Workshop: Implementing Multi-Layer Container and Kubernetes Security for Automated DevSecOps

Red Hat

Agenda:

- DevSecOps Intro
- Lab Info and walkthrough
- Lab 1 - 3
- Break
- Lab 4 - 5
- Q & A

Workshop Info:

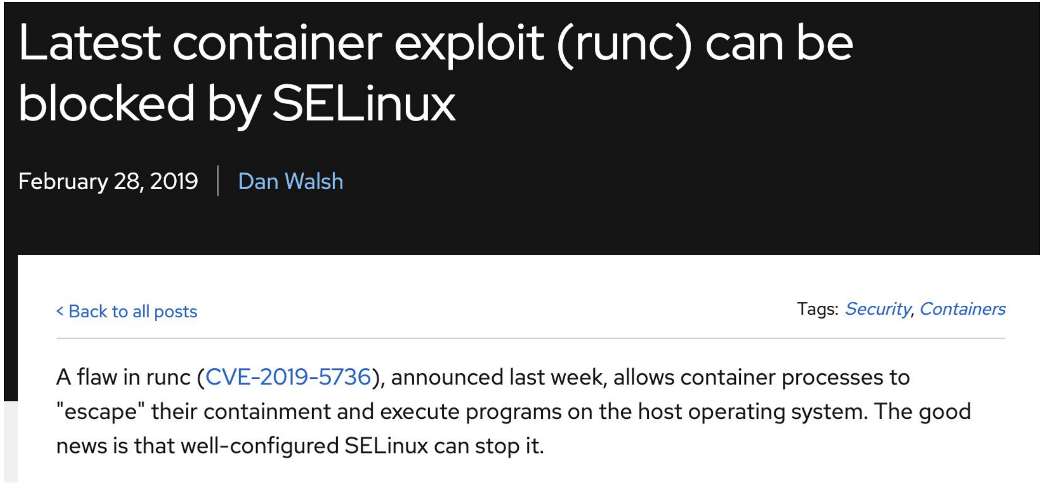
Get a lab env: <Insert GuidGrabber client link>

Activation Key:

Lab Guide: http://bit.ly/rht-security-workshop

Built-in container runtime protection

SELinux and Security Context Constraints



Latest container exploit (runc) can be blocked by SELinux

February 28, 2019 | Dan Walsh

< Back to all posts

Tags: *Security*, *Containers*

A flaw in runc (CVE-2019-5736), announced last week, allows container processes to "escape" their containment and execute programs on the host operating system. The good news is that well-configured SELinux can stop it.

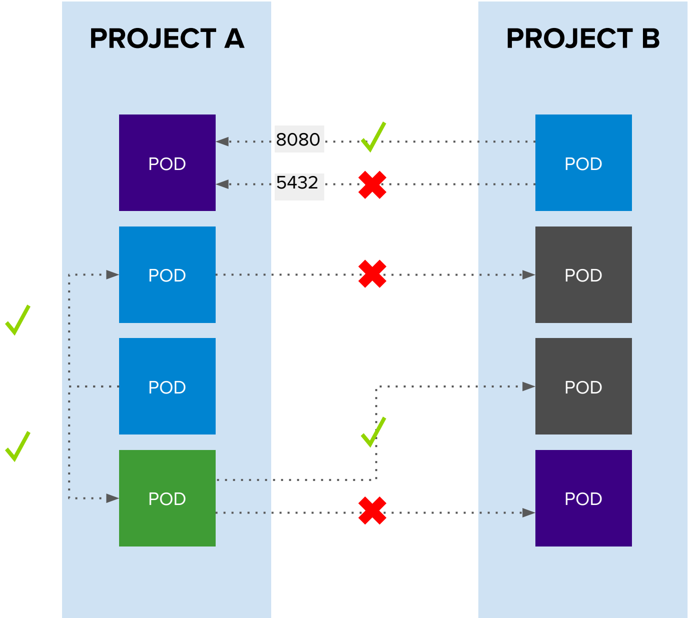
https://www.redhat.com/en/blog/latest-container-exploit-runc-can-be-blocked-selinux

Security Context Constraint

Admission controller

- By default, containers cannot run with privilege on OpenShift (restricted SCC)
- Limit access to SCC's that relax policies
  - anyuid, privileged
- Avoid modifying default policies
- Create custom policies when necessary and scope access appropriately
- Design containers with SCC's in mind
- Test third party containers for supportability

NetworkPolicy

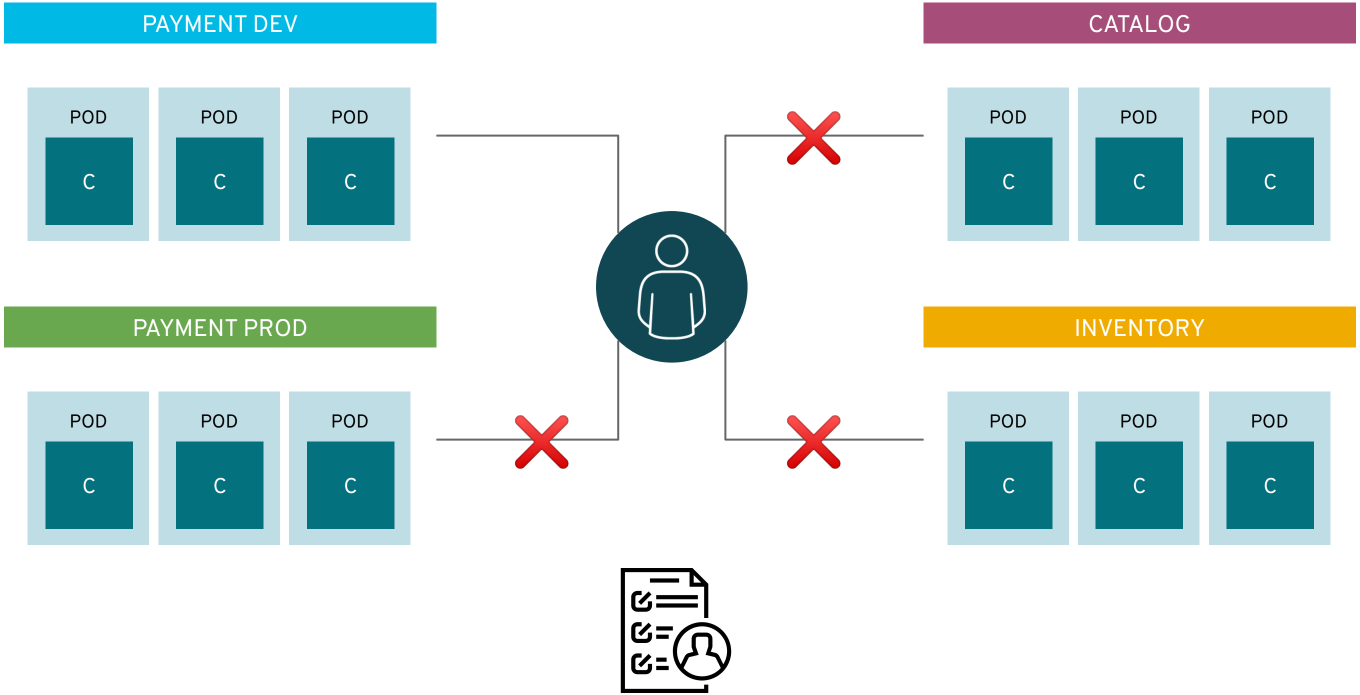


Example Policies

- Allow all traffic inside the project
- Allow traffic from green to gray
- Allow traffic to purple on 8080

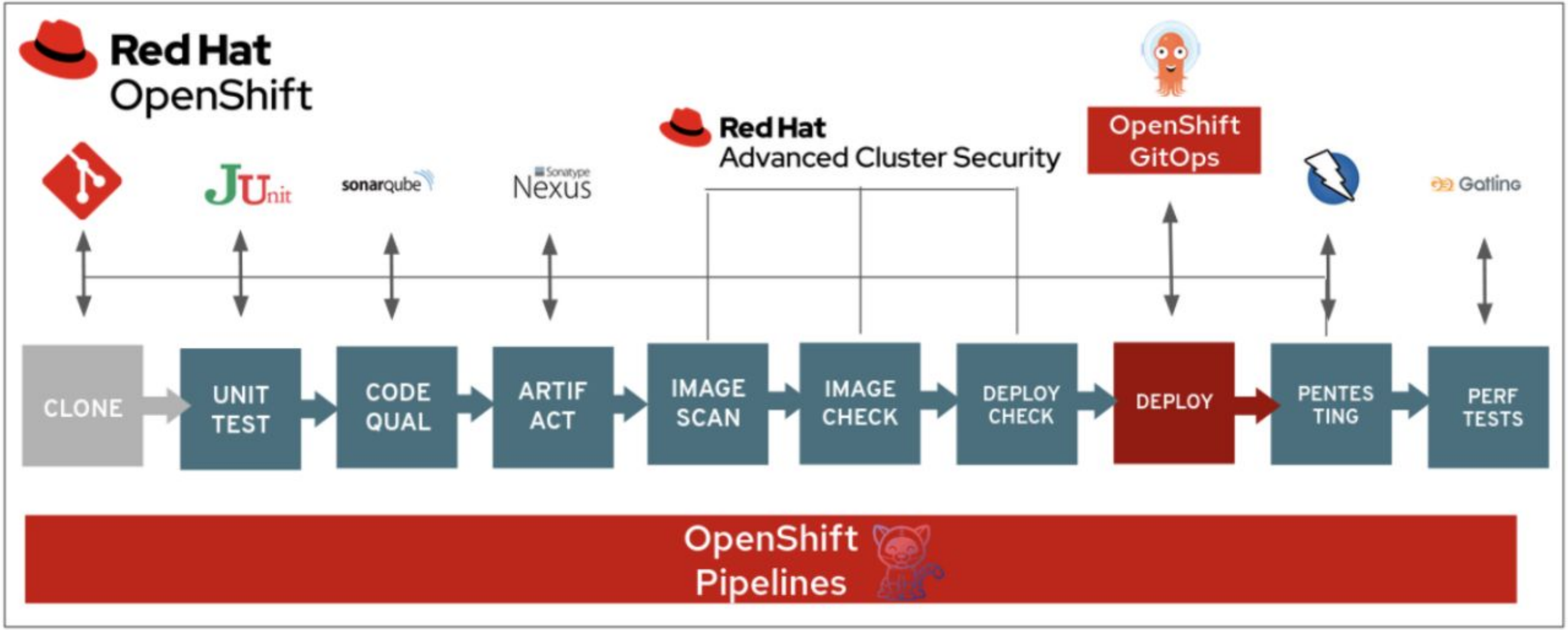
```
apiVersion: extensions/v1beta1
kind: NetworkPolicy
metadata:
  name: allow-to-purple-on-8080
spec:
  podSelector:
    matchLabels:
      color: purple
  ingress:
  - ports:
    - protocol: tcp
      port: 8080
```

Projects isolate applications across teams, groups and departments

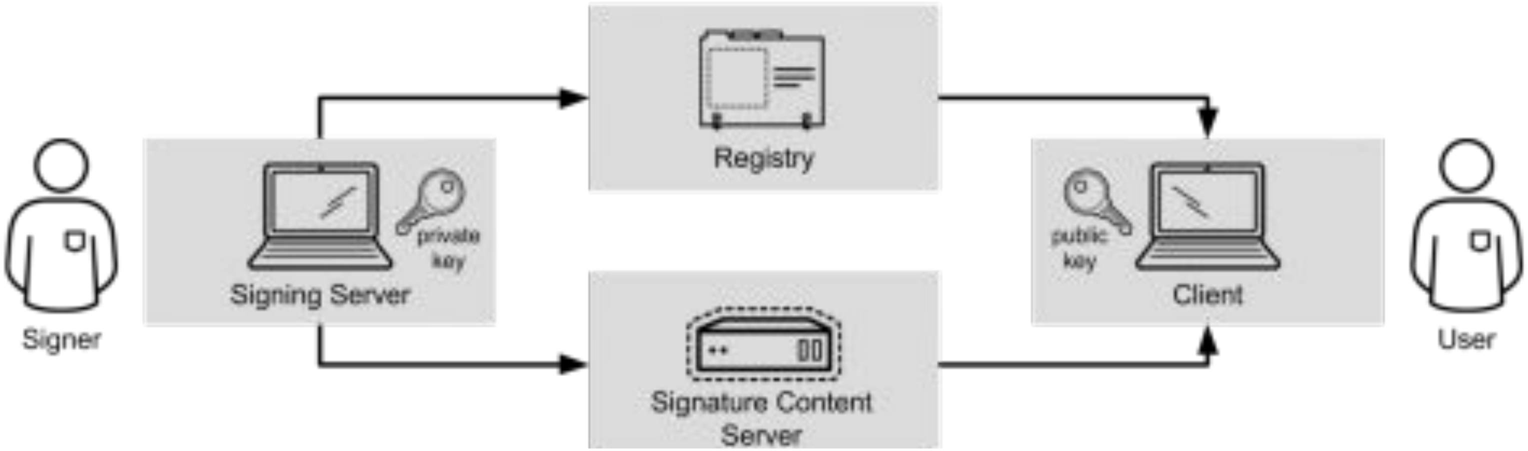


Enforced with IAM & RBAC

Integrate Security in your CI/CD Pipeline



CONTAINER IMAGE SIGNING



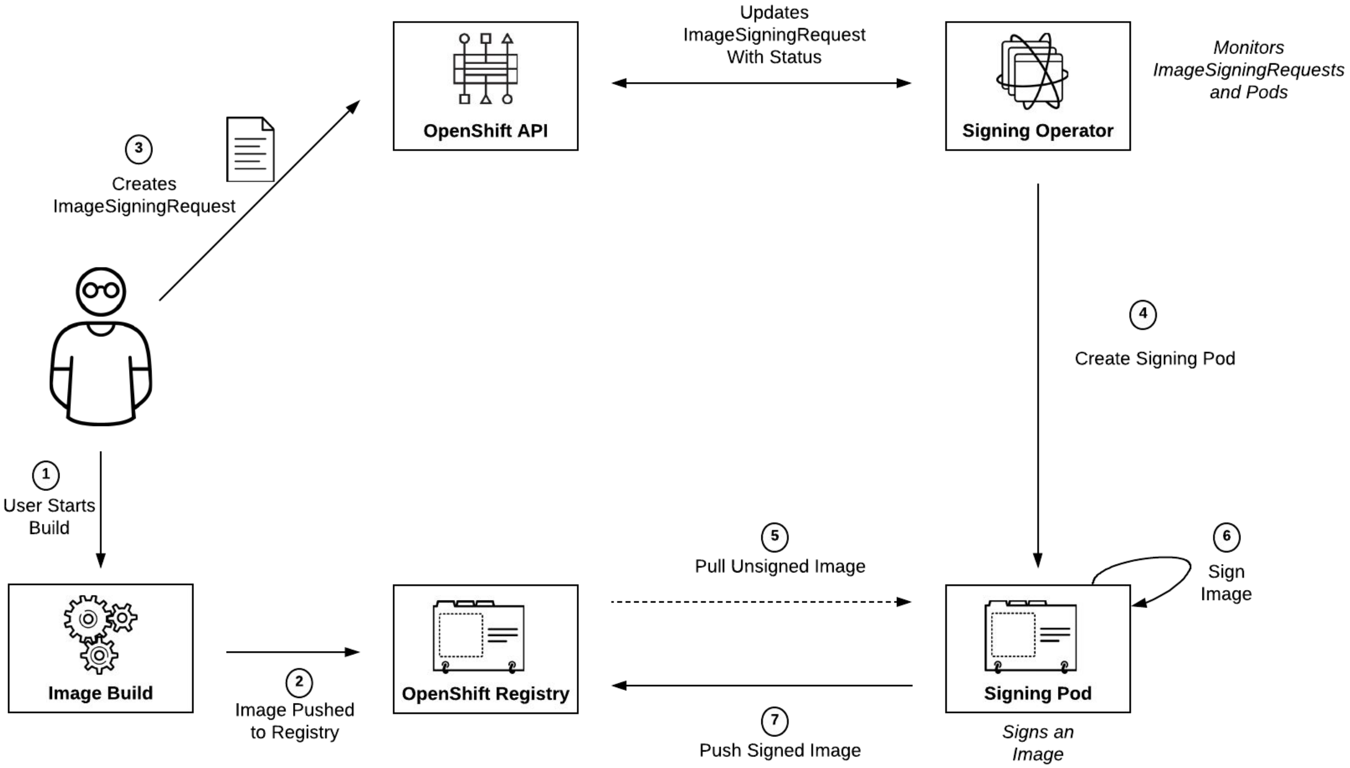
Verify provenance of images

Registry independent

Supports multiple signatures

Enforce signatures at node level via signing trust policy

IMAGE SIGNING IN PRACTICE



Lab 5

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

Red Hat
Summit
May 10-11, 2022

https://www.redhat.com/en/summit

Below is a collection of briefs, ebooks, and collateral aligned to a variety of security subtopics. These can be handed out at your workshop if in-person, shared with attendees during the workshop, or sent out as a followup to attendees.

https://red.ht/securityinfo

- Detail: A layered approach to container and Kubernetes security
- Detail: Definitive guide to Red Hat OpenShift security
- E-book: Red Hat OpenShift security guide
- E-book: State of Kubernetes security report
- E-book: Boost Hybrid Cloud Security
- E-book: Application development security
- Whitepaper: Kubernetes-native security
- Whitepaper: A definitive guide to achieving DevSecOps in Kubernetes environments
- E-book: Architecting for HIPAA Security Rule
- Datasheet: Red Hat Advanced Cluster Security for Kubernetes

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.

in linkedin.com/company/red-hat

youtube.com/user/RedHatVideos

f facebook.com/redhatinc

twitter.com/RedHat

Red Hat