Security first: Automating CI/CD pipelines and policing applications

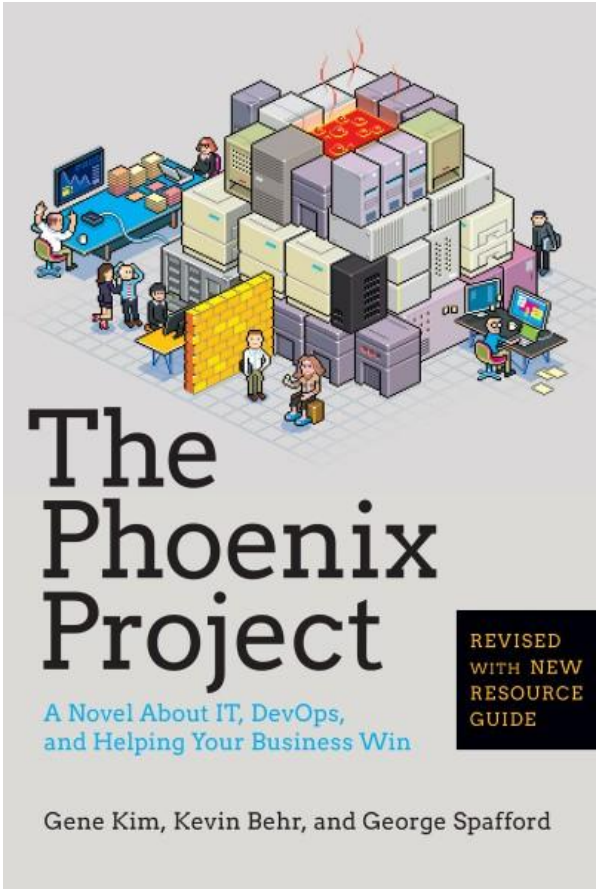
Justin Goldsmith
Senior Architect FSI Consulting
jgoldsmith@redhat.com

HOW DEVS AND OPS VIEW SECURITY

Red Hat

WHY DevSecOps?

- DevOps “purists” point out that security was always part of DevOps
- Did people just not read the book? Are practitioners skipping security?
- DevSecOps practitioners say it’s about how to **continuously integrate** and **automate** security at **scale**



Red Hat

Source: IT Revolution, DevOps Enterprise abstract word cloud, 2014.

Red Hat

Source: IT Revolution, DevOps Enterprise abstract word cloud, 2014.

Has much changed?

Ironically. Shift-left much?

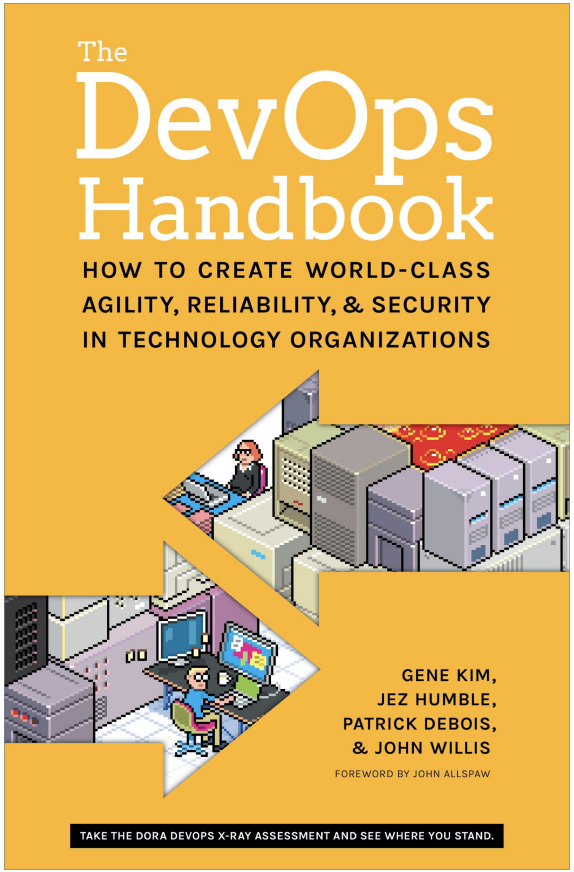
PART VI—THE TECHNICAL PRACTICES OF INTEGRATING INFORMATION SECURITY, CHANGE MANAGEMENT, AND COMPLIANCE

Part VI Introduction

22 Information Security as Everyone's Job, Every Day **23** Protecting the Deployment Pipeline and Integrating into Change Management and Other Security and Compliance Controls Conclusion to the DevOps Handbook: *A Call to Action*

Additional Material

Appendices Additional Resources Endnotes Index Acknowledgments Author Biographies



Red Hat

GLASS HALF EMPTY, GLASS HALF FULL

*"... we estimate that **fewer than 20% of enterprise security architects have engaged with their DevOps initiatives** to actively and systematically incorporate information security into their DevOps initiatives; and fewer still have achieved the high degrees of security automation required to qualify as DevSecOps."*

*"**By 2019, more than 70%** of enterprise DevOps initiatives will have incorporated automated security vulnerability and configuration scanning for open source components and commercial packages, **up from less than 10% in 2016.**"*

DevSecOps: How to Seemlessly Integrate Security Into DevOps, Gartner Inc. September 2016

Red Hat

Security is seen as an inhibitor to DevOps

Gartner

DevSecOps: How to Seamlessly Integrate Security Into DevOps

Published: 30 September 2016 **ID:** G00315283

Analyst(s): Neil MacDonald, Ian Head

Information security architects must integrate security at multiple points into DevOps workflows in a collaborative way that is largely transparent to developers, and preserves the teamwork, agility and speed of DevOps and agile development environments, delivering "DevSecOps."

Key Challenges

- DevOps compliance is a top concern of IT leaders, but information security is seen as an inhibitor to DevOps agility.
- Security infrastructure has lagged in its ability to become "software defined" and programmable, making it difficult to integrate security controls into DevOps-style workflows in an automated, transparent way.
- Modern applications are largely "assembled," not developed, and developers often download and use known vulnerable open-source components and frameworks.

Challenges:

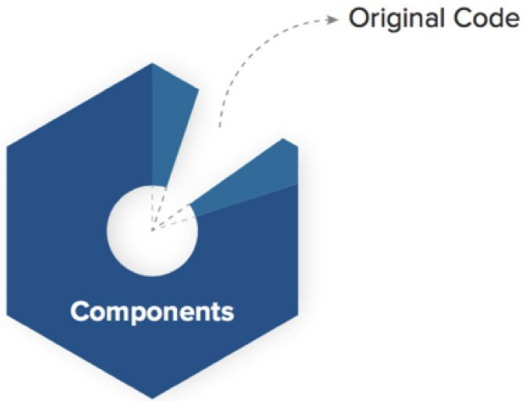
- Security infrastructure has lagged in its ability to become ‘software defined’ and programmable, making it difficult to integrate…
- Modern applications are largely ‘assembled,’ not developed, and developers often download and use known vulnerable open-source components and frameworks

Red Hat

Applications are ‘assembled’…

…utilizing billions of available libraries, frameworks and utilities

- Not all are created equal, some are healthy and some are not
- All go bad over time, they age like milk, not like wine
- Data shows enterprises consumed an average 229,000 software components annually, of which 17,000 had a known security vulnerability.



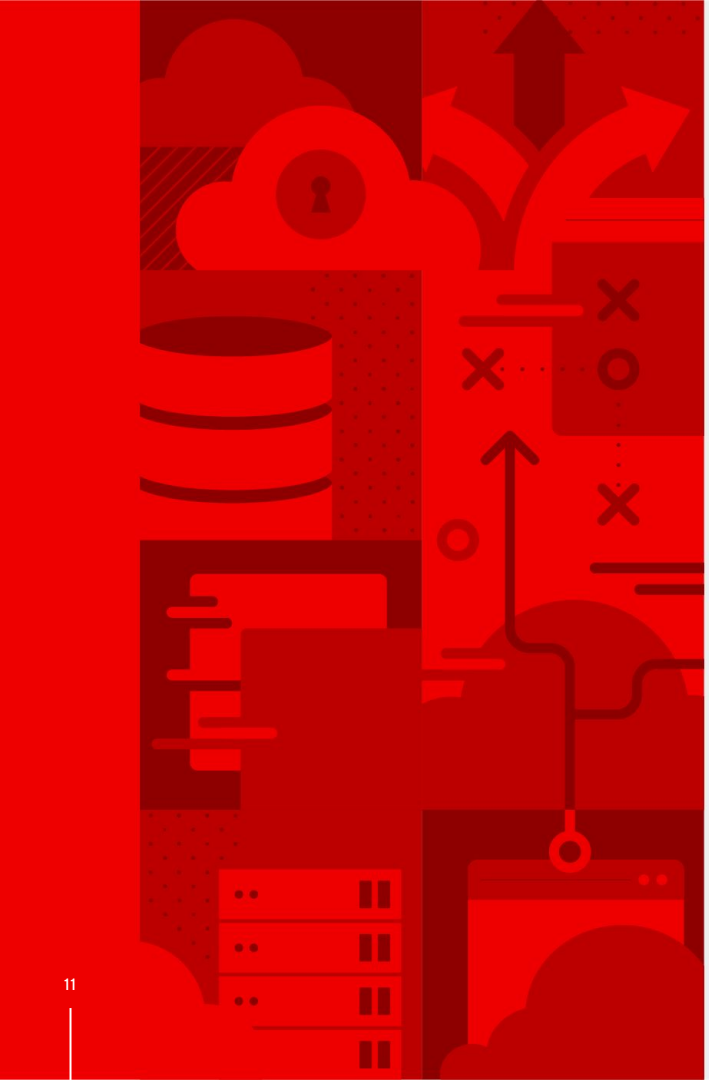
80% to 90% of modern apps consist of assembled components.

Red Hat

THE PERFECT STORM

- Cloud
- DevOps
- Open Source Software innovation explosion
- Containers/Microservices
- Digital transformation

Red Hat



DevSecOps: The open source way

Red Hat

YOU MANAGE RISK BY


Securing the Assets


Securing the Dev


Securing the Ops

Red Hat

SECURING THE ASSETS

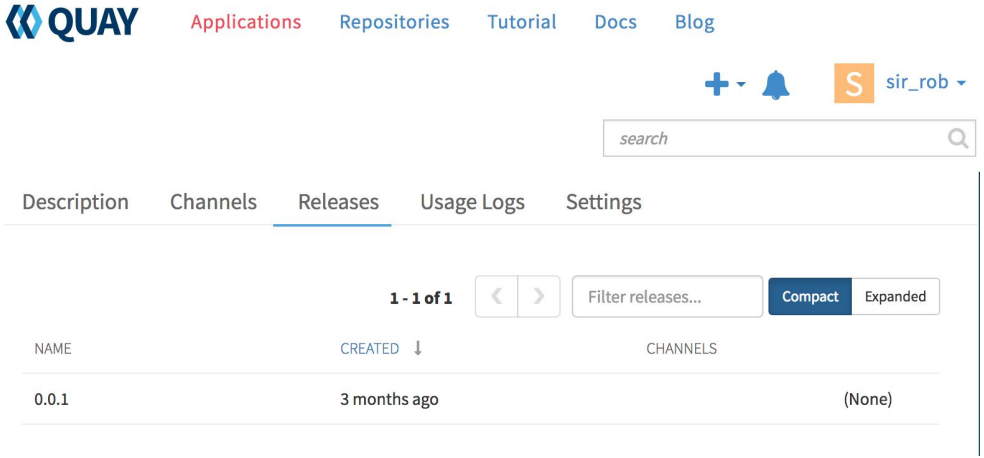
- Building code
  - Watching for changes in how things get built
  - Signing the builds
- Built assets
  - Scripts, binaries, packages (RPMs), containers (OCI images), machine images (ISOs, etc.)
  - Registries (Service, Container, App)
  - Repositories (Local on host images assets)

Safe at Titan Missile Museum
https://upload.wikimedia.org/wikipedia/commons/5/59/Red_Safe%2C_Titan_Missile_Museum.jpg

SECURING THE SOFTWARE ASSETS - E.G. IMAGE REGISTRY

Public and private registries

- Do you require a private registry?
- What security meta-data is available for your images?
- Are the images in the registry updated regularly?
- Are there access controls on the registry? How strong are they? Who can push images to the registry?



Red Hat

SECURING THE ASSETS

HEALTH - Security freshness

- Freshness Grade for container security.
- Monitor image registry to automatically replace affected images
- Use policies to gate what can be deployed: e.g. if an image is below a certain freshness grade.

Grade A: This image has no missing Critical or Important security errata. It may be missing errata that fix Moderate or Low security flaws.

Grade B: This image may be missing Critical or Important security errata, but no missing Critical flaw is older than 7 days and no missing Important flaw is older than 30 days (from the date the CVE was first fixed in an erratum). It may be missing errata that fix Moderate or Low security flaws, of any age.

Grade C: This image may be missing Critical or Important security errata, but no missing Critical flaw is older than 30 days and no missing Important flaw is older than 90 days (from the date the CVE was first fixed in an erratum). It may be missing errata that fix Moderate or Low security flaws, of any age.

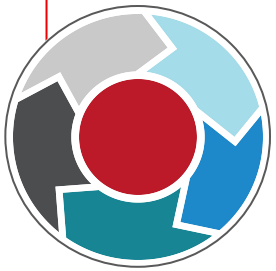
Grade D: This image may be missing Critical or Important security errata, but no missing Critical flaw is older than 90 days and no missing Important flaw is older than 365 days (from the date the CVE was first fixed in an erratum). It may be missing errata that fix Moderate or Low security flaws, of any age.

Grade E: This image may be missing Critical or Important security errata, but no missing Critical or Important flaw is older than 365 days (from the date the CVE was first fixed in an erratum). It may be missing errata that fix Moderate or Low security flaws, of any age.

Grade F: This image may be missing Critical or Important security errata, and they are older than 365 days (from the date the CVE was first fixed in an erratum). It may be missing errata that fix Moderate or Low security flaws, of any age. Or the container is out of its lifecycle.

Grade Unknown: This image cannot be scanned as it is missing metadata required to perform the freshness grade calculation.

Red Hat



RED HAT'S SECURE SUPPLY CHAIN

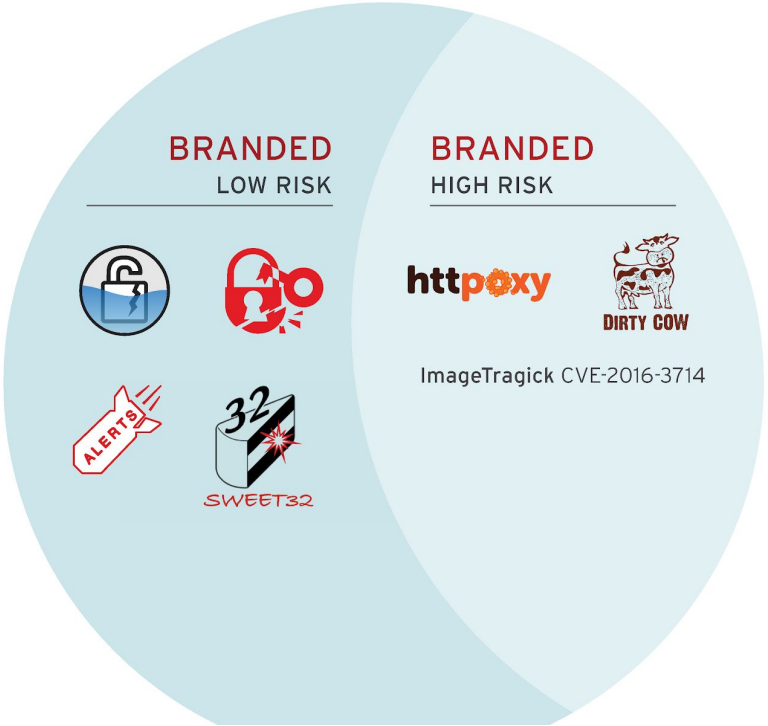
- Community leadership
- Package selection
- Manual inspection
- Automated inspection
- Packaging guidelines
- Trusted builds

- Quality assurance
- Certifications
- Signing
- Distribution
- Support
- Security updates/patches

Red Hat

Red Hat Security Response

“No hype” assessment independent of vulnerability branding



NOT BRANDED
HIGH RISK

Kernel keychain overflow CVE-2016-0728

glibc overflow CVE-2015-7547

Samba DCE/RPC CVE-2015-5370

Overcloud image password CVE-2016-4474

JGroups auth bypass CVE-2016-2141

Kernel challenge ack CVE-2016-5696

BIND DoS CVE-2016-2776+

Red Hat

SECURING THE DEVELOPMENT PROCESS

- Likely many parallel builds
- Source code
  - Where is it coming from?
  - Who is it coming from?
- Supply Chain Tooling
  - CI tools (e.g. Jenkins)
  - Testing tools
  - Scanning Tools (e.g. Black Duck, Sonatype)

Boeing's Everett factory near Seattle
https://upload.wikimedia.org/wikipedia/commons/c/c8/At_Boeing%27s_Everett_factory_near_Seattle_%289130160595%29.jpg

Vulnerability Analysis Complements SAST/DAST

Static and Dynamic Analysis

- Discover common security patterns
- Challenged by nuanced bugs
- Focuses on your code; not upstream

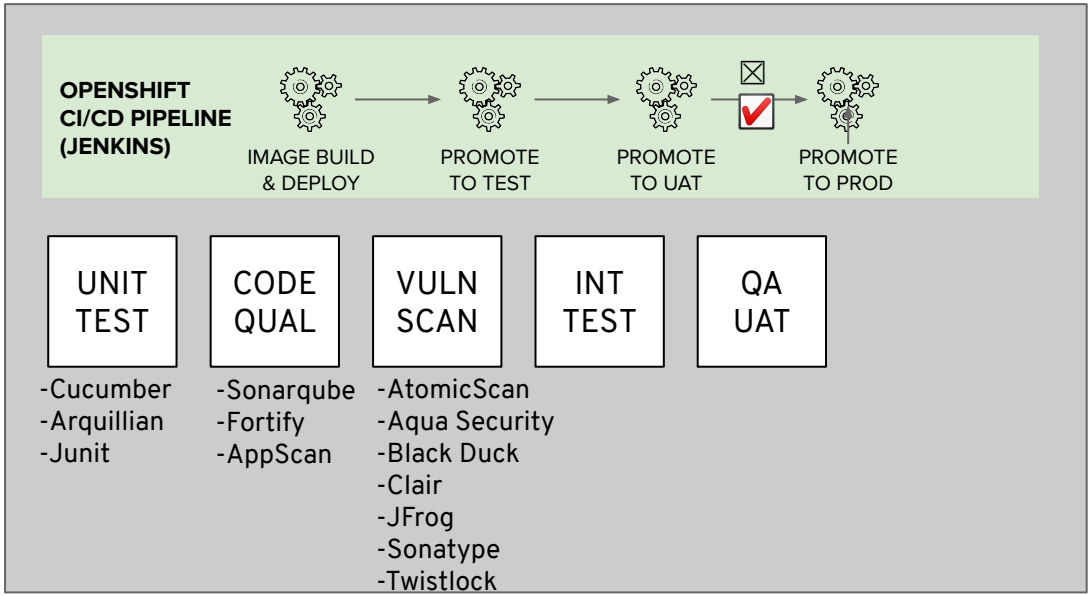
Vulnerability Analysis

- Identifies vulnerable dependencies
- 3000+ disclosures in 2015
- 4000+ disclosures in 2016

Red Hat

SECURING THE DEVELOPMENT

- Integrate security testing into your build / CI process
- Use automated policies to flag builds with issues



CODEREADY WORKSPACES

A collaborative container-native development solution that runs in OpenShift on-premises or in the cloud. Based on Eclipse Che

Container Workspaces

Workspace replicas to end “works on my machine” and enable team collaboration.

DevOps Integrations

Reference developer workspaces from any issue, failed build, or git notification.

Protect Source Code

Full access to source code without any of it landing on hard-to-secure laptops.

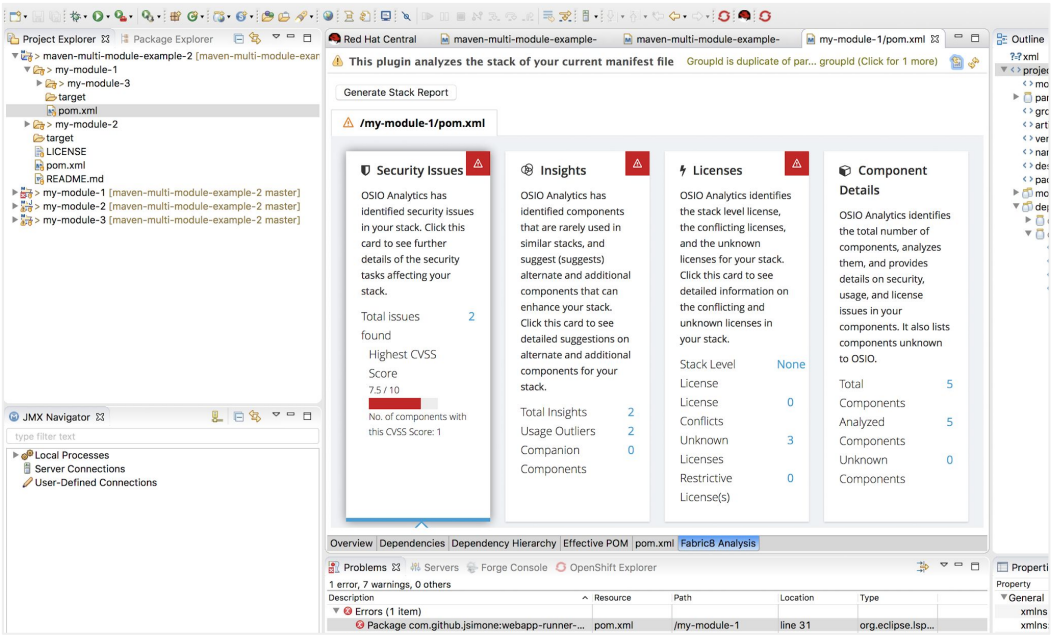
Built In Security: OpenShift running on Red Hat Linux, with development containers using secure Red Hat Linux.

Red Hat

SOURCE CODE DEPENDENCY ANALYTICS

The dependency analytics service provides security and license warnings for any dependency in a project - helping developers to fix problems earlier in the cycle.

- Find CVEs in any package
- Discover license mismatches
- Supported for Java and Node
- Help developers find critical issues before they hit production



Red Hat

SECURING THE OPERATIONS

Deployment

- Trusted registries and repos
- Signature authenticating and authorizing
- Image scanning
- Policies
- Ongoing assessment with automated remediation

Mission Control - Apollo 13
https://c1.staticflickr.com/4/3717/9460197822_9f6ab3f30c_b.jpg

Red Hat

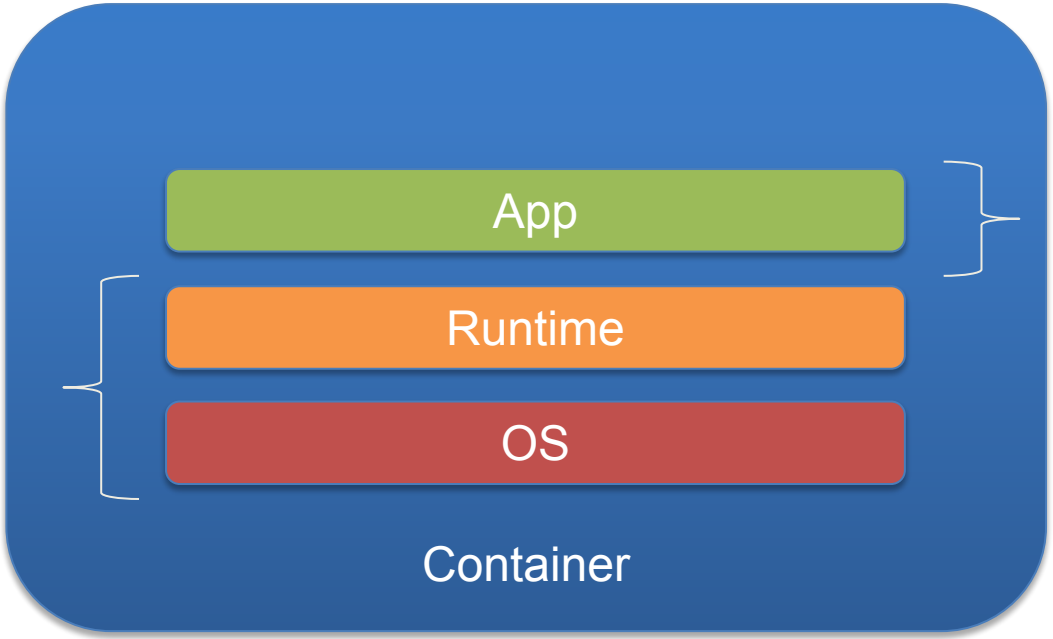
Vulnerability Scanning - Clair

Red Hat

CONTAINERS: TOP TO BOTTOM

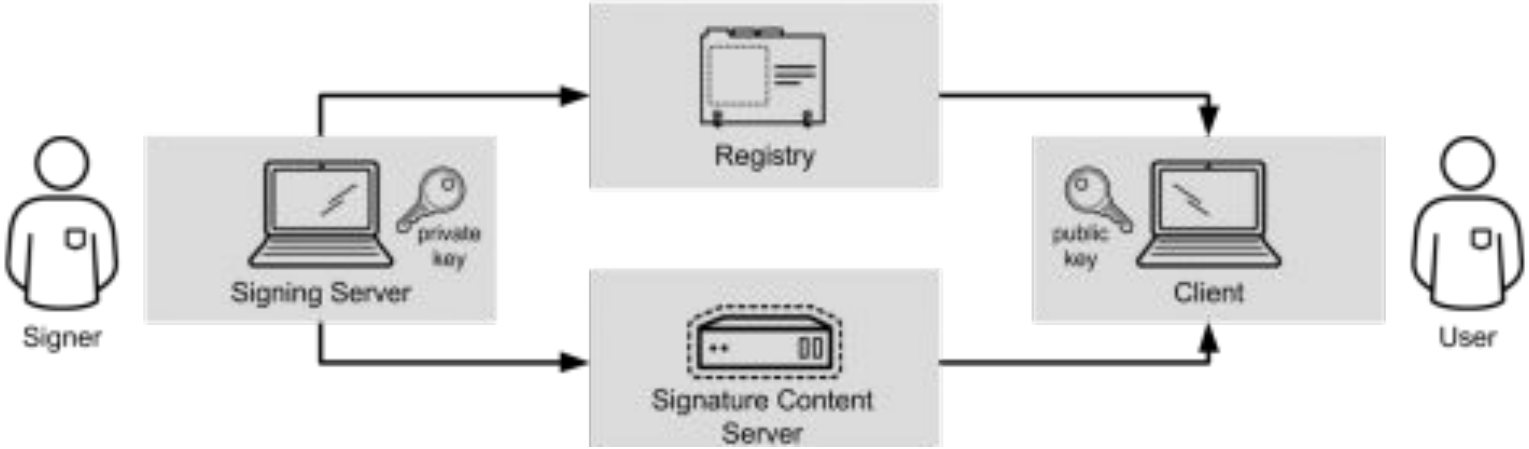
RED HAT® QUAY

clair



Red Hat

CONTAINER IMAGE SIGNING



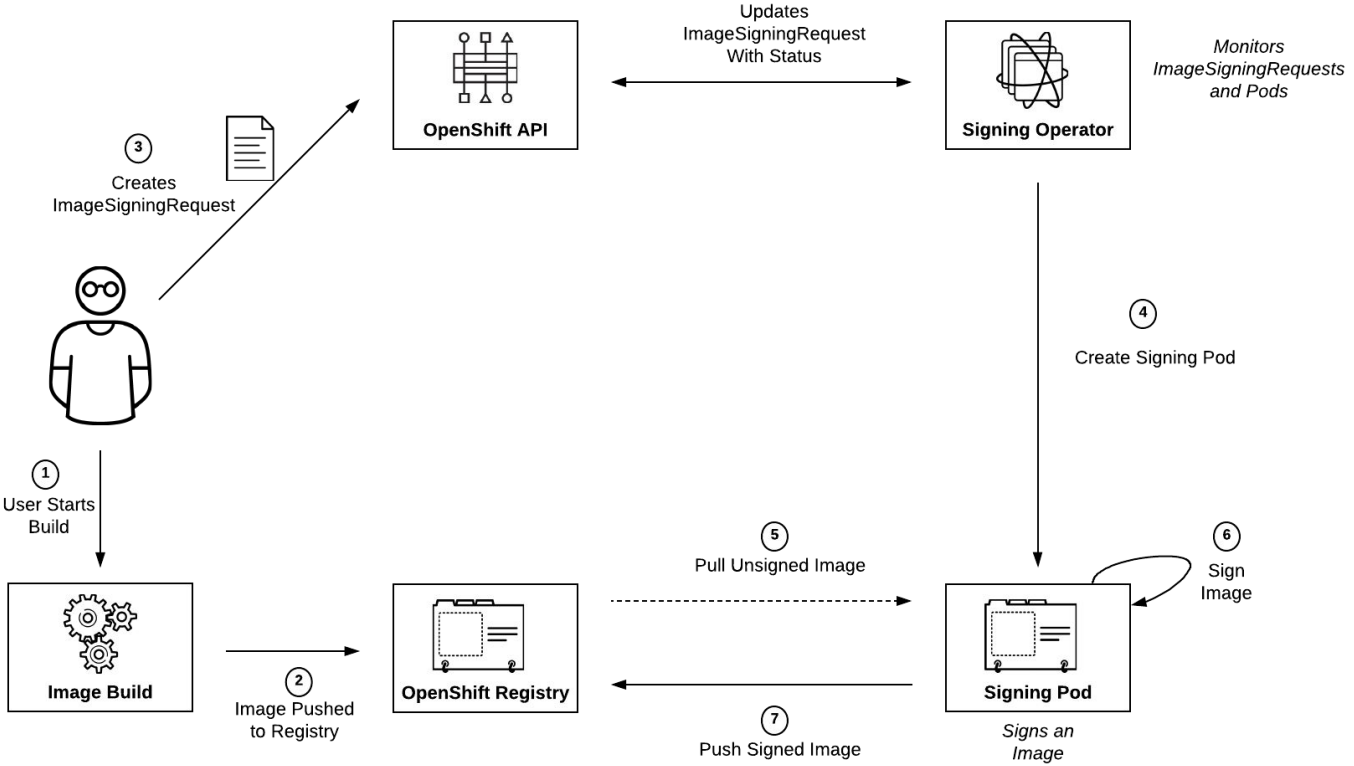
Verify provenance of images

Registry independent

Supports multiple signatures

Enforce signatures at node level via signing trust policy

IMAGE SIGNING IN PRACTICE



Red Hat

CUSTOM RESOURCE DEFINITIONS

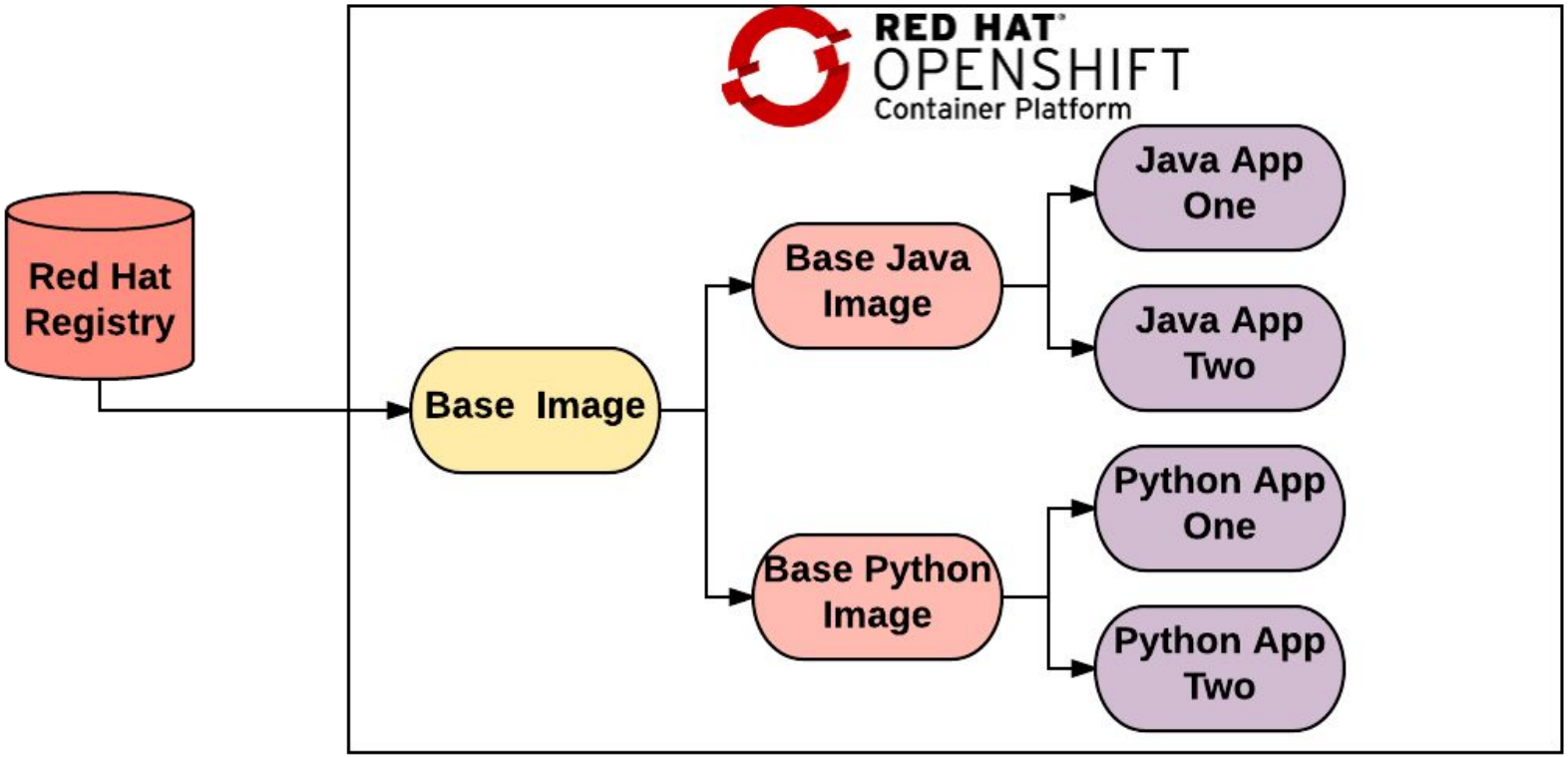
Custom Resource Definitions (CRD's) extend OpenShift capabilities by allowing users to define their own resources

Image signing operator monitors *ImageSigningRequest* resources and takes action based on defined state

- Image and signing key

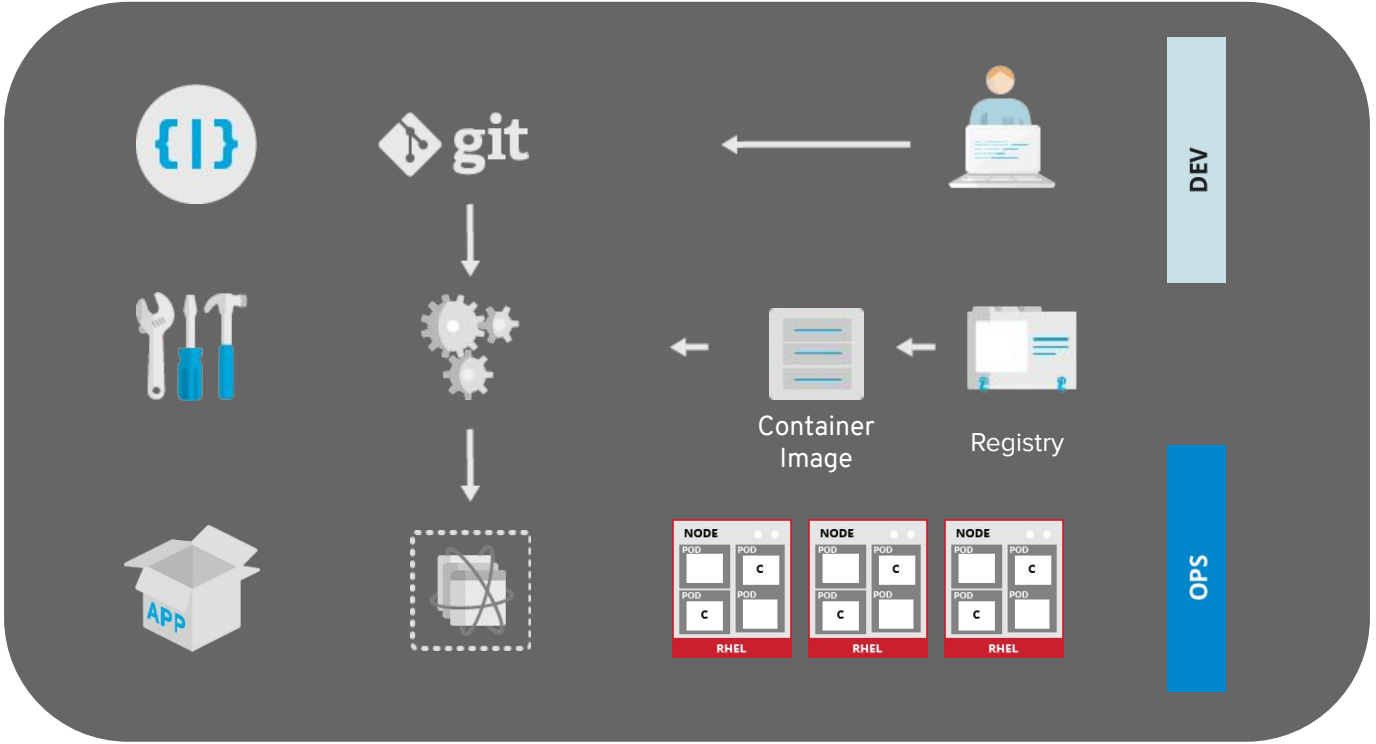
Operator provides feedback on resulting state after signing action in *status* field

Cascading Builds



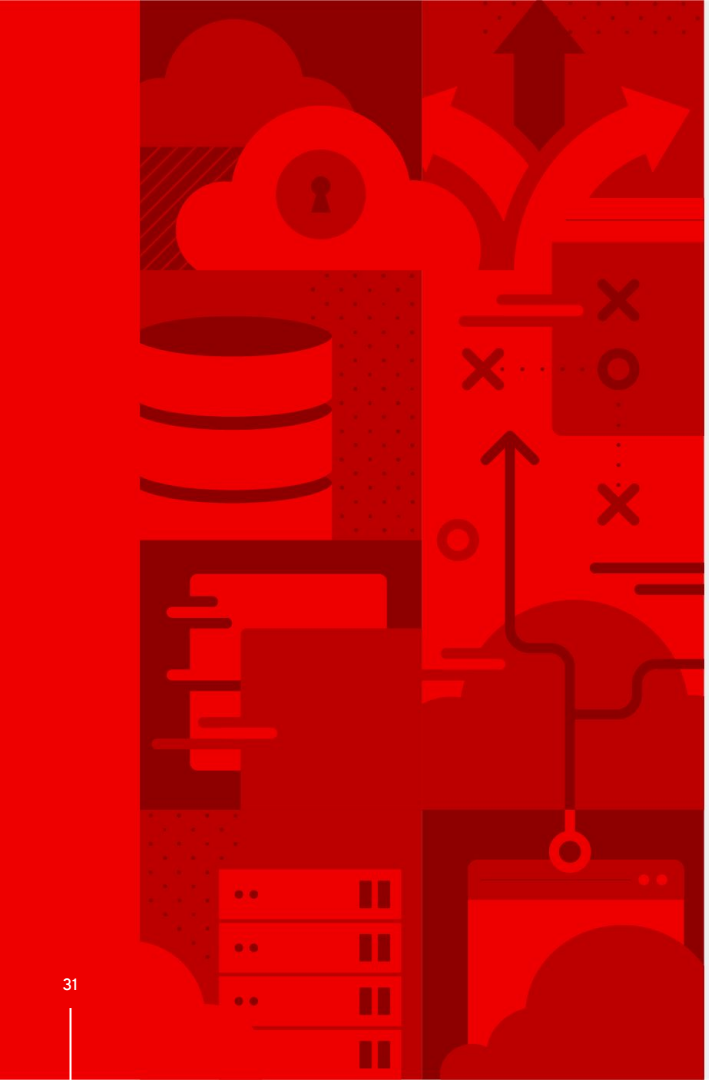
CONTINUOUS SECURITY

Continuous Integration / Continuous Deployment / Continuous Security



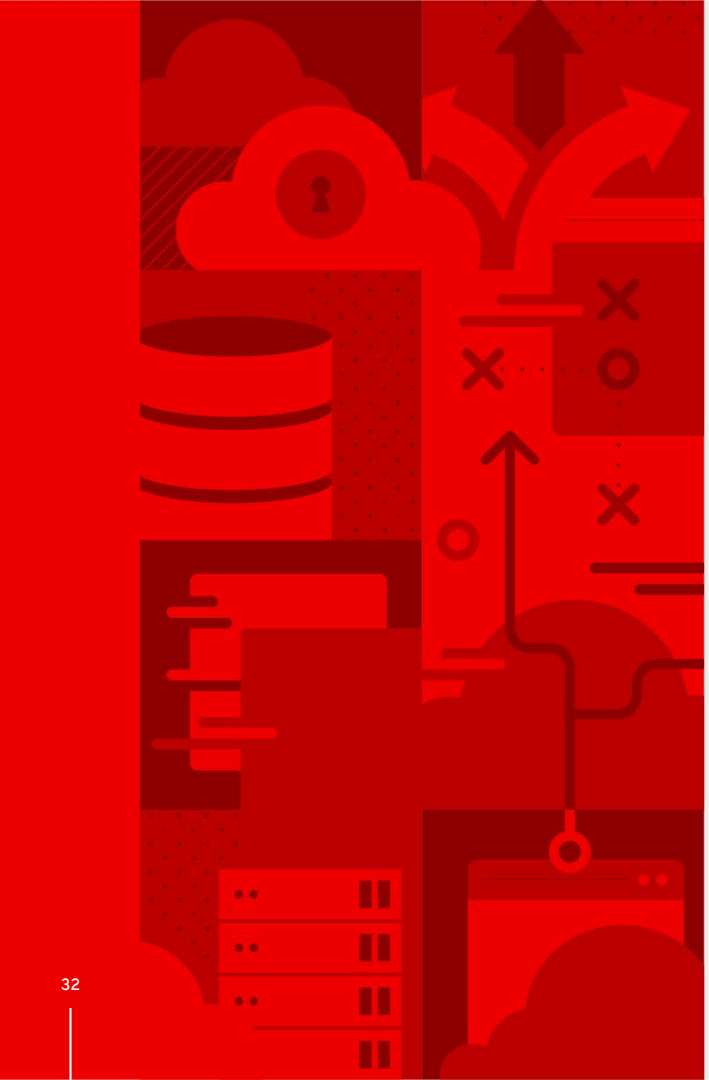
Trust is temporal: rebuild and redeploy as needed

Red Hat



Demo

Red Hat



Questions

Red Hat

Next Steps

- Speak with a Red Hat expert here at Security Symposium
- Look for the slides in a “Thank You” email from us in the next few days
- Stay up to date with Red Hat at redhat.com/security
- Visit redhat.com/events to find out about workshops and other events like this one coming to your area

Thank you for coming.

Feedback or questions?

infrastructure@redhat.com