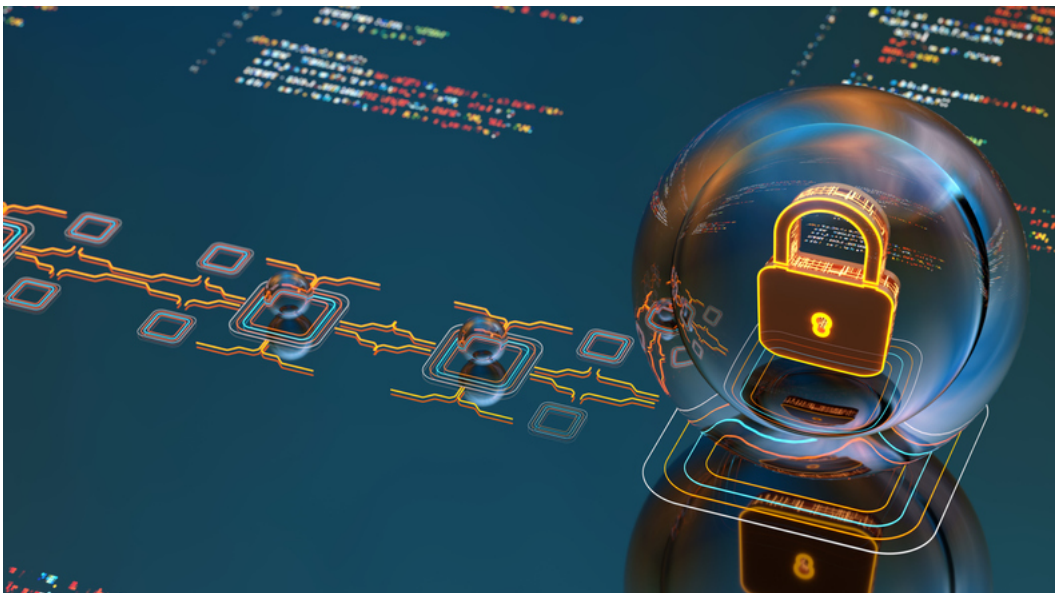


The State of Vulnerability Management in DevSecOps

Sponsored by

Rezilion

Independently conducted by Ponemon Institute LLC

Publication Date: September 2022

The State of Vulnerability Management in DevSecOps

September 2022

Part 1. Introduction

Sponsored by Rezilion, the purpose of this research is to understand the state of organizations' DevSecOps efforts to manage vulnerabilities throughout the software attack surface. Ponemon Institute surveyed 634 IT and IT security practitioners who are knowledgeable about their organizations' attack surface and effectiveness in managing vulnerabilities.

All organizations have adopted DevSecOps or are in the process of adopting a DevSecOps approach. According to the research, the lack of the right security tools is the primary barrier to having an effective DevSecOps program. This challenge is followed by a lack of workflow integration and the growing vulnerability backlog.

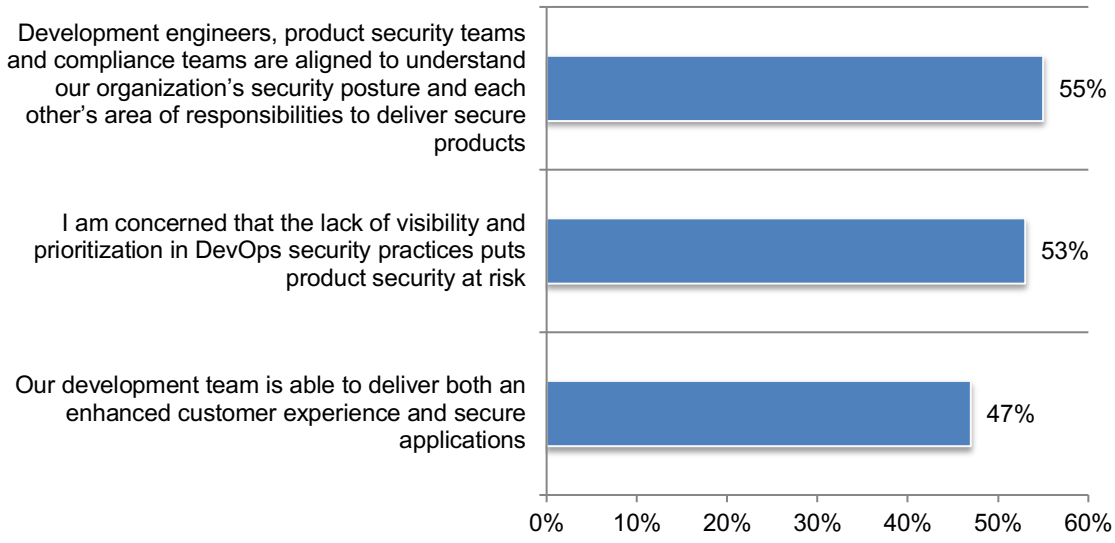
A key takeaway from this research is the time involved in dealing with a massive backlog of vulnerabilities that puts a drain on an organization's productivity and finances. More than half of participants in this research (66 percent) say their backlog consists of more than 100,000 vulnerabilities. Seventy-seven percent of respondents say it takes longer than 21 minutes to detect, prioritize and remediate just one vulnerability in production and 80 percent say their organizations spend more than 16 minutes to detect just one vulnerability in development.

At the heart of having a successful vulnerability management program is alignment between DevSecOps and the development team in being able to achieve both innovation and security when delivering products. Figure 1 summarizes the relationship between DevSecOps and operations. Only 47 percent of respondents say their organizations' development team delivers both an enhanced customer experience and secure applications and 53 percent of respondents are concerned that the lack of visibility and prioritization in DevOps security practices puts product security at risk.

Fifty-five percent of respondents say their development engineers, product security teams and compliance teams are aligned to understand their organizations' security posture and each other's area of responsibilities to deliver secure products.

Figure 1. Perceptions about the state of DevSecOps and vulnerability management

Strongly agree and Agree responses combined



The following are key takeaways from the research.

In this research, we have defined DevSecOps (short for development, security and operations) as the automation of the integration of security at every phase of the software development lifecycle from initial design through integration, testing, deployment and software delivery.

The two primary reasons to adopt DevSecOps are to improve the collaboration between development, security and operations and reduce the time to patch vulnerabilities, according to 45 percent of respondents. In addition to improving collaboration and reducing time to patch, 41 percent of respondents say it automates the delivery of secure software without slowing the software development cycle (SDLC).

Almost half of respondents say their organizations have a vulnerability backlog. Forty-seven percent of respondents say in the past 12 months organizations had applications that have been identified as vulnerable but not remediated. On average, 1.1 million individual vulnerabilities were in this backlog in the past 12 months and an average of 46 percent were remediated. However, respondents say their organizations would be satisfied if 29 percent of vulnerabilities in a year were remediated.

The inability to prioritize what needs to be fixed is the primary reason vulnerability backlogs exist, according to 47 percent of respondents. A primary reason for the existence of backlogs is not having enough information about risks that would exploit vulnerabilities (45 percent of respondents) and the lack of effective tools (43 percent of respondents).

Forty-seven percent of respondents say their organizations have adopted a **shift right strategy,** which enables continuous feedback from users. Fifty-one percent of respondents believe the benefit of a shift right strategy empowers engineers to test more, test on time and test late.

Organizations are slightly more effective in prioritizing their most critical vulnerabilities than patching vulnerabilities. Fifty-two percent of respondents say their organizations' prioritization of critical vulnerabilities is very effective but only 43 percent of respondents say timely patching is highly effective.

Vulnerability patching is mostly delayed because of the difficulty in tracking whether vulnerabilities are being patched in a timely manner. Difficulty in tracking (51 percent of respondents) is followed by the inability to take critical applications and systems off-line so they can be patched quickly (49 percent of respondents).

Automation significantly shortens the time to remediate vulnerabilities. Fifty-six percent of respondents say their organizations use automation to assist with vulnerability management. Of these respondents, 59 percent say their organizations automate patching, 47 percent say prioritization is automated and 41 percent say reporting is automated. Each week, the IT security team spends most of its time on the remediation of vulnerabilities. Sixty percent of respondents with automation say it significantly shortens the time to remediate vulnerabilities (43 percent) or slightly shortens the time (17 percent).

DevOps is an approach based on lean and agile principles to quickly deliver software that enables organizations to quickly seize market opportunities. Fifty-one percent of respondents say they have some involvement in their organization's DevOps activities. As shown Fifty-two percent of these respondents say they are involved in vulnerability management and 49 percent of these respondents say they are involved in application security.

Certain features are important to creating secure applications or services. Sixty-five percent of respondents say the ability to perform tests as part of the workflow instead of stopping, testing, fixing and restarting development is very important and 61 percent of respondents say automating vulnerability, scanning and remediation at every stage of the SDLC is very important.

The inability to quickly detect vulnerabilities and threats is the number one reason vulnerabilities are difficult to remediate in applications. Sixty-one percent of respondents say it is very difficult or difficult to remediate vulnerabilities in applications. Why it is so difficult is because of the inability to quickly detect vulnerabilities and threats (55 percent of respondents), the inability to quickly perform patches on applications in production (49 percent of respondents) followed by the lack of enabling security tools (43 percent of respondents).

More than half of organizations focus only on those vulnerabilities that pose the most risk. Fifty-three percent of respondents believe it is important to focus on only those vulnerabilities that pose the most risk and not on remediating all vulnerabilities. Forty-nine percent of respondents say their organization remediates all vulnerabilities because it does not know which ones pose the most risk.

Testing applications and keeping an inventory of business-critical applications are steps that have been fully or partially implemented. To manage vulnerabilities, 45 percent of respondents say their organizations test the application for vulnerabilities using automation and 44 percent of respondents say their organizations have created and maintained an inventory of applications and assess their business criticality.

Software Bill of Materials (SBOM) is a list of components in a piece of software. Software vendors often create products by assembling open source and commercial components. The SBOM describes the components in the product. A dynamic SBOM is updated automatically whenever a release or change occurs. Forty-one percent of respondents say their organizations use SBOM. Risk assessment and compliance with regulations are the top two features of these organizations' SBOMs. While 70 percent of respondents say continuous automatic updates are important or very important, only 47 percent say their SBOM features continuous updates.

The growing software attack surface is a high concern. importance to 10 = high importance. Seventy-one percent of respondents say their organizations are very or highly concerned about risks created by the growing software attack surface. A higher percentage of respondents (77 percent) believe it is very or highly important.

Despite the concerns, most organizations are not effective in both knowing the attack surface and securing it. Only 43 percent of respondents say their organizations' effectiveness is very high and only 45 percent of respondents say their organizations are effective in knowing the attack surface.

Elimination of complexity and eliminate vulnerabilities that are exploitable are the most important steps to safeguard the attack surface. Sixty percent of respondents say the elimination of complexity in the software attack surface vulnerabilities that are exploitable (56 percent of respondents) will reduce threats to the attack surface. This is followed by knowledge of all software components (51 percent of respondents). Only 26 percent of respondents say regular network scans reduce threats.

Part 2. 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.

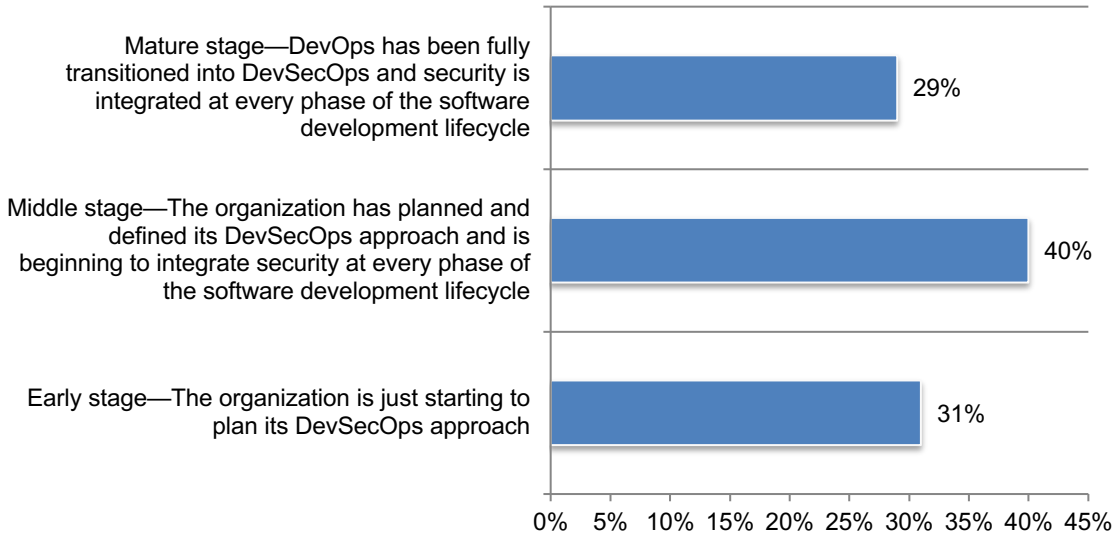
- DevSecOps: the benefits and challenges
- Reducing the vulnerability backlog
- Creating secure applications and services
- Steps taken to minimize risks in the software attack surface

DevSecOps: the benefits and challenges

Most organizations have achieved a mature DevSecOps approach. All organizations represented in this study are either planning or have planned their DevSecOps to improve security in the development of applications.

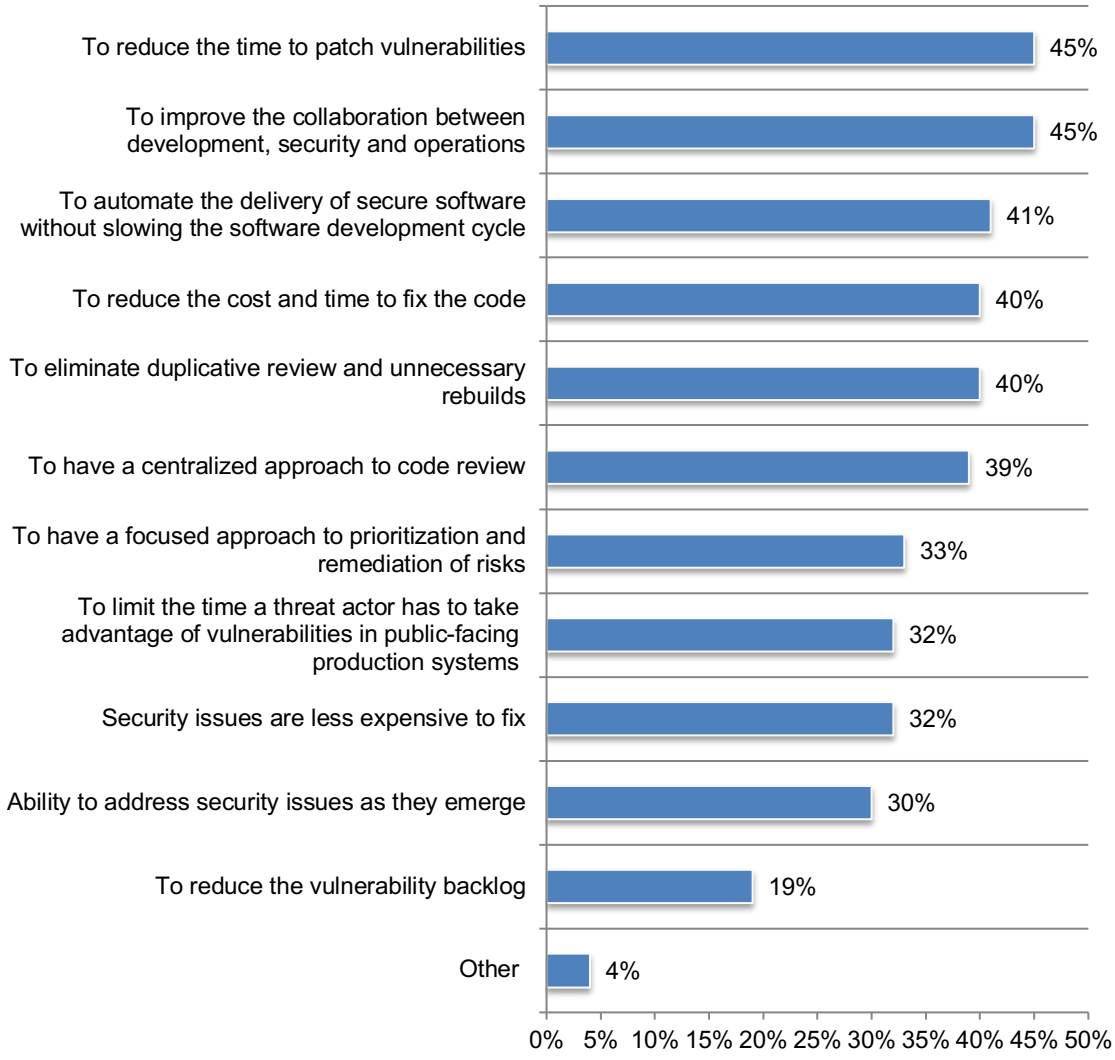
According to Figure 2, 69 percent of respondents say their organizations have either achieved a mature stage with DevOps fully transitioned into DevSecOps and security is integrated at every phase of the software development lifecycle (SDLC) (29 percent of respondents) or are beginning to integrate it at every phase of the software development lifecycle.

Figure 2. What best describes the maturity of your organization's DevSecOps?



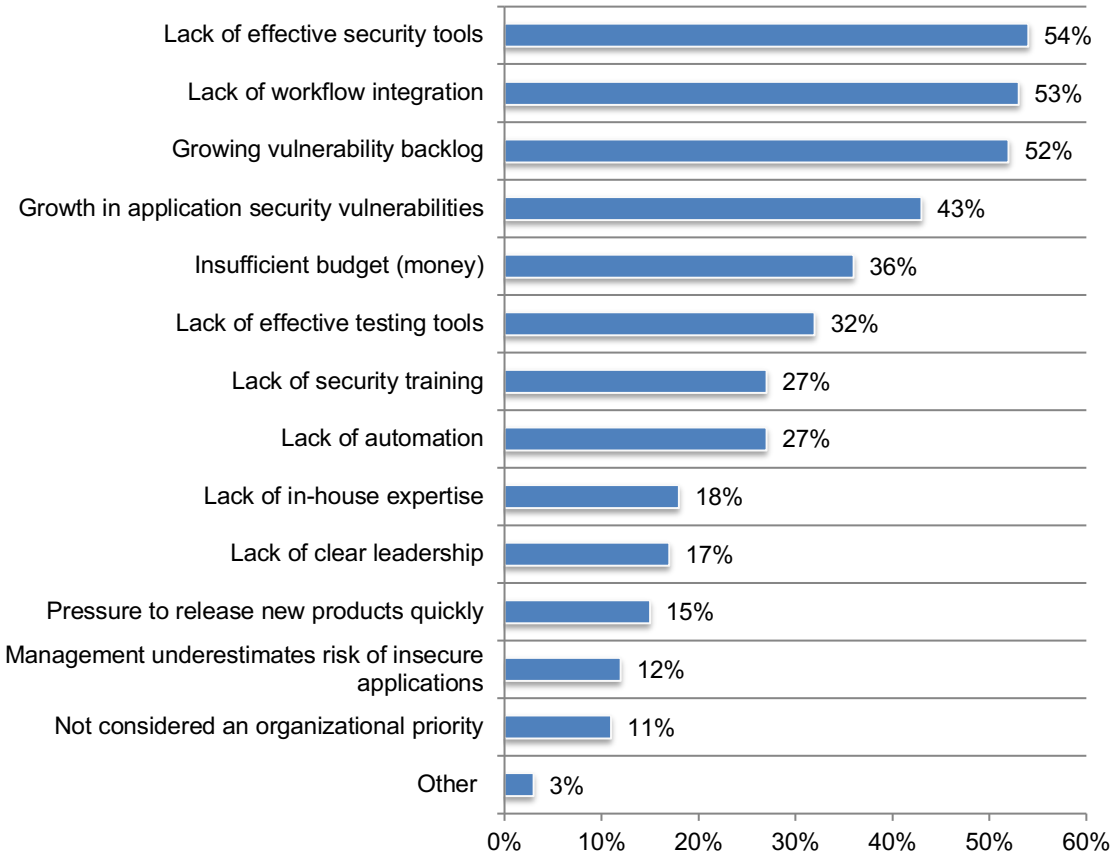
The two primary reasons to adopt DevSecOps are to improve the collaboration between development, security and operations and reduce the time to patch vulnerabilities, according to 45 percent of respondents. Figure 3 lists the benefits of a DevSecOps approach. In addition to improving collaboration and reducing time to patch, 41 percent of respondents say it automates the delivery of secure software without slowing the software development cycle (SDLC).

Figure 3. What are the primary reasons for adopting DevSecOps?
Four responses permitted



Organizations need the right security tools to achieve a mature DevSecOps. Figure 4 presents a list of the challenges to achieving a fully effective DevSecOps. The primary barriers are the lack of effective security tools (54 percent of respondents), the lack of workflow integration (53 percent of respondents) and the growing vulnerability backlog (52 percent of respondents).

Figure 4. What are the challenges to having a fully effective DevSecOps?
Four responses permitted

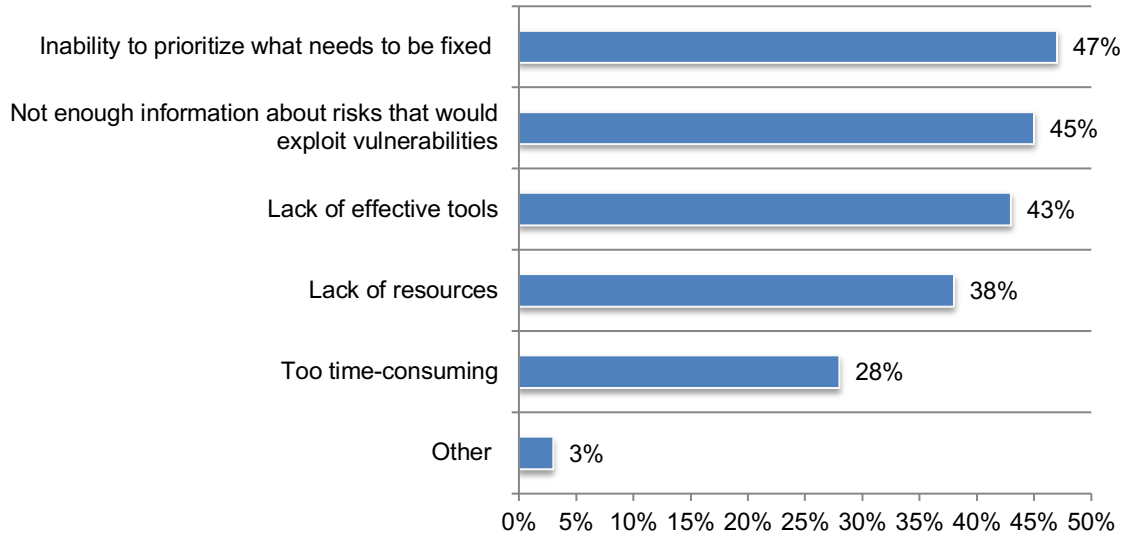


Reducing vulnerability backlogs

Almost half of respondents say their organizations have a vulnerability backlog. Forty-seven percent of respondents say in the past 12 months organizations had applications that have been identified as vulnerable but not remediated. On average, 1.1 million individual vulnerabilities were in this backlog in the past 12 months and an average of 46 percent were remediated. However, respondents say their organizations would e satisfied if 29 percent of vulnerabilities in a year were remediated.

The inability to prioritize what needs to be fixed is the primary reason vulnerability backlogs exist, according to 47 percent of respondents. According to Figure 5, a primary reason for the existence of backlogs is not having enough information about risks that would exploit vulnerabilities (45 percent of respondents) and the lack of effective tools (43 percent of respondents).

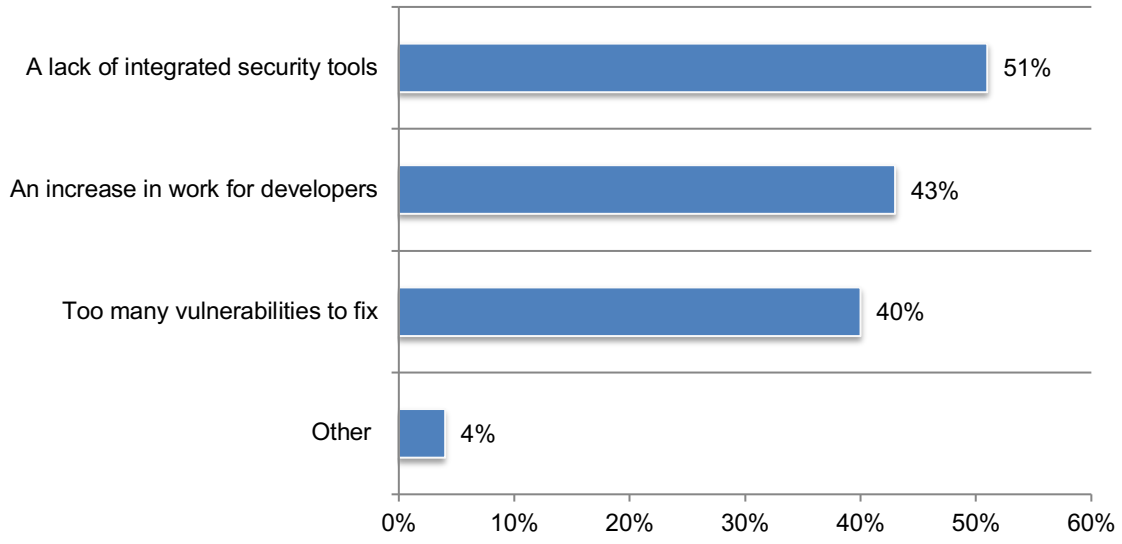
Figure 5. What were the challenges to remediating this vulnerability backlog?
More than one response permitted



A shift left strategy is where problem resolution and other activities are moved as close as possible to the end user. An effective shift left approach should not increase work for developers but rather help them to be more effective. Shifting left should reduce developer's vulnerability backlogs and help them prioritize what is exploitable while delivering innovative products.

The primary challenge to having a shift left strategy is a lack of integrated security tools. Fifty-two percent of respondents say their organizations have adopted a shift left strategy as described above. Respondents do believe there are challenges caused by a shift left strategy that make it difficult to create innovative applications or services. As shown in Figure 6, the lack of integrated security tools, an increase in work for developers and too many vulnerabilities are challenges.

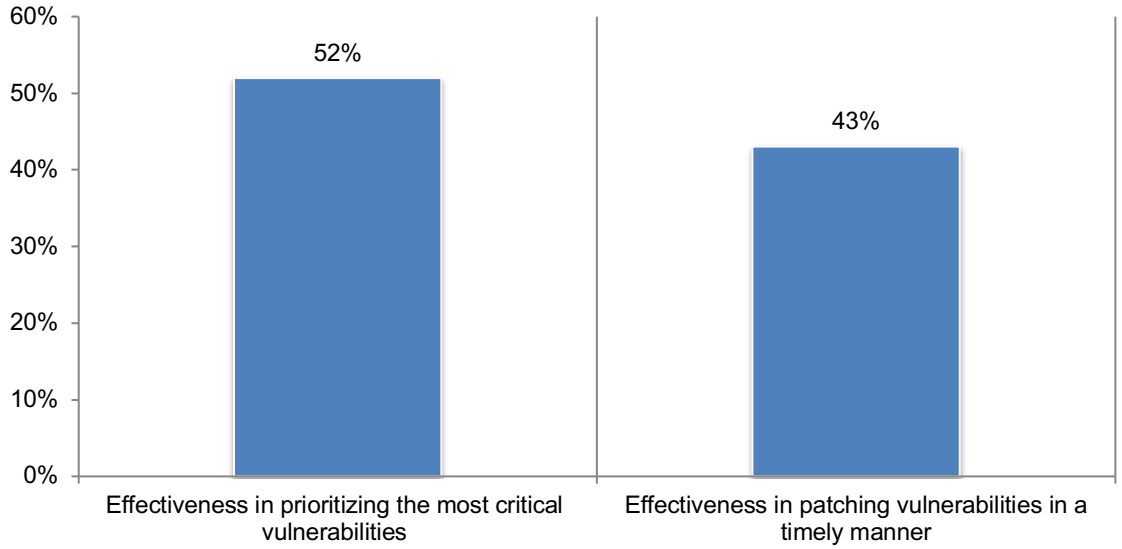
Figure 6. What challenges does a shift left strategy pose to the ability to create innovative applications or services?
More than one response permitted



Forty-seven percent of respondents say their organizations have adopted a **shift right strategy,** which enables continuous feedback from users. Fifty-one percent of respondents believe the benefit of a shift right strategy empowers engineers to test more, test on time and test late.

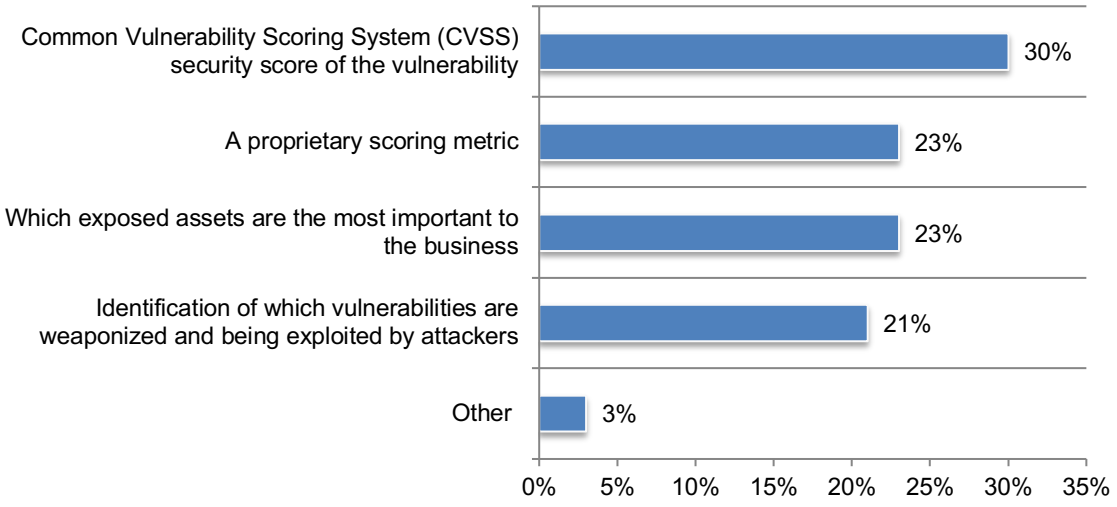
Organizations are slightly more effective in prioritizing their most critical vulnerabilities than patching vulnerabilities. Respondents were asked to rate their organizations' effectiveness in prioritizing and patching vulnerabilities on a scale from 1 = not effective to 10 = highly effective. Figure 7 presents the 7+ responses. As shown, 52 percent of respondents say their organizations' prioritization of critical vulnerabilities is very effective but only 43 percent of respondents say timely patching is highly effective.

Figure 7. Effectiveness in prioritizing and patching vulnerabilities in a timely manner
On a scale from 1= low effectiveness to 10 = high effectiveness, 7+ responses presented



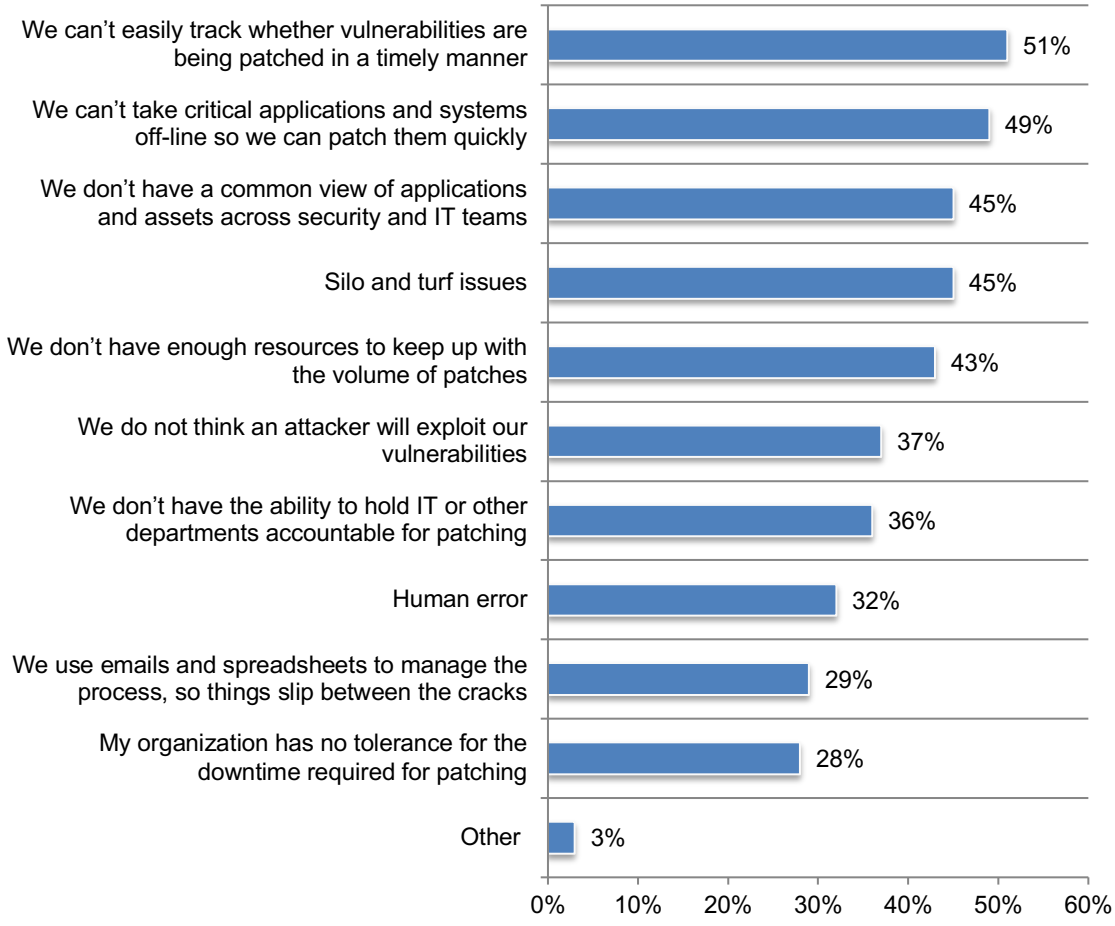
The Common Vulnerability Scoring System (CVSS) security score of the vulnerability is the number one method for prioritizing vulnerabilities, as shown in Figure 8. This is followed by which exposed assets are the most important to the business and a proprietary scoring metric (both 23 percent of respondents).

Figure 8. What is your primary method for prioritizing vulnerabilities



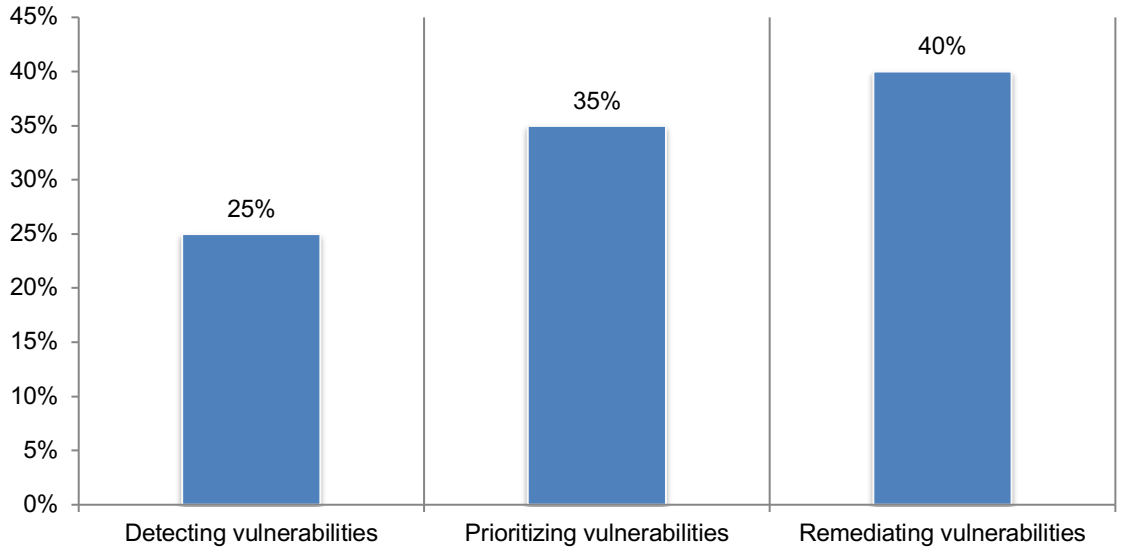
Vulnerability patching is mostly delayed because of the difficulty in tracking whether vulnerabilities are being patched in a timely manner. Figure 9 provides reasons for causing major delays in vulnerability patching processes. Difficulty in tracking (51 percent of respondents) is followed by the inability to take critical applications and systems off-line so they can be patched quickly (49 percent of respondents).

Figure 9. Which factors cause major delays in your vulnerability patching process?
More than one response permitted



Most time spent weekly on vulnerability management is dedicated to remediating (40 percent) and prioritizing vulnerabilities 35 percent, as shown in Figure 10.

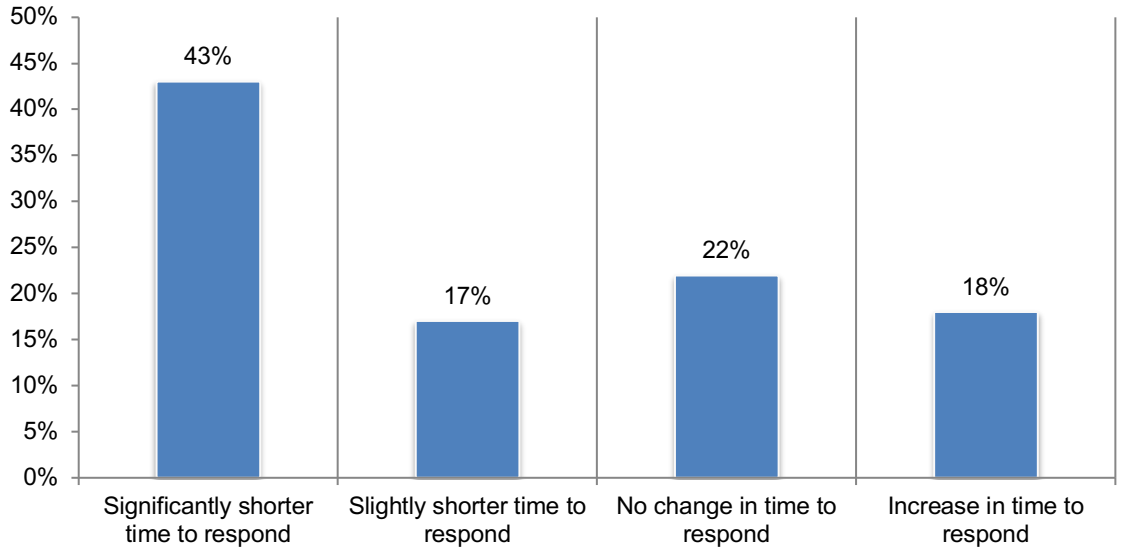
Figure 10. How much time does your team spend weekly on the following vulnerability management activities?



Automation significantly shortens the time to remediate vulnerabilities. Fifty-six percent of respondents say their organizations use automation to assist with vulnerability management. Of these respondents, 59 percent say their organizations automate patching, 47 percent say prioritization is automated and 41 percent say reporting is automated.

As shown above, each week the IT security team spends most of its time on the remediation of vulnerabilities. According to Figure 11, 60 percent of respondents with automation say it significantly shortens the time to remediate vulnerabilities (43 percent) or slightly shortens the time (17 percent).

Figure 11. How has automation impacted the time it takes to remediate vulnerabilities?



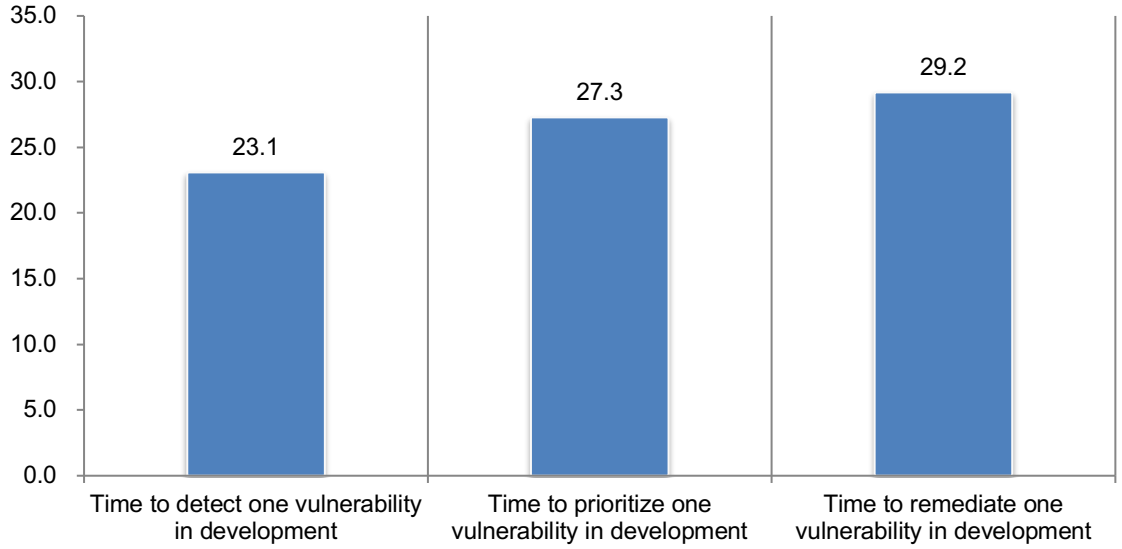
Following is a breakdown of the time to detect, prioritize and remediate one vulnerability in development, production and in the infrastructure.

According to the research:

- In development, it takes the most time to remediate and prioritize one vulnerability
- In production, the most time is spent on detection and remediation
- In the infrastructure, IT/infrastructure engineers spend the most time is spent to prioritize one vulnerability
- In the infrastructure, the vulnerability team spends the most time on prioritizing and remediating vulnerabilities

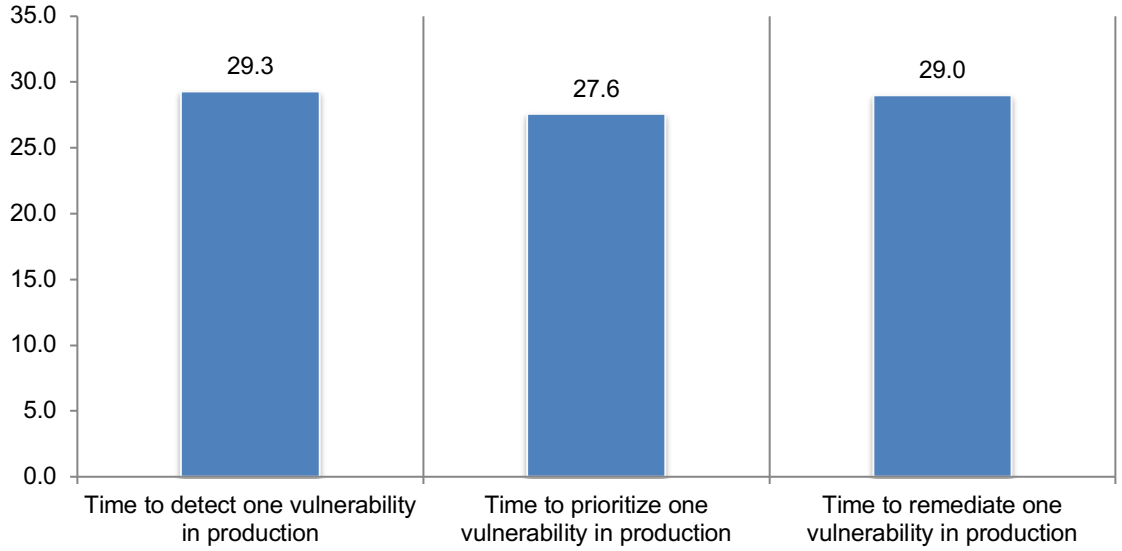
According to Figure 12, in development, it takes on average 23 minutes to detect one vulnerability, 27 minutes to prioritize one vulnerability and 29 minutes to remediate one vulnerability.

Figure 12. The time to detect, prioritize and remediate one vulnerability in development
Extrapolated values presented



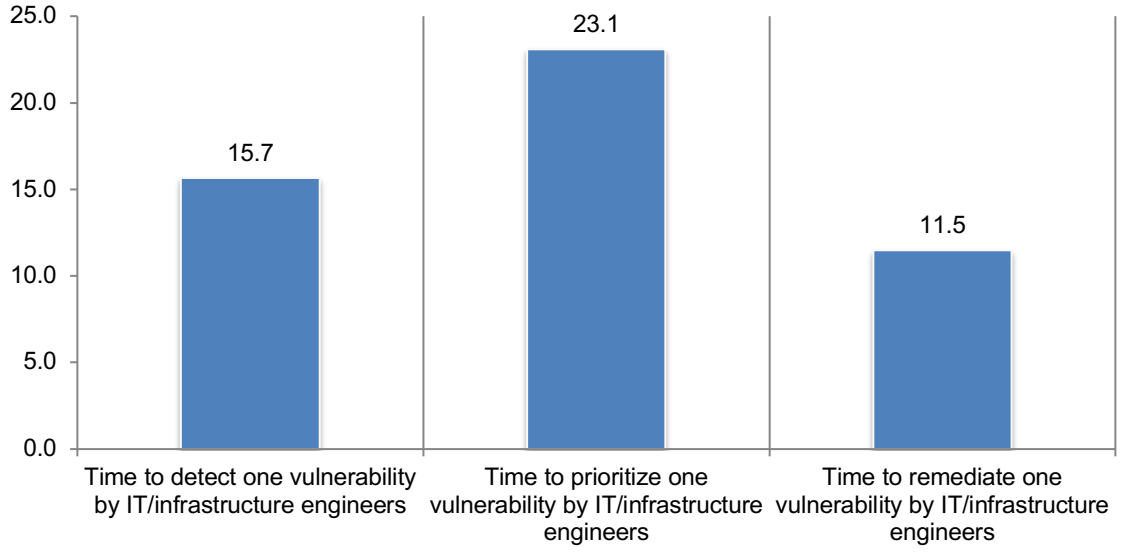
In production, it takes 29 minutes to detect one vulnerability, 28 minutes to prioritize one vulnerability and 29 minutes to remediate one vulnerability, as shown in Figure 13.

Figure 13. The time to detect, prioritize and remediate one vulnerability in production
Extrapolated values presented



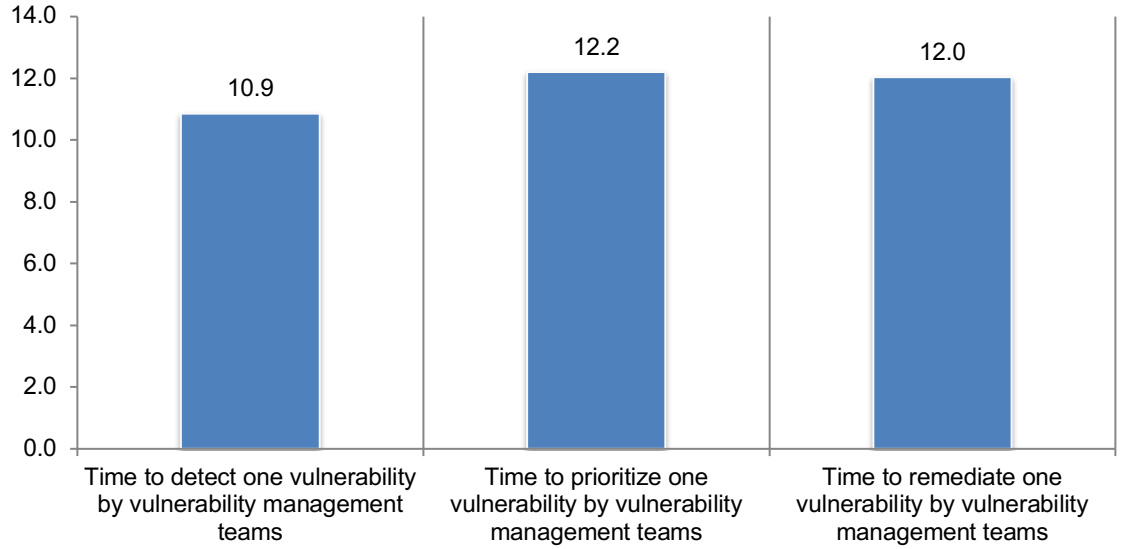
Sixty-three percent of respondents consider their organizations' infrastructure critical. According to Figure 14, on average, it takes 16 minutes to detect one vulnerability by IT/infrastructure, 23 minutes to prioritize one vulnerability by IT/infrastructure and 12 minutes to remediate one vulnerability by IT/infrastructure engineers.

Figure 14. The time to detect, prioritize and remediate one vulnerability by IT/infrastructure engineers
Extrapolated values presented



On average, it takes 11 minutes to detect one vulnerability by vulnerability management teams, 12 minutes to prioritize one vulnerability by vulnerability management teams and 12 minutes to remediate one vulnerability by vulnerability management teams, as show in Figure 15.

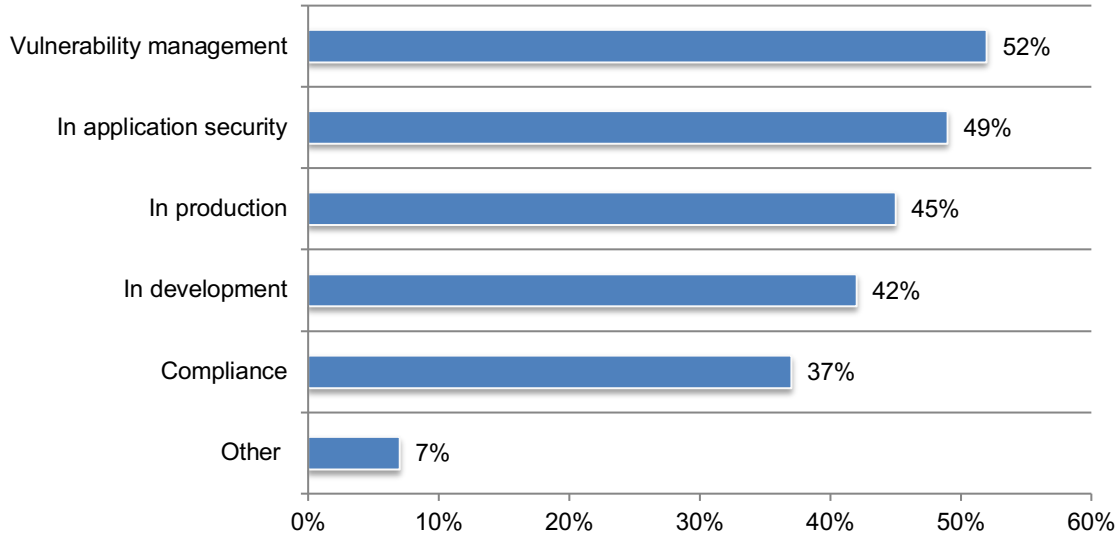
Figure 15. The time to detect, prioritize and remediate one vulnerability by vulnerability management teams in the infrastructure
Extrapolated values presented



Creating secure applications and services

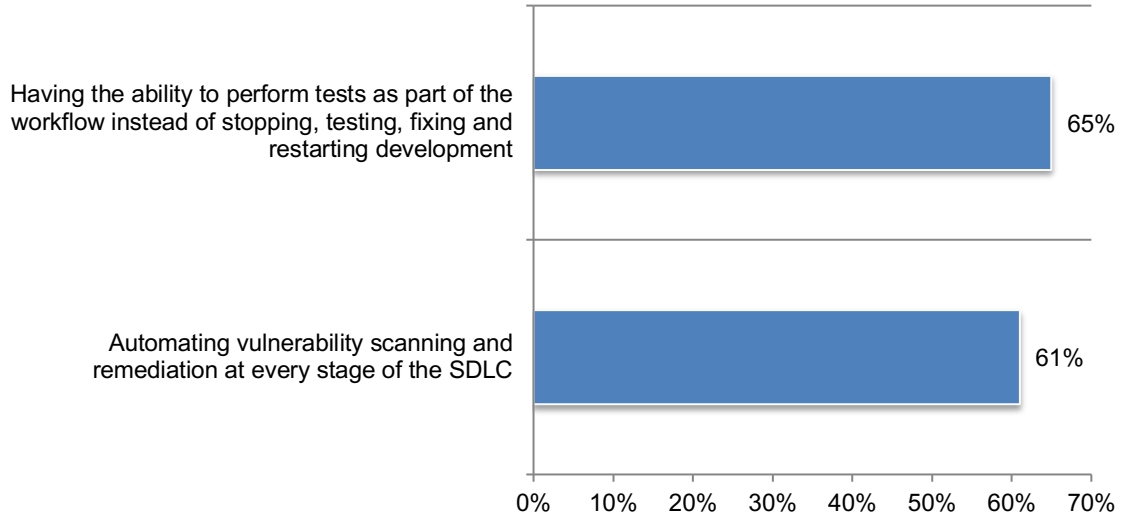
DevOps is an approach based on lean and agile principles to quickly deliver software that enables organizations to quickly seize market opportunities. Fifty-one percent of respondents say they have some involvement in their organization's DevOps activities. As shown in Figure 16, 52 percent of these respondents say they are involved in vulnerability management and 49 percent of these respondents say they are involved in application security.

Figure 16. How are you involved in your organization's DevOps activities?
More than one response permitted



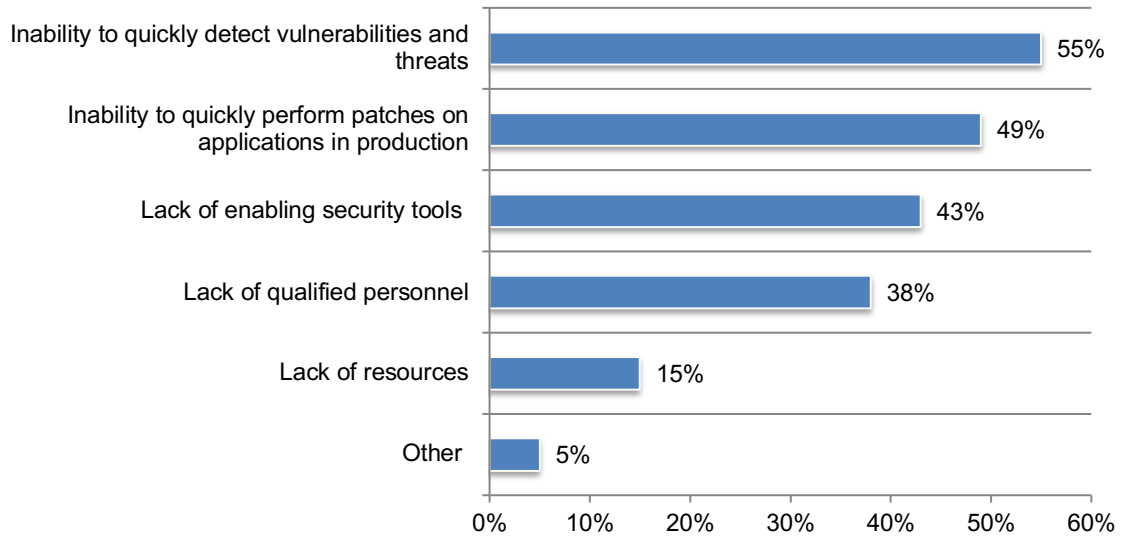
Certain features are important to creating secure applications or services. Respondents were asked to rate certain features in creating secure applications or services on a scale of 1 = not important to 10 = very important. Figure 17 presents the very important features (7+ on the 10-point scale). Sixty-five percent of respondents say the ability to perform tests as part of the workflow instead of stopping, testing, fixing and restarting development is very important and 61 percent of respondents say automating vulnerability, scanning and remediation at every stage of the SDLC is very important.

Figure 17. Importance of features in creating secure applications or services
On a scale from 1 = not important to 10 = very important, 7+ responses presented



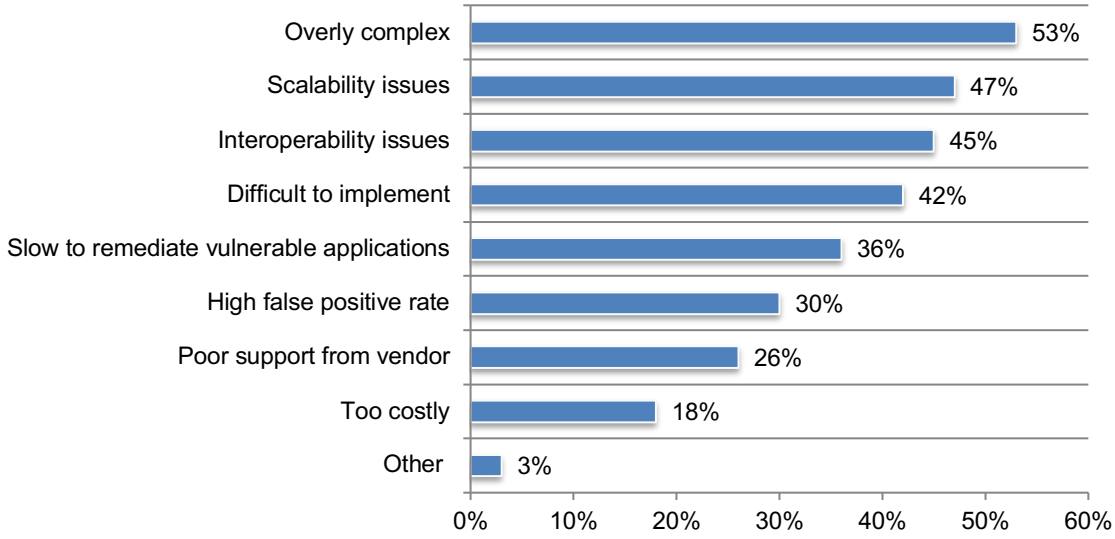
The inability to quickly detect vulnerabilities and threats is the number one reason vulnerabilities are difficult to remediate in applications. Sixty-one percent of respondents say it is very difficult or difficult to remediate vulnerabilities in applications. As shown in Figure 18, 55 percent of respondents say it is the inability to quickly detect vulnerabilities and threats and 49 percent of respondents say it is the inability to quickly perform patches on applications in production followed by the lack of enabling security tools (43 percent of respondents).

Figure 18. Why is it difficult to remediate vulnerabilities in applications?
More than one response permitted



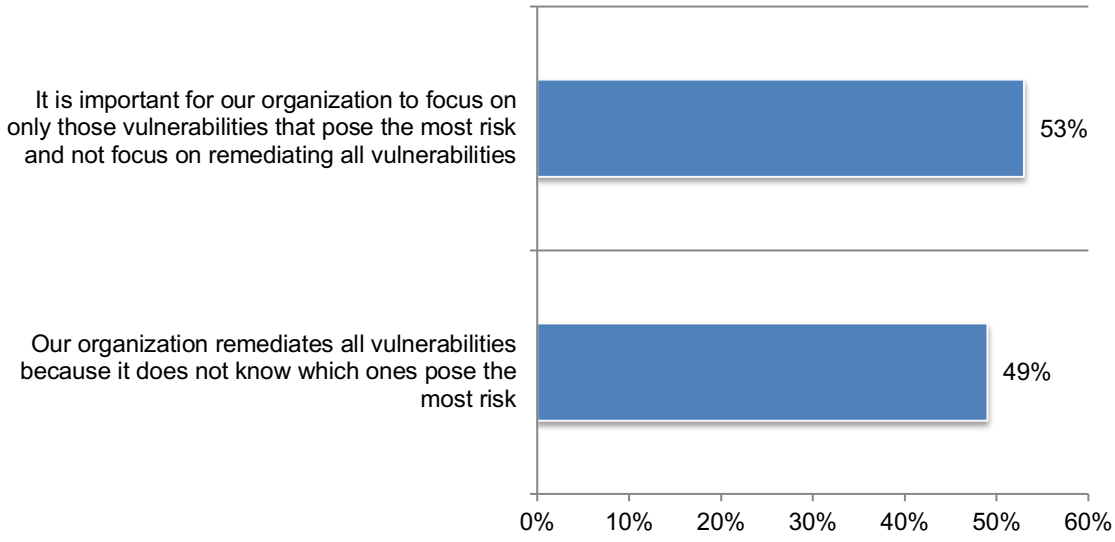
Current solutions used to remediate vulnerabilities in applications are too complex. Figure 19 lists pain points in current technologies used to remediate vulnerabilities. As shown, 53 percent of respondents say they are overly complex, 47 percent say it is scalability and 45 percent say it is interoperability issues.

Figure 19. What are the primary pain points with current solutions used to remediate vulnerabilities in applications?
Three responses permitted



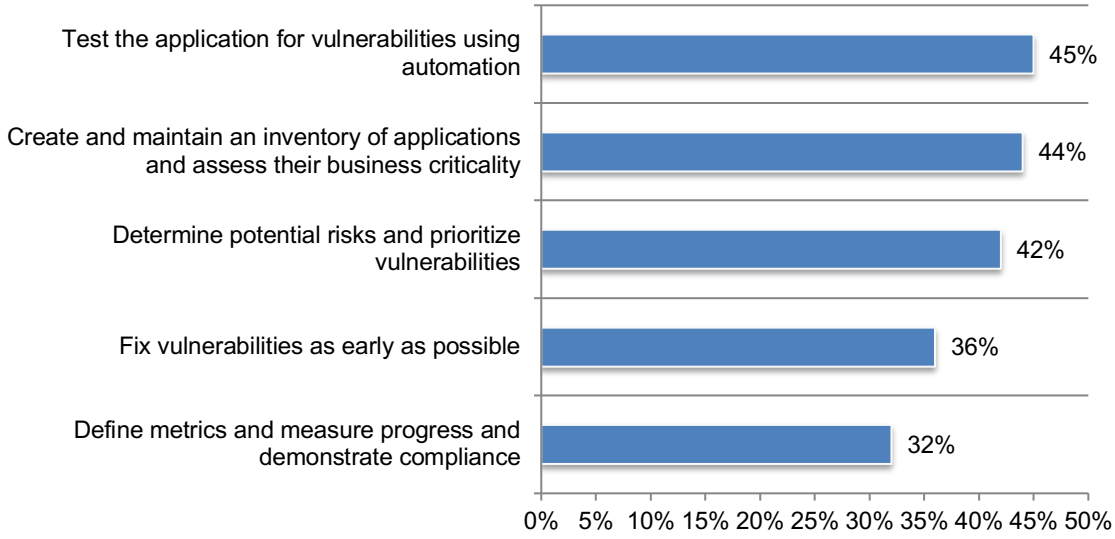
More than half of organizations focus only on those vulnerabilities that pose the most risk. According to Figure 20, 53 percent of respondents believe it is important to focus on only those vulnerabilities that pose the most risk and not on remediating all vulnerabilities. Forty-nine percent of respondents say their organization remediates all vulnerabilities because it does not know which ones pose the most risk.

Figure 20. Perceptions on the remediation of vulnerabilities
Strongly agree and Agree responses combined



Testing applications and keeping an inventory of business-critical applications are steps that have been fully or partially implemented. As shown in Figure 21, to manage vulnerabilities 45 percent of respondents test the application for vulnerabilities using automation and 44 percent of respondents say their organizations have created and maintained an inventory of applications and assess their business criticality.

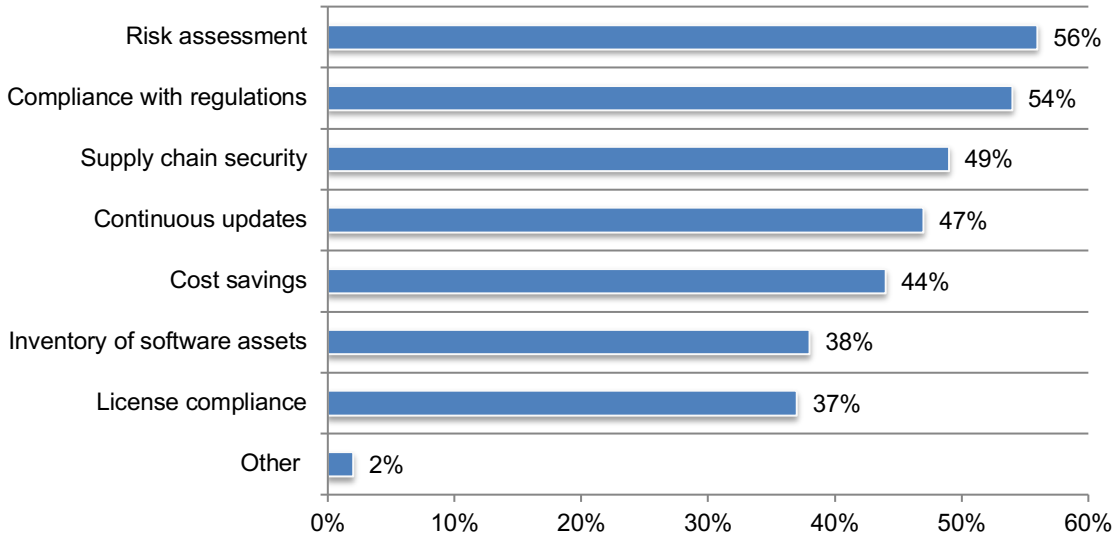
Figure 21. Fully or partially implemented steps taken to manage application security risks
Fully implemented and Partially implemented responses combined



Software Bill of Materials (SBOM) is a list of components in a piece of software. Software vendors often create products by assembling open source and commercial components. The SBOM describes the components in the product. A dynamic SBOM is updated automatically whenever a release or change occurs. Forty-one percent of respondents say their organizations use SBOM.

Risk assessment and compliance with regulations are the top two features of these organizations' SBOMs, as shown in Figure 22. While 70 percent of respondents say continuous automatic updates are important or very important, only 47 percent say their SBOM features continuous updates.

Figure 22. Which of the following are features of your organization's SBOM
More than one response permitted

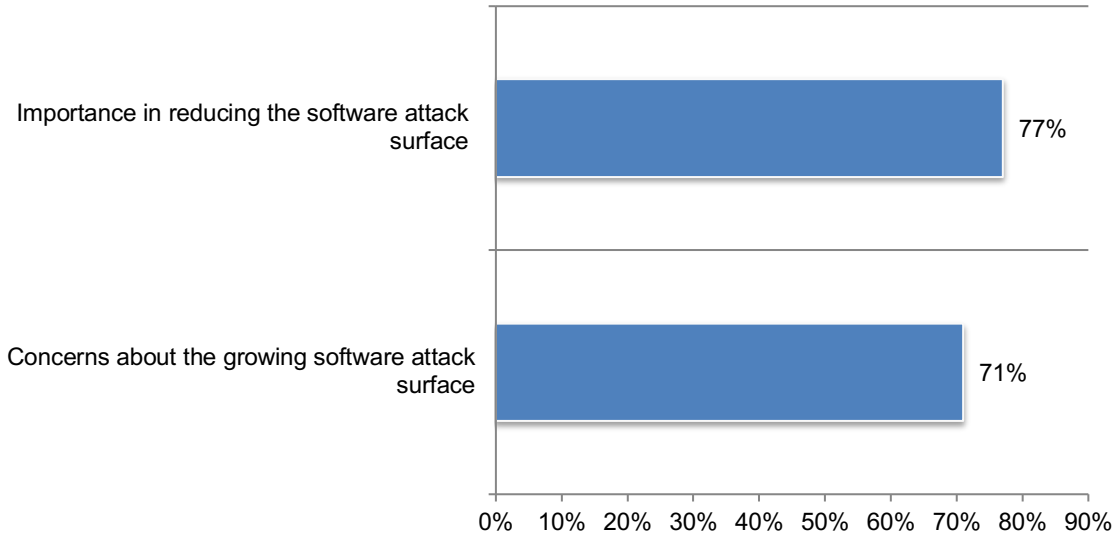


Minimizing risks in the software attack surface

The growing software attack surface is a high concern. Respondents were asked to rate their level of concern about the growing software attack surface from 1 = low concern to 10 = high concern as well as the importance of reducing the software attack surface from 1 = low importance to 10 = high importance. Figure 23 presents the 7+ responses on the 10-point scale. Seventy-one percent of respondents say their organizations are very or highly concerned about risks created by the growing software attack surface. A higher percentage of respondents (77 percent) believe it is very or highly important.

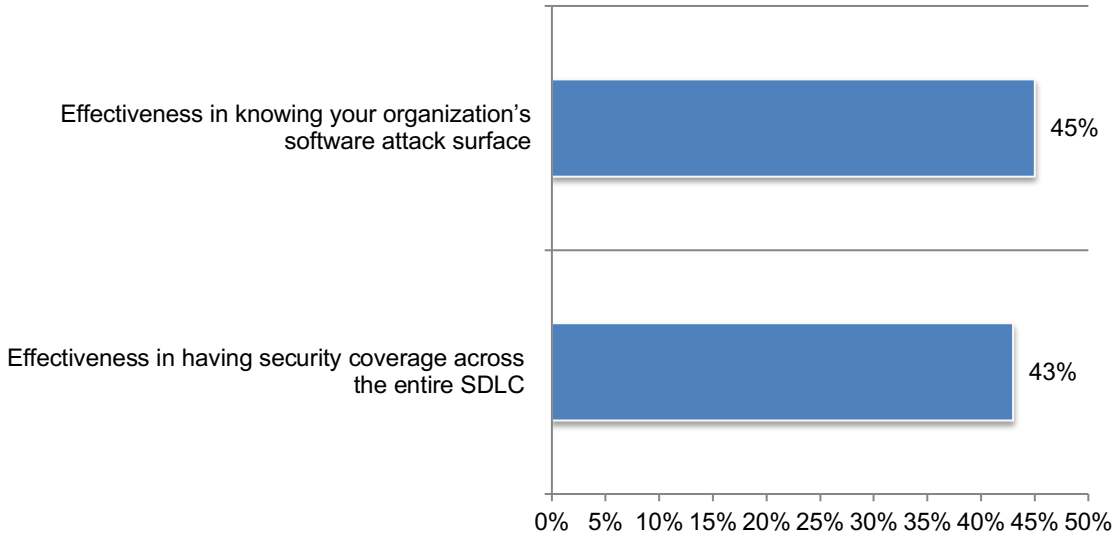
Figure 23. Concern about the growing software attack surface and importance in reducing the software attack surface

On a scale from 1 = low concern/low importance to 10 = high concern/high importance, 7+ responses presented



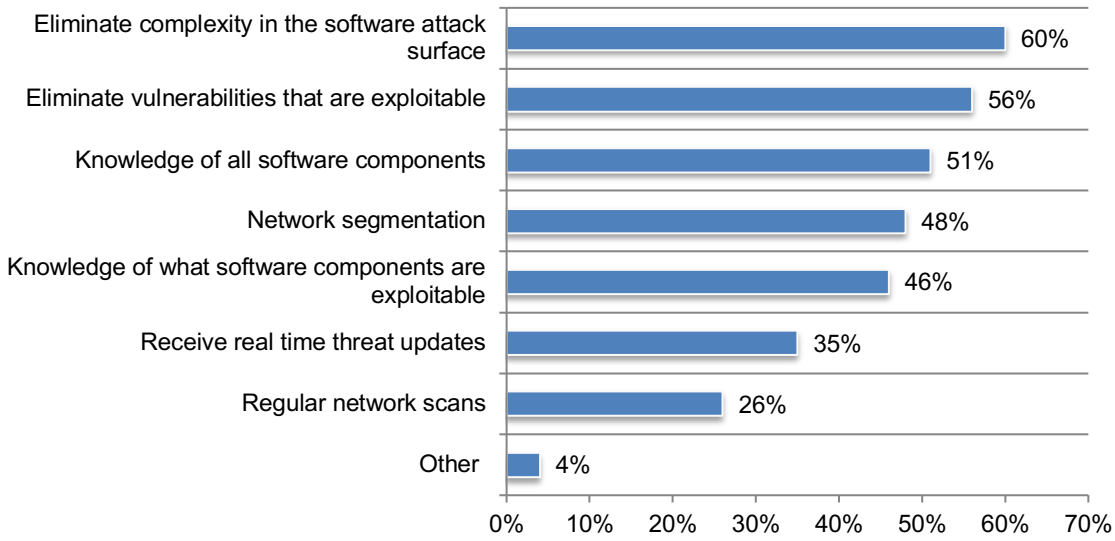
Despite the concerns, most organizations are not effective in both knowing the attack surface and securing it. Respondents were asked to rate their level of effectiveness in having security across the entire SDLC and knowing their organization's attack surface from 1 = low effectiveness to 10 = high effectiveness. Figure 24 presents the 7+ responses on the 10-point scale. Only 43 percent of respondents say their organizations' effectiveness is very high and only 45 percent of respondents say their organizations are effective in knowing the attack surface.

Figure 24. Effectiveness in securing the SDLC and knowing the software attack surface
On a scale from 1 = low effectiveness to 10 = high effectiveness, 7+ responses presented



Elimination of complexity and eliminate vulnerabilities that are exploitable are the most important steps to safeguard the attack surface. As shown in Figure 25, 60 percent of respondents say the elimination of complexity in the software attack surface vulnerabilities that are exploitable (56 percent of respondents) will reduce threats to the attack surface. This is followed by knowledge of all software components (51 percent of respondents). Only 26 percent of respondents say regular network scans reduce threats.

Figure 25. The most important steps to reduce threats to the software attack surface
More than one response permitted



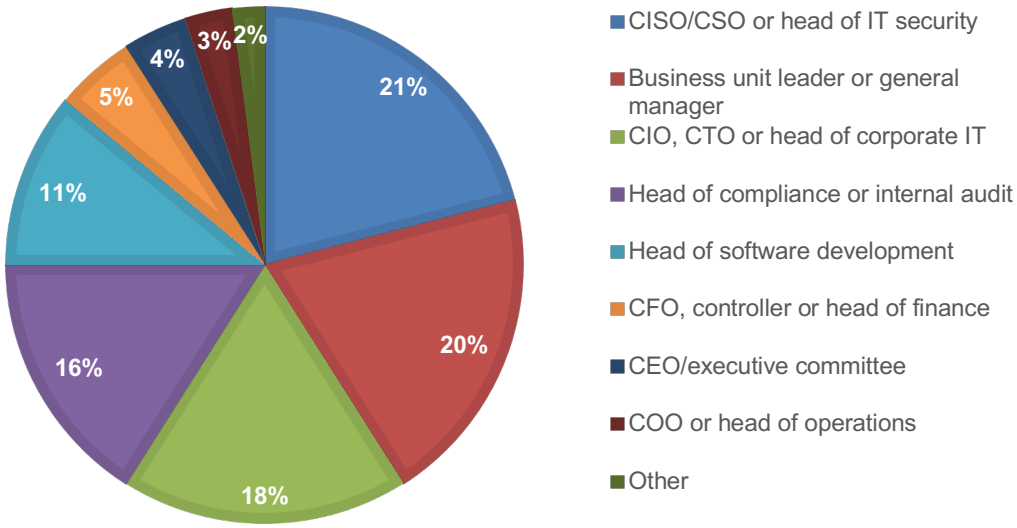
Part 3. Methodology

A sampling frame of 16,510 IT and IT security practitioners who are knowledgeable about their organizations' attack surface and effectiveness in managing vulnerabilities were selected as participants to this survey. Table 1 shows 698 total returns. Screening and reliability checks required the removal of 64 surveys. Our final sample consisted of 634 surveys or a 3.8 percent response.

Table 1. Sample response	Freq	Pct%
Sampling frame	16,510	100.0%
Total returns	698	4.2%
Rejected or screened surveys	64	0.4%
Final sample	634	3.8%

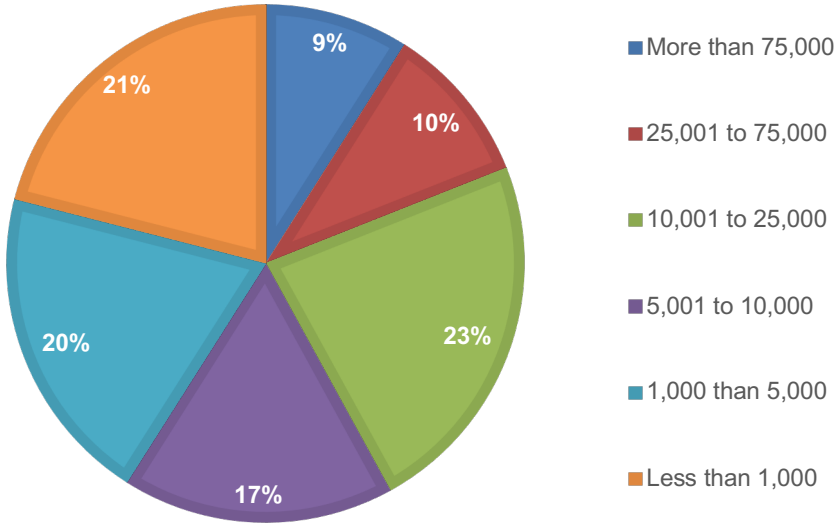
Pie chart 1 reports the respondent's direct reporting channel. Twenty-one percent of respondents report directly to the CISO/CSO or head of IT security, 20 percent of respondents report to the business unit leader or general manager, 18 percent of respondents report to the CIO, CTO or head of corporate IT, and 16 percent of respondents report to the head of compliance or internal audit.

Pie chart 1. Direct reporting channel



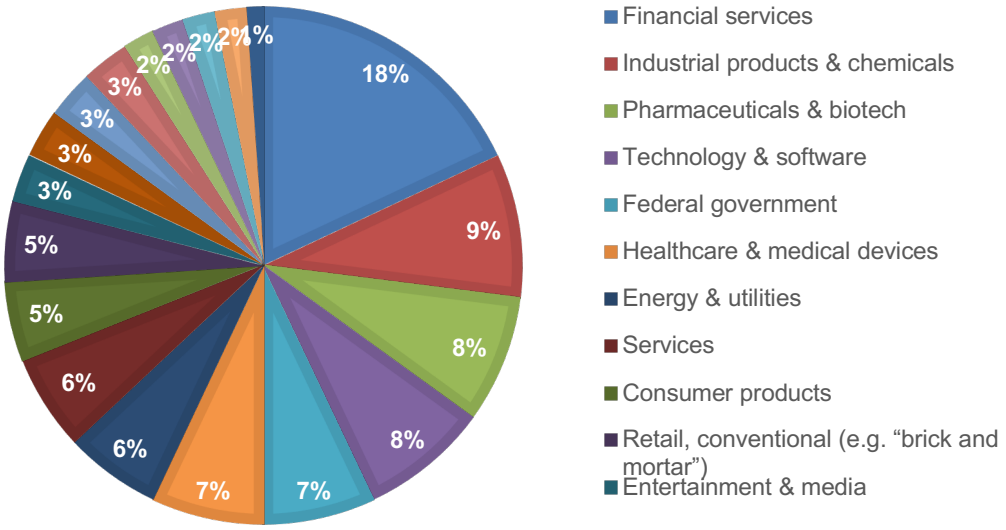
As shown in Pie chart 2, 59 percent of respondents are from organizations with a global headcount of more than 5,000 employees.

Pie chart 2. Global full-time headcount



Pie chart 3 reports the industry focus of respondents' organizations. This chart identifies financial services (18 percent) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by industrial products and chemicals (9 percent of respondents), pharmaceuticals and biotech (8 percent of respondents), technology and software (8 percent of respondents), federal government (7 percent of respondents) and healthcare and medical devices (7 percent of respondents).

Pie chart 3. Primary industry focus



Part 4. 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.

- 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.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of IT or IT security professionals. 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.

- 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.

Part 5. Appendix with the detailed audited findings

The following tables provide the percentage frequency of responses to all survey questions. All survey responses were captured in July 2022.

Survey response	Freq
Total sampling frame	16,510
Total survey returns	698
Rejected survey	64
Final sample	634
Response rate	3.8%

S1. What best defines your level of knowledge about the software attack surface and vulnerability management?	Pct%
Very knowledgeable	37%
Knowledgeable	44%
Somewhat knowledgeable	19%
No knowledge (stop)	0%
Total	100%

S2. Has your organization adopted a DevSecOps approach or is it in the process of adopting a DevSecOps approach as defined above?	Pct%
Yes	100%
No (stop)	0%
Total	100%

S3. Which of the following activities do you do? Please select all that apply.	Pct%
Detect vulnerabilities	47%
Ensure compliance	43%
Implement security technologies	53%
Prioritize vulnerability	62%
Resolve vulnerabilities	58%
Secure applications and data	53%
Supply chain security	60%
Test applications	49%
Write secure code (developer)	55%
None of the above (stop)	0%
Total	480%

S4. Please select the **one** job title that best describes your role or function in IT/ IT security.	Pct%
Chief Information Officer (CIO)	11%
Chief Information Security Officer (CISO)	15%
Chief Security Architect	4%
Chief Security Officer (CSO)	6%
Compliance/legal	5%
DevSecOps team	15%
Director/manager IT	11%
Director/manager IT security	8%
Security engineering	12%
Security Operations Center (SOC)	8%
Security Products Testing	5%
None of the above (stop)	0%
Total	100%

Part 2. Attributions about DevSecOps and DevOps

Please rate each statement using the following scale: **Strongly Agree and Agree response**	Strongly Agree or Agree response
Q1a. Our development team is able to deliver both an enhanced customer experience and secure applications.	47%
Q1b. I am concerned that the lack of visibility and prioritization in DevOps security practices puts product security at risk.	53%
Q1c. Development engineers, product security teams and compliance teams are aligned to understand our organization's security posture and each other's area of responsibilities to deliver secure products.	55%

Part 3. Background on DevSecOps and DevOpsQ2a. Do you have any involvement in your organization's DevOps activities?	Pct%
Yes	51%
No (please skip to Q3)	49%
Total	100%

Q2b. If yes, how are you involved? Please select all that apply.	Pct%
Compliance	37%
In application security	49%
In development	42%
In production	45%
Vulnerability management	52%
Other (please specify)	7%
Total	232%

Q3. What best describes the maturity of your DevSecOps?	Pct%
Early stage—The organization is just starting to plan its DevSecOps approach	31%
Middle stage—The organization has planned and defined its DevSecOps approach and is beginning to integrate security at every phase of the software development lifecycle	40%
Mature stage—DevOps has been fully transitioned into DevSecOps and security is integrated at every phase of the software development lifecycle	29%
Total	100%

Q4. What are the primary reasons your organization is adopting or has adopted DevSecOps? Please select the top **four** reasons.	Pct%
Ability to address security issues as they emerge	30%
Security issues are less expensive to fix	32%
To automate the delivery of secure software without slowing the software development cycle	41%
To eliminate duplicative review and unnecessary rebuilds	40%
To have a centralized approach to code review	39%
To have a focused approach to prioritization and remediation of risks	33%
To improve the collaboration between development, security and operations	45%
To limit the time a threat actor has to take advantage of vulnerabilities in public-facing production systems	32%
To reduce the cost and time to fix the code	40%
To reduce the time to patch vulnerabilities	45%
To reduce the vulnerability backlog	19%
Other (please specify)	4%
Total	400%

Q5. What are the challenges or pain points to having a fully effective DevSecOps? Please select your top **four** challenges.	Pct%
Growing vulnerability backlog	52%
Growth in application security vulnerabilities	43%
Insufficient budget (money)	36%
Lack of automation	27%
Lack of clear leadership	17%
Lack of effective security tools	54%
Lack of effective testing tools	32%
Lack of in-house expertise	18%
Lack of security training	27%
Lack of workflow integration	53%
Management underestimates risk of insecure applications	12%
Not considered an organizational priority	11%
Pressure to release new products quickly	15%
Other (please specify)	3%
Total	400%

Q6a. Has your organization adopted a **shift left strategy**?	Pct%
Yes	52%
No (please skip to Q8)	48%
Total	100%

Q6b. If yes, what are the challenges a shift left strategy poses to the ability to create innovative applications or services? Please select all that apply.	Pct%
An increase in work for developers	43%
A lack of integrated security tools	51%
Too many vulnerabilities to fix	40%
Other (please specify)	4%
Total	138%

Q7a. Has your organization adopted a **shift right strategy**?	Pct%
Yes	47%
No (please skip to Q8)	53%
Total	100%

Q7b. If yes, the benefit of a shift right strategy is that it empowers engineers to test more, test on time and test late.	Pct%
Strongly agree	23%
Agree	28%
Unsure	11%
Disagree	24%
Strongly disagree	14%
Total	100%

Part 4. SDLC and vulnerability management

Q8. Using the following 10-point scale, please rate the importance of the following features in creating secure applications or services. 1 = not important to 10 = very important.

Q8a. Having the ability to perform tests as part of the workflow instead of stopping, testing, fixing and restarting development.	Pct%
1 to 2	7%
3 to 4	15%
5 to 6	13%
7 to 8	33%
9 to 10	32%
Total	100%
Extrapolated value	6.86

Q8b. Automating vulnerability scanning and remediation at every stage of the SDLC.	Pct%
1 to 2	12%
3 to 4	15%
5 to 6	12%
7 to 8	30%
9 to 10	31%
Total	100%
Extrapolated value	6.56

Q9. Using the following 10-point scale, please rate your organization's effectiveness in prioritizing the most critical vulnerabilities from 1= low effectiveness to 10 = high effectiveness.	Pct%
1 to 2	10%
3 to 4	17%
5 to 6	21%
7 to 8	23%
9 to 10	29%
Total	100%
Extrapolated value	6.38

Q10. Using the following 10-point scale, please rate your organization's effectiveness in patching vulnerabilities in a timely manner from 1 = low effectiveness to 10 = high effectiveness.	Pct%
1 to 2	21%
3 to 4	15%
5 to 6	21%
7 to 8	30%
9 to 10	13%
Total	100%
Extrapolated values	5.48

Q11. How much time does your team spend weekly on the following vulnerability management activities? Please ensure the allocation sums to 100 percent	Points
Detecting vulnerabilities	25
Prioritizing vulnerabilities	35
Remediating vulnerabilities	40
Total percentage of time (100 points)	100

Q12a. On average, how much time does it take to **detect** one vulnerability in **development**?	Pct%
Less than 5 minutes	4%
5 minutes to 10 minutes	10%
11 minutes to 15 minutes	15%
16 minutes to 20 minutes	22%
21 minutes to 30 minutes	23%
More than 30 minutes	26%
Total	100%
Extrapolated values	23.1

Q12b. On average, how much time does it take to **detect** one vulnerability in **production**?	Pct%
Less than 5 minutes	5%
5 minutes to 10 minutes	2%
11 minutes to 15 minutes	8%
16 minutes to 20 minutes	8%
21 minutes to 30 minutes	30%
More than 30 minutes	47%
Total	100%
Extrapolated values	29.3

Q13a. On average, how much time does it take to **prioritize** one vulnerability in **development**?	Pct%
Less than 5 minutes	3%
5 minutes to 10 minutes	4%
11 minutes to 15 minutes	8%
16 minutes to 20 minutes	22%
21 minutes to 30 minutes	23%
More than 30 minutes	40%
Total	100%
Extrapolated values	27.3

Q13b. On average, how much time does it take to **prioritize** one vulnerability in **production**?	Pct%
Less than 5 minutes	4%
5 minutes to 10 minutes	5%
11 minutes to 15 minutes	6%
16 minutes to 20 minutes	8%
21 minutes to 30 minutes	41%
More than 30 minutes	36%
Total	100%
Extrapolated values	27.6

Q14a. On average, how much time does it take to **remediate** one vulnerability in **development**?	Pct%
Less than 5 minutes	0%
5 minutes to 10 minutes	1%
11 minutes to 15 minutes	5%
16 minutes to 20 minutes	12%
21 minutes to 30 minutes	45%
More than 30 minutes	37%
Total	100%
Extrapolated values	29.2

Q14b. On average, how much time does it take to **remediate** one vulnerability in **production**?	Pct%
Less than 5 minutes	5%
5 minutes to 10 minutes	2%
11 minutes to 15 minutes	8%
16 minutes to 20 minutes	8%
21 minutes to 30 minutes	32%
More than 30 minutes	45%
Total	100%
Extrapolated values	29.0

Q15. Does your organization consider its infrastructure critical?	Pct%
Yes	63%
No (please skip to Q19)	37%
Total	100%

Q16a. On average, how much time does it take to **detect** one vulnerability by **IT/infrastructure engineers**?	Pct%
Less than 5 minutes	25%
5 minutes to 10 minutes	32%
11 minutes to 15 minutes	8%
16 minutes to 20 minutes	6%
21 minutes to 30 minutes	10%
More than 30 minutes	19%
Total	100%
Extrapolated value	15.7

Q16b. On average, how much time does it take to **detect** one vulnerability by **vulnerability management teams**?	Pct%
Less than 5 minutes	32%
5 minutes to 10 minutes	33%
11 minutes to 15 minutes	15%
16 minutes to 20 minutes	9%
21 minutes to 30 minutes	6%
More than 30 minutes	5%
Total	100%
Extrapolated value	10.9

Q17a. On average, how much time does it take to **prioritize** one vulnerability by **IT/infrastructure engineers**?	Pct%
Less than 5 minutes	4%
5 minutes to 10 minutes	10%
11 minutes to 15 minutes	15%
16 minutes to 20 minutes	22%
21 minutes to 30 minutes	23%
More than 30 minutes	26%
Total	100%
Extrapolated value	23.1

Q17b. On average, how much time does it take to **prioritize** one vulnerability by **vulnerability management teams**?	Pct%
Less than 5 minutes	32%
5 minutes to 10 minutes	24%
11 minutes to 15 minutes	20%
16 minutes to 20 minutes	12%
21 minutes to 30 minutes	3%
More than 30 minutes	9%
Total	100%
Extrapolated value	12.2

Q18a. On average, how much time does it take to **remediate** one vulnerability by **IT/infrastructure engineers**?	Pct%
Less than 5 minutes	21%
5 minutes to 10 minutes	39%
11 minutes to 15 minutes	21%
16 minutes to 20 minutes	8%
21 minutes to 30 minutes	6%
More than 30 minutes	5%
Total	100%
Extrapolated value	11.5

Q18b. On average, how much time does it take to **remediate** one vulnerability by **vulnerability management teams**?	Pct%
Less than 5 minutes5 minutes to 10 minutes	24%
11 minutes to 15 minutes	33%
16 minutes to 20 minutes	21%
21 minutes to 30 minutes	10%
More than 30 minutes	5%
Total	7%
Extrapolated value	100%
	12.0
Q19. Once you detect a **critical or high-risk** vulnerability in your environment, on average how long does it take to patch?	Pct%
Immediately	1%
1 week	3%
2 weeks	6%
3 weeks	7%
4 weeks	10%
5 weeks	11%
6 weeks	14%
7 weeks	16%
8 weeks	15%
9 weeks	13%
More than 9 weeks	4%
Total	100%
Extrapolated value (weeks)	6.08

Q20a. Does your organization use automation to assist with vulnerability management?	Pct%
Yes	56%
No (please skip to Q22)	44%
Total	100%

Q20b. If yes, what steps do you automate? Please select all that apply.	Pct%
Prioritization	47%
Patching	59%
Reporting	41%
Other (please specify)	3%
Total	150%

Q20c. If yes, how has automation impacted the time it takes to remediate vulnerabilities?	Pct%
Significantly shorter time to respond	43%
Slightly shorter time to respond	17%
No change in time to respond	22%
Increase in time to respond	18%
Total	100%

Q22. What is your primary method for prioritizing vulnerabilities? Please select **one** choice.	Pct%
Common Vulnerability Scoring System (CVSS) security score of the vulnerability	30%
Identification of which vulnerabilities are weaponized and being exploited by attackers	21%
Which exposed assets are the most important to the business	23%
A proprietary scoring metric	23%
Other (please specify)	3%
Total	100%

Q23. Which factors below cause major delays in your vulnerability patching process? Please select all that apply.	Pct%
Human error	32%
My organization has no tolerance for the downtime required for patching	28%
Silo and turf issues	45%
We can't easily track whether vulnerabilities are being patched in a timely manner	51%
We can't take critical applications and systems off-line so we can patch them quickly	49%
We do not think an attacker will exploit our vulnerabilities	37%
We don't have a common view of applications and assets across security and IT teams	45%
We don't have enough resources to keep up with the volume of patches	43%
We don't have the ability to hold IT or other departments accountable for patching	36%
We use emails and spreadsheets to manage the process, so things slip between the cracks	29%
Other (please specify)	3%
Total	398%

Part 5. Application security risk

Q24a. How difficult is it to remediate vulnerabilities in applications? Please select one best choice.	Pct%
Very difficult	36%
Difficult	25%
Somewhat difficult (please skip to Q25)	16%
Not difficult (please skip to Q25)	14%
Easy (please skip to Q25)	9%
Total	100%

Q24b. [If very difficult or difficult] Why is it difficult to remediate vulnerabilities in applications? Please select all that apply.	Pct%
Inability to quickly detect vulnerabilities and threats	55%
Inability to quickly perform patches on applications in production	49%
Lack of enabling security tools	43%
Lack of qualified personnel	38%
Lack of resources	15%
Other (please specify)	5%
Total	205%

Q25. In the past 12 months, did your organization have a vulnerability backlog (i.e. applications that have been identified as vulnerable but not been remediated)?	Pct%
Yes	47%
No (please skip to Q27)	48%
Don't know (please skip to Q27)	5%
Total	100%

Q26a. In the past 12 months, what is the approximate number of individual vulnerabilities were in this backlog?	Pct%
Less than 10,000	3%
10,001 to 40,000	7%
40,001 to 60,000	10%
60,001 to 100,000	14%
100,001 to 250,000	12%
250,001 to 500,000	16%
500,001 to 1,00,000	13%
1,000,001 to 2,500,000	9%
2,500,001 to 5,000,000	8%
More than 5,000,000	8%
Total	100%
Extrapolated value	1,086,220

Q26b. In the past 12 months, on average, what percentage of these vulnerable applications were remediated?	Pct%
Less than 5%	4%
5 to 10%	12%
11 to 25%	17%
26 to 50%	21%
51 to 75%	25%
76 to 100%	21%
Total	100%
Extrapolated value	46%

Q26c. What percentage of these vulnerabilities in the backlog if remediated would be considered a success?	Pct%
Less than 5%	22%
5 to 10%	13%
11 to 25%	15%
26 to 50%	31%
51 to 75%	14%
76 to 100%	5%
Total	100%
Extrapolated value	29%

Q26d. In the past 12 months, how long did it take to remediate this backlog?	Pct%
Less than 1 week	5%
1 week to 2 weeks	17%
3 weeks to 4 weeks	23%
5 weeks to 6 weeks	29%
7 weeks to 8 weeks	13%
9 weeks to 10 weeks	6%
More than 10 weeks	7%
Total	100%
Extrapolated value (weeks)	5.02

Q26e. What were the challenges to remediating this vulnerability backlog? Please select all that apply.	Pct%
Inability to prioritize what needs to be fixed	47%
Lack of effective tools	43%
Lack of resources	38%
Not enough information about risks that would exploit vulnerabilities	45%
Too time-consuming	28%
Other (please specify)	3%
Total	204%

Q27. What are the primary pain points with current solutions used to remediate vulnerabilities in applications? Please select the top three pain points.	Pct%
Difficult to implement	42%
High false positive rate	30%
Interoperability issues	45%
Overly complex	53%
Poor support from vendor	26%
Scalability issues	47%
Slow to remediate vulnerable applications	36%
Too costly	18%
Other (please specify)	3%
Total	300%

Q28. Using the following 10-point scale, please rate how important is it for your organization to reduce its vulnerability backlog from 1 = not important to 10 = highly important.	Pct%
1 to 2	1%
3 to 4	13%
5 to 6	16%
7 to 8	23%
9 to 10	47%
Total	100%
Extrapolated values	7.54

Q29. It is important for our organization to focus on only those vulnerabilities that pose the most risk and not focus on remediating all vulnerabilities.	Pct%
Strongly agree	25%
Agree	28%
Unsure	15%
Disagree	18%
Strongly disagree	14%
Total	100%

Q30. Our organization remediates all vulnerabilities because it does not know which ones pose the most risk.	Pct%
Strongly agree	23%
Agree	26%
Unsure	18%
Disagree	14%
Strongly disagree	19%
Total	100%

Q31. Following are five strategically important steps for managing application security risk. Please indicate the extent to which your organization is doing each one. **Fully implemented and partially implemented combined response combined.**	Fully or partially implemented
Q31a. Create and maintain an inventory of applications and assess their business criticality.	44%
Q31b. Test the application for vulnerabilities using automation.	45%
Q31c. Determine potential risks and prioritize vulnerabilities.	42%
Q31d. Fix vulnerabilities as early as possible.	36%
Q31e. Define metrics and measure progress and demonstrate compliance.	32%

Q32. How familiar are you with Software Bill of Materials (SBOM) as defined above?	Pct%
Very familiar	32%
Familiar	34%
Somewhat familiar	19%
Not familiar (please skip to Q34)	15%
Total	100%

Q33. Has your organization adopted the use of SBOM?	Pct%
Yes	41%
No (please skip to Q34)	59%
Total	100%

Q34. Using the following 10-point scale, please rate the importance of continuous automatic updates from 1 = low importance to 10 = high importance.	Pct%
1 to 2	0%
3 to 4	16%
5 to 6	14%
7 to 8	24%
9 to 10	46%
Total	100%
Extrapolated values	7.50

Q35. Which of the following are the features of your organization's SBOM? Please select all that apply.	Pct%
Compliance with regulations	54%
Continuous updates	47%
Cost savings	44%
Inventory of software assets	38%
License compliance	37%
Risk assessment	56%
Supply chain security	49%
Other (please specify)	2%
Total	327%

Q36. Using the following 10-point scale, please rate your organization's concern about the growing software attack surface from 1 = low concern to 10 = high concern.	Pct%
1 to 2	3%
3 to 4	10%
5 to 6	16%
7 to 8	32%
9 to 10	39%
Total	100%
Extrapolated value	7.38

Q37. Using the following 10-point scale, please rate your organization's effectiveness in having security coverage across the entire SDLC from 1 = low effectiveness to 10 = high effectiveness.	Pct%
1 to 2	22%
3 to 4	18%
5 to 6	17%
7 to 8	25%
9 to 10	18%
Total	100%
Extrapolated value\	5.48

Q38. Using the following 10-point scale, please rate your organization's effectiveness in knowing your organization's software attack surface from 1 = low effectiveness to 10 = high effectiveness.	Pct%
1 to 2	24%
3 to 4	21%
5 to 6	10%
7 to 8	25%
9 to 10	20%
Total	100%
Extrapolated value	5.42

Q39. Using the following 10-point scale, please rate the importance in reducing the software attack surface from 1 = low importance to 10 = high importance.	Pct%
1 to 2	5%
3 to 4	6%
5 to 6	12%
7 to 8	34%
9 to 10	43%
Total	100%
Extrapolated value	7.58

Q40. What are the most important steps to reduce threats to your organization's software attack surface? Please select all that apply.	Pct%
Eliminate complexity in the software attack surface	60%
Eliminate vulnerabilities that are exploitable	56%
Knowledge of all software components	51%
Knowledge of what software components are exploitable	46%
Network segmentation	48%
Receive real time threat updates	35%
Regular network scans	26%
Other (please specify)	4%
Total	326%

Part 6. Organization and respondents' demographics

D1. What best describes your direct reporting channel?	Pct%
CEO/executive committee	4%
COO or head of operations	3%
CFO, controller or head of finance	5%
CIO, CTO or head of corporate IT	18%
Head of software development	11%
Business unit leader or general manager	20%
Head of compliance or internal audit	16%
CISO/CSO or head of IT security	21%
Other	2%
Total	100%

D2. What range best describes the full-time headcount of your global organization?	Pct%
Less than 1,000	21%
1,000 than 5,000	20%
5,001 to 10,000	17%
10,001 to 25,000	23%
25,001 to 75,000	10%
More than 75,000	9%
Total	100%

D3. What best describes your organization's primary industry classification?	Pct%
Communications	2%
Consumer products	5%
Defense contractor	1%
Education & research	2%
Energy & utilities	6%
Entertainment & media	3%
Federal government	7%
Financial services	18%
Healthcare & medical devices	7%
Hospitality	2%
Industrial products & chemicals	9%
Pharmaceuticals & biotech	8%
Professional services	3%
Retail, conventional (e.g. "brick and mortar")	5%
Retail, Internet	3%
Services	6%
State & local government	3%
Technology & software	8%
Transportation	2%
Other (please specify)	0%
Total	100%

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.