The 2025 State of Application Security Training

Primary research findings

Introduction

In 2025, companies that build software in the U.S., Canada, and the UK are prioritizing application security (AppSec) training to address evolving cyber threats. This study of individuals in medium to large software-developing companies highlights key trends, including the growing role of compliance mandates. Over 80% of organizations require security training, with frameworks like NIST 853, OWASP Top 10 and PCI DSS driving implementation.. Compliance remains the top motivator, cited by over half of respondents. However, organizations struggle with training effectiveness, with the top three frustrations of those being trained being: 1) the content is not delivered through relevant security tools, 2) the content is often outdated or repetitive, and 3) the content is not customized and therefore not applicable to their role.

To bridge these gaps, there are numerous options to build knowledge over a career, 20 of which the report explores. The top five include instructor-led courses, interactive training methods, live cloud labs, interactive hands-on training platforms, and on-the-job tutorials. Timing is critical, with one in four respondents preferring training during cloud configuration and coding phases to integrate security earlier in the development cycle. Certifications are also seen as valuable, with accredited individuals reporting benefits such as career advancement, increased compensation, and an improved ability to guide team members on security best practices. Budgeting varies widely, with almost half of companies allocating between $500 and $700 per employee annually.

AI and machine learning are playing an increasing role in cybersecurity strategies, with most organizations leveraging AI/ML to some extent and about four in ten making it a central pillar of their security operations. As AI reshapes cybersecurity, three-quarters of companies anticipate greater investment in formal and on-the-job security training.

Commissioned Surveys By Security Compass

Survey Participants

- 150 respondents from the US (73%), Canada (17%) and the UK (10%) in companies with a minimum of 100 developers.
- Targeted individual contributors (69%) primarily alongside managers and above (31%) who had self-reported competency in secure coding standards and regulations.

The survey was conducted by Golfdale Consulting

"Compliance may require AppSec training, but leading organizations go further, ensuring it truly benefits their developers. At Security Compass, we provide advanced eLearning that integrates AI, automation, and real-world scenarios, with customized role-based content that equips teams with the skills to build secure software from day one. By embedding security into development workflows, companies not only meet requirements but gain a competitive edge in resilience and innovation."

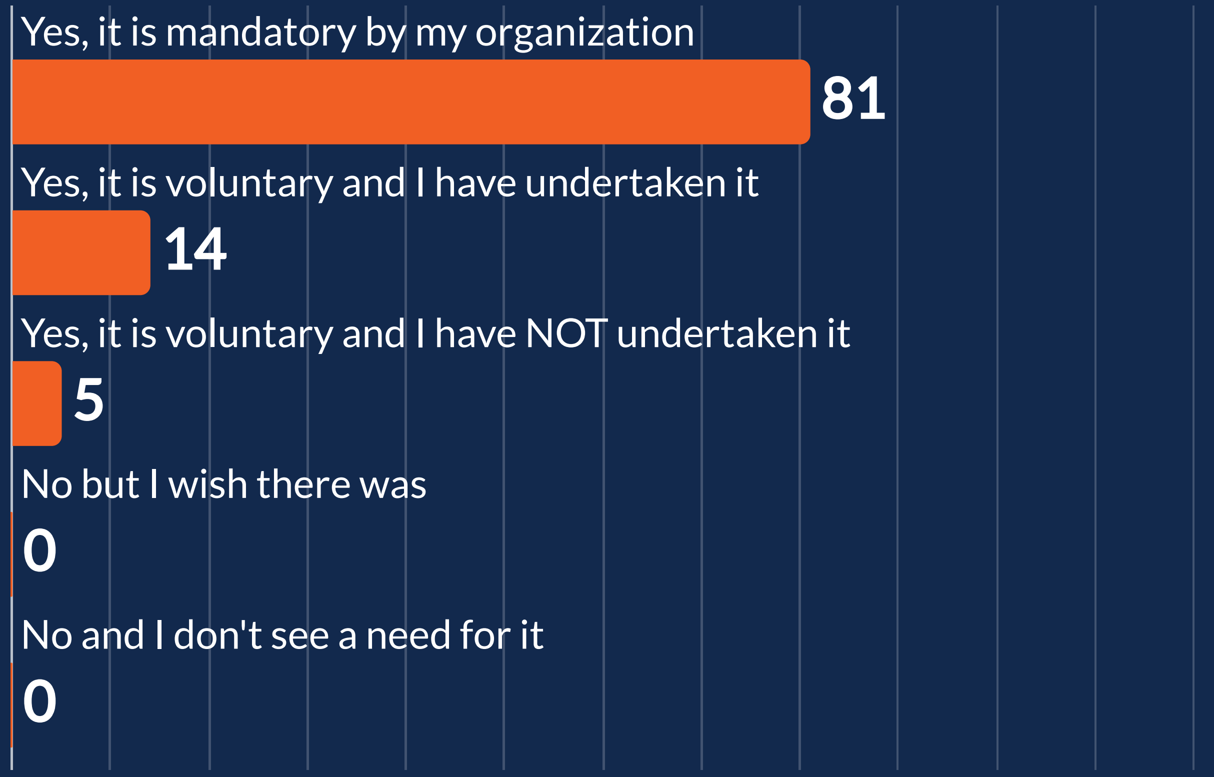
ROHIT SETHI
CEO, Security Compass

Security Compliance Training

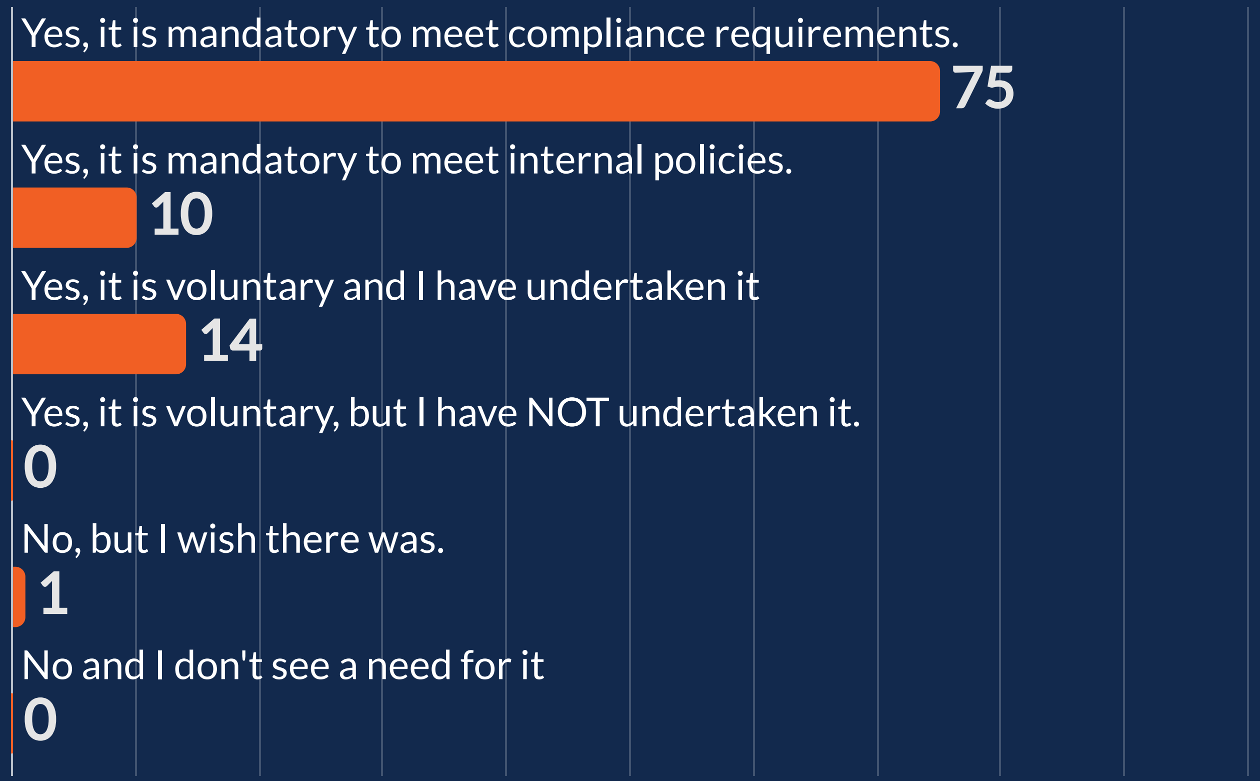
In 2025 we see security compliance training as a necessity by 8 out of 10 organizations that build custom software. Where this is lacking, practitioners do so voluntarily. More specifically, application security training is either mandatory or set as an internal policy by some 85% of software producing companies.

Overall	50 to 499 Devs	500 to 999 Devs	1000 to 4999 Devs

Security Compliance Training



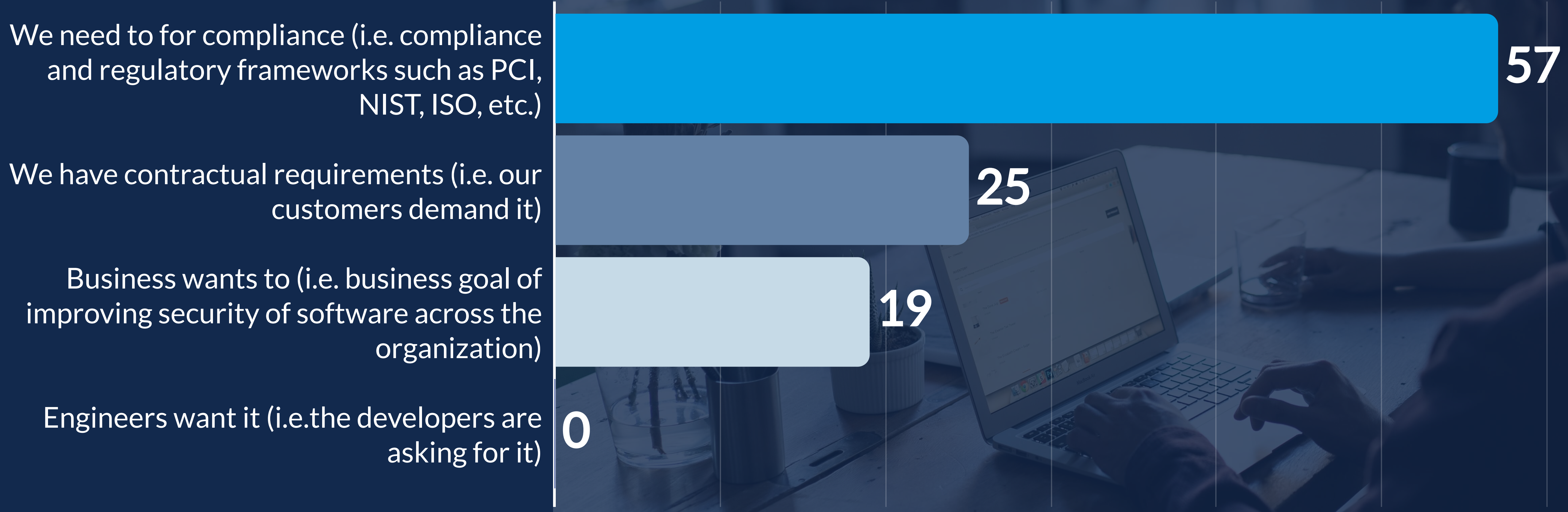
Application Security Training



#1 Driver of AppSec Training

Compliance requirements drive AppSec Training.

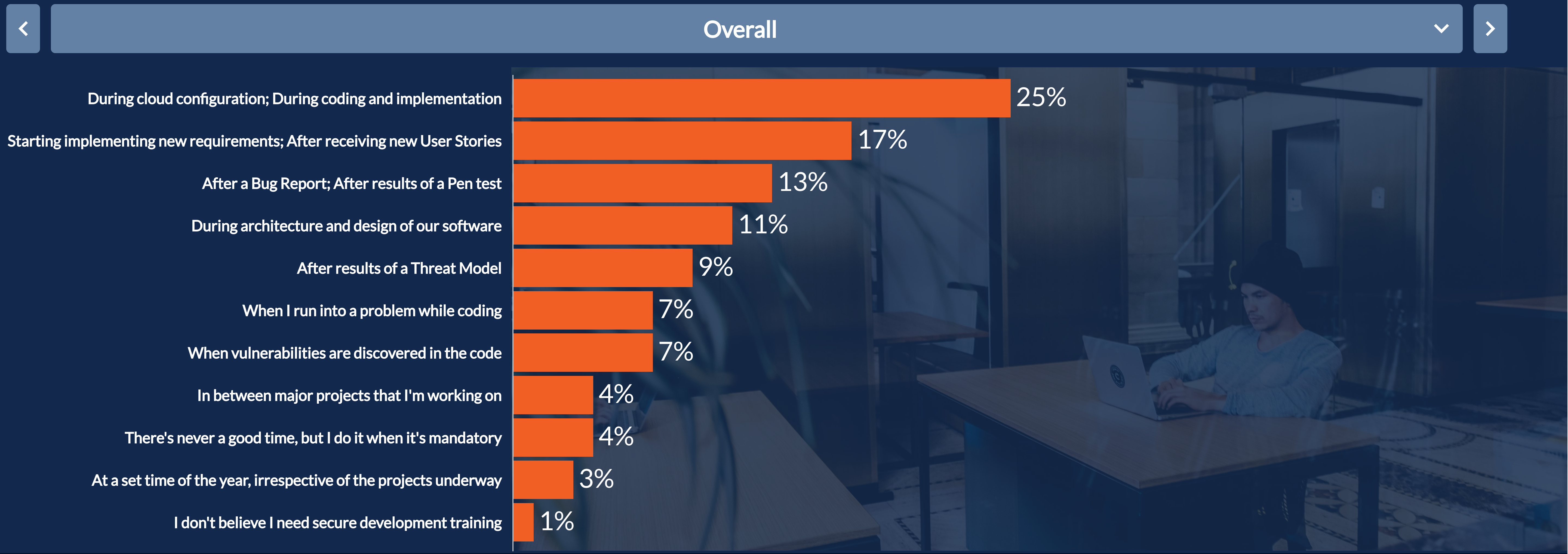
Driver of AppSec Training



Best Time for Application Security Training

Most commonly, appsec training is preferred during coding/configuration and/or when starting new requirements/receiving new user stories.

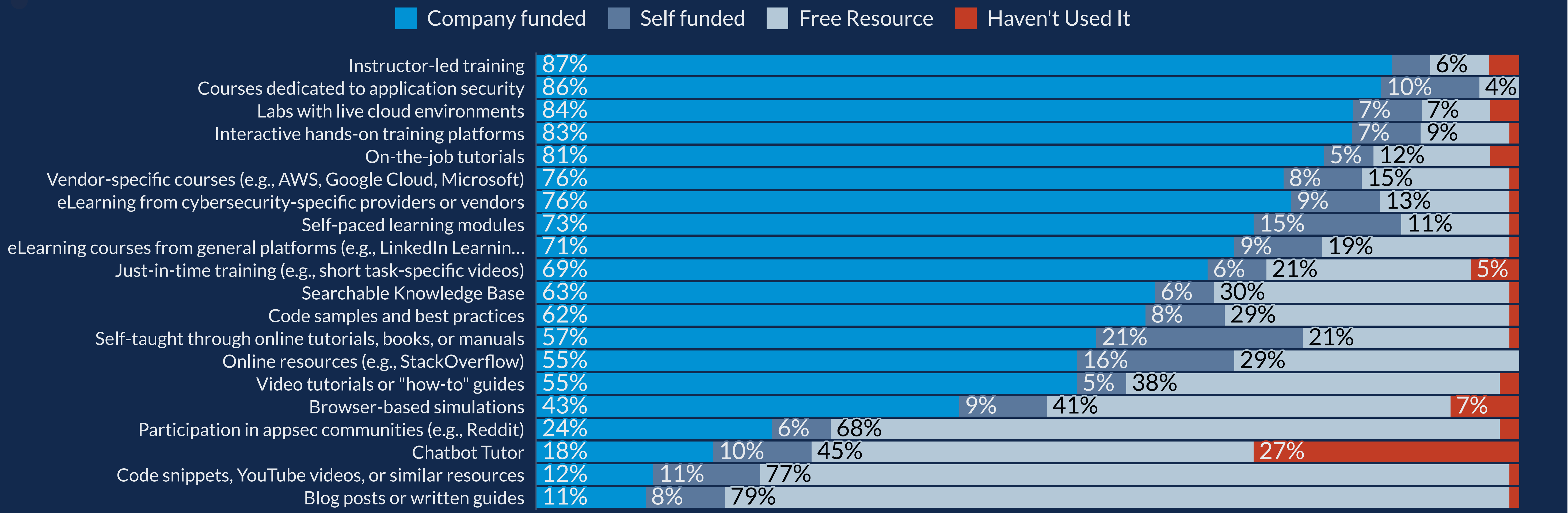
Best Time for Training



Methods to Build AppSec Knowledge

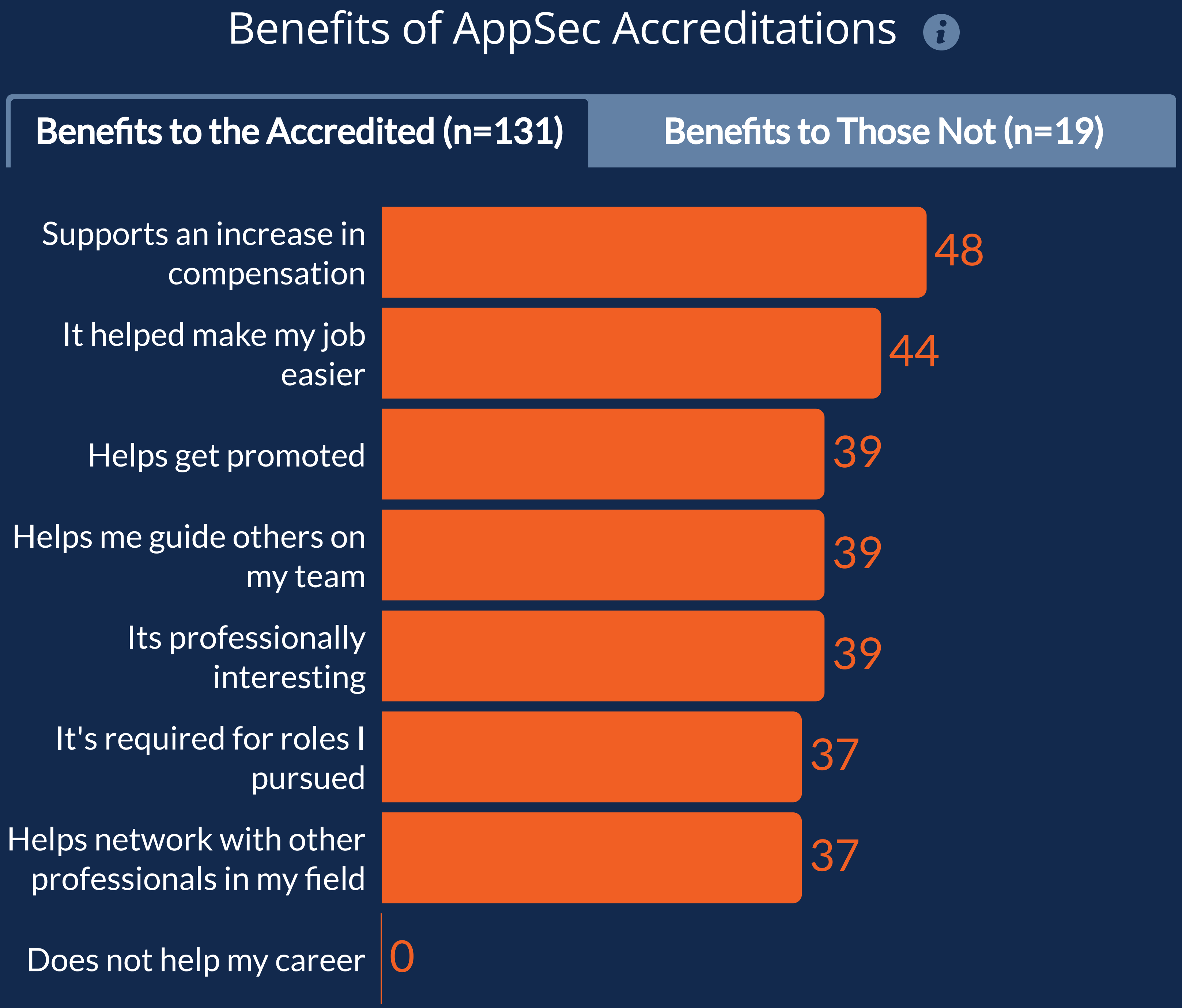
There are numerous options to build knowledge over a career. The top five include instructor-led courses, interactive training methods, live cloud labs, interactive hands-on training platforms, and on-the-job tutorials.

Methods Used in a Lifetime to Build Knowledge



Benefits of AppSec Accreditation

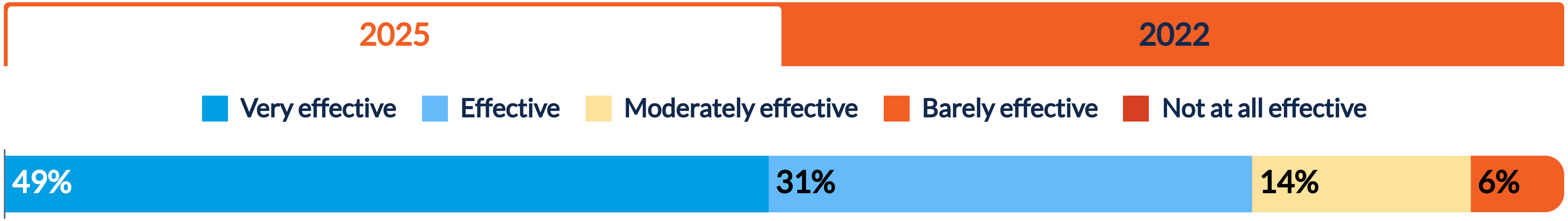
Supporting an increase in compensation and helping make their job easier are the benefits most readily experienced by those accredited. Those who have not yet been accredited also agree that there would be benefits to do so; most notably, helping network with other professionals.



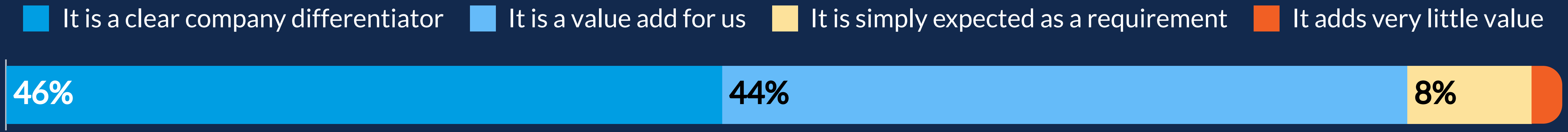
Effectiveness and Value of AppSec Training

AppSec Training is generally considered effective, and has moderately improved over the past few years. Over 4 in 10 view accreditation as a company differentiator and ISC2 accreditations in particular as extremely valuable.

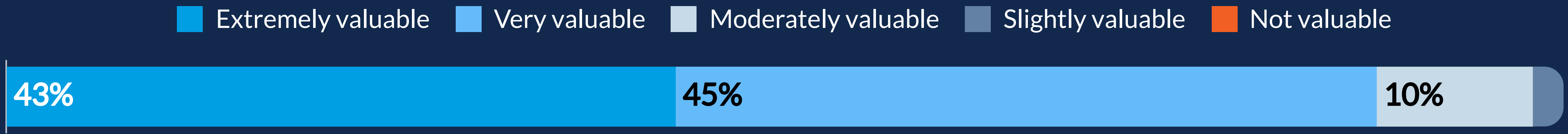
Effectiveness of AppSec Training



Value of Certifications for the Company

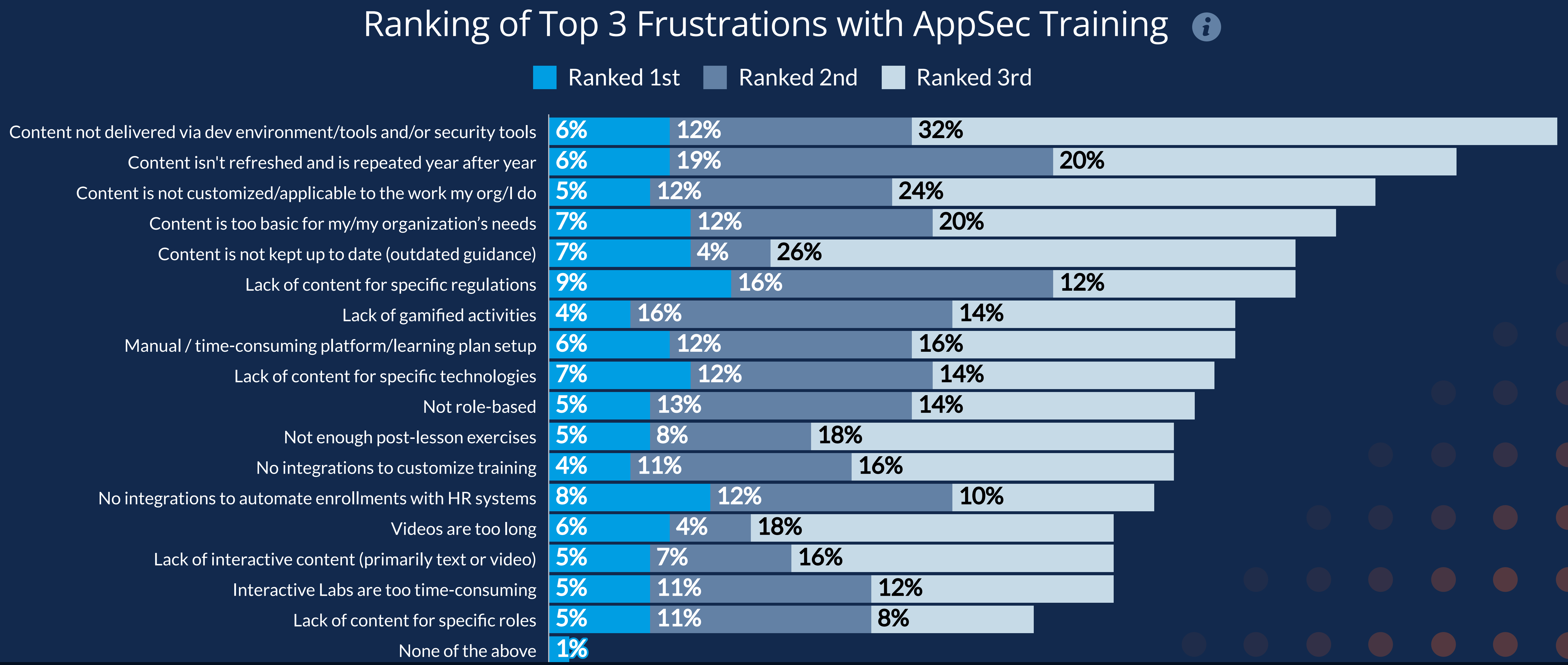


Value of ISC2 Accreditations



Top Frustrations with AppSec Training

The top 3 frustrations with AppSec training involve how content is delivered, kept current and customized to the role of the person taking it.

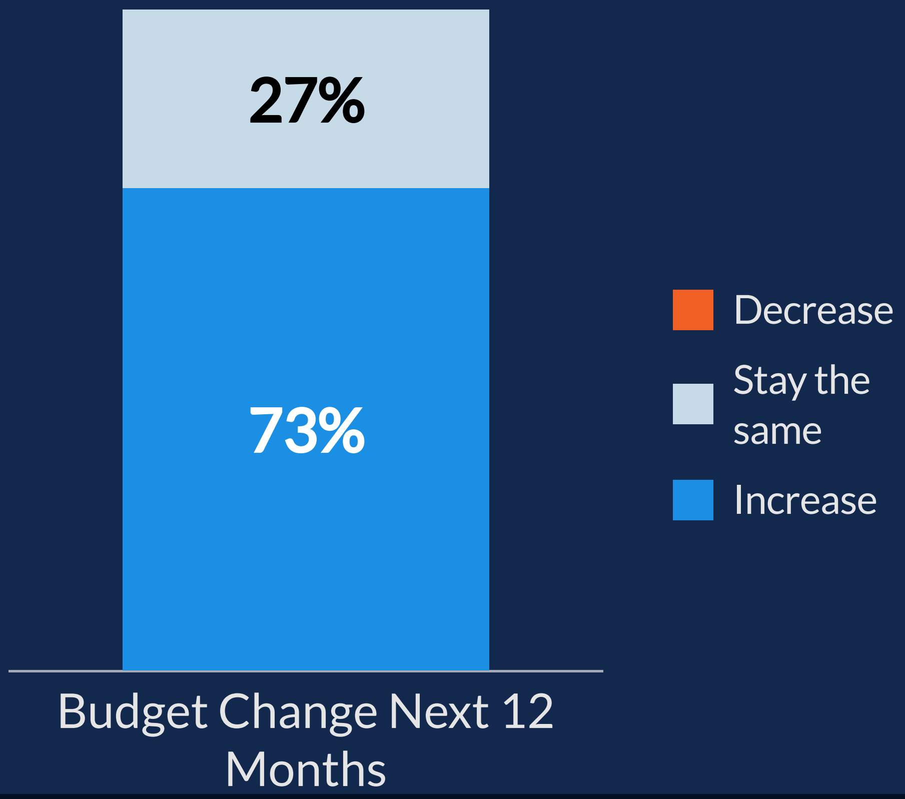


Ranking of Top 3 Frustrations with AppSec Training

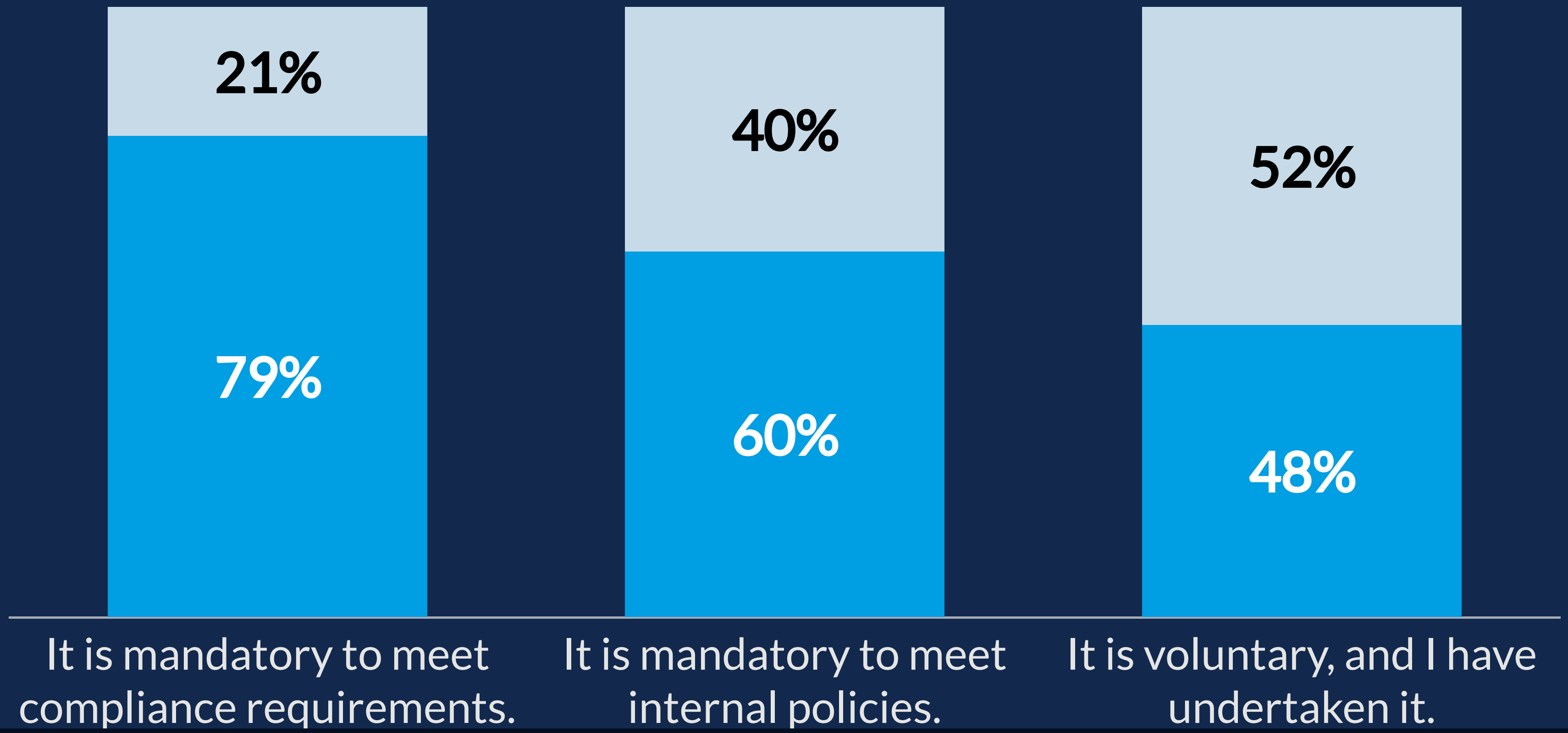
AppSec Annual Budget Expectations

No one indicated that their budgets for AppSec training would decrease with almost a quarter expecting it to increase in the next 12 months. Expectations for an increase were most felt by those whose companies make it mandatory to meet compliance requirements, less so for those who only have the mandate internally, and less again for those who undertake it voluntarioly.

Budget Expectations



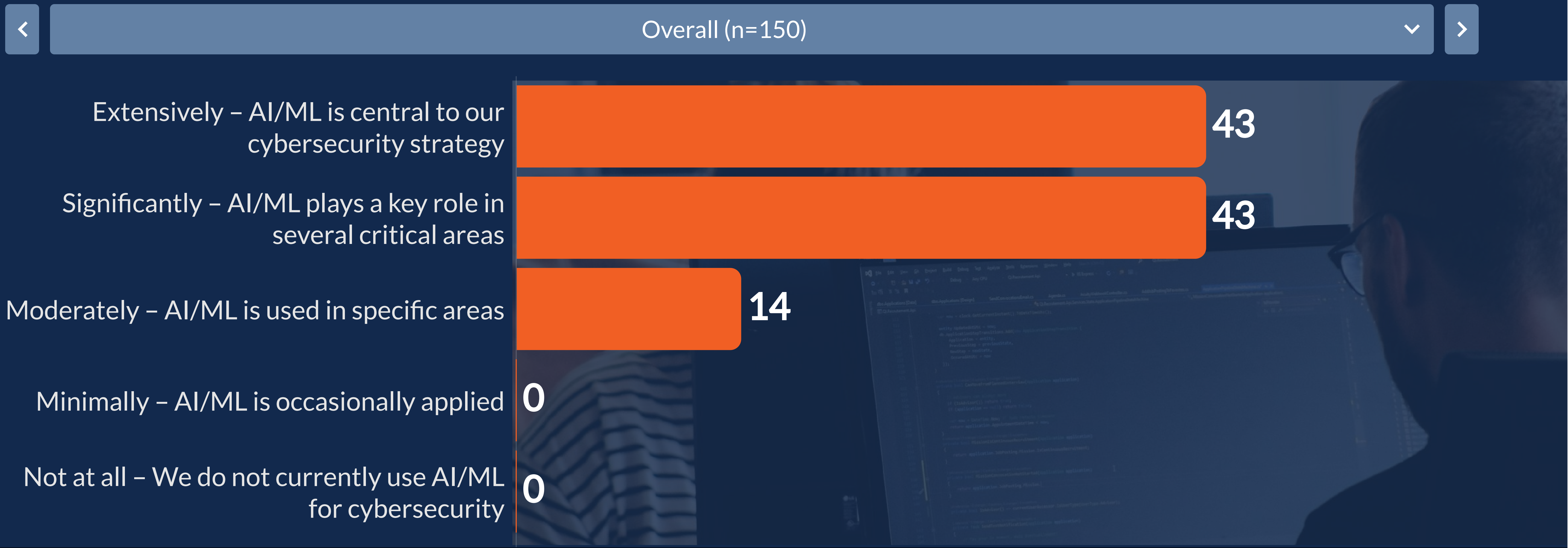
Budget Expectations by AppSec Training Offered by Org to Stay Current With New Threats and Vulnerabilities



Leveraging AI/ML to Mitigate Cyber Threats

Seven out of ten government agencies have made AI integration a major priority in their product development. By contrast, just 2% of government agencies that build software have set AI aside and have no plans to integrate it into their products.

Leverage AI/ML to Mitigate Threats



Conclusion

Security compliance training is a standard requirement for most teams developing software, ensuring they stay aligned with evolving regulations and best practices. Where training is not required, many professionals voluntarily seek it out to stay current. Application security (AppSec) training is also a priority, primarily driven by compliance mandates and contractual obligations.

Developers prefer AppSec training during critical phases such as cloud configuration, coding implementation, and when receiving new requirements. Training is least likely to be taken at set intervals or between major projects. Yet, challenges persist. Developers' top frustrations include training that isn’t integrated into security tools, outdated or repetitive content, and a lack of role-specific customization. Throughout their careers, developers have built AppSec knowledge through a mix of instructor-led courses, interactive hands-on platforms, live cloud labs, and on-the-job tutorials. AI is playing an increasing role, with nearly 40% of organizations making it central to their security strategy and most leveraging it in some capacity for cybersecurity training and automation.

Most expect to maintain or expand their security training investment in the year ahead, particularly if AppSec training is mandatory to meet compliance requirements. AppSec accreditation delivers clear benefits, helping professionals advance their careers, increase compensation, and strengthen team security practices. Organizations view security certifications as a clear differentiator, with nearly half considering them a valuable asset in building customer and partner trust. Recognized credentials, such as ISC2 accreditations, are widely regarded as critical to maintaining a strong cybersecurity posture.

Secure Development Resources

For more cybersecurity resources please visit: https://resources.securitycompass.com/
Phone: 1-888-777-2211 | . Email: contact@securitycompass.com

About Security Compass
Security Compass helps organizations build secure and compliant software by design. SD Elements, our core platform, enables teams to identify potential threats and generate security requirements before coding begins. Seamless integrations with existing DevSecOps tools and workflows enable developers to produce secure code efficiently. Our Application Security Training combines a rigorous curriculum with hands-on labs, equipping developers with the skills to build secure software with confidence. To discover how Security Compass enables secure software development at scale, visit www.securitycompass.com.

About Golfdale Consulting, Inc.
Golfdale Consulting Inc., trusted advisors to growth focused business leaders. Golfdale expertise and hands-on approach with senior executives spans three critical areas: 1) global market research and insights; 2) analytics and the application of decision sciences; and 3) advocacy for evidence based regulatory reform and market impact. Follow Golfdale Consulting on Twitter @_golfdale or visit https://golfdaleconsulting.com/