



DevSecOps Maturity Briefing

New Benchmarks for CIOs & CISOs

Executive Summary

In 2026, DevSecOps maturity is defined less by tool counts and more by how effectively enterprises integrate speed, security, and governance on a unified platform — a shift reflected in a decade of research linking platform practices to higher delivery performance and stability.

GitLab's 2025 Global DevSecOps report highlights an operational reality worth prioritizing: **teams are losing ~7 hours per person, per week, to process inefficiencies driven by fragmented toolchains**, AI-related bottlenecks, and compliance overhead. A large majority view platform engineering as the path to reclaim that time.

Leading CIOs and CISOs are responding with three moves: consolidate onto a DevSecOps platform to curb integration tax and improve visibility, embed supply chain assurance in pipelines, and measure time to security alongside industry metrics so velocity and risk improve together.

The takeaway is straightforward: **treat DevSecOps as an enterprise platform capability** — not a collection of tools — to reduce waste, tighten compliance, and demonstrate speed and security with board-ready metrics.



According to GitLab's 2025 Global DevSecOps report, **fragmented toolchains and compliance complexity cost teams ~7 hours per person, per week**

DevSecOps Maturity Model

This four-stage maturity model reflects how enterprises are evolving DevSecOps from fragmented execution to risk-adaptive delivery.

The stages are not tied to company size or industry. They reflect architectural and organizational choices that can be observed across regulated and non-regulated environments alike.

Stage 1: Tool-Centric Delivery

At this stage, DevSecOps is implemented primarily through disconnected tools and team-specific pipelines.

Security scanning is typically bolted on late in the development lifecycle, often after code has already been merged or deployed. Continuous Integration (CI) pipelines vary widely between teams, and there is little standardization of controls or reporting.

Common characteristics include:

- Multiple CI tools and security scanners with overlapping functionality
- Manual hand-offs between development and security teams
- Security findings that arrive late and generate significant rework
- Limited visibility for leadership into actual risk posture

Primary risk:

Security is a bottleneck rather than an enabler, and leadership lacks a clear, consistent view of exposure.

Also: Slow remediation; low signal to noise; duplicative spend

Key KPIs (baseline):

- Deployment Frequency (weekly-monthly)
- Lead Time for Changes (weeks)
- Change Failure Rate (>15%)
- Failed Deployment Recovery Time (days)



Executive Move:

Initiate portfolio-level tool rationalization and unified policy baseline.

DevSecOps Maturity Model

Stage 2: Shift-Left, with Policy as Code

Organizations at this stage move security earlier in the lifecycle and begin to standardize controls.

Security testing is integrated into CI pipelines, and policies are increasingly expressed as code rather than manual checklists. Software Bill of Materials (SBOM) is often generated during builds, though usage and enforcement may be inconsistent.

Common characteristics include:

- Integrated Static Application Security Testing (SAST), dependency scanning, and Infrastructure as Code (IaC) scanning in CI
- Policy checks embedded in pipelines rather than external reviews
- Early adoption of SBOM generation for first-party code
- Improved collaboration between development and security teams

Primary risk:

While detection improves, governance remains fragmented across tools, teams, and environments.

KPIs (target):

- Deployment Frequency (days-weekly)
- Lead Time (<1 week)
- CFR ($\leq 10\%$)
- Time to Remediate Criticals (<7 days)



Executive Move:

Fund platform runway (golden pipelines, shared runners, secrets management) and SBOM ingestion processes for vendor software.

DevSecOps Maturity Model

Stage 3: Platform Engineering and Continuous Compliance

At this stage, DevSecOps operates through a shared platform with built-in guardrails.

Rather than each team building and maintaining its own pipelines, the organization provides standardized, secure delivery paths that teams can adopt with minimal friction. Compliance evidence and audit artifacts are generated automatically as part of delivery.

Common characteristics include:

- Golden pipelines, paved developer paths
- Centralized policy with federated execution across teams
- Build provenance, artifact signing, and SBOMs generated by default
- Automated evidence collection for audits and customer reviews
- Clear executive visibility into delivery and security performance

Primary benefit:

Security and compliance become predictable outcomes of delivery, not separate processes.

KPIs (target):

- Deployment Frequency (daily)
- Lead Time (<1 day–1 week)
- CFR ($\leq 5\%$)
- Failed Deployment Recovery Time (hours)
- Rework Rate trending down



Executive Move:

Consolidate to a unified DevSecOps platform (reduce 25+ tools to single-digit core) and codify continuous compliance mapped to Secure Software Development Framework (SSDF) and sector frameworks.

DevSecOps Maturity Model

Stage 4: AI-Augmented, Risk-Adaptive Delivery

At the highest level of maturity, AI is used to accelerate delivery while governance adapts dynamically to risk.

AI assists with code review, test generation, and vulnerability triage, but human-in-the-loop controls remain mandatory for high-risk changes. Risk signals from across the pipeline influence policy enforcement in real time.

Common characteristics include:

- AI-assisted development embedded directly into pipelines
- Mandatory human review for security-critical changes
- Dynamic policy enforcement based on risk, not static rules
- Continuous compliance rather than point-in-time assessments

Primary outcome:

High-delivery velocity with defensible, measurable risk management.

KPIs (elite):

- Deployment Frequency (on demand)
- Lead Time (<1 day)
- CFR ($\leq 5\%$)
- Recovery (minutes–hours)
- Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR) for vulnerabilities measured in hours
- 7+ hours/week reclaimed from coordination waste



Executive Move:

Treat AI as a force multiplier with controls: mandate human review, expand red-teaming for AI outputs, and embed “trust but verify” workflows.

Benchmarks That Matter To Executives

Across mature organizations, a consistent set of benchmarks is emerging as meaningful indicators of DevSecOps health:

- Deployment frequency and lead time improve without increasing failure rates
- Change failure rate and recovery time are measured, tracked, and trending downward
- Rework caused by late security findings is actively reduced
- Supply chain assurance coverage approaches full adoption for first-party code
- AI usage is governed, with clear review, approval, and audit mechanisms

These benchmarks provide far more insight than tool counts, scan volumes, or compliance checklists.



What This Means for CIOs & CISOs

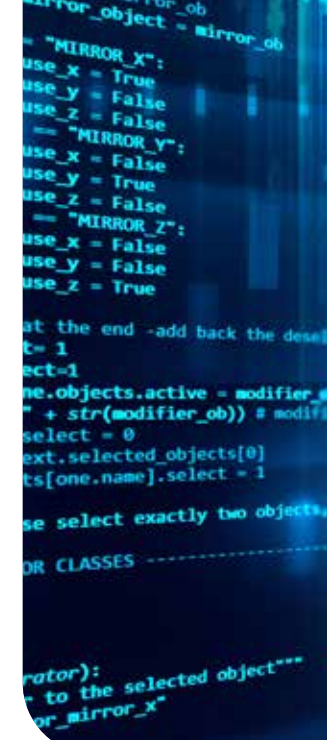
The organizations pulling ahead share a common mindset:

**DevSecOps is an enterprise platform capability,
not a collection of security tools.**

For CIOs, this means treating delivery platforms as strategic infrastructure that directly impacts speed, cost, and resilience.

For CISOs, it means shifting focus from reactive controls to embedded, measurable risk reduction that scales with the business.

The most successful leaders are simplifying, standardizing, and governing DevSecOps at the platform level while enabling teams to move faster inside clearly defined guardrails.



How Data Intensity Can Help

For leaders who want control of self-managed GitLab without the operational burden, Data Intensity offers a dedicated, fully managed DevSecOps platform on Oracle Cloud Infrastructure. You get a single-tenant GitLab environment with your update cadence, your architecture, and your guardrails – not a shared SaaS schedule – so you can align changes to risk windows, enforce policy as code, and standardize evidence capture for audits.

The service includes 24x7 monitoring and support, automated backups and disaster-recovery tiers, and scalable designs up to thousands of users, all on OCI's high-performance, security-forward, cost-efficient infrastructure. The result is faster time to security, stronger compliance posture, and clearer visibility across pipelines and artifacts.

Running complex Oracle-powered workloads is in our DNA. We're an Oracle MSP with decades of managed services experience and a repeatable process for moving and managing mission-critical workloads on OCI. That heritage – architecture design, licensing savvy, 24x7 operations, disaster recovery, patching, and SLA-backed performance – is the same operating discipline we apply to your GitLab platform so your teams can focus on delivery while we handle day-to-day resilience.

If your mandate is to shift security left, improve audit readiness, and reduce tool sprawl – while keeping control of when you patch and upgrade – Data Intensity's managed GitLab on OCI offers a secure, single-tenant DevSecOps foundation that scales with your business.



About Data Intensity

Data Intensity is an Oracle Strategic MSP partner delivering managed services for the complex lifecycle of Oracle-powered workloads. Offering a complete portfolio under one roof, we provide full-stack, technical, and functional application managed services on any cloud.

Additionally, we maximize and future-proof our clients' Oracle investments through effective license position assessments and cloud-independent migration services.

Learn more at dataintensity.com.



DATA  INTENSITY

dataintensity.com



833.746.8506