AI and the journey to secure software development

Automation is evolving from identifying vulnerabilities to providing seamless, AI-assisted developer workflows

Joel Krooswyk
GitLab

THE DRIVE TO SHIFT SECURITY LEFT IN THE development process has been highly effective. But it has also created more work for developers, who might spend several hours trying to resolve a single vulnerability in their codebase. As a result, some days developers can devote only a fraction of their time to actually writing code.

By automating and optimizing DevSecOps workflows, we can still shift security left while relieving developers from the burden of some complex remediation. It begins with a workflow that leverages fully automated security scanning to rapidly identify vulnerabilities as well as providing suggested remediation for vulnerabilities and on-demand remediation training to educate developers on what they are getting into.

MINIMIZING THE SECURITY BURDEN FOR DEVELOPERS

The rapid evolution of artificial intelligence is making new advances possible. The opportunities go well beyond AI-assisted code creation. AI features are being expanded across the entire software development life cycle. When it comes to security, having AI assist by making code functionality clear or explaining a vulnerability in detail reduces the time required to remediate risk.

According to GitLab's 7th annual Global DevSecOps Report: Security Without Sacrifices, developers who use a DevSecOps platform were more likely to have implemented automation and AI/machine learning for testing than those who do not. In fact, 62% of developers leveraging AI use it to check code, up from 51% in 2022.

The next leg of this journey, which is already underway, brings AI assistance into the remediation process whenever possible. In this scenario, AI not only suggests a fix but may give developers the option to apply that fix with the click of a button. Auto-remediated code would still be subject to existing code review and approval processes, providing human validation of the fix.

I'm excited about the implications for efficiency, enabling developers to focus on innovation rather than remediation.

TRAINING MODELS ON THE RIGHT DATA

Additionally, it is vitally important to think about how these AI models are trained. What datasets are the models pulling from? Is the information coming from a trustworthy source? How is data privacy handled?

Generative AI needs to be grounded in privacy, security and transparency. Secure, AI-powered features are dependent on the data and the environment in which they exist. Furthermore, because the technology supports the entire software development life cycle, it's not just a matter of training AI on data, but appropriately applying AI at each stage of software development.

Ultimately, the explosion in AI adoption will help drive a transformational approach in which an AI-assisted DevSecOps platform ensures scale, security and compliance for mission-critical software. ■

Joel Krooswyk is federal CTO at GitLab.