# The evolution of DevSecOps: Integrating AI for enhanced security



In the rapidly evolving landscape of software development, security has transcended its previous status as an afterthought to become a pivotal requirement, especially in the realm of B2B software. The DevPro Journal has gathered insights from industry experts who discuss the significant trends reshaping DevSecOps as we approach the year 2025. These insights reveal how the integration of artificial intelligence (AI) is set to revolutionise operational patterns across various sectors.

One of the primary shifts anticipated in 2025 is the transition from a "shift-left" approach to a more comprehensive "shift-everywhere" philosophy within DevSecOps. Dylan Thomas, Senior Director of Product and Engineering at OpenText Cybersecurity, described this evolution as essential for organisations striving to enhance their security practices significantly. He explained that leveraging the right tools at appropriate stages of the DevSecOps cycle will yield improved efficiency. Thomas elaborated on the role of lightweight analysis in integrated development environments (IDEs) which will enable developers to catch potential security issues early in the development process. Further, he noted the importance of automation in pull requests and continuous integration/continuous deployment (CI/CD) pipelines, with a focus on core functions such as Static Application Security Testing (SAST), Software Composition Analysis (SCA), and increasingly, Dynamic Application Security Testing (DAST) for API security.

Thomas emphasised the transformative role of generative AI in accelerating DevSecOps automation and scalability. As this technology increases the pace of software production, the need for mature DevSecOps environments becomes even more crucial to ensure ongoing security integration. He stated, “Intelligent use of generative AI will also address persistent challenges, such as the scarcity of security experts, by automating the review and remediation of code vulnerabilities.” Moreover, organisations that embed generative AI into their software will encounter new security risks, necessitating innovative solutions that redefine DevSecOps maturity.

The importance of log data in the observability landscape was underscored by Joe Kim, CEO of Sumo Logic. He highlighted that the surge in digitalisation witnessed throughout 2024 has heightened the necessity for collaboration between development, security, and operations teams. This teamwork is vital for addressing pressing issues concerning technology and security operations. Kim pointed to the rise of AI-powered observability platforms that leverage both traditional AI and machine learning (ML) alongside generative AI technologies. As he noted, “In 2025, the insight that resides in organisations’ structured and unstructured log data will be unlocked,” thus presenting opportunities for deeper analysis and understanding of applications and digital services. By the end of 2025, such capabilities may also integrate with business analytics to enhance "Customer Observability" — a concept aimed at facilitating better business decision-making.

Adding to the conversation, Tal Levi-Joseph, VP of Software Engineering at OpenText, stated that the dual forces of AI and DevSecOps will revolutionise the software delivery process, optimising speed and security. Levi-Joseph indicated that generative AI and large language models will be fundamental to automating testing procedures, thereby enhancing product quality and pinpointing risks. He described the ongoing journey towards a more autonomous delivery model, asserting that as security is seamlessly embedded into every development stage, organisations will better harness real-time customer feedback to provide solutions that offer substantive value.

This convergence of AI technology and DevSecOps principles underscores a significant paradigm shift within the software development industry, heralding a new era of innovation where efficiency and security operate hand in hand. With the integration of AI becoming increasingly central to these operations, businesses are poised to implement security measures that can adapt and scale alongside technological advancements, ensuring they remain resilient in the face of evolving threats.

Source: [Noah Wire Services](https://www.noahwire.com)

## References

* <https://dev.to/s3cloudhub/devops-technology-in-2025-trends-innovations-and-future-directions-16fc> - Corroborates the emphasis on DevSecOps practices, including security automation, compliance-as-code, and real-time threat modeling, as well as the rise of platform engineering and multi-cloud strategies in 2025.
* <https://www.devopsdigest.com/2025-devsecops-predictions-part-1> - Supports the role of AI in DevSecOps, including automation, vulnerability remediation, and the integration of security into every step of the development process.
* <https://www.devopsdigest.com/2025-devsecops-predictions-part-1> - Highlights the use of generative AI and large language models to automate testing, enhance product quality, and pinpoint risks, aligning with the shift towards autonomous delivery.
* <https://checkmarx.com/learn/appsec/features-the-best-devsecops-tools-will-have-in-2025/> - Details the must-have features for future-ready DevSecOps tools, including unified security, automation, AI, and seamless developer collaboration, as well as code-to-cloud security and CI/CD security.
* <https://checkmarx.com/learn/appsec/features-the-best-devsecops-tools-will-have-in-2025/> - Explains the importance of AI and machine learning in analyzing data, identifying patterns, and detecting zero-day vulnerabilities and advanced persistent threats in real-time.
* <https://www.enterprisesecuritytech.com/post/2025-tech-predictions-how-ai-and-devsecops-will-reshape-security-and-development> - Discusses the evolution of DevSecOps into an integrated model with embedded observability and security capabilities across the development lifecycle, and the role of AI in automating security checks and vulnerability scans.
* <https://www.enterprisesecuritytech.com/post/2025-tech-predictions-how-ai-and-devsecops-will-reshape-security-and-development> - Mentions the rise of AI-powered observability platforms and the integration of log data analysis with business analytics to enhance customer observability.
* <https://www.devopsdigest.com/2025-devsecops-predictions-part-1> - Corroborates the importance of collaboration between development, security, and operations teams, and the role of AI in streamlining processes and ensuring quality, performance, and security.
* <https://checkmarx.com/learn/appsec/features-the-best-devsecops-tools-will-have-in-2025/> - Supports the need for tools that foster collaboration, prioritize real risks, and integrate seamlessly into diverse ecosystems without sacrificing agility in DevSecOps.
* <https://www.enterprisesecuritytech.com/post/2025-tech-predictions-how-ai-and-devsecops-will-reshape-security-and-development> - Highlights the transformative role of generative AI in addressing persistent challenges such as the scarcity of security experts by automating the review and remediation of code vulnerabilities.