Enterprise Strategy Group by TechTarget

RESEARCH INSIGHTS

Optimizing Application Security Effectiveness

Best Practices to Secure and Protect Modern Software Applications

Melinda Marks, Practice Director, Cybersecurity, Enterprise Strategy Group

October 2023

Contents

Executive Summary 3
Business Risk: A Growing Catalyst 5
The Need for Alignment Around Business Goals 6
Best Practices for Effective Programs 8
Embrace DevOps to Drive Agility and Ease the Pivot to DevSecOps 9
Use DevSecOps Tools and Processes to Automate Security Checks 10
Address Third-party and/or Open Source Software 12
Centralize Security for Visibility and Control 13
Establish Security Collaboration Early in Development 15
Leverage SBOMs for Inventory and a Full Understanding of Code 18
Conclusion 20
How Mend Can Help 21
Research Methodology and Respondent Demographics/Firmographics 21

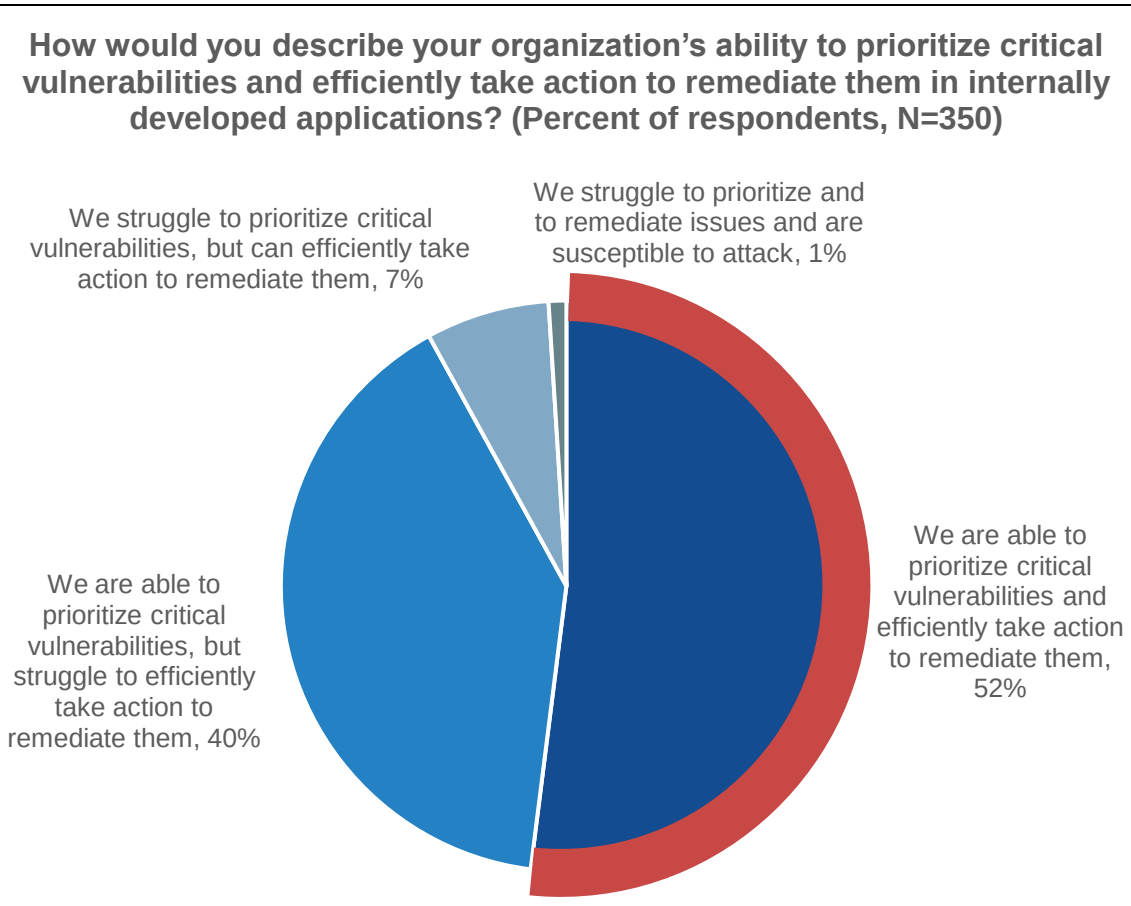
Executive Summary

Businesses are modernizing their software development processes to speed up software delivery and are rapidly scaling the utilization of cloud-native approaches with cloud services, including microservices-based architectures, continuous integration and delivery (CI/CD) pipelines, and increased usage of third-party code. But this activity also requires security teams to keep up with the increasing speed and volume of releases.

To gain insight into the state of security teams' ability to keep up with software development, TechTarget's Enterprise Strategy Group surveyed 350 application developers (27%) and senior security decision-makers (73%) with oversight and visibility into their organization's cybersecurity programs and associated business outcomes.

The results were concerning. Only 52% of companies say they can effectively remediate a critical vulnerability, and even fewer application security practitioners (44%) agree with that assessment.

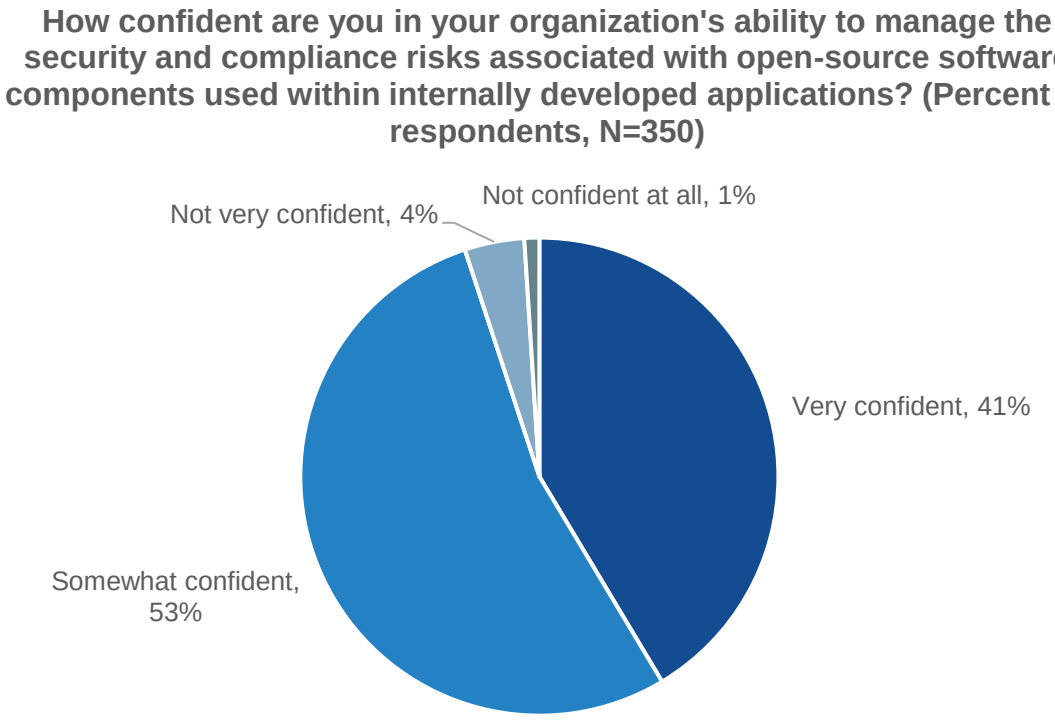
Figure 1. Ability to Prioritize and Efficiently Remediate Critical Vulnerabilities in Internally Developed Applications



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Similarly, just 41% of organizations are very confident in their ability to manage the security and compliance risks associated with open source software components used within internally developed applications. It's clear that security teams need a better way to scale to support the needs of development to drive better business results.

Figure 2. Confidence in Ability to Manage Security and Compliance Risks with Open Source Software Components



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Modern application security strategies must support and enable modern software development, even as it rapidly scales. But how is this best accomplished? The data shows that when security teams can collaborate and align with development to support their workflows and requirements, security teams can optimize their effectiveness to scale with development and, most importantly, mitigate risk to stay ahead of threats.

By analyzing the practices of those organizations that can effectively remediate critical vulnerabilities, we identified key patterns among the organizations that could efficiently remediate critical vulnerabilities as compared with those that could not. The research shows that the following tactics efficiently secure and protect applications and have had a measurable impact on program effectiveness:

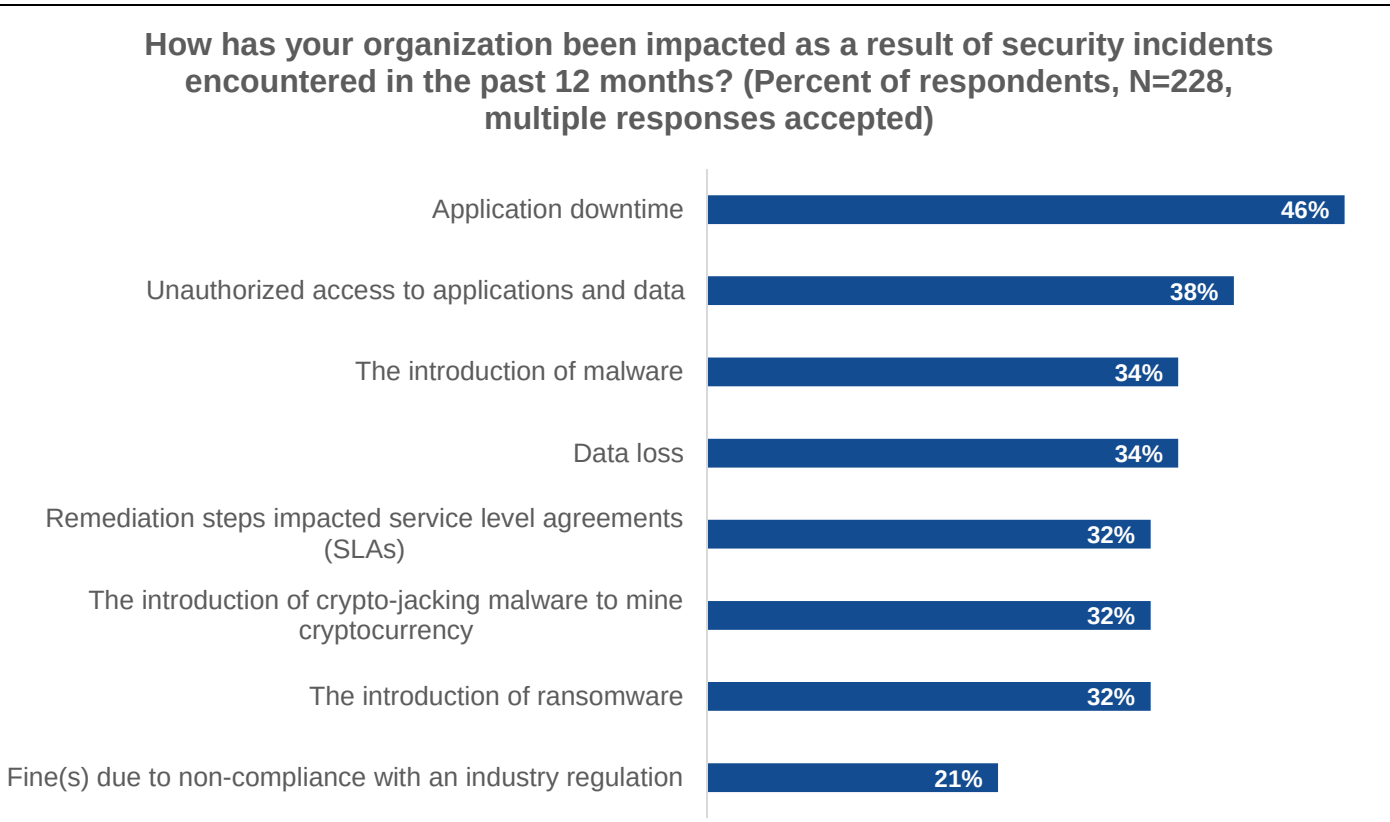
- **Effective programs have more fully embraced DevOps.** Organizations that report the ability to efficiently remediate vulnerabilities were more than twice as likely as organizations without the ability to remediate vulnerabilities to report they have extensively embraced DevOps (46% versus 20%).
- **Effective programs have more extensive DevSecOps adoption and automation of security workflows.** These organizations have automated the identification and remediation of configuration and software vulnerabilities before deployment to production more often (78% versus 61%).
- **Effective programs treat open source vulnerabilities with more urgency.** Organizations that report the ability to efficiently remediate vulnerabilities were more than twice as likely to report that they treat all open source vulnerabilities in their apps as a “must fix” (60% versus 28%).
- **Effective programs know what’s in their code.** Organizations able to efficiently remediate vulnerabilities were also more likely to say they view being able to answer questions about their code as critical, including:

- Where did code come from (49% versus 31%)?
- Who has access to code components (49% versus 33%)?
- Where is the code stored (45% versus 33%)?
- Can we document the composition of their code (OSS, third-party, 43% versus 23%)?

Business Risk: A Growing Catalyst

The potential consequences of a security incident pose increasing business risk, making application security a board-level priority for 85% of the survey respondents. Enterprise Strategy Group research indicates that 69% of organizations have directly encountered at least one serious security incident from a software vulnerability over the last 12 months. Furthermore, in the aggregate, organizations have experienced an average of three *serious* security incidents resulting from these types of vulnerabilities. Moreover, these incidents frequently lead to issues like application downtime, unauthorized data or application access, data loss, and malware infections.

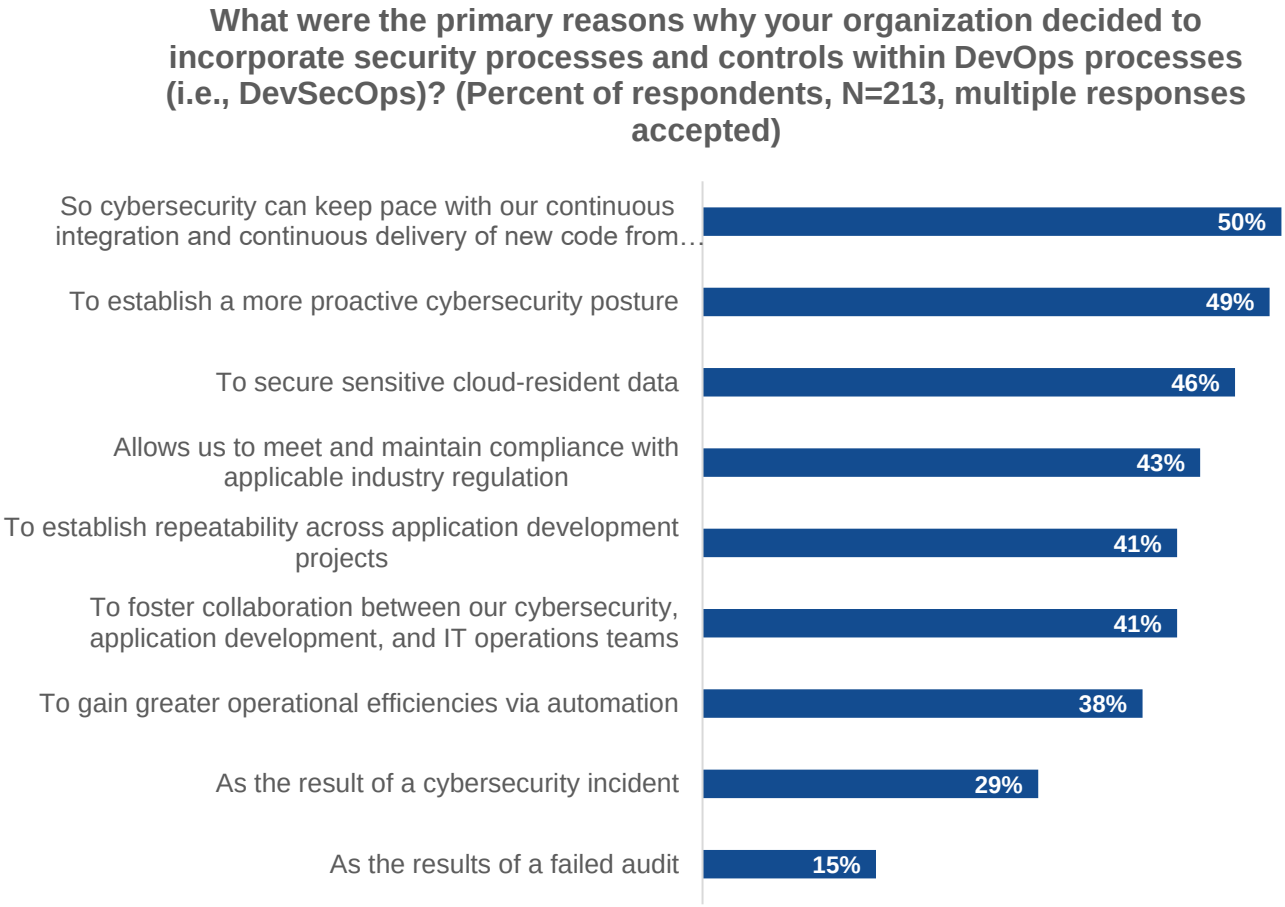
Figure 3. Impact of Security Incidents Encountered in the Past 12 Months



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

As a result, practices such as DevSecOps are growing in importance as companies look for ways to support the fast-paced CI/CD model, enhance their ability to proactively manage security risk, and reinforce the security of sensitive data in cloud environments. Just 4% of respondents reported their organization had yet to discuss how to implement security processes within DevOps.

Figure 4. Primary Reasons for DevSecOps Adoption

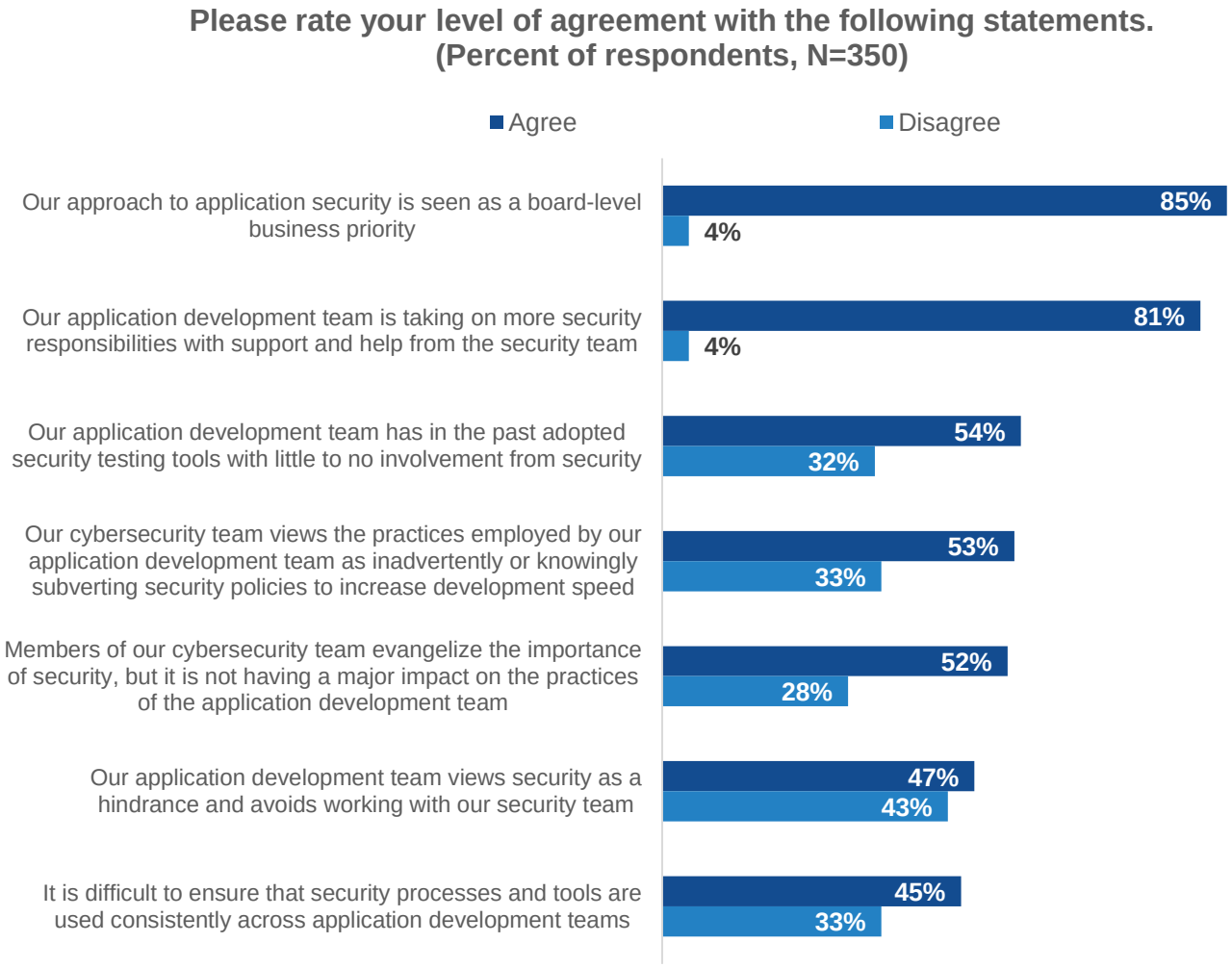


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The Need for Alignment Around Business Goals

While 85% of organizations said their approach to application security is seen as a board-level business priority, the research indicates challenges when security and development teams are not aligned. For example, 54% said the application teams have adopted security testing tools with little to no involvement from security, and 53% said the cybersecurity team feels the developers may subvert security policies in order to speed up development. There were discrepancies across teams in this area; IT and security professionals are 1.7x times more inclined to acknowledge that application developers occasionally bypass security policies in favor of accelerating development speed (60% versus 30%).

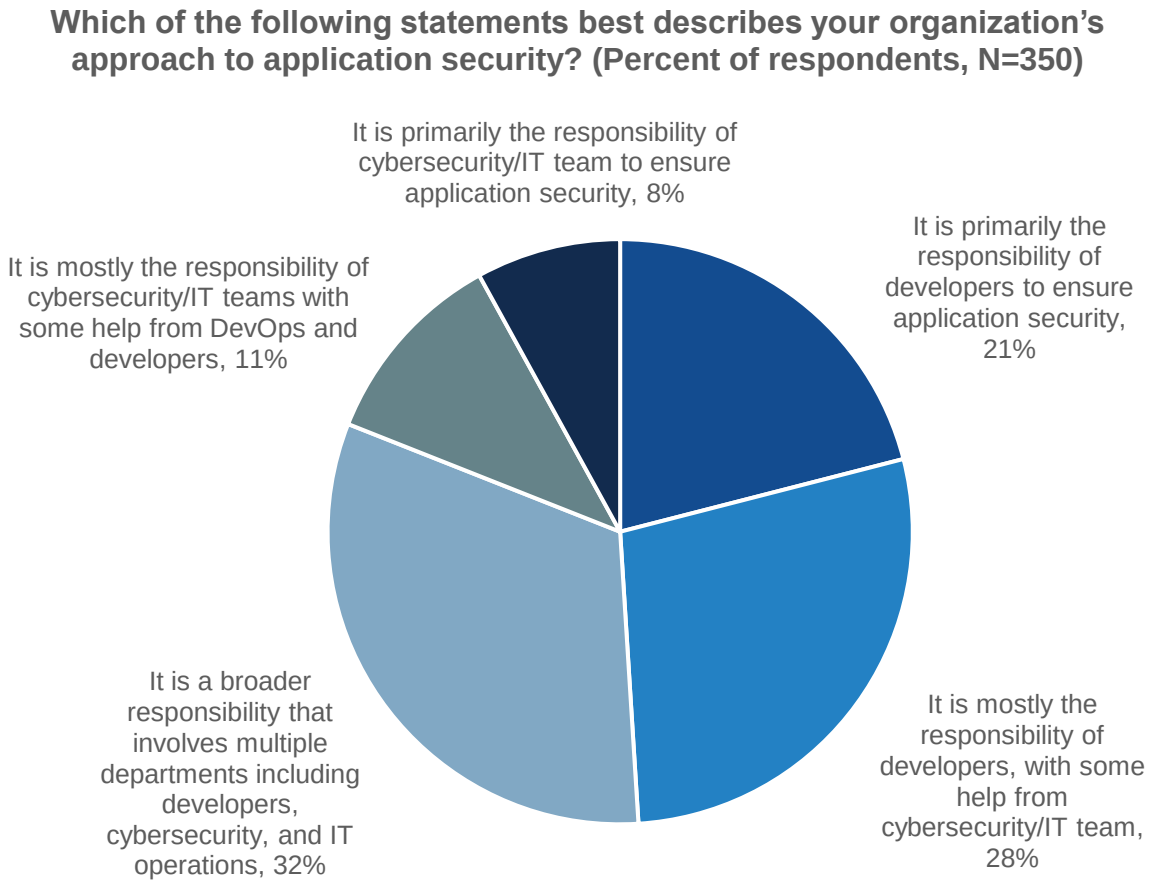
Figure 5. Level of Agreement With Statements Related to the Relationship Between Application Developers and Cybersecurity Teams



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

The research also revealed disconnects in understanding who has responsibility for cybersecurity. For nearly half of organizations (49%), developers are primarily or mostly responsible for application security, while 19% said it is mostly or primarily the responsibility of the cybersecurity or IT teams. It is worth noting that this perception is influenced by respondents' roles, as only 7% of the developers saw cybersecurity or IT teams as mostly or entirely responsible, while IT and security practitioners stated they were mostly or entirely responsible 23% of the time.

Figure 6. Organization's Approach to Application Security



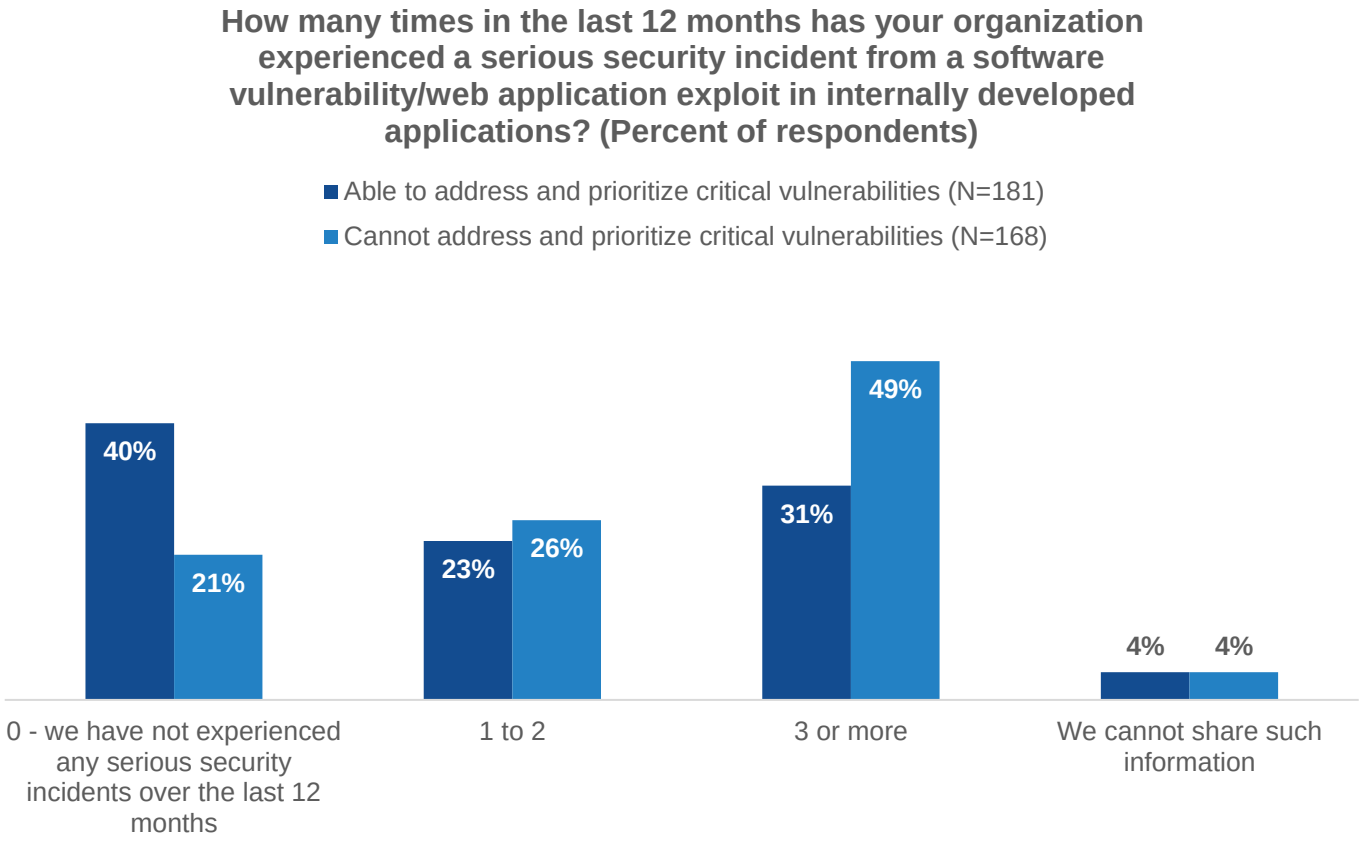
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Cybersecurity and IT teams and developers can address their application security challenges by collaborating to set common goals aligned with business needs, such as application uptime and availability, customer service, and protection of company and customer data. Teams should understand their respective responsibilities and establish goals with clear KPIs to focus their efforts, measure their effectiveness, and incrementally improve their programs.

Best Practices for Effective Programs

Let's start with the ultimate KPI for application security programs: lower security incident rates. Organizations that report the ability to efficiently remediate vulnerabilities were nearly twice as likely to say they have not experienced any serious security incidents tied to a software vulnerability/web application exploit in internally developed applications over the last 12 months.

Figure 7. Serious Security Incidents Experienced From a Software Vulnerability/Web Application Exploit in Internally Developed Applications



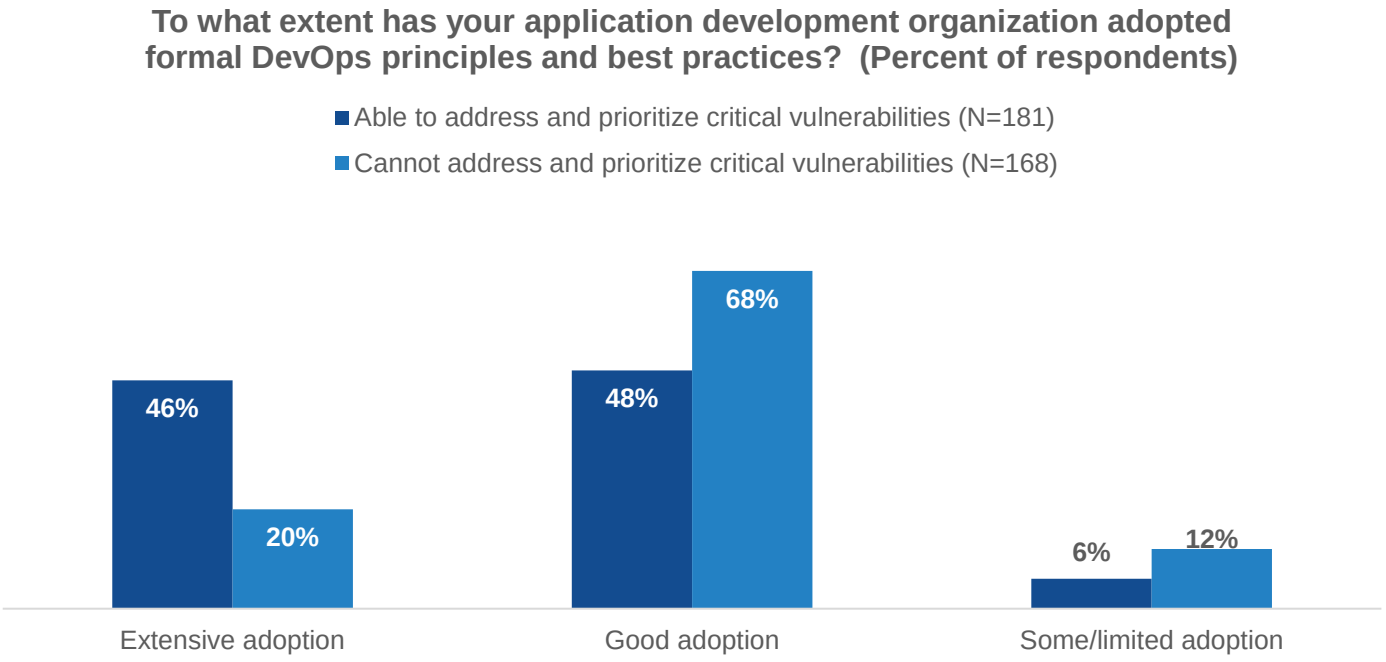
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

How did these companies achieve success? The research shows there are several best practices contributing to the success of highly effective application security programs. These best practices are examined in the remainder of this report. By adopting these tactics, organizations can measurably improve their security program effectiveness.

Embrace DevOps to Drive Agility and Ease the Pivot to DevSecOps

The research revealed that organizations that report the ability to efficiently remediate vulnerabilities were more than twice as likely to say they have extensively embraced DevOps (46% versus 20%). This may be from developers' and security teams' familiarity and experience with DevOps processes helping them address security efficiently, ideally incorporating security into developer tools and processes.

Figure 8. Adoption of Formal DevOps Principles and Best Practices by Application Development Teams

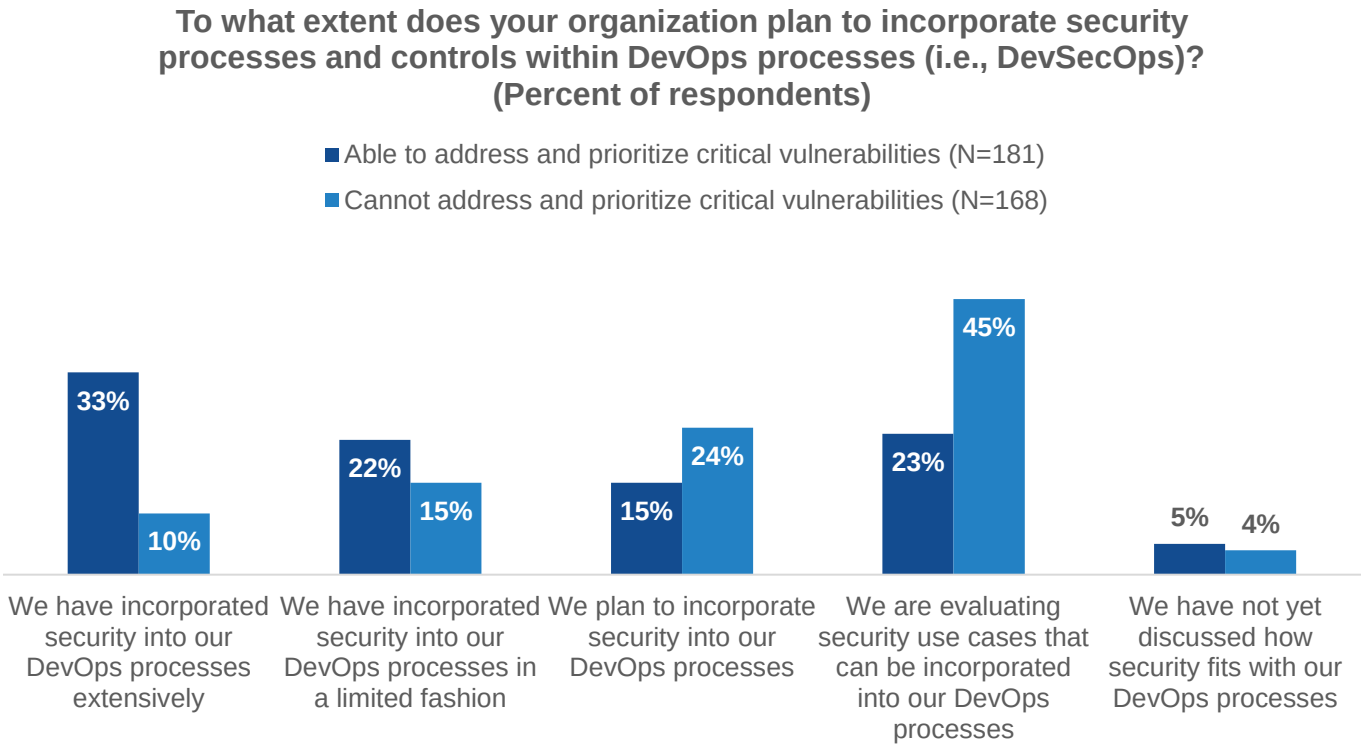


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Use DevSecOps Tools and Processes to Automate Security Checks

Similarly, the research shows that incorporating security processes into DevOps processes and developer workflows optimizes remediation efficiency. The organizations able to keep up with vulnerabilities are 3.3x more likely to report that they have extensively incorporated security into development processes (i.e., DevSecOps, 33% versus 10%).

Figure 9. The Extent to Which Organizations Plan to Incorporate Security Processes and Controls Within DevOps Processes (i.e., DevSecOps)

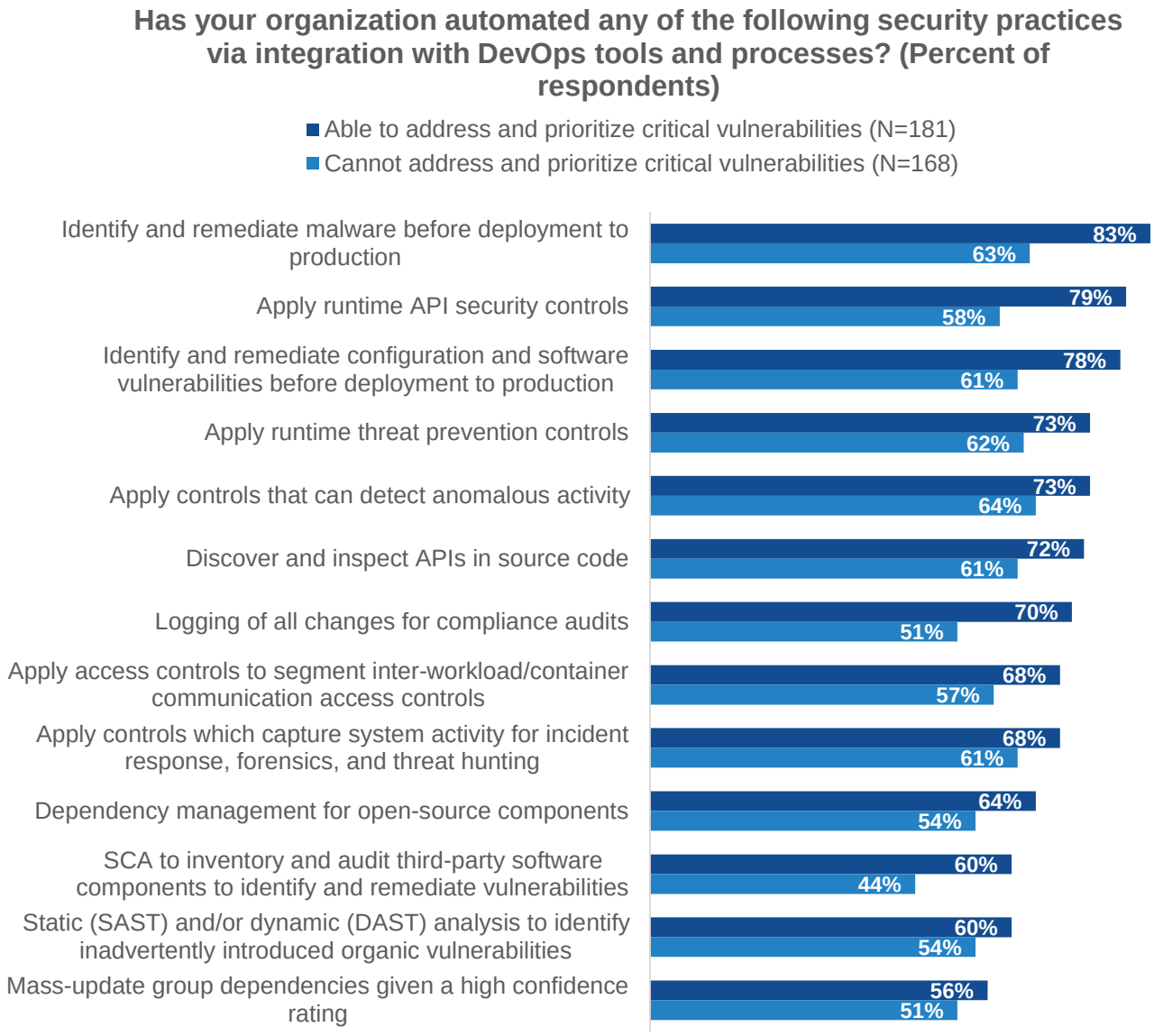


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

More specifically, these organizations do the following:

- Apply runtime API security controls (79% versus 58%).
- Automate the identification and remediation of configuration and software vulnerabilities before deployment to production more often (78% versus 61%).
- Discover and inspect APIs in source code (72% versus 61%).
- Apply runtime threat prevention controls (e.g., anti-malware, application control, virtual patching, intrusion prevention, 73% versus 62%).
- Log all changes for compliance audits (i.e., compliance-as-code, 70% versus 51%).
- Apply dependency management for open source components (64% versus 54%).
- Use software composition analysis (SCA) tools to inventory and audit third-party software components to identify and remediate vulnerabilities (60% versus 44%).

Figure 10. Security Practices Automated via Integration With DevOps Tools and Processes



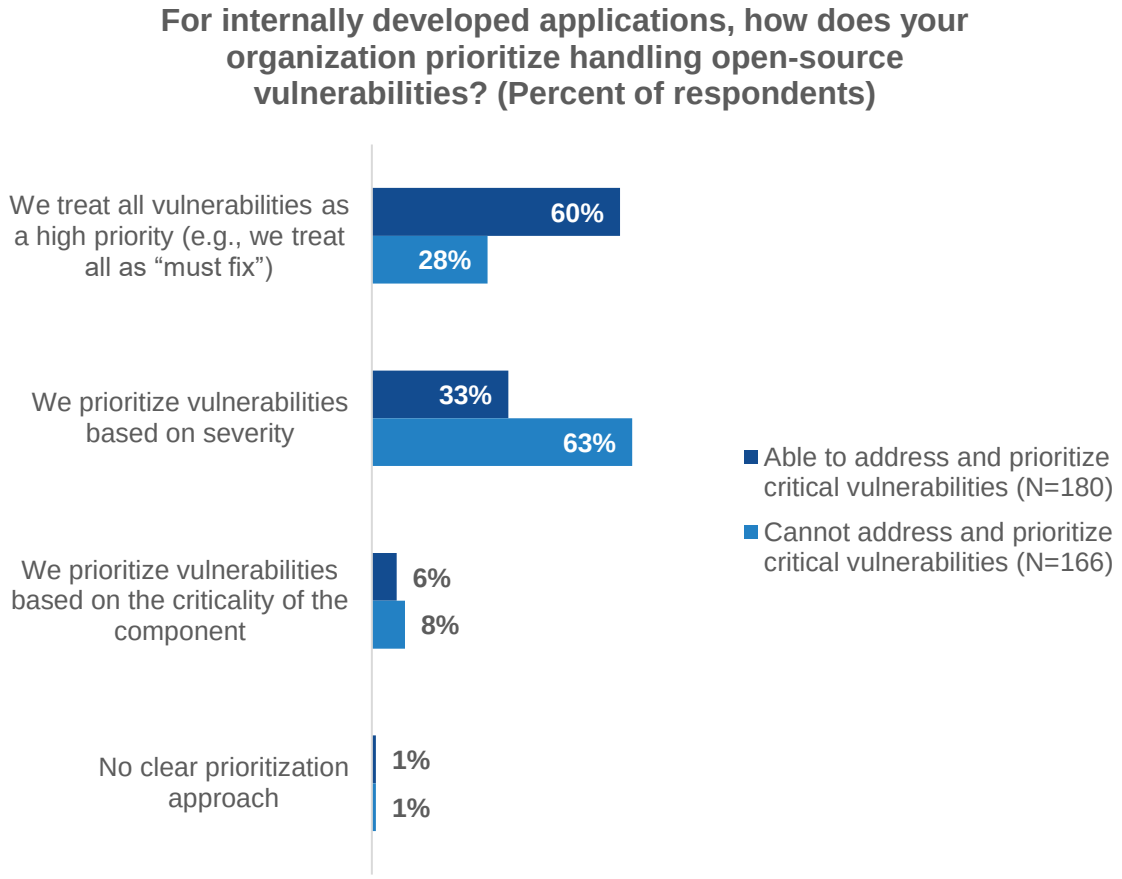
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Address Third-party and/or Open Source Software

Developers are also working faster because they can utilize vast libraries of third-party and open source software (OSS) to build their applications, which saves them time. While it is a valuable tool for developers to build sophisticated software, it is important to ensure the OSS is secure. The research reinforced this, showing that organizations that report the ability to efficiently remediate application vulnerabilities were more than twice as likely to report that they treat all open source vulnerabilities in their apps as a “must fix.”

While we would expect this approach to be unwieldy in practice, at a high level it shows the importance of securing OSS and addressing organizations’ concern about software supply chain attacks.

Figure 11. Prioritization of Open Source Vulnerabilities in Internally Developed Applications



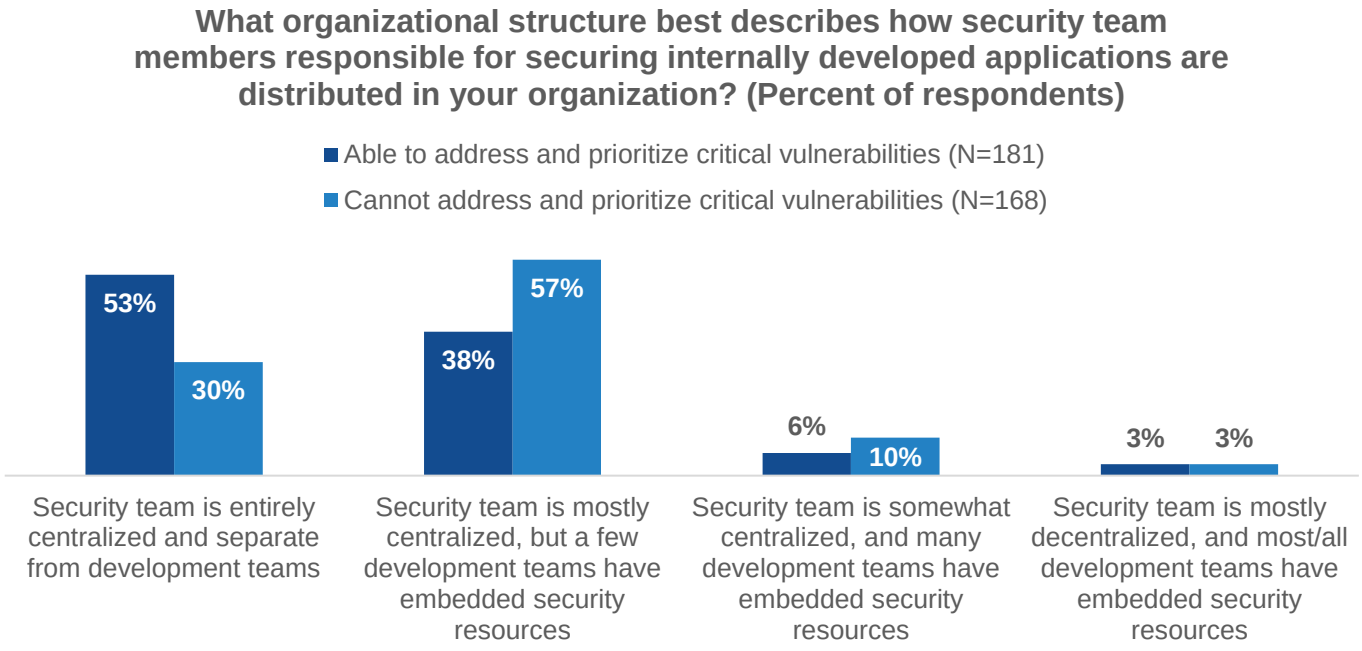
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Centralize Security for Visibility and Control

The role of security teams has changed with modern application development. Whereas monolithic applications and waterfall development processes meant security teams were responsible for testing, finding, and remediating security issues, with modern application development, as we've discussed, it's more efficient to shift many security tasks and responsibilities left to developers. But this means a new role for security teams—one that requires centralized control and visibility to manage risk.

In this study, the organizations that reported the ability to efficiently remediate vulnerabilities were much more likely to say their security team is entirely centralized and separate from development teams (53% versus 30%).

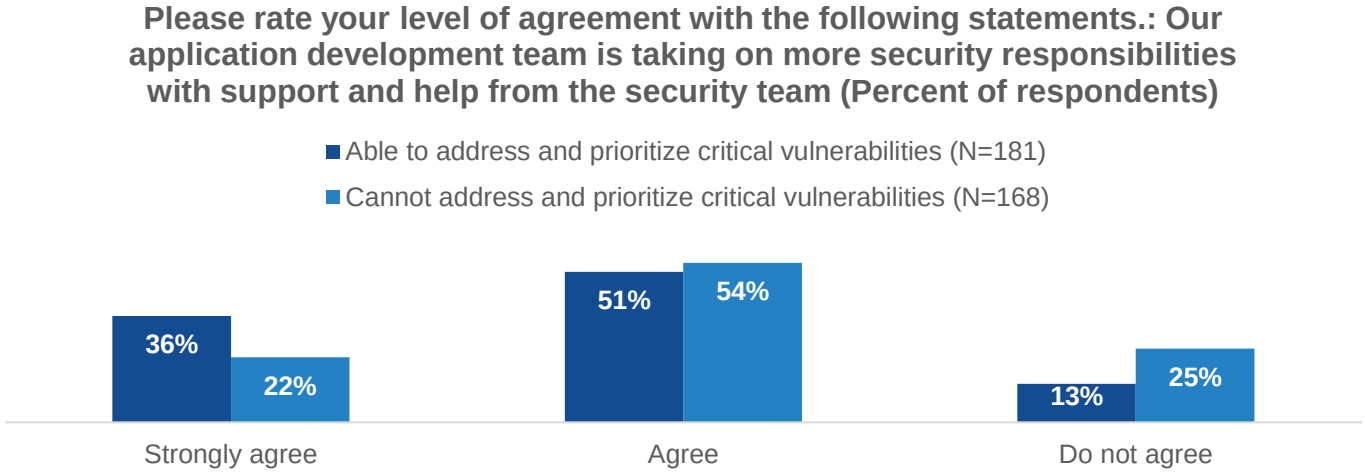
Figure 12. Organizational Structure That Best Describes How Security Team Members Responsible for Securing Internally Developed Applications Are Distributed



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Additionally, they were more likely to strongly agree that their application development teams are taking on more security responsibilities with support and help from the security team (36% versus 22%). So, the data shows the effectiveness of security taking on an oversight and guidance role while developers are tapped to put security fixes into place.

Figure 13. Application Development Teams Are Taking on More Security Responsibilities With Support and Help From the Security Team

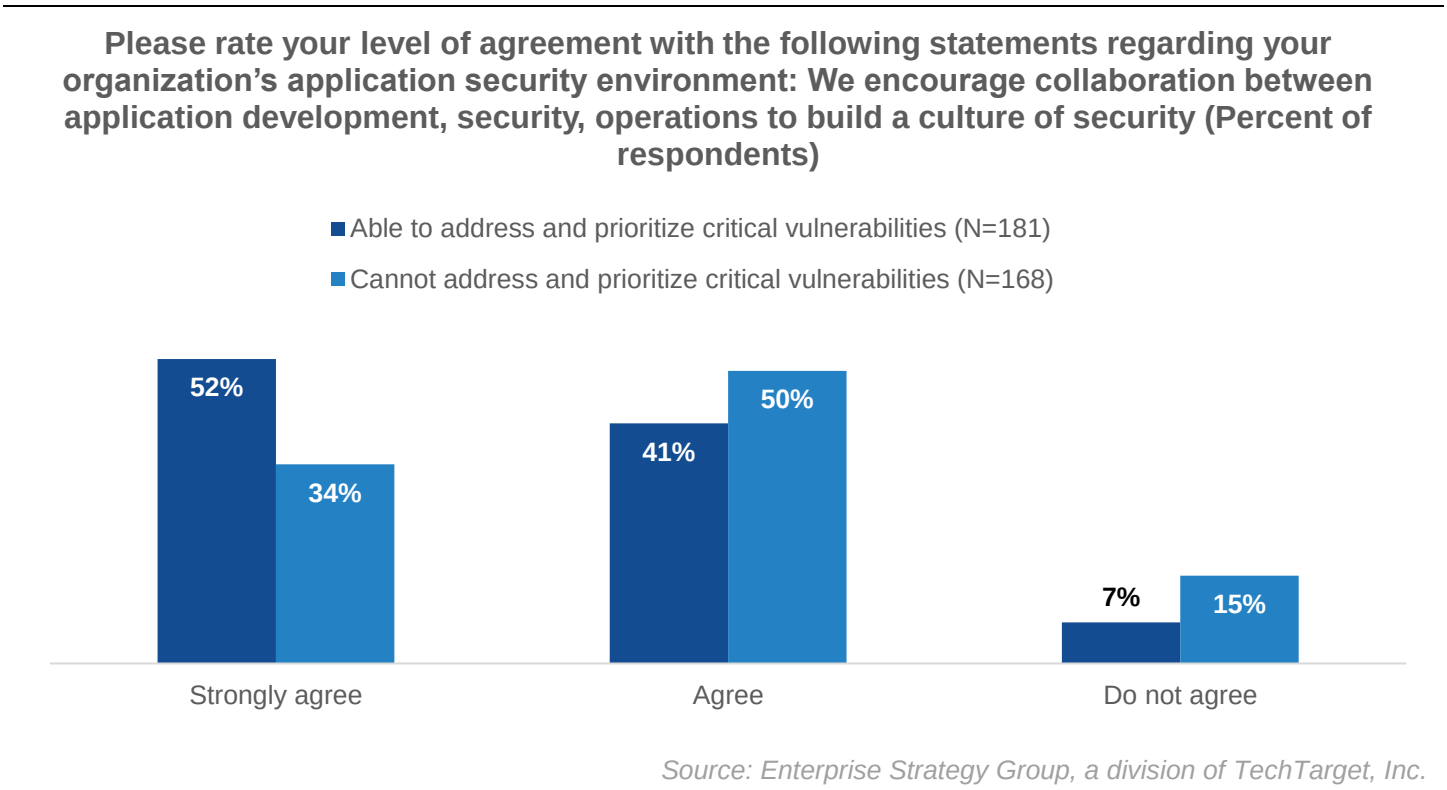


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Establish Security Collaboration Early in Development

Organizations that report the ability to efficiently remediate vulnerabilities were also much more likely to strongly agree that they encourage collaboration between application development, security, and operations to build a culture of security (52% versus 34%). Indeed, organizations that initiated collaboration during the "requirements and design" phase of the software development lifecycle (SDLC) exhibited a notably lower average of 2.3 serious security incidents, compared with 3.2 incidents experienced by organizations that engaged in collaboration during later stages of the SDLC. This correlation underscores the potential effectiveness of early-stage teamwork in bolstering security measures and minimizing vulnerability-related risks.

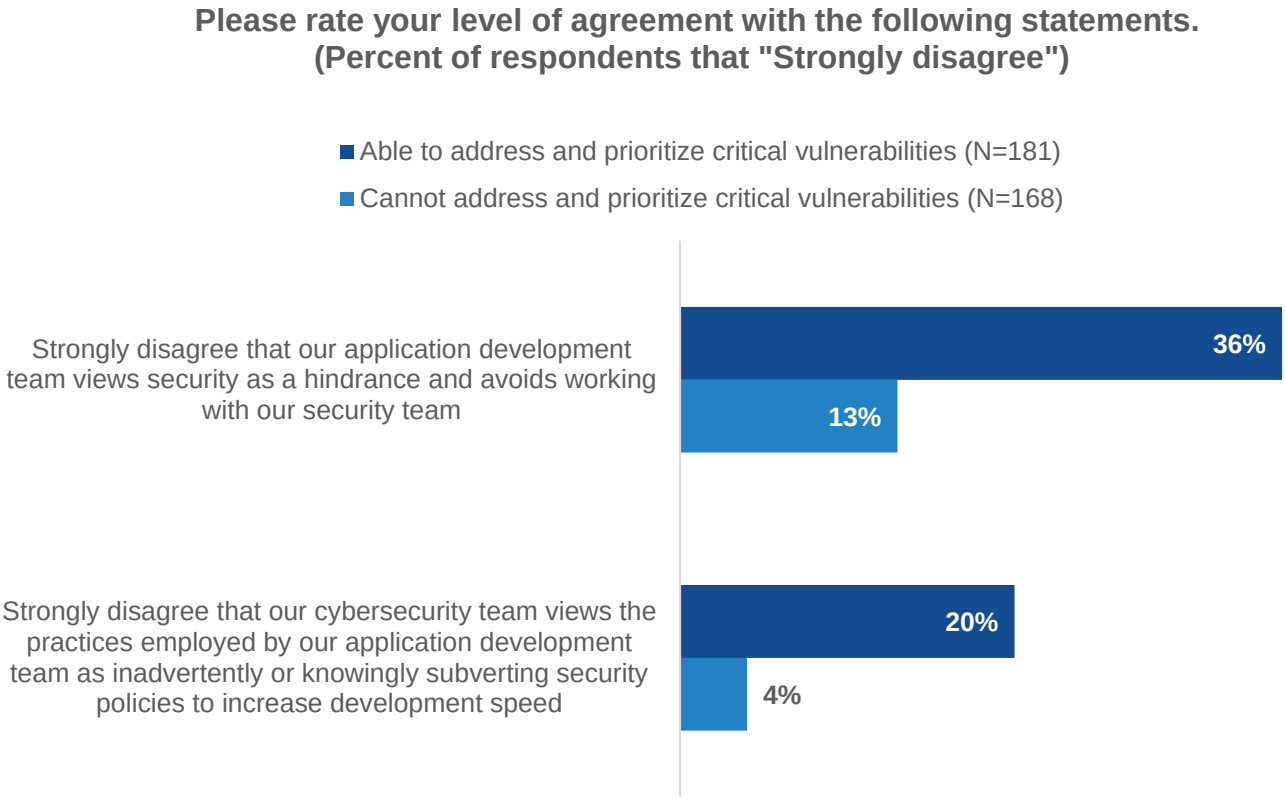
Figure 14. Level of Agreement With the Following Statement: 'We Encourage Collaboration Between Application Development, Security, and Operations to Build a Culture of Security'



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Respondents from these same organizations are much more likely to strongly disagree that their development team views security as a hindrance and avoids working with them (36% versus 13%), and they are more likely to strongly disagree that their cybersecurity team views the practices employed by the application development team as inadvertently or knowingly subverting security policies to increase development speed (20% versus 4%).

Figure 15. Comparing Organizations' Level of Agreement With the Following Statements

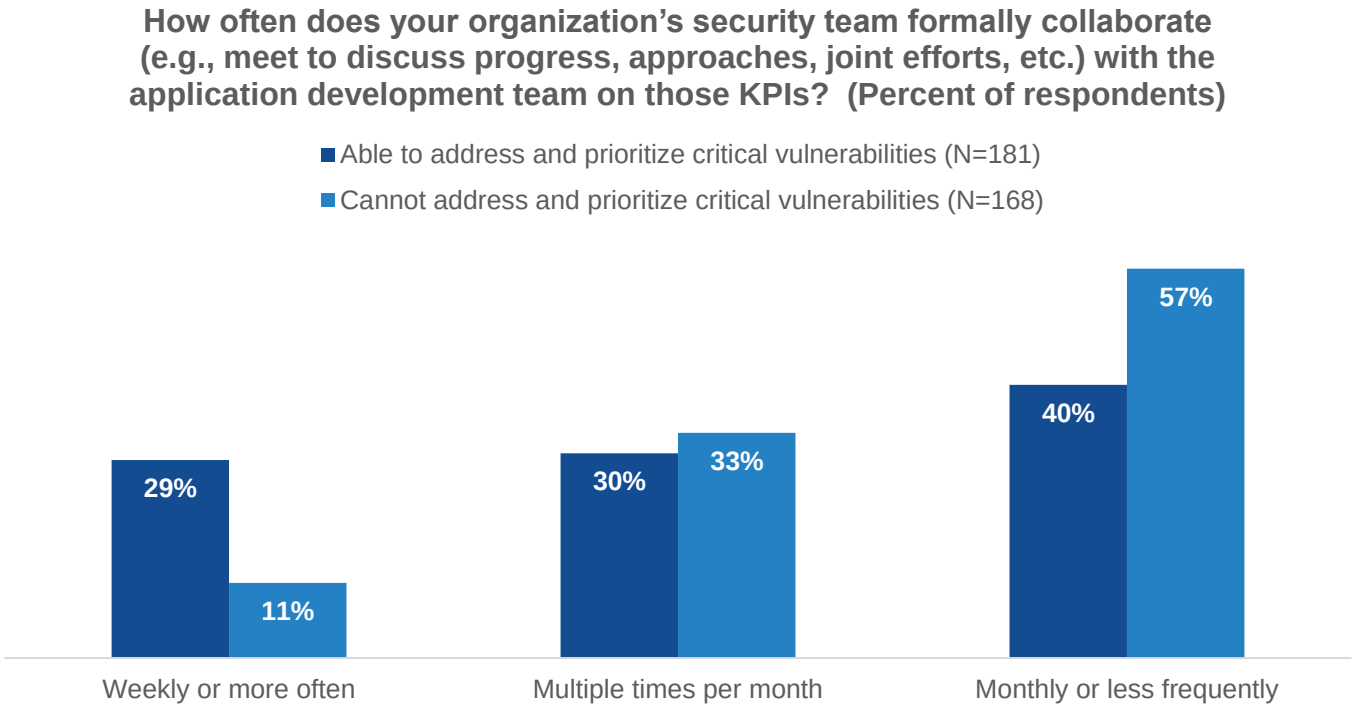


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Respondents at these organizations report developers are more likely to be willing to take several steps to implement secure coding practices. These teams also more frequently collaborate on at least a weekly basis (29% versus 11%).

This combination of data shows the human element of "doing security right." That is, organizations that have achieved superior security outcomes more often have successfully created a culture of security and shared responsibility, bolstering two-way trust between developers and security teams. Teams that meet more often typically have more success in prioritizing vulnerabilities.

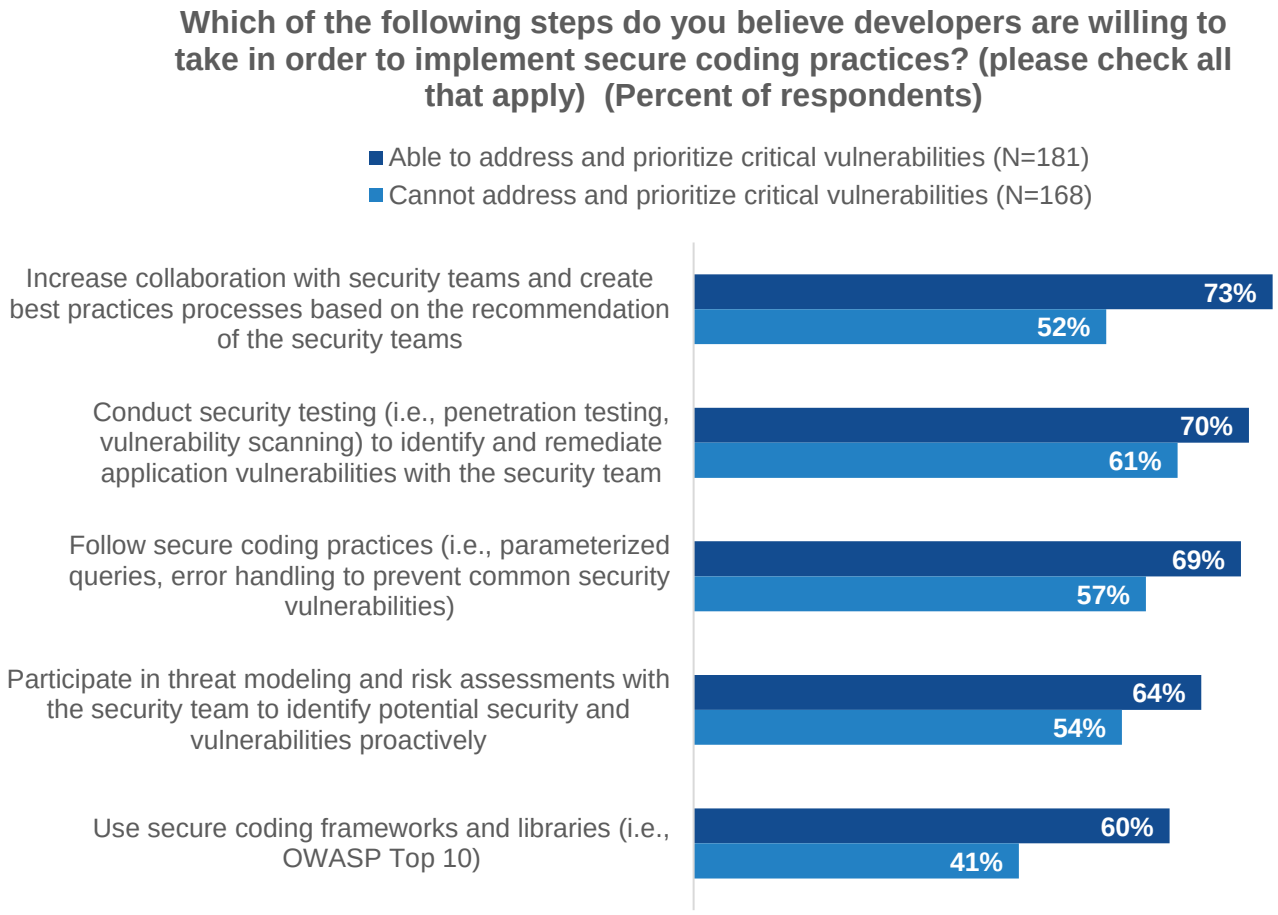
Figure 16. Frequency of Collaboration Between the Security Team and the Application Development Team on KPIs



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

We also see that when developers are willing to collaborate with security teams and take their recommendations on best practices, they are more successful with efficient remediation.

Figure 17. Steps Developers Are Willing to Take in Order to Implement Secure Coding Practices

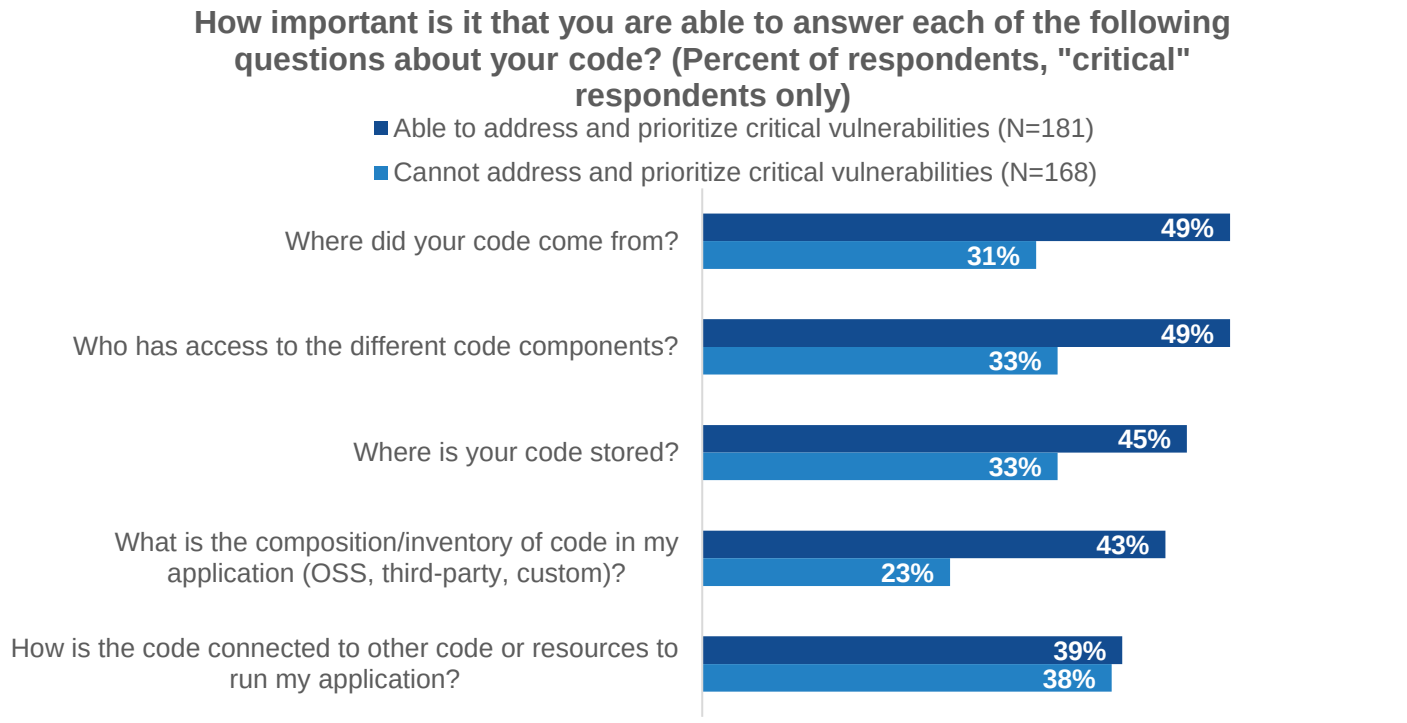


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Leverage SBOMs for Inventory and a Full Understanding of Code

Organizations able to efficiently remediate vulnerabilities were also more likely to say they view being able to answer questions about their code as critical, including understanding where their code came from (49% versus 31%), determining who has access to code components (49% versus 33%), knowing where their codes is stored (45% versus 33%), and being able to document the composition of their code (OSS, third-party, 43% versus 23%).

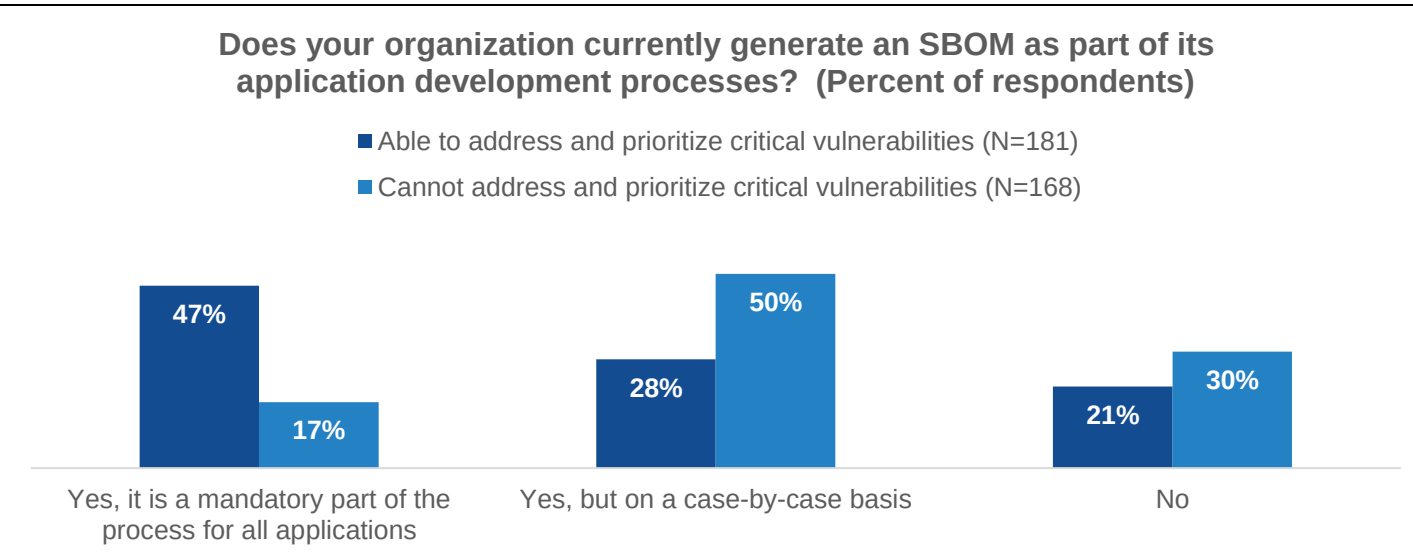
Figure 18. Perceived Criticality of Answering the Following Questions



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

To help glean these answers, these organizations are much more apt to say generating a software bill of materials (SBOM) is a mandatory part of their development process for all applications (47% versus 17%).

Figure 19. Are Organizations Generating SBOM as Part of Their Application Development Processes?



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

These actions are a major force behind these respondents being 2.9x as likely to be very confident in their organization's ability to manage the security and compliance risks associated with open source software components used within internally developed applications (60% versus 21%).

Figure 20. Organizations' Confidence Level in Managing Risks Associated With OSS Components Used Within Internally Developed Applications

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Conclusion

Our study shows organizations can optimize efficiency to effectively remediate application security vulnerabilities. The results revealed several best practices that have had a measurable impact on program effectiveness:

- Alignment and collaboration between development and security teams due to shared goals and KPIs, including application uptime, customer service, and data protection.
- DevSecOps adoption to incorporate security processes into development, ideally utilizing automation, to make it easy for developers to take on more security responsibilities and efficiently remediate their code.
- Security roles focused on centrally managing risk, supporting the training of developers, selecting tools, and gaining visibility and control to effectively manage risk and optimize efficiency for rapid response.
- Understanding complete application composition, including third-party and OSS application components that are increasingly used to speed development, in order to protect applications from software supply chain attacks.

Organizations should leverage solutions that address these areas to streamline vulnerability remediation without slowing development down. When security teams can partner with development teams to help them efficiently secure the components of their software, both teams can work more efficiently to meet their goals of delivering secure products to fuel company growth.

How Mend Can Help

Mend.io helps organizations build world-class AppSec programs that reduce risk and accelerate development, using tools built into the technologies that software and security teams already use. Its automated technology protects organizations from supply chain and malicious package attacks, vulnerabilities in open source and custom code, and open source license risks.

LEARN MORE

Research Methodology and Respondent Demographics/Firmographics

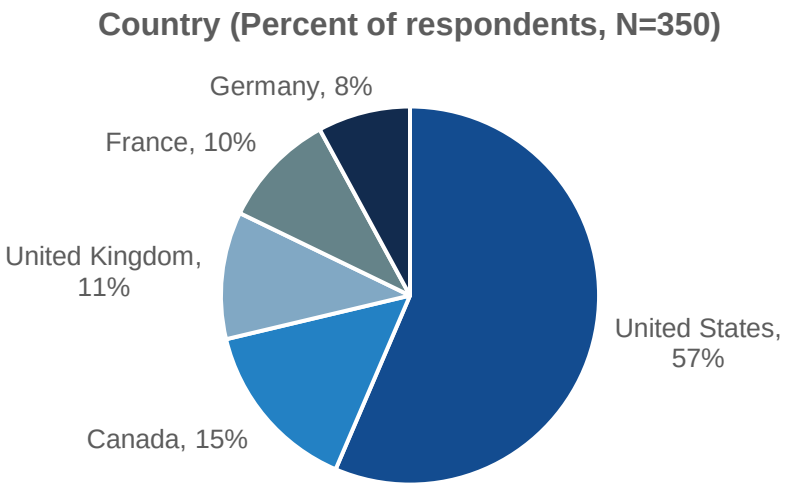
In the second quarter of 2023, Enterprise Research Group conducted a blind study of 350 respondents, consisting of application developers (27%) and senior security decision makers (73%) with oversight of or visibility into AppSec programs and associated business outcomes.

Organizations represented included small to midsize companies (100 to 999 employees, 29%) and enterprises (1,000+ employees, 71%) organizations, and the sample was composed of a horizontal mix of industry verticals. The research spanned North America (U.S. and Canada, 71%) and EMEA (France, Germany, and the U.K.).

All respondents were provided with an incentive to complete the survey in the form of cash awards and/or cash equivalents. Note: Totals in figures and tables throughout this report may not add up to 100% due to rounding, and the margin of error on a sample size of N=350 is + or – 5 percentage points.

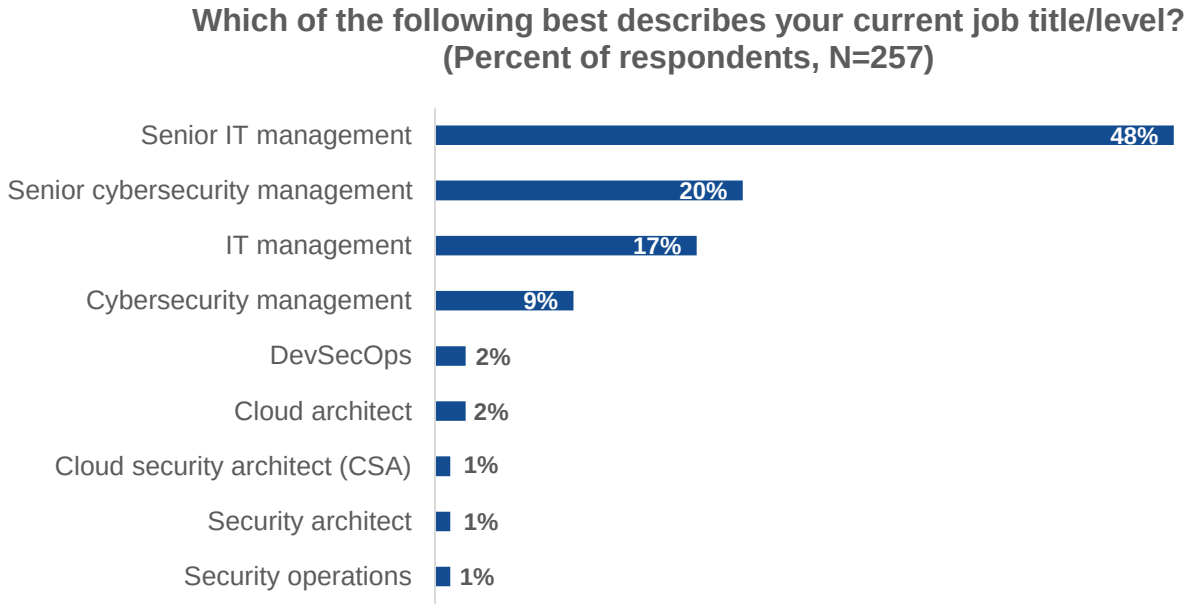
Figures 21-26 detail the demographics and firmographics of the respondent base.

Figure 21. Respondents by Country



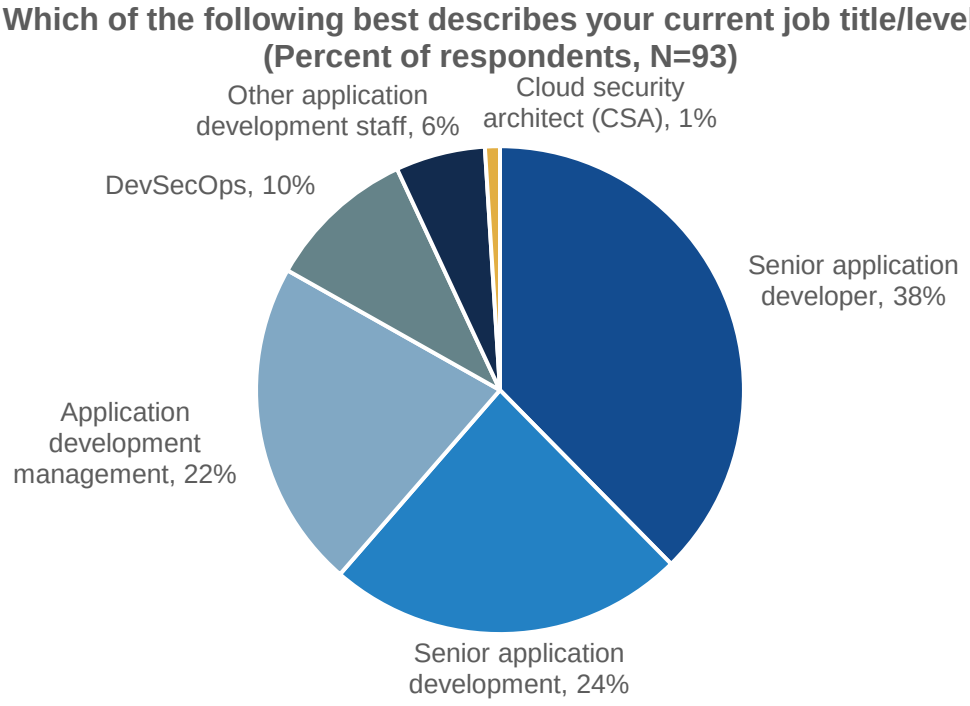
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 22. Respondents by Job Title (IT/Cybersecurity Respondents)



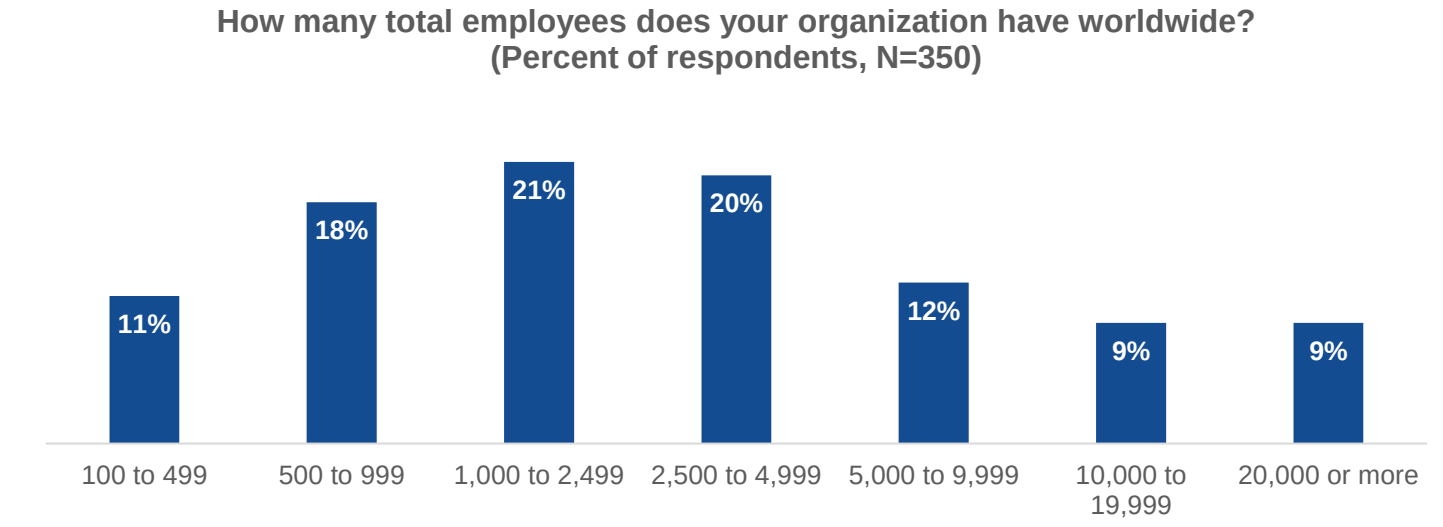
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 23. Respondents by Job Title (Application Development/Software Engineering Respondents)



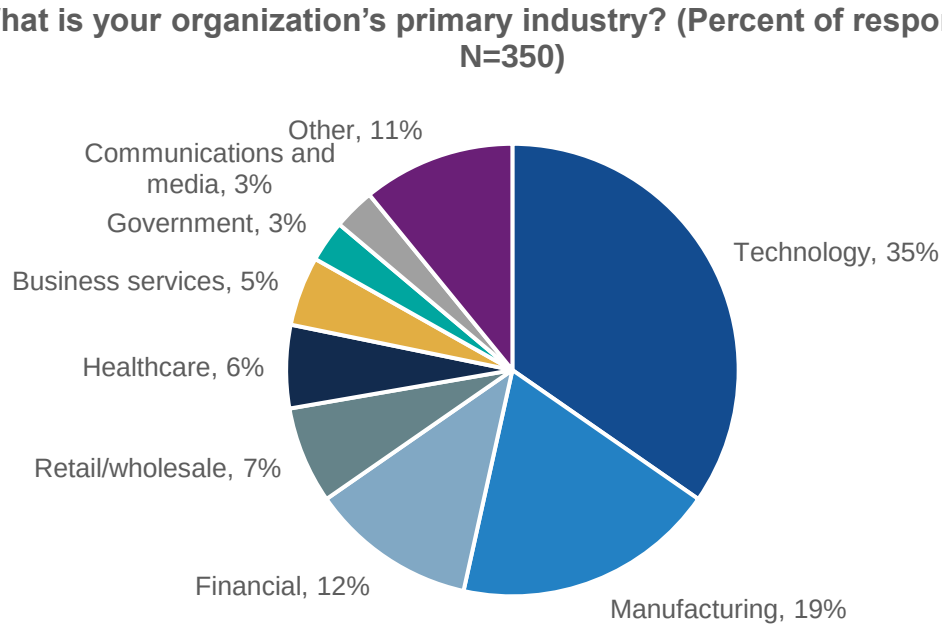
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 24. Respondents by Company Size



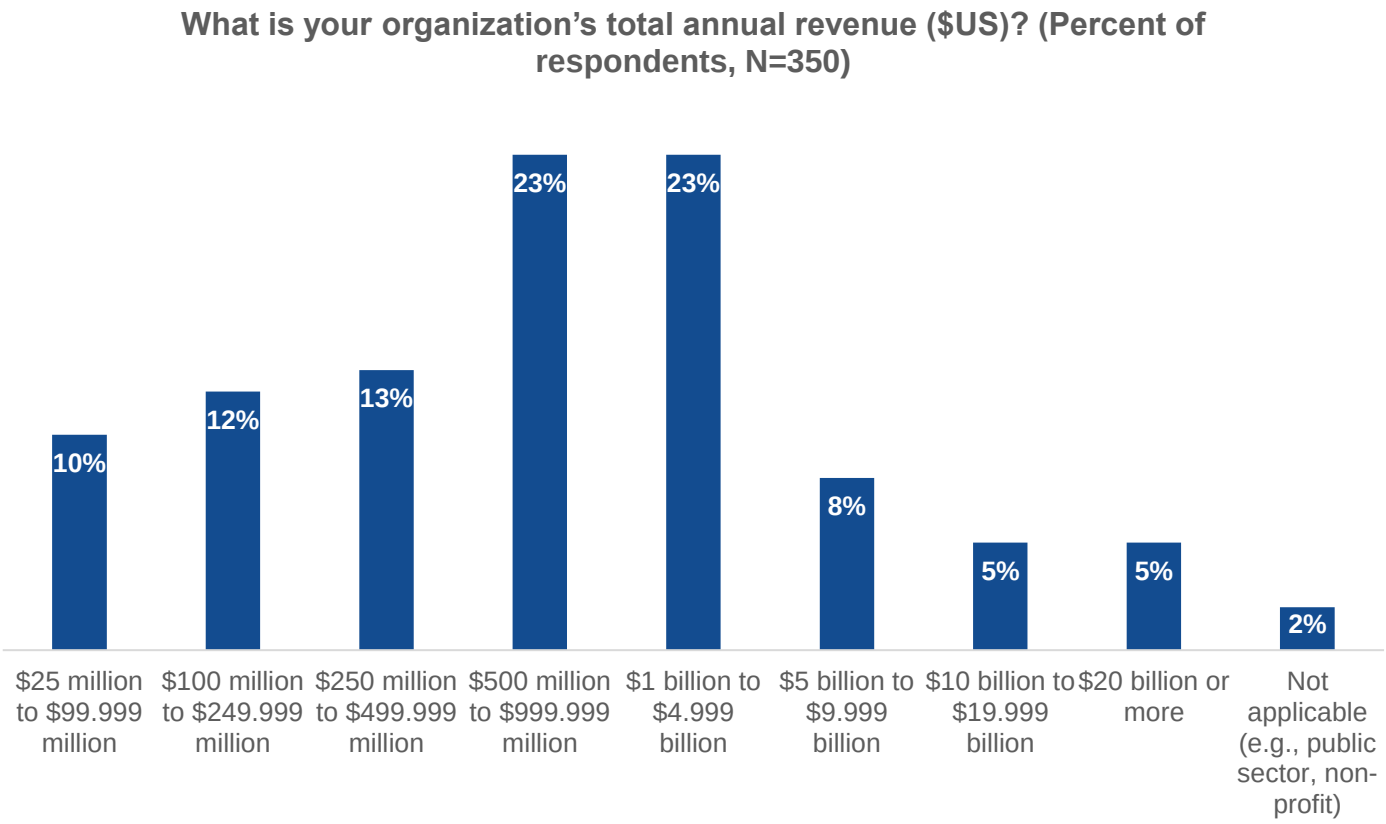
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 25. Respondents by Industry



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Figure 26. Respondents by Annual Revenue



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com