# OpenShift & Kubernetes Show-and-Tell Series

## http://red.ht/openshiftshowandtell

| Date/Time (PST) | Better Together "Seeing is Believing" Technical Thursdays |
|---|---|
| 8/19 12:00-12:45 PM | From first-mile multicluster provisioning to last-mile application delivery with Red Hat Advanced Cluster Management for Kubernetes and Red Hat OpenShift GitOps |
| 8/26 12:00-12:45 PM | From first-mile data resiliency to last-mile disaster recovery with Red Hat Data Services and Red Hat OpenShift |
| 9/2 12:00-12:45 PM | Application portability and multicluster management with Red Hat Advanced Cluster Management for Kubernetes and Red Hat OpenShift across the hybrid cloud |
| 9/9 12:00-12:45 PM | Advanced observability and policy compliance with Red Hat Advanced Cluster Security for Kubernetes, Red Hat Advanced Cluster Management for Kubernetes and Red Hat OpenShift across the hybrid cloud |
| 9/16 12:00-12:45 PM | From first-mile image scanning to last-mile software delivery with Red Hat Advanced Cluster Security for Kubernetes and Red Hat OpenShift Pipelines |
| 9/23 12:00-12:45 PM | Bringing Windows-based applications and VM-based databases to Red Hat OpenShift with Red Hat OpenShift Virtualization and Windows Containers |

# OpenShift & Kubernetes Show-and-Tell Series

- Please direct your Q&A into the primetime forum.

- We have technologists from our Cloud Platforms business unit and the field monitoring the Q&A

- Any outstanding questions will be addressed at the end of the presentation or responses will be facilitated after the briefing.

- The content will be made available after the call on the Red Hat BrightTALK channel.

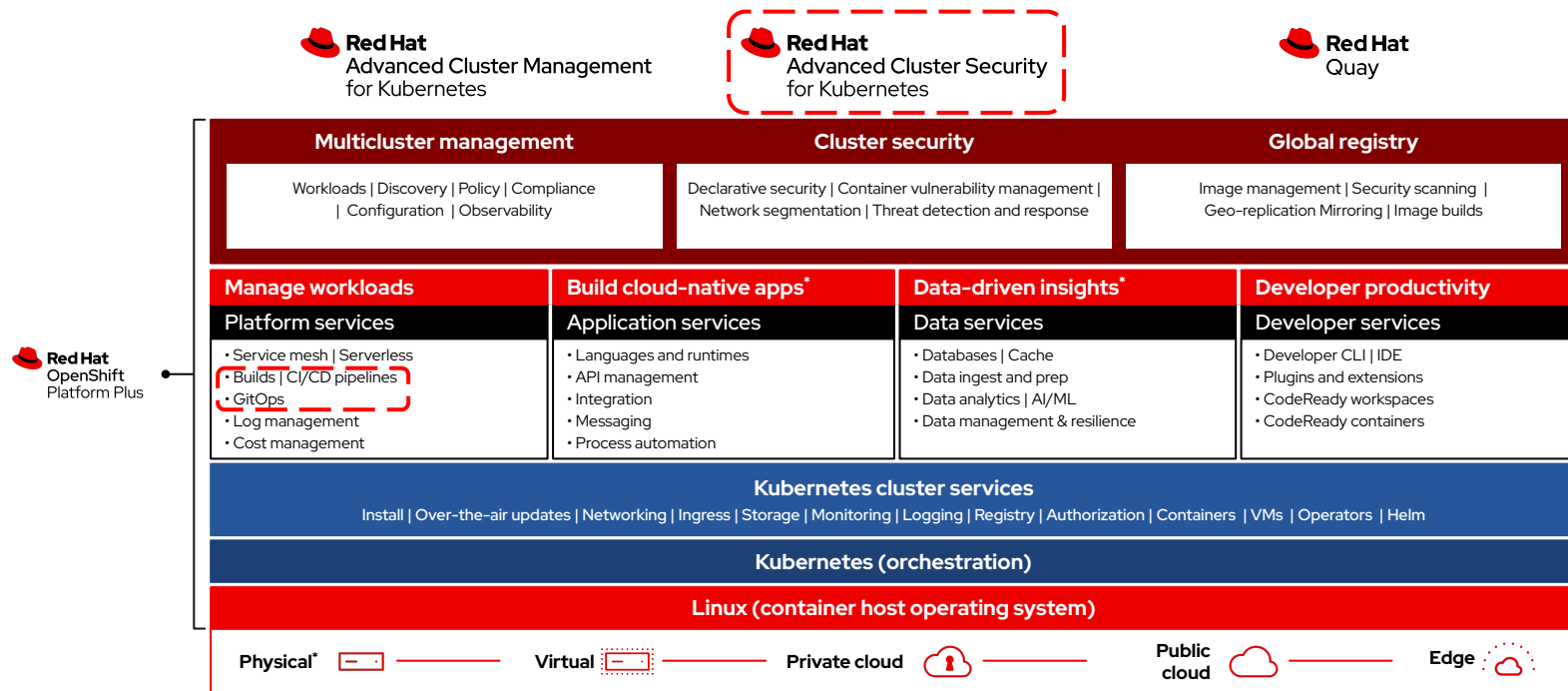- For questions regarding these sessions, please contact your Red Hat account team

Red Hat

From first-mile image scanning to last-mile software delivery with Red Hat Advanced Cluster Security for Kubernetes and Red Hat OpenShift Pipelines

Girish Krishnan

Principal Architect

Vinay Bhalerao

Sr Solutions Architect

Jp

**Red Hat**

# Draw Me a Picture!

**Red Hat**
Advanced Cluster Management
for Kubernetes

**Red Hat**
Advanced Cluster Security
for Kubernetes

**Red Hat**
Quay

**Red Hat**
OpenShift
Platform Plus

| Multicluster management | Cluster security | Global registry |
|---|---|---|
| Workloads \| Discovery \| Policy \| Compliance \| Configuration \| Observability | Declarative security \| Container vulnerability management \| Network segmentation \| Threat detection and response | Image management \| Security scanning \| Geo-replication Mirroring \| Image builds |

| Manage workloads | Build cloud-native apps* | Data-driven insights* | Developer productivity |
|---|---|---|---|
| **Platform services** | **Application services** | **Data services** | **Developer services** |
| • Service mesh \| Serverless<br>• Builds \| CI/CD pipelines<br>• GitOps<br>• Log management<br>• Cost management | • Languages and runtimes<br>• API management<br>• Integration<br>• Messaging<br>• Process automation | • Databases \| Cache<br>• Data ingest and prep<br>• Data analytics \| AI/ML<br>• Data management & resilience | • Developer CLI \| IDE<br>• Plugins and extensions<br>• CodeReady workspaces<br>• CodeReady containers |

**Kubernetes cluster services**
Install | Over-the-air updates | Networking | Ingress | Storage | Monitoring | Logging | Registry | Authorization | Containers | VMs | Operators | Helm

**Kubernetes (orchestration)**

**Linux (container host operating system)**

**Physical*** — **Virtual** — **Private cloud** — **Public cloud** — **Edge**

4

* Red Hat OpenShift® includes supported runtimes for popular languages/frameworks/databases. Additional capabilities listed are from the Red Hat Application Services and Red Hat Data Services portfolios.

**Red Hat**

# Red Hat Advanced Cluster Security for Kubernetes

A cloud workload protection platform and cloud security posture management to enable you to "shift left"

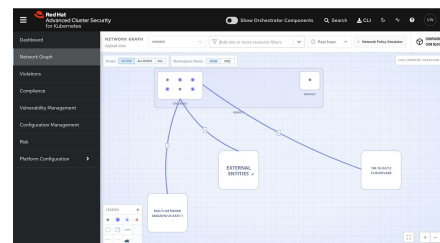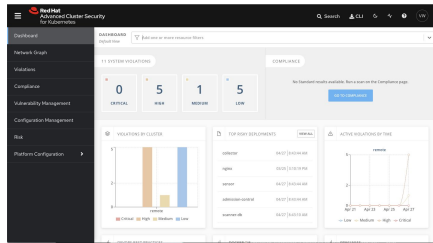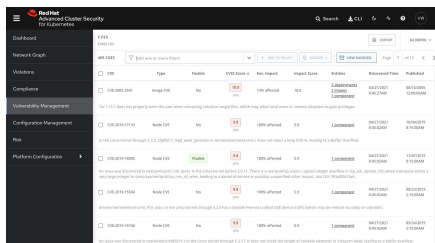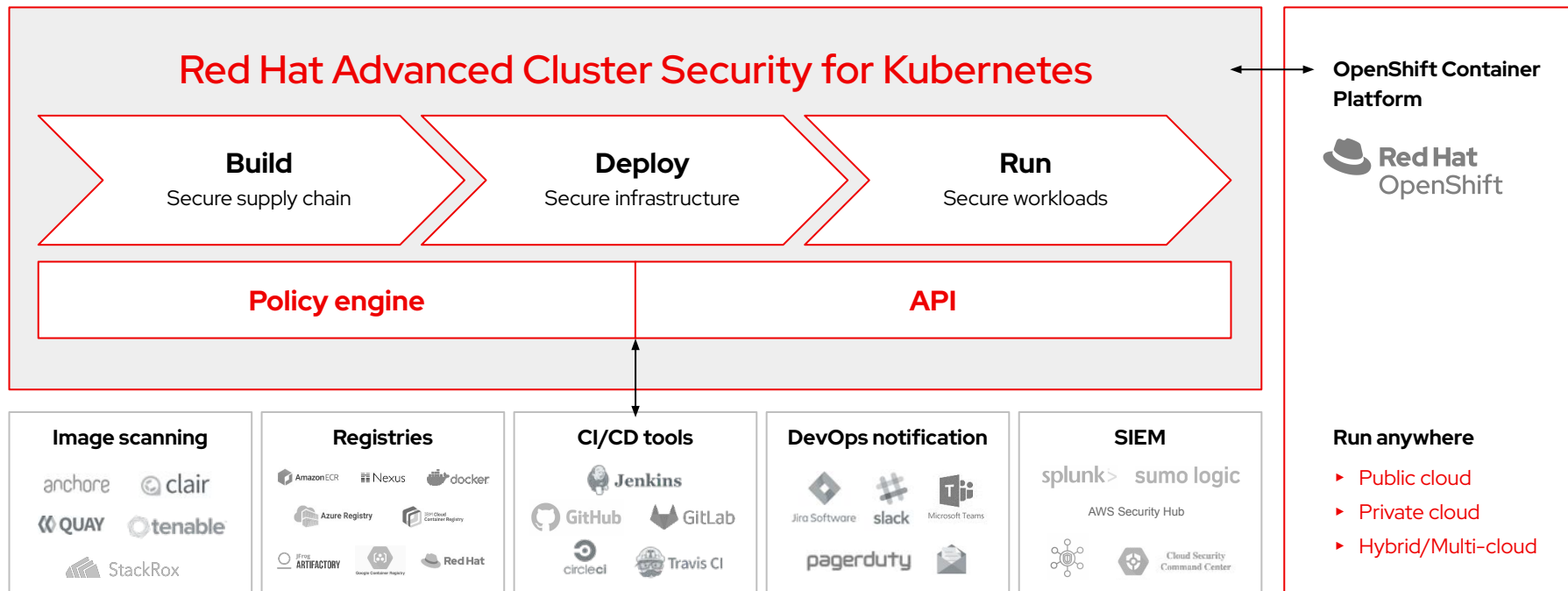| Shift left | Kubernetes security posture management (KSPM) | Cloud workload protection (CWPP) |
|---|---|---|
| Secure supply chain | Secure infrastructure | Secure workloads |
| Extend scanning and compliance into development (DevSecOps) | Leverage built-in Kubernetes security posture management to identify and remediate configurations and deployments | Maintain and enforce a "zero-trust execution" approach to workload protection |

Red Hat

# Red Hat ACS Integration and Focus

Red Hat Advanced Cluster Security for Kubernetes

**Red Hat Advanced Cluster Security for Kubernetes**

OpenShift Container Platform

**Build**
Secure supply chain

**Deploy**
Secure infrastructure

**Run**
Secure workloads

**Policy engine**

**API**

**Image scanning**
anchore    clair
QUAY    tenable
StackRox

**Registries**
Amazon ECR    Nexus    docker
Azure Registry    IBM Cloud Container Registry
JFrog ARTIFACTORY    Google Container Registry    Red Hat

**CI/CD tools**
Jenkins
GitHub    GitLab
circleci    Travis CI

**DevOps notification**
Jira Software    slack    Microsoft Teams
pagerduty

**SIEM**
splunk>    sumo logic
AWS Security Hub
Cloud Security Command Center

**Run anywhere**
‣ Public cloud
‣ Private cloud
‣ Hybrid/Multi-cloud

6

# Continuous Integration and Continuous Delivery

| Build | Test | Security Checks | Release | Deploy Stage | Deploy Prod |

**OpenShift Builds**

Automate building container images using Kubernetes tools

**OpenShift Pipelines**

Kubernetes-native on-demand delivery pipelines

**OpenShift GitOps**

Declarative GitOps for multi-cluster continuous delivery

GitHub    GitLab    Azure DevOps    Travis CI

Red Hat

# OpenShift Pipelines

## Built for Kubernetes

Cloud-native pipelines taking advantage of Kubernetes execution, operational model and concepts

## Scale on-demand

Pipelines run and scale on-demand in isolated containers, with repeatable and predictable outcomes

## Secure pipeline execution

Kubernetes RBAC and security model ensures security consistently across pipelines and workloads

## Flexible and powerful

Granular control over pipeline execution details on Kubernetes, to support your exact requirements

Powered by **TEKTON**

Red Hat

# OpenShift GitOps

## Multi-cluster config management

Declaratively manage cluster and application configurations across multi-cluster OpenShift and Kubernetes infrastructure with Argo CD

## Automated Argo CD install and upgrade

Automated install, configurations and upgrade of Argo CD through OperatorHub

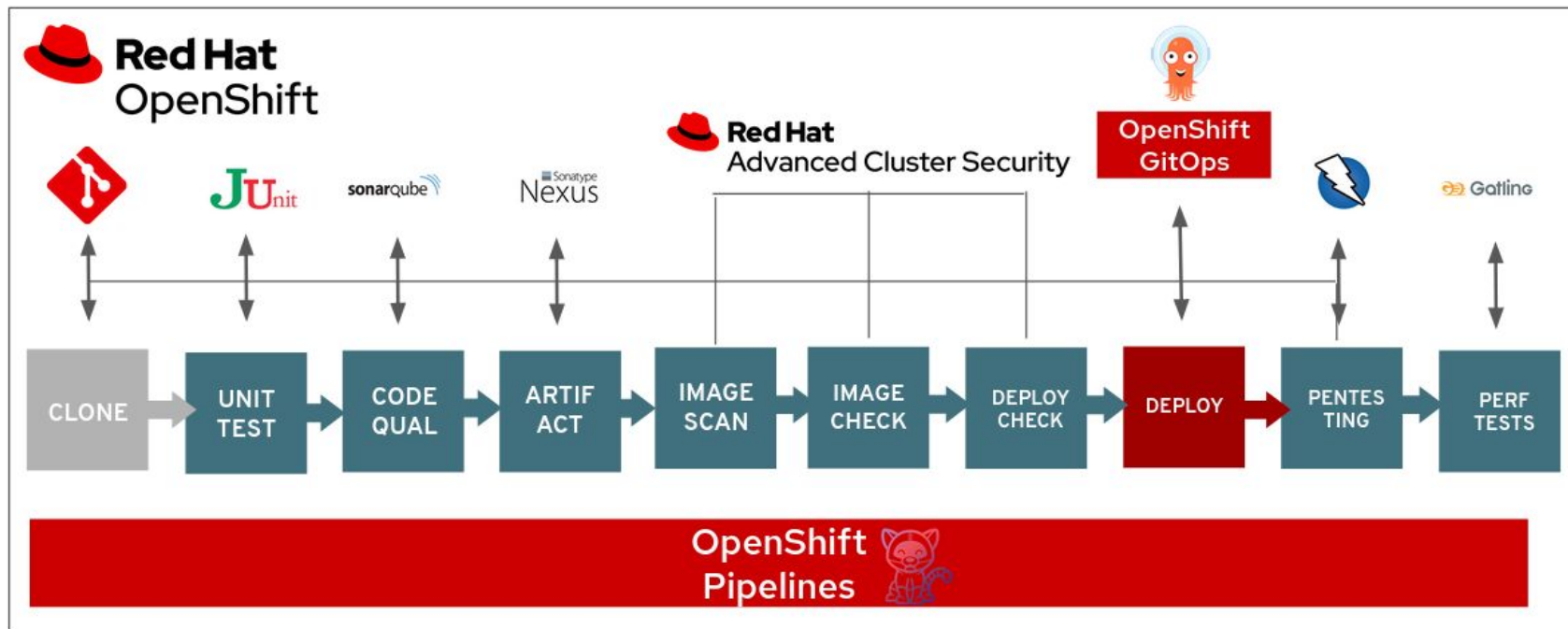## Opinionated GitOps bootstrapping

Bootstrap end-to-end GitOps workflows for application delivery using Argo CD and Tekton with GitOps Application Manager CLI

## Deployments and environments insights

Visibility into application deployments across environments and the history of deployments in the OpenShift Console

Powered by argo

Red Hat

# Securing your CI/CD pipeline for software delivery

https://github.com/rcarrata/devsecops-demo#devsecops-pipeline-demo

# Tell me what you are about to show me



Red Hat
OpenShift
Container Platform

Red Hat
Advanced Cluster Security
for Kubernetes

Continuous Integration (CI)

Continuous Delivery (CD)

Secure Software Delivery

ChatOps Integration

# Closing Thoughts: Securing Software Supply Chain

**Best practices (Control application security)**

**Red Hat UBI**
▶ Use trusted sources for external content such as base images

**Red Hat Quay**
▶ Use a trusted private registry to manage supply chain risk

**OpenShift Pipelines**
▶ Automate your CI/CD pipeline to enable rapid updates

**Red Hat CodeReady**
**Red Hat Advanced Cluster Security**
▶ Integrate security tools (KubeLinter, ACS scanner) and gates in your pipeline to identify
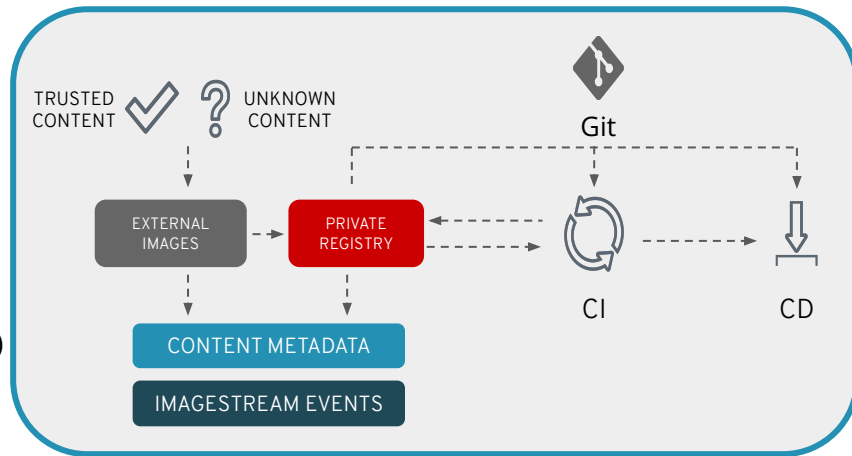  - Known vulnerabilities
  - Application misconfigurations

**Red Hat Advanced Cluster Management**
▶ Use policy–based deployment tools to manage application placement (e.g. locality)

# Q&A

Red Hat

# Thank you

Red Hat is the world's leading provider of
enterprise open source software solutions.
Award-winning support, training, and consulting
services make Red Hat a trusted adviser to the
Fortune 500.

linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat

Red Hat

# The CI/CD pipeline for containers needs automation

TRUSTED CODE REPOS

**Red Hat**
Advanced Cluster Security

CCB
Rapid Approval

| REQ | DEV | UNIT TEST | CODE QUAL | SEC SCAN | INT TEST | QA UAT | PROD |

Pipeline Tasks

AUTOMATE
QUALITY & SECURITY

- Code Ready
- IDE Plugins
- Quay with Clair
- Jenkins
- Tekton

- Automate rebuild / redeploy
  - Source to Image
  - ImageStreams
- Allow / Disallow registry access
- Security Context Constraints

**Red Hat**
CodeReady

**Red Hat**
Quay

**Red Hat**
OpenShift

Hat

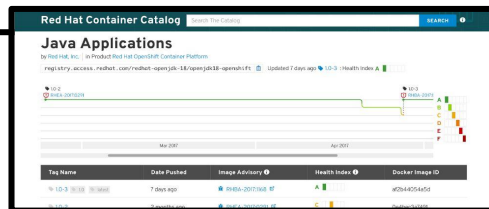# Securing your CI/CD pipeline for software delivery

## *Automated quality and security: because you can't inspect quality into a product*

Automatically prohibit untrusted
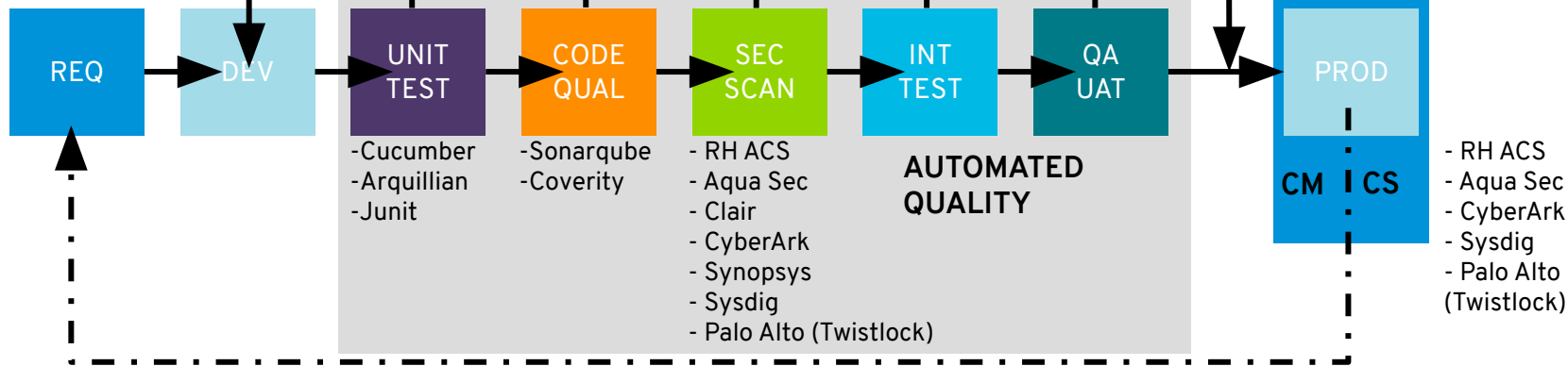containers via Openshift policy

Trusted repos
registry.redhat.io

Private registry
- RH Quay
- JFrog Artifactory
- Sonatype Nexus

**Red Hat Container Catalog**

**Java Applications**
by Red Hat, Inc. | In Product Red Hat OpenShift Container Platform

registry.access.redhat.com/redhat-openjdk-18/openjdk18-openshift | Updated 7 days ago ❤ 1.0-3 | Health Index A

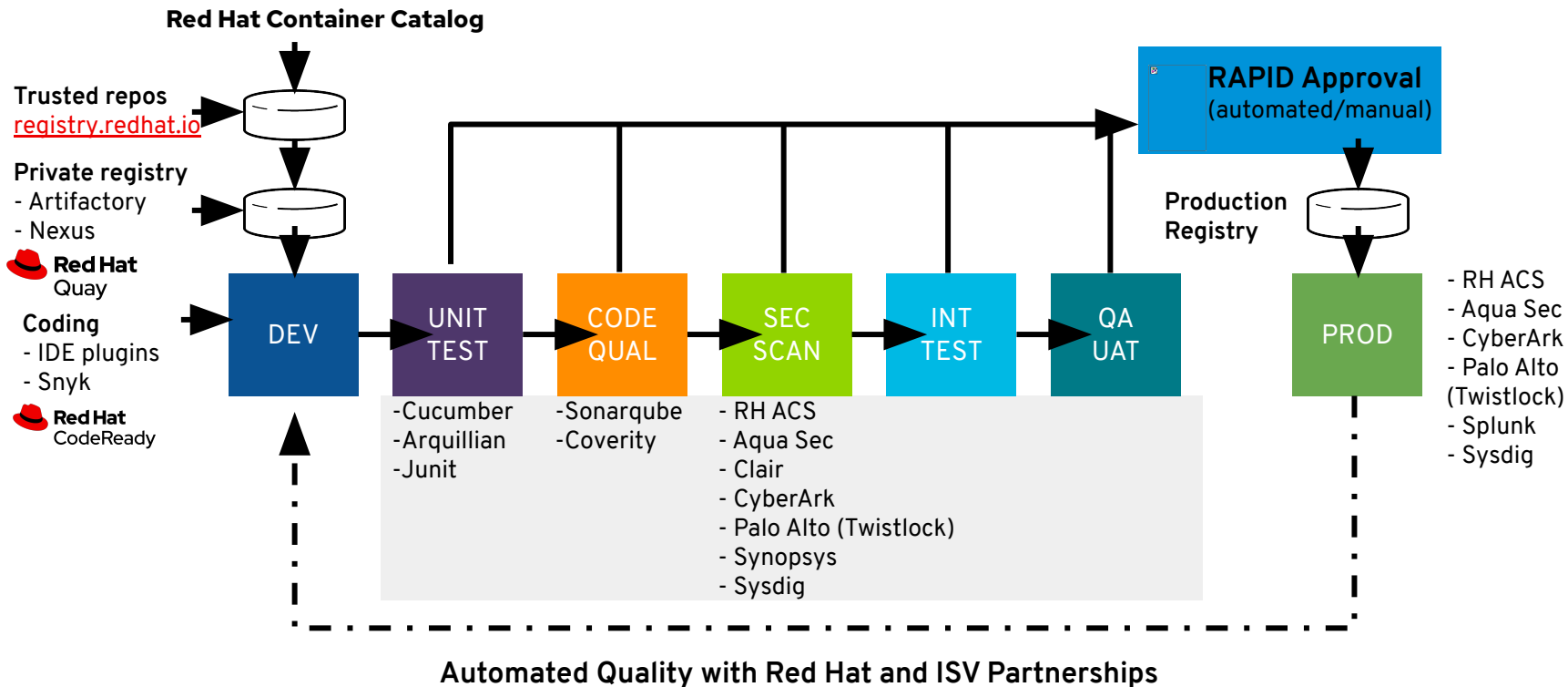| Tag Name | Date Pushed | Image Advisory ❶ | Health Index ❶ | Docker Image ID |
|----------|-------------|------------------|----------------|-----------------|
| 1.0-3 | 7 days ago | RHBA-2017:0168 | A | a2b44054a5d |

Secure Supply Chain
of Quality Parts
- Quality Assurance
- Certifications
- Signing & Secure
- Distribution

Change Control Board
**RAPID ATO**

| REQ | DEV | UNIT TEST | CODE QUAL | SEC SCAN | INT TEST | QA UAT | PROD CM \| CS |
|-----|-----|-----------|-----------|----------|----------|--------|--------------|

-Cucumber
-Arquillian
-Junit

-Sonarqube
-Coverity

- RH ACS
- Aqua Sec
- Clair
- CyberArk
- Synopsys
- Sysdig
- Palo Alto (Twistlock)

**AUTOMATED
QUALITY**

- RH ACS
- Aqua Sec
- CyberArk
- Sysdig
- Palo Alto
(Twistlock)

**OPENSHIFT SOFTWARE FACTORY**

Red Hat Container Catalog: Java Applications
More about the Container Health Index

🎩 **Red Hat**

# Securing your CI/CD Pipeline with Red Hat

**Red Hat Container Catalog**

**Trusted repos**
registry.redhat.io

**Private registry**
- Artifactory
- Nexus

**Red Hat** Quay

**Coding**
- IDE plugins
- Snyk

**Red Hat** CodeReady

**RAPID Approval** (automated/manual)

**Production Registry**

**DEV**

**UNIT TEST**
-Cucumber
-Arquillian
-Junit

**CODE QUAL**
-Sonarqube
-Coverity

**SEC SCAN**
- RH ACS
- Aqua Sec
- Clair
- CyberArk
- Palo Alto (Twistlock)
- Synopsys
- Sysdig

**INT TEST**

**QA UAT**

**PROD**

- RH ACS
- Aqua Sec
- CyberArk
- Palo Alto (Twistlock)
- Splunk
- Sysdig

**Automated Quality with Red Hat and ISV Partnerships**

Red Hat Container Catalog: Java Applications
More about the Container Health Index

# KubeLinter: Enforce Kubernetes security best practices
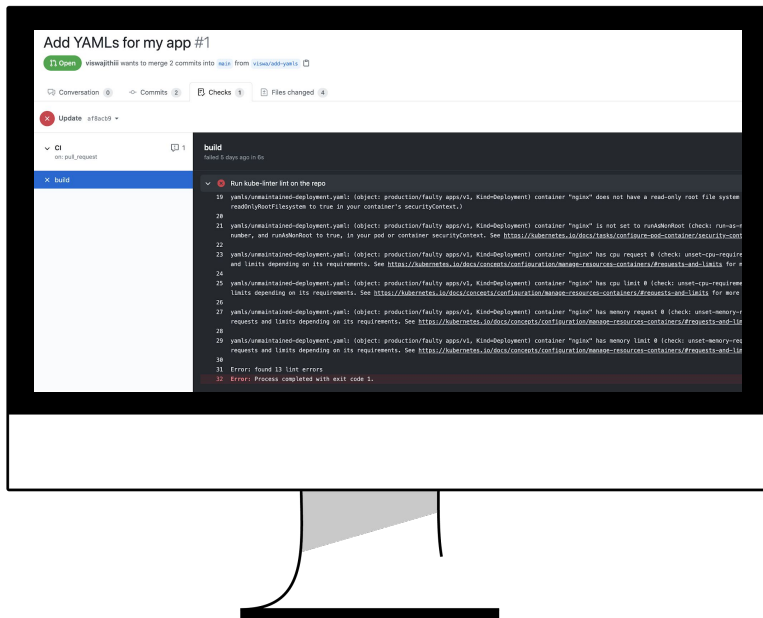


## KubeLinter as a GitHub action

▸ Checks Kubernetes YAML files and Helm charts

▸ 16 default checks

▸ Extensible with custom checks

▸ Integrates with any CI tool

https://github.com/stackrox/kube-linter

Red Hat