Red Hat Summit

Connect

DevSecOps con ACS

Àngel Ollé Blázquez
Specialist Solution Architect

José Ángel de Bustos
Specialist Solution Architect

Red Hat | intel

"Open Source proudly user from the middle 90s, intensely engaged with Open Source promotion not only in my personal life but in my professional career as well. More than 15 years of experience in IT I work as a Senior Solutions Architect."

José Ángel de Bustos
Red Hatter

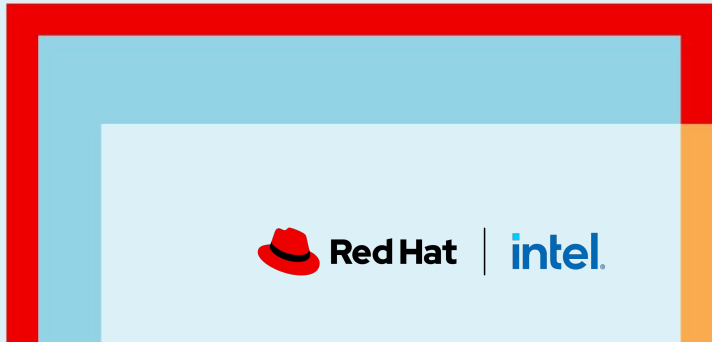
Red Hat | intel

"Specialist Solution Architect, focused on development and middleware technologies.
Software security enthusiast."

Àngel Ollé Blázquez
Red Hatter

Red Hat | intel.

Challenges



DevSecOps Challenges for Developers

Red Hat | intel.

DevSecOps Challenges for Developers

Red Hat | intel.

DevSecOps Challenges for Developers

Red Hat | intel.

DevSecOps Challenges for Developers

Red Hat | intel.

DevSecOps Challenges for Security Department

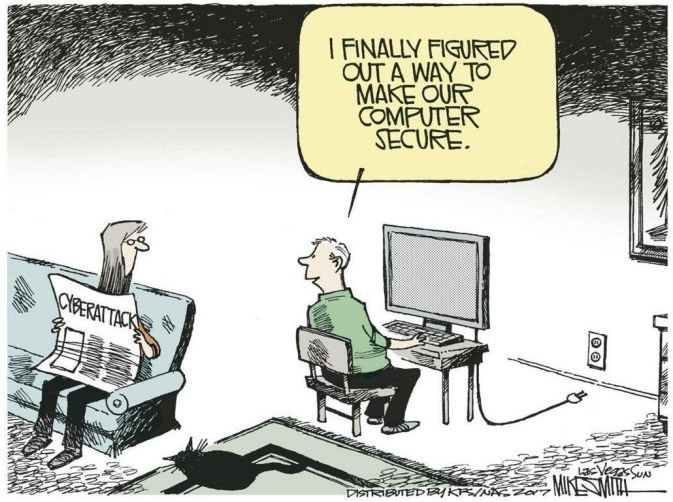
Red Hat | intel.

DevSecOps Challenges for Security Department

"Somebody broke into your computer, but it looks like the work of an inexperienced hacker."

DevSecOps Challenges for Security Department

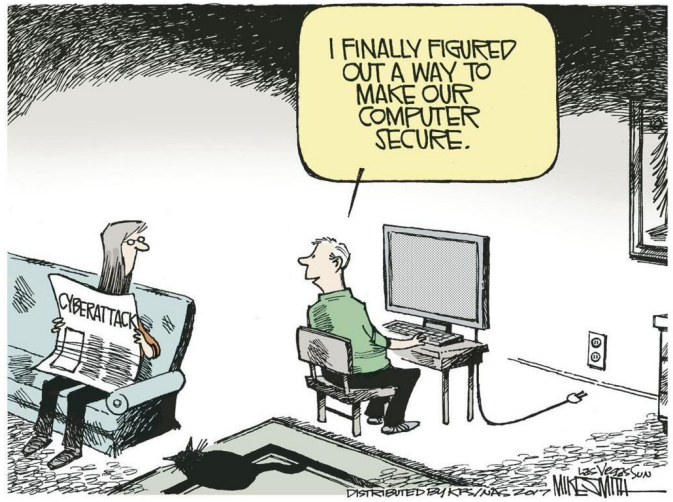
"Somebody broke into your computer, but it looks like the work of an inexperienced hacker."



Red Hat | intel.

DevSecOps Challenges for Security Department

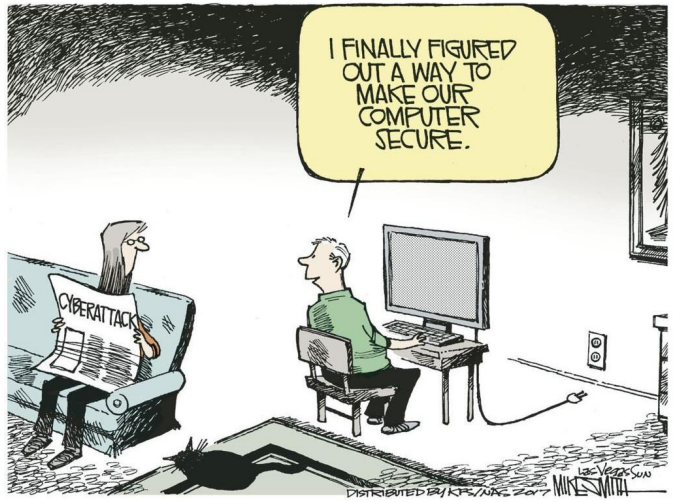
"Somebody broke into your computer, but it looks like the work of an inexperienced hacker."



Red Hat | intel.

DevSecOps Challenges for Security Department

"Somebody broke into your computer, but it looks like the work of an inexperienced hacker."



The cybersecurity program you want to run

The cybersecurity program you're forced to run on your current budget

Red Hat | intel.

Red Hat Advanced Cluster Security for Kubernetes (ACS)

Red Hat | intel

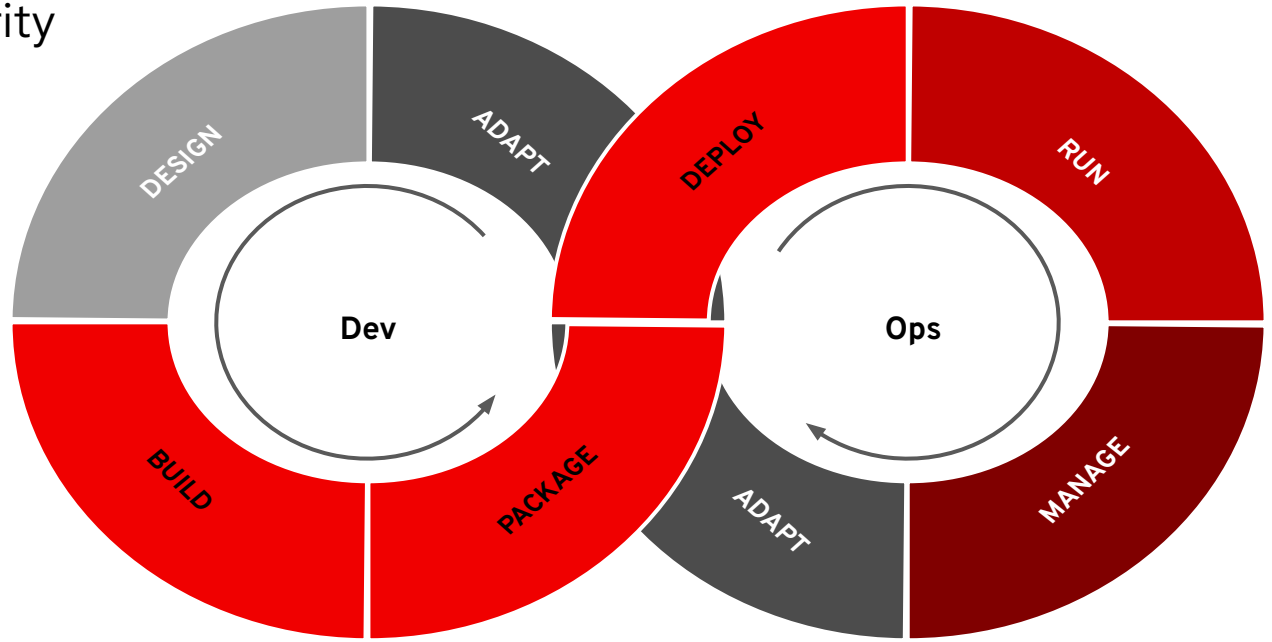
Containers and Kubernetes need DevSecOps

Security is not a product, but a process

Control Application Security

Protect the Platform

Detect & Respond to Runtime Threats



DevSecOps

Kubernetes is the standard for application innovation...

- Microservices architecture
- Declarative definition
- Immutable infrastructure

...and Kubernetes-native security is increasingly critical

- Secure supply chain
- Secure infrastructure
- Secure workloads

DevOps | DevSecOps | Security

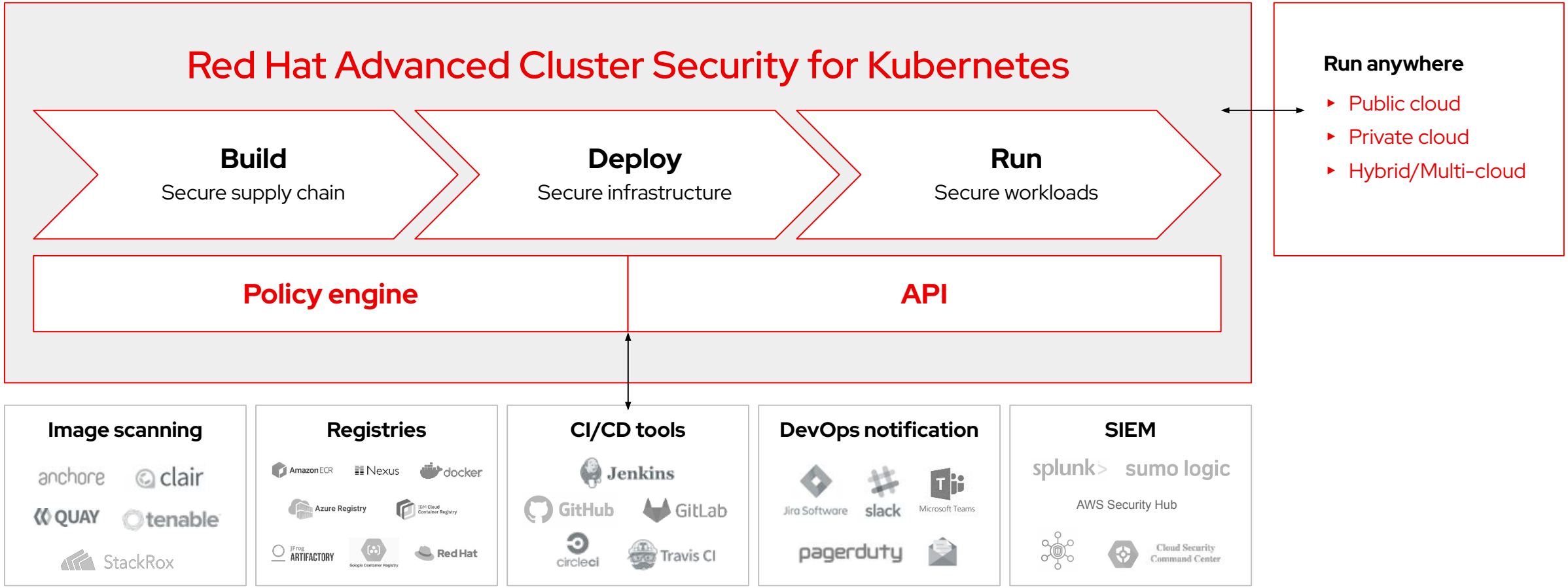
Red Hat Advanced Cluster Security for Kubernetes

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

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

DevSecOps

The first Kubernetes-native security platform



Red Hat | intel

Red Hat Advanced Cluster Security: Use Cases

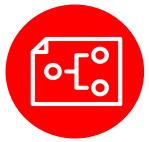
Security across the entire application lifecycle

Vulnerability Management

Protect yourself against known vulnerabilities in images and running containers

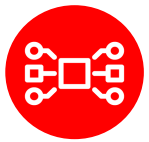
Configuration Management

Ensure your deployments are configured according to security best practices



Risk Profiling

Gain context to prioritize security issues throughout OpenShift and Kubernetes clusters



Network Segmentation

Apply and manage network isolation and access controls for each application

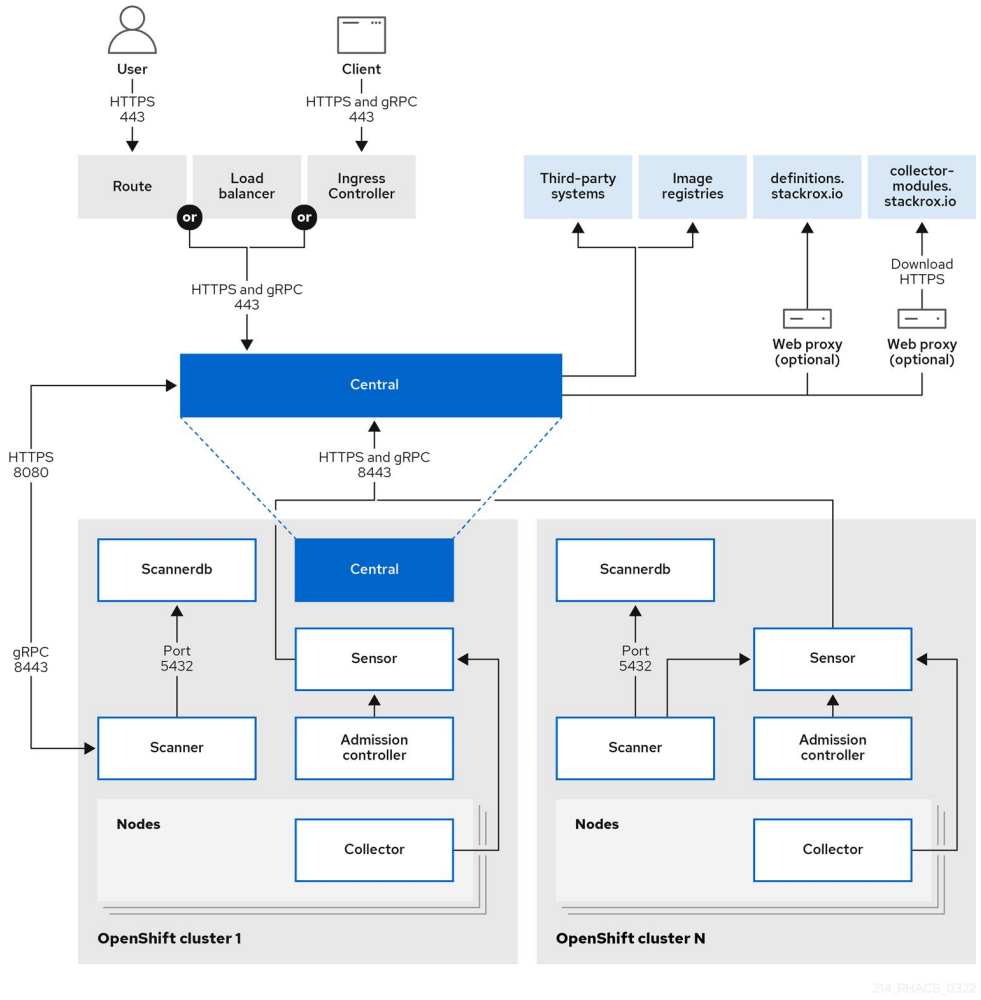
Compliance

Meet contractual and regulatory requirements and easily audit against them

Detection and Response

Carry out incident response to address active threats in your environment

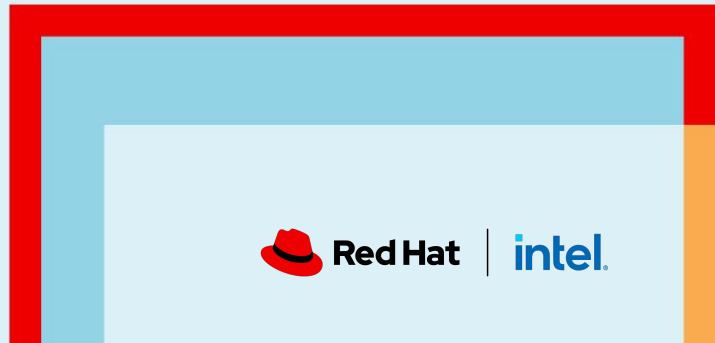
Architecture



- **Central** is the RHACS application management interface and services. It handles data persistence, API interactions, and user interface (RHACS Portal) access. You can use the same Central instance to secure multiple OpenShift Container Platform or Kubernetes clusters.
- **Sensor** is the service responsible for monitoring the cluster. It handles interactions with the OpenShift Container Platform or Kubernetes API server for policy detection and enforcement, and it coordinates with Collector.
- The **Admission Controller** prevents users from creating workloads that violate security policies in RHACS.
- **Collector** analyzes and monitors container activity on cluster nodes. It collects information about container runtime and network activity and sends the collected data to Sensor.
- RHACS installs a lightweight version of **Scanner** on each secured cluster to enable scanning of images in the integrated registry (ACS 3.69.1 or newer).

Red Hat | intel.

Demo



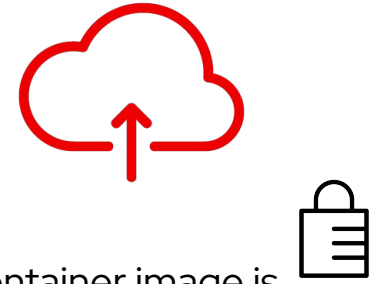
DevSecOps

1 New release is developed

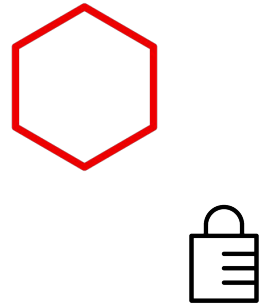
2 Container image is created

3 Container image is stored in a registry

4 Container image is deployed to a cloud-native platform



5 Pod/container is running in production



DevOps | DevSecOps | Security

Red Hat | intel

DevSecOps

1 New release is developed

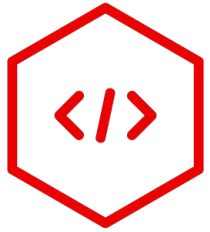
Static code analysis and language analysis built-in to CI/CD pipelines

```
$ npm audit
# npm audit report

ansi-html  *
Severity: high
Uncontrolled Resource Consumption in ansi-html -
https://github.com/advisories/GHSA-whgm-jr23-g3j9
fix available via `npm audit fix --force`
Will install react-scripts@5.0.0, which is a breaking change
…
…
160 vulnerabilities (136 moderate, 22 high, 2 critical)

To address issues that do not require attention, run:
  npm audit fix

To address all issues (including breaking changes), run:
  npm audit fix --force
```

Red Hat | intel

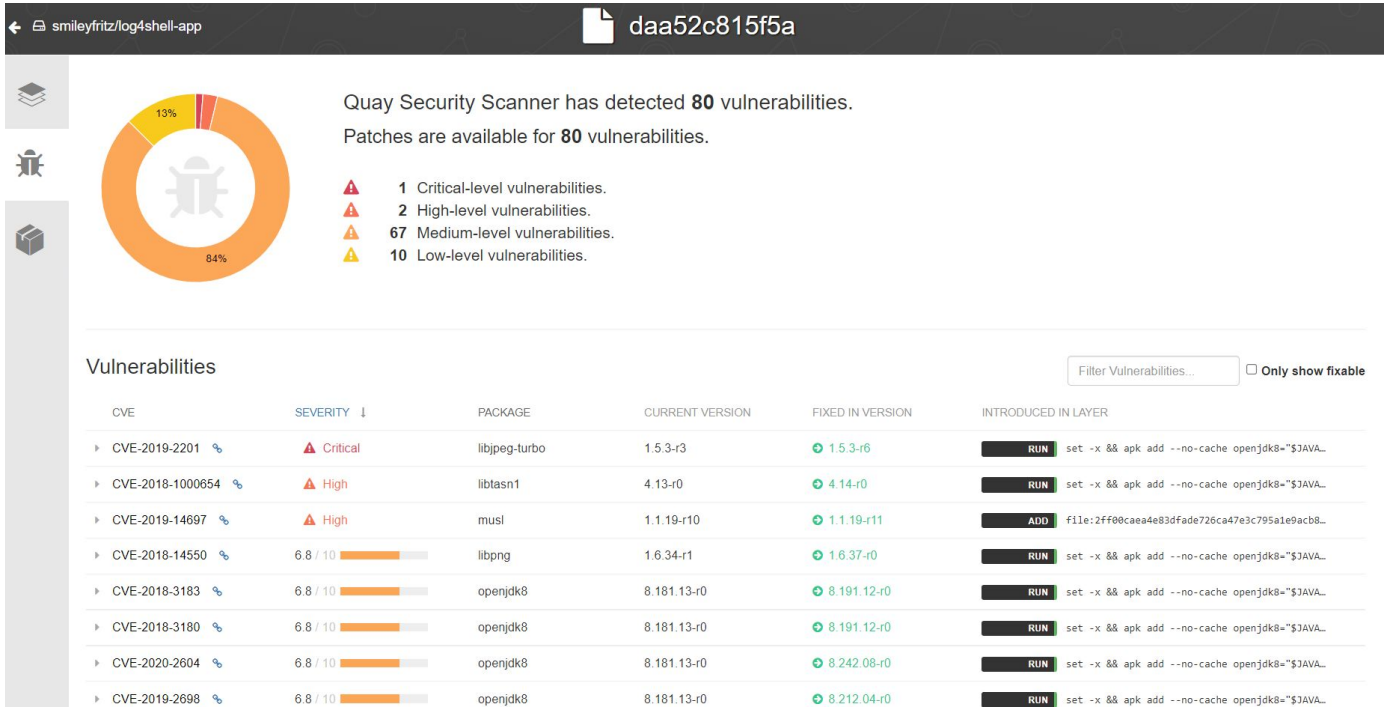
DevSecOps

1 New release is developed



2 Container image is created

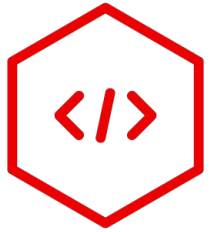
CVE scanning and container configuration analysis



Red Hat | intel

DevSecOps

1 New release is developed



2 Container image is created

3 Container image is stored in a registry

Container signatures and image provenance
Container signatures embedded in container image manifests

Role-based access controls

DevSecOps

1 New release is developed

2 Container image is created

3 Container image is stored in a registry

Deploy-time admission control
Containers must be scanned and pass security policy before being accepted to the container platform

Container signatures are validated, and unsigned deployments are not permitted

4 Container image is deployed to a cloud-native platform

Red Hat | intel

DevSecOps

Runtime security controls
Detecting processes running inside the container, and responding to indicators of compromise

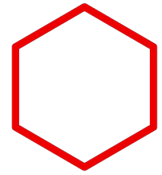
1 New release is developed

2 Container image is created

3 Container image is stored in a registry

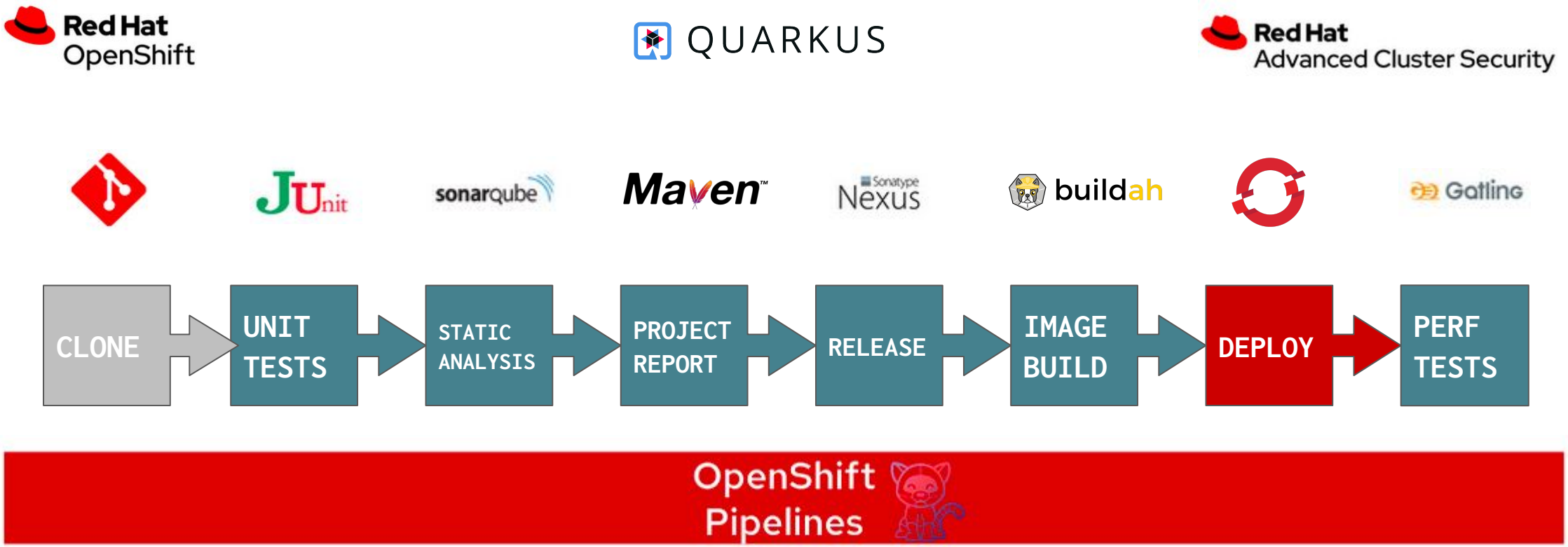
4 Container image is deployed to a cloud-native platform

5 Pod/container is running in production

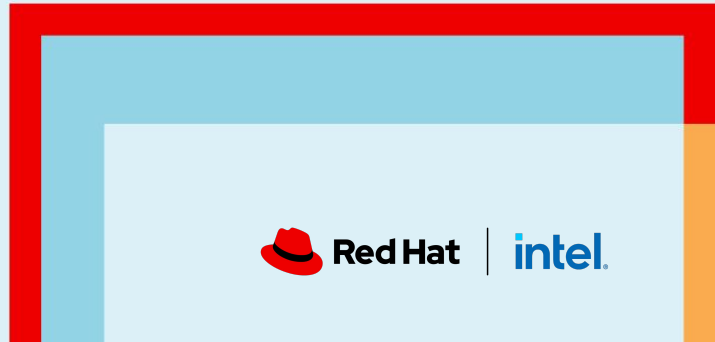


Red Hat | intel

DevSecOps Demo with ACS



Wrap up



Wrap up

- Continuous security that enables our organization to securely build, deploy and run cloud-native applications anywhere
- Gain comprehensive Kubernetes security by securing the supply chain, infrastructure and workloads.
- Reduce operational risk and increase developer productivity by using kubernetes native solutions.
- Control, protect, detect and respond with continuous security for containers and Kubernetes.
- Security across the entire application lifecycle.

Resources

Red Hat | intel.

Red Hat Advanced Cluster Security Resources

- Red Hat Advanced Cluster Security for Kubernetes product documentation.
- Red Hat Advanced Cluster Security Workshop.
- Red Hat Advanced Cluster Security GitHub repositories.

Red Hat Summit

Connect

Thank you

 linkedin.com/company/red-hat

 facebook.com/redhatinc

 youtube.com/user/RedHatVideos

 twitter.com/RedHat

Red Hat | intel