What is DevSecOps?

1 November 2026 · 5 min read · blogs.iictp.org/what-is-devsecops

DevSecOps means building security into the way software is developed and operated, instead of checking it at the end. Security checks run automatically in the delivery pipeline, and developers, operations and security staff share responsibility for the result.

TL;DR The short version

- DevSecOps builds security into how software is developed and run instead of checking it at the end.
- Pipelines run secret, dependency, code, image and infrastructure scans, with quick checks on every change and slower ones less often.
- Developers own the security of what they build, and progress is measured by how long findings stay open and how fast fixes ship.

Read online, listen to it, or change the text size: https://blogs.iictp.org/what-is-devsecops

What does “shift left” mean?

It means finding security problems earlier in the life of a change, when they are cheaper to fix. A flaw caught in a pull request takes minutes to correct, while the same flaw found after release can take days and may already have been exploited.

Which checks belong in the pipeline?

Common ones are secret scanning, dependency and licence scanning, static analysis of code, scanning of container images and infrastructure definitions, and tests that exercise the running application. Each should give fast, clear feedback to the developer who made the change.

How do you avoid slowing teams down?

Run quick checks on every change and slower ones less often, tune rules to reduce false alarms, and make failures easy to understand. If developers learn to ignore the tool because it is noisy, it protects nothing.

What does shared responsibility look like?

Developers own the security of what they build and fix findings in their own code. Security staff provide guidance, tooling and threat modelling, and set policy. Operations teams manage access, patching and monitoring.

How do you measure progress?

Track how long findings stay open, how many reach production, and how quickly you can ship a fix. These show whether security is keeping pace with delivery, whereas counting alerts or scans only measures activity.

Related credential: Certified Technical Practitioner. Explore the exam facts and syllabus.

Sources and further reading

1. OWASP. DevSecOps Guideline. owasp.org/www-project-devsecops-guideline/.
2. NIST. SP 800-218, Secure Software Development Framework. csrc.nist.gov.

Published by IICTP, an independent technical credential body, on 1 November 2026. The current version of this post is at https://blogs.iictp.org/what-is-devsecops. More guides: blogs.iictp.org.