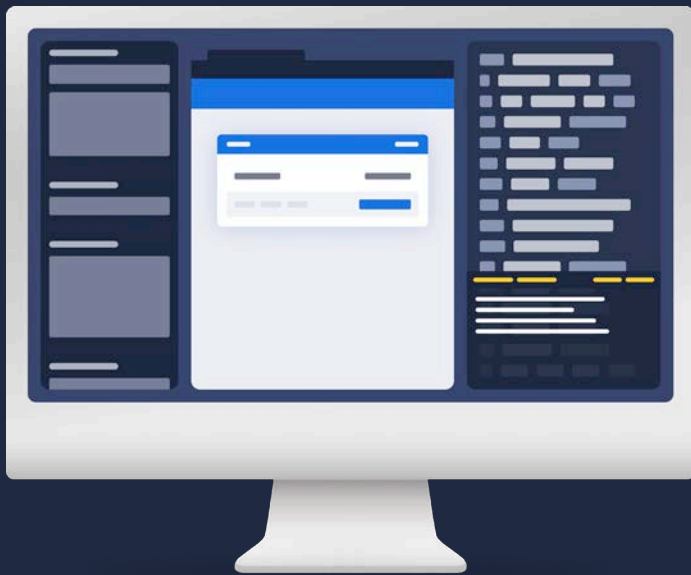


Whitepaper

Agile learning platforms and the ROI of developer driven security



+

>
accenture

Agile learning platforms and the ROI of developer driven security

Overview

The fast-paced nature of software development has made it easier for developers to quickly ship code, but this can come at the cost of reduced application security. Poor code leaves companies vulnerable to threats, especially as cybercriminals become more sophisticated. The 2023 U.S. National Cybersecurity Strategy now holds software vendors accountable for security in a way they have never been before. The U.S. Cybersecurity & Infrastructure Security Agency (CISA) requires vendors to make software “secure-by-design” and thus puts the onus on software makers to sell safe products out of the box instead of pushing that responsibility on to consumers and businesses.

An important aspect in this cultural shift is to foster critical thinking and ingrain the latest secure coding practices into the active development community of an organization. The major benefit is not only a reduction of the attack surface of an organization but a considerable improvement of developer productivity and software release velocity.

The 2023 U.S. National Cybersecurity Strategy now holds software vendors accountable for security

Challenge

The challenge for companies is no longer just shipping fast code, but also shipping code securely. To do this, a modern software development life cycle that integrates agile learning and secure code practices is necessary. Choosing the optimal solution that has real business impact can be difficult. Traditional learning and upskilling efforts for security tend to fail because they take the developer out of their day-to-day workflow, deliver long, tedious courses with out-of-date information, and provide no way of reinforcing the material or connecting the education to their daily work.






Solutions that apply agile learning methods are more effective. In our customer’s experience, the result is cutting the number of vulnerabilities introduced by developers by half, while reducing risk and cost.

Agile learning systems for secure code offer multiple dynamic pathways to gain skills, starting with foundational principles and building towards more advanced concepts with an agile strategy of progressive layering.

Even though we live in a world of sophisticated AI and vulnerability scanners, the most difficult and important factor in a successful AppSec modernization program is to achieve a cultural shift in the security awareness and secure coding practice of the development team. Many large organizations still don't have an agile learning platform for secure coding. Secure coding practices can be challenging to implement but they have the potential of significantly reducing risk and cost.

Agile learning platform ROI

The key factors to include in the ROI calculation for an agile learning investment include:

-  **Licensing costs**
-  **Developer average fully-loaded salary**
-  **The average vulnerability count found in static code scanning or penetration testing**
-  **The average number of critical and high risk vulnerabilities**
-  **The average time it takes to remediate vulnerabilities**

By investing in an agile secure code learning platform, organizations gain the ability to identify internal security champions but also the ability to baseline the team, identifying weaker developers who are most likely to introduce vulnerabilities. By identifying and focusing on weaker developers first, the organization can execute a targeted upskilling strategy that supports less experienced developers to write better quality code. Making the secure code learning experience as frictionless as possible and building it into the daily software development process of an organization is an important factor of success.

Long term customers of Secure Code Warrior have shown that the positive effects on ROI are not only measurable but lead to a quick payback of the license and time investment. Organizations are seeing improved internal efficiency across several dimensions: risk reduction, breach prevention, and improved developer productivity.

Accenture recently integrated Secure Code Warrior into its Intelligent Application Security Platform (IASP). This proprietary platform is used internally at Accenture as well as part of large security delivery engagements for its clients. When viewing and triaging vulnerabilities in IASP, developers are then able to take secure coding classes tailored to the unique vulnerability and language of the application. This fundamentally changes the way secure code training is performed, aligning to a more agile way of learning and providing more precise education when and where developers need it.

“The whole thing has to start in the heads of management. Investing in the training of developers is not a lost investment, but an investment into quality, productivity, and the reputation of the company.”

Klaus Klinger, DevSec Awareness Evangelist at Allianz

Larger organizations use potentially thousands to tens of thousands of developers to generate, enhance, scan, test and fix hundreds of internal and third-party applications. Accenture estimates that blended developer costs for an organization is between \$75 and \$85 per hour. Increasingly, developers are having to spend more of their fixing vulnerabilities, resulting in dampened productivity and slower go-to-market times. Developers who use Secure Code Warrior see immediate value in more secure code and greater productivity. One large financial services company noted that 47% fewer vulnerabilities were introduced into production and on average the open vulnerability count was reduced by nearly half, from 236 days to 115 days.



PRODUCTIVITY

2.48x

Developers who use Secure Code Warrior see immediate value in more secure code and greater productivity.








BREACH PREVENTION

47%

Fewer vulnerabilities were introduced into production and on average the open vulnerability count was reduced by nearly half, from 236 days to 115 days.

These results show clearly that the SCW agile learning platform can be a financially viable component in a proactive security strategy. Other results and benefits obtained by enterprise customers include:

-  An average of 148% improvement in developer productivity
-  Given the high volume of vulnerabilities identified in a secure development process, the cost to fix is often in the 7-8 figures.
-  Accenture has observed that as vulnerability risk begins to grow, organizations are then forced to redeploy personnel to address short-term, tactical remediation campaigns
-  The positive results of implementing secure code from the beginning include faster release cycles, greater developer productivity, less re-work, risk mitigation, and higher quality applications with a better customer experience.
-  A secure code educated developer produces fewer vulnerabilities, reducing the bug fix queue and increasing the velocity of software release for the organization.

Investnet introduced a companywide upskilling program with Secure Code Warrior in fall of 2021 and instigated a culture shift to prove that SCW-educated developers are fixing 2.7x more vulnerabilities than their untrained peers.

“With Secure Code Warrior, you can stay ahead and take a proactive approach to mitigate that potential chain of vulnerabilities through agile secure code learning.”

Derek Fisher, Head of Product Security

Summary

The SCW agile learning platform stands out as a proactive approach to security with substantial financial benefit, both in terms of cost and waste avoidance and by accelerating the code remediation vulnerabilities faster. In addition, by raising the security intelligence of the developer organization, a culture of “security is everyone’s job” builds over time.

Secure Code Warrior has the largest content base with more than 63 development languages/frameworks.

Developers benefit from proven vulnerability education that teaches them the root cause of an issue and how to fix them. When integrated with leading software scanning technology, SCW makes existing security tool investments more valuable. Instead of Google searches or submitting code into unsecured AI engines, developers can trust SCW content and can retire the tech debt with confidence. Its learning platform has hints and a point system so that developers never have the frustration of getting stuck in an exercise and they receive positive feedback in the learning process while creating usable secure code at the same time.

Call to action

An agile learning platform such as Secure Code Warrior enables developers to not only write better code from the start but also sparks a culture shift towards secure code by design within the organization. Secure Code Warrior delivers the most effective learning solution to over 600 enterprises for developers to learn, apply, and retain software security principles, resulting in secure, resilient released software. As a global leader in application development and security services, Accenture can help enterprises realize the same value in agile secure code training.

About Secure Code Warrior

Secure code learning for today's developers

Secure Code Warrior gives your developers the skills to write secure code. Our learning platform is the most effective secure coding solution because it uses agile learning methods for developers to learn, apply, and retain software security principles. Over 600 enterprises trust Secure Code Warrior to implement agile learning security programs, deliver secure software rapidly, and create a culture of developer-driven security.

[Request a demo](#)

[Try Secure Code Warrior for free](#)

Find us on social:





**SECURE
CODE
WARRIOR**