BRIEF

Shift left *(and achieve compliance)* with repeatable secure coding skills

> Almost every developer team these days employs some form of compliance training, whether it's part of an initial certification process, used to ensure that a company is staying within the bounds of industry frameworks or governmental regulations, or as part of an annual requirement or review. It's an important step, because if an organization can't meet basic compliance requirements, then it's workers can't realistically perform their duties.

Compliance rules exist for a reason, because anyone working within the field those rules cover must have at least a fundamental understanding of all the relevant processes and procedures, as well as any applicable laws.

While compliance training is important, completing the mandated minimum requirements does not ensure true application security. This is especially true of developers trying to integrate secure coding skills into their daily workflow. Almost every developer undergoes some form of compliance training, and yet when surveyed, 67% admitted that they often left vulnerabilities in their code.

67% **of developers admitted that they often left vulnerabilities in their code.**

Why?

> For the second year, Secure Code Warrior conducted *The state of developer-driven security survey, 2022* in partnership with Evans Data Corp in December 2021. We surveyed 1,200 developers globally to understand the skills, perceptions, and behaviors when it comes to secure coding practices, and their impact and perceived relevancy in the software development lifecycle (SDLC).

In terms of why compliance training is not achieving improved software security, this is an issue that we have been talking about for a long time. The recent survey simply spotlights this problem.

On the one hand, developers are being asked to step up to new roles by including cybersecurity throughout the software development process, including as they are initially writing the code for applications and programs. But writing secure code, or even just learning all about the cybersecurity issues and vulnerabilities that could affect it, is not an easy task. In the survey, 63% of the developers said that writing secure code was a difficult task.

The difficulty of writing secure code should not come as a surprise. There is a reason why so many high-paying cybersecurity jobs are going unfulfilled, with over 3.5 million worldwide openings at last count. If it was easy work, everyone would be jumping into that field. Learning how to combat threats and eliminate vulnerabilities within code is difficult, and the threat landscape is constantly changing. Static compliance training or one-time classes can't keep up or provide the kind of education developers need. It may check a box in terms of compliance, but can't provide real application security assurances for your organization or enable developers to write secure code, or the skills to find and fix code vulnerabilities.

Learning how to combat threats and eliminate vulnerabilities within code is difficult, and the threat landscape is constantly changing.

Compliance and security training are important, but different

> Organizations must start to realize and acknowledge what compliance training can do, and what it can't. Don't abandon compliance training, especially if it's mandated by law. And especially because (even with current training methods) 92% of survey respondents stated that they needed at least some training in compliance-related issues or security frameworks, with 50% stressing the need for significant compliance training.

The compliance frameworks they were most interested in training with included those that are specific to various industries, though several general cybersecurity frameworks also made the list. They included the CIS Security Framework, PCI DSS, the OWASP Top 10, MISRA C, ISO/IEC, the Health Insurance Portability and Accountability Act (HIPAA) and others.

So yes, train in those frameworks, but understand that checking a box on compliance training does not equal providing a foundation for the ongoing creation of secure code.

Instead, view compliance training as part of an ongoing opportunity to expand your developer's secure coding skills that can be repeated outside of the compliance cycle, so they can create and release secure software every day. Shift the priority from achieving compliance to enabling development teams to code securely with continuous learning.

By investing time and resource in developer enablement then those yearly check-box compliance exercises or exams will become a breeze for your staff to pass and complete, while benefiting from improved productivity overall.

92% **of survey respondents stated that they needed at least some training in compliance-related issues or security frameworks.**

How can you make the shift to developer-driven security?

> Developers overwhelmingly said that training was valuable, but took issue with the type of training that they have received regarding secure coding over the years. Developers said they wanted to see more of an emphasis on practical training using real-world examples that were relevant to their jobs (30%). More interactivity was also seen as critical by 26% of the respondents, especially if they were able to actually practice writing secure code as part of those exercises.

A desire to receive more guided training focusing on the specific vulnerabilities they were most likely to encounter in their industry or sector was seen as important to 23% of the developers surveyed, while 22% wanted to see more real-world vulnerability examples in their training courses.

It's clear that simply providing static, non-interactive training (which is typically the experience for compliance training) has little value in terms of repeatable developer security skills. Instead, organizations should focus on things like just-in-time training, where developers are taught about security as they work. You might even consider implementing a tiered learning program.

With a tiered approach, larger topics are typically broken down into discrete learning experiences or concepts. As developers progress, more advanced concepts are layered on top of those already mastered, just like physical scaffolding is constructed as a building grows higher. This makes for a proven method to teach a difficult and constantly evolving topic like cybersecurity, by first breaking it down into smaller, less complex chunks and then building more complexity on top of that foundation.

However you decide to approach your developer security skills program, keeping it separate from compliance exercises will be key. Both compliance and security training are important, and both require different approaches to achieve success.

It's clear that simply providing static, non-interactive training (which is typically the experience for compliance training) has little value in terms of repeatable developer security skills.

For further reading

Whitepapers

The challenges (and opportunities) to improve software security

The preventative, developer-driven approach to software security

Report

The state of developer-driven security 2022

Visit our case studies to find out how we're helping to empower development teams in their quest to write secure code from the start of the SDLC.

About Secure Code Warrior

Smarter, faster secure coding

Secure Code Warrior builds a culture of security-driven developers by giving them the skills to code securely. Our flagship Learning Platform delivers relevant skills-based pathways, hands-on missions, and contextual tools for developers to rapidly learn, build, and apply their skills to write secure code at speed.

Established in 2015, Secure Code Warrior has become a critical component for over 450 enterprises including leading financial services, retail and global technology companies across the world.