



How DevSecOps platforms help secure the software supply chain

Rob Williams

Senior Solutions Architect, Asia Pacific

GitLab

Market & customer expectations are changing more rapidly than ever

Development teams must increase their velocity and security to match.



Software released 2x+ faster in 2025 by most of companies

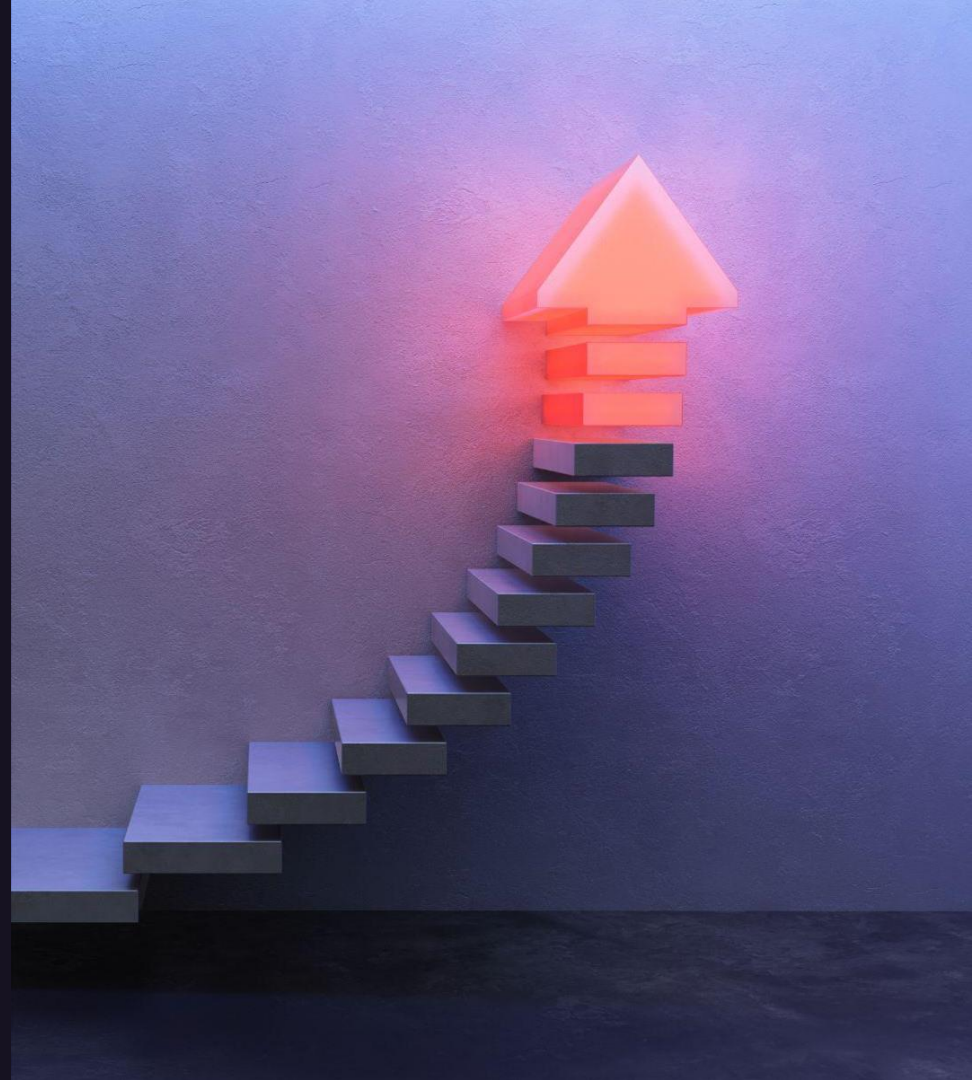


>25% of code worked on is from open source libraries by majority of developers

Source: GitLab 2025 DevSecOps Report



© 2025 GitLab Inc.



Despite advanced security tools, faster development opens the door to risky code, components and practices

Recent security breaches and attacks:

-  500M customer records breached with unauthorized cloud database access
-  10B passwords leaked
-  Unpatched software and 3rd party dependencies
-  Content update failure put airlines and banks on halt



The risk is real
with third-party
software and open
source libraries

Software supply chain attack impacts repo of large Discord bot community

News Analysis

27 Mar 2024 • 6 mins

Application Security

DevSecOps

Malware

The incident shows the snowball effect a single malicious package source development ecosystem.



Supply chain attack against GitHub Action triggers massive exposure of secrets

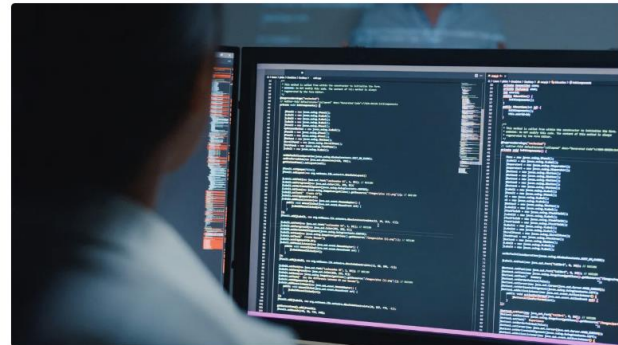
The incident highlights ongoing security concerns in the software supply chain.

Published March 17, 2025



David Jones

Reporter

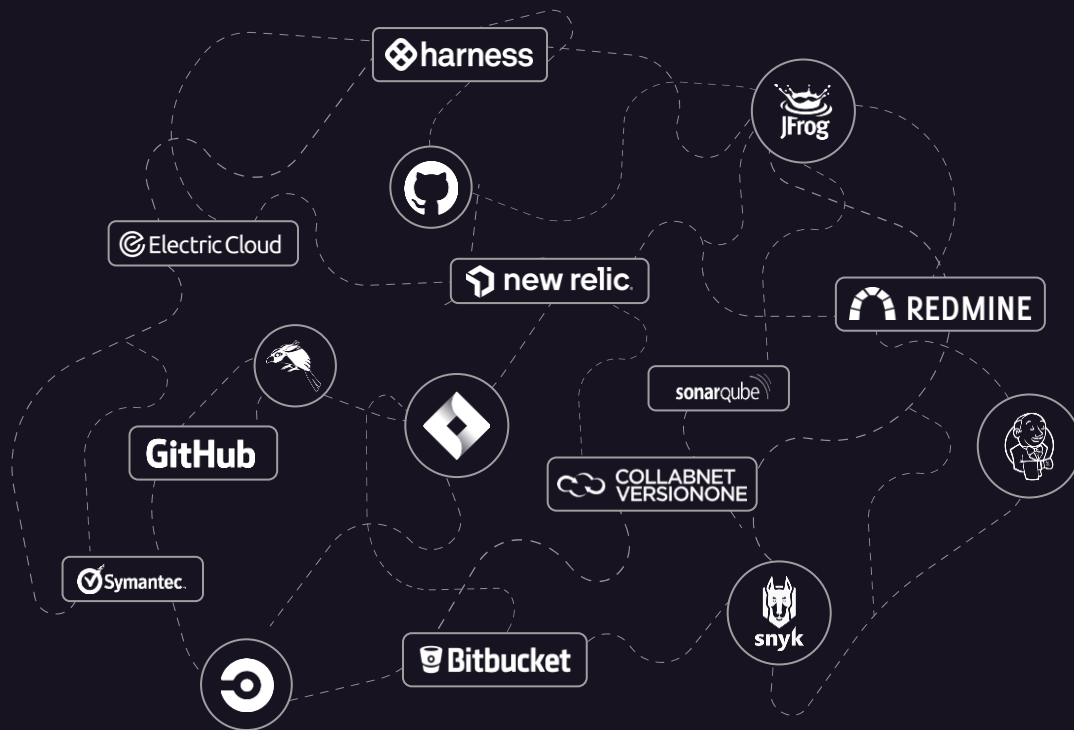


MTStock Studio via Getty Images



Tool chain sprawl makes security practices harder to enable

- ✗ 100s of tools
- ✗ Multiple data models
- ✗ Complexity & risk
- ✗ Lack of transparency



AI can be a double edged sword



AI will offer significant advantages in terms of time and cost efficiencies when leveraged by security teams



AI poses additional risks and threats to businesses



Key emerging priorities for CISOs in 2025



AI Governance Evolution



Enhanced Supply Chain Security



Cloud Security Maturity



Emerging Software Bill Of Materials priorities for CISOs



Automation and Integration



Enhanced SBOM Requirements



Compliance Considerations



Key Compliance Frameworks and Regulations for 2025 in Australia



ISM Guidelines for Software Development



APRA: Prudential Policy for Financial Services institutions



Information Security Registered Assessors Program (IRAP)



Essential 8



Telecommunications Act



Cyber and Infrastructure Security Centre



The cost of remediating security vulnerabilities

\$59.5B

Annually cost of software bugs*

300

Cost of software developer hours**

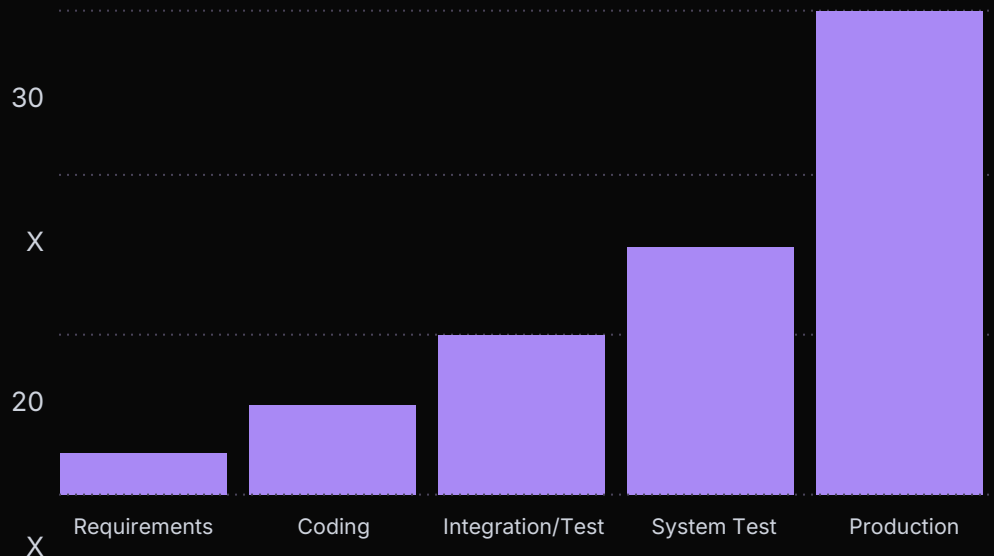
Stage	Hours*	Cost
Coding stage	2.4	\$740
Integration stage	4.1	\$1,230
System stage	6.2	\$1,860
Production stage	13.1	\$3,930

*(NIST - Impact of Inadequate Software Testing

**2019 SW Dev Price Guide

Cost of Remediation

*X is a normalized unit of cost and can be expressed in terms of person-hours, dollars, etc.



Source: National Institute of Standards and Technology (NIST)

Holistic software supply chain security (SSCS)

Securing the components, activities, and practices involved in the development and deployment of software coupled with Application Security.



Software supply chain security: key components

Governance

Ongoing review, audit, and enforcement of all controls

Source

- Application Security: SAST, IAC Scanning, Secret detection
- Source code controls
- Developer Education

Dependencies

- Software Composition Analysis
- SBOM management

Build

- Isolated build environments
- Release evidence
- Build signing & artifact attestation

Release

- Secure CI/CD tunnel
- Application security: API security, DAST



Identify the Gap: Value Stream Management

1. Visualise DevSecOps work streams
2. Identify risk through DevSecOps inefficiencies
3. Take action to optimise DevSecOps work streams to deliver the highest possible velocity of value



Identify



Measure



Visualise



Optimise



Optimising Security in the Software Delivery Lifecycle

Current DevSecOps State

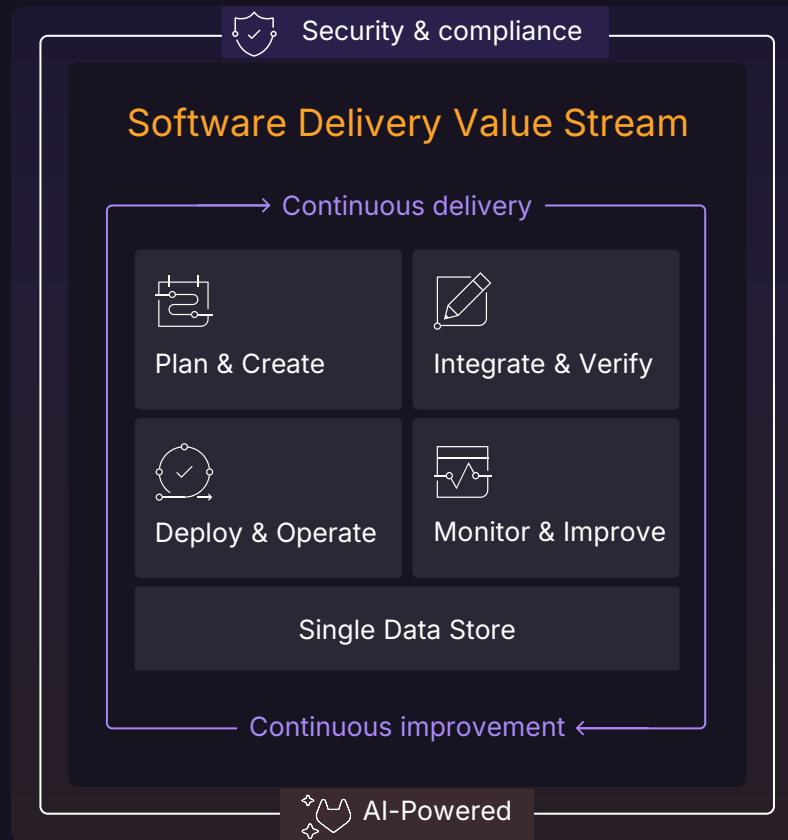


Desired DevSecOps Future State



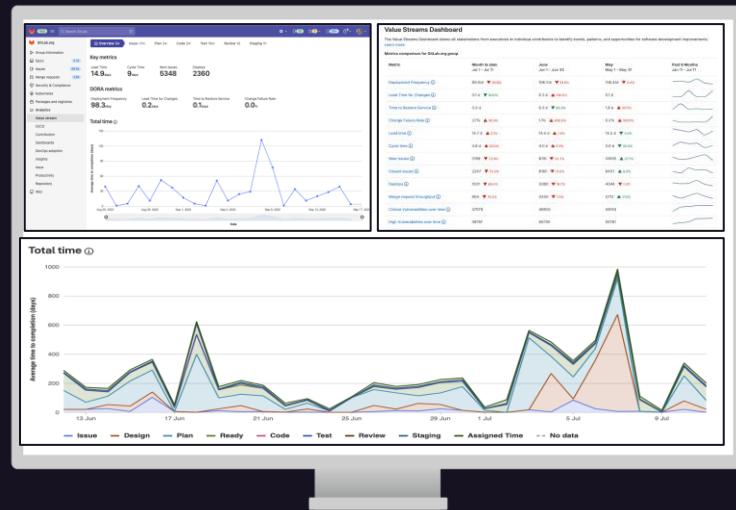
Consolidated DevSecOps platforms

- ✓ Enhanced security
- ✓ Improved efficiency
- ✓ Better visibility and compliance
- ✓ Cost savings
- ✓ Scalability and flexibility



GitLab Value Stream Management (VSM) enables executive visibility across value streams

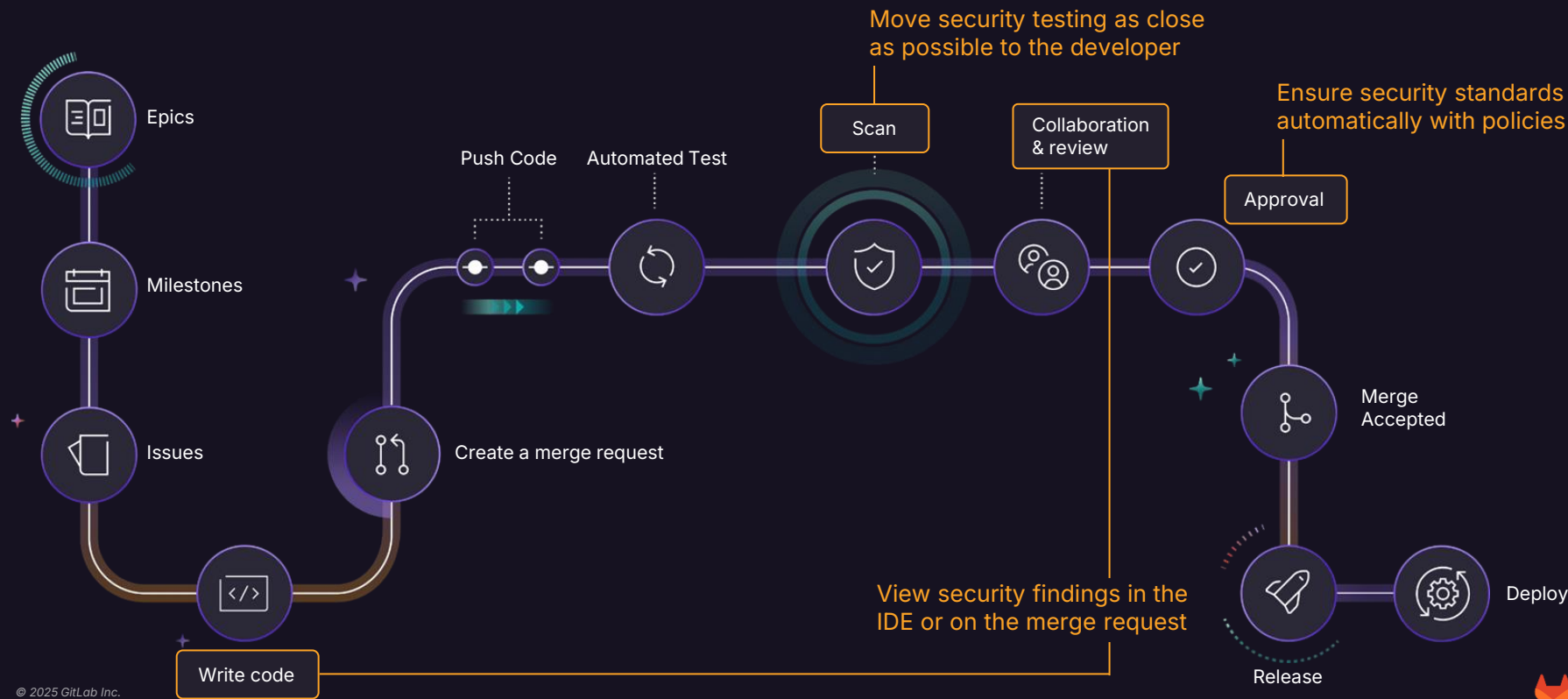
- ✓ **Value streams dashboards** and metrics to identify security bottlenecks and deficiencies resulting in improved visibility into the organization's security posture.
- ✓ **Holistic visibility** and platform approach allows security leaders to gain a comprehensive understanding of security performance, facilitating informed decision-making.
- ✓ **Improved collaboration** to align security goals with other teams, fostering a shared understanding of security objectives.



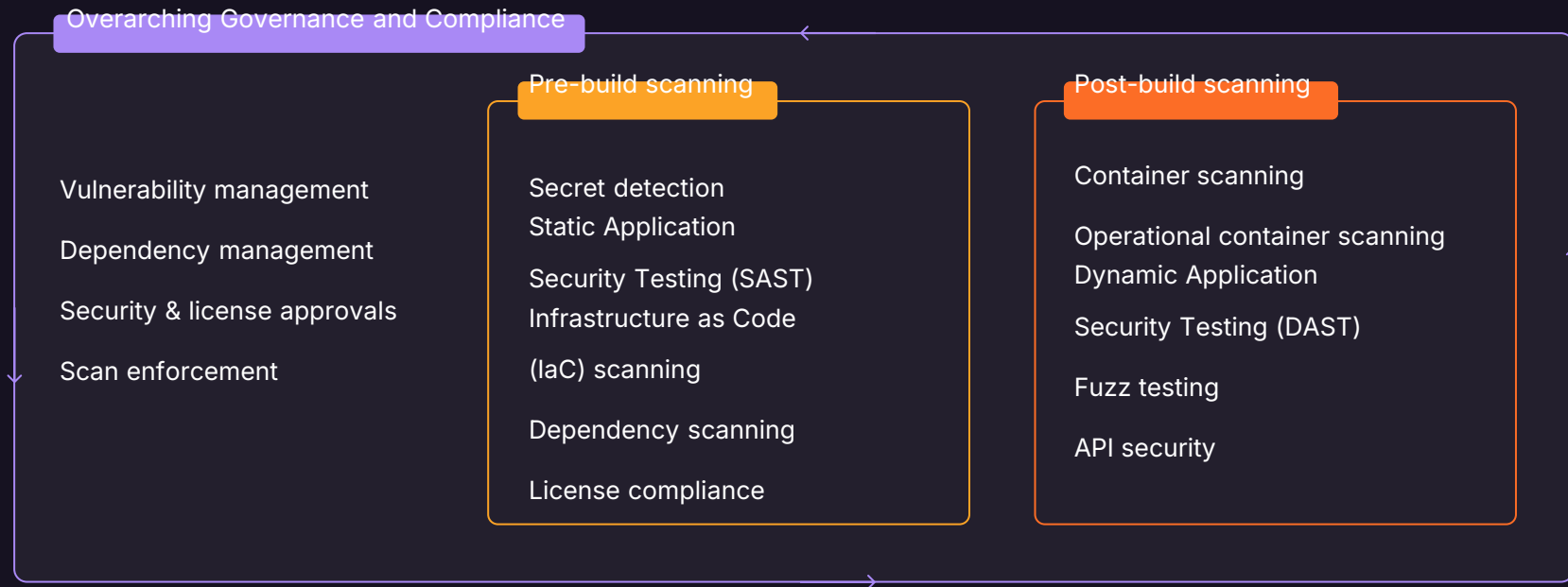


How do we integrate Security,
Compliance and Risk Management
earlier in the software delivery cycle?

Shifting Left: Vulnerability scanning & triage in the developer workflow

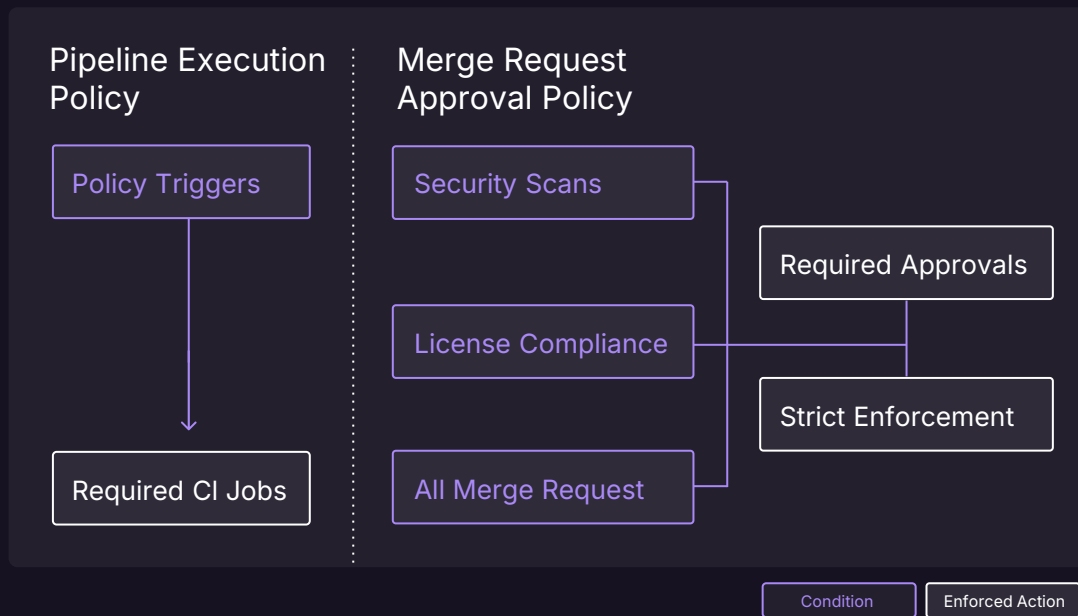


Breadth of application security scanning required to address the gap in 2025

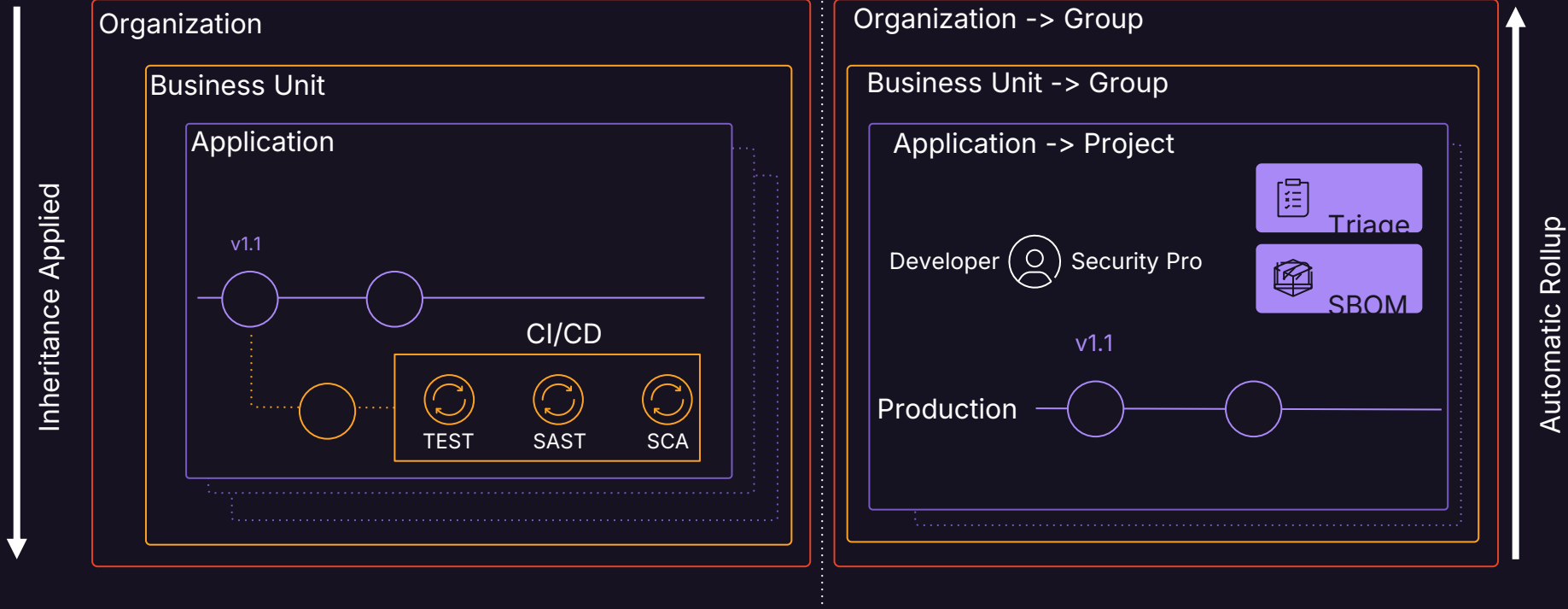


Comprehensive governance & compliance

- ✓ Software supply chain security
- 📋 Separation of duties
- 🏆 Fully audited change history
- 👤 Two-person change approval
- ⚙️ Policy as code
- 📈 Enforceability at scale



Scaled to address organizational risk



How to optimise Security, Compliance and Risk Management in 2025

CISOs should consider:



Declarative oversight and governance



Promote creation of secure and efficient code



Establish and refine the secure software supply chain



Empower consistent collaboration with single source of truth



Improve speed and stability in software delivery



Automate and augment with AI





Creating better,
secure code **faster**