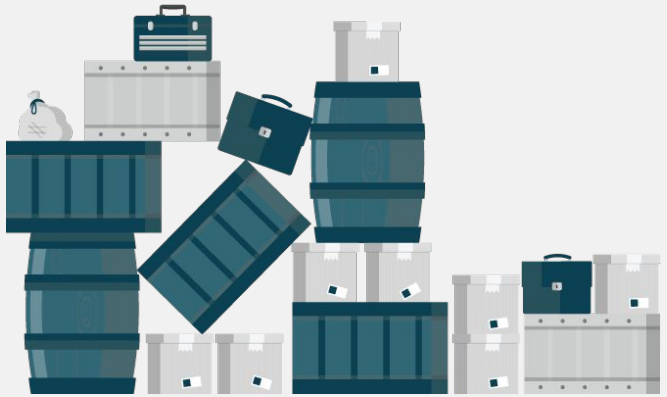
redhat.

Continuous Change and IT Security

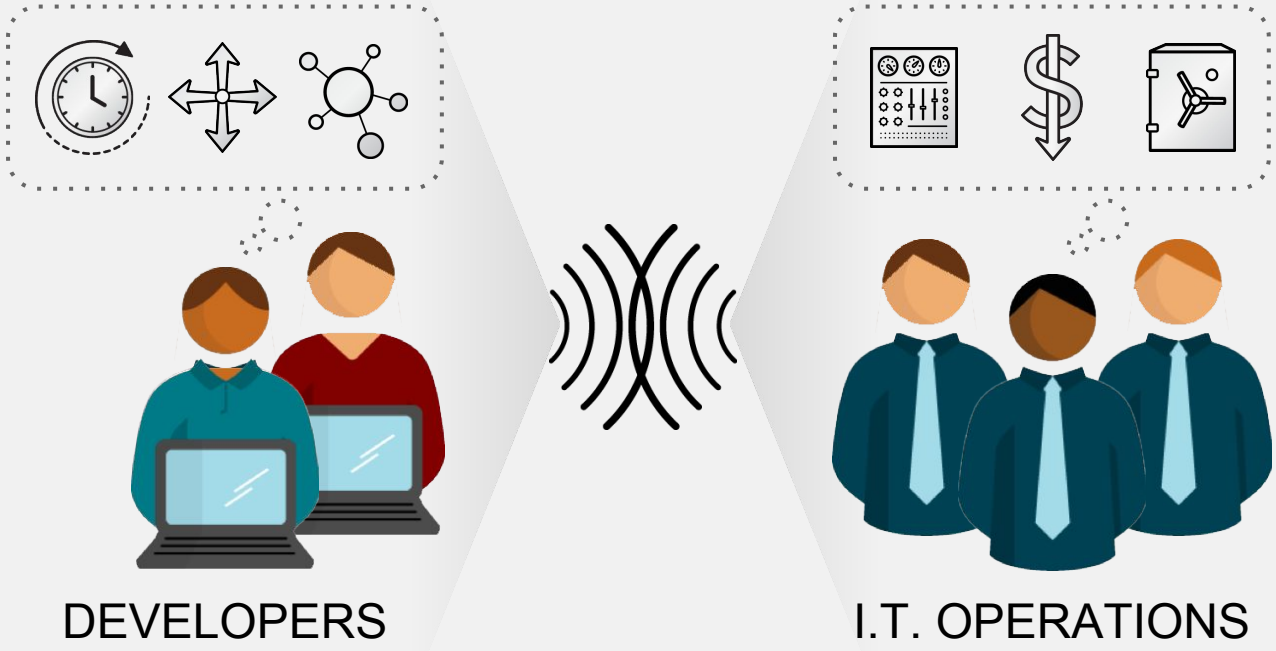
Shawn Wells
Chief Security Strategist
U.S. Public Sector
shawn@redhat.com || 443-534-0130

The Problem

Applications require complicated installation and integration every time they are deployed



THE PROBLEM



DEVOPS

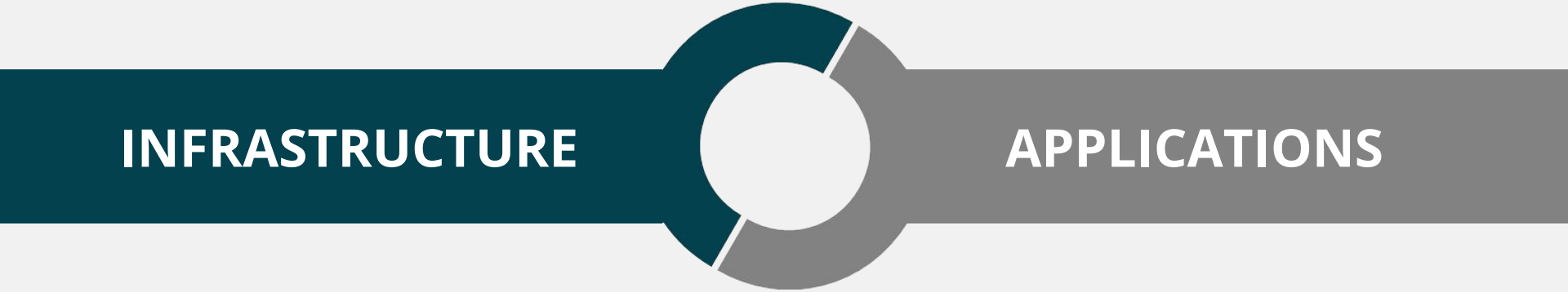
Everything as code	Application monitoring
Automate everything	Rapid feedback
Continuous Integration/Delivery	Rebuild vs. Repair
Application is always “releaseable”	Delivery pipeline

A Solution

Adopting a container strategy will allow applications to be easily shared and deployed.

WHAT ARE CONTAINERS?

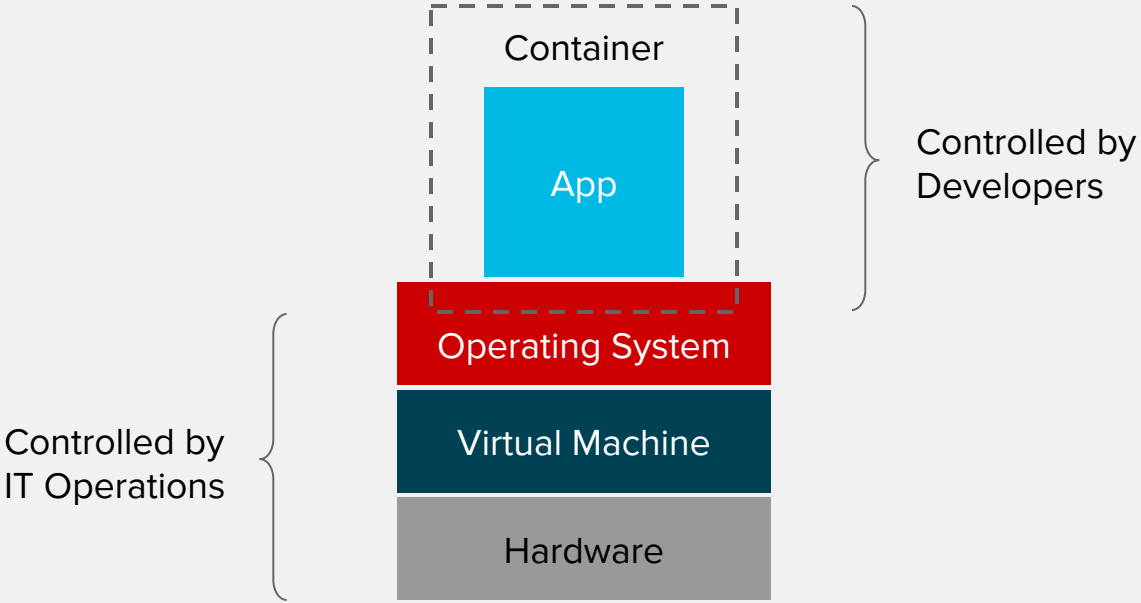
It Depends Who You Ask



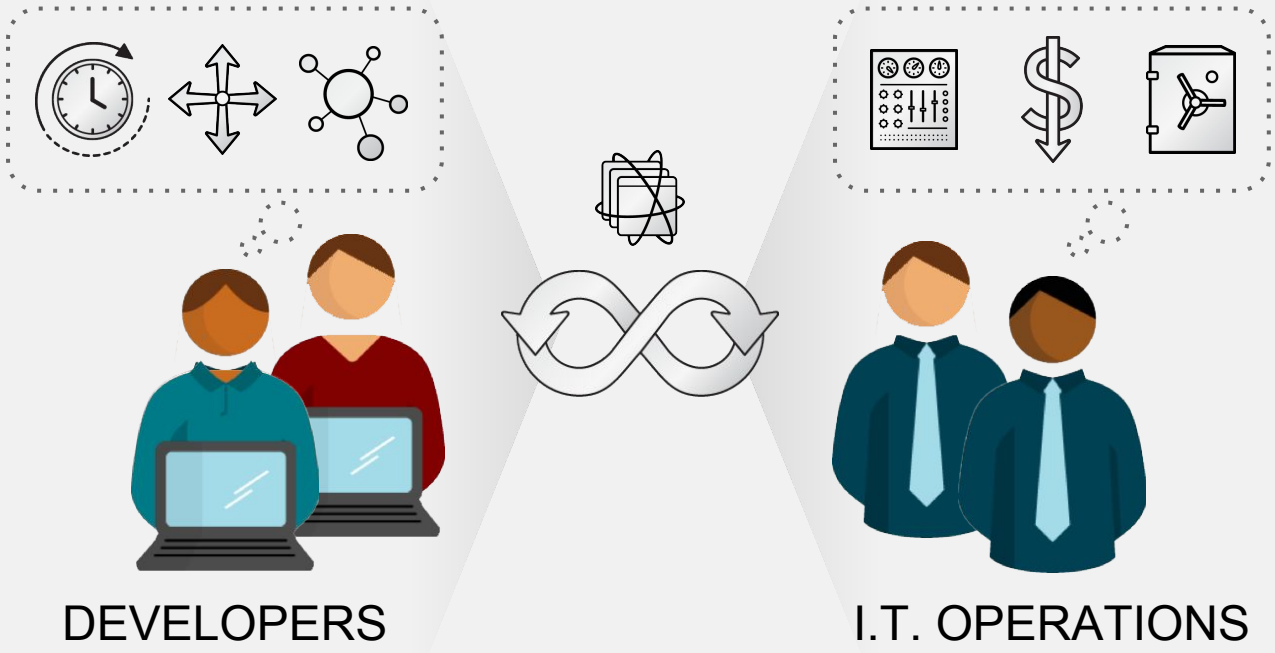
- Sandboxed application processes on a shared Linux OS kernel
- Simpler, lighter, and denser than virtual machines
- Portable across different environments

- Package my application and all of its dependencies
- Deploy to any environment in seconds and enable CI/CD
- Easily access and share containerized components

A SOLUTION

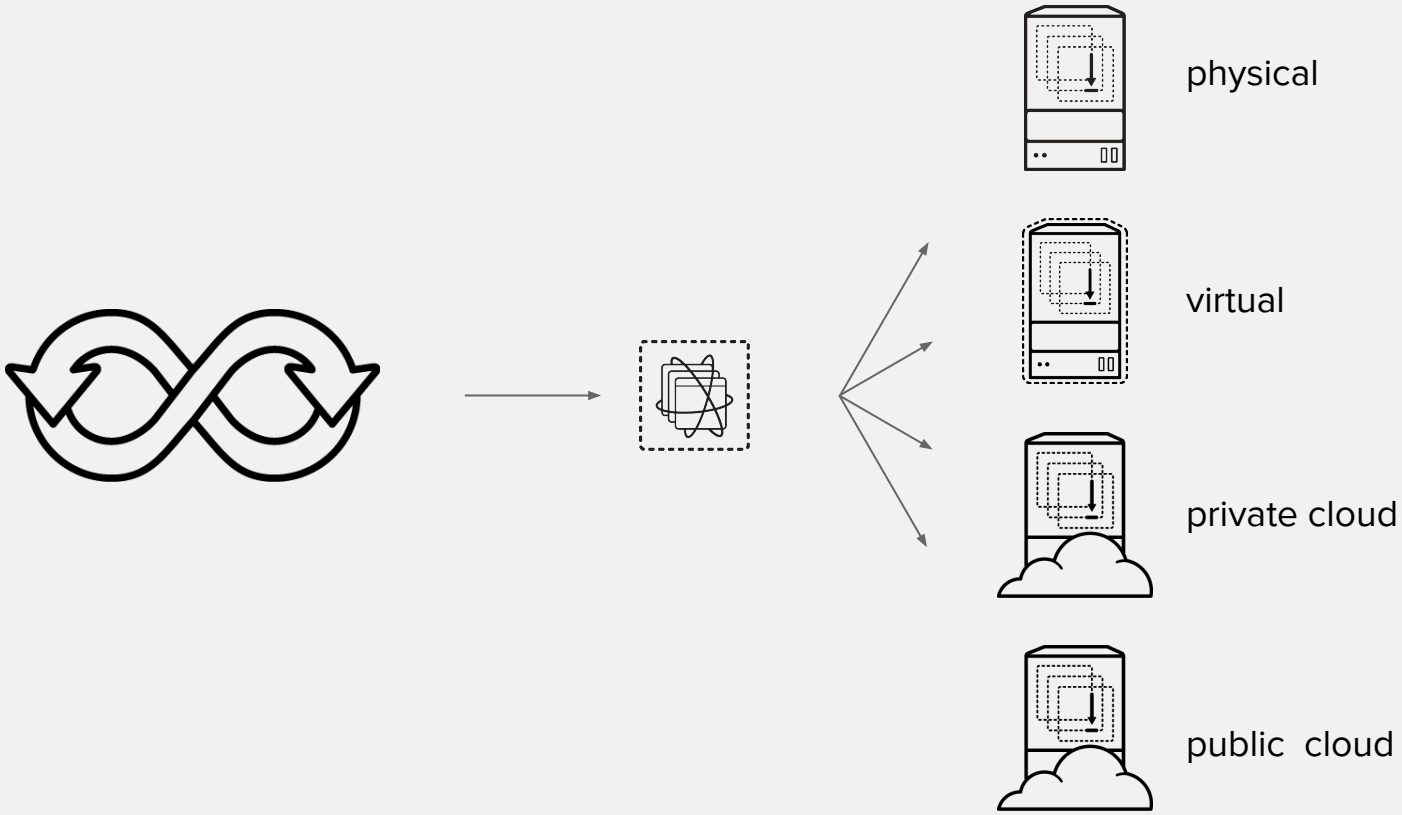


A SOLUTION

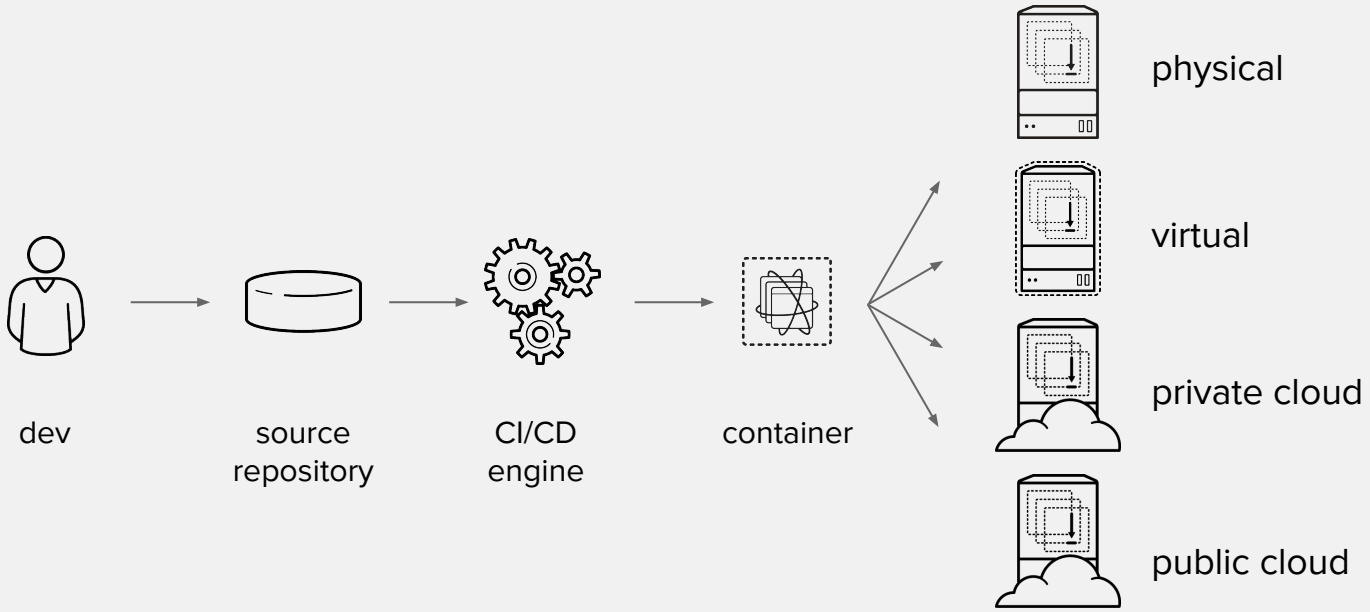


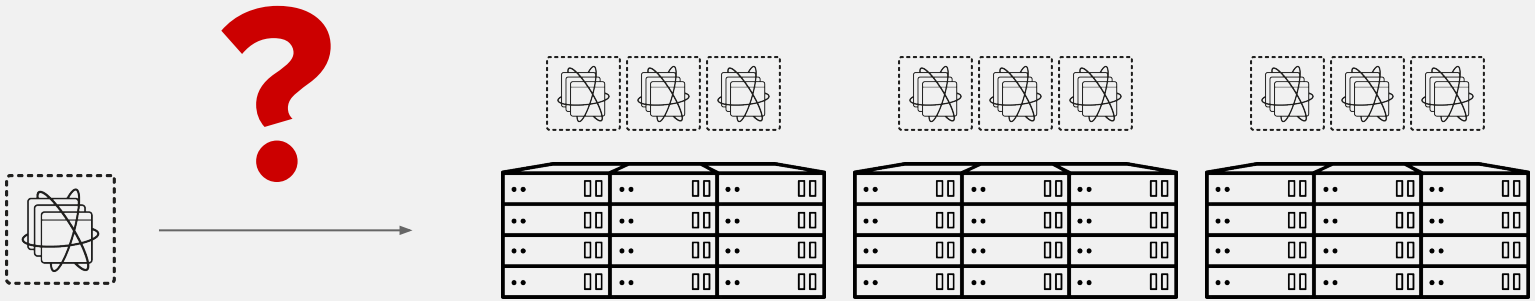
```
$ docker build -t app:v1 .
```

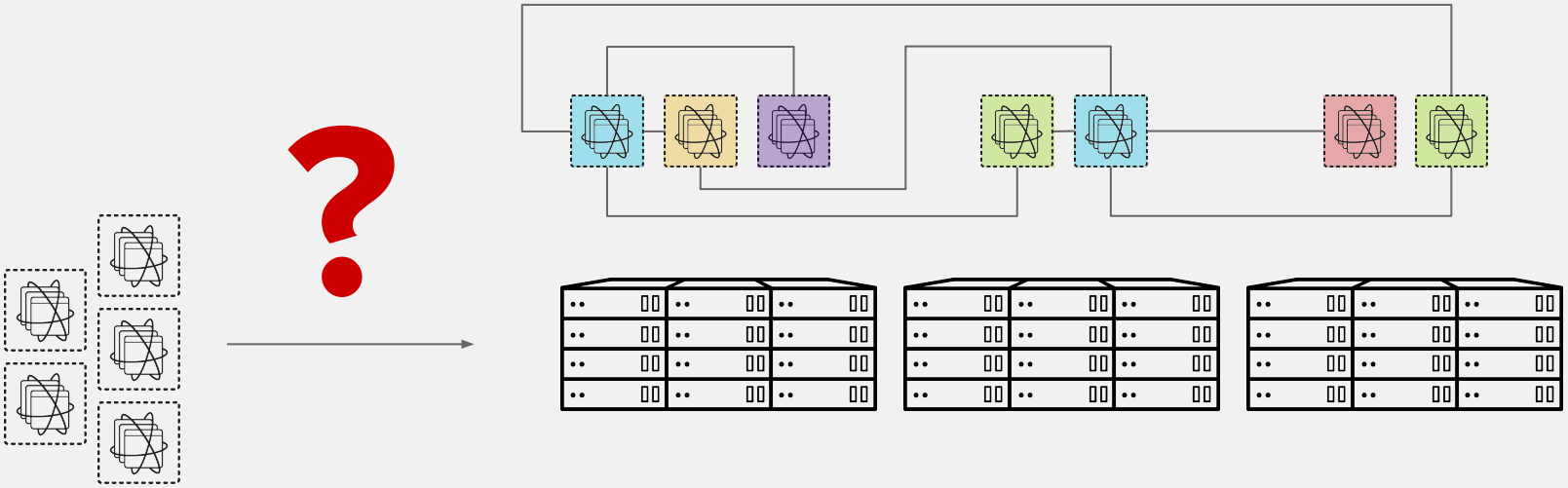
```
$ docker build -t app:v1 .

$ docker run app:v1
```



DEVOPS WITH CONTAINERS







WE NEED MORE THAN JUST CONTAINERS

Scheduling
Decide where to deploy containers

Security
Control who can do what

Lifecycle and health
Keep containers running despite failures

Scaling
Scale containers up and down

Discovery
Find other containers on the network

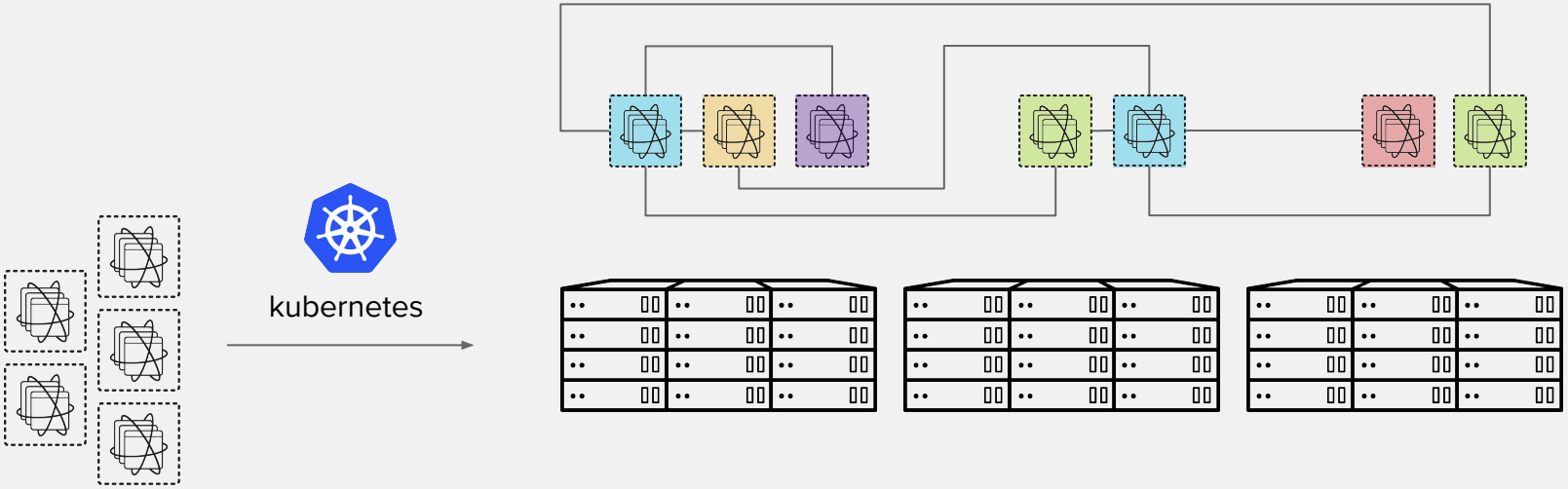
Persistence
Survive data beyond container lifecycle

Monitoring
Visibility into running containers

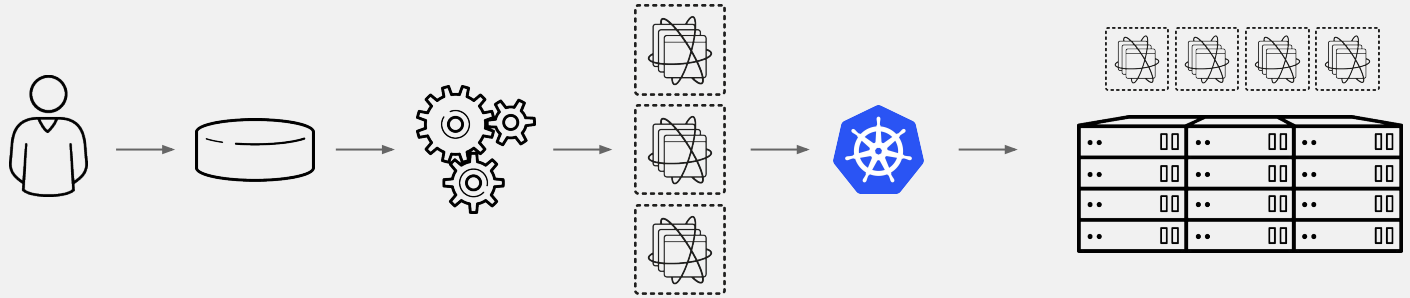
Aggregation
Compose apps from multiple containers

Kubernetes is an open-source system for automating deployment, operations, and scaling of containerized applications across multiple hosts

kubernetes



DEVOPS WITH CONTAINERS AND KUBERNETES



INDUSTRY CONVERGING ON KUBERNETES

INDUSTRY CONVERGING ON KUBERNETES

CSRA Achieves Highest Cloud Services Security Accreditation

Home > Media Room > Multimedia Library > CSRA Achieves Highest Cloud Services Security Accreditation

June 23, 2016

RELATED

Digital Platforms / Digital Services / Amazon Web Services / Microsoft / FedRAMP FISMA High Baseline Accreditation

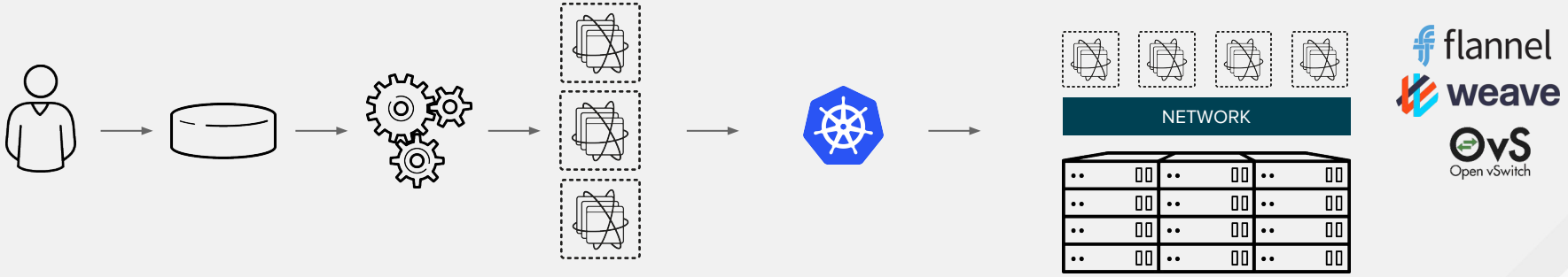
COLLECTIONS

Cloud
Integrated Technology Center

CSRA, Amazon Web Services and Microsoft Azure Earn FedRAMP FISMA High Baseline Authority to Operate

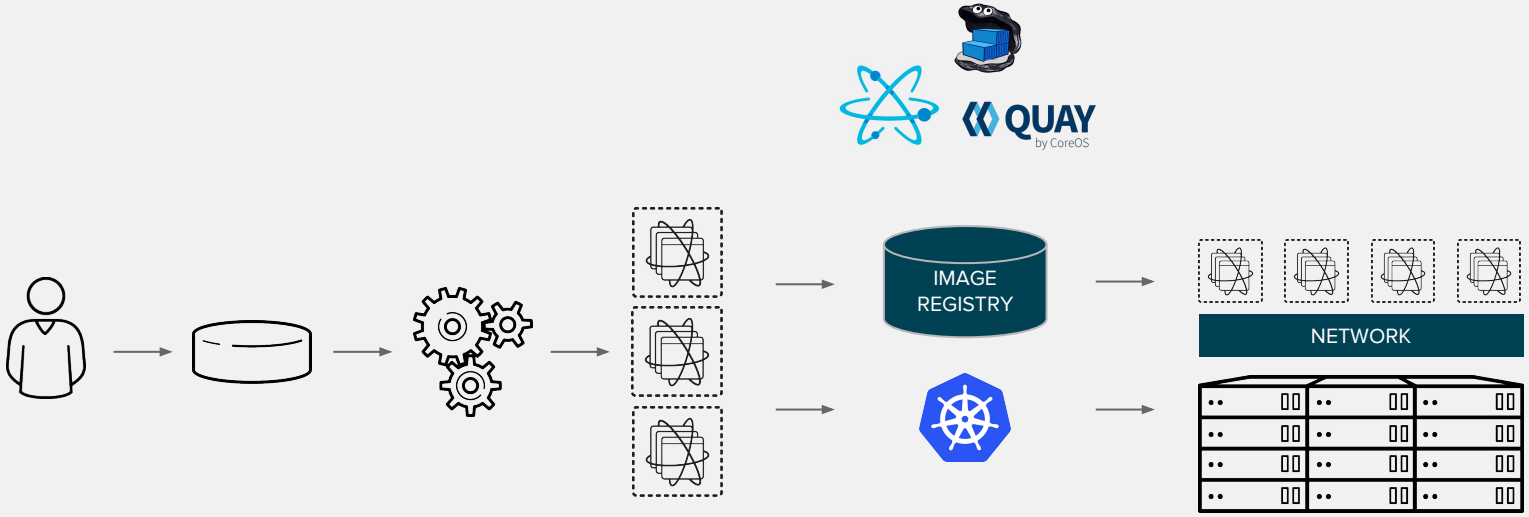
Falls Church, Va., June 23, 2016 – CSRA Inc. (NYSE:CSRA), a leading provider of next-generation IT solutions and professional services to government organizations, today announced its operating subsidiary, CSRA LLC (formerly CSC Government Solutions LLC), is one of three cloud service providers, including Amazon Web Services and Microsoft Azure to meet rigorous security standards and achieve a Federal Risk Authorization Management Program (FedRAMP) Federal Information Security Management (FISMA) High Baseline accreditation.

DEVOPS WITH CONTAINERS AND KUBERNETES



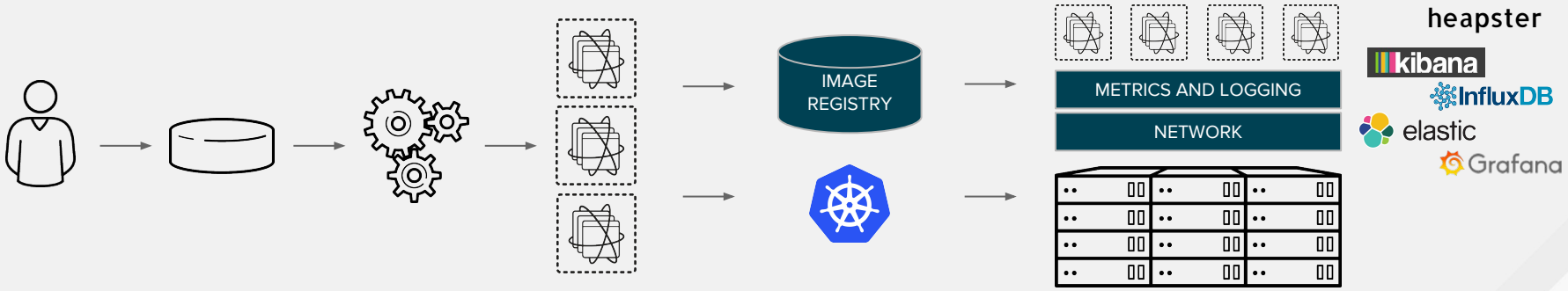
Not enough! Need networking

DEVOPS WITH CONTAINERS AND KUBERNETES



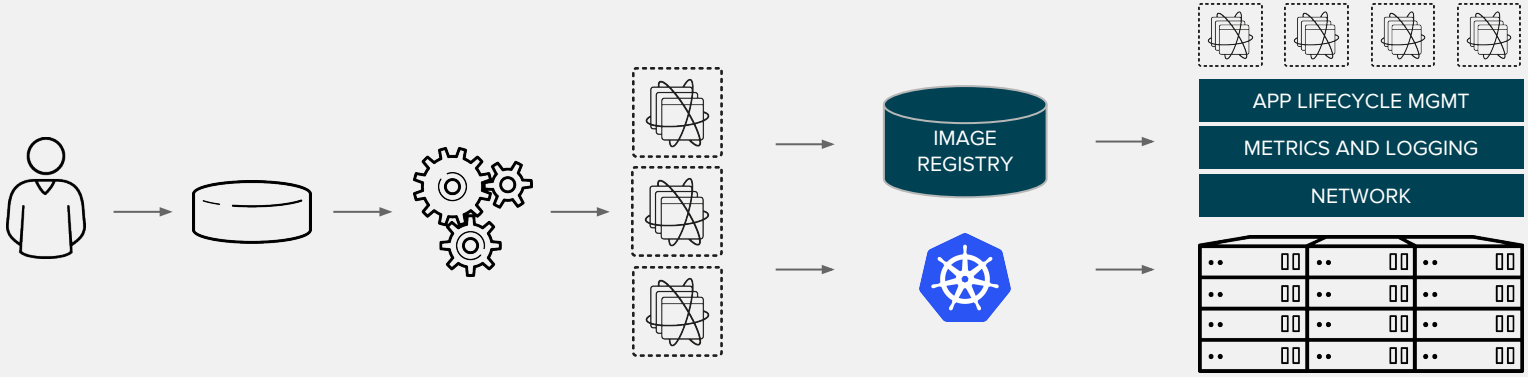
Not enough! Need an image registry

DEVOPS WITH CONTAINERS AND KUBERNETES



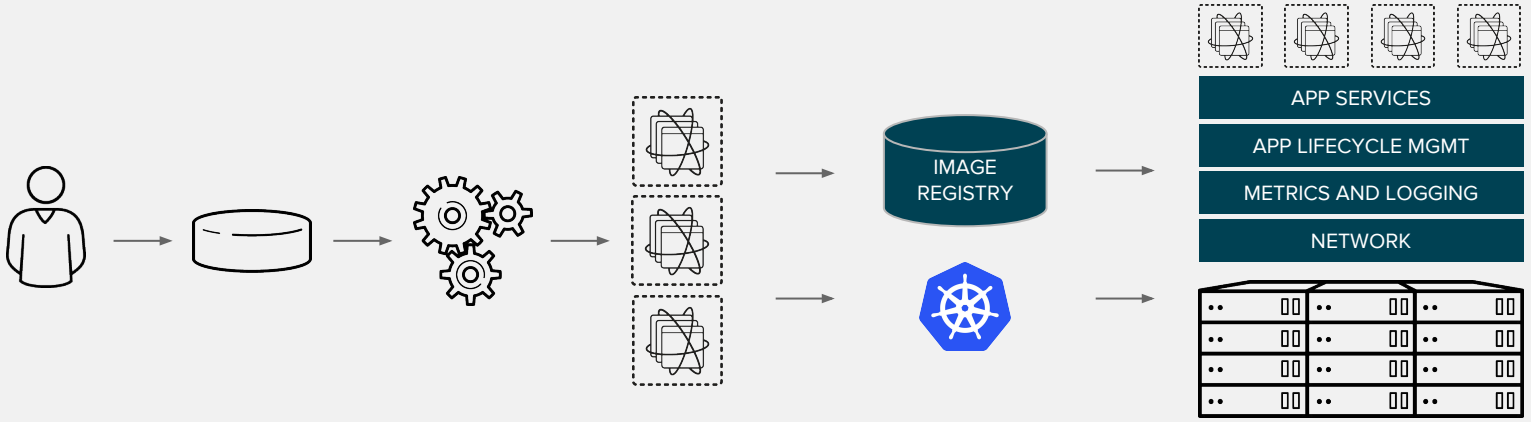
Not enough! Need metrics and logging

DEVOPS WITH CONTAINERS AND KUBERNETES



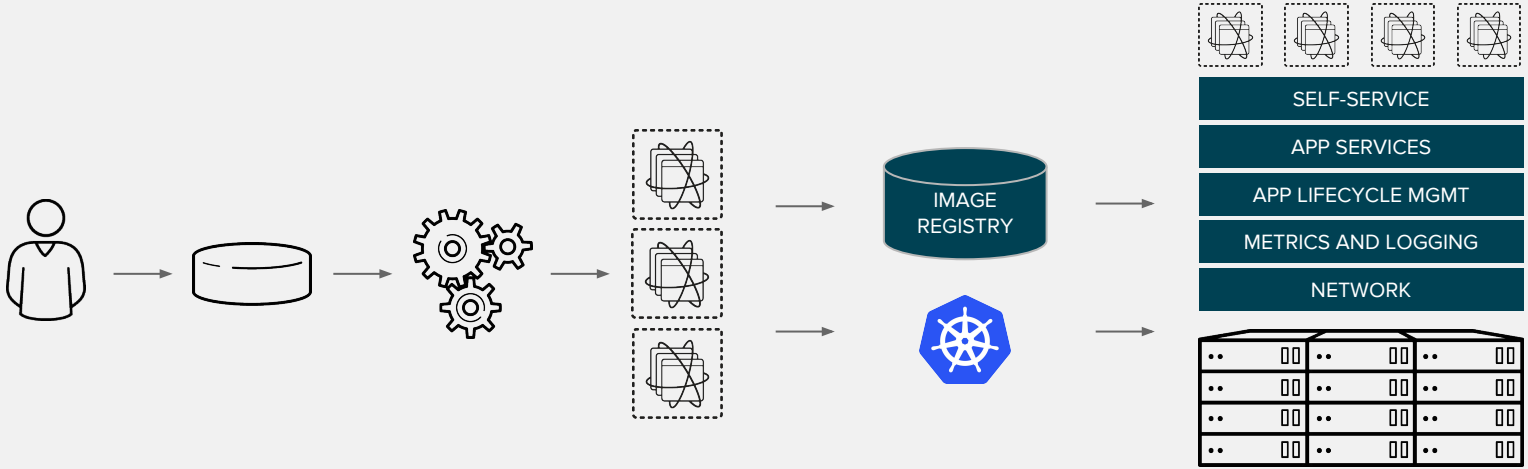
Not enough! Need application lifecycle management

DEVOPS WITH CONTAINERS AND KUBERNETES



Not enough! Need application services e.g. database and messaging

DEVOPS WITH CONTAINERS AND KUBERNETES



Not enough! Need self-service portal

NOT ENOUGH, THERE IS MORE!

Multi-tenancy	Teams and Collaboration
Routing & Load Balancing	Quota Management
CI/CD Pipelines	Image Build Automation
Role-based Authorization	Container Isolation
Capacity Management	Vulnerability Scanning
Infrastructure Visibility	Chargeback

Container application platform based on Docker and Kubernetes for building, distributing and running containers at scale

OpenShift for Government Accreditations & Standards

OCTOBER 2016

RHEL7 COMMON CRITERIA
- EAL4+
- Container Framework
- Secure Multi-tenancy

DECEMBER 2016

RHEL7 FIPS 140-2 CERTIFIED
- Data at Rest
- Data in Transport

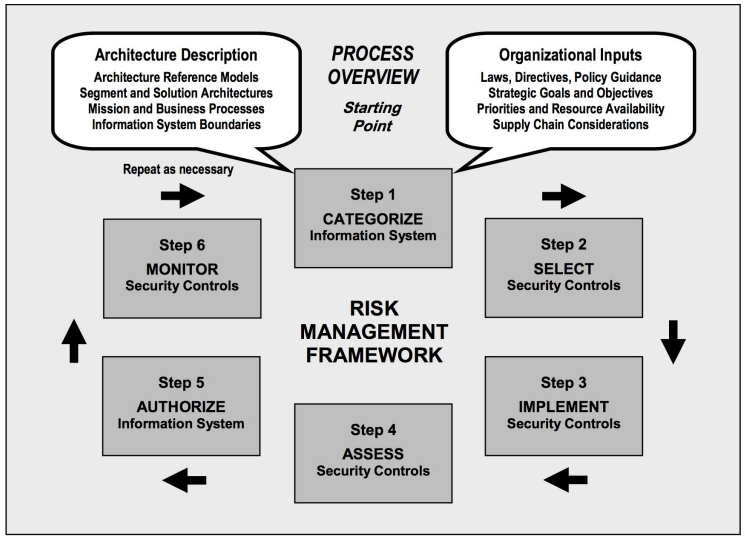
MARCH 2017

INDUSTRY FIRST: NIST CERTIFIED CONFIGURATION AND VULNERABILITY SCANNER FOR CONTAINER

JUNE 2017

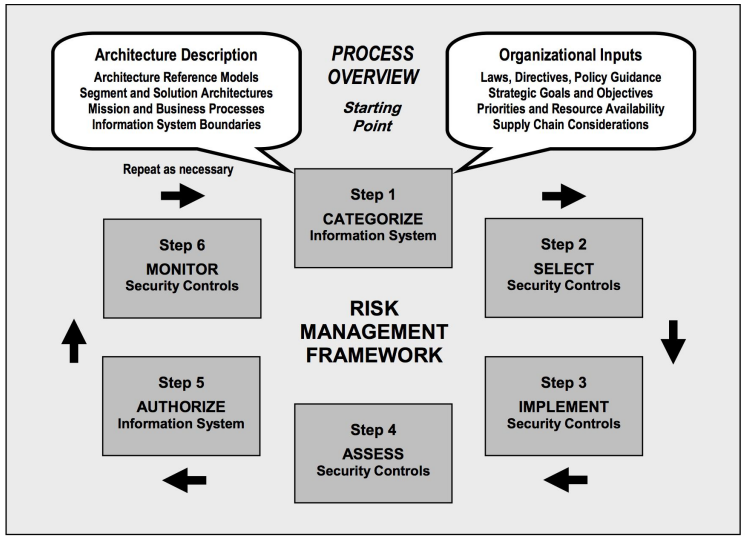
OPENSHIFT BLUEPRINT FOR AZURE
(FedRAMP MODERATE)

Meanwhile, in Government: FISMA from an earlier era



- Written in 2003-2004
- Pre GovCloud, C2S, MilCloud
- Pre DevOps, Infrastructure as Code
- Multi-year dev/ship cycles common
- Waterfall dominant
- IT was more manual a decade ago

Meanwhile, in Government: FISMA from an earlier era



Telos®

Xacta®, featuring the AWS Enterprise Accelerator for Compliance

AWS and Telos® – Accelerating secure and compliant cloud deployments.

The Business Case for Xacta featuring the AWS Enterprise Accelerator for Compliance

The key to AWS and Xacta saving you time and effort is the ability to inherit common security controls and automate key compliance processes. According to an analysis conducted by Telos:

- The estimated effort for a typical deployment of the NIST Risk Management Framework for a small system is 2,546 labor hours over a six-month period.
- Applying Xacta featuring the AWS Enterprise Accelerator for Compliance would reduce the effort to a conservative estimate of 2,062 hours over 3-4 months, with the potential for additional timeline compression as the organization matures.

https://www.telos.com/assets/Telos-AWS-white-paper.pdf

18F's Project Boise

https://boise.18f.gov

- No lingua franca
- Workflows are localized, proprietary
- Automating ATOs is a huge, vague goal
- Continuous Monitoring portends a growing compliance burden
- Compliance prompts collaboration

OpenSCAP

Community created *portfolio* of tools and content to assess systems for known vulnerabilities.

Project: https://open-scap.org
Code: https://github.com/OpenSCAP

National Security Agency

NSAgov

Follow

Block or report user

Overview | Repositories 0 | Stars 8

Popular repositories

apache/nifi

Mirror of Apache NiFi

Java ★ 461 ⑂ 429

OpenSCAP/scap-security-guide

Baseline compliance content in SCAP formats

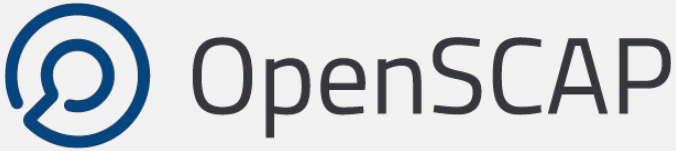
XSLT ★ 227 ⑂ 120

OpenAttestation/OpenAttestation

Software Development Kit to enable remotely retrieval and verify target platforms integrity

Java ★ 65 ⑂ 43

https://github.com/nsagov



RHEL7 STIG content, rebased in RHEL 7.3:

- 6,180 commits from 95 people
- 441,055 lines of code

OpenSCAP interpreter contains:

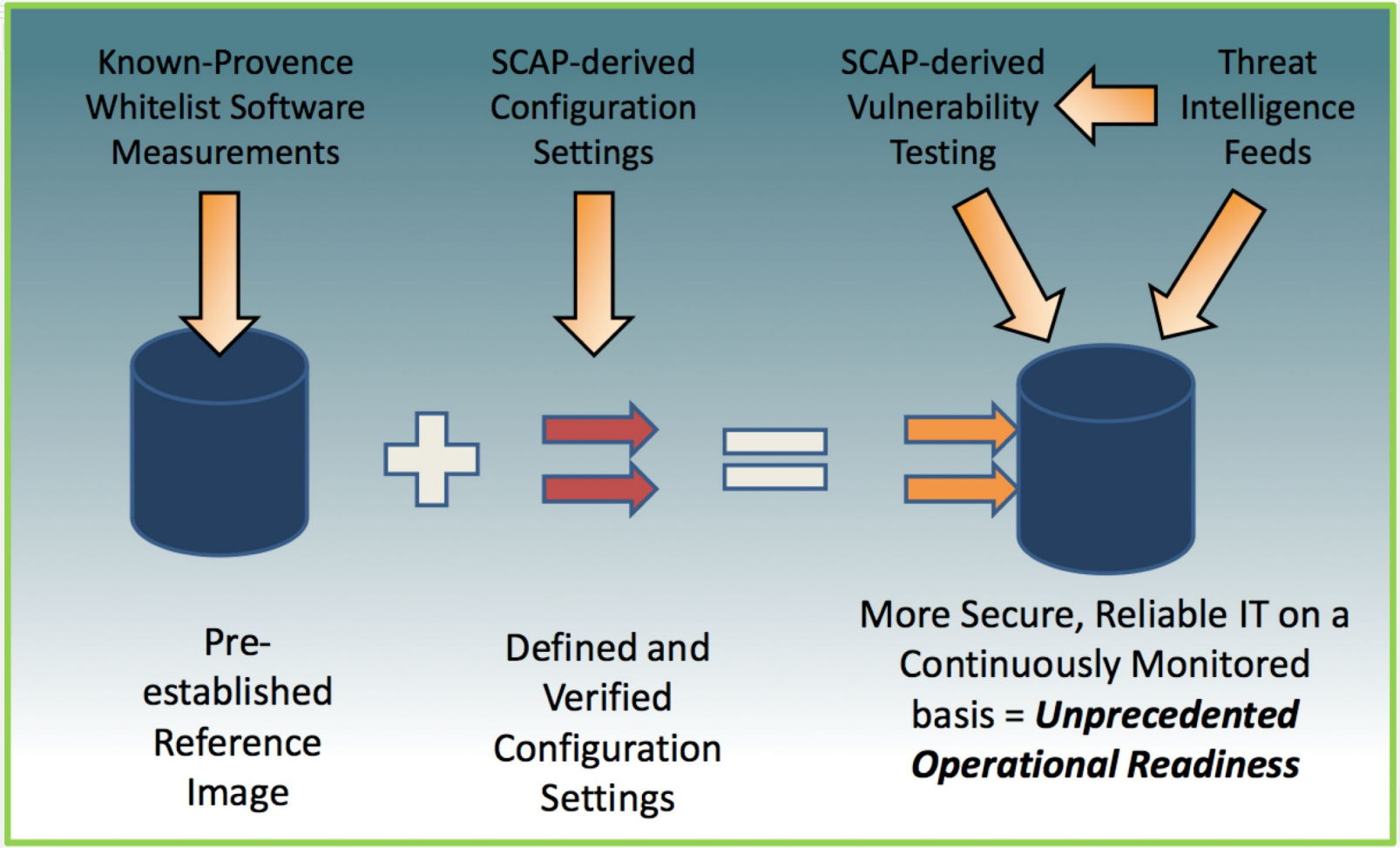
- 6,811 commits from 74 people
- 157,775 lines of code

“Security Button” RHEL7 Installer:

- 6 people, 90 days

Shipping in RHEL 7:

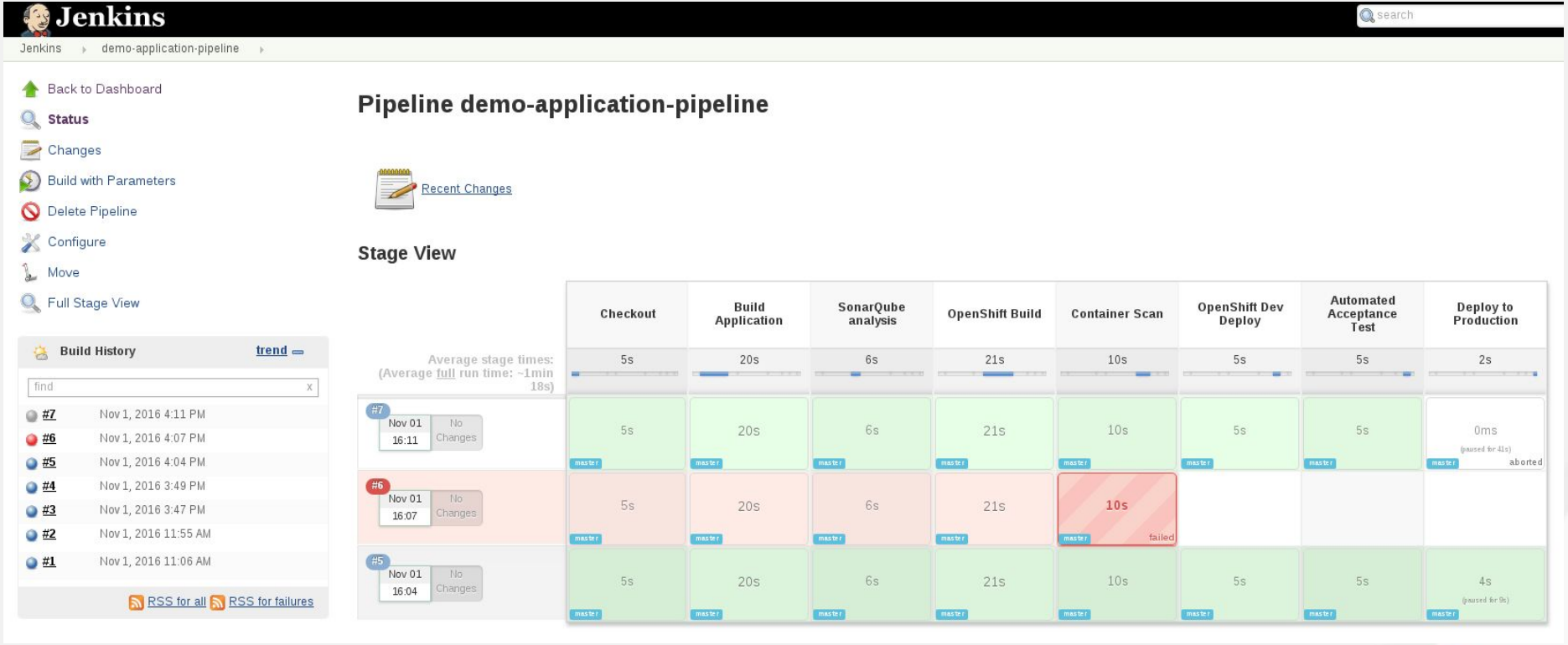
- **Intelligence Community:** C2S and CS2
- **DoD:** RHEL7 Vendor STIG
- **Civilian:** USGCB/OSPP
- **Justice:** FBI Criminal Justice Info. Systems (FBI CJIS)


Known-Provence Whitelist Software Measurements
SCAP-derived Configuration Settings
SCAP-derived Vulnerability Testing
Threat Intelligence Feeds
Pre-established Reference Image
Defined and Verified Configuration Settings
More Secure, Reliable IT on a Continuously Monitored basis = Unprecedented Operational Readiness

Atomic Scan

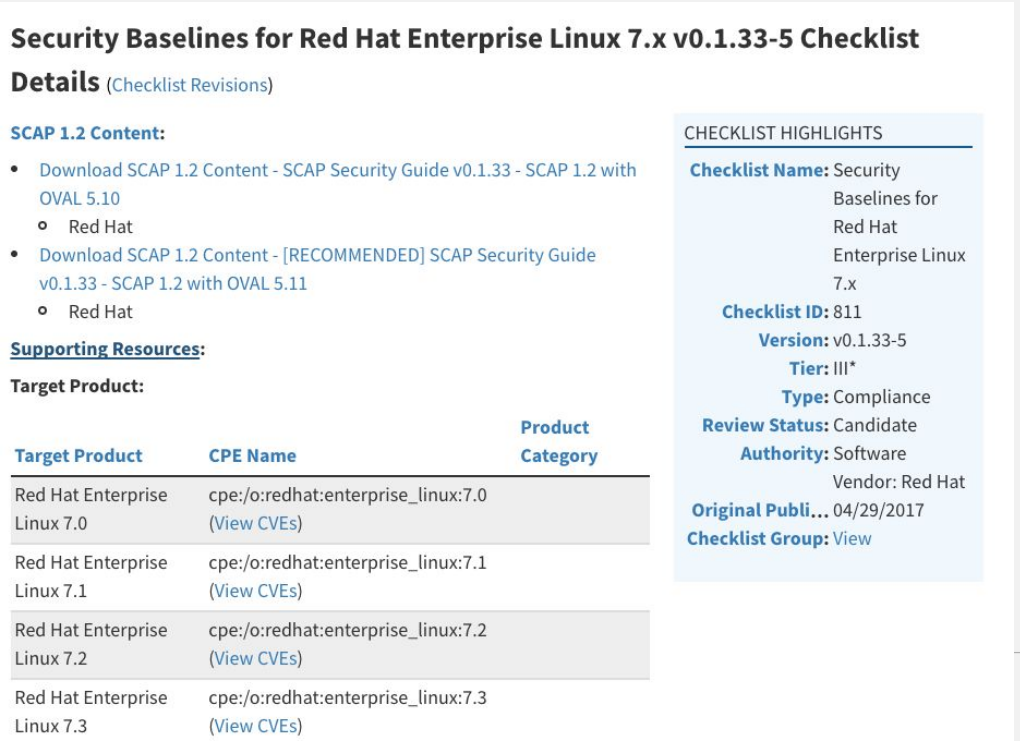
Enables multiple container scanners

Example Pipeline



NIST National Checklist Program

https://nvd.nist.gov/ncp/repository



Security Baselines for Red Hat Enterprise Linux 7.x v0.1.33-5 Checklist

Details (Checklist Revisions)

SCAP 1.2 Content:

- Download SCAP 1.2 Content - SCAP Security Guide v0.1.33 - SCAP 1.2 with OVAL 5.10
  - Red Hat
- Download SCAP 1.2 Content - [RECOMMENDED] SCAP Security Guide v0.1.33 - SCAP 1.2 with OVAL 5.11
  - Red Hat

Supporting Resources:

Target Product:

Target Product	CPE Name	Product Category
Red Hat Enterprise Linux 7.0	cpe:/o:redhat:enterprise_linux:7.0 (View CVEs)	
Red Hat Enterprise Linux 7.1	cpe:/o:redhat:enterprise_linux:7.1 (View CVEs)	
Red Hat Enterprise Linux 7.2	cpe:/o:redhat:enterprise_linux:7.2 (View CVEs)	
Red Hat Enterprise Linux 7.3	cpe:/o:redhat:enterprise_linux:7.3 (View CVEs)	

CHECKLIST HIGHLIGHTS

Checklist Name: Security Baselines for Red Hat Enterprise Linux 7.x
Checklist ID: 811
Version: v0.1.33-5
Tier: III*
Type: Compliance
Review Status: Candidate
Authority: Software Vendor: Red Hat
Original Publi... 04/29/2017
Checklist Group: View

"U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications."

redhat.

Contact Info

EMail: shawn@redhat.com

LinkedIn: https://www.linkedin.com/in/shawndwells/

Cell: 443-534-0130 (US EST)

OpenSCAP Slides + Videos:
https://github.com/OpenSCAP/scap-security-guide/wiki/Collateral-and-References

OpenShift Ansible Scripts: https://github.com/redhatdemocentral/ocp-install-demo