Proactive Compliance in Application Development

The Dynamic Supply Chains

Joel Krooswyk
Federal CTO, GitLab

Real resilience starts when compliance stops being a checkbox and becomes part of how software is built. Shipping code fast is no longer enough. It has to be built securely, responsibly, and in full compliance with evolving regulatory expectations. As the speed of delivery accelerates and software supply chains grow more complex, organizations need smarter, more scalable ways to stay ahead of risk and regulations.

This session explored how integrating compliance directly into DevOps workflows helps teams drive automation, enforce policy as code, and stay audit-ready without slowing innovation. Attendees learned how modern development teams can address open source software (OSS) risk, manage software supply chains, and embed auditability into every phase of the development lifecycle. With threats evolving faster than ever, the session emphasized that compliance is not a barrier to innovation; it's a foundation for secure, scalable development.

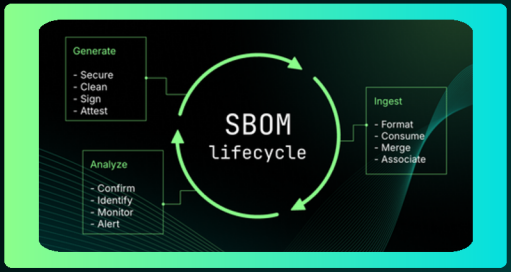
Key Takeaways

1. Integrating compliance into DevOps processes via automation, templated starts, and policy-as-code reduces risk and increases speed-to-market.
2. Organizations must leverage AI-led remediation, enforce compliance via pipelines, and use cryptographic attestation to ensure trust at scale.
3. Unmaintained open source components and API vulnerabilities require continuous visibility and proactive dependency management.
4. Software Bills of Materials (SBOMs) and comprehensive audit trails build traceability that is key to compliance and resilience.

agility25 BY LOGICGATE

Proactive Compliance in Application Development

The Dynamic Supply Chains



In an increasingly dynamic and regulated development environment, the session ***Proactive Compliance in Application Development: The Dynamic Supply Chain*** delivered a compelling case for shifting from reactive, audit-centric compliance to proactive, code-driven assurance. ***Joel Krooswyk, Federal CTO at GitLab***, guided attendees through the growing intersections of GRC, DevSecOps, and AI, outlining how organizations can embed compliance directly into their development workflows without sacrificing innovation.

The session addressed the challenge of maintaining compliance in the face of rapidly evolving cybersecurity policies, OSS risk, and heightened software liability. Key concepts included “compliance as code,” templated project starts, and policy pipeline enforcement designed to operationalize compliance from the very first commit. Krooswyk emphasized the necessity of security scanning, API protections, dependency tracking, and SBOM lifecycle management to monitor and enforce standards across distributed teams.

> By 2026, 70% of enterprises in regulated verticals will have integrated compliance as code into their DevOps toolchains, reducing risk management and improving lead time by at least 15%.

-2023 Gartner Market Guide for Continuous Compliance Automation Tools in DevOps

The session underlined the importance of AI-led remediation and automated workflows to detect threats in real-time, backed by artifact-based auditability and integrated vulnerability dashboards. Real-world insights included a shout-out to Risk Cloud’s continuous monitoring, illustrating how an SBOM lifecycle can form the backbone of a trustworthy supply chain.

linkedin.com/in/joelrkrooswyk

ag25