redhat.

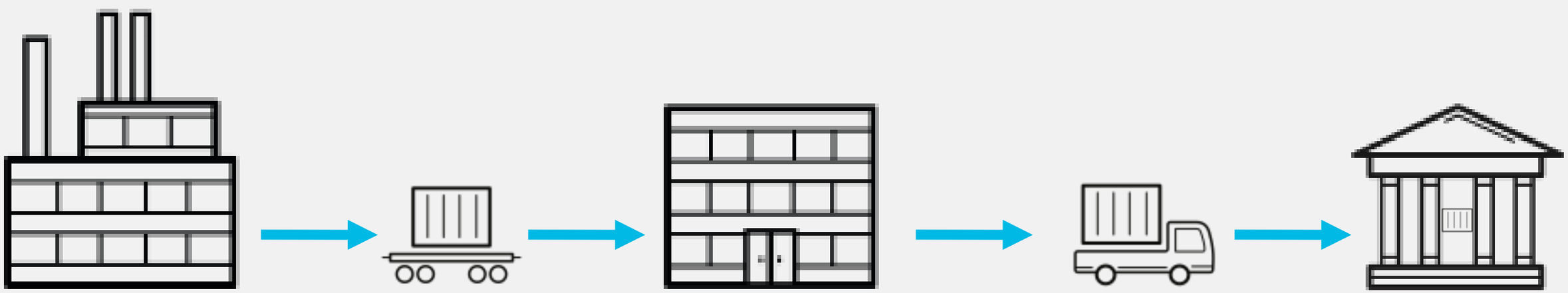
Secure Container Pipelines

Brad Sollar

Sr. Solution Architect

Red Hat Public Sector

Open Source Software - supply chain



Open Source Software - supply chain

You are using containers, but what are you doing for;

Container Image provenance?

Static & Dynamic testing?

Audits & Gates for Builds ?

Container Image Provenance

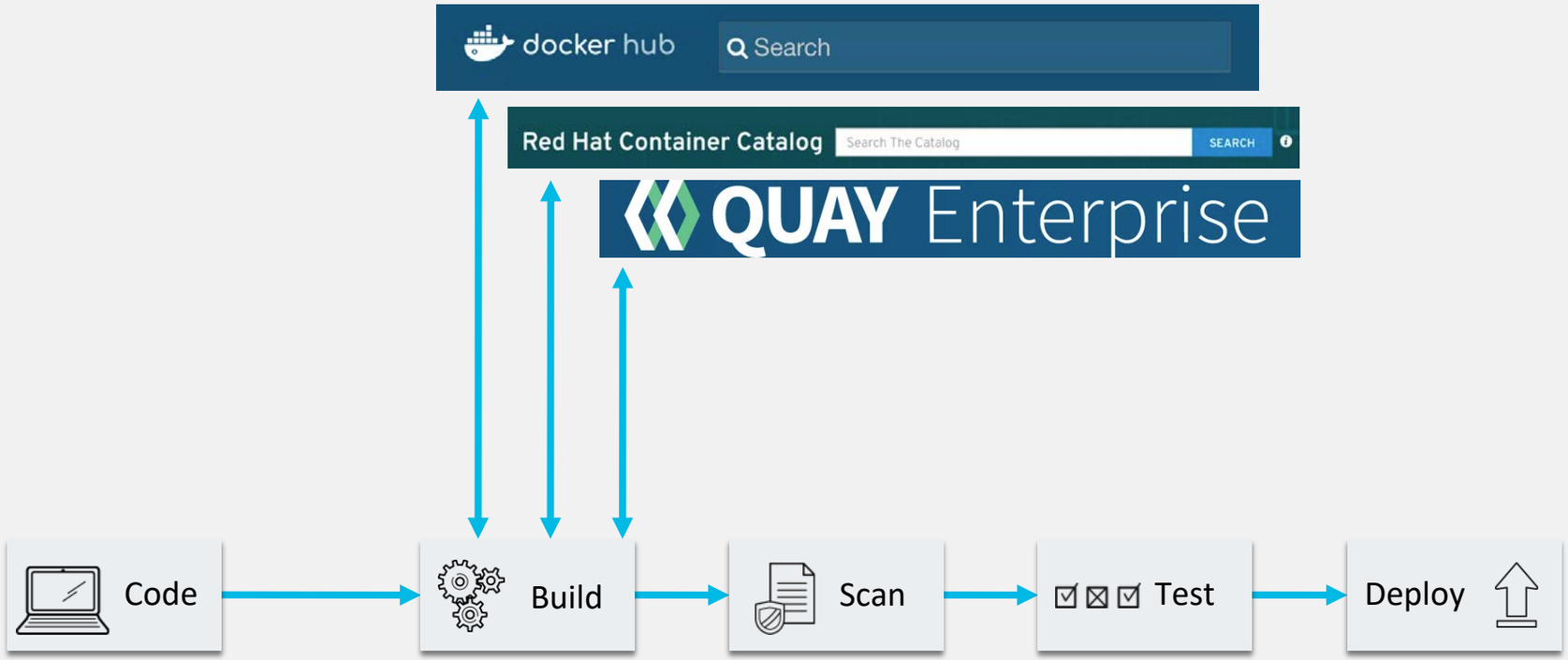
Container Image Provenance

Where do your containers come from?

- In an enterprise environment you dont want your developers pulling code down off the internet unless it's coming from verified sources.
- Its very easy for someone to commit malicious code inside a container in the hopes someone will pull it down and use it.
- This can be especially bad if you run your containers as Root.

Container Image Provenance

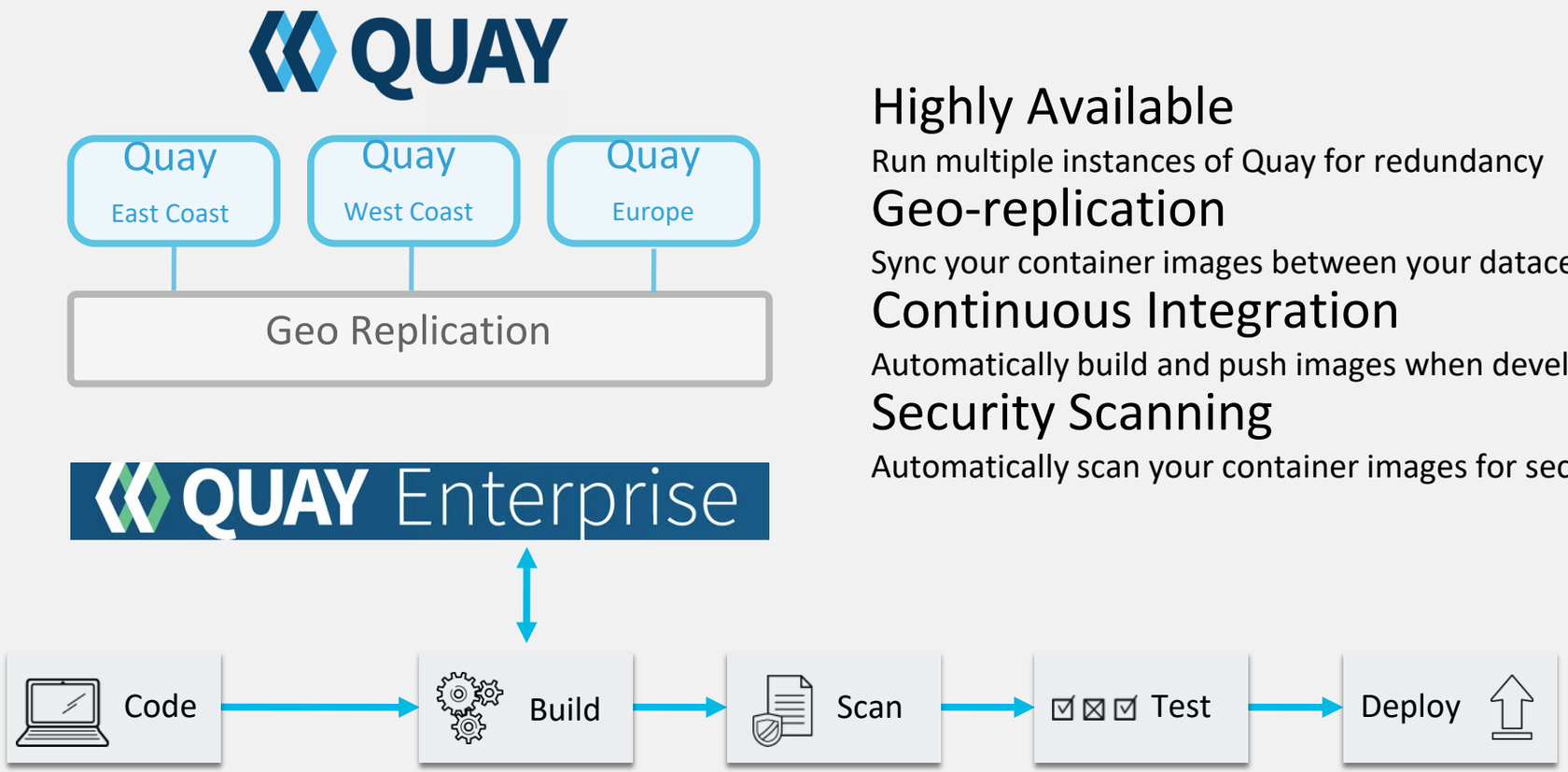
Pull Software from Trusted Sources



redhat.

Container Image Provenance

High Availability for Registries



Highly Available

Run multiple instances of Quay for redundancy

Geo-replication

Sync your container images between your datacenters

Continuous Integration

Automatically build and push images when developers commit code

Security Scanning

Automatically scan your container images for security vulnerabilities

Container Image Provenance

Pull Software from Trusted Sources

Images need to be maintained, meaning they are frequently scanned and updated.

Its good for container catalogs to provide the history of an image, each time it is updated a new tag is created.

Platform for building and running Node.js 6 applications ☆

by Red Hat, Inc. | in Product Red Hat Enterprise Linux

`registry.access.redhat.com/rhscl/nodejs-6-rhel7` Updated 18 days ago 6-15 : Health Index A

Overview | Get this image | Tech Details | Documentation | Tags

Tag Name	Date Pushed	Image Advisory	Health Index	Docker Image ID
6-15 6 latest	18 days ago	RHBA-2018:0228	A	ae9be2ffb565
6-14.15	a month ago	RHBA-2018:0072	B	1772382ef071
6-14.14	3 months ago	RHBA-2017:3333	B	f0545658c642
6-14.12	3 months ago	RHBA-2017:3191	B	ba1bb425f138
6-14.11	4 months ago	RHBA-2017:3000	D	96a89d880a8b
6-14.8	4 months ago	RHBA-2017:2866	D	c2b03bd051ac
6-14.6	5 months ago	RHBA-2017:2634	D	fba56b5381b7
6-14.5	6 months ago	RHBA-2017:2416	D	6db4b5e86f94
6-14.4	8 months ago	RHBA-2017:1661	D	8f5c07fbdb32
6-14.3	8 months ago	RHBA-2017:1526	D	aa36ded7284a
6-14.2	9 months ago	RHBA-2017:1362	D	7821c65f5dbc
6-14.1	10 months ago	RHEA-2017:1160	D	5ee10742254b

redhat.

Container Image Provenance

Pull Software from Trusted Sources

- Is your platform able to secure role-based-access to images?

Container Image Provenance

Pull Software from Trusted Sources

- Is your platform able to secure role-based-access to images?
- Is the platform able to track changes over time?

Container Image Provenance

Pull Software from Trusted Sources

- Is your platform able to secure role-based-access to images?
- Is the platform able to track changes over time?
- Is your registry highly available?

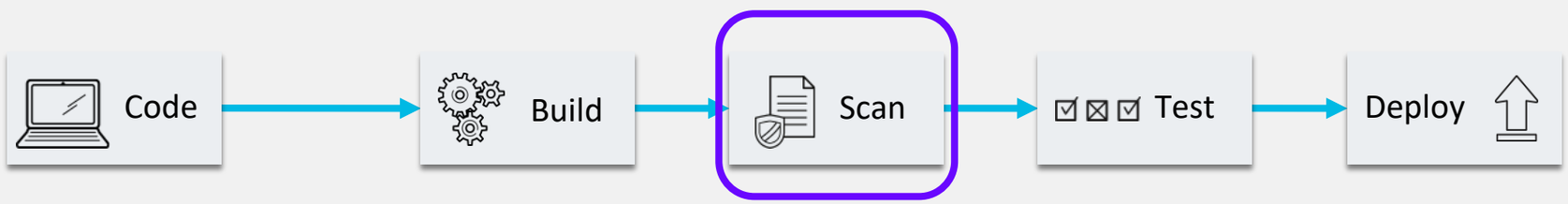
Container Security Testing

Security Testing of Code

Static vs. Dynamic testing

Static: static analysis is performed on code without actually executing the program.

Dynamic: dynamic testing actually executes the code for testing

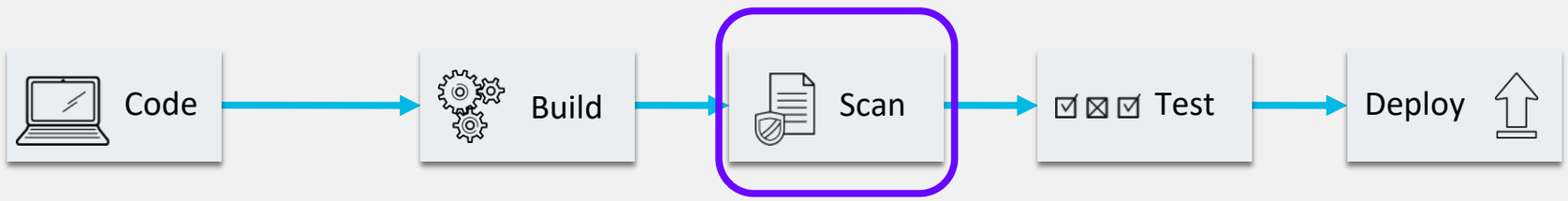


Security Testing of Code

Static vs. Dynamic testing

Some common <u>static</u> code analysis tools:

sonarqube VERACODE MICRO FOCUS Klocwork

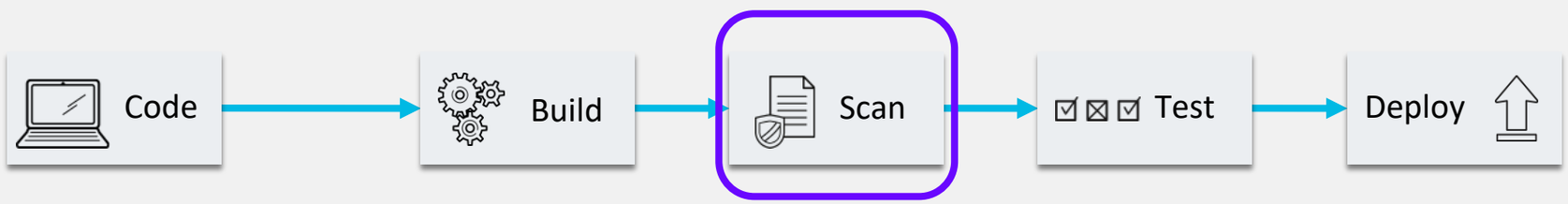


Security Testing of Code

Static testing

There are a fair amount of tools that can integrate now into CI/CD pipelines to provide static testing. Here are some common issues they look for:

- duplicated code
- coding standards
- unit tests
- code coverage
- code complexity
- comments
- bugs
- security vulnerabilities.



https://github.com/mre/awesome-static-analysis

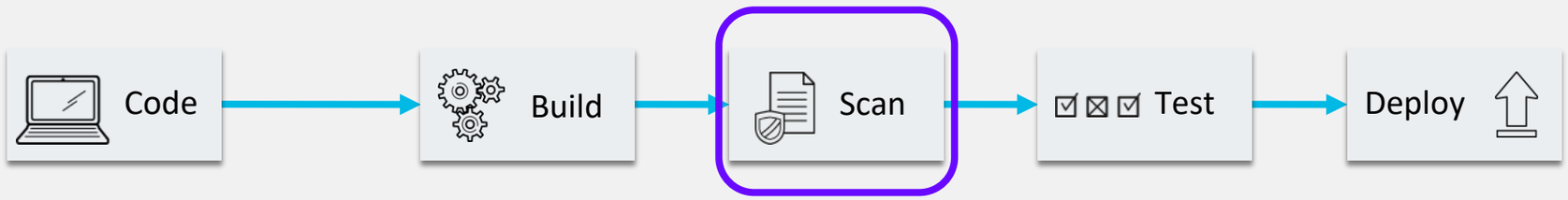
Security Testing of Code

Dynamic testing

Dynamic testing executes the application and uses inputs into the application to look for anomalous behavior, or observe for violations of policy.

There are two main types:

- Vulnerability Scanning
- Penetration Testing



Security Testing of Code

Dynamic testing

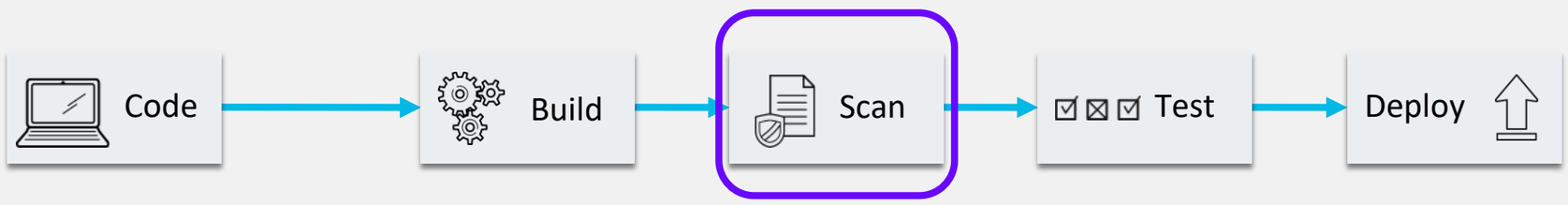
Some common dynamic code analysis tools:

OWASP ZAP

metasploit®

Nessus® vulnerability scanner

OpenSCAP



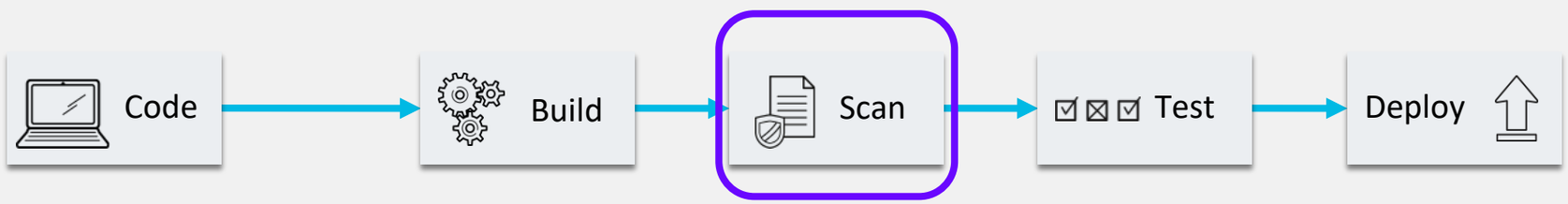
redhat.

Security Testing of Code

Dynamic testing

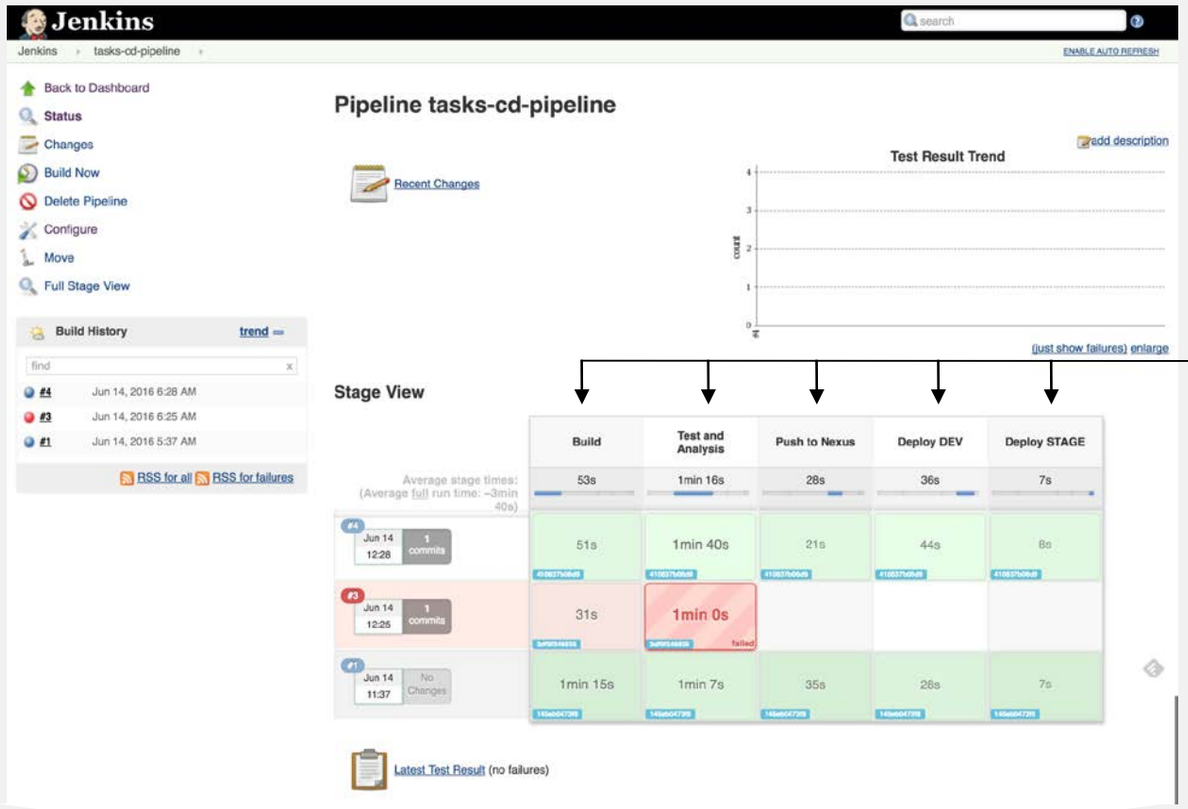
Dynamic scanning tools can look for:

- container or application misconfigurations
- vulnerable build dependencies
- vulnerable OSS components
- web/application vulnerabilities
- logic bugs



Security Testing of Code

Testing - Pipelines



- Build
- Test & Analysis
- Push to Nexus
- Deploy to Dev
- Deploy to Stage

https://blog.openshift.com/cicd-with-openshift/

Security Testing of Code

Static testing - Pipelines Jenkinsfile

cicd-template.yaml

```
jenkinsfile: |-
  pipeline {
    agent {
      label 'maven'
    }
  stages {
  stage('Build App') {
    steps {
      git branch: 'eap-7', url: 'http://gogs:3000/gogs/openshift-tasks.git'
      script {
         def pom = readMavenPom file: 'pom.xml'
         version = pom.version
      }
      sh "${mvnCmd} install -DskipTests=true"
    }
  }
  stage('Scan') {
```


https://blog.openshift.com/cicd-with-openshift/

Security Testing of Code

Static testing - Pipelines Jenkinsfile

```
stage('Static Analysis') {
        steps {
         script {
          if (env.WITH_SONAR.toBoolean()) {
            sh "${mvnCmd} sonar:sonar -Dsonar.host.url=http://sonarqube:9000 -DskipTests=true"
          } else {
            sh "${mvnCmd} site -DskipTests=true"

            step([$class: 'CheckStylePublisher', unstableTotalAll:'300'])
            step([$class: 'PmdPublisher', unstableTotalAll:'20'])
            step([$class: 'FindBugsPublisher', pattern: '**/findbugsXml.xml',)
            step([$class: 'JacocoPublisher'])
            publishHTML (target: reportDir: 'target/site', reportFiles: 'project-info.html)
          }
        }
      }
    }
```


https://blog.openshift.com/cicd-with-openshift/

Security Testing of Code

Static & Dynamic testing - Pipelines

- Can you automate all the Static and Dynamic tests?

Security Testing of Code

Static & Dynamic testing - Pipelines

- Can you automate all the Static and Dynamic tests?
- Can you add security tools to your DevOps Pipeline?

Security Testing of Code

Static & Dynamic testing - Pipelines

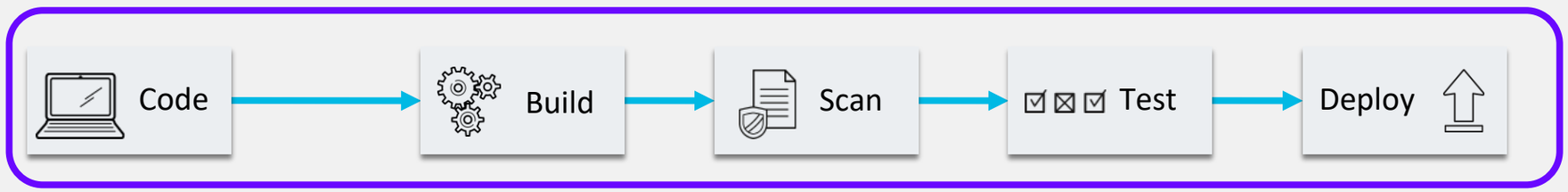
- Can you automate all the Static and Dynamic tests?
- Can you add security tools to your DevOps Pipeline?
- Can the tools themselves be containerized?

Audits & Gates for Pipelines

Audits for Pipelines

Are you able to answer critical questions about your software supply chain like;

- Understanding the container signature?
- Known CVEs?
- Which base images were used?
- RPM quality?
- Who deployed what instance when?
- A combination of all the above?

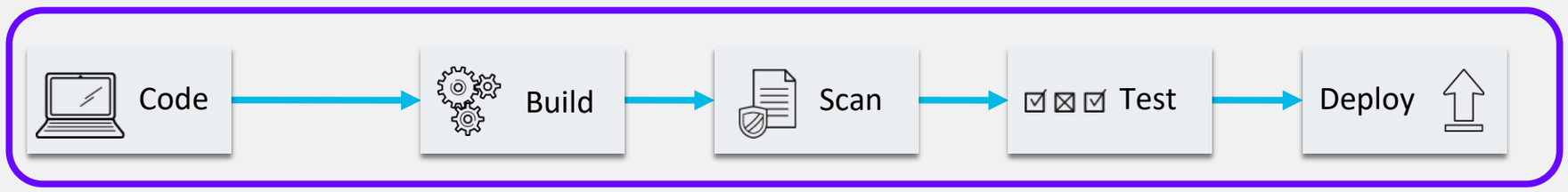


Gates for Pipelines

Can you ensure checks are being performed at each stage and enforced?

Binary Authorization is used to enforce central control and enforcement of software life cycle process.

- Deployment to the next stage is prevented unless the artifact passes all tests.
- When an artifact successfully completes a stage, an attestation on that artifact is created which asserts success.



Audits & Gates for Pipelines

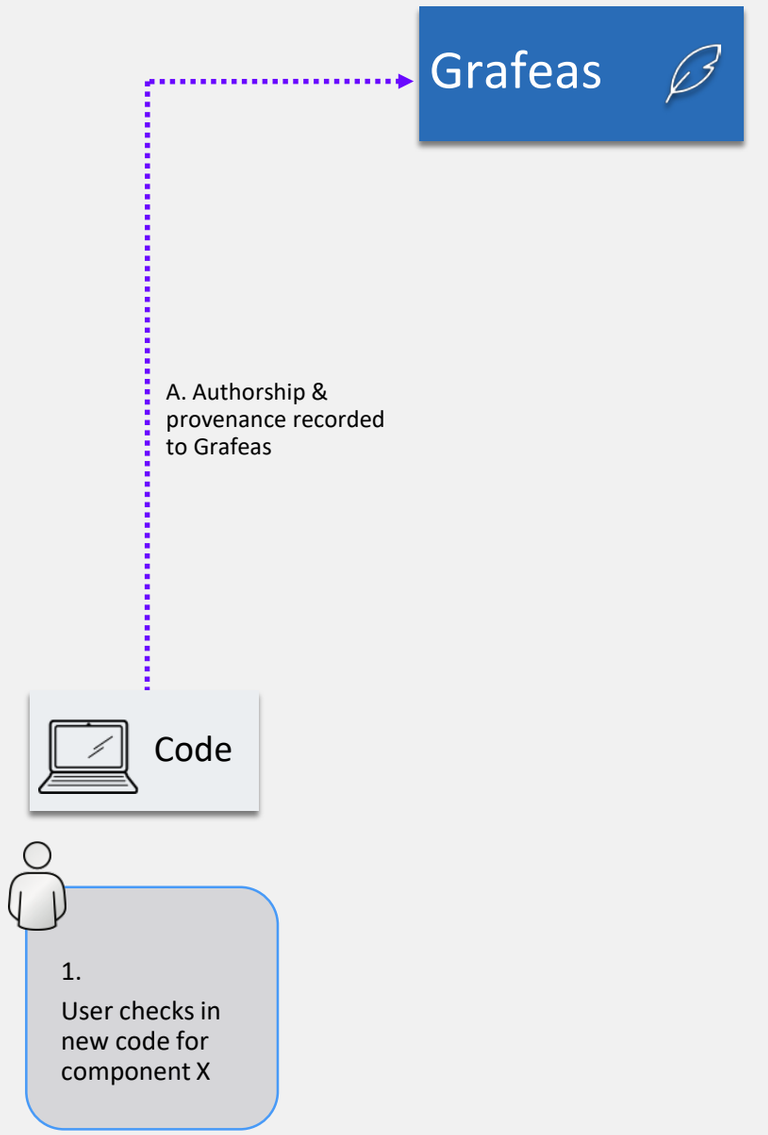
Grafeas & Kritis to audit your pipeline and enforce policy

https://grafeas.io/docs/

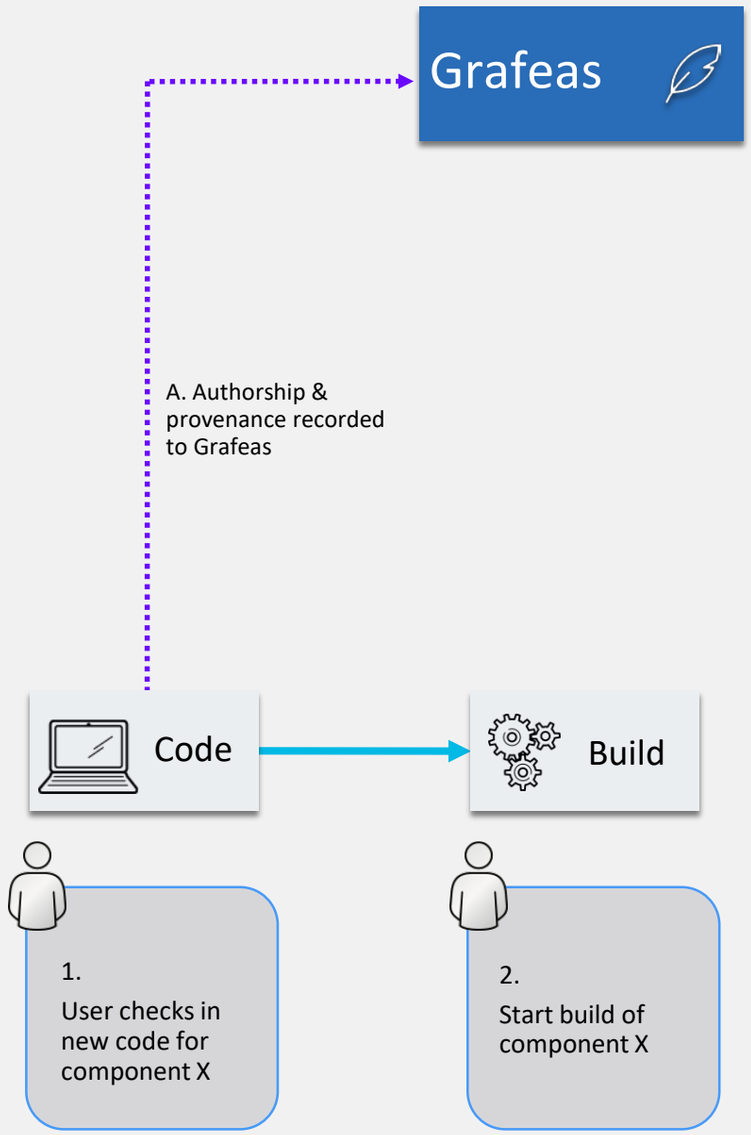
Audits & Gates for Pipelines

1.
User checks in new code for component X

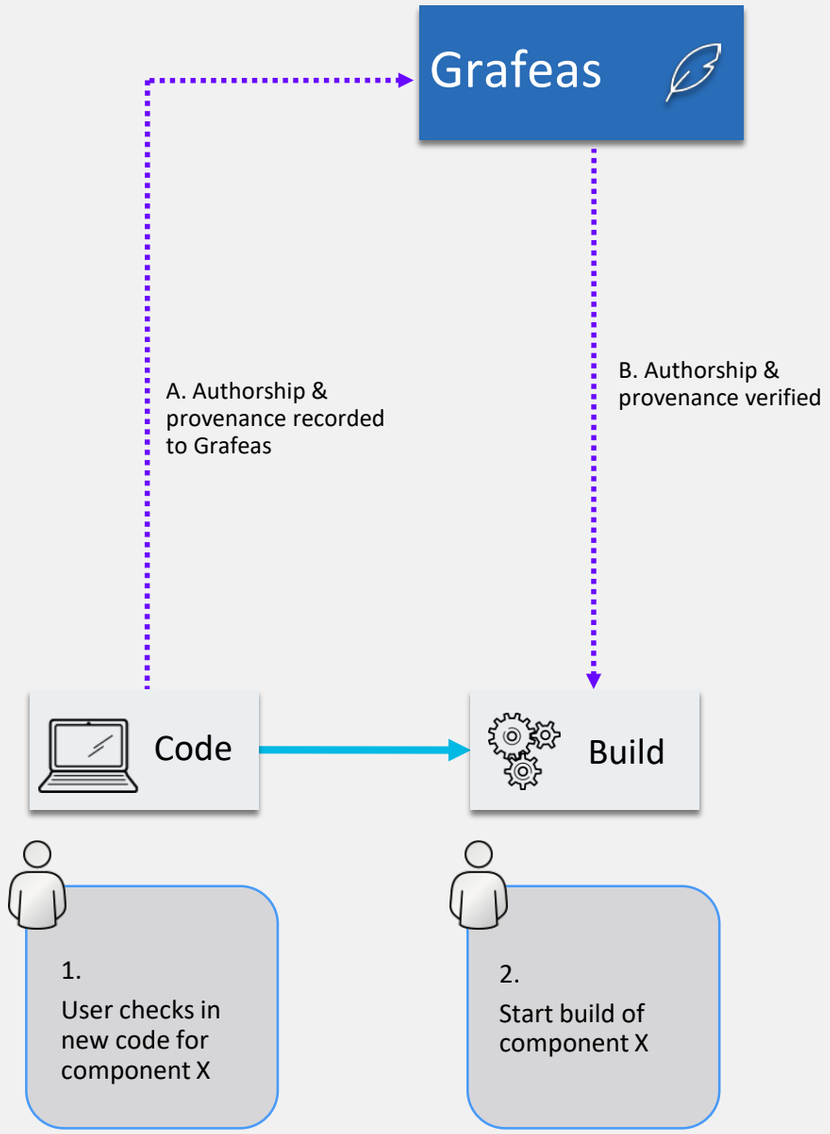
Audits & Gates for Pipelines



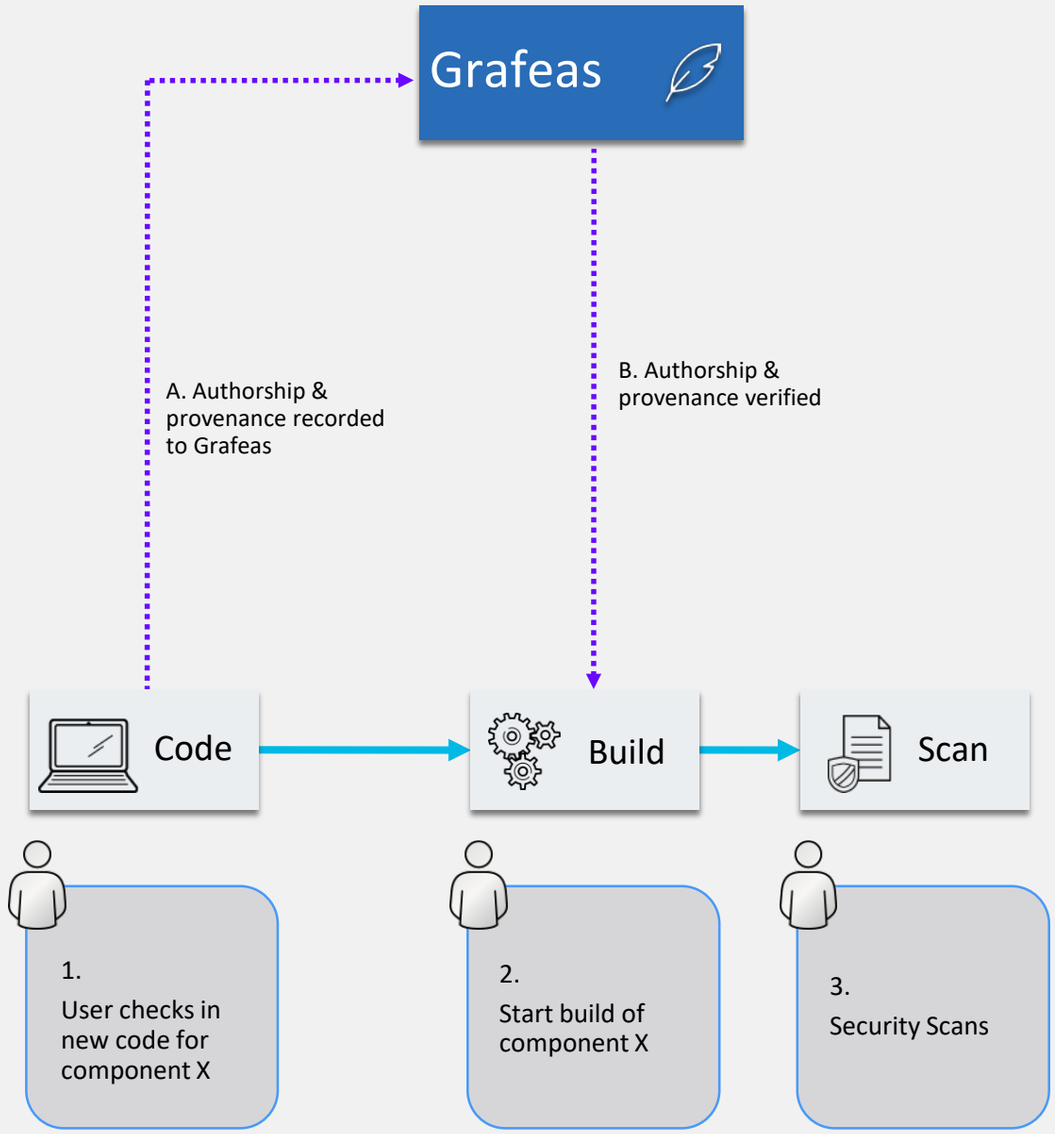
Audits & Gates for Pipelines



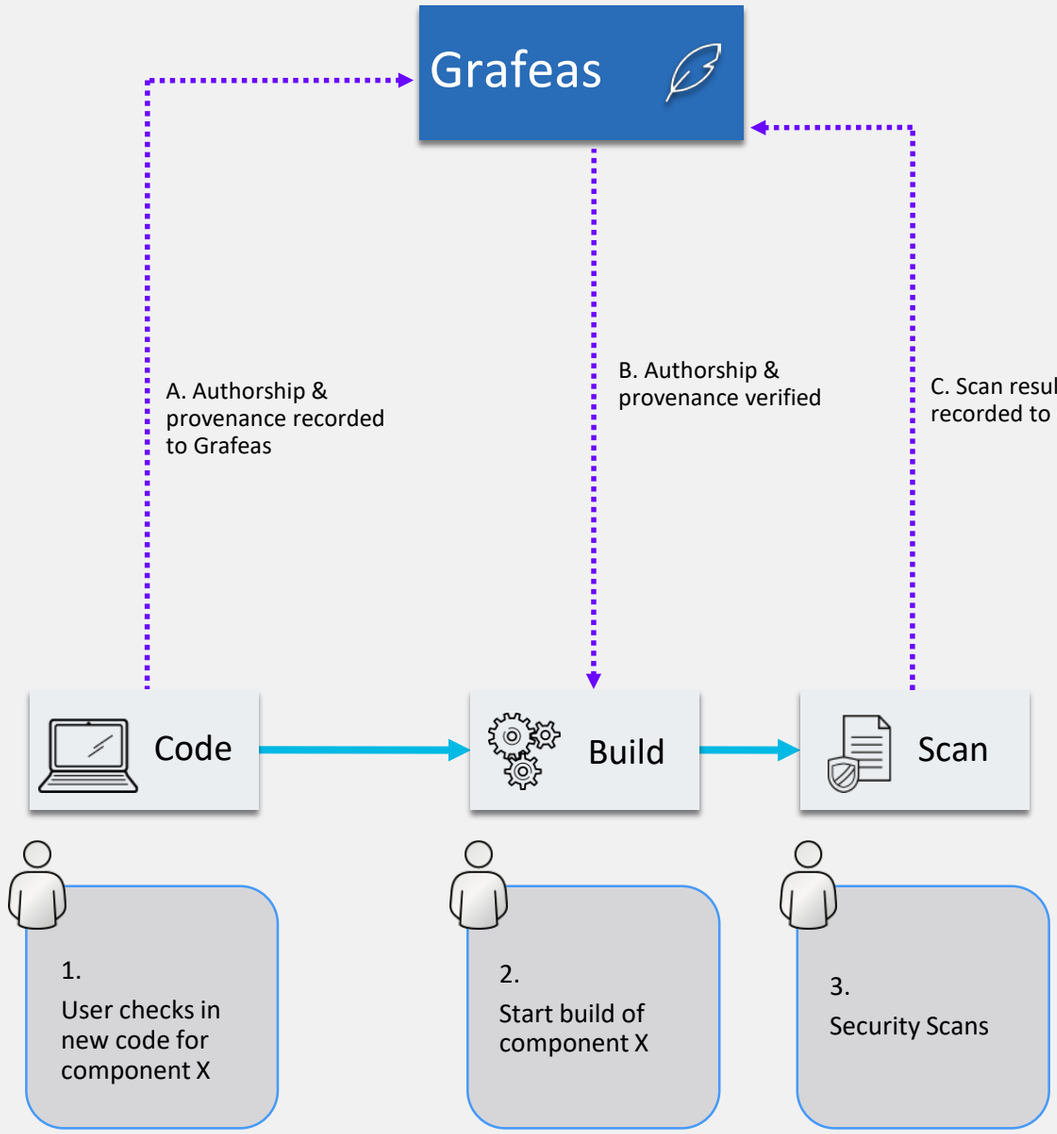
Audits & Gates for Pipelines



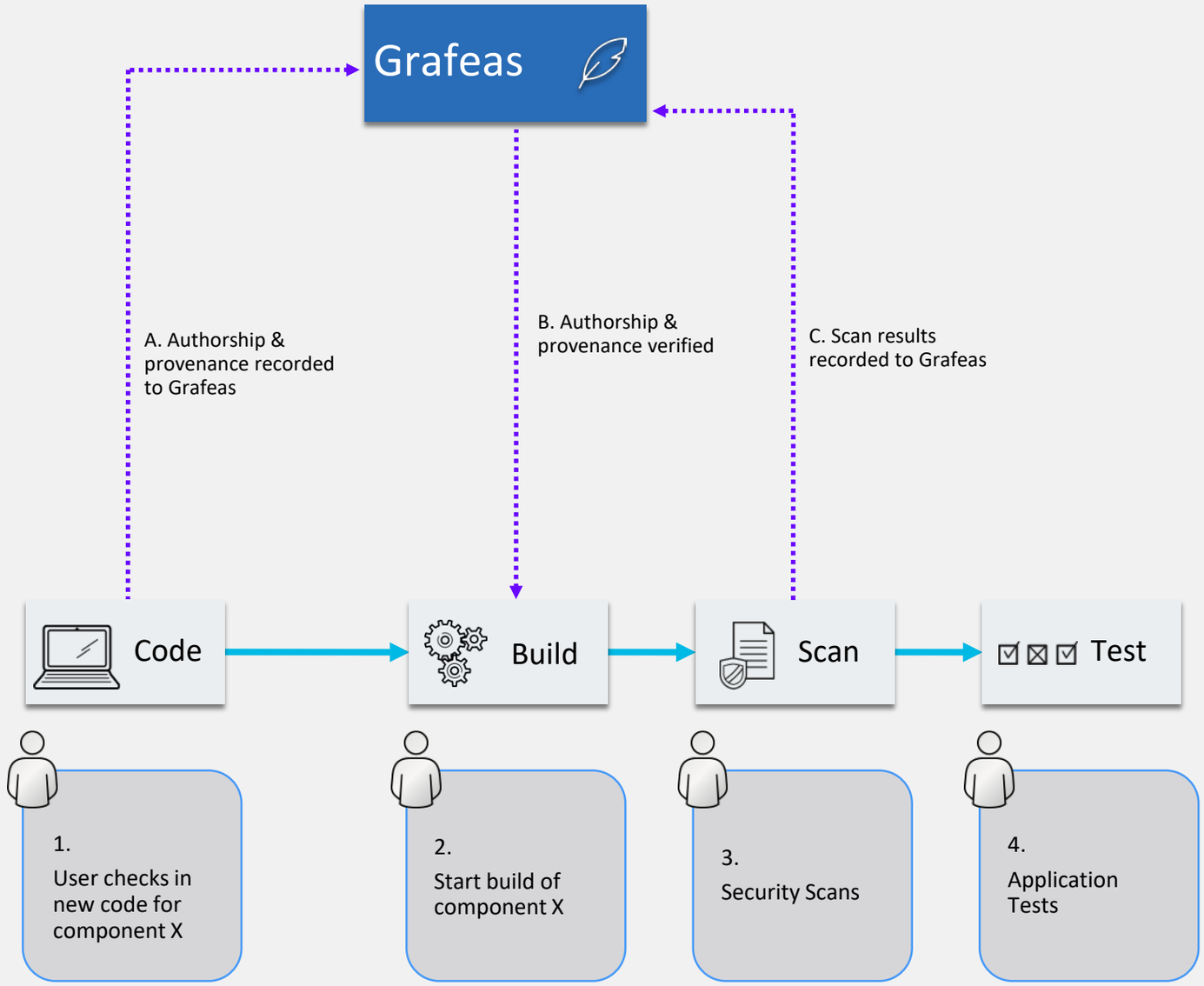
Audits & Gates for Pipelines



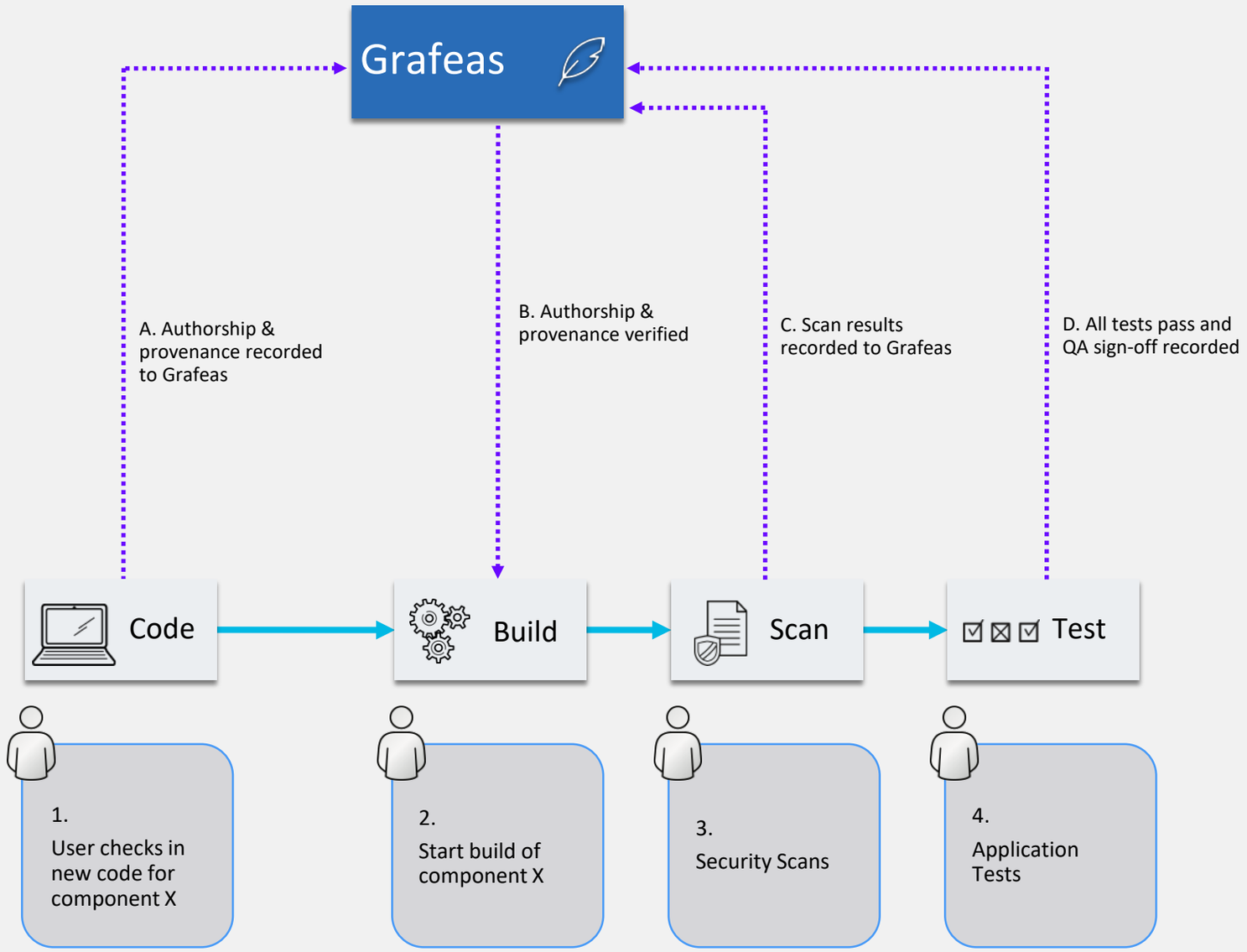
Audits & Gates for Pipelines



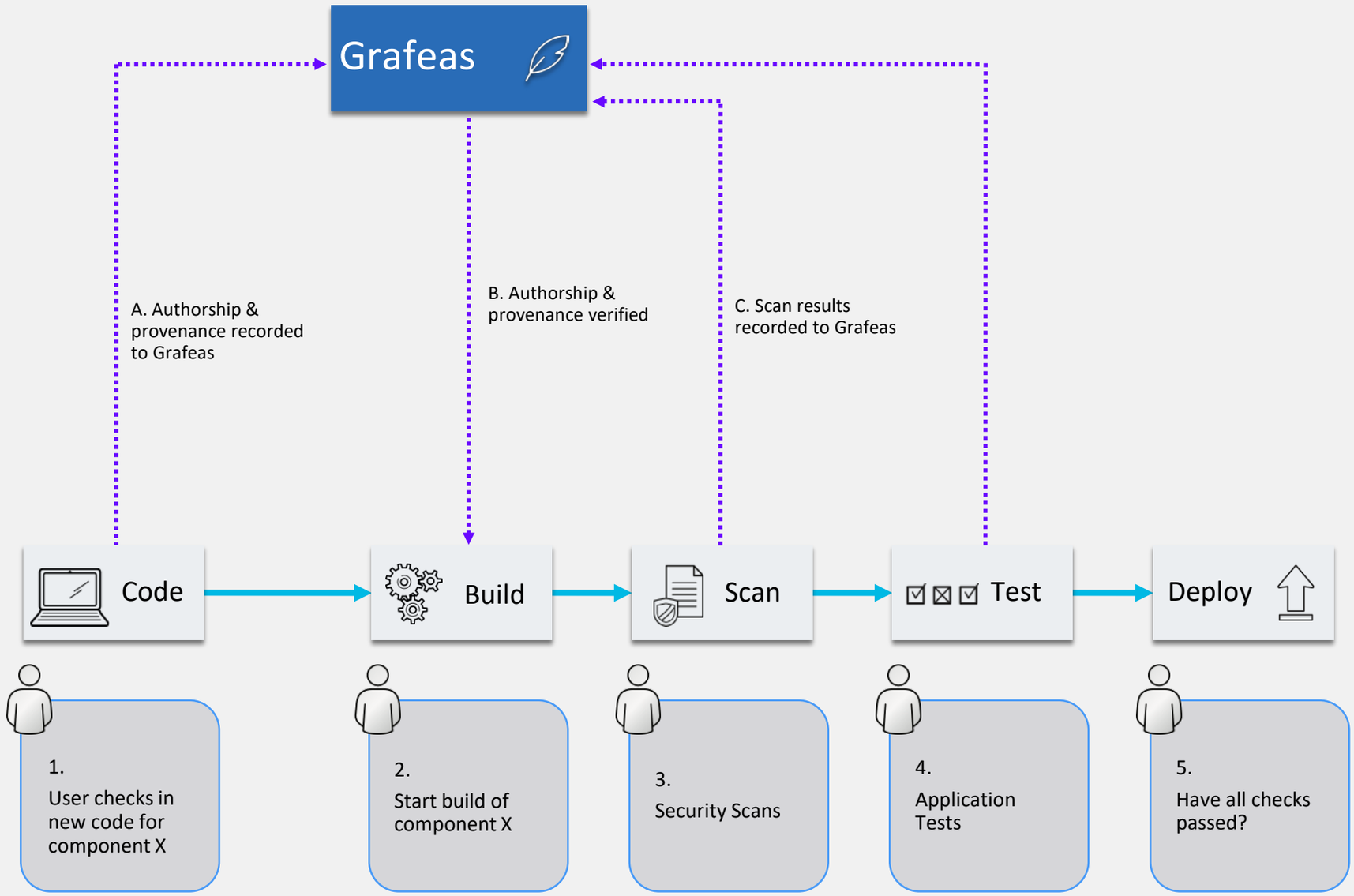
Audits & Gates for Pipelines



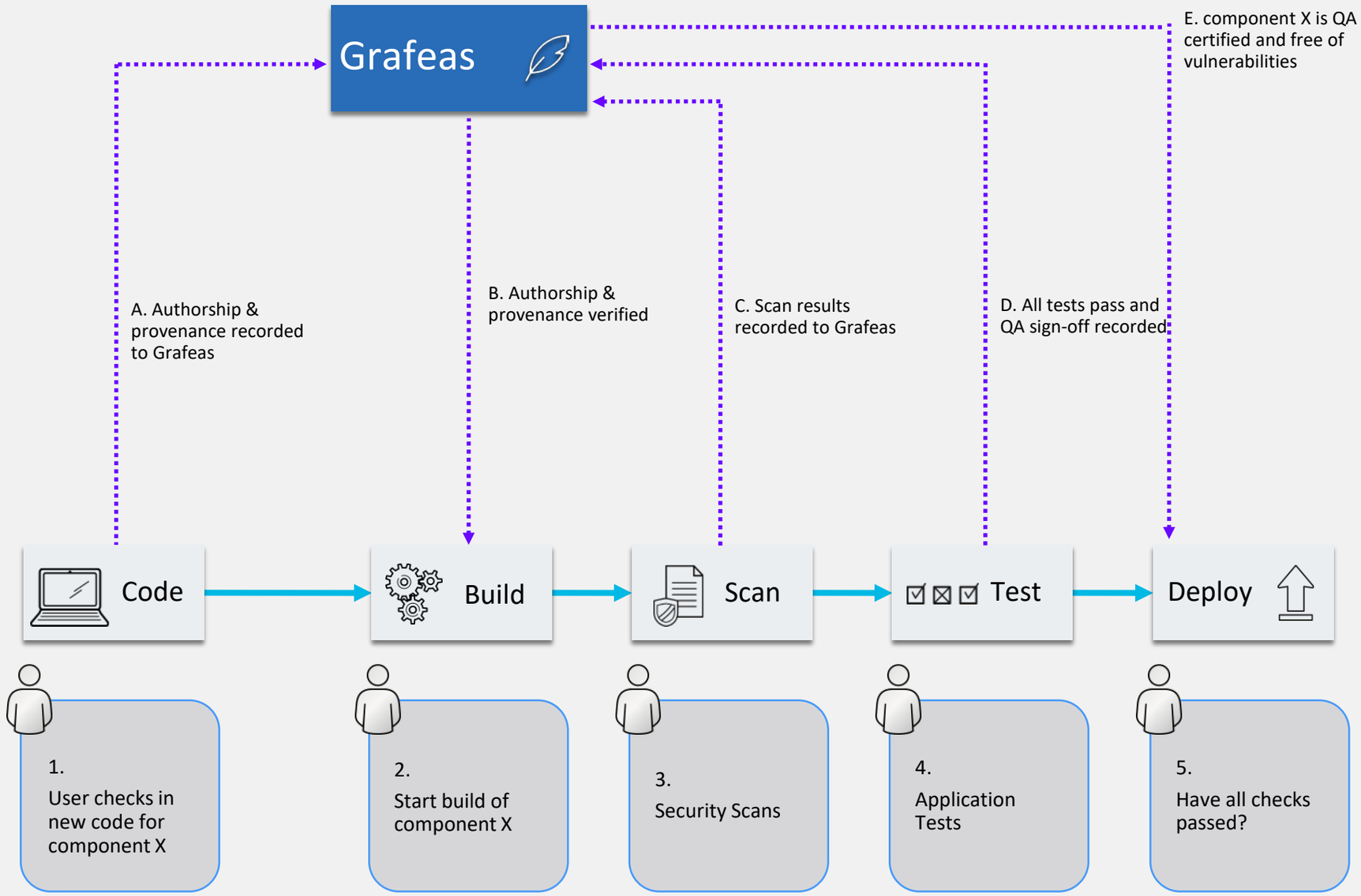
Audits & Gates for Pipelines



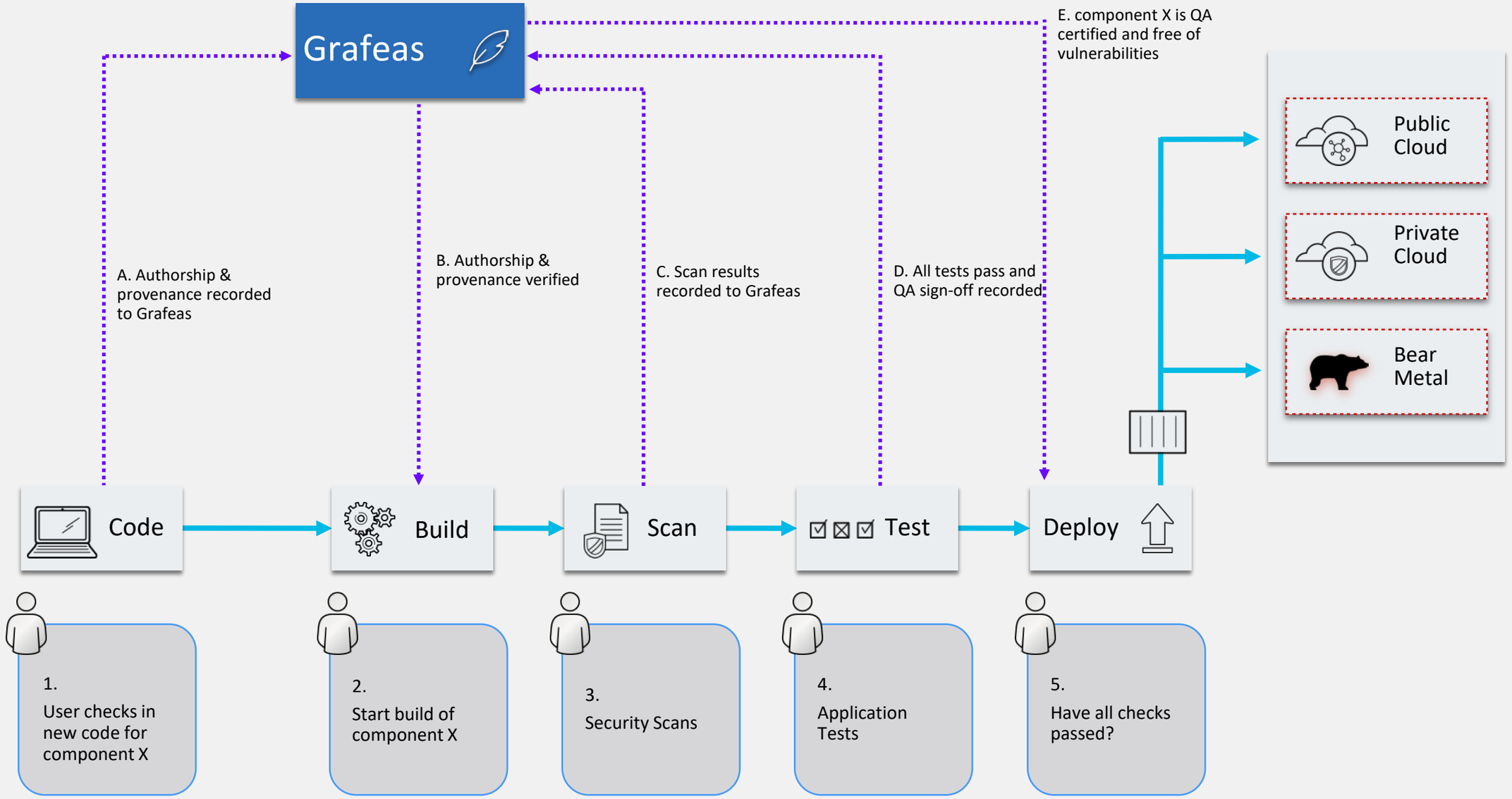
Audits & Gates for Pipelines



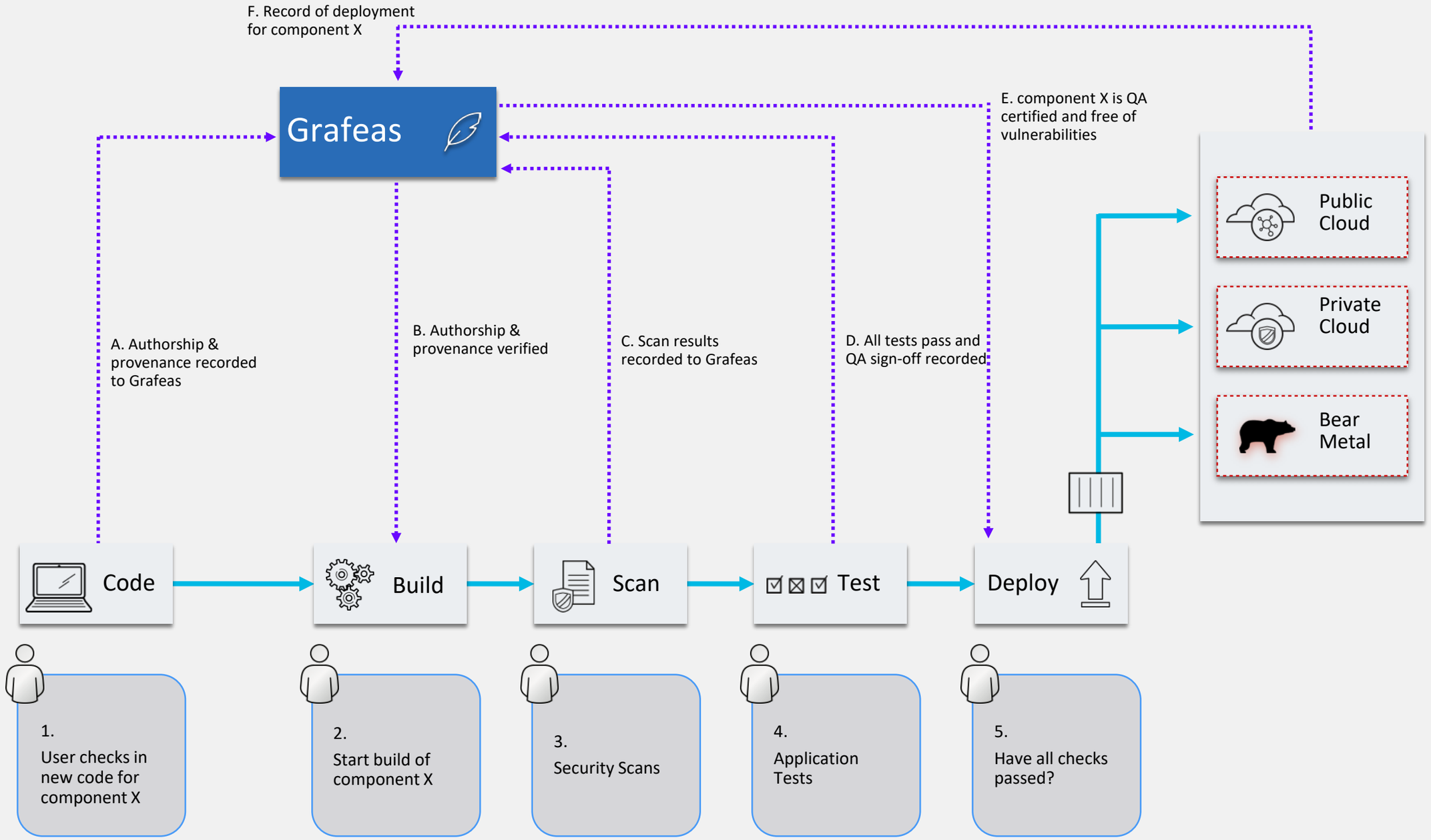
Audits & Gates for Pipelines



Audits & Gates for Pipelines



Audits & Gates for Pipelines



redhat.

Platform Questions

Is your platform as secure as it can be?

Container Image provenance

- Can you control where your containers come from?
- Role-based-access to images?

Platform Questions

Is your platform as secure as it can be?

Container Image provenance

- Can you control where your containers come from?
- Role-based-access to images?

Static & Dynamic testing

- Can you automate all the Static and Dynamic tests?
- Can you add security tools to your DevOps Pipeline?
- Can the tools them selfs be containerized?

Platform Questions

Is your platform as secure as it can be?

Container Image provenance

- Can you control where your containers come from?
- Role-based-access to images?

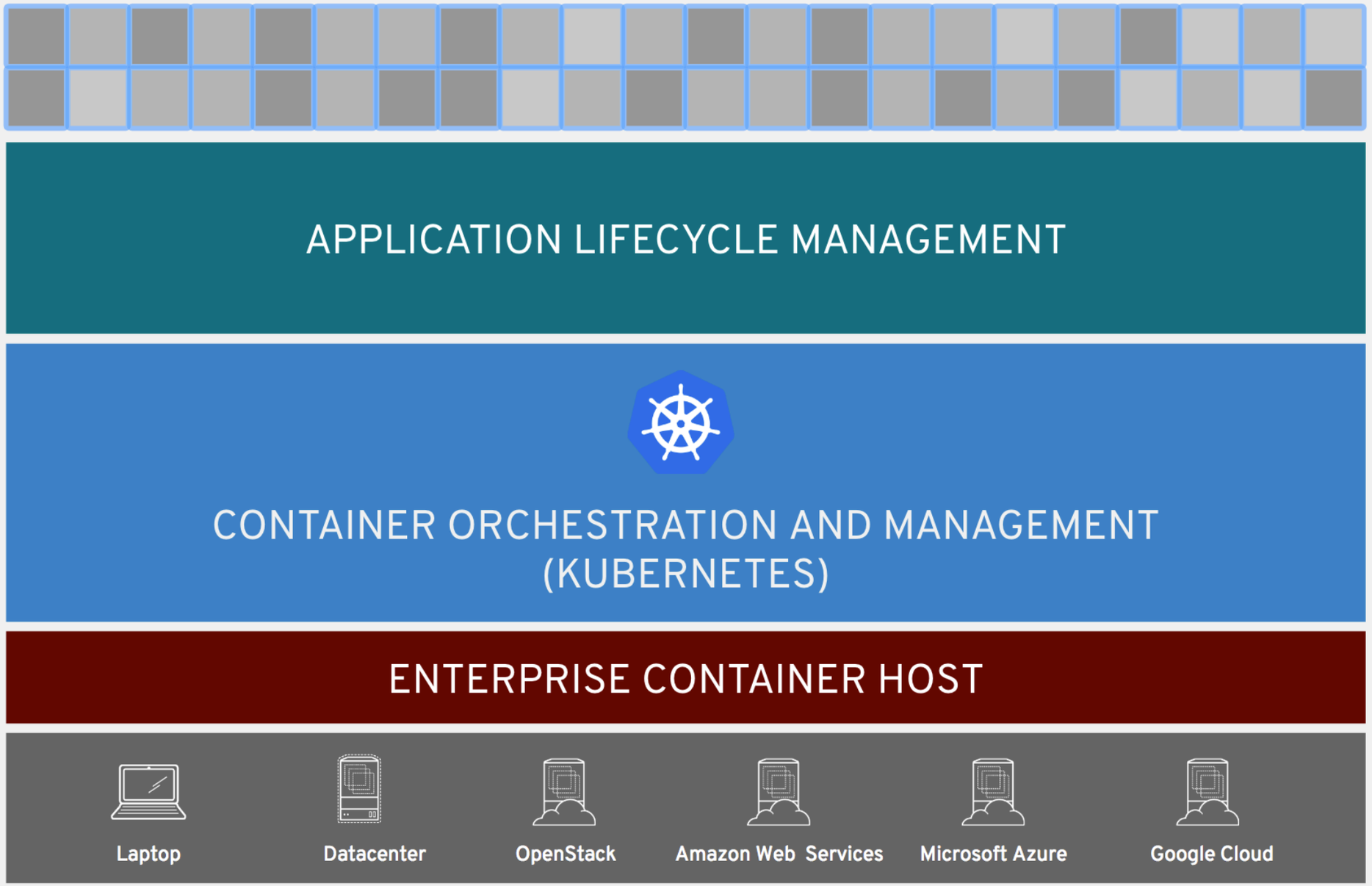
Static & Dynamic testing

- Can you automate all the Static and Dynamic tests?
- Can you add security tools to your DevOps Pipeline?
- Can the tools them selfs be containerized?

Audits & Gates for Pipelines

- Understanding the container signature?
- Known CVEs?
- Which base images were used?
- RPM quality?
- Who deployed what instance when?
- Enforce Gates for promotion to next stages?

Enterprise Kubernetes



ANY
CONTAINER

RED HAT®
OPENSHIFT

ANY
INFRASTRUCTURE

redhat.

OpenShift

S2P OpenShift as a Service

Red Hat provides OpenShift Container Platform (OCP) as a managed S2P service.

This service is available to all programs and provides a multi-tenant, hosted Linux Container as a service.

The solution is currently running with an interim ATO in both Development and Test. Full ATO is pending for Production. At the moment NASP is providing this service free to programs.

Questions?

redhat.

Thank You!

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos