VERACODE

# Generative AI's Role in Secure Software Development

## Brian Roche, Chief Product Officer of Veracode, on Emerging "Security by Design" Considerations

iSMG
INFORMATION SECURITY
MEDIA GROUP

VERACODE

**BRIAN ROCHE**

*With over two decades of experience in engineering leadership positions, Roche leads agile organizations, implements DevSecOps, and delivers SaaS-based solutions with global teams at scale. He has held several leadership positions at EMC, Cognizant and most recently at Medidata.*

Developers want to move quickly and they want security to be “a natural part” of every step in the software development life cycle. Generative AI can play a pervasive role in helping cybersecurity keep up the pace, according to **Brian Roche**, chief product officer at Veracode.

“Generative AI will be part of everything we do, part of developers’ vernacular and the way that they work from now into the future,” he said. Ultimately, the goal is to not trade speed for secure code, he said. In this video interview with Information Security Media Group at RSA Conference 2023, Roche also discusses:

- The “relentless pressure” to get software to market quickly;
- The role of generative AI in software security by design;
- Veracode’s AI solution that produces “fixed recommendations for developers.

## DELIVERING SECURE CODE QUICKLY

**VARUN HARAN:** What are the biggest challenges that face the software industry today?

**BRIAN ROCHE:** The focus right now is on developers being able to deliver secure code quickly. It’s been that way for the past 10 years.

> “The patterns of behavior for developers are transitioning from monolithic, architected applications to microservices-based applications and, ultimately, they want software security to be a natural part of every step in the SDLC.”

There’s relentless pressure to get to market fast. And more recently, there’s been a lot of buzz around AI and ML, which are not new. But we’ve all heard about ChatGPT and that has really changed the industry for a lot of us. That’s what we’re going to talk about today – how that enables developers to innovate more quickly while simultaneously reducing software security debt. So a lot has changed, but a lot is still the same.

## HOW GENERATIVE AI CAN HELP

**HARAN:** It has been a binary or an exclusive choice, saying either you go for speed or you go for security, but not both. And if you do both, it’s going to really drag. The need today is to do it on the fly continuously. What role do you think generative AI is going to play in securing software?

**ROCHE:** Generative AI is going to be part of everything that we do, part of developers’ vernacular and the way that they work from now into the future. Veracode’s mission is to be the platform that brings together software developers and software security professionals so that they can deliver a software more quickly. And with the introduction of our Veracode Fix product, we now enable developers to innovate more quickly while simultaneously reducing security debt, so we don’t have to choose between speed and secure code, which we had to do in the past.

The patterns of behavior for developers are transitioning from monolithic, architected applications to microservices-based applications and, ultimately, they want software security to be a natural part of every step in the SDLC. That’s where I see AI coming to bear – automating the deployment of containers and remediating containers that are not secure in production. AI and ML and large learning models will be pervasive without being invasive and will be part of every single step of the SDLC.

## VERACODE’S AI SOLUTION

**HARAN:** So far, the use of AI in software development has been restricted to just being an assistant or augmenting what the coder is doing, but here we’re talking about making security a big part of it. How is Veracode bringing AI into the entire concept of shifting security left or security by design? What is your AI solution all about?

**ROCHE:** It’s always been our mission to shift security as early as possible in the development cycle, and we’ve done so as best in class with static code analysis and software composition analysis, which are imperative today. But those are focused on finding and not on presenting automated remediations for developers. Today, we see developers uploading their code and ultimately their IP to a server, whereas Veracode's approach is much different. It's still based on the transformer architecture under the covers, so it has all the benefits of the GPT model, but it's on a curated dataset that's proprietary to us. So we're not testing or refining this on our customers' code. We've got a finely tuned data set that we use to produce fixed recommendations for developers.

**HARAN:** So, it's an applied AI use case trained on Veracode's decades of data

**ROCHE:** That's right.

## APPLYING AI THROUGHOUT THE SDLC

**HARAN:** In the next half decade or so, is there going to be a need for IAST and DAST code review, or is it just completely going to shift to AI?

**ROCHE:** Everything is going to change. You're going to see new technologies become part of our vernacular and our workflow. You're going to see AI and ML become a part of the natural development of the SDLC. We're going to look to prevent the import or the ingestion of open-source libraries that are not secure, because what's better than trying to scan code is to prevent it from ever being brought into the codebase. We'll have the ability to identify drift in production so you can identify a container – or any of its dependencies – that are not secure and be able to remediate that or present a potential fix to a developer. We're going to be a natural part of the SDLC, as we were in the past, but we're going to bring AI to bear in every single one of those steps.

Technology is changing, and AI and ML can help solve the problems that we've been struggling with. There's not a single customer that I meet with or a single developer that says, "I feel good about my security posture. I feel like I'm burning down that technical debt." Most of them are not. So this is an opportunity for us now to bring a technology to bear to enable them to innovate more quickly and not have to choose between secure software and delivering software quickly. Speed and time to market is a differentiator, and that's what we're all trying to do.

> "This is an opportunity for us now to bring a technology to bear to enable developers to innovate more quickly and not have to choose between secure software and delivering software quickly."

# Veracode Envisions a World Where Software Is Developed Secure From the Start

Securing software is no small task. That's why Veracode was created. We help you easily integrate application security into your software development life cycle. Working with your developers in the environments where they work. Securing open-source libraries. Educating your developers so that development is secure from the start. Connecting your security and development teams, ensuring compliance to policy.

Click here to learn more: **www.veracode.com**

## About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU INFO SECURITY® Just for Credit Unions GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk® TODAY CAREERS INFO SECURITY® Data Breach. TODAY Prevention. Response. Notification. CyberEd.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io