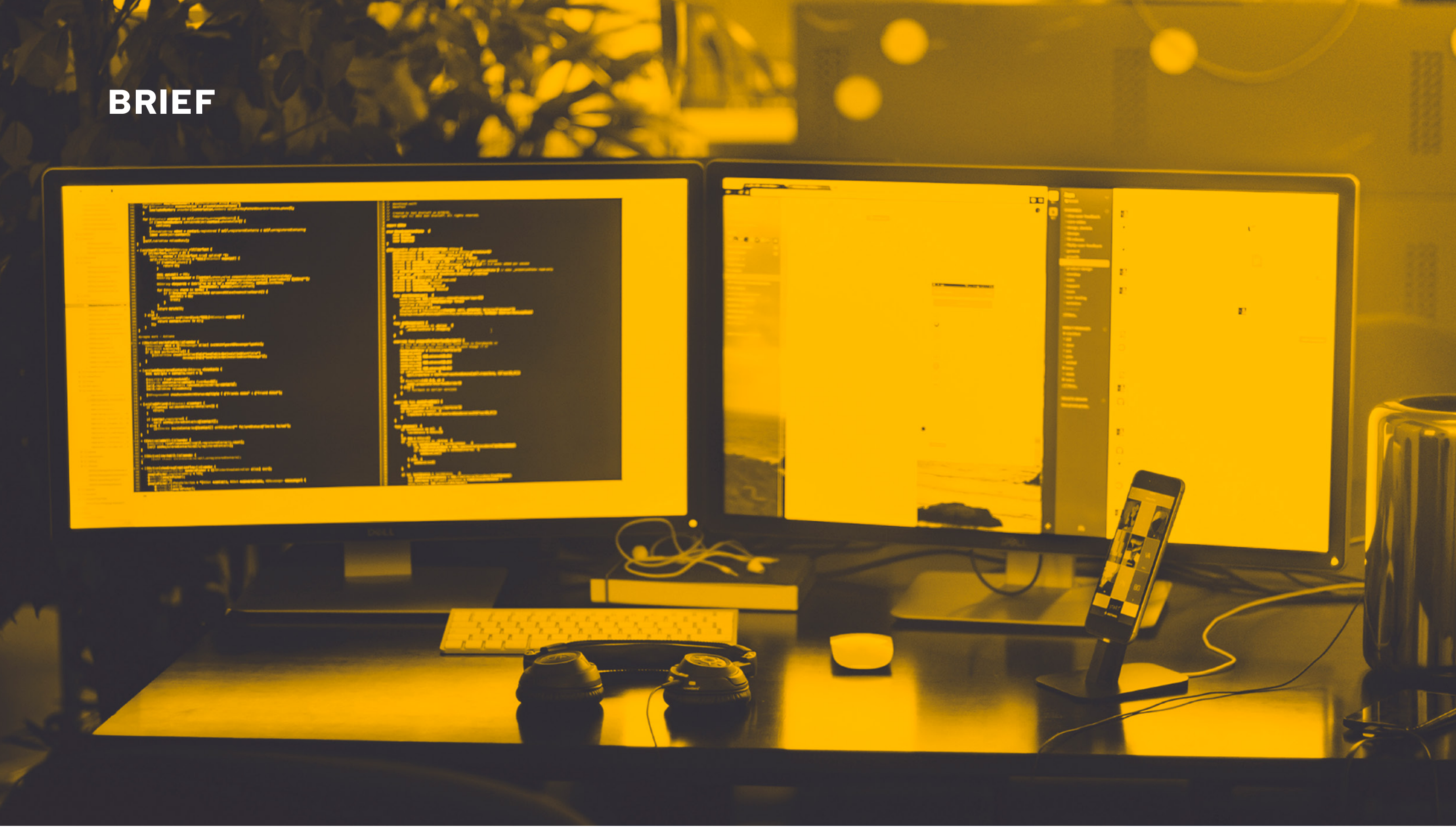
BRIEF



Why you need more than scanning tools to create secure code

For many years, scanning tools have been used to find vulnerabilities in software as an inherent part of the development process to ship 'quality' code. A recent report revealed that the application security tools market is tracking for **'explosive' growth between now and 2025**, a strong indication of their undisputed role in successful DevSecOps practices, and increasing industry relevance in the face of growing volumes of code with potential security vulnerabilities.

But, as cybercriminals become increasingly sophisticated in how they find and exploit vulnerabilities to their advantage, organizations cannot continue to rely on scanning tools alone, as they may have done in the past.

SECURE CODE WARRIOR

Why?

Many reasons. Starting with a statistic from the IBM Security Intelligence Index Report which highlighted that almost half of all successful data breaches are directly related to software vulnerabilities (known and unknown). Combine that figure with the fact that scanning tools can only detect *known* vulnerabilities, and that threat actors continue to evolve their methods of exploitation, and it's clear that organizations need a more comprehensive approach to ensure code security.

3 reasons why you need more than scanning tools to deliver secure code, fast

1. **There are a lot of false positives (and negatives)**
2. **The real bugs need to be manually sorted from the phantom bugs, which eats into already stretched man hours**
3. **Scanners find, they don't fix**

There is no singular tool that will find every vulnerability in every language and every codebase, and studies like this one demonstrate that tools only cover a relatively small percentage of potential flaws and zero-day threats. Adding more tools means a security tech stack can become bloated and ineffective, essentially delaying vulnerability remediation and software release velocity.

Not to mention the additional time and resource required to set up and run multiple tools, which will in turn place further burden on already strained resources in reviewing an abundance of false positives (and false negatives).

Scanning tools find, but they don't fix, and false positives/negatives due to coding errors (which are simple fixes for a security-aware developer) are a drain on security experts that could be spending their time on hairier security issues.

The shift to DevSecOps

The two key benefits of DevSecOps are *speed* and *security*. When done correctly, development teams deliver better, more secure code - faster and cheaper. A true DevSecOps approach considers 'people' to be as fundamental as tools and processes in order to be successful.

The concept of security being everyone's responsibility is starting to be widely recognized, and implementing tools as part of a secure development process will continue to play a significant role in the fast delivery of secure software. But in order to conquer threat actors that often use advanced technologies like artificial intelligence to scan for and exploit previously unknown vulnerabilities, organizations need to leverage and enable their developers to be the first line of defense.

Those who know software best are the developers who have painstakingly created it. They have powerful knowledge on how users interact with it, where the features are used, and when sufficiently security-aware, they can recognise potential scenarios where it could break or be exploited.

With the right skills and resources, security-enabled developers can eliminate common vulnerabilities and recognise potential exploits to reduce risk at the start of the software development lifecycle (SLDC), allowing teams to reduce the reliance on tools and increase release velocity with less rework.

> **“If you start secure, you don't have to 'become' secure – the latter is a lot harder to achieve. It reduces developer workload and work time. It reduces the risk of revisiting issues and trying to put in place a fix when the software is already live in people's environments. Doing it right the first time is key”** *SCW Customer.* ”

When developers are armed to find and fix potential vulnerabilities at the start of the development lifecycle you shift the balance of detection versus prevention, and significantly reduce risk. Take the examples of a global financial services SCW customer who saw a 50% reduction in software vulnerabilities within 3 months of their developers starting to learn how to identify and remediate insecure code.

Technology, people and process

It's long been recognized in cybersecurity strategies that technology, people and process each play an equal role in building a robust security posture.

Not only do tools only find/fix problems, but most aren't able to recommend solutions. Remediation advice given to developers can often be cumbersome and difficult to work into their tech stack causing further delays to release deadlines. Organizations looking to deliver secure software at speed must improve their DevSecOps capability (process) by balancing their reliance on scanning tools (technology), with security-aware developers (people) that have access to contextual, hands-on learning that build and grow skills as vulnerabilities and attack vectors evolve.

Security-aware and enabled developers mean that DevSecOps can reach its full potential, with alignment between developer teams and AppSec in a security-first culture that is prepared to tackle new and evolving threats (almost) as fast as they emerge.

Further reading

- SCW Case Studies
- If AppSec tooling is the silver bullet, why are so many companies not firing it?
- The DevSecOps Super Bowl: How security champions can support your team to victory against late-stage vulnerabilities

ABOUT SECURE CODE WARRIOR

Secure Code Warrior makes secure coding a positive and engaging experience for developers as they increase their software security skills. Our flagship Learning Platform delivers relevant skills based pathways for developers to write secure code at speed; whilst intelligent and contextual developer tools fix security flaws in real-time.

Our vision is to inspire a global community of security-conscious developers to embrace a preventative, secure coding practice that enables them to ship quality code faster - so they can create kick-ass software whilst benefiting from improved productivity, reduced costs, lower risk and easier compliance. Established in 2015, our customers include major financial institutions, telcos, retail, governments and global technology companies across Europe, North America and Asia-Pacific.

info@securecodewarrior.com

securecodewarrior.com