Red Hat Summit

Connect

Red Hat

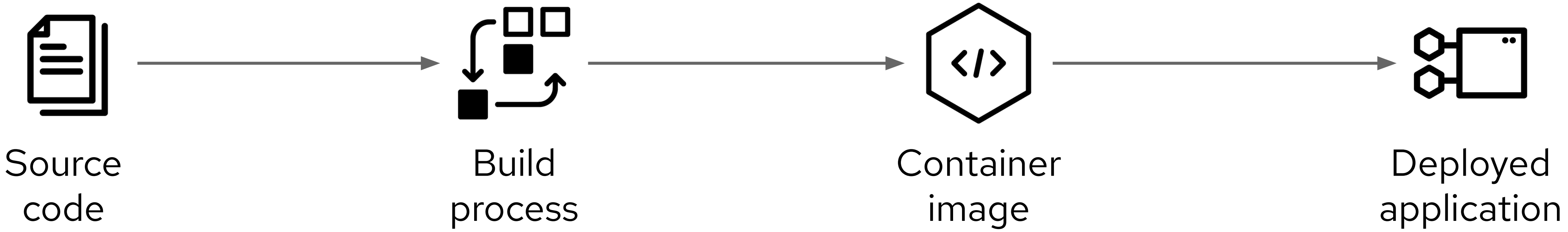
Optimizing Development Efficiency & Application Security

Red Hat Secure Software Supply Chain

Mark Roberts
Principal Solution Architect
Red Hat

Secure Software Supply Chain

The what ...



Secure Software Supply Chain

The how …

Red Hat OpenShift

- Secure and scalable platform
- Underpinned by RHEL CoreOS
- Same experience wherever used
- Managed service options
  - ROSA
  - ARO
  - OpenShift Dedicated

Red Hat Advanced Cluster Security for Kubernetes

- Container native security solution
- Standards based compliance validation
- Vulnerability analysis
- Policies delivered at installation
- Integration with CI / CD processes
- Available as-a-service if required

Red Hat Trusted Software Supply Chain

OpenShift Pipelines

- Container native workflows
- Standardised tasks

OpenShift GitOps

- Automate application deployment
- Synchronisation of Git content

Red Hat

Secure Software Supply Chain

The why ...

Software supply chain attacks: a matter of when, not if

Ransom paid but a mere fraction to the overall downtime and recovery costs of a data breach

742%

average annual increase in software supply chain attacks over the past 3 years[1]

20%

data breaches due to a compromised software supply chain[2]

78%

have initiatives to increase collaboration between DevOps and Security teams[3]

92%

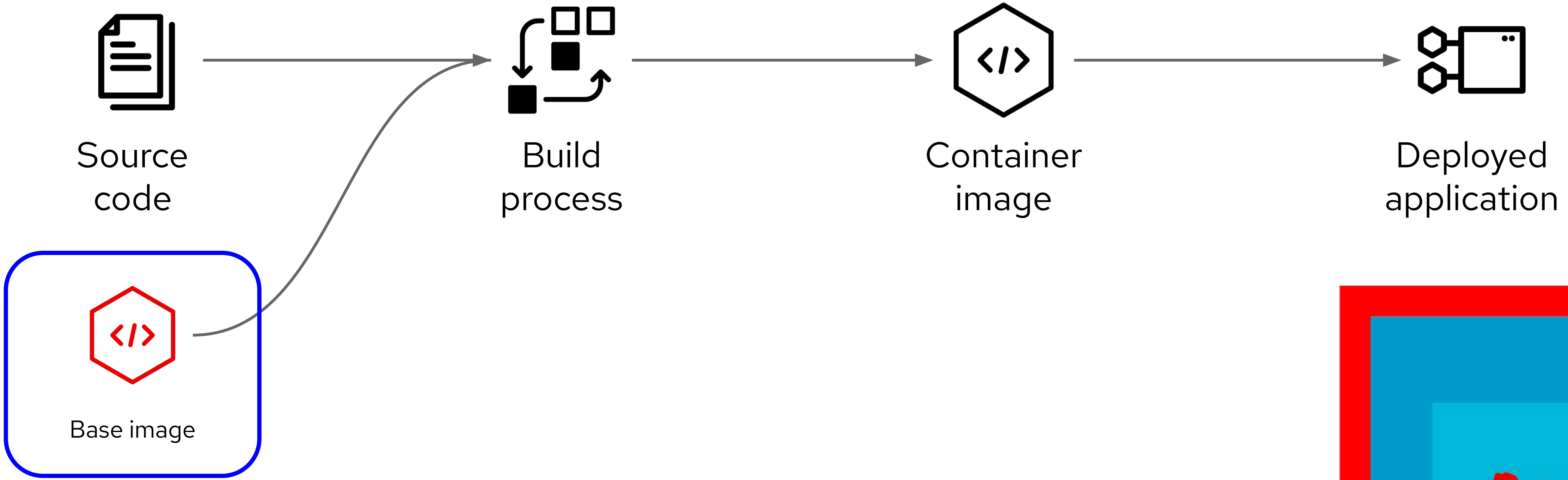
say enterprise open source solutions are important as their business accelerates to the open hybrid cloud[4]

Red Hat

[1] State of the Software Supply Chain | [2] Cost of a Data Breach 2022 - IBM Report | [3]State of Kubernetes Security Report 2022 - Red Hat Report | [4]State of Enterprise Open Source 2022 - Red Hat Report

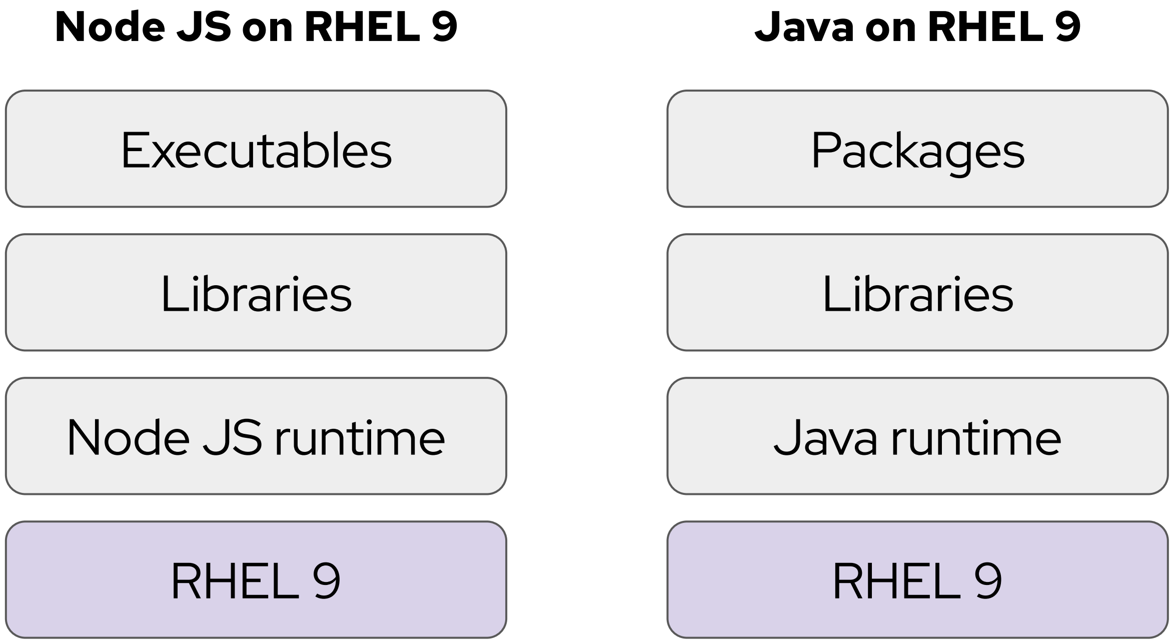
Starting point -

Where to put the built application



Managing the base image

- Layer software onto an original base
- Build your own or download someone else’s
  - What does that contain?
- For greater confidence –
  - build your own from a common base



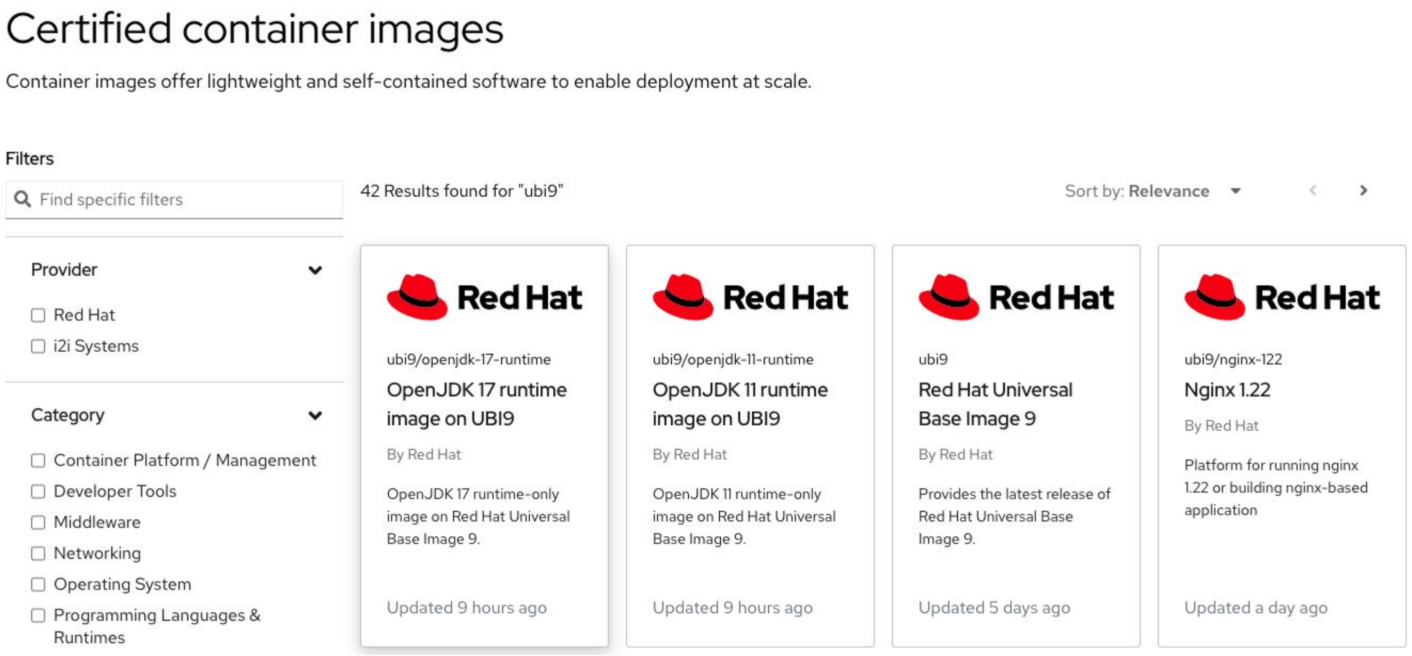
Node JS on RHEL 9	Java on RHEL 9
Executables	Packages
Libraries	Libraries
Node JS runtime	Java runtime
RHEL 9	RHEL 9

Red Hat

Red Hat Container Catalog

Discover certified container images from Red Hat and third-party providers that enable and extend your Red Hat environments

- Supported and certified images
- Range of technologies - database platforms, language runtimes, middleware, metrics etc.



Certified container images

Container images offer lightweight and self-contained software to enable deployment at scale.

Filters

Find specific filters

42 Results found for "ubi9"

Sort by: Relevance

Provider

□ Red Hat
□ i2i Systems

Category

□ Container Platform / Management
□ Developer Tools
□ Middleware
□ Networking
□ Operating System
□ Programming Languages & Runtimes

Red Hat

ubi9/openjdk-17-runtime

OpenJDK 17 runtime image on UBI9

By Red Hat

OpenJDK 17 runtime-only image on Red Hat Universal Base Image 9.

Updated 9 hours ago

Red Hat

ubi9/openjdk-11-runtime

OpenJDK 11 runtime image on UBI9

By Red Hat

OpenJDK 11 runtime-only image on Red Hat Universal Base Image 9.

Updated 9 hours ago

Red Hat

ubi9

Red Hat Universal Base Image 9

By Red Hat

Provides the latest release of Red Hat Universal Base Image 9.

Updated 5 days ago

Red Hat

ubi9/nginx-122

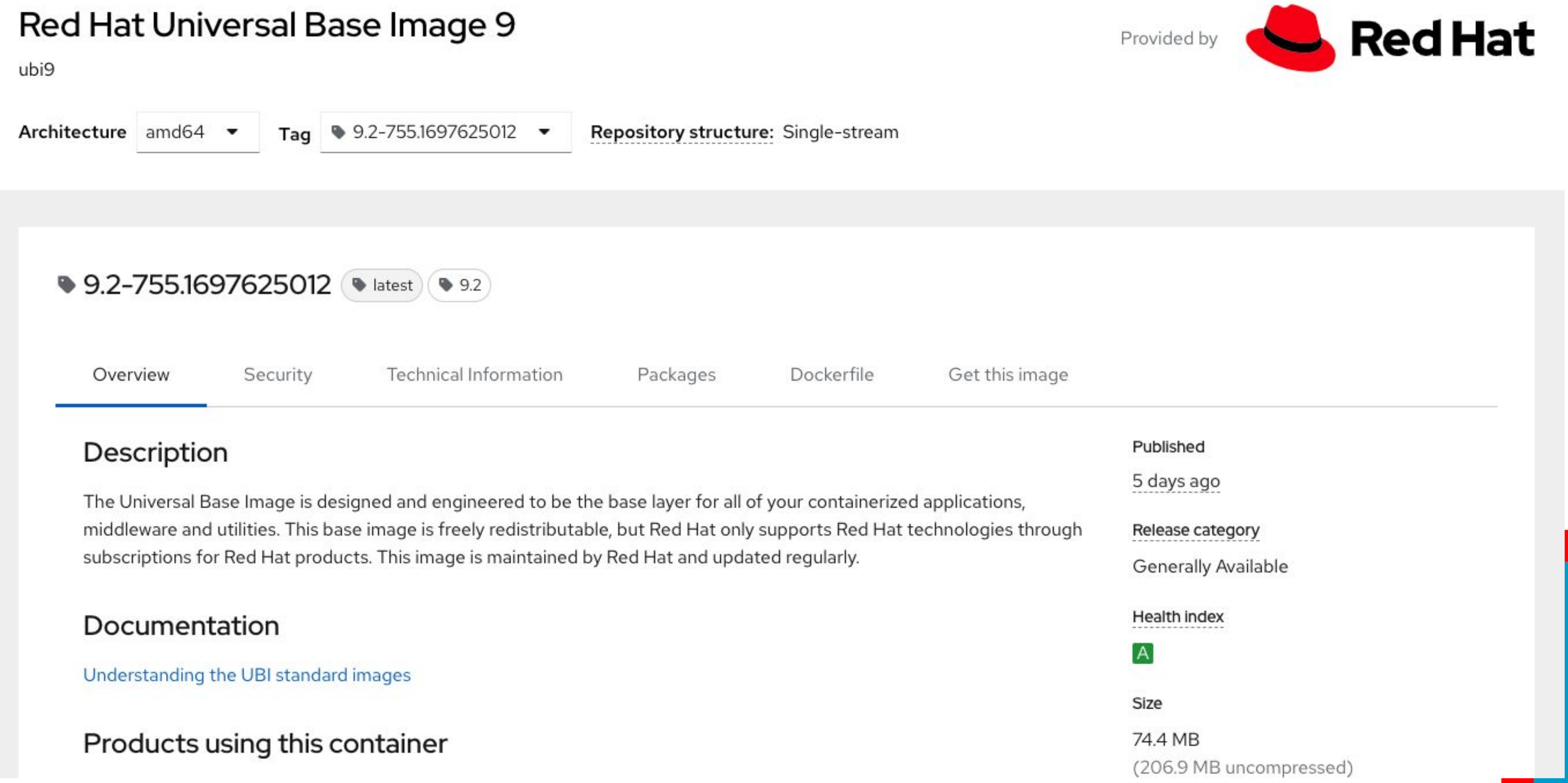
Nginx 1.22

By Red Hat

Platform for running nginx 1.22 or building nginx-based application

Updated a day ago

Red Hat Container Catalog



Red Hat Universal Base Image 9

ubi9

Provided by Red Hat

Architecture amd64 **Tag** 9.2-755.1697625012 **Repository structure:** Single-stream

9.2-755.1697625012 latest 9.2

Description

The Universal Base Image is designed and engineered to be the base layer for all of your containerized applications, middleware and utilities. This base image is freely redistributable, but Red Hat only supports Red Hat technologies through subscriptions for Red Hat products. This image is maintained by Red Hat and updated regularly.

Documentation

Understanding the UBI standard images

Products using this container

Published

5 days ago

Release category

Generally Available

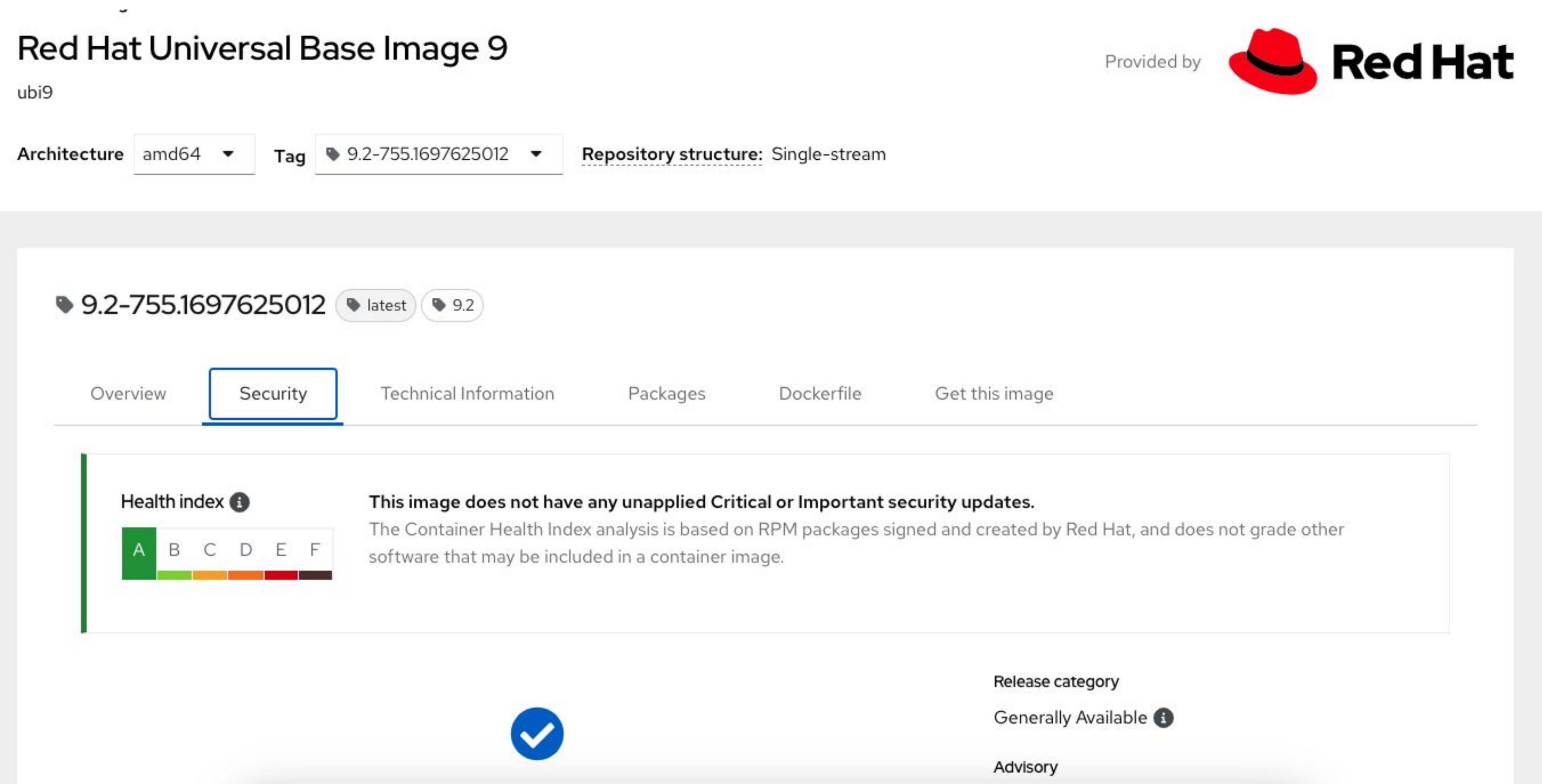
Health index

A

Size

74.4 MB
(206.9 MB uncompressed)

Red Hat Container Catalog



Red Hat Universal Base Image 9

ubi9

Provided by Red Hat

Architecture amd64 **Tag** 9.2-755.1697625012 **Repository structure:** Single-stream

9.2-755.1697625012 latest 9.2

Health index

A B C D E F

This image does not have any unapplied Critical or Important security updates.

The Container Health Index analysis is based on RPM packages signed and created by Red Hat, and does not grade other software that may be included in a container image.

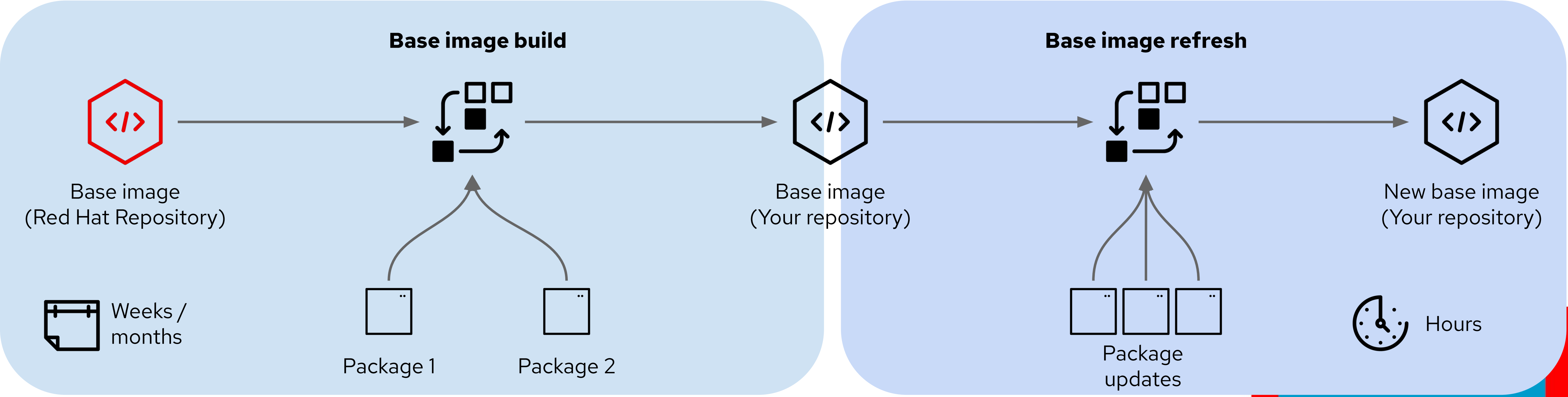
Release category

Generally Available

Advisory

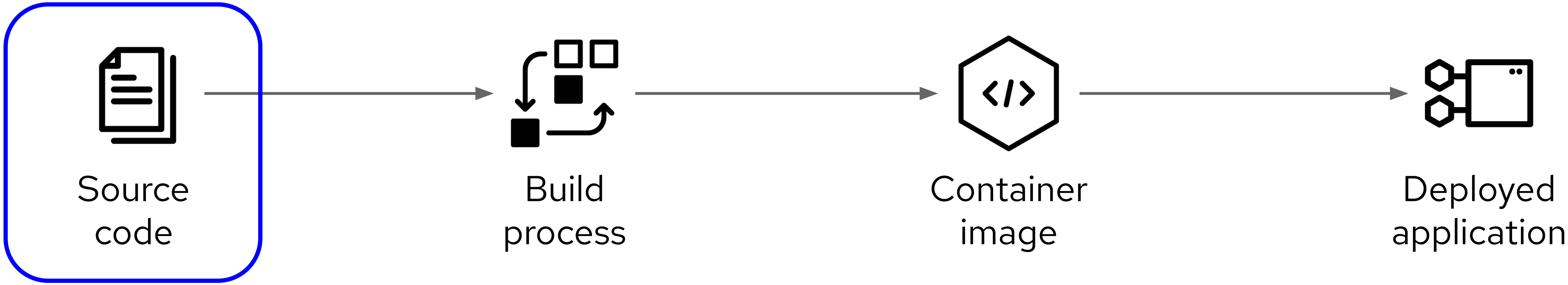
Maintaining a base image

- Base image management is important
- Manage the scope of change between image build and image update



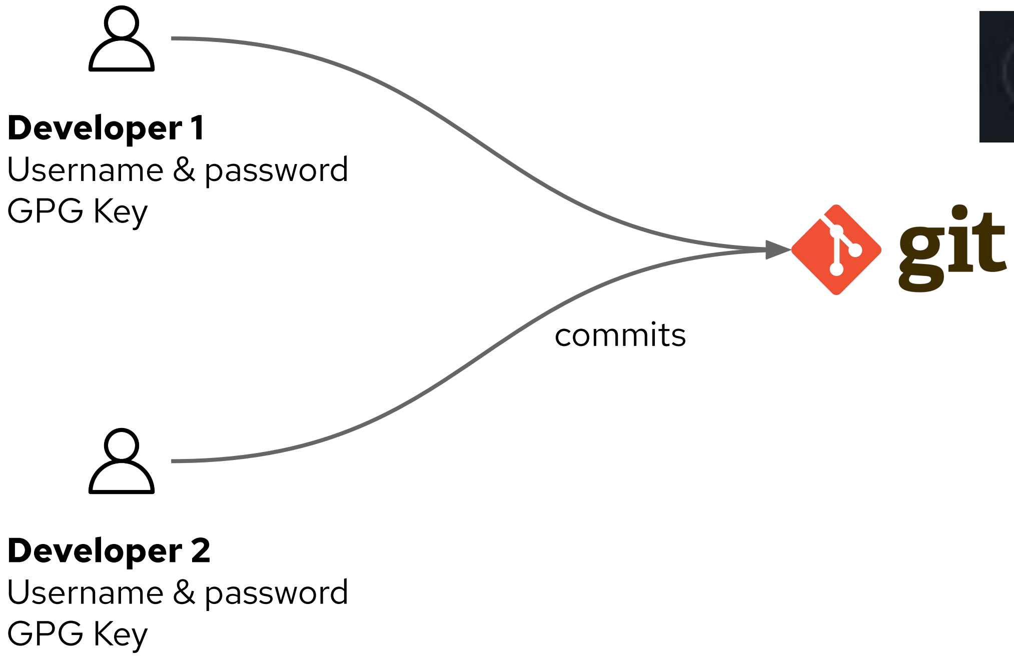
OpenShift
Pipelines

It all begins with the source code



Securing Git Commits

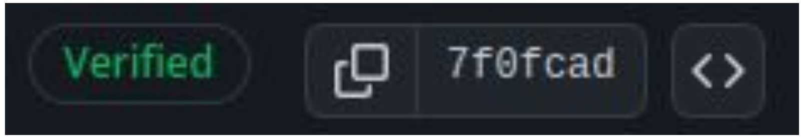
- Git commits can be secured with a GPG Key
- Verification indication appears on commits and further processes can be performed
- GPG Keys can also be verified in the CI process
- Additional layer of security and assurance



Developer 1
Username & password
GPG Key

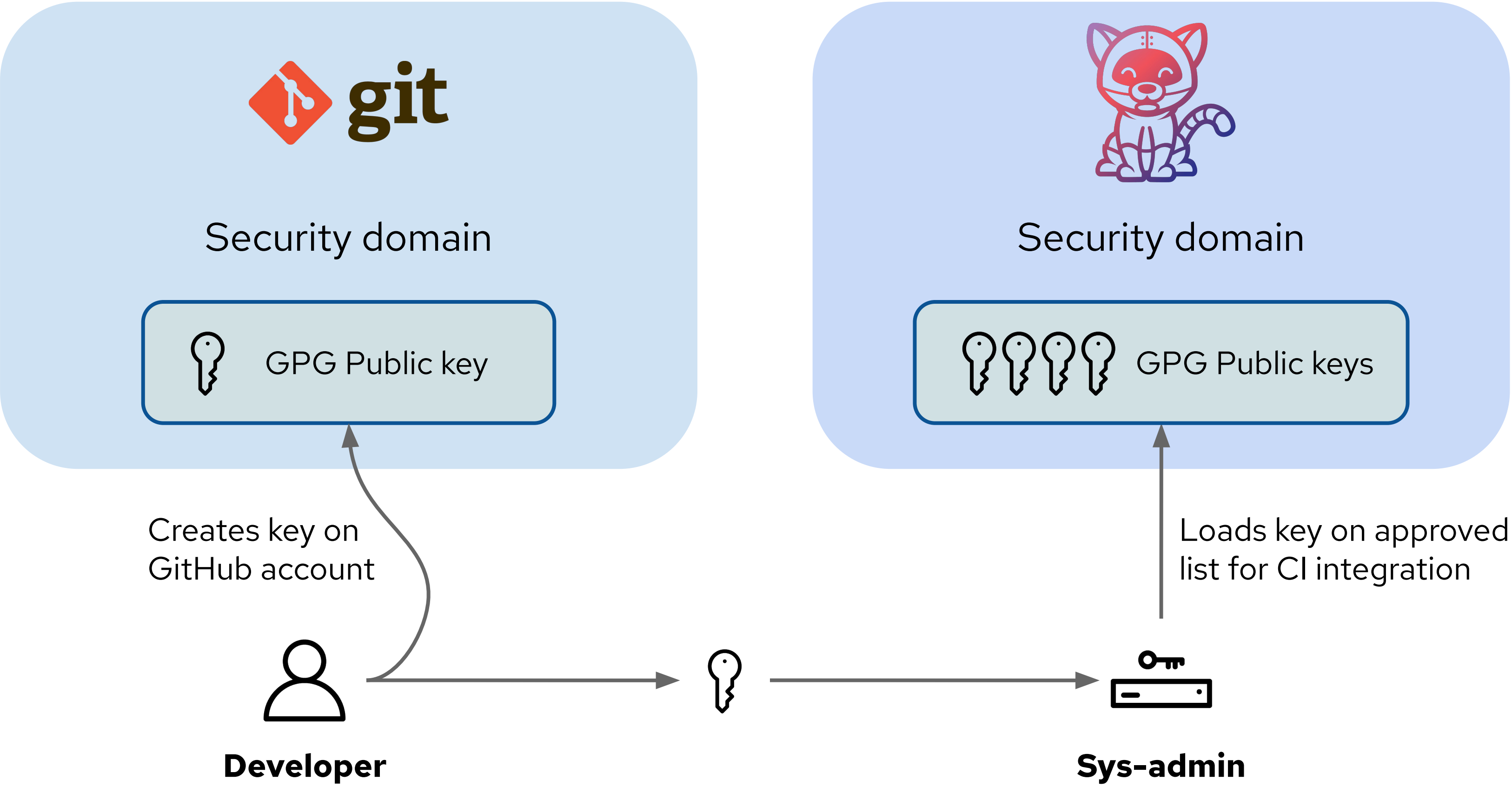
commits

Developer 2
Username & password
GPG Key



Extend Secure Git into Pipeline

- OpenShift Pipelines automates the validation of Git commits

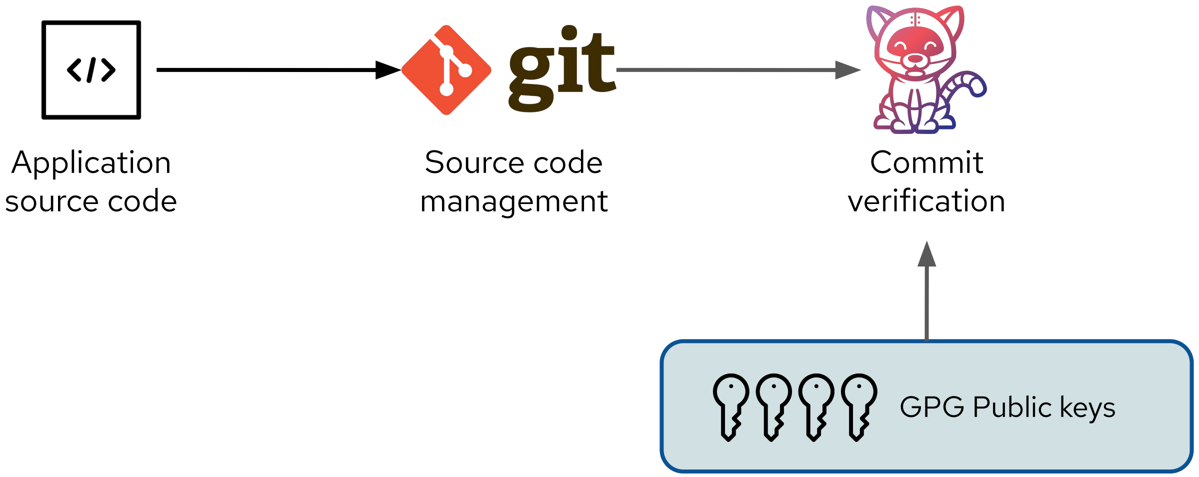


Verify source commits within the Pipeline

- Clone the source code ready to build
- Verify source commits

```
git verify-commit HEAD
```

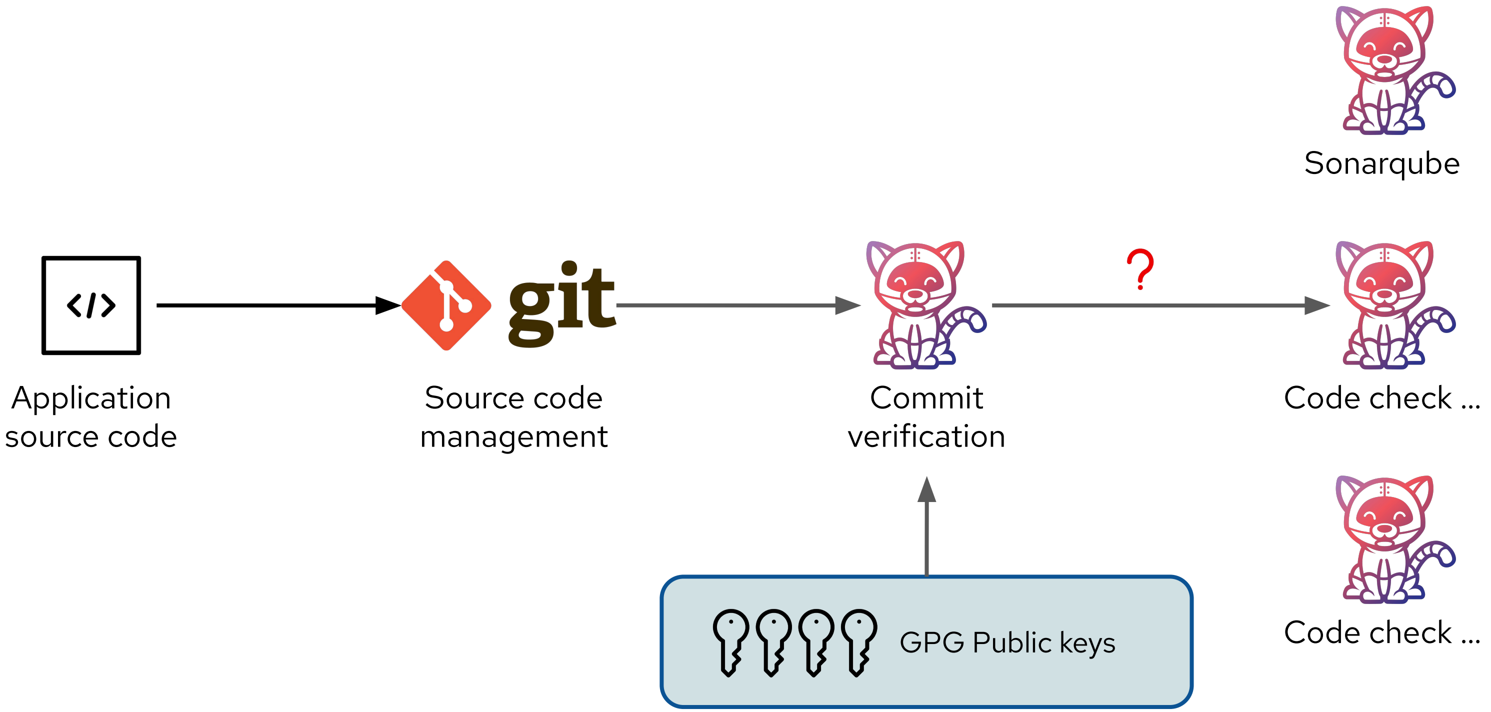
- Next step proceeds if the verify source is successful



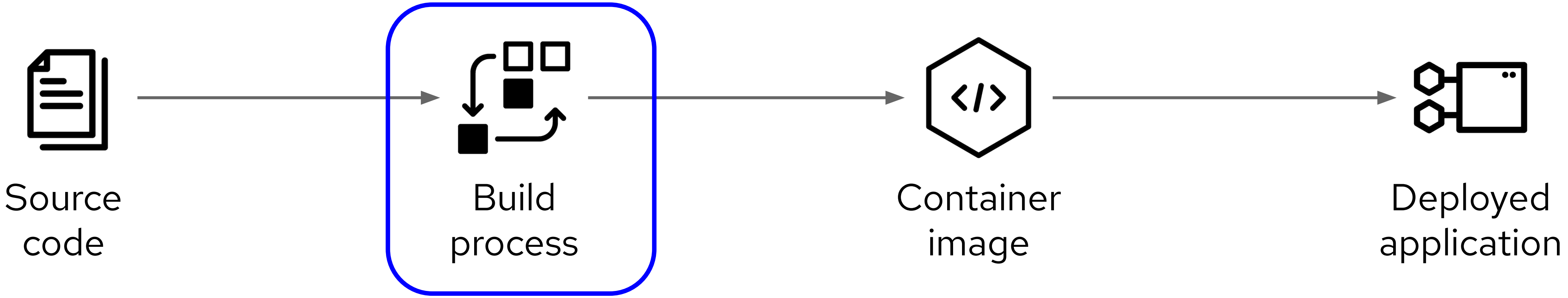
- Standardised task used for verification
- Easy to consume in a teams pipeline
- Results can explain reason for any issues

Source code quality analysis phase

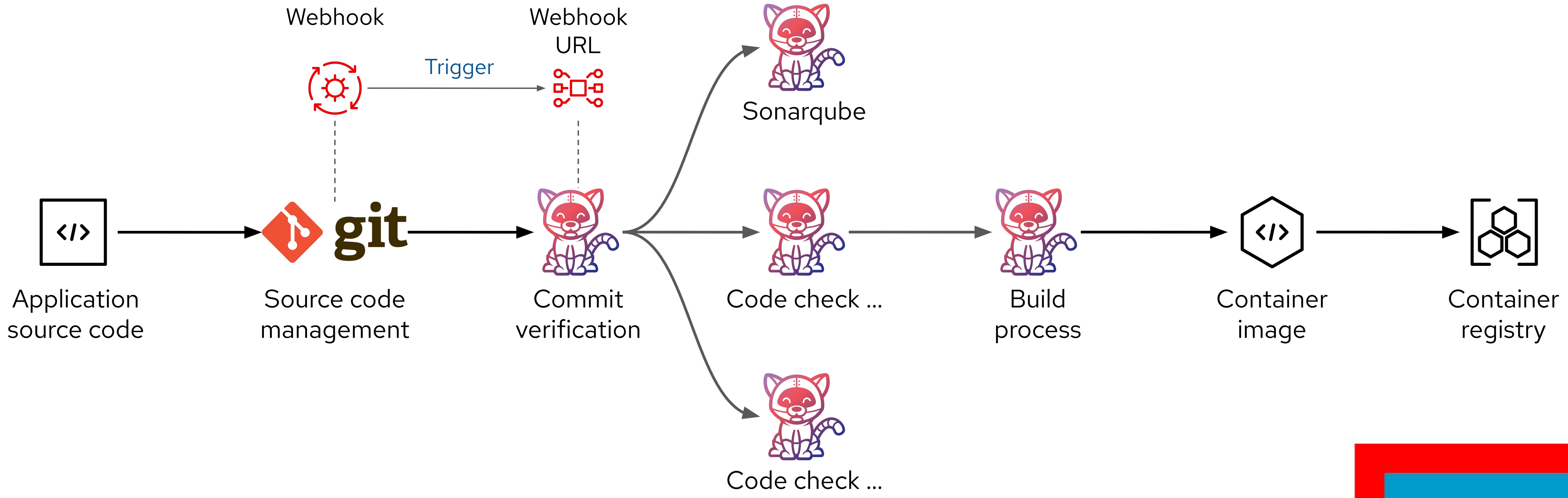
- Use a variety of source code analysis tools
- Validate results against success criteria
- Control progression of build process



The basic build and delivery process

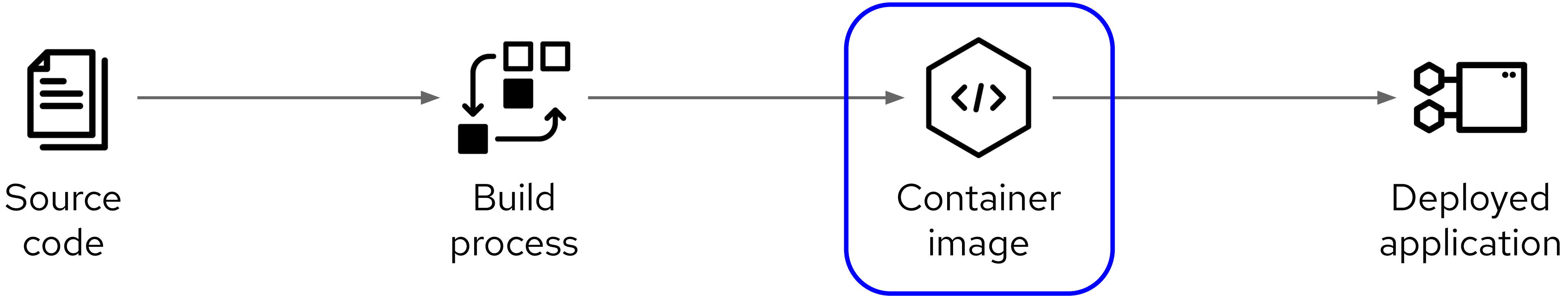


CI Process - Up to Container Creation



OpenShift Pipelines

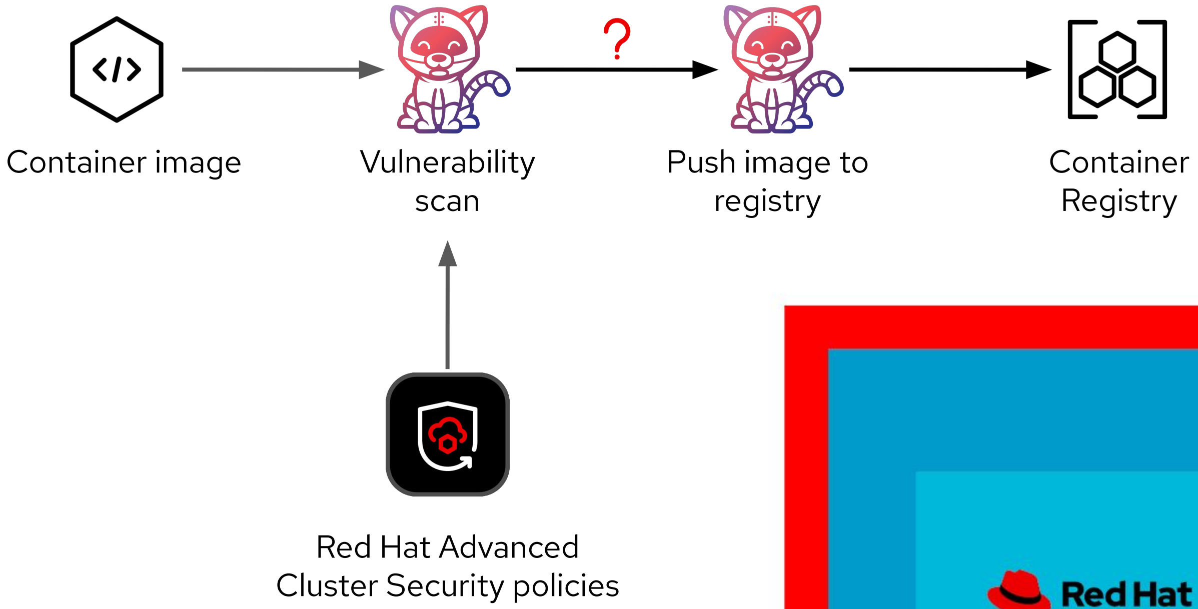
Do we have any issues with the container image ?



Red Hat
Advanced Cluster Security
for Kubernetes

Container image vulnerability scanning

- Any container image creation process should include a vulnerability scan
- Report on critical vulnerabilities with remediation information
- 'Shift-left' to ensure vulnerabilities become a developer (everyones) responsibility
- Standardised task used for verification
- Easy to consume in a teams pipeline
- Results can explain reason for any issues

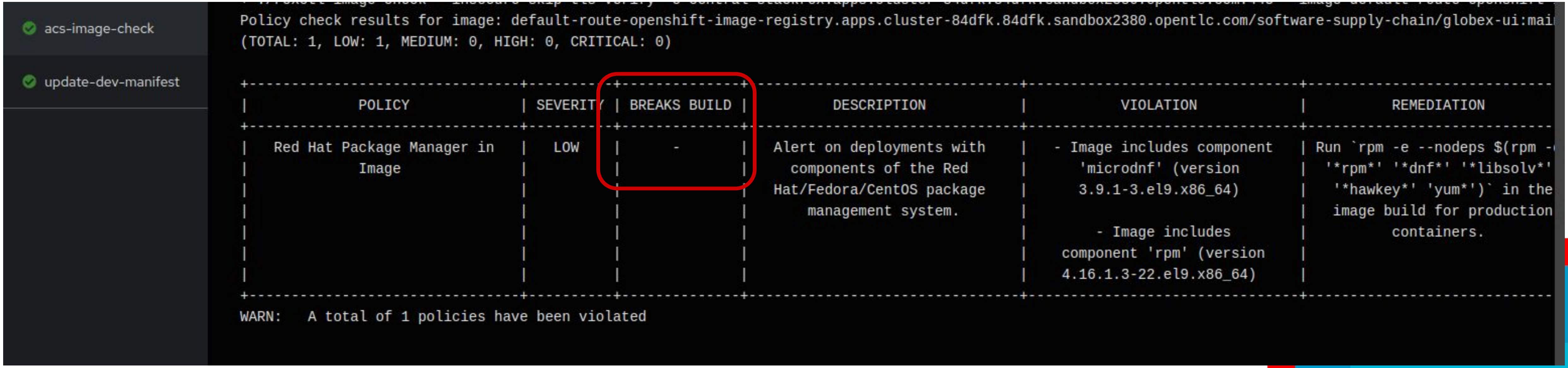


Red Hat

Red Hat
Advanced Cluster Security
for Kubernetes

Image vulnerability scanning

- Report on violations against your policies
- Developer centric information on what to do to remediate a problem



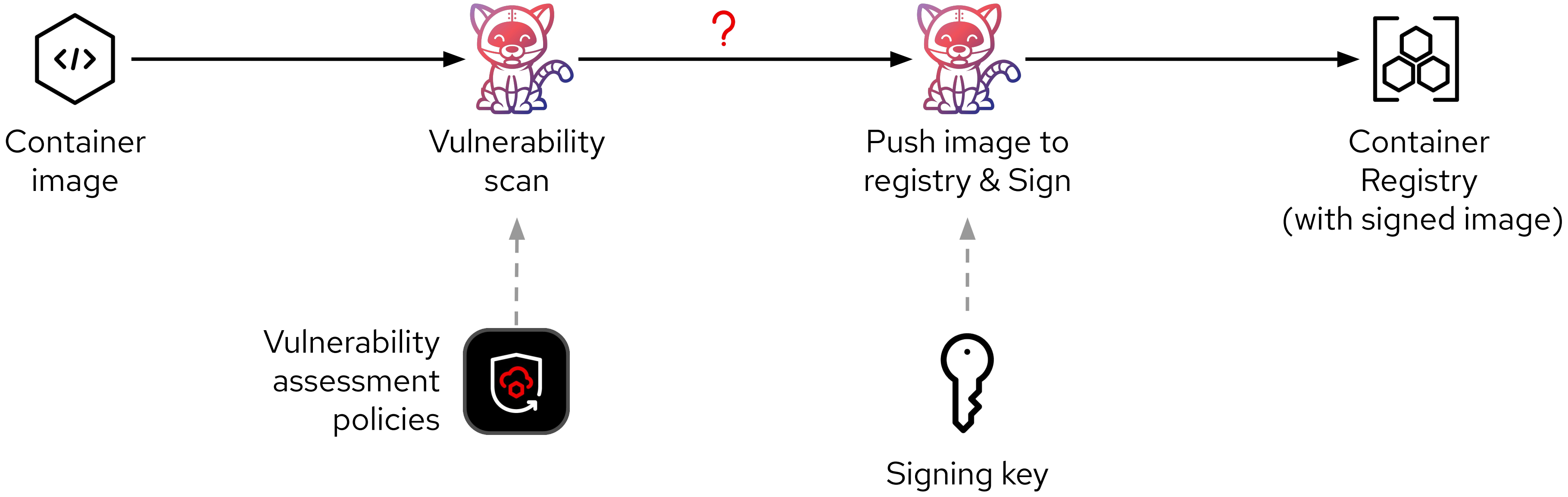
```
Policy check results for image: default-route-openshift-image-registry.apps.cluster-84dfk.84dfk.sandbox2380.opentlc.com/software-supply-chain/globex-ui:mai
(TOTAL: 1, LOW: 1, MEDIUM: 0, HIGH: 0, CRITICAL: 0)

+--------------------------------+----------+--------------+--------------------------------+--------------------------------+------------------------------
|             POLICY             | SEVERITY | BREAKS BUILD |          DESCRIPTION           |           VIOLATION            |          REMEDIATION
+--------------------------------+----------+--------------+--------------------------------+--------------------------------+------------------------------
|   Red Hat Package Manager in   |   LOW    |      -       |   Alert on deployments with    | - Image includes component     | Run `rpm -e --nodeps $(rpm -
|             Image              |          |              |    components of the Red       |     'microdnf' (version        |  '*rpm*' '*dnf*' '*libsolv*'
|                                |          |              |  Hat/Fedora/CentOS package     |     3.9.1-3.el9.x86_64)        |   '*hawkey*' 'yum*')` in the
|                                |          |              |     management system.         |                                |  image build for production
|                                |          |              |                                |      - Image includes          |         containers.
|                                |          |              |                                |  component 'rpm' (version      |
|                                |          |              |                                |  4.16.1.3-22.el9.x86_64)       |
+--------------------------------+----------+--------------+--------------------------------+--------------------------------+------------------------------
WARN:   A total of 1 policies have been violated
```

Red Hat

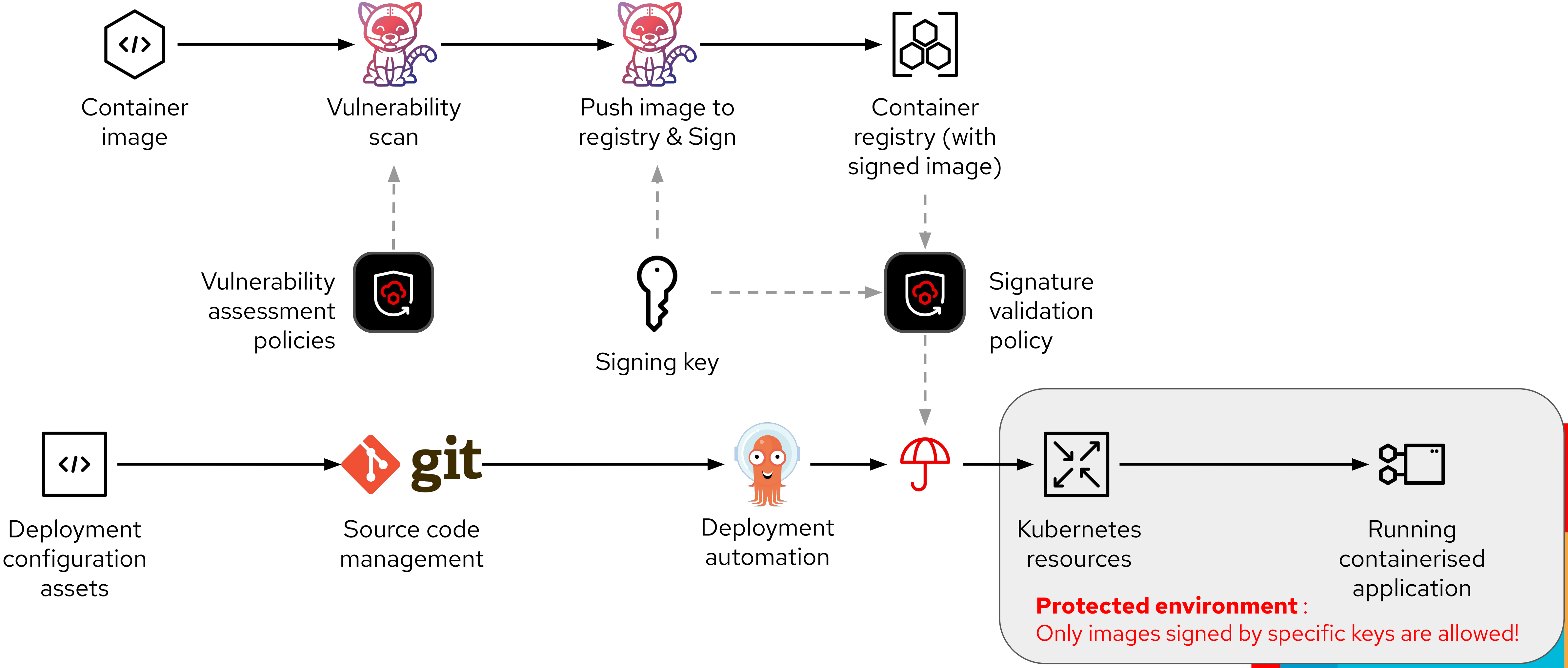
Signing Container Images

- Do you get container images from third parties ?
- Do you send container images to clients ?
- What assurance do we have for the provenance of an image


Container image
?
Vulnerability scan
Push image to registry & Sign
Container Registry (with signed image)
Vulnerability assessment policies
Signing key

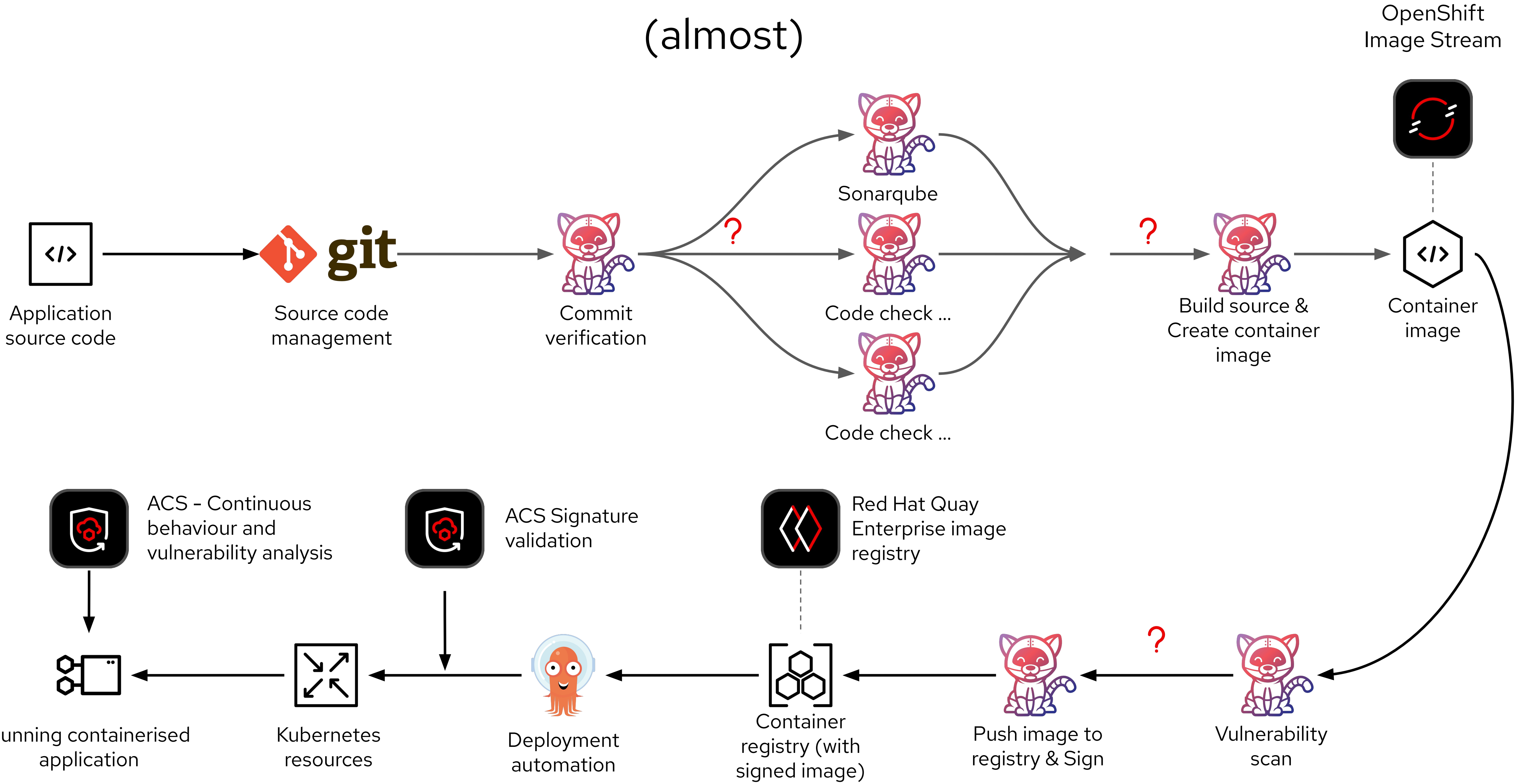
Red Hat
Advanced Cluster Security
for Kubernetes

Signing Container Images -
Control of the deployment

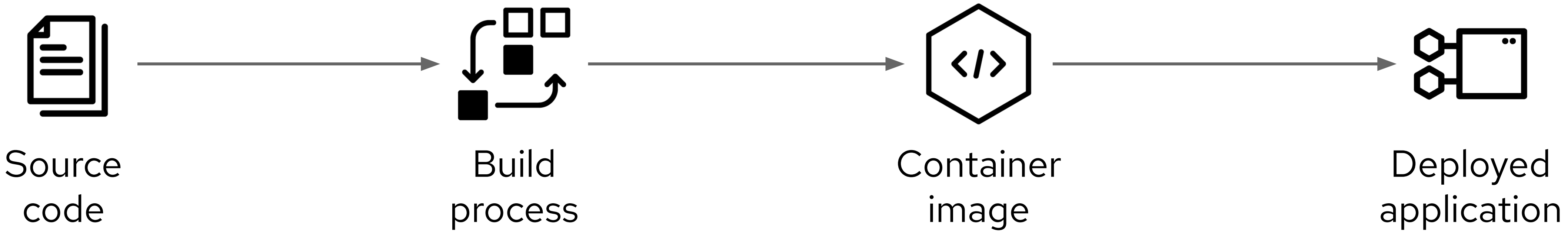

Container image
Vulnerability scan
Push image to registry & Sign
Container registry (with signed image)
Vulnerability assessment policies
Signing key
Signature validation policy
Deployment configuration assets
git
Source code management
Deployment automation
Kubernetes resources
Running containerised application

Protected environment :
Only images signed by specific keys are allowed!

Summary - The complete process (almost)


OpenShift Image Stream
Application source code
git
Source code management
Commit verification
?
Sonarqube
Code check ...
Code check ...
?
Build source & Create container image
Container image
ACS - Continuous behaviour and vulnerability analysis
ACS Signature validation
Red Hat Quay Enterprise image registry
?
Running containerised application
Kubernetes resources
Deployment automation
Container registry (with signed image)
Push image to registry & Sign
Vulnerability scan

Secure Software Supply Chain



- ✔ Validation of commits
- ✔ Analysis of code

- ✔ Pluggable tasks
- ✔ Serverless execution

- ✔ Vulnerability analysis
- ✔ Signed image checks

- ✔ Behaviour analysis
- ✔ Vulnerability checks

Red Hat
OpenShift

Red Hat
Advanced Cluster Security
for Kubernetes

OpenShift
Pipelines

OpenShift
GitOps

Red Hat

What’s next

- Have a chat today
- Get in touch - mroberts@redhat.com
- Schedule some time - web meeting or face to face
- Search the Red Hat blog site : https://www.redhat.com/en/blog

Red Hat
Summit

Thank you

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat