GitLab

10 Tips for Shifting Left with GitLab and Deimos

Enable your teams to run faster and more efficiently

Cyber attacks and cybersecurity threats continue to be one of the highest priorities for organizations. As such, the developer's role continues to evolve. Over half of developers surveyed in GitLab's 2022 Global DevSecOps survey say that they are "fully responsible" for security in their organizations, a 14% increase over 2021 — signaling that security practices are continuing to shift left.

Shifting left — designing software with security best practices built in to detect and fix vulnerabilities earlier in the software development life cycle (SDLC) — enables teams to run more efficiently and release software faster.

While 57% of security team members told GitLab their organization has either shifted security left or is planning to this year, you may be unsure how to get started.

Here are 10 tips to help your teams shift left for more efficient DevSecOps.

1 Measure time

How much time is lost remediating vulnerabilities after code is merged? Measure this, then look for a pattern in the type or source of those vulnerabilities, and make the necessary adjustments for improvement.

2 Identify bottlenecks

Where are the pain points and bottlenecks between security protocols and processes? Identify these, and then create and execute a resolution plan.

3 Start small

Make small code changes — they are easier to review, secure, and launch more quickly than large project changes.

4 Eliminate waterfall

Are people still holding on to waterfall-style security processes within the SDLC? Eliminating or reducing waterfall will help your organization prevent the struggle to change direction as needs arise.

5 Automate scans

Are manual processes slowing down and hampering the process of discovering vulnerabilities? Automate findings into a merge request for easier review, finding sources, and accessibility for developers to address.

6 Update workflows

Are security scans included in your developers' workflow? Building and integrating security into developer workflows enable them to find and fix vulnerabilities before the code ever leaves their hands.

7 Demonstrate compliance

Is unplanned and unscheduled work delaying releases? Automating and implementing compliance frameworks help with consistency across development environments, teams, and applications.

8 Security Reports

Do your developers have access to SAST and DAST reports? These valuable tools help dev teams build secure coding practices, fixing vulnerabilities as part of their workflow.

9 Smarter teams

Empower the security team to work smarter with security dashboards into both resolved and unresolved vulnerabilities, where the vulnerabilities reside, who created them, and their status for remediation.

10 Ditch the toolchain

Streamline and reduce your toolchain so that employees can focus their attention on a single interface — a single source of truth.

Shift left with GitLab and Deimos

GitLab helps you initiate a proactive security strategy to discover vulnerabilities earlier in the SDLC. Security and compliance are embedded within The One DevOps Platform, with an end-to-end DevSecOps workflow that enables you to understand and manage risk. Automatically scan for vulnerabilities on a feature branch so you can remediate vulnerabilities before pushing to production.

GitLab empowers customers and users to innovate faster, scale more easily, and serve and retain customers more effectively. Learn more about how GitLab and Deimos can help you shift security left and secure your software supply chain.

Talk to an expert today >

DEIMOS