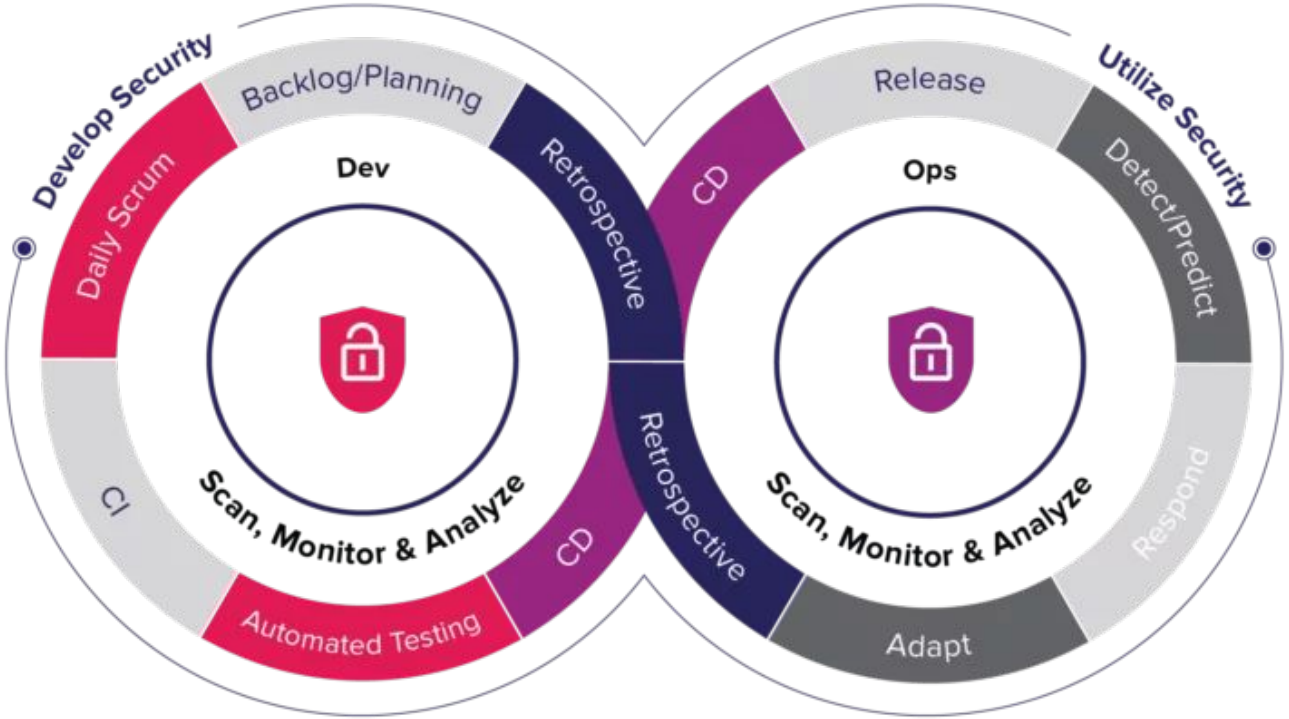
CloudBees®

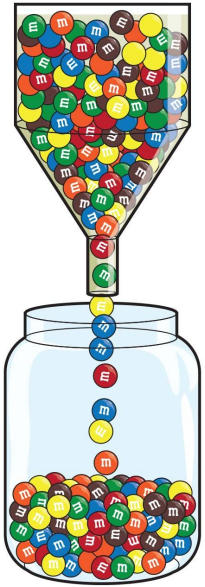
A Systems Approach to Software Supply Chain Security and Continuous ATO

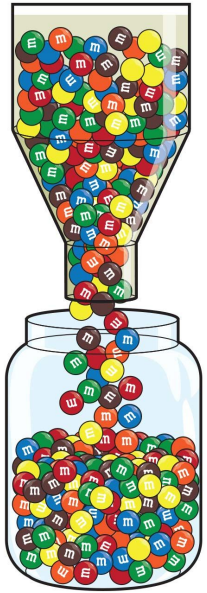
Tyler Johnson, Federal CTO

DevOps and cATO



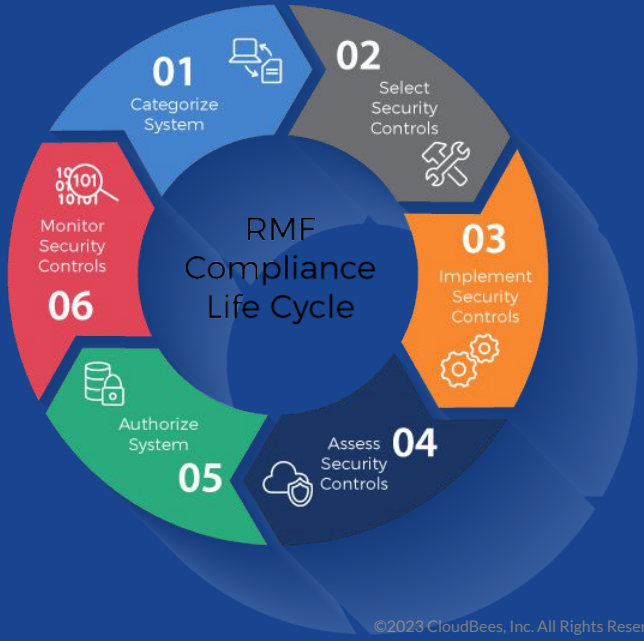
CloudBees.





Maintain Velocity

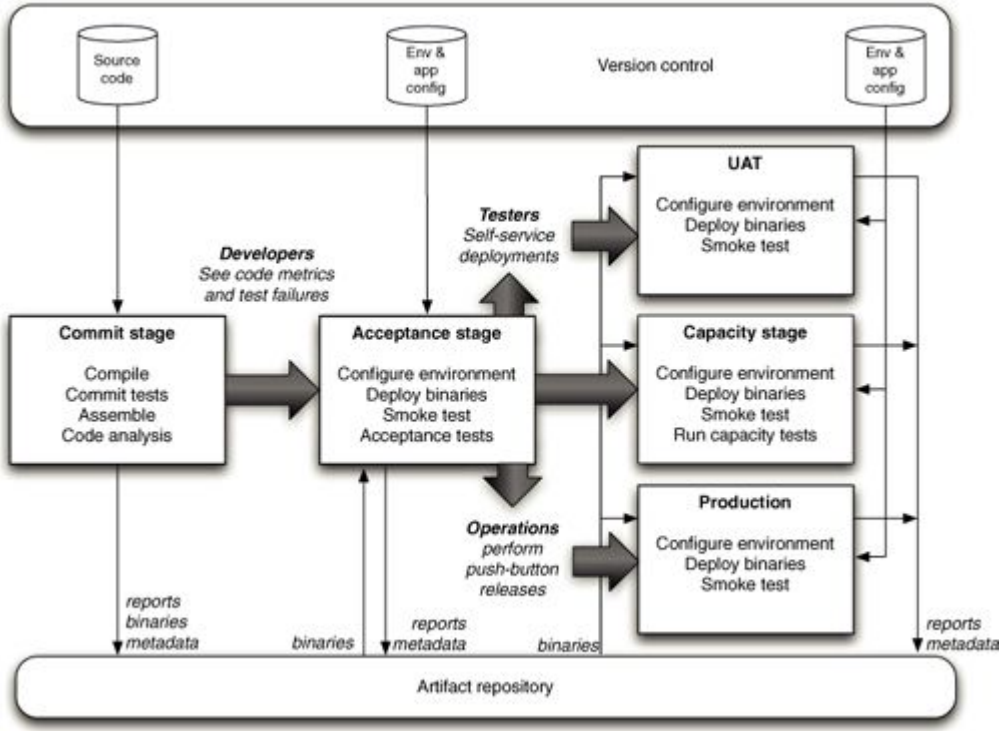
How do agile processes maintain velocity through operations?

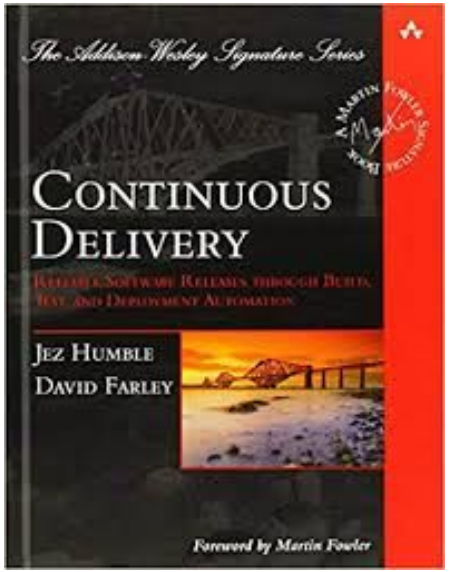


CloudBees.

Increasing confidence in build's production readiness

Environments become more production like



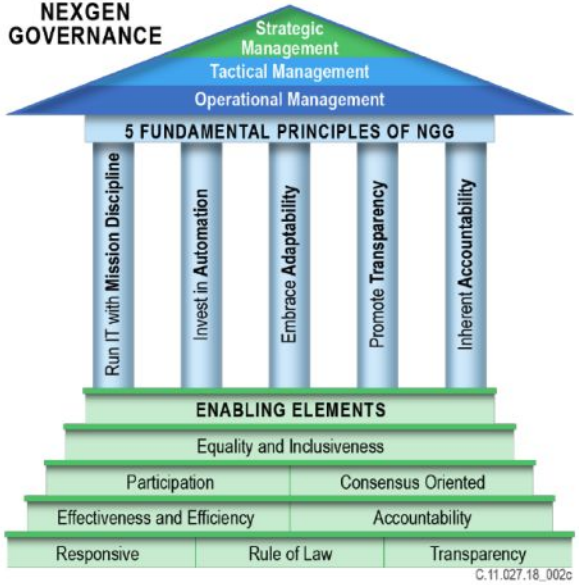


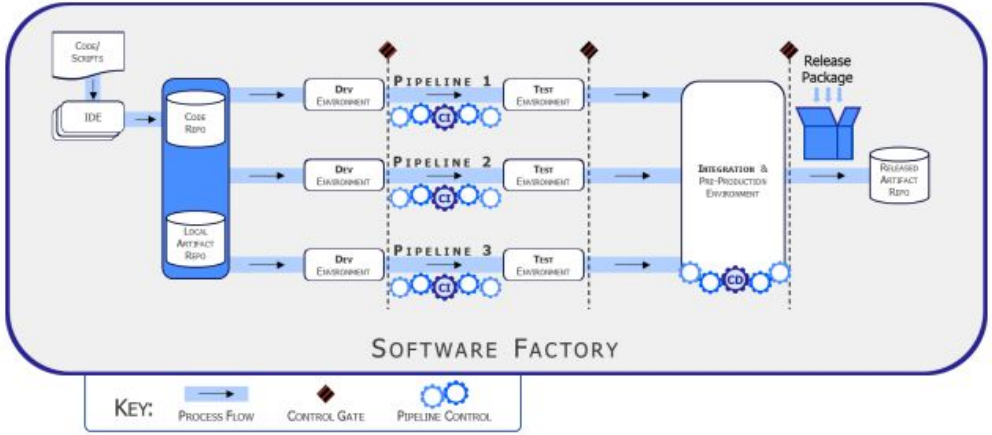
Basic Deployment Pipeline

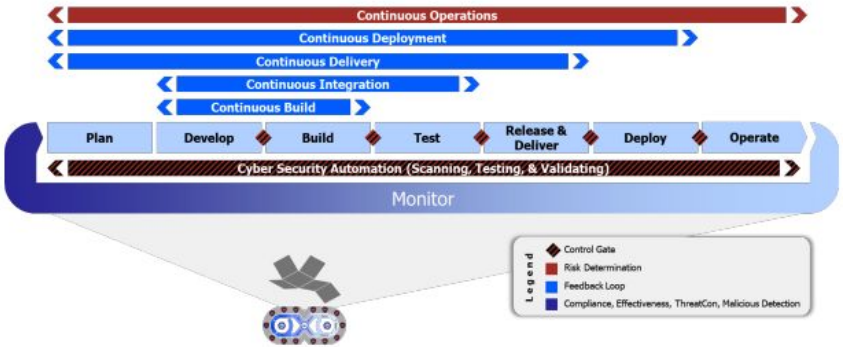
Faster feedback

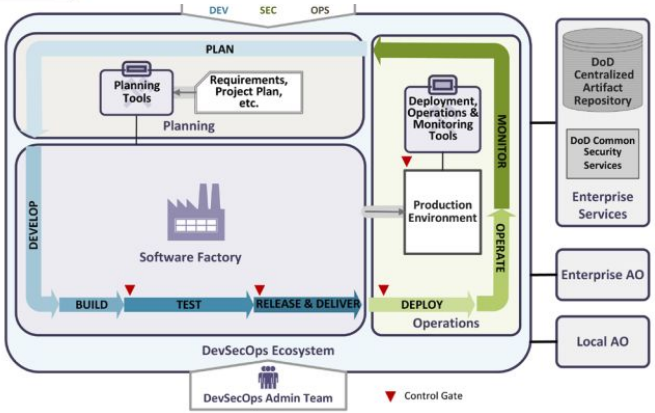
CloudBees.

HOW?









CloudBees.

DevSecOps Maturity in context

Developer Focus ←  → Operations Focus

Discipline	**Agile** An incremental approach to identifying, prioritizing, and coordinating feature development	**Continuous integration** Automated commit, build and testing of code in the development environment	**Continuous delivery** Software changes continuously delivered to stakeholders in any environment	**Continuous ATO** Software changes continuously deployed with ATO into production.
Env.	**Development**		**Production / Prod-like**	**Live production**

Stage

LEFT **Upstream** … **Downstream** RIGHT

Define	Plan	Code	Compile	Build	Unit test	Analyze	Integrate	Int. test	Package	Place	Load test	Acct. test	Release	Deploy	Monitor

Rapid changes ◄- ► **User feedback**

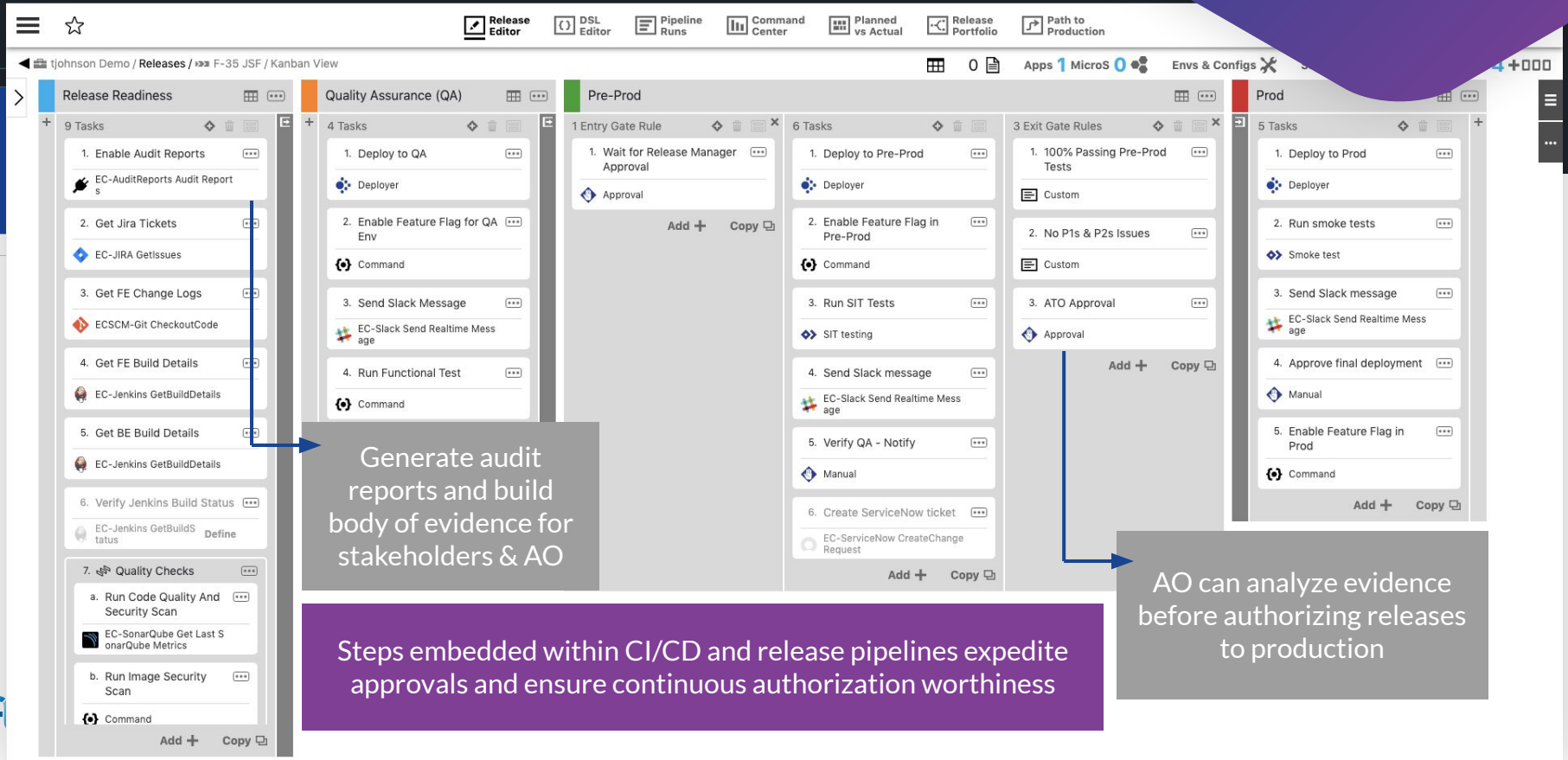
CloudBees.

"Current RMF implementation focuses on obtaining system authorizations (ATOs) but falls short in implementing continuous monitoring of risk once authorization has been reached."

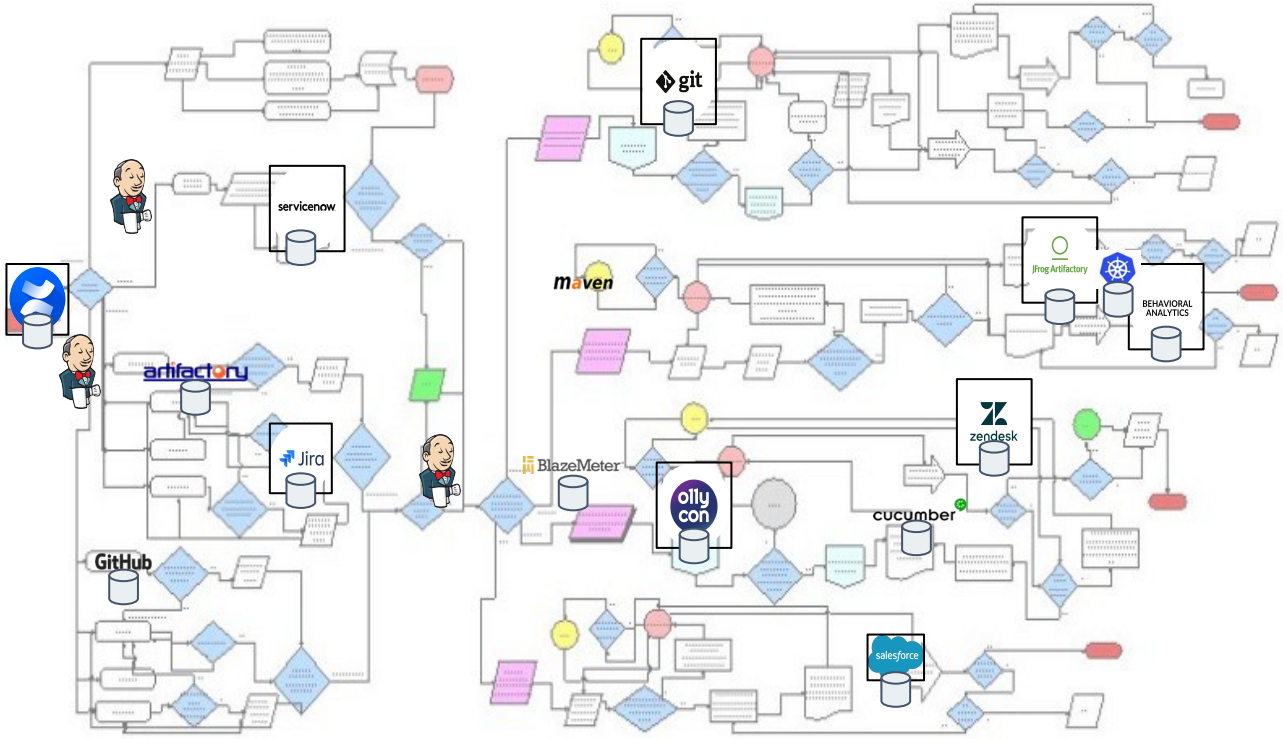
CloudBees

Modeled Reference Design

Layer 1



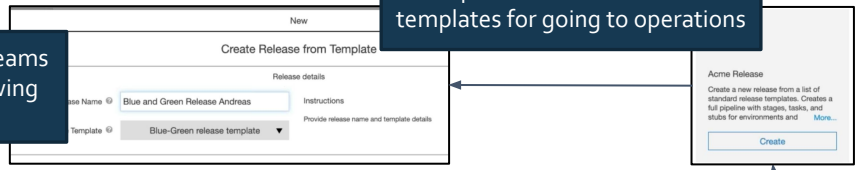
The problem is… building and releasing software is complicated.

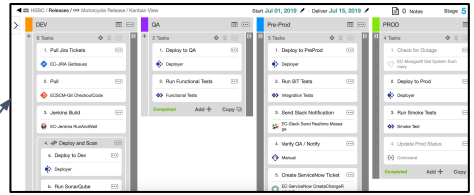


Operational Context

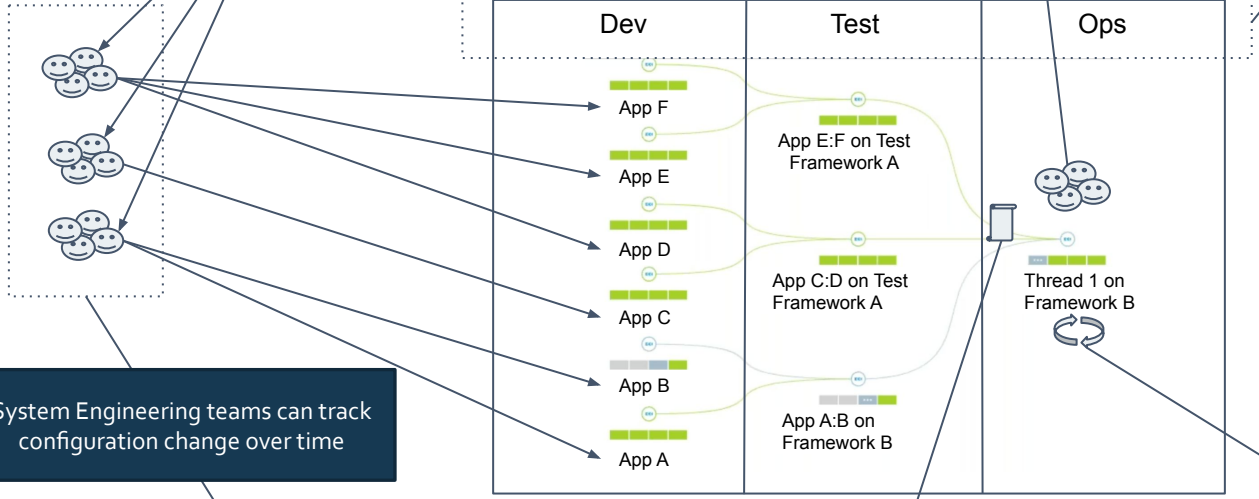
Operations teams define templates for going to operations

Distributed development teams can build confidently knowing integration is assured

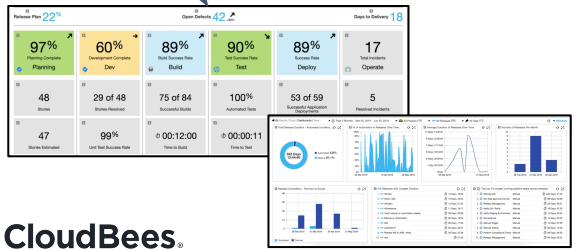


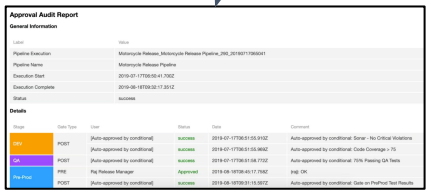


Management can track metrics on all teams and progress against program closure

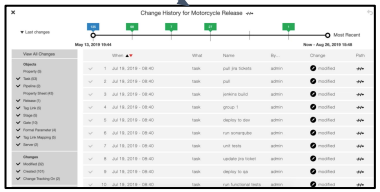


System Engineering teams can track configuration change over time





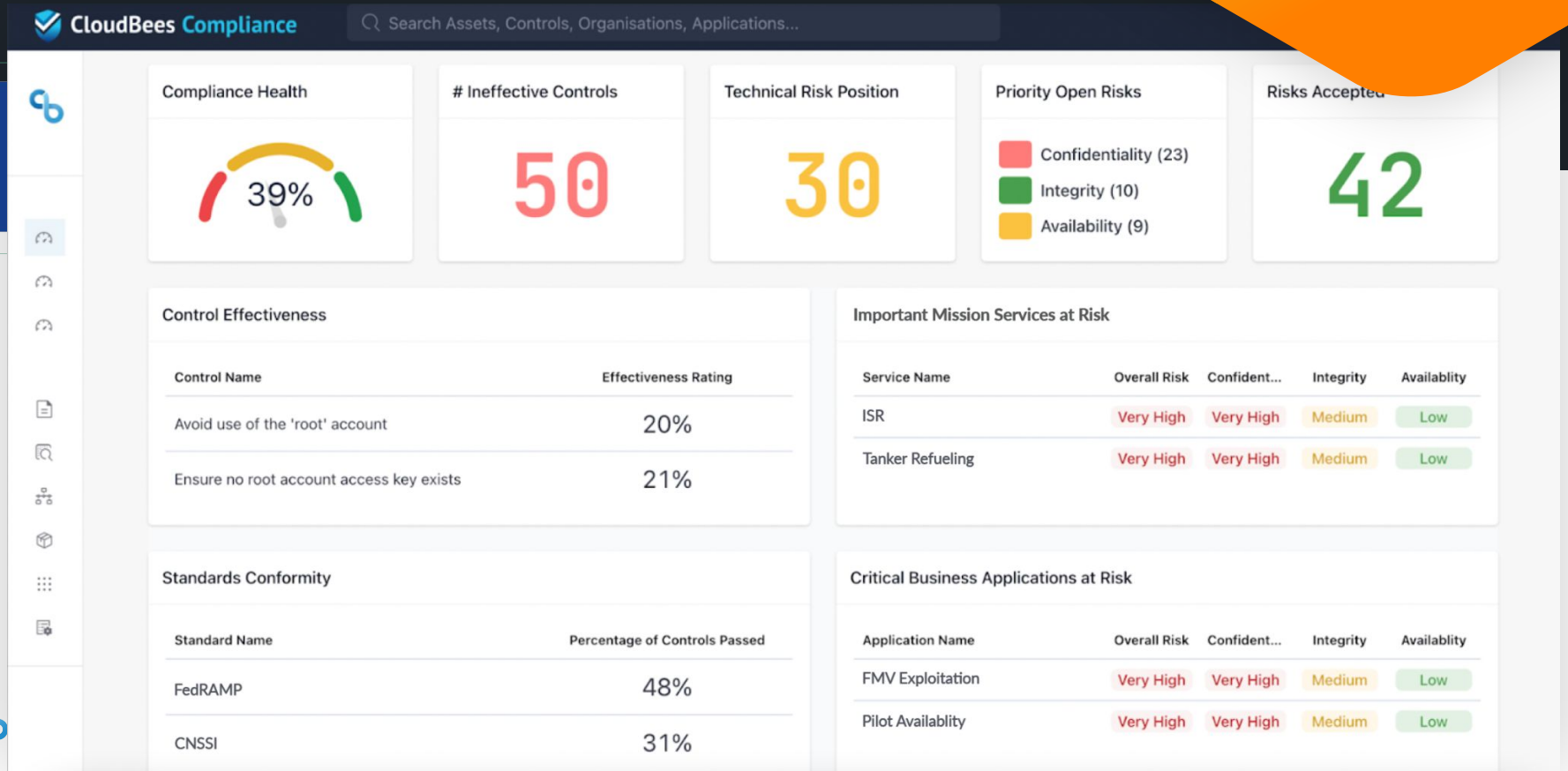
IA can aggregate evidence from DevSecOps tools and enforce compliance goals



CloudBees.

Ongoing Visibility

Layer 2



Compensating Controls - Automated Mitigation

Mean Time to Mitigate

Layer 3

Feature flag as kill switch

- Everyone has to follow the same build method
- Kill features, not the experience

Automated roll back to known good state

- Rehearsed and integral to the system
- When a bigger hammer is required

CloudBees®

118TH CONGRESS
1ST SESSION

S. 917

[Report No. 118–32]

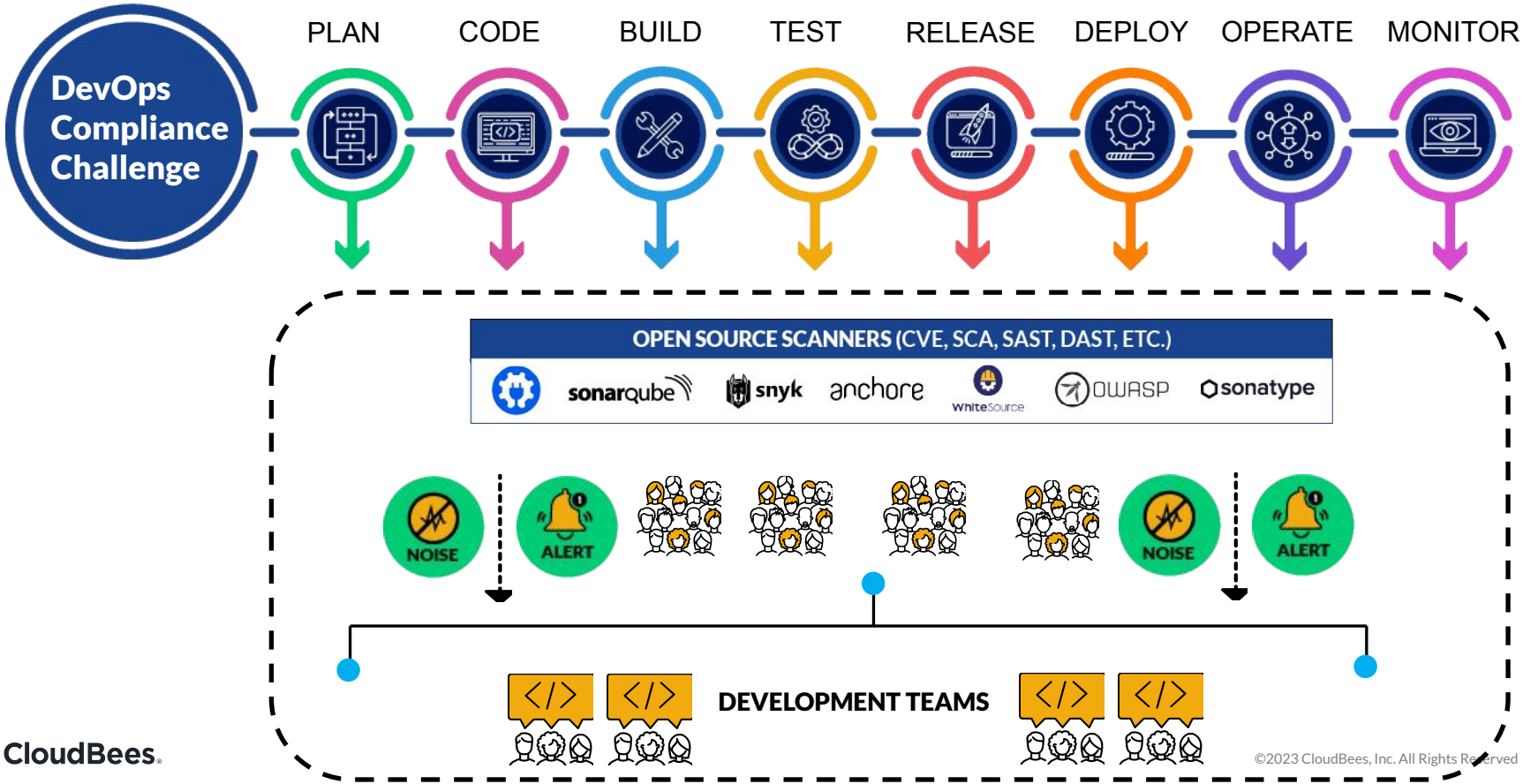
IN THE SENATE OF THE UNITED STATES

March 22, 2023

Mr. Peters (for himself and **Mr. Hawley**) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

Open Source Software Act

Enterprise Compliance Challenge



CloudBees.

ISO27001
SOC2 HIPAA
FedRamp CCM NIST 800-53

CIS for AWS, GCP & Azure
CSA CCM NIST CSF
PCI DSS GDPR

Real-time Events

anchore sonatype WhiteSource

sonarqube OWASP

Open Source Scanners

Microsoft Azure Google Cloud aws

OPA

Compliance Engine

Compliance Team

Automatically translate and dispatch compliance issues into team-focused and actionable tasks

PLAN CODE BUILD TEST RELEASE DEPLOY OPERATE MONITOR

CloudBees.

Keys to a Secure Software Supply Chain

Security/Dev Collab

- Security defines standards
- Improve developer experience
- Increase velocity
- Improve risk posture

Appropriate Tooling

- Low/No Code approach for security
- Consumable by different personas
- Enable rapid response and RT/NRT feedback

Automated Controls

- Continuously assess
- Evidence as a service
- Control gates prevent non-compliant deployment

Centralized Toolsets

- Enterprise view
- Project view
- Persona-specific dashboards
- Centralized authoritative security/compliance/defect tracking to reduce noise

Thanks!

Tyler Johnson - Federal CTO
tjohnson@cloudbees.com
(703)980-2777
https://www.linkedin.com/in/tyler-johnson-rva/

CloudBees®