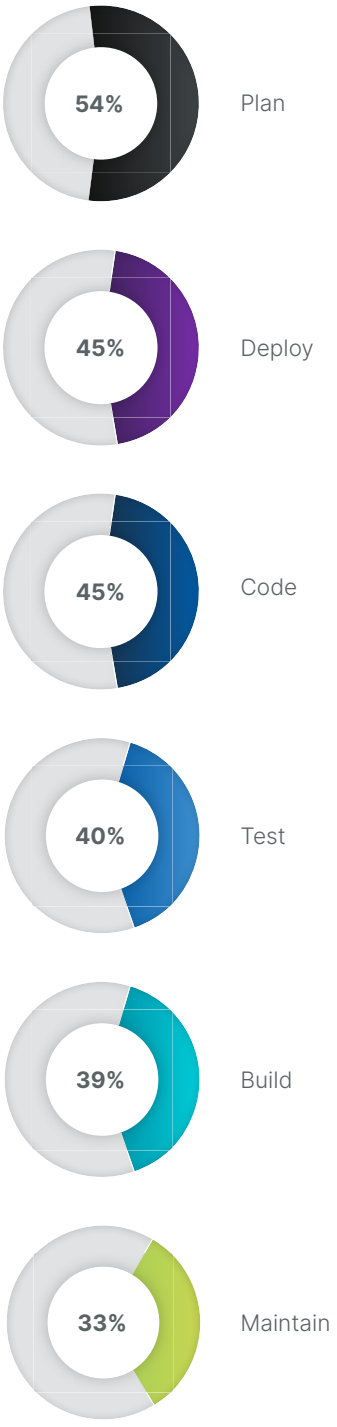
- **Tabletop exercises and ransomware readiness are the top two red teaming activities.** Tabletop exercises are used to prepare for cybersecurity incidents and are considered one of the best ways to assess ransomware readiness and establish a plan to address weaknesses in an organization's ability to both prevent and recover from attacks. Sixty-three percent of respondents say their organization uses these exercises to test offensive security posture, and 55 percent say their organizations test ransomware readiness.

- **Penetration testing is most often used to test third-party and internally developed applications in an offensive security testing strategy.** Penetration testing is a manual security testing method that organizations use to provide a comprehensive overview of the quality and effectiveness of their security controls. Using pen testing, components or applications that need testing are identified, isolated, and targeted. Because penetration tests are targeted, the vulnerabilities identified are often more complex and business-impacting. Sixty-seven percent of respondents say their organization is pen testing third-party software, and 64 percent pen test their own software. Fifty-eight percent say they use code review, and 50 percent say they conduct threat modeling.

FIGURE 3

Phases where offensive security testing is implemented in the SDLC.

More than one response permitted.



Offensive security testing in the software development life cycle (SDLC) is most often implemented in the planning phase. The SDLC is the process of planning, writing, modifying, and maintaining software. Almost half of respondents (48 percent) incorporate offensive security testing into their SDLC.

Of those, 54 percent of respondents say offensive security testing occurs in the planning phase, when organizations typically brainstorm, set goals, and identify high-level risks. Forty-five percent test during code development, and 45 percent also stated they test when the applications are deployed.

- **Pen testing is the most popular strategy for detecting security vulnerabilities in the cloud.** Fifty-nine percent of respondents say their organization uses pen testing to detect cloud vulnerabilities. Forty-one percent say their organizations use threat analysis. Threat analysis is a cybersecurity strategy that aims to assess an organization's security protocols, processes, and procedures to identify threats, vulnerabilities, and even gather knowledge of a potential attack before they happen.

- **Organizations are confident in their ability to identify assets and exposures across the external and internal attack surface.** Forty-seven percent of respondents say their organization's offensive security strategy includes testing of internal and external networks/attack surface. Sixty-four percent are testing assets for exposure continuously (37 percent) or daily (27 percent). Forty-nine percent say their organizations are discovering assets continuously (26 percent) or daily (23 percent).

Key Findings

In this section, we provide an analysis of the research. The complete findings are presented in the Appendix of this report. The report is organized according to the following topics.

- How organizations maximize the value of offensive security
- Offensive security testing in red teaming, application security, the cloud, internal and external network, and IoT devices
- Industry differences: Financial Services, Health and Pharmaceutical, Technology and Software, and Industrial and Manufacturing

HOW ORGANIZATIONS MAXIMIZE THE VALUE OF OFFENSIVE SECURITY

Organizations select third parties for their offensive security testing based on their effectiveness, customization of engagements, and quality of deliverables.

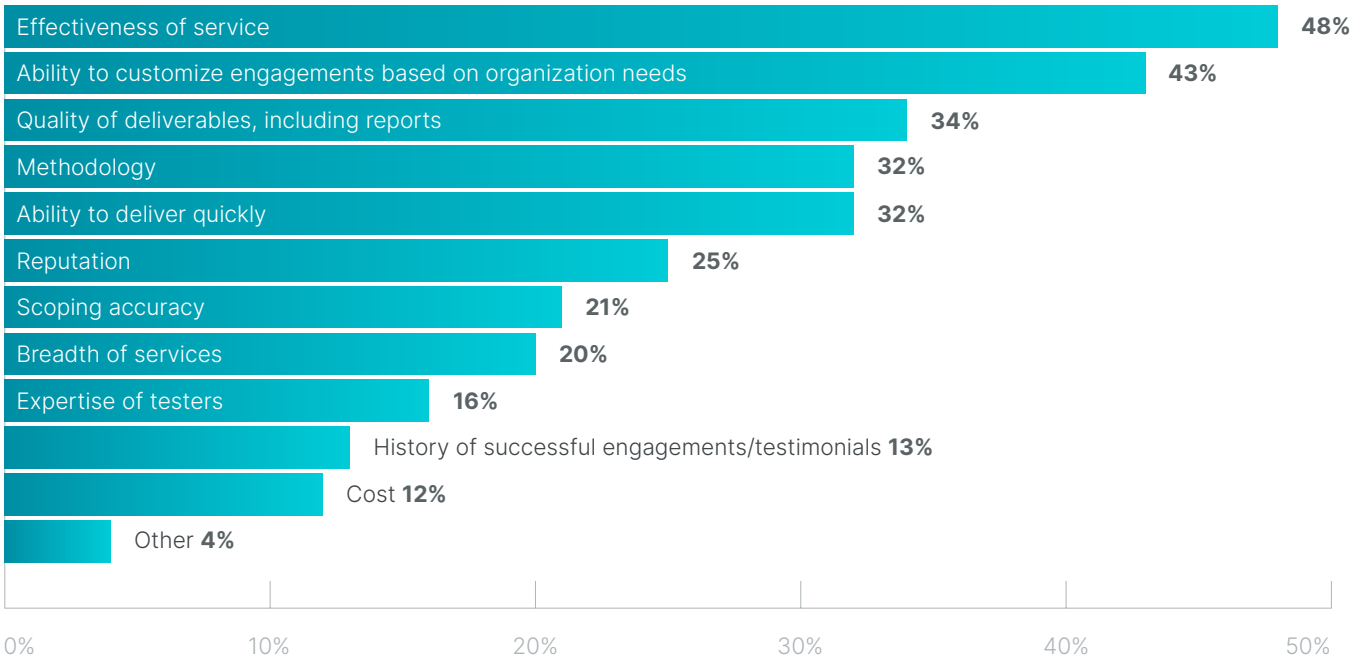
Sixty-eight percent of respondents say their organizations conduct offensive security testing with third-party offensive security service providers. Twenty-seven percent rely on external testing only, while 41percent combine testing by both internal and third-party offensive security service providers.

As shown in Figure 4, the three most important criteria when engaging offensive security vendors are effectiveness of services (48 percent of respondents), ability to customize engagements based on the needs of the organization (43 percent), and quality of deliverables, including reports (34 percent).

FIGURE 4

What criteria are most important when engaging vendors who offer offensive security services?

Three choices permitted.

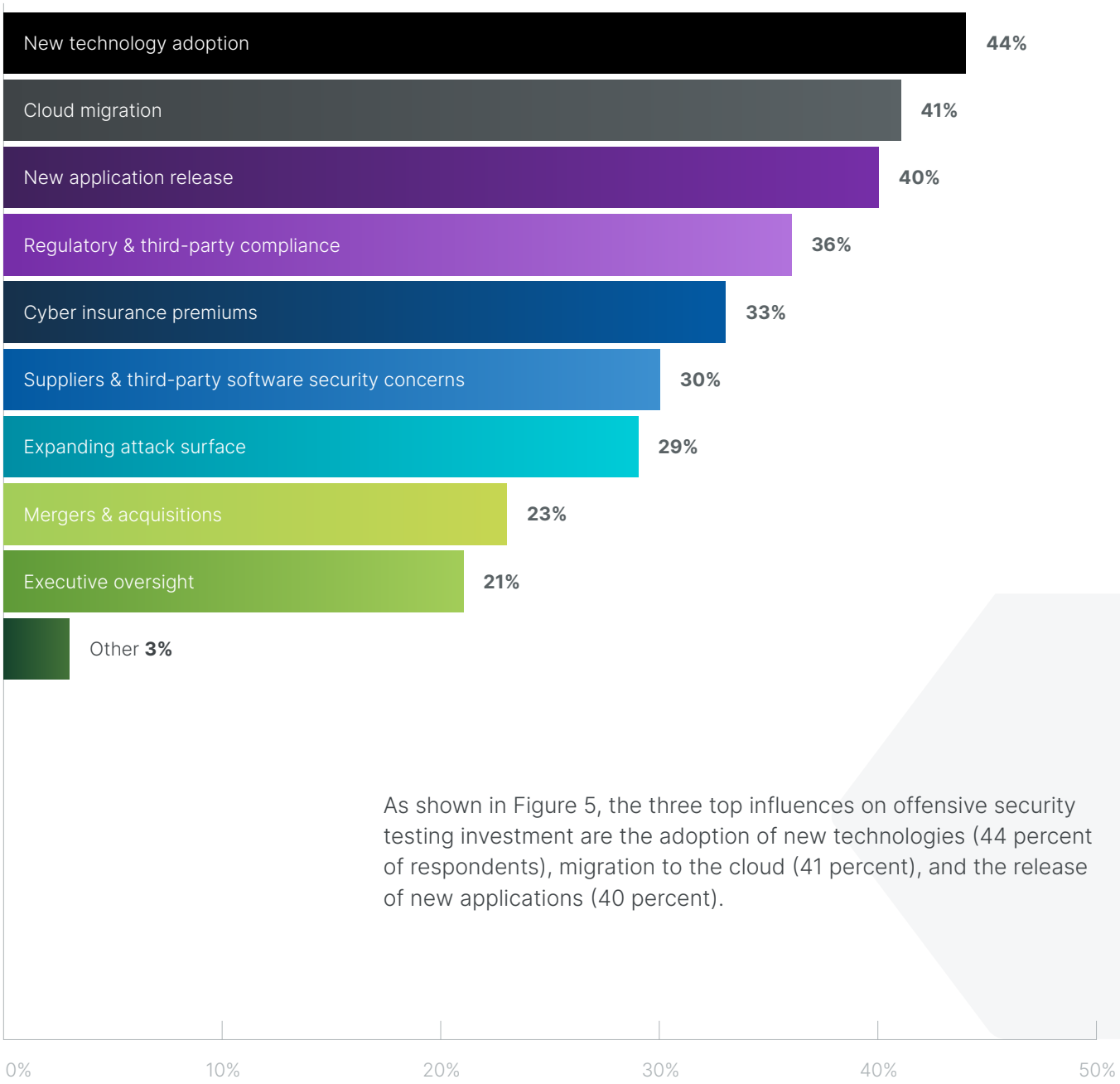


Changes in organizations' security strategies can influence adoption of offensive security testing.

FIGURE 5

Why organizations invest in offensive security testing.

Three choices permitted.



As shown in Figure 5, the three top influences on offensive security testing investment are the adoption of new technologies (44 percent of respondents), migration to the cloud (41 percent), and the release of new applications (40 percent).

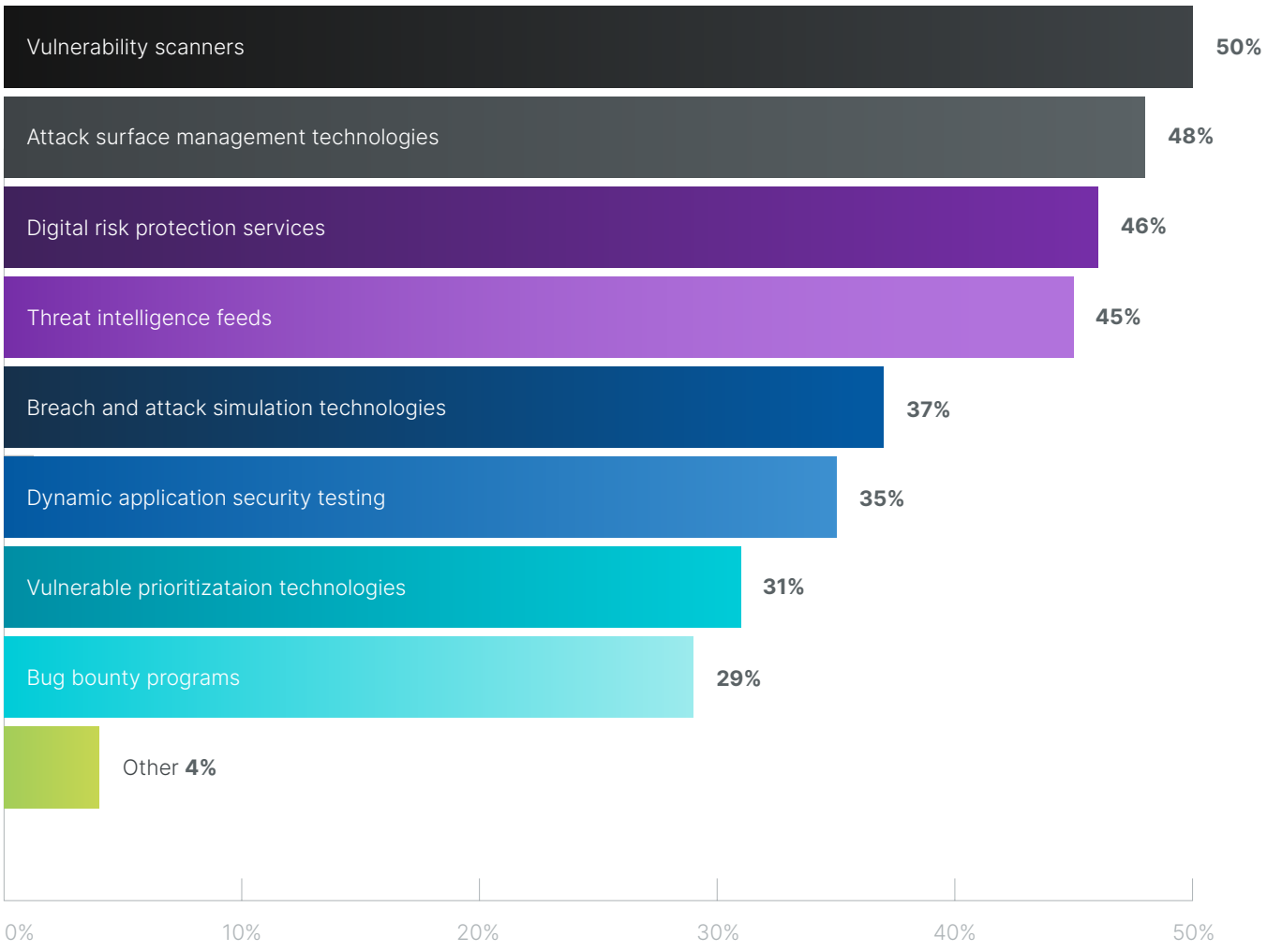
Vulnerability scanners and attack surface management solutions are the technologies most frequently purchased to support offensive security initiatives.

As shown in Figure 6, vulnerability scanners are the most important tools used to discover exposures and/or facilitate offensive security testing (50 percent of respondents). Vulnerability scans identify potential flaws in the system and rank them in order of severity depending on various factors. Almost half (48 percent) say their organizations use attack surface management technologies and digital risk protection services (46 percent).

FIGURE 6

What security tools/services does your organization use to discover exposures and/or facilitate offensive security testing?

More than one choice permitted.

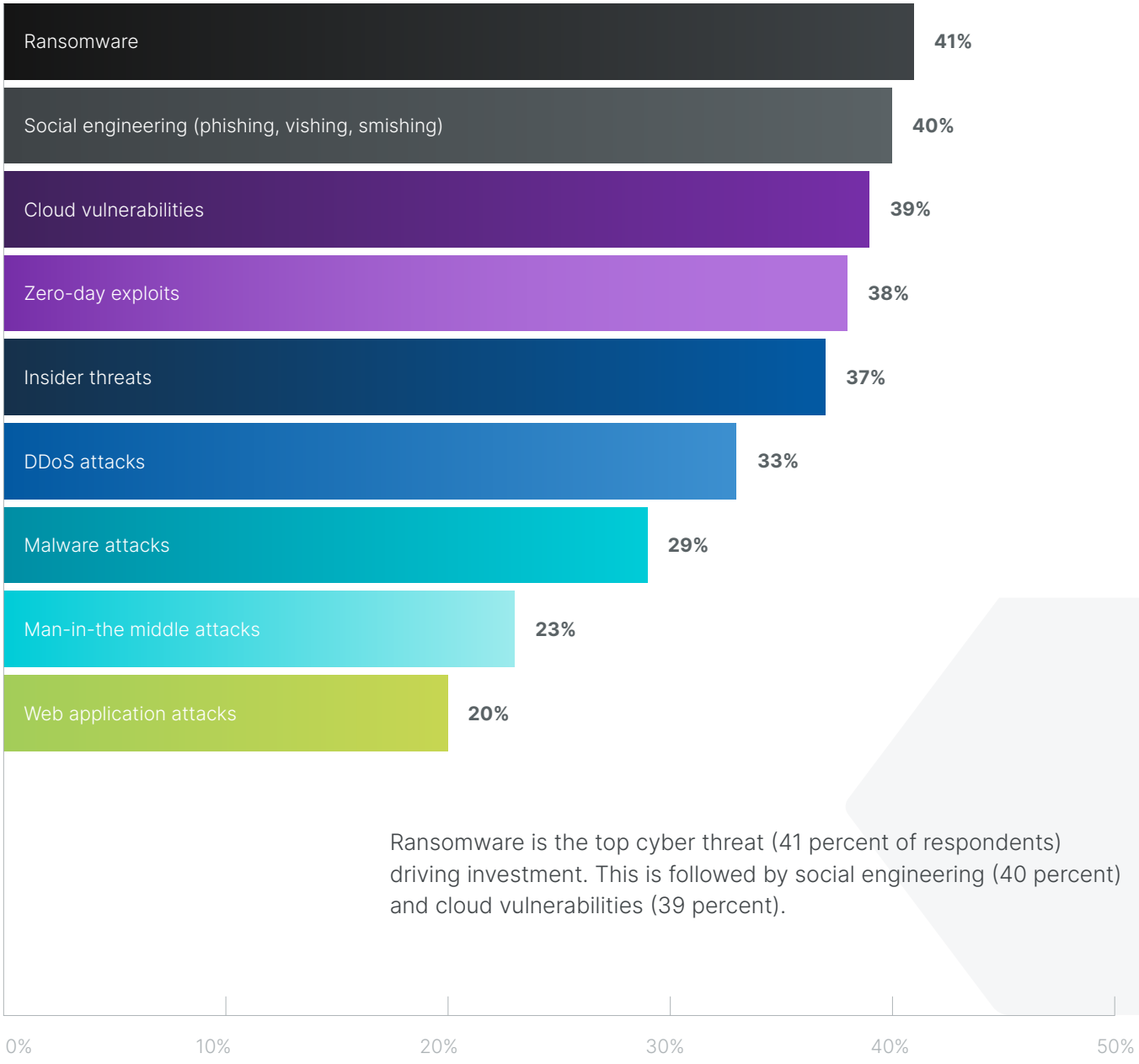


More than half of respondents (52 percent) say offensive security testing helps their organizations harden their defenses against the cyber threats listed in Figure 7.

FIGURE 7

What types of cyber threats are driving your offensive security investments?

Three choices permitted.



Ransomware is the top cyber threat (41 percent of respondents) driving investment. This is followed by social engineering (40 percent) and cloud vulnerabilities (39 percent).

OFFENSIVE SECURITY TESTING IN RED TEAMING, APPLICATION SECURITY, THE CLOUD, INTERNAL AND EXTERNAL NETWORK, AND IOT DEVICES

Only those respondents who stated they have red teaming, application security testing, IoT testing, internal and external network testing, and/or cloud security testing in their offensive security strategy are included in this section.

Most organizations include red teaming in their offensive security testing strategy.

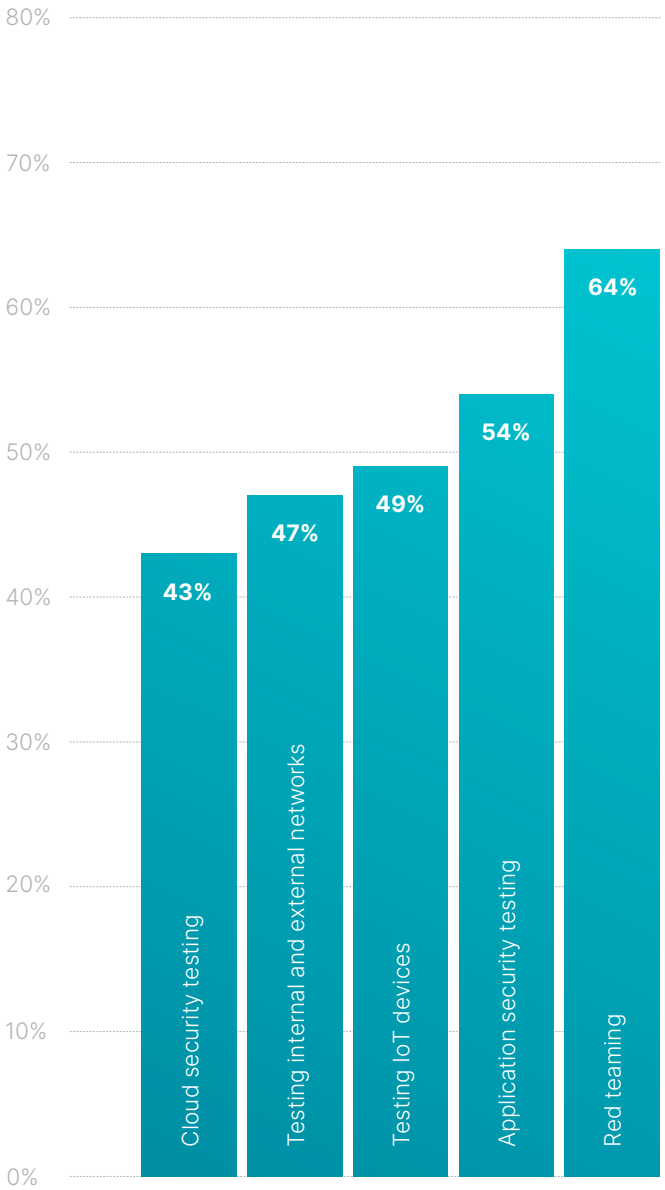
Red teaming is the practice of rigorously challenging an organization's ability to identify and mitigate tactics, techniques, and procedures designed to evade advanced security controls and processes. Sixty-four percent of respondents say their offensive security strategies include red teaming, according to Figure 8.

Offensive security testing strategies also include the following: application security testing (54 percent of respondents), testing IoT devices (49 percent), testing internal and external networks (47 percent), and cloud security testing (43 percent).

FIGURE 8

Which offensive security tests does your organization conduct?

Yes responses presented.



Offensive security testing in the cloud produces the greatest advancements in improving security posture.

Respondents were asked to rate the effectiveness of red teaming, application security, cloud security testing, and IoT devices on a scale from 1 = not effective to 10 = highly effective. Figure 9 presents the highly effective respondents (7+ on the 10-point scale).

As shown, cloud security testing is the most effective in improving organizations' resilience (57 percent) followed by red teaming (47 percent). Forty-three percent say offensive security testing is highly effective in improving the security of IoT devices, and 42 percent say application security testing is highly effective.

Organizations recognize the value of offensive security testing and plan to increase their investments.

Respondents were asked how their investments in offensive security testing will change in the next one to two years on a scale from significant increase to significant decrease. Figure 10 presents the significant and moderate increases combined. The biggest increases, either significant or moderate, will be made for IoT device security (62 percent) and cloud security (60 percent) over the next two years. As discussed before, cloud migration is a major driver in organizations' decision to adopt offensive security testing.

FIGURE 9

Effectiveness in offensive security testing strategy.

On a scale of 1 = not effective to 10 = highly effective, 7+ responses presented.

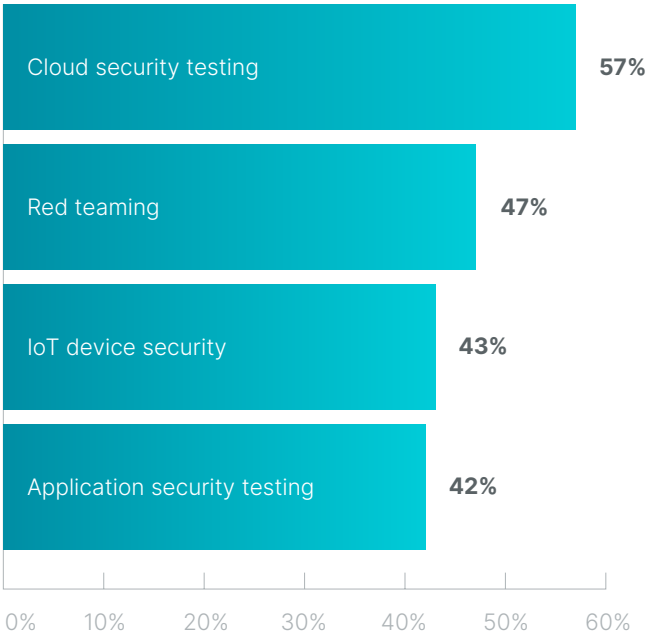
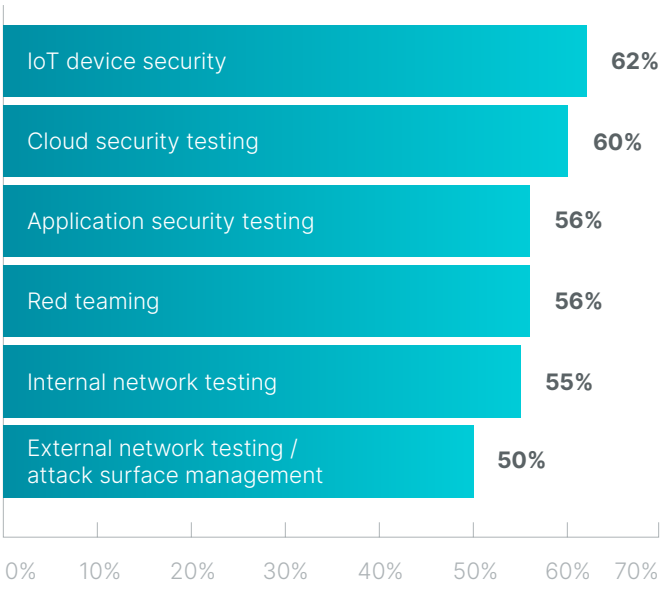


FIGURE 10

How will your investments increase in the next one to two years for offensive security testing?

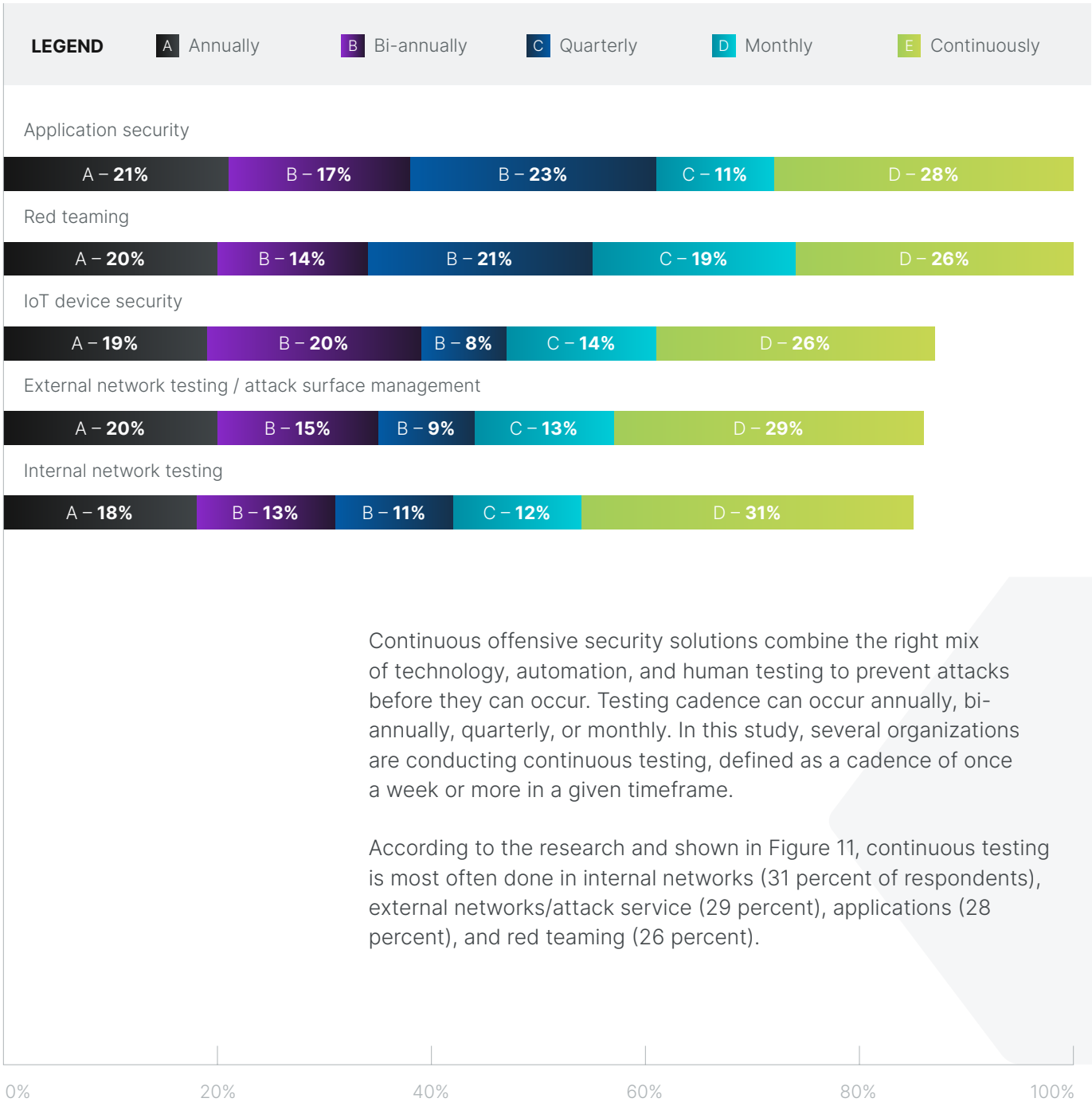
Significant and Moderate increase responses combined.



Continuous testing is important for outpacing adversaries.

FIGURE 11

How frequently do you plan to conduct testing in the next one to two years?



Continuous offensive security solutions combine the right mix of technology, automation, and human testing to prevent attacks before they can occur. Testing cadence can occur annually, bi-annually, quarterly, or monthly. In this study, several organizations are conducting continuous testing, defined as a cadence of once a week or more in a given timeframe.

According to the research and shown in Figure 11, continuous testing is most often done in internal networks (31 percent of respondents), external networks/attack service (29 percent), applications (28 percent), and red teaming (26 percent).

Tabletop exercises and ransomware readiness are the top two red teaming activities.

Tabletop exercises are used to prepare for cybersecurity incidents and are considered one of the best ways to assess ransomware readiness and establish a plan to address weaknesses in the organization's ability to both prevent and recover from attacks. As shown in Figure 12, 63 percent of respondents say their organizations use these exercises to test offensive security posture, and 55 percent say their organizations test ransomware readiness.

A red team is a group of internal security professionals who use specialized skills to execute covert attacks that evade advanced detection and response controls and processes. According to Figure 13, 70 percent of respondents have an internal red team (38 percent) or plan to build an internal team (32 percent). However, if there is a lack of in-house expertise in conducting red teaming, an external red team may be engaged. Thirty percent say their organizations anticipate using an external red team on an as needed basis.

FIGURE 12

Most important red team exercises.

More than one response permitted.

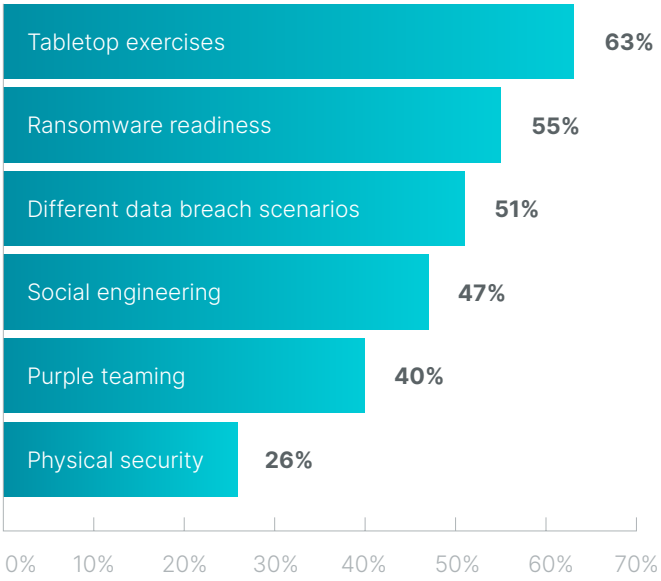
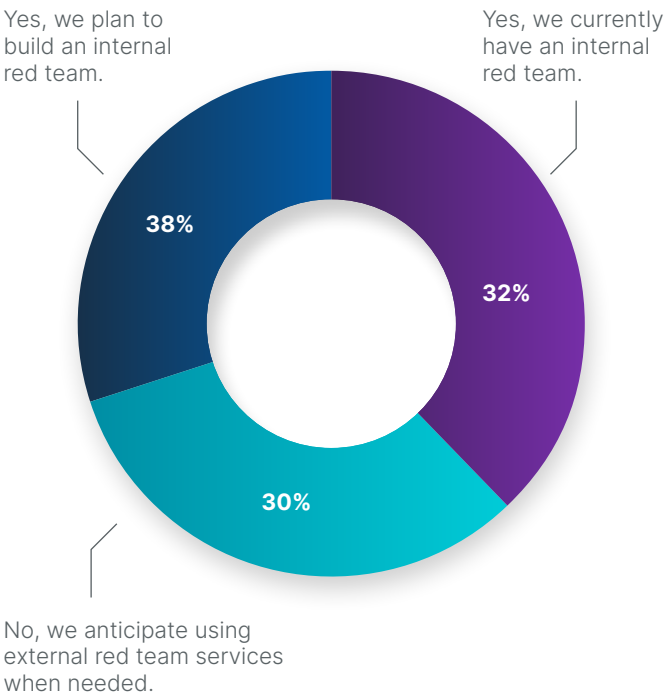


FIGURE 13

Does your organization have or plan to build an internal red team?

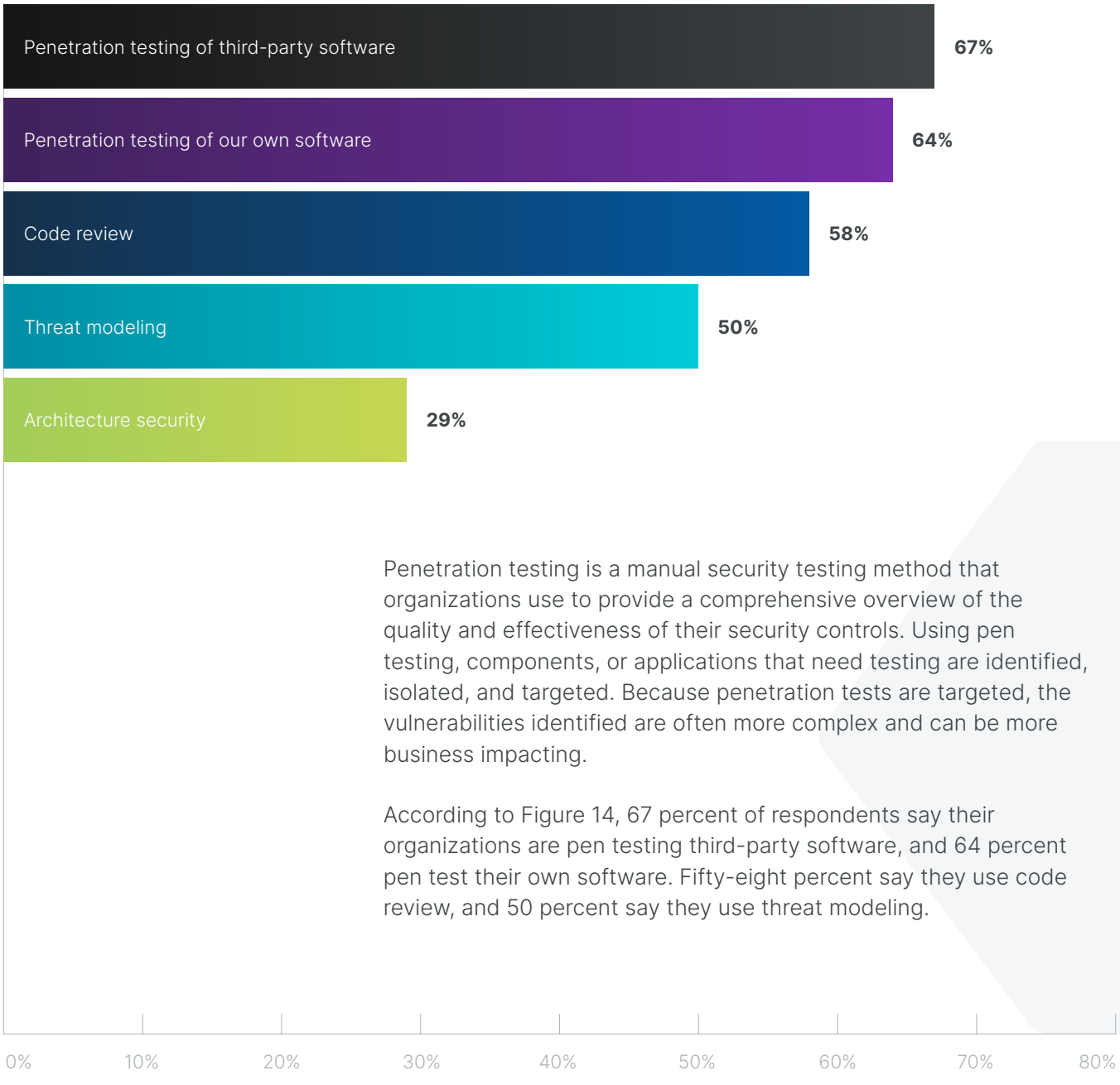


Penetration testing is the most often used offensive security strategy to test third-party and internally developed applications.

FIGURE 14

Types of application security testing conducted.

More than one response permitted.



Penetration testing is a manual security testing method that organizations use to provide a comprehensive overview of the quality and effectiveness of their security controls. Using pen testing, components, or applications that need testing are identified, isolated, and targeted. Because penetration tests are targeted, the vulnerabilities identified are often more complex and can be more business impacting.

According to Figure 14, 67 percent of respondents say their organizations are pen testing third-party software, and 64 percent pen test their own software. Fifty-eight percent say they use code review, and 50 percent say they use threat modeling.

Offensive security testing in the software development life cycle (SDLC) is most often implemented in the planning phase.

The SDLC is the process of planning, writing, modifying, and maintaining software. Almost half of respondents (48 percent) implement application security testing in the SDLC.

Of those, 54 percent of respondents say offensive security testing occurs in the planning phase, when organizations typically brainstorm, set goals, and identify high-level risks. Forty-five percent test during code development, and 45percent also stated they test when the applications are deployed. Only 33 percent say their organizations are testing during the maintenance phase of the SDLC.

Pen testing is the most used tactic to detect security vulnerabilities in the cloud.

As shown in Figure 16, 59 percent of respondents say their organizations use pen testing to detect vulnerabilities. Threat analysis, used by 41 percent of responding organizations, is a cybersecurity strategy that aims to assess an organization's security protocols, processes, and procedures to identify threats, vulnerabilities, and even gather knowledge of a potential attack before they happen.

FIGURE 15

In which phases in the SDLC is your organization implementing application security testing?

More than one response permitted.

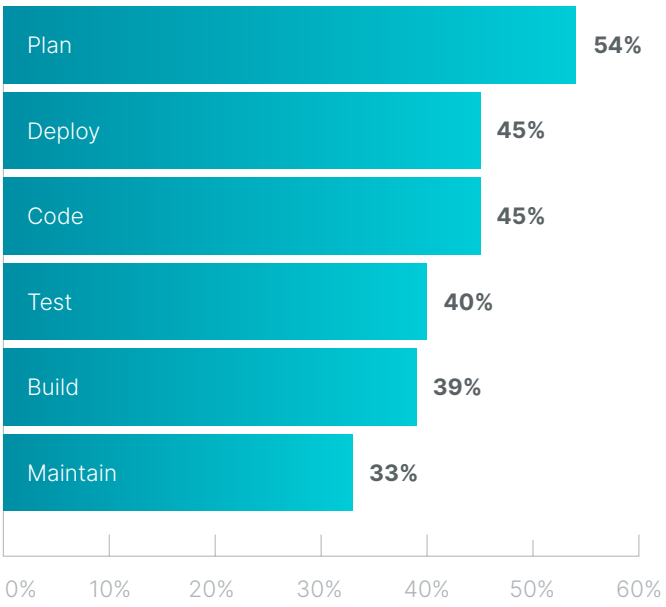


FIGURE 16

How cloud security is tested.

More than one response permitted.

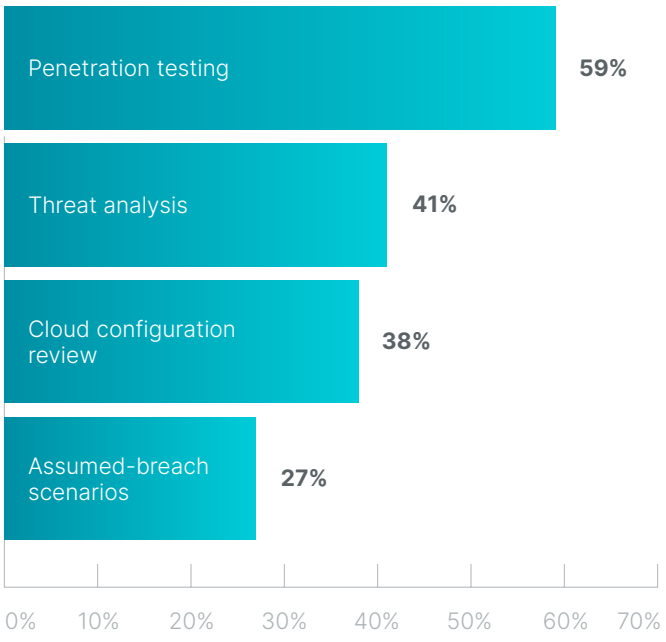
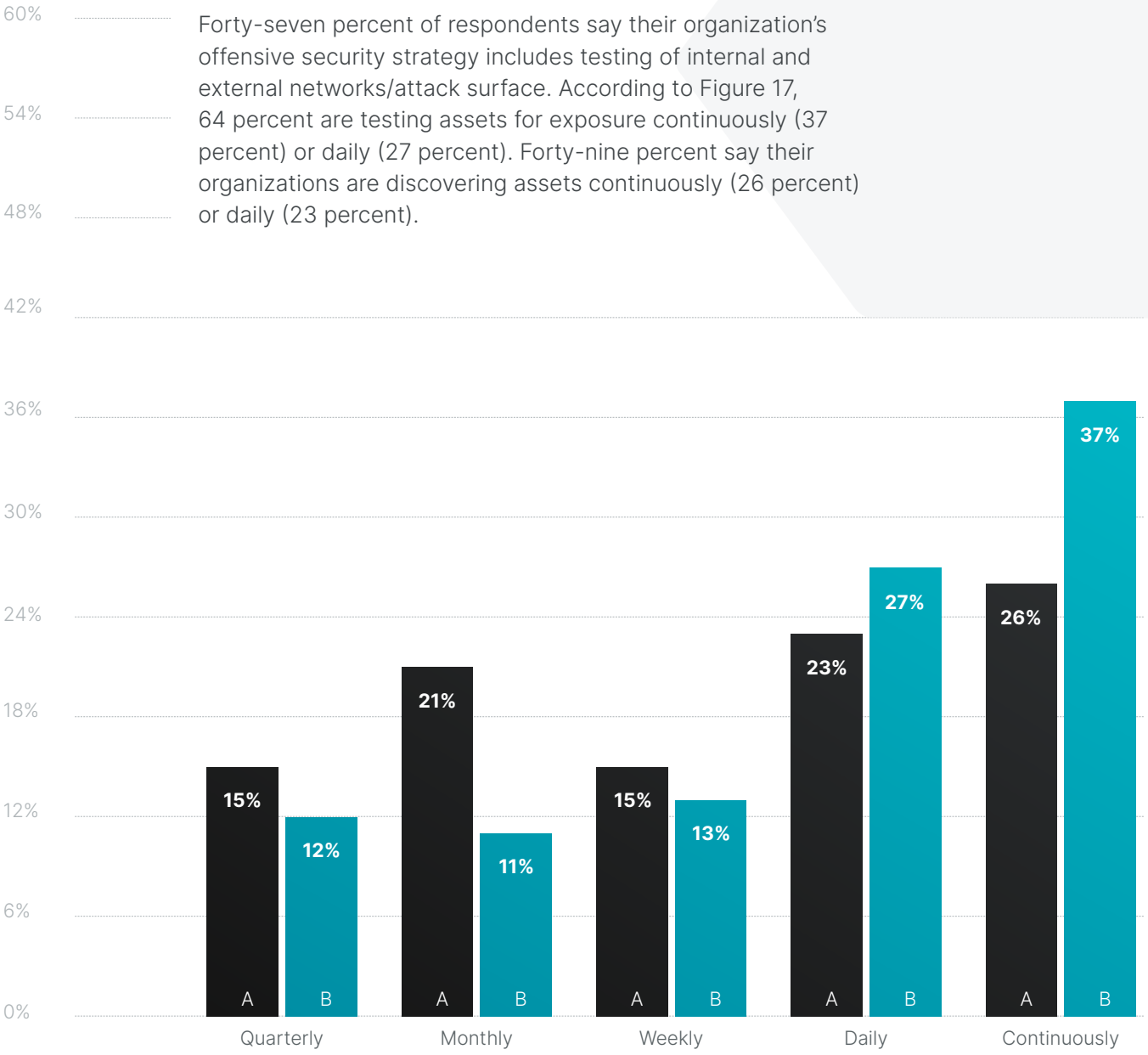


FIGURE 17

How often is your organization discovering assets across the attack surface, and how often is your organization testing your assets for exposure?

Forty-seven percent of respondents say their organization's offensive security strategy includes testing of internal and external networks/attack surface. According to Figure 17, 64 percent are testing assets for exposure continuously (37 percent) or daily (27 percent). Forty-nine percent say their organizations are discovering assets continuously (26 percent) or daily (23 percent).



LEGEND

A Frequency of discovering assets across the attack surface

B Frequency of testing your assets for exposure

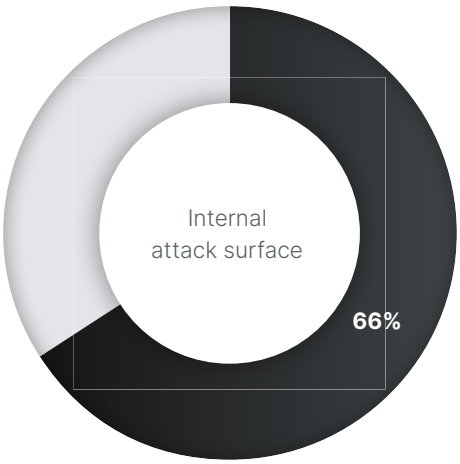
Organizations are confident in their ability to identify assets and exposures across the external and internal attack surface.

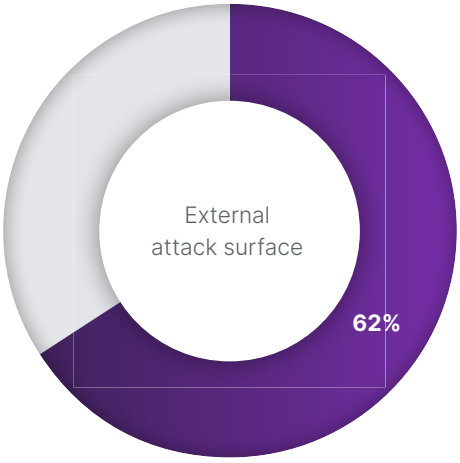
Respondents were asked to rate their organizations' confidence in the ability to identify assets and exposures across the external and internal attack surface on a scale from 1 = not confident to 10 = highly confident. Figure 18 presents the highly confident respondents (7+ on the 10-point scale). As shown, there is a high degree of confidence in identifying assets and exposures in both the internal and external attack surfaces.

FIGURE 18

Organizations are confident in their ability to identify assets and exposures across the external and internal attack surface.

On a scale from 1 = not confident to 10 = highly confident, 7+ responses presented.





INDUSTRY DIFFERENCES: FINANCIAL SERVICES, HEALTHCARE, TECHNOLOGY AND SOFTWARE, AND INDUSTRIAL NAD MANUFACTURING

In this section, we present an analysis of how the current state of offensive security differs among organizations in the Financial Services (FS – 133 respondents), Healthcare and Pharmaceutical (HC – 100 respondents), Technology and Software (TC – 113 respondents), and Industrial and Manufacturing (IM – 99 respondents) industries.

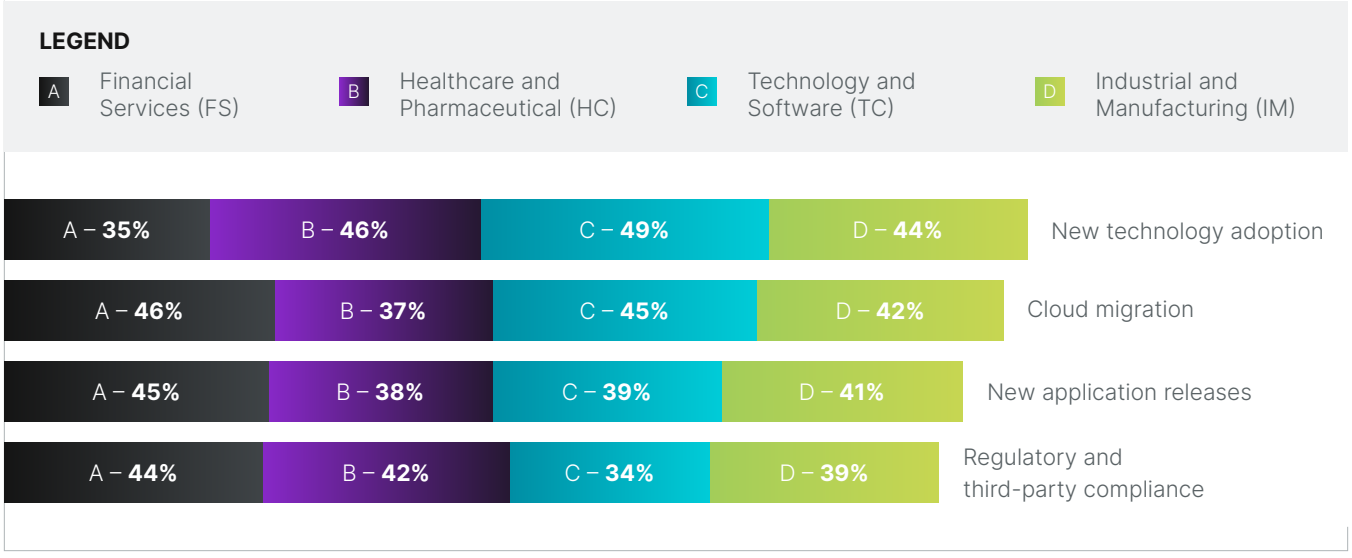
There are interesting differences among industries in why they are investing in offensive security testing.

According to Figure 19, **Healthcare and Pharmaceutical,** as well as **Technology and Software,** industries are most likely to invest in offensive security testing when new technologies are adopted (46 percent and 49 percent, respectively). **Financial Services** (46percent) and **Technology and Software** (45 percent) are most likely to cite cloud migration as a reason to adopt offensive security testing.

FIGURE 19

What use cases have driven adoption of offensive security testing?

More than one response permitted.

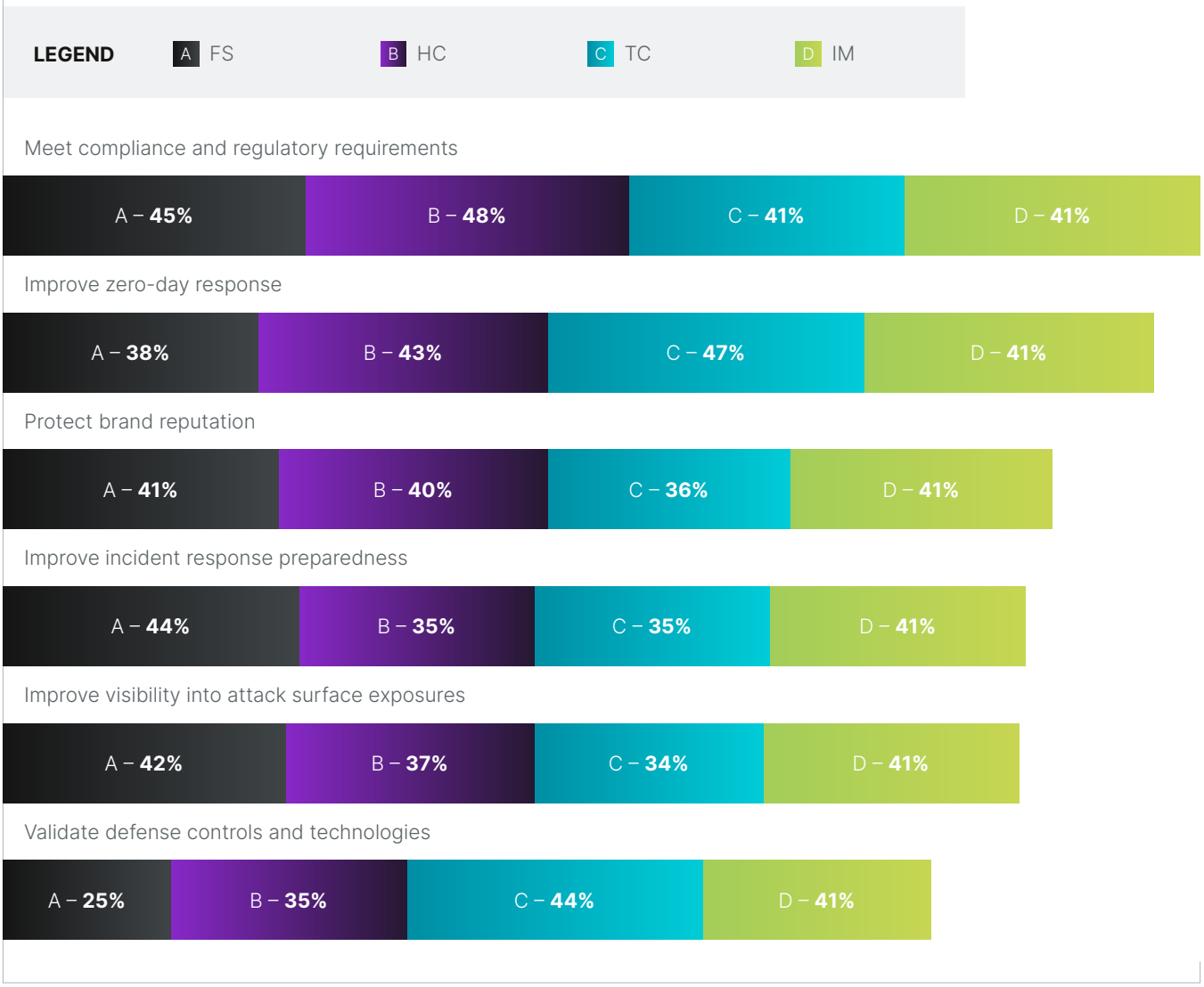


The offensive security testing goals for **Financial Services** are primarily to meet compliance and regulatory requirements (45 percent of respondents) and to improve incident response preparedness (44 percent). The primary goal for **Healthcare and Pharmaceutical** is to meet compliance and regulatory requirements (48 percent). **Technology and Software** organizations say improving zero-day response is their primary objective (47 percent).

FIGURE 20

What are your organization's offensive security testing goals?

More than one response permitted.



Respondents in the **Financial Services** (67 percent) and **Healthcare and Pharmaceutical** (63 percent) sectors report the highest rate of efficacy with offensive security testing in hardening defenses, as shown in Figure 21.

Healthcare and Pharmaceutical organizations are most likely to use vulnerability scanners (55 percent of respondents), attack surface management technologies (53 percent), and threat intelligence feeds (48 percent). **Financial Services** are most likely to use vulnerability scanners (49 percent) and digital risk protection services (45 percent). **Technology and Software** organizations are most likely to use breach and attack simulation (BAS) technologies (43 percent).

FIGURE 21

How effective has offensive security testing been in helping your organization harden its defenses against your cyber threats?

On a scale from 1 = not confident to 10 = highly confident, 7+ responses presented.

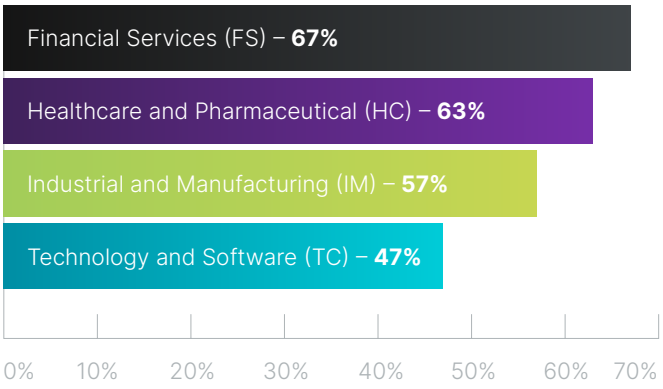
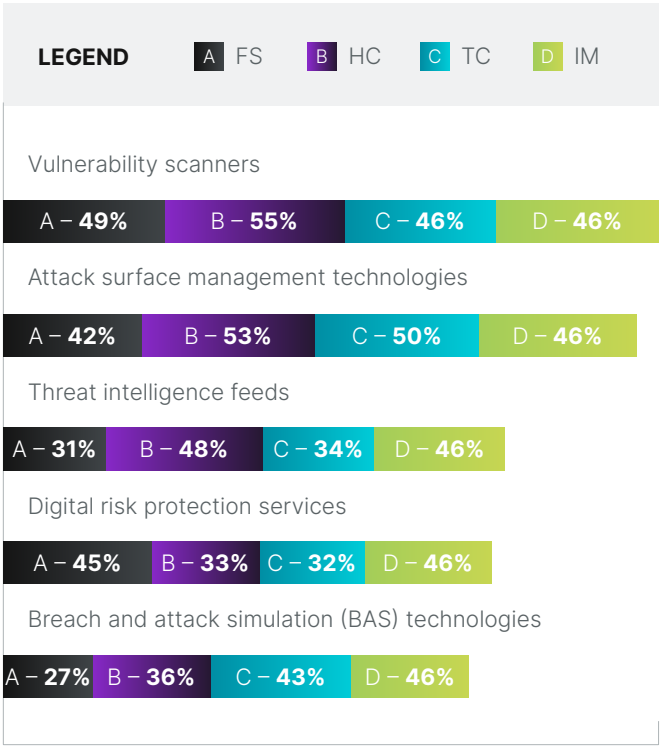


FIGURE 22

What security tools are used to discover exposures and/or facilitate offensive security testing? Q3

More than one response permitted.



Methodology

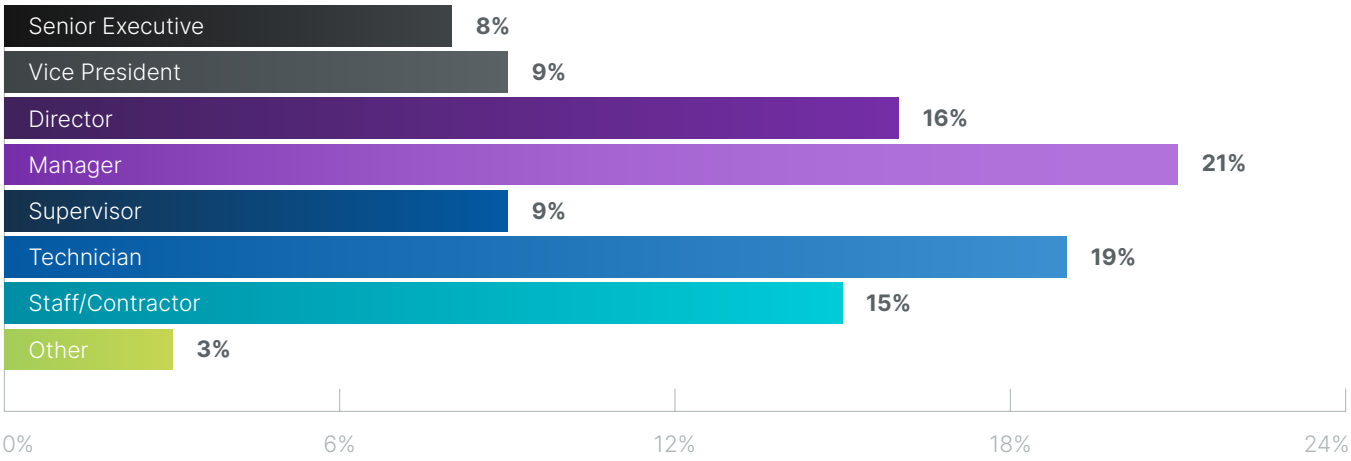
A sampling frame of 16,898 IT and security practitioners in organizations who perform offensive security testing were selected as participants for this survey. Table 1 shows 733 total returns, or completed surveys. Screening and reliability checks required the removal of 69 surveys. Our final sample consisted of 664 surveys or a 3.9 percent response.

Table 1. Sample Response	Frequency	Pct%
Sampling frame	16,898	100.0%
Total returns	733	4.3%
Rejected surveys	69	0.4%
Final sample	664	3.9%

Figure 23 reports the respondent's organizational level within participating organizations. By design, more than half (54 percent) of respondents are at or above the manager level. The largest category at 21 percent is manager.

FIGURE 23

Current position within the organization.



As shown in Figure 24, 21 percent of respondents report to the CIO, 18 percent report to the chief security officer/executive protection, and 17 percent report to the chief information security officer.

LEGEND

- A Chief Information Officer
- B Chief Security Officer/ Executive Protection
- C Chief Information Security Officer
- D Chief Technology Officer
- E Chief Risk Officer
- F CEO/Executive Committee
- G Compliance Officer
- H Human Resources VP
- I Other
- J Chief Financial Officer
- K General Counsel

Figure 25 reports the industry classification of respondents' organizations. This chart identifies financial services (20 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments, and credit cards. This is followed by technology and software (17 percent), healthcare and pharmaceutical (15 percent), industrial and manufacturing (15 percent), and services (10 percent).

FIGURE 24

Direct reporting channel.

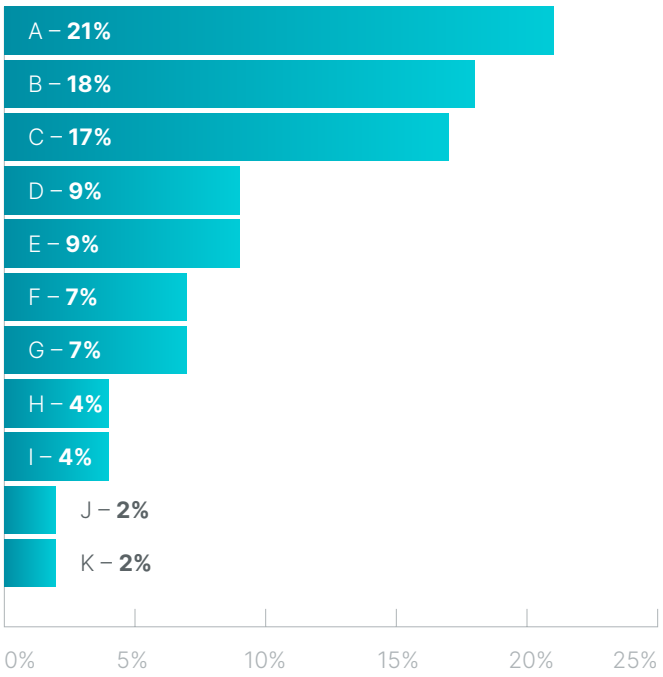


FIGURE 25

Primary industry classification.

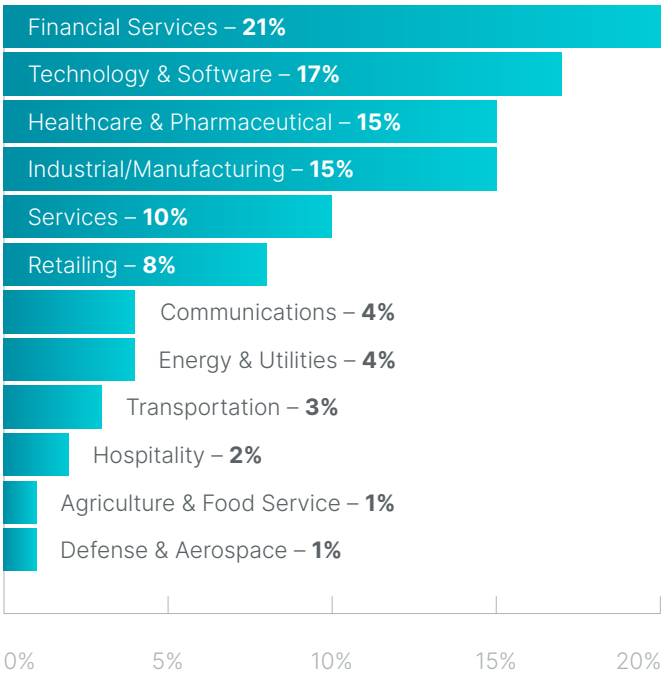
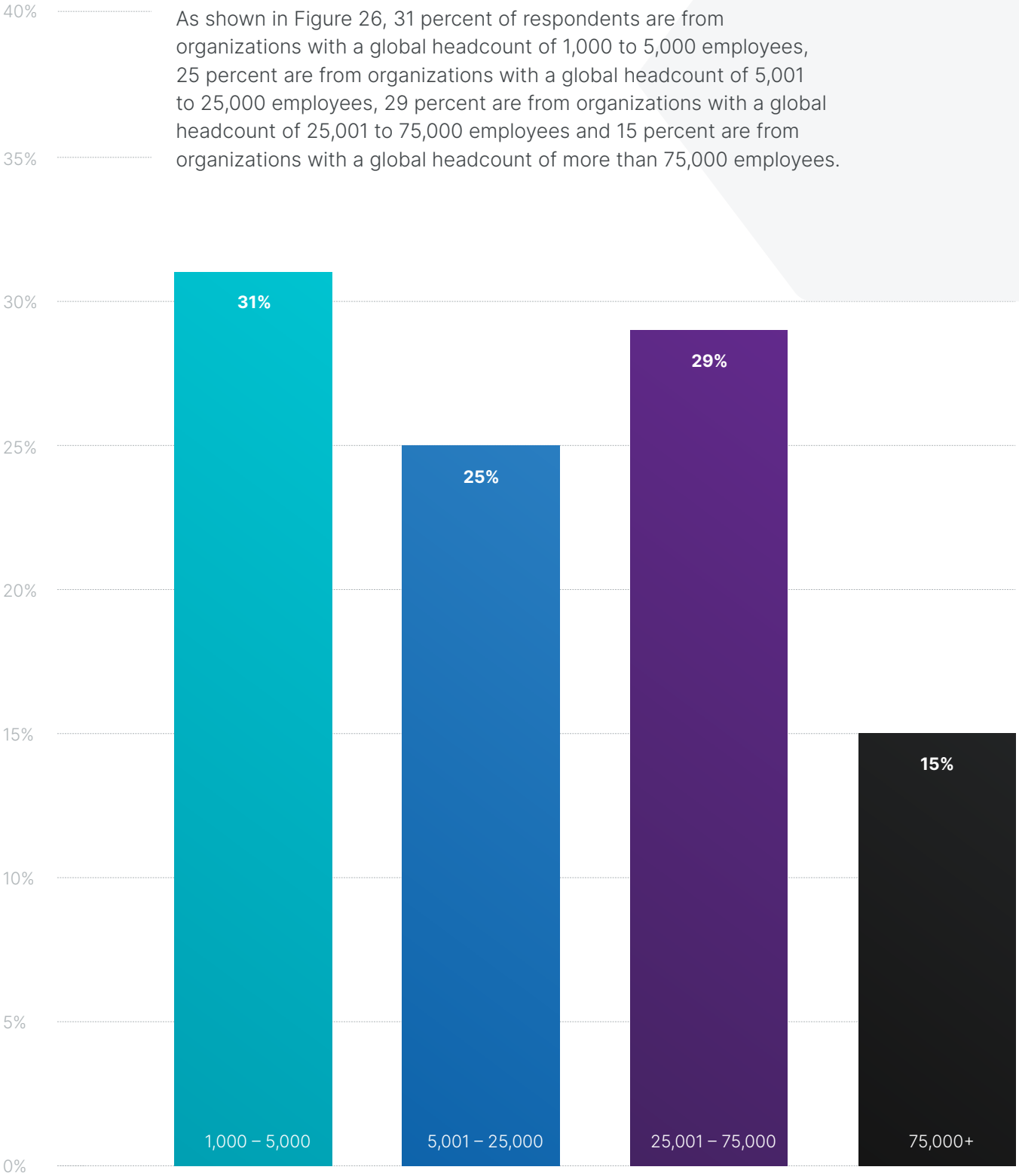


FIGURE 26

Global full-time headcount.

As shown in Figure 26, 31 percent of respondents are from organizations with a global headcount of 1,000 to 5,000 employees, 25 percent are from organizations with a global headcount of 5,001 to 25,000 employees, 29 percent are from organizations with a global headcount of 25,001 to 75,000 employees and 15 percent are from organizations with a global headcount of more than 75,000 employees.



Caveats to This Study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

1 Non-response bias

The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

2 Sampling-frame bias

The accuracy is based on contact information and the degree to which the list is representative of IT and IT practitioners in organizations who perform offensive security testing. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

3 Self-reported results

The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

Appendix

The following tables provide the detailed audited findings, such as the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured in April 2023.

Survey Response	Frequency
Total sample frame	16,898
Total returns	733
Rejected surveys	69
Final sample	664
Response rate	3.9%

S1. Does your organization currently perform any offensive security testing?	Pct %
Yes	100%
No (Stop)	0%
Total	100%

S2. What statement best describes the maturity of your organization's security strategy? Please select one choice only.	Pct %
A fully mature security strategy with activities and technologies fully deployed and maintained across the organization.	39%
A very mature security strategy with most activities and technologies defined and deployed across the organization.	29%
A mature security strategy with many activities deployed across the organization but some activities are still in the planning stage.	32%
A maturing security strategy with many activities still in the planning or early execution stage (Stop).	0%
Unsure (Stop)	0%
Total	100%

PART 1. BACKGROUND ON OFFENSIVE SECURITY PRACTICES IN YOUR ORGANIZATION

Q1. **What is your organization's approach to offensive security testing? Please select one choice only.**	**Pct %**
Testing internally only (please skip to Q3)	32%
Testing with third-party offensive security service providers only (please proceed to Q2)	27%
A combination of testing by both internal and third-party offensive security service providers (please proceed to Q2)	41%
Total	100%

Q2. **What criteria are most important when engaging offensive security vendors? Please select the top three criteria only.**	**Pct %**
Ability to customize engagements based on the needs of our organization	43%
Ability to deliver quickly	32%
Breadth of services	20%
Cost	12%
Effectiveness of services	48%
Expertise of testers	16%
History of successful engagements/testimonials	13%
Methodology	32%
Quality of deliverables, including reports	34%
Reputation	25%
Scoping accuracy	21%
Other (please specify)	4%
Total	300%

Q3. **What security tools does your organization use to discover exposures and/or facilitate offensive security testing? Please select all that apply.**	**Pct %**
Attack surface management technologies	48%
Breach and Attack Simulation (BAS) technologies	37%
Bug bounty programs	29%
Digital risk protection services	46%
Dynamic Application Security Testing (DAST)	35%
Threat intelligence feeds	45%
Vulnerability prioritization technologies	31%
Vulnerability scanners	50%
Other (please specify)	4%
Total	325%

Q4. Which of the following use cases have driven offensive security testing in your organization in the last 18 months? Please select your top three cases.	Pct %
Cloud migration	41%
Cyber insurance premiums	33%
Executive oversight	21%
Expanding attack surface	29%
Mergers and acquisitions	23%
New application releases	40%
New technology adoption	44%
Regulatory and third-party compliance	36%
Suppliers and third-party software security concerns	30%
Other (please specify)	3%
Total	300%

Q5. Which of the following goals or objectives are you trying to achieve with offensive security testing? Please select your top three choices.	Pct %
Meet compliance and regulatory requirements	42%
Protect brand reputation	37%
Improve zero-day response	42%
Validate defense controls and technologies	32%
Defend against advanced adversaries and targeted threat groups	39%
Lower cyber insurance premiums	30%
Improve visibility into attack surface exposures	40%
Improve incident response preparedness	38%
Other (please specify)	0%
Total	300%

Q6. Offensive testing has effectively satisfied the top three objectives our organization is trying to achieve with offensive security testing. Please rate this statement using the scale provided below.	Pct %
Strongly agree	31%
Agree	33%
Unsure	12%
Disagree	10%
Strongly disagree	14%
Total	100%

PART 3. ATTACKS THAT DRIVE INVESTMENTS IN OFFENSIVE SECURITY

Q7. What types of cyber threats are driving your offensive security investments? Please select your top three choices.	Pct %
Cloud vulnerabilities	39%
DDoS attacks	33%
Insider threats	37%
Malware attacks	29%
Man-in-the middle attacks	23%
Ransomware	41%
Social engineering (phishing, vishing, smishing)	40%
Web application attacks	20%
Zero-day exploits	38%
Total	300%

Q8. How effective has offensive security testing been in helping your organization harden its defenses against your top three threats on a scale from 1 = not effective to 10 = highly effective?	Pct %
1 or 2	14%
3 or 4	19%
5 or 6	15%
7 or 8	31%
9 or 10	21%
Total	100%

PART 4. OFFENSIVE SECURITY SECURITY IN RED TEAMING

Q9. Does your organization's offensive security strategy include Red Teaming?	Pct %
Yes	64%
No (please skip to Q14)	36%
Total	100%

Q10. Which Red Team services are most important for your organization to test? Please select all that apply.	Pct %
Different data breach scenarios	51%
Physical security	26%
Purple Teaming	40%
Ransomware readiness	55%
Social engineering	47%
Tabletop exercises	63%
Total	282%

Q11. How effective is Red Teaming in improving your organizational security preparedness? Please rate effectiveness on a scale of 1 = not effective to 10 = highly effective.	Pct %
1 or 2	15%
3 or 4	18%
5 or 6	20%
7 or 8	25%
9 or 10	22%
Total	100%

Q12a. How will your investments in Red Teaming change in the next one to two years?	Pct %
Significant increase	21%
Moderate increase	35%
No increase	25%
Moderate decrease	12%
Significant decrease	7%
Total	100%

Q12b. How frequently do you plan to conduct Red Teaming in the next one to two years?	Pct %
Annually	20%
Bi-annually	14%
Quarterly	21%
Monthly	19%
Continuously	26%
Total	100%

Q13. Does your organization have or plan to build an internal Red Team?	Pct %
Yes, we currently have an internal Red Team	38%
Yes, we plan to build an internal Red Team	32%
No, we anticipate using external Red Team services when needed	30%
Total	100%

PART 5. OFFENSIVE SECURITY IN APPLICATION SECURITY

Q14. Does your organization's offensive strategy include application security testing?	Pct %
Yes	54%
No	46%
Total	100%

Q15. If yes, which types of application security testing has your organization conducted? Please select all that apply.	Pct %
Architecture security	29%
Code review	58%
Penetration testing of our own software	64%
Penetration testing of third-party software	67%
Threat modeling	50%
Total	268%

Q16a. Is your organization implementing application security testing in the software development lifecycle (SDLC)?	Pct %
Yes	48%
No (please skip to Q17a)	45%
Not applicable (please skip to Q17a)	7%
Total	100%

Q16b. If yes, in which phases in the SDLC is your organization implementing application security testing? Please select all that apply.	Pct %
Plan	54%
Code	45%
Build	39%
Test	40%
Deploy	45%
Maintain	33%
Total	256%

Q17a. How will your organization's investments in offensive security for application security testing change in the next one to two years?	Pct %
Significant increase	23%
Moderate increase	33%
No increase	27%
Moderate decrease	10%
Significant decrease	7%
Total	100%

Q17b. How frequently do you plan on conducting application security testing in the next one to two years?	Pct %
Annually	21%
Bi-annually	17%
Quarterly	23%
Monthly	11%
Continuously	28%
Total	100%

Q18. Overall, how effective is application security testing for your organization? Please rate effectiveness on a scale of 1 = not effective to 10 = highly effective.	Pct %
1 or 2	12%
3 or 4	20%
5 or 6	26%
7 or 8	30%
9 or 10	12%
Total	100%

PART 6. OFFENSIVE SECURITY FOR THE CLOUD

Q19. Does your organization conduct offensive cloud security testing?	Pct %
Yes	43%
No	57%
Total	100%

Q20. Which cloud service providers is your organization currently using? Please select all that apply.	Pct %
AWS	41%
Azure	38%
GCP	21%
Oracle	23%
IBM	23%
Alibaba	14%
Other public cloud (please specify)	16%
Private cloud	8%
Total	100%

Q21. Within cloud security testing, which services are important to your organization? Please select all that apply.	Pct %
Cloud configuration review	38%
Threat analysis	41%
Penetration testing	59%
Assumed-breach scenarios	27%
Total	165%

Q22a. How will your organization's investments in cloud security testing change in the next one to two years?	Pct %
Significant increase	27%
Moderate increase	33%
No increase	16%
Moderate decrease	15%
Significant decrease	9%
Total	100%

Q22b. How frequently will your organization conduct cloud security testing in the next one to two years?	Pct %
Annually	16%
Bi-annually	13%
Quarterly	22%
Monthly	20%
Continuously	29%
Total	100%

Q23. Overall, how effective is cloud security testing for your organization? Please rate effectiveness on a scale of 1 = not effective to 10 = highly effective.	Pct %
1 or 2	10%
3 or 4	14%
5 or 6	19%
7 or 8	30%
9 or 10	27%
Total	100%

PART 7. OFFENSIVE SECURITY TESTING OF THE INTERNAL & EXTERNAL NETWORK

Q24. Does your organization's offensive security strategy include testing the internal and external networks?	Pct %
Yes	47%
No (please skip to Part 32)	53%
Total	100%

Q25. Does your organization use an attack surface management solution?	Pct %
Yes	38%
No	62%
Total	100%

Q26. How often is your organization discovering assets across your organization's attack surface? Please select only one choice.	Pct %
Continuously	26%
Daily	23%
Weekly	15%
Monthly	21%
Quarterly	15%
Total	100%

Q27. How often is your organization testing your assets for exposure? Please select only one choice.	Pct %
Continuously	37%
Daily	27%
Weekly	13%
Monthly	11%
Quarterly	12%
Total	100%

Q28. How confident is your organization in identifying assets and exposures across its external attack surface? Please rate confidence on a scale from 1 = not confident to 10 = highly confident.	Pct %
1 or 2	10%
3 or 4	12%
5 or 6	16%
7 or 8	28%
9 or 10	34%
Total	100%

Q29. How confident is your organization in identifying assets and exposures across its internal attack surface? Please rate confidence on a scale from 1 = not confident to 10 = highly confident.	Pct %
1 or 2	8%
3 or 4	9%
5 or 6	17%
7 or 8	27%
9 or 10	39%
Total	100%

Q30a. How will your investments in internal network testing change in the next one to two years?	Pct %
Significant increase	32%
Moderate increase	23%
No increase	19%
Moderate decrease	10%
Significant decrease	16%
Total	100%

Q30b. How frequently will your organization conduct internal network testing in the next one to two years?	Pct %
Annually	18%
Bi-annually	13%
Quarterly	11%
Monthly	12%
Continuously	31%
Not applicable	15%
Total	100%

Q31a. How will your organization's investments in external network testing/ attack surface management change in the next one to two years?	Pct %
Significant increase	18%
Moderate increase	32%
No increase	21%
Moderate decrease	13%
Significant decrease	16%
Total	100%

Q31b. How frequently will your organization conduct external network testing/attack surface management in the next one to two years?	Pct %
Annually	20%
Bi-annually	15%
Quarterly	9%
Monthly	13%
Continuously	29%
Not applicable	14%
Total	100%

PART 8. OFFENSIVE SECURITY FOR IOT DEVICES

Q32. Does your organization's offensive security strategy include testing IoT devices?	Pct %
Yes	49%
No (please skip to Part 9)	51%
Total	100%

Q33. How effective is offensive security testing in improving the security of your organization's IoT devices? Please rate effectiveness on a scale from 1 = not effective to 10 = highly effective.	Pct %
1 or 2	15%
3 or 4	25%
5 or 6	17%
7 or 8	32%
9 or 10	11%
Total	100%

Q34a. How will your organization's investments in offensive security for IoT device security change in the next one to two years?	Pct %
Significant increase	33%
Moderate increase	29%
No increase	18%
Moderate decrease	11%
Significant decrease	9%
Total	100%

Q34b. How frequently will offensive security practices for IoT device security be conducted in the next one to two years?	Pct %
Annually	19%
Bi-annually	20%
Quarterly	8%
Monthly	14%
Continuously	26%
Not applicable	13%
Total	100%

PART 9. DEMOGRAPHICS

D1. What organizational level best describes your current position?	Pct %
Senior Executive	8%
Vice President	9%
Director	16%
Manager	21%
Supervisor	9%
Technician	19%
Staff/Contractor	15%
Other (please specify)	3%
Total	100%

D2. Check the primary person you or your IT security leader reports to within the organization.	Pct %
CEO/Executive Committee	7%
Chief Financial Officer	2%
General Counsel	2%
Chief Information Officer	21%
Chief Technology Officer	9%
Compliance Officer	7%
Human Resources VP	4%
Chief Security Officer/Executive Protection	18%
Chief Information Security Officer	17%
Chief Risk Officer	9%
Other (please specify)	4%
Total	100%

D3. What industry best describes your organization's industry focus?	Pct %
Agriculture & food service	1%
Communications	4%
Defense & aerospace	1%
Energy & utilities	4%
Financial services	20%
Health & pharmaceutical	15%
Hospitality	2%
Industrial/manufacturing	15%
Retailing	8%
Services	10%
Technology & software	17%
Transportation	3%
Total	100%

D4. What is the worldwide headcount of your organization?	Pct %
1,000 to 5,000	31%
5,001 to 25,000	25%
25,001 to 75,000	29%
75,000+	15%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or call at 1.800.887.3118.

PONEMON INSTITUTE – Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy, and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant, or improper questions.

About Bishop Fox

Bishop Fox is the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments.

We've worked with more than 25% of the Fortune 100, half of the Fortune 10, eight of the top 10 global technology companies, and all of the top global media companies to improve their security. Our Cosmos platform, service innovation, and culture of excellence continue to gather accolades from industry award programs including Fast Company, Inc., SC Media, and others, and our offerings are consistently ranked as "world class" in customer experience surveys.

We've been actively contributing to and supporting the security community for almost two decades and have published more than 16 open-source tools and 50 security advisories in the last five years. Learn more at **bishopfox.com** or follow us on **Twitter**.

Cosmos

Cosmos proactively defends dynamic attack surfaces by combining advanced technology, automation, and expert-driven testing to continuously identify and remediate high-risk exposures before attackers even know they exist.

Leveraging a proprietary asset discovery and exposure reconnaissance engine, Cosmos continuously discovers and maps your ever-changing attack surface and identifies dangerous vulnerabilities targeted by attackers.

Acting as an extension of your security team, our operators provide deep insights into findings, deliver real-time answers to pressing questions, and conduct on-demand retesting to validate remediation procedures and accelerate the closure of attack windows.

Consulting Services

Red Teaming & Readiness

We utilize advanced offensive tools and tactics that mimic real-world adversaries to identify exploitable weaknesses in your organization while stress testing your incident responders and their playbooks for handling active, persistent attackers.

Application Penetration Testing

Our award-winning, in-depth application penetration testing goes well beyond discovering vulnerabilities to analyze the inner workings of your applications and identify critical issues, exposure points, and business logic flaws.

Cloud Penetration Testing

Fortify your cloud defenses with a complete testing methodology that extends beyond configuration reviews to illuminate high-risk entry points, overprivileged access, and susceptible internal pathways that are commonly targeted by attackers.

CONNECT WITH US

Get started today.

Are you ready to start "defending forward"? Get in touch with our offensive security experts today to explore solutions that meet your unique business needs.

Request a Meeting | Explore Cosmos

8240 S. Kyrene Rd. • Tempe, AZ 85284
480.621.8967
hello@bishopfox.com • bishopfox.com