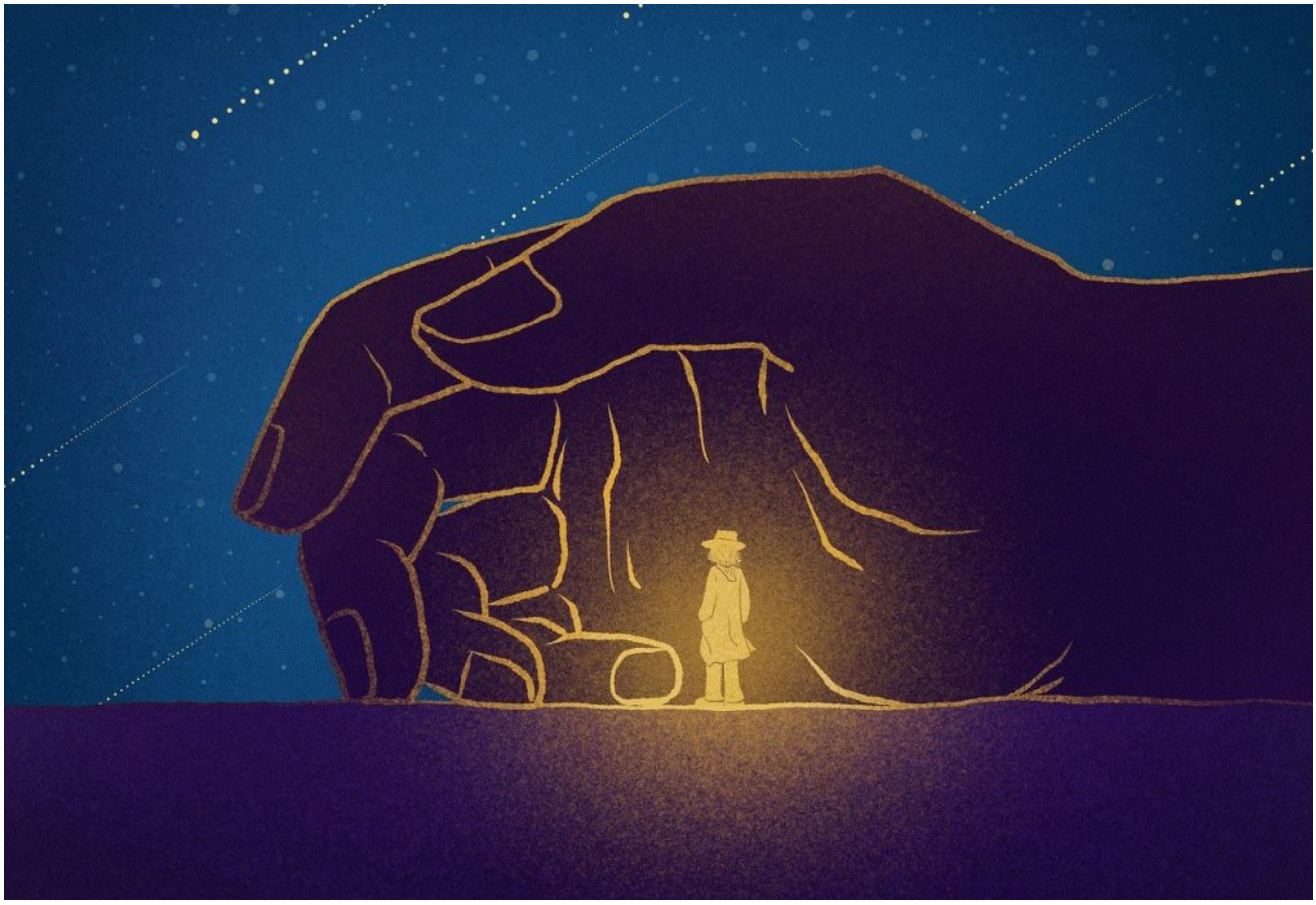
THENEWSTACK

AI / DEVOPS / SECURITY / TECH CAREERS

Will Generative AI Kill DevSecOps?

GenAI isn't going to run DevSecOps off, but it certainly is making them run down. How can security teams keep up with this speed of code?

Feb 15th, 2024 3:00am by Jennifer Riggins



THENEWSTACK

We'd love to hear what you think.

LONDON — The majority of your engineers are already using generative AI. By now, they're likely to have experienced dramatic developer productivity and job satisfaction gains, or at least a decrease in cognitive load. GenAI has become the new Stack Overflow that developers rely on for fast answers. But with great speed, comes great risk.

Last year, researchers at Purdue University found that ChatGPT's code was wrong 52% of the time. Last month, GitClear released a report that uncovered an overall decrease in code quality due to an over-reliance on GitHub Copilot.

The core problems behind both pieces of GenAI research are:

1. A chatbot is trained to give a persuasive answer whether it knows the correct one or not.
2. A chatbot's response is based on the probability of being accepted, not on its accuracy or on how it fits within the context of your overall codebase.
3. A chatbot does not consider the perspective of long-term code maintainability, leading to simply more code and technical debt being created.
4. The speed at which generative AI assists in code creation makes it nearly impossible for DevSecOps teams to keep up.

"Is generative AI safe to run in production?" Hannah Foxwell, product director at Snyk, rhetorically posed at the State of Open Con last week. No matter the size or vertical of your organization, she reflected, "These tools are so, so powerful, they make you so, so much more efficient, that AI-generated code will be running in production, whether you officially allow it or not, because your developers will find a way to use it, whether you allow them to or not."

Foxwell sat on a panel along with Snyk colleague and senior security advocate Sonya Moisset, and GitLab solutions architects Dominique Top and Stefania Chaplin, to explore how GenAI affects the aims of DevSecOps, which looks to integrate security throughout the software development lifecycle (SDLC).

In short, it's changing everything. Even if you can keep your developers from feeding sensitive information into these large language models (LLMs), the velocity of generative AI adoption puts all organizations' security at risk. Making the role of DevSecOps professionals — as facilitators of communication and collaboration between teams — even more essential. Let's talk about what DevSecOps practitioners are facing and how they can best proceed — with caution — in this Age of GenAI.

Is Speed the Problem?

Foxwell called generative AI for software engineering a "step change in velocity." Top said the whole industry will be transformed beyond recognition. But while we are still working out the use cases and benefits of generative AI, there's no doubt that it's making the role of the DevSecOps professional so much tougher.

5. Penetration Testing with Kali Linux as a Docker Container

More than half of cybersecurity professionals are burnt out. Add to that, there are 3.4 million cybersecurity job openings leaving them understaffed.

"These teams were already struggling to keep up with the pace of developments — the complexity of environments, the sprawl of technologies," Foxwell said. "I think it's a compounding effect on the security teams I talk to who were already struggling with the velocity of development."

After a year of obsession with developer productivity, this begs the question if we as an industry are moving too fast just for fast's sake. Or if we are trading developer burnout for security burnout.

"Everybody is really focused on: How can we enable our developers to go really quickly?" Top said. "At a significant amount of organizations, the security people are like: Hold on a minute. What are we doing here? Why are we doing this? Can we please just have a look at why we are doing this, like inserting AI in something?"

Over the past year since ChatGPT was released, she reflected, most companies are rushing into an "early adopter mindset" when security is still opaque. "We still rely on our security teams to make sure that what does get released into production is safer," but "trying to keep up with that rate of change is difficult."

Still, GenAI is here to stay — developers are not going to easily give up these productivity wins. So what's a DevSecOps pro to do?

Can AI-Generated Code Be Trusted for Critical Applications?

Now that there's more code being "written" than ever before, DevSecOps automation becomes even more crucial. Except that security automation relies on a deep understanding of your systems. But, with GenAI, you don't often know what's under the hood.

did.

We're at the very early stages of this technology, she reminded the State of Open Con audience, still figuring out what, if any, degree of control we have over it.

Moisset added that, while it's not a guarantee, a good decision influencer is considering if the creators of these LLMs even have public AI ethics principles.

"I'm very much of the opinion that you should never trust something that's auto-generated," Top said. "You don't know where it's coming from. You don't know what the basis of it is, which is why organizations need to build processes and habits around double-checking everything."

Don't just run security scans on your code, but try to understand what the GenAI tools themselves are doing.

"Say I'm looking underneath for how is this code populated. Is it some training set based on a lot of open source repos? A lot of them are not secured because they haven't implemented security," Moisset said, so you should "scan your security tools to make sure that code has the same level of security that we have within our pipeline."

DevSecOps Must Do Better

Beyond having automation and guardrails in place, you also need security policies at the company level, Moisset said, to make sure that DevSecOps understands all the generative AI tools colleagues are using. Then you can educate them on how to use it, like creating and communicating a generative AI policy.

Because a total ban on GenAI just won't fly. When Italy temporarily banned ChatGPT, Foxwell said there was a visible decrease in productivity across the country's GitHub organizations, but, when it was reinstated, "what also picked up was the usage of tools that circumvented all of the government policies and firewalls around the prevention of using these" tools.

Engineers always find a way.

chatbot.

"It's back to educating the users and developers that it's good to use AI, we should be using AI, but we need to actually put guardrails around it," she said, which also demands an understanding of how your customers interact with GenAI.

A theme throughout the panel was that security folks aren't just there to do but rather to teach. This includes continuously reminding staff to not put sensitive information into generative AI, like private information, proprietary code or API keys.

Sure, there will be mistakes, but it's the job of DevSecOps teams to shine a light on those mistakes in order to foster collective learning. When things go inevitably wrong, maintain a blameless culture where nobody is at fault.

As Foxwell put it, reframe your questioning: "What system was in place that allowed that problem to occur and what can we do better next time?"

How Can DevSecOps Help Itself?

"DevSecOps is about people, process and technology — in that order," Top said.

In a world where AI plays an increasingly important role, Chaplin asked what skills and expertise will be more valuable to DevSecOps practitioners.

"Have some basics around AI and Ml. I'm not talking about having a PhD in those domains, but just having a basic understanding of what is going on, how it works," in order to assist collaboration and communication between teams, which Moisset said is the crux of the DevSecOps role.

No matter which tool your organization is adopting, she said, that communication must include why you're adopting a tool — or why you shouldn't — especially when it is helping make devs' AI usage more secure.

But that could backfire too.

adoption of your security practices, you end up with blind spots and introduce risk, so we need to make it really easy for developers to adopt good security practices — and that comes down to automation."

Just make sure that security automation doesn't unintentionally slow developers down by creating a lot of irrelevant noise via a thousand JIRA tickets. She emphasized that not all AI risks are equal, especially within the context of your organization, so be very intentional about what gates and guardrails you implement.

"It's about interpreting all of that data that you can gather through automation, and then really being very specific about what risk that is and how you need to fix it," Foxwell said. It's the job of DevSecOps, she continued, to compound the existing security bottlenecks as well, as they'll be perceived as a greater offense in contrast to AI making software development so much faster.

It's also up to the DevSecOps team to examine all the pieces of the software development lifecycle puzzle, Top added, including performing value stream assessments and Wardley mapping in order to gain a better understanding of the relationship between each sociotechnical segment of your organization. It's especially important to understand, she continued, what each developer is putting into the continuous integration pipeline — are things still getting deployed via a toss over the fence? Does it just get thrown back if things go wrong?

In the Age of AI, cross-organizational empathy is a crucial skill for DevSecOps professionals.

How Can DevSecOps Support GenAI Adoption?

One of the biggest concerns of the panelists was about the career path of junior developers — who aren't always considered in DevOps optimization. In particular, Top is worried that more senior engineers will look at the chatbots as a way to cut back on some mentoring duties, versus the power of having "a meaningful conversation with another human who has the experience, who has seen it being deployed into production at large organizations or small organizations, having different points of view."

facilitate this change, makes sure we still nurture young talent to the point where they can actually have career progression."

As developers, especially more junior devs, grow an over-reliance on GenAI, there is a concern that they aren't making a habit of double-checking their work and the bots' work.

"Whether it's coming from Stack Overflow or other sources, you actually need to scan that piece of code just to make sure that it follows your policies," Moisset said. "So we need to have automation and you have to create tools that place that within your pipeline."

How Can GenAI Assist DevSecOps?

It's not all about risks. generative AI has the potential to help devs learn more about their code in a conversational manner — which in turn gives it the potential to increase security.

"How can we support anyone in the software developer lifecycle by using some AI-related things?" Top considered, pointing to some early GenAI wins like issue summaries, documentation, and summarizing cross-functional and customer conversations. She also sees a future where devs can use GenAI for "explaining vulnerabilities like: What part of my code is wrong? What's the potential impact of what I'm trying to release into the wild?"

Of course, success with this, she continued, all comes down to making sure the models aren't being trained to be biased or compromised, which the C-suite seems completely unprepared to deal with. She recalled being recently at a roundtable where a CTO was all-in on everything generative AI, while the CISO wanted to block everything for fear of malicious intent. "So I'm interested to see what kind of protection or additional pieces of software people are writing like frameworks to make sure that it's all becoming safer."

DevSecOps teams don't just need to be concerned with the software developer lifecycle, but with how the whole organization is engaging with this new technology like never before.

DevSecOps teams are already using applications with AI, like Darktrace and Crosstrek. Moisset says it's up to the DevSecOps team to train the users — the "sec allies" — to leverage these new tools too.

For right now, DevSecOps will be writing a lot of tests, but, in the future, Howell predicts "the models will get better and they'll be able to correct themselves." Quality is coming.

Despite the nature of security professionals who are constantly searching for weaknesses, the panel ended on an optimistic note. Generative AI will likely transform DevSecOps, but it's not going to assist them out of a job.

As Top said, "I do strongly believe there's always going to be a need for human intervention."

TNS

Jennifer Riggins is a culture side of tech storyteller, journalist, writer, and event and podcast host, helping to share the stories where culture and technology collide and to translate the impact of the tech we are building. She has been...

Read more from Jennifer Riggins →

TRENDING STORIES

1. Best Practices for Storing Access Tokens in the Browser
2. Will Generative AI Kill DevSecOps?
3. Linux: Create Encrypted Tunnels with SSH Port Forwarding

THENEWSTACK

INSIGHTS FROM OUR SPONSOR

garden

Garden's DevOps platform simplifies environment management and testing for cloud-native apps. We're improving the developer experience and speeding up the software delivery cycle by reducing friction, CI bottlenecks, and context-switching overhead.

Learn More →

One year of remote development environments on K8s | garden.io
8 January 2024

Cross-cutting concerns in microservices development | garden.io
8 January 2024

Continuous Integration tools: Are we too dependent on them? | garden.io
5 January 2024

Developer velocity: Encouraging efficiency and top performance | garden.io
5 January 2024

Developer productivity tools: A different approach in 2024 | garden.io
5 January 2024

Preview environments: Everything you need to know | garden.io
5 January 2024

FOLLOW TNS

TNS DAILY

THENEWSTACK

A newsletter digest of the week's most important stories & analyses.

EMAIL ADDRESS

SUBSCRIBE

ARCHITECTURE

Cloud Native Ecosystem
Containers
Edge Computing
Microservices
Networking
Serverless
Storage

ENGINEERING

AI
Frontend Development
Software Development
API Management
Python
JavaScript
TypeScript
WebAssembly
Cloud Services
Data
Security

FOLLOW TNS

TNS DAILY

Tech Careers
Tech Culture
DevOps
Kubernetes
Observability
Service Mesh

Newsletter
TNS RSS Feeds

THE NEW STACK

About / Contact
Sponsors
Sponsorship
Contributions

FOLLOW TNS

Disclosures Terms of Use Privacy Policy Cookie Policy