DevSecOps

9 Ways DevOps and Automation Bolster Security and Compliance

CloudBees®

Introduction

Given the increasing number of data breaches and new, global legislation protecting consumers' personal data, security and compliance remain critical to businesses' survival. Yet, enterprise security teams - with their more conservative approach to risk mitigation - are still perceived by DevOps teams as the "release prevention department." Meanwhile, security teams view DevOps' increased release velocity as a threat to governance, security and regulatory controls.

In an attempt to satisfy both DevOps and security teams, some organizations moved towards a "shift security left" approach, which looked to integrate security earlier in the development process and called it DevSecOps. The result did show improvement in the quality of software being released, but security exposures remained in the process itself and limited an organization's ability to detect, mitigate and remediate issues in production.

More recently, forward-looking enterprises have recognized that DevSecOps goes well beyond "shifting security left" to "shifting security everywhere." By baking security processes and technology into the core automation and DevOps practices they employ across the entire software delivery lifecycle, enterprises can discover more issues prior to release, detect and prevent drift and elegantly respond to post-release issues. The complete DevSecOps approach ensures software is secure in development, delivery and in production.

DevOps Makes Security and Compliance the Path of Least Resistance

DevOps provides a huge opportunity for better security. Many of the practices that come with DevOps, such as standardized automation, test orchestration, fast feedback loops, improved visibility and collaboration and consistent release practices, are fertile ground for integrating security and audit as built-in aspects of DevOps processes.

DevOps automation spans the entire pipeline, from code development and testing, to infrastructure configuration, to deployment and running in production. When done right, DevOps enables you to:

Secure from the Start

Security must be integrated from the early stages of DevOps processes, and not remain a separate activity at the very end of the software delivery pipeline. It becomes a quality requirement similar to other tests run as part of the software delivery process. Just as continuous integration enables “shifting everywhere” by accelerating testing and feedback loops to discover bugs earlier in the process, DevOps processes “shift security everywhere” by incorporating automated security and compliance testing, while also enforcing the use of approved components.

Secure Automatically

As more and more tests and processes are automated, there is less risk of introducing security flaws due to human error. Tests become efficient and can cover more ground, and processes are more consistent and predictable. So, if something does break or an insecure component sneaks into the pipeline, it's easier to pinpoint and fix the root cause of the problem and ensure compromised code never makes it into production.

Secure Throughout

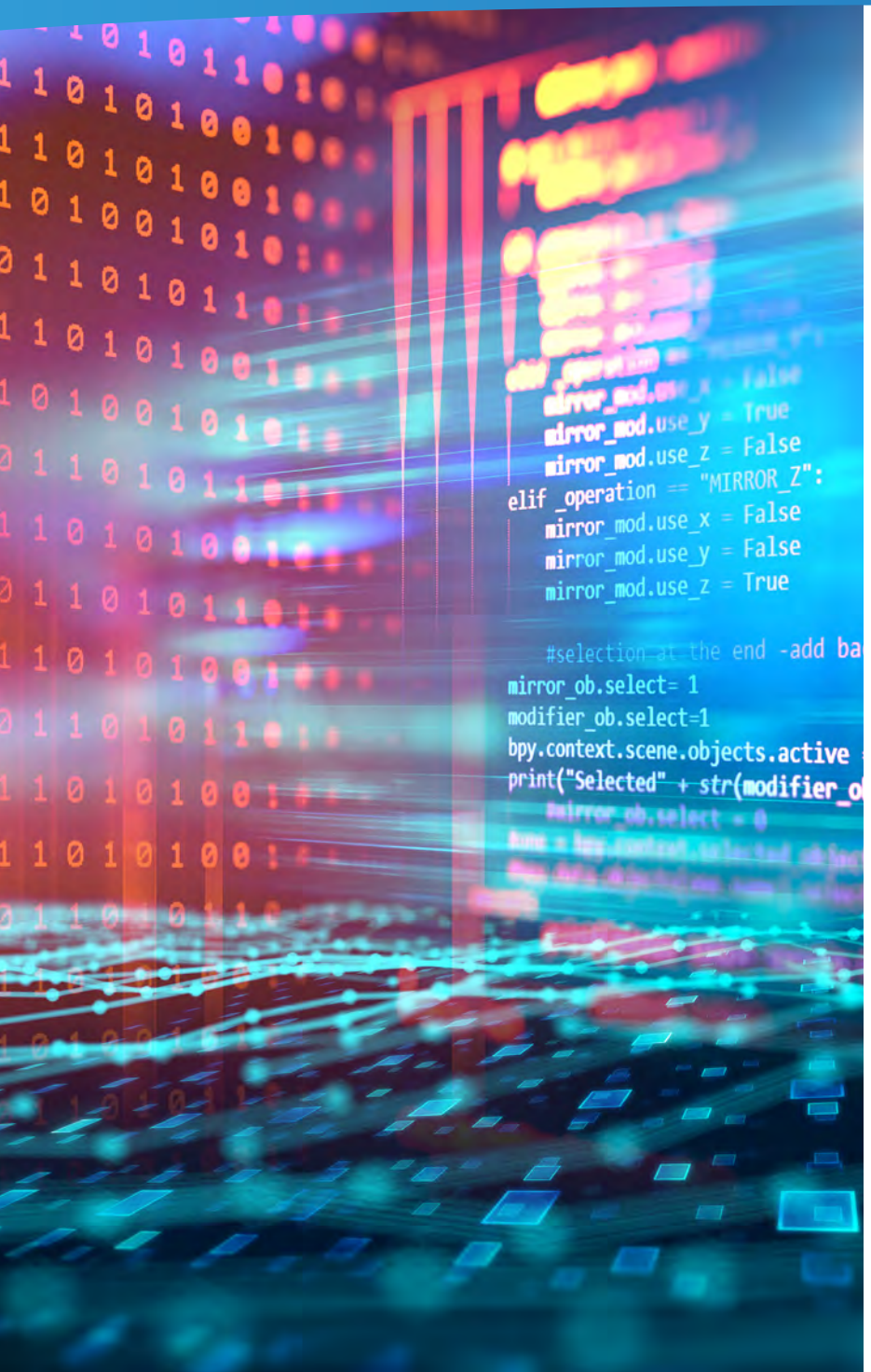
In using tools that are shared across the different functions --and managing their usage with a single, secure pipeline orchestration platform that spans development, QA, and operations -- organizations gain visibility and control over the entire systems development life cycle. The automated pipeline becomes a closed-loop process for testing, reporting, instantly mitigating, and resolving security concerns.

Improve Communications and Eliminate Blame

By integrating security tools and tests as part of the pipeline used by Dev and Ops to deploy updates, information security (InfoSec) becomes a key component of the delivery pipeline and an enabler of the entire process. With everyone on the same page and using the same pipeline, Security, Development, and Operations teams share a common language and have a common understanding of the situation. In turn, post-incident finger-pointing is replaced with incremental fixes to the application code and the pipeline that address concerns as they arise.

Fix Things Quickly

Unfortunately the occasional security breach or vulnerability may happen, requiring quick action to resolve the issue . Mean Time to Detect and Mean Time to Repair are two key metrics for measuring resilience. Closing the time lag between detection and remediation is vital. Tracking the state and locations of all components, applications, environments, and pipeline stages greatly simplifies and accelerates reporting and correction. Having the ability to turn off the vulnerability instantly, without a rollback, gives even more time to develop and release a fix.

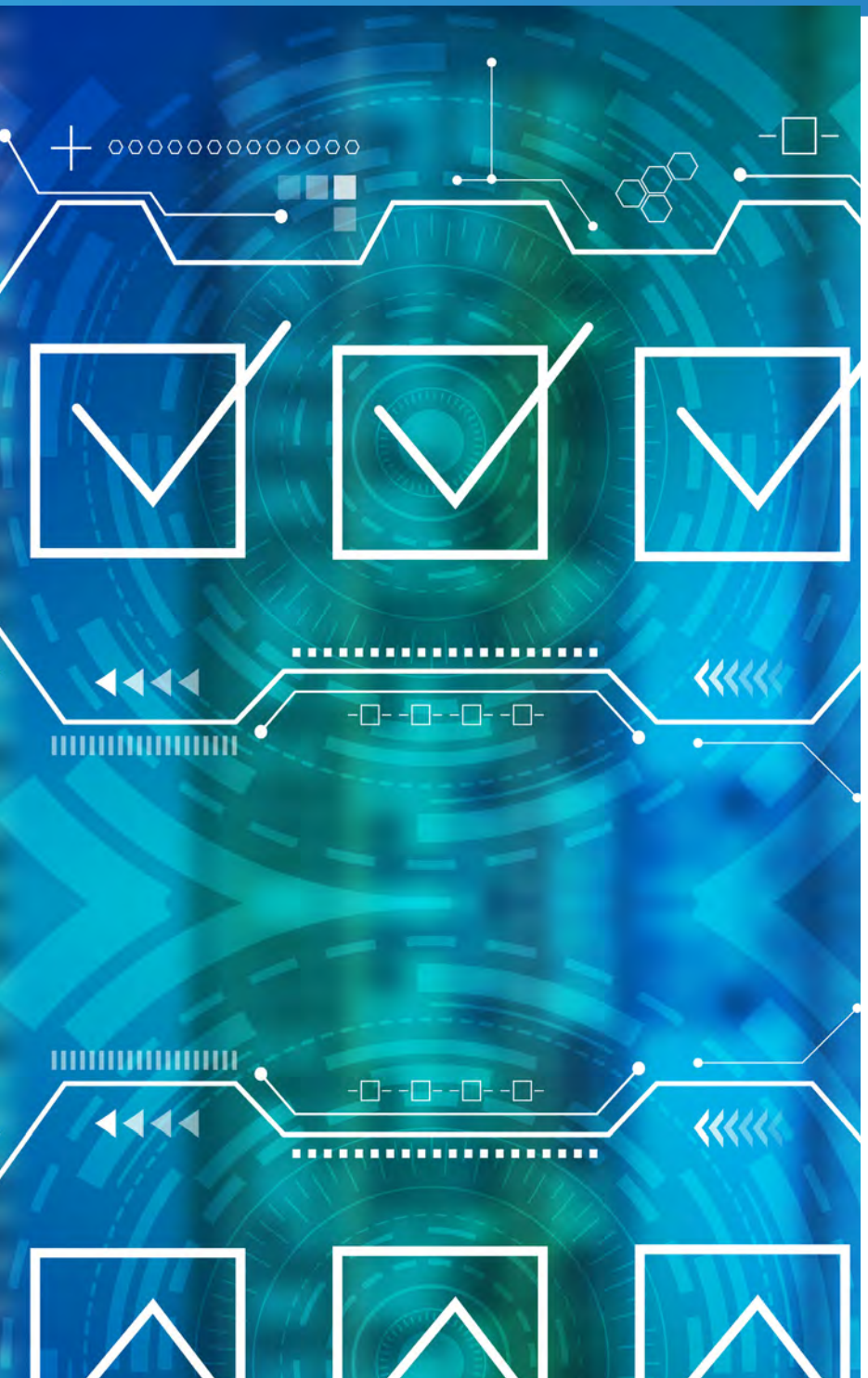


Enable Developers and Ensure Governance

Devs want DevOps tools and automation to enable experimentation, not constrain it. Operations and InfoSec want DevOps tools to provide standardization and compliance reporting. Look to achieve both with a governed and secure software pipeline that can absorb existing technology and processes easily, while also enabling incremental improvement and continual re-alignment with company standards over time.

Secure the Code and the Tools that Deliver It

Just like code, software pipelines that are auditable and can be easily versioned and refactored to provide manageable systems that are both protected and compliant. Access controls should manage who can make changes to the code as well as the pipeline, and dictate which versions of the pipeline are to be used as part of any approved processes. This ensures that no one can “accidentally” change a critical vulnerability scanning flag, bypass a security compliance check or sneak in untested code without some record of who did it, and why.



Enable One-Click Compliance Reporting

The primary benefit of automation is consistent, repeatable outcomes for similar actions that are automatically logged and documented. It also comes with the extra benefit of the irrefutable proof that what was done is what was promised to be done – the foundation of compliance. Since DevOps spans the entire pipeline, it provides traceability from code change to release, making auditing much easier.
As automation expands from build, test and integration cycles, to deployment and release processes, a DevOps automation platform simultaneously captures the data for the audit trail, the security log and compliance reporting. Compliance reporting becomes a one-click effort, eliminating manual intervention or hours spent backtracking manual processes and actions.

Accelerate Safe, Secure Releases

When security and compliance controls are an integral part of DevOps workflows, this becomes the foundation for long term success. However, shifting security left also accelerates releases by detecting and remediating problems - before they get into production. It is the difference between the few minutes of retesting a piece of code in the development stage versus the hours, days or even weeks it takes to rerun the entire release orchestration process.

Summary

Security, governance and QA are everyone's responsibility, not an afterthought. Organizations that automate security throughout the development, delivery and production stage with hardened, reusable pipelines, required testing thresholds and automated detection and mitigation, get products to market faster while concurrently making their systems more resilient. DevOps becomes a resource for Security --rather than a threat-- and Security becomes the path of least resistance.

About

CloudBees is the industry's leading DevOps technology platform delivering the world's first end-to-end continuous software delivery management system. CloudBees enables developers to focus on what they do best: Build stuff that matters—while providing peace of mind to management with powerful risk mitigation, compliance and governance tools.

Used by 50% of the Fortune 500, CloudBees is helping thousands of companies harness the power of continuous everything and gets them on the fastest path from great idea, to great software, to amazing customer experiences, to being a business that changes lives.

Visit CloudBees at www.cloudbees.com.

CloudBees CI is built on top of Jenkins, an independent community project. Read more about Jenkins at: www.cloudbees.com/jenkins/about

© 2020 CloudBees, Inc. CloudBees is a registered trademark and CloudBees CI, CloudBees CD, CloudBees Cloud Native CI/CD, CloudBees Feature Flags, CloudBees Build Acceleration and CloudBees CodeShip are trademarks of CloudBees. Other products or brand names may be trademarks or registered trademarks of their respective holders.

0820v00

CloudBees, Inc.
4 North Second Street | Suite 1270
San Jose, CA 95113
United States
www.cloudbees.com
info@cloudbees.com