
KubeCon
CloudNativeCon
Europe 2023
TiKV

KubeCon | CloudNativeCon

Europe 2023

Fight Back Against Cyber Risk in the Software Supply Chain with a Secure and Compliant DevSecOps Pipeline for Regulated Environments

Krishna Rajeesh Nallur Valiyaveettil

IBM Cloud for Financial Services

Brendan Kelly

IBM Cloud for Financial Services

Agenda

- What is Cyber Risk and how does it affect the Software Supply Chain?
- What is the current regulated environment landscape and what are the regulatory requirements?
- What is DevSecOps and how can it combat Cyber Risk?
  - Continuous Integration
  - Continuous Delivery/Deployment
  - Continuous Compliance
- Case Study – BIAN
- Lessons Learned

Cyber Risk affecting SW Supply Chains

KubeCon | CloudNativeCon Europe 2023

45%

of organizations worldwide will have experienced attacks on their software supply chains by 2025, a three-fold increase from 2021. (Gartner)

$4.35M

Global average cost of data breach (IBV)

Regulated Environments Tension

HIGHER MAGNITUDE 'FRICTION'

Key Focus for Chief Security Officer/ Chief Risk Officer

Risk exposure
Unknown, 3rd party data centers, complexity to meet critical bank requirements

Compliance
300M+ pages of FSS regulations, cost of regulation>10% of revenue

Security
$347B projected value at risk ('19-'23) including reputation risk

REGULATORY APPROVAL

Agility
Leverage core system investment, reduced OpEx and CapEx

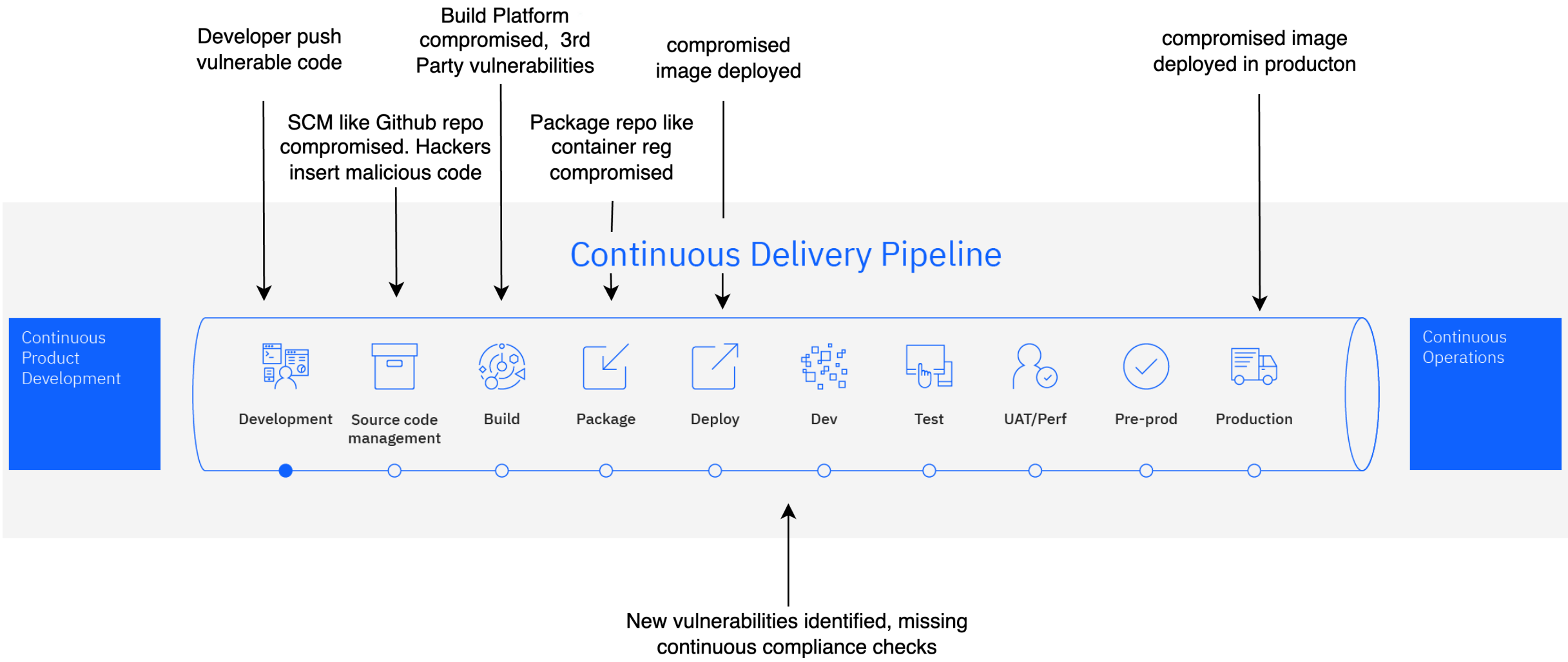
Innovation
Trusted ecosystem, accelerated speed-to-market

SPEED

HIGHER MAGNITUDE 'OPPORTUNITY'

Key Focus for Line of Business/ IT Transformation Leader

Supply Chain Risks



DevSecOps Pipeline Principles

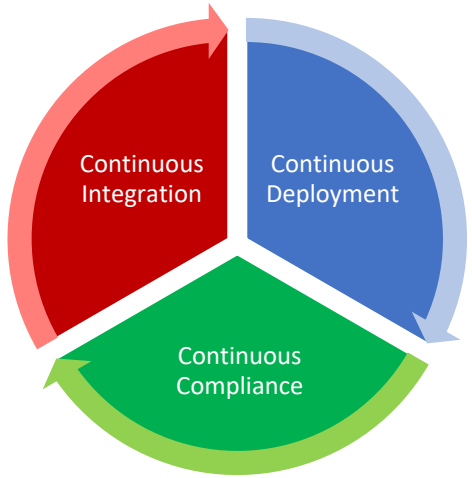
- Everything as Code

- Support multiple development languages
  - Java, NodeJS, GoLang, Python, Terraform
  - Custom framework to allow integration with any language

- Consistent approach for any application
  - Shared pipeline templates and processes

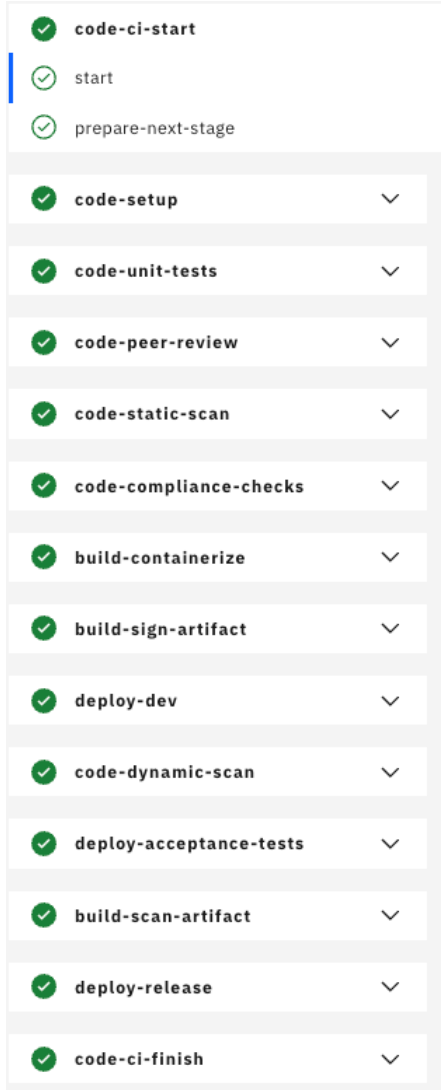
- Focus on security - ”Shift-left”
  - Automated scanning and testing throughout
  - Identify and resolve problems *before* deploying to production environments
  - Continuous compliance for deployed applications

- Open-source
  - Built upon open-source tooling – Tekton pipelines, OWASP Zap, SonarQube, git



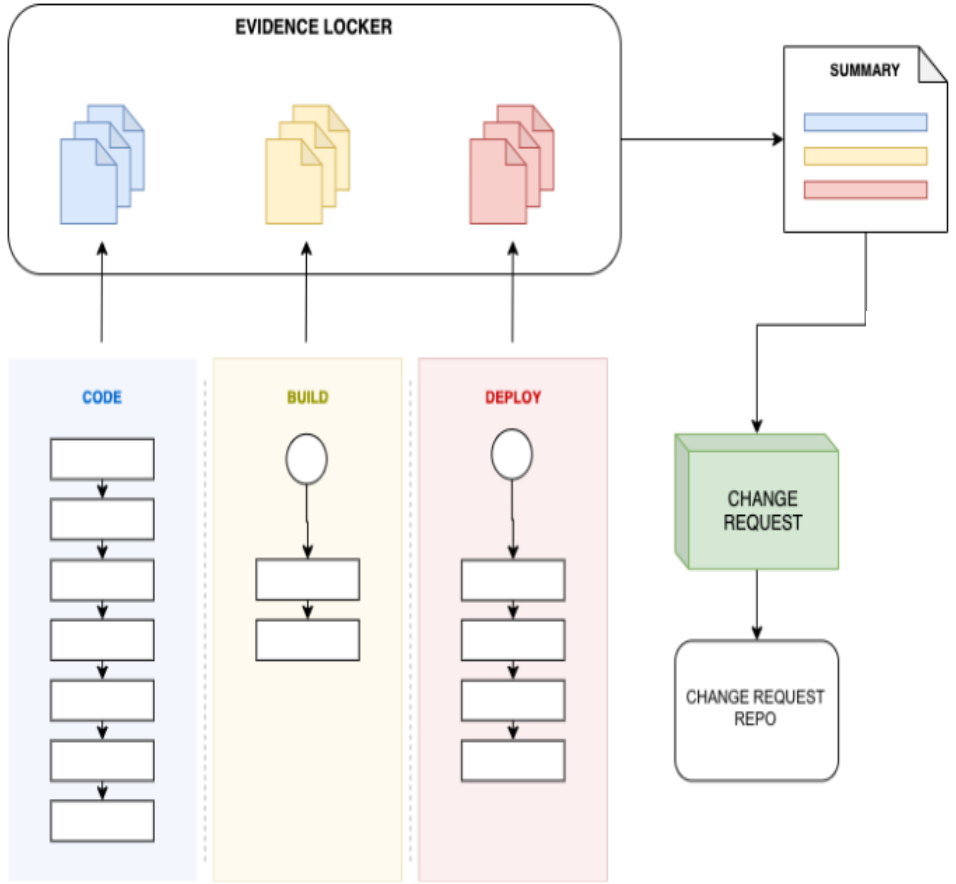
Continuous Integration

- Robust code review and branch protection checks
- Unit testing
  - Can be mandated and logged in evidence storage
- Vulnerability scans
  - Static code scans
  - Dynamic code scans
  - Dependency checks
  - Image scans
  - CIS benchmarks
- Secret detection



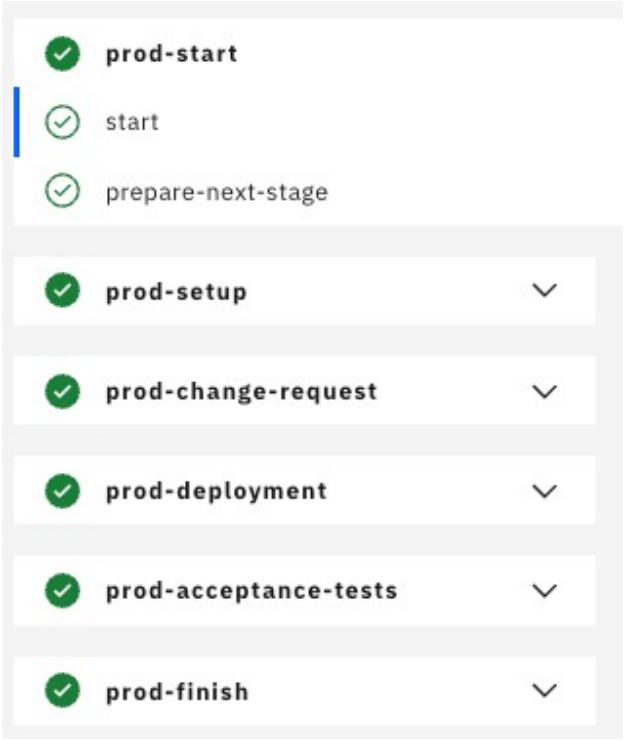
Continuous Integration

- Signed build artifacts
  - Enforced requirement for signatures
  - Skopeo integration
- SBOM generation
  - Dependency tree
  - OS packages
  - Open-source software license checks
  - Uses OWASP CycloneDX standard
- Evidence gathering and retention
  - Data is stored in immutable object storage buckets
- Builds release inventory

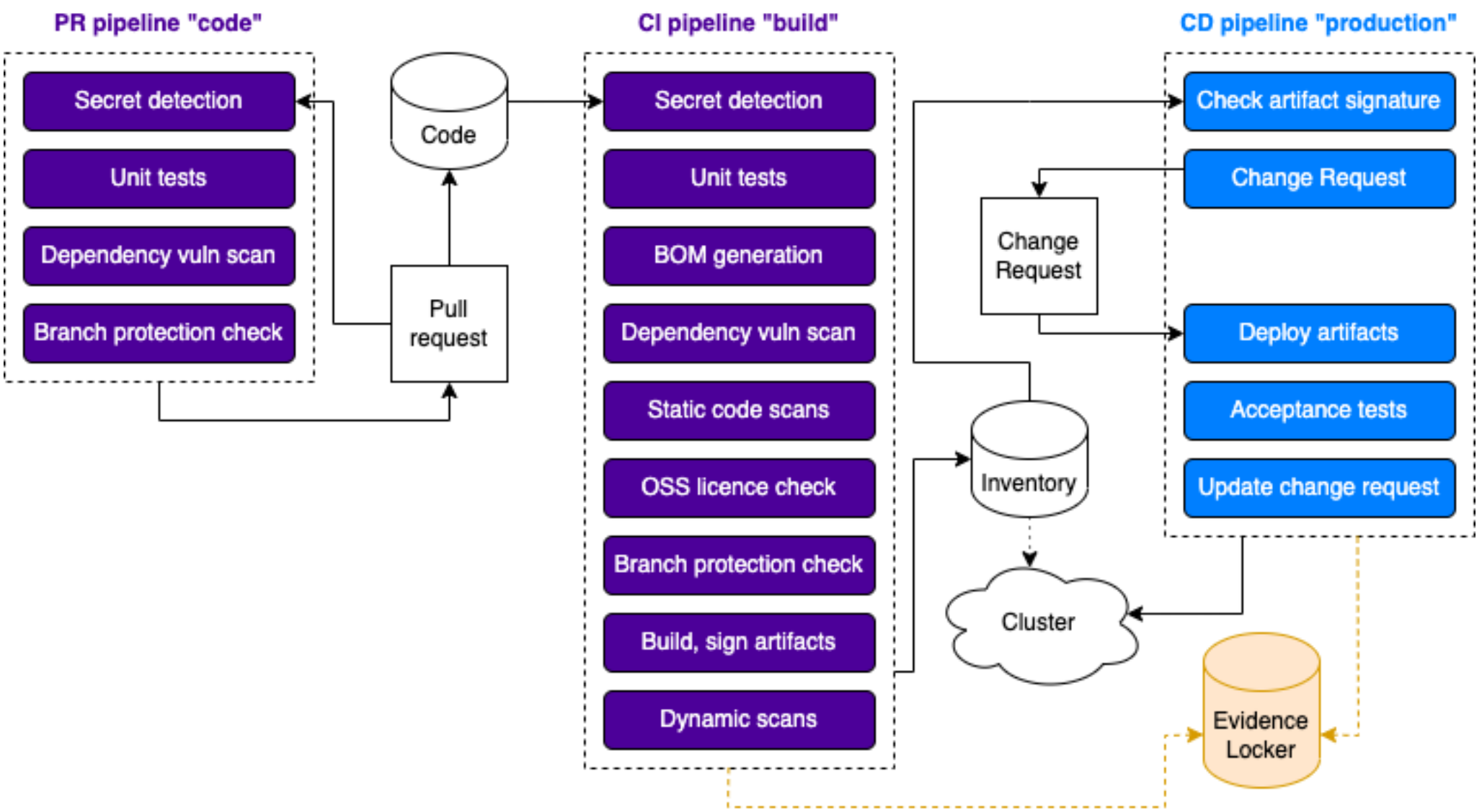


Continuous Delivery/Deployment

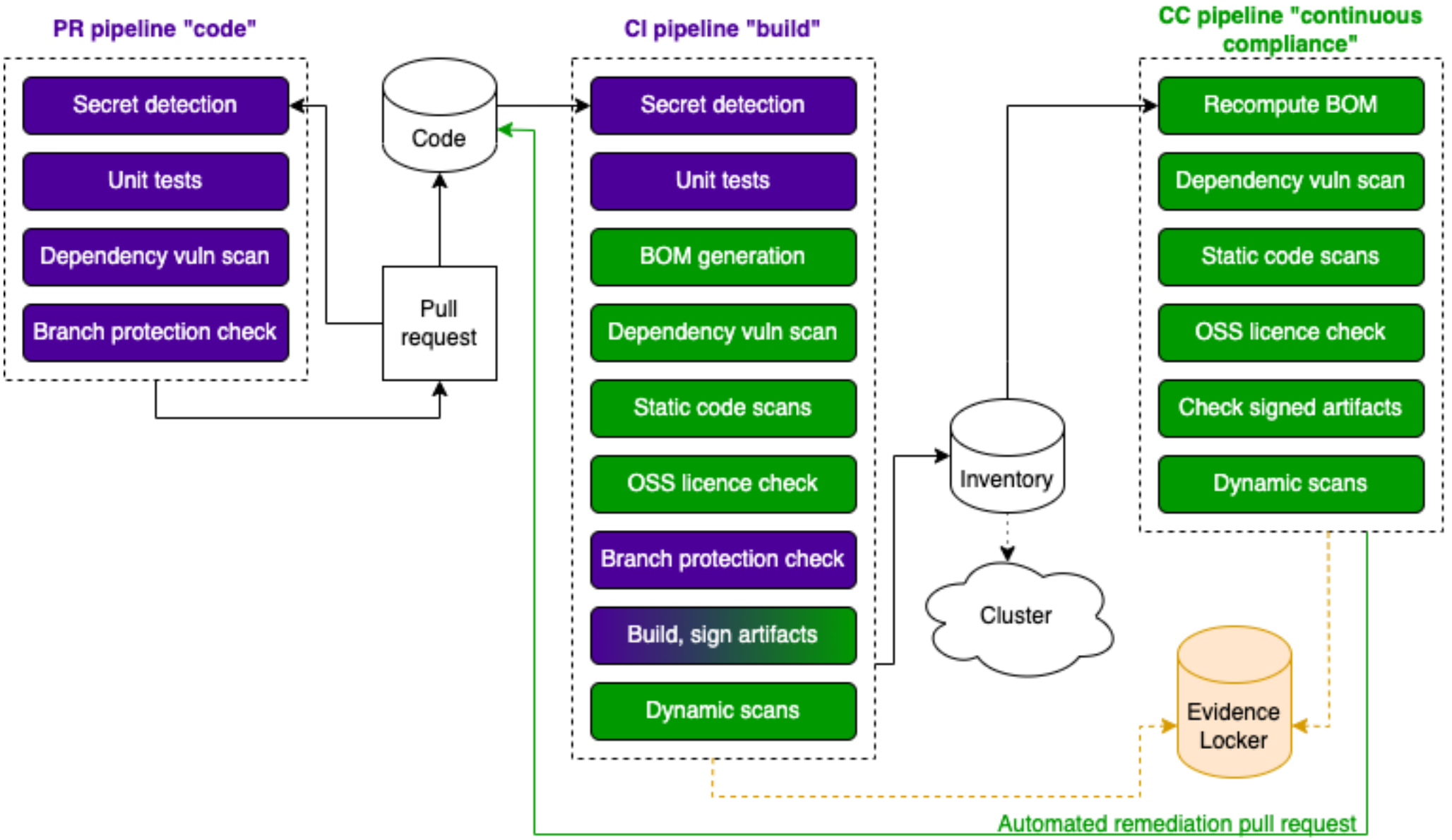
- GitOps-based release promotion between environments
- Automatic change management system
  - Deployment readiness calculations
  - Automatic change document generation
  - Uses logged vulnerabilities/failures from CI process
- Aggregated SBOM and evidence for each release
- Enforcement of signed artifact deployment
- Ability to deploy to various architectures:
  - Single or multiple Kubernetes/OpenShift clusters
  - Satellite/on-premise/hybrid locations
  - Custom targets – e.g., virtual servers, mainframes



DevSecOps Pipeline – CI / CD

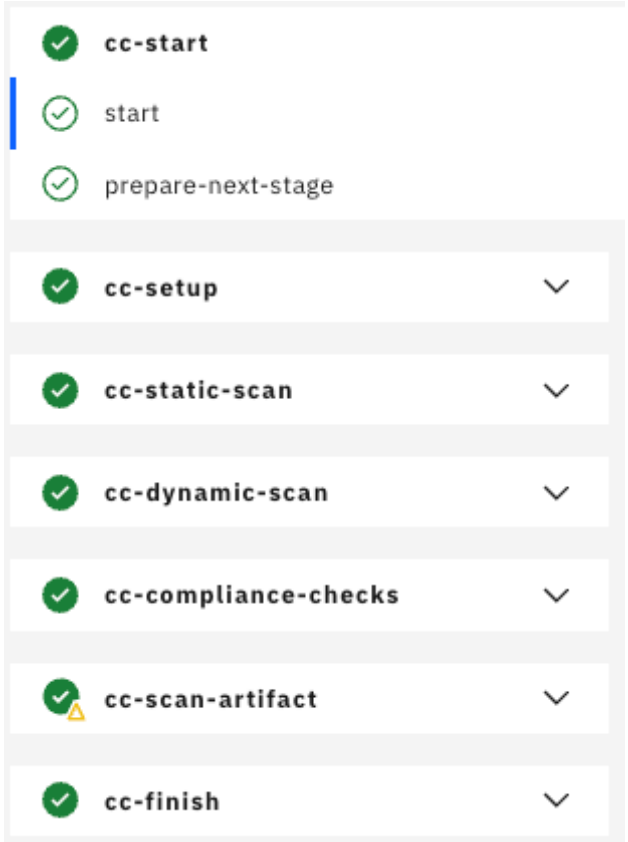


DevSecOps Pipeline – CC



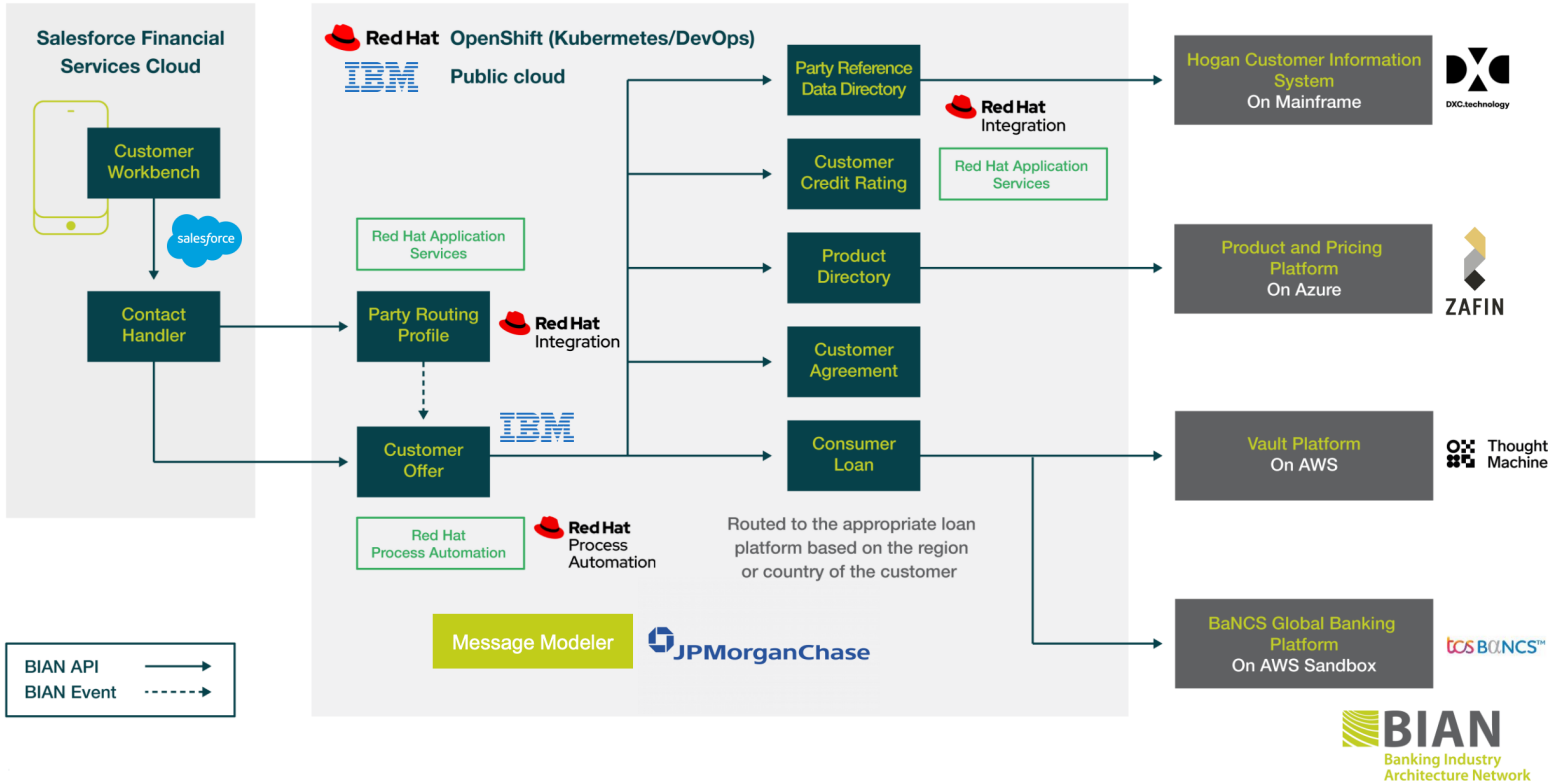
Continuous Compliance

- Continuous Compliance pipeline
  - Same scans as CI – dependency checks, source code scans etc.
  - This allows us to detect newly-reported vulnerabilities
- Integrated issue management
  - CI can determine if issue is new or previously tracked/exempted
  - Deployment readiness calculated with this in mind
  - CI/CD cannot introduce new issues into production environments
  - Based on NIST RA-5
- Continuous production release revalidation post-deployment
- Alerting and reporting
- Can be scheduled to run on any timescale

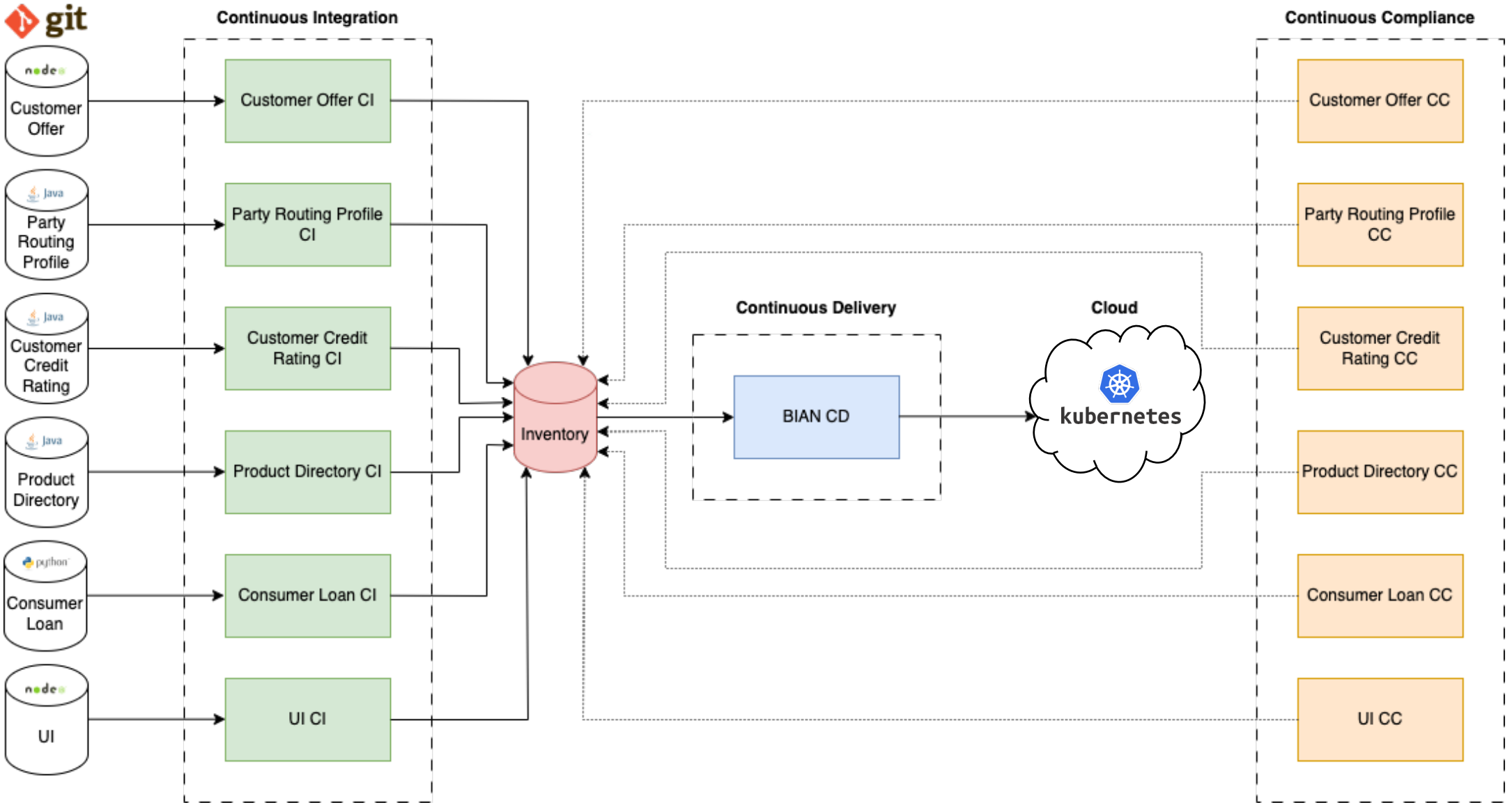


Case Study - BIAN

- **The Banking Industry Architecture Network (BIAN**) is a collaborative not-for-profit ecosystem formed of leading banks, technology providers, consultants and academics from all over the globe. It was created to establish, promote and provide a common framework for banking interoperability.
- **BIAN Coreless Initiative** supports Core Banking renewal and empowers financial institutions to select best-of-breed partners to help bring new services to market quickly and efficiently through BIAN architectures.
- **Coreless V2 Scenario:** A consumer procures a loan tailored for her needs, through a safe and secure online channel offered by a bank. The bank application employs an ecosystem of partner applications interoperating on the BIAN architecture to deliver this service.



BIAN Pipeline Flow



Lessons Learned

- Start with Continuous Compliance
  - Detect vulnerabilities, and track them
- Look to eliminate vulnerabilities with provider team
  - Can add exemptions for non-critical issues
- Combine deployment toolchains
  - Use the inventory to deploy each microservice in turn
- Educate each component/microservice provider
  - Challenge: Components developed by different ISVs
- Reusability
  - Use shared libraries
  - Combine CI toolchains for similar applications
  - Can use backing CLI with other CI systems e.g., Jenkin

Call to Action

- You can reduce your Cyber Risk by improving your pipelines with DevSecOps capabilities:
  - Reliable, repeatable automation
    - Everything as code!
  - Mitigate security risks as early as possible
  - Maintain compliance by continually scanning deployments

- Learn more about DevSecOps capabilities and tools
  - Cocoa, scanning tools, vulnerability assessors, compliance mechanisms

- Join us for a detailed session/demo at IBM Booth – Thursday at 15:00 CET

KubeCon CloudNativeCon
Europe 2023
North America 2021

Please scan the QR Code above
to leave feedback on this session