

David DeSanto, GitLab: AI's impact on software development in 2024



About the Author

By Ryan Daws | 7th December 2023

Categories: Approaches, Artificial Intelligence, Developer, Development Tools, DevOps, Hacking & Security,



Ryan is a senior editor at TechForge Media with over a decade of experience covering the latest technology and interviewing leading industry figures. He can often be sighted at tech conferences with a strong coffee in one hand and a laptop in the other. If it's geeky, he's probably into it. Find him on Twitter (@Gadget_Ry) or Mastodon (@gadgetry@techhub.social)

David DeSanto, Chief Product Officer at [GitLab](#), foresees a paradigm shift in the realm of software development in 2024—with AI taking centre stage.

GitLab's [2023 Global DevSecOps Report](#) serves as the foundation for these predictions, offering a glimpse into the future landscape of organisations' software development toolchains.

AI bias: A hurdle on the path to progress

In the short term, the accelerated integration of AI tools may present a formidable challenge: an upswing in biased outputs.

As AI services draw from the internet to build their training data, inherent biases woven into the fabric of the online world may seep into these tools.

DeSanto contends that this transitional phase – marked by biased outputs – will catalyse the establishment of rigorous ethical guidelines and targeted training interventions. This, in turn, will bolster the discernment and impartiality of AI tools.

Code testing workflows

The trajectory of AI's evolution in DevSecOps is poised to reshape code testing methodologies. Currently, half of all testing involves AI—a figure projected to surge to 80 percent by the close of 2024, heralding a near-complete automation within two years.

While this promises heightened productivity and accuracy, organisations must grapple with aligning existing processes with the efficiency and scalability offered by AI. This shift demands a reevaluation of traditional testing roles and practices.

Threats to privacy and IP

As AI-powered code creation becomes a staple in organisations' software development practices, the looming spectre of significant AI-introduced vulnerabilities and intellectual property loss comes into focus.

Without concerted efforts to fortify privacy measures and safeguard intellectual property, the industry faces potential repercussions for software security, corporate confidentiality, and customer data protection.

AI integration: From luxury to standard

2024 is earmarked as the year when AI integration transcends luxury, becoming a standard practice. More than two-thirds of businesses are expected to embed AI capabilities within their products and services.

This seismic shift signifies a transformative phase, with companies evolving into AI-centric entities. Organisations will leverage the technology not just to stay competitive but to drive innovation and deliver enhanced value across all market sectors.

As the digital landscape undergoes this profound transformation, businesses must navigate the challenges posed by biased outputs, adapt to the evolving role of AI in code testing, and fortify safeguards against potential threats to privacy and intellectual property.