BRIEF

Establishing a cohesive approach to developer-led security

In response to major security breaches like the SolarWinds campaign, which used a software update process to infect over 18,000 users of the popular Orion management software, including many top corporations and government agencies, there is an increased push for more effective developer-led security efforts. Organizations of all sizes are starting to question their 'software supply chain', and demanding that the developers making their software have verified security skills and awareness.

Even the United States government is calling for better developer-led security practices and a strengthening of the software supply chain. Those concepts are a key component of an Executive Order on Improving the Nation's Cybersecurity issued by President Biden.

Overall, the developer community has been receptive to the idea of shifting security to earlier in the software development lifecycle (SDLC) through programs and movements like DevSecOps. And when recently surveyed, the developer community said that they valued the security training that they received to support that effort.

Software vulnerabilities continue to be exploited, and even developers admit that they sometimes leave 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).

The survey confirmed that writing quality code was a top priority for the development community. However the survey also identified several reasons why the training being given to developers, while seen as valuable, is nevertheless falling well short of the goal of helping to secure the software supply chain. 33% said that they were still leaving vulnerabilities in their code because, even after whatever training was provided, they still did not know how to identify or fix known vulnerabilities. And an overwhelming 92% said they needed at least some level of additional training in security, while 50% said that a lot more training was required.

It's clear that the developer community values whatever training they are being given. However, when questioned about the barriers to adoption of secure coding practices, a lack of time was cited as the number one reason, followed by a fifth of respondents citing a lack of a cohesive approach as the culprit. Training was seen more as a one-off event instead of a part of an ongoing strategic effort to incorporate security into developer workflows and utilized on a daily basis.

As such, developers aren't enabled to build and retain secure coding skills as part of a cohesive and ongoing program across their organizations. We can also conclude that the training currently received is not particularly effective or comprehensive given that many developers say they still can't identify and fix common vulnerabilities.

92% **of developers said they needed at least some level of additional training in security, while 50% said that a lot more training was required.**

What can organizations do to fix the situation?

> It's interesting that developers overwhelmingly said that they needed more security training. And while they valued the training they received, that might be a situation where they are simply happy with whatever they can get.

When asked to comment on ways to improve their training, their real thoughts on the issue began to surface. In general, most of the training that developers received was limited, non-interactive, only somewhat targeted at their job responsibilities, and not part of an overall or ongoing plan to help improve their organization's security skills and awareness.

According to the developers surveyed, if organizations want to improve the effectiveness of the training being offered, it should be presented as one part of a comprehensive approach to promoting a greater emphasis on security throughout the SDLC. In addition, developers had specific requests to make their training more valuable. One of the most popular suggestions was to include more use cases and hands-on examples of situations they were likely to encounter from a security perspective. Another popular response to improve effectiveness was for education to eventually cover increasingly complex or difficult scenarios – a move that would likely also require a more cohesive approach and a long term plan for continual learning and skills development.

Developers also stressed the need for more interactivity and maybe even adding a competitive element. In general, training where users simply watch a video or listen to a lecture with no opportunity for hands-on, contextual learning is not seen as effective or especially valuable when trying to teach a complex and (perceived to be) difficult skill like secure coding.

Developers also stressed the need for more interactivity and maybe even adding a competitive element.

What other elements are important when adopting a cohesive security approach?

> Training is of course critical when trying to improve the security awareness and skills of an organization's developer community. And ensuring that learning is ongoing, interactive, relevant, and contextual is a necessity. But a truly cohesive approach to better security awareness goes even beyond that.

A truly cohesive approach must consider what is needed to foster a genuine developer-led security culture. It may require changing the focus from the typical ways of managing and building developer teams. For example, developers have traditionally been evaluated based on how quickly they could code. But a cohesive approach to security might involve changing those long held metrics and values. Instead, evaluations could shift emphasis away from rewarding raw speed and instead reward those developers who can create quality code that is also secure - meaning that it is free from vulnerabilities.

It could also involve the developer community itself as part of the effort. Instead of simply mandating security to developers, consider creating or appointing security champions from the community. These would be talented and security aware developers who distinguish themselves either in training or as part of the newly focused metrics evaluations. They should also be willing to help other developers enhance their skills, thus improving the development community from within.

It's an increasingly effective part of a cohesive approach to security. According to the Gartner security research firm, the best security champions from development communities are organized and proactive, enthusiastic about security, and work well in collaborative environments. They are team players, and alongside better training and support, can help your organization better focus on creating a powerful and robust developer-led culture of security.

A truly cohesive approach must consider what is needed to foster a genuine developer-led security culture. It may require changing the focus from the typical ways of managing and building developer teams.

For further reading

Whitepapers

The challenges (and opportunities) to improve software security
The preventative, developer-driven approach to software security
The DevsSecOps Super Bowl: How security champions can support your team

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.