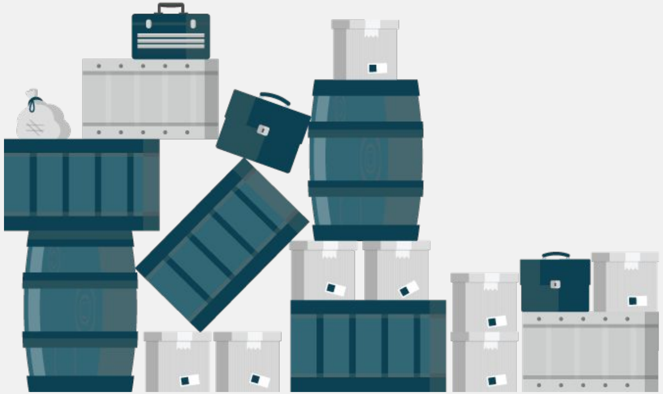
CONTINUOUS MONITORING OF CONTAINERS

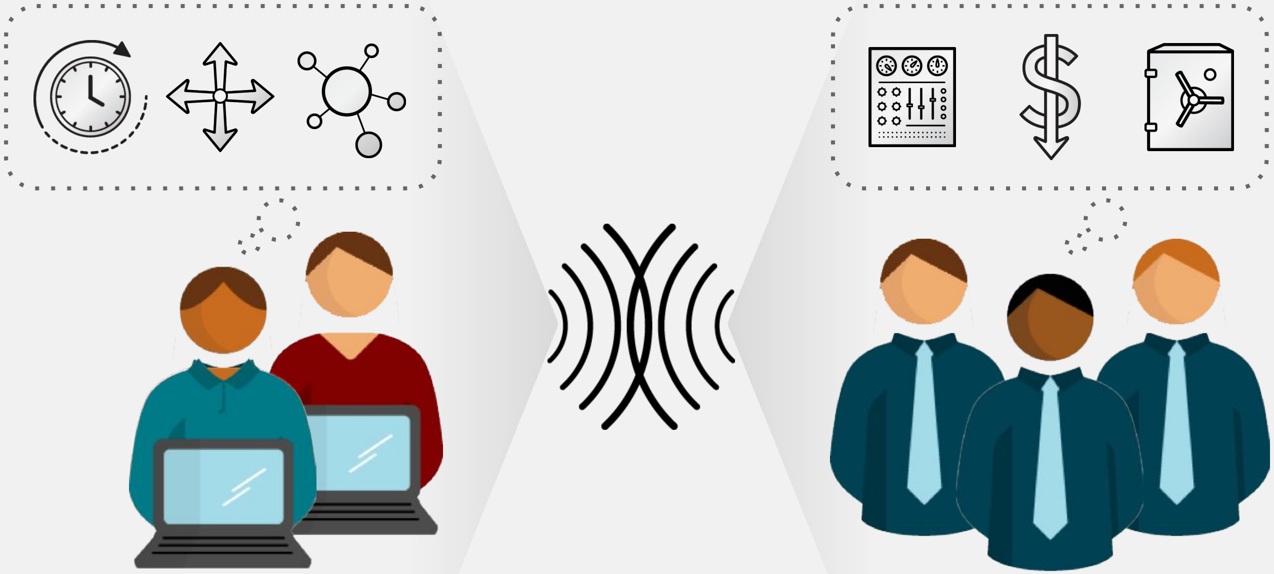
Shawn Wells
Chief Security Strategist
U.S. Public Sector
shawn@redhat.com || 443-534-0130

The Problem

Applications require complicated installation and integration every time they are deployed



THE PROBLEM



DEVELOPERS

I.T. OPERATIONS

DEVOPS

- Everything as code
- Automate everything
- Continuous Integration/Delivery
- Application is always “releaseable”

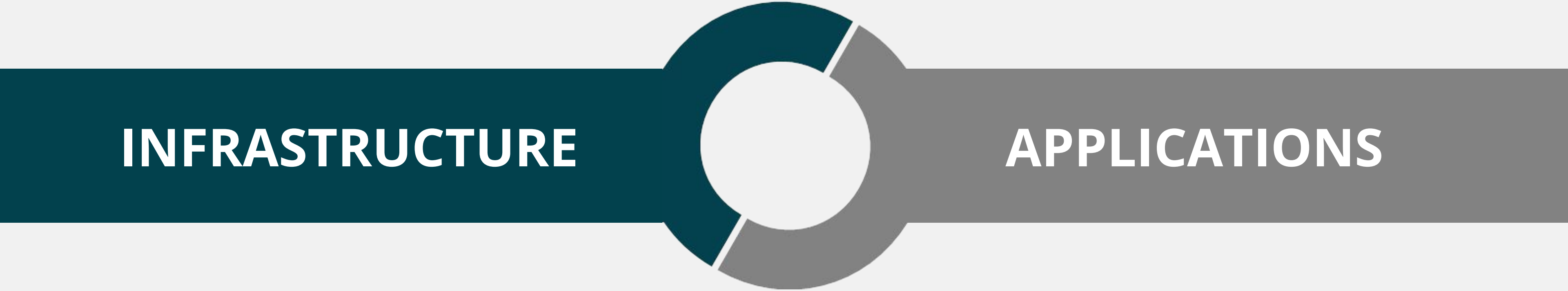
- Application monitoring
- Rapid feedback
- Rebuild vs. Repair
- Delivery pipeline

A Solution

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

WHAT ARE CONTAINERS?

It Depends Who You Ask



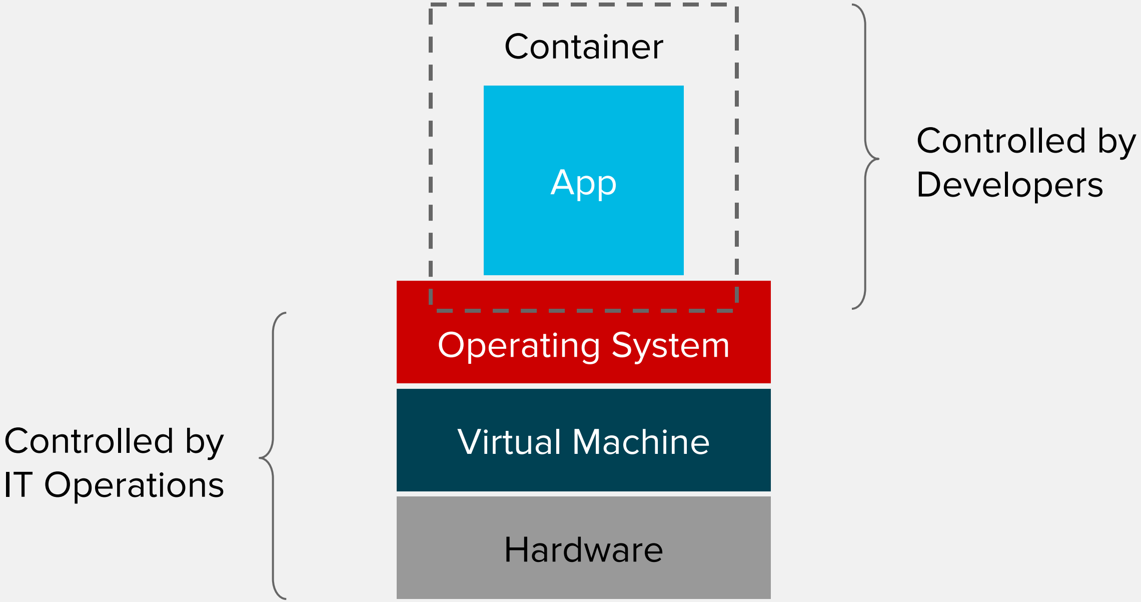
INFRASTRUCTURE

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

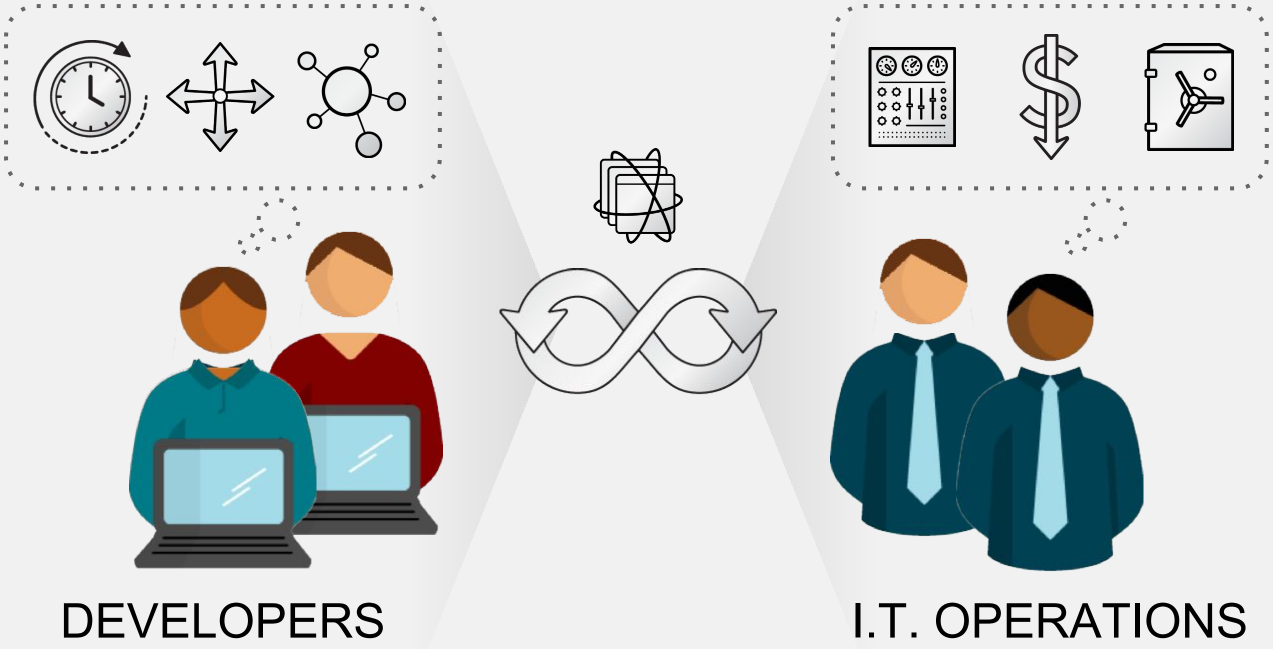
APPLICATIONS

- 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

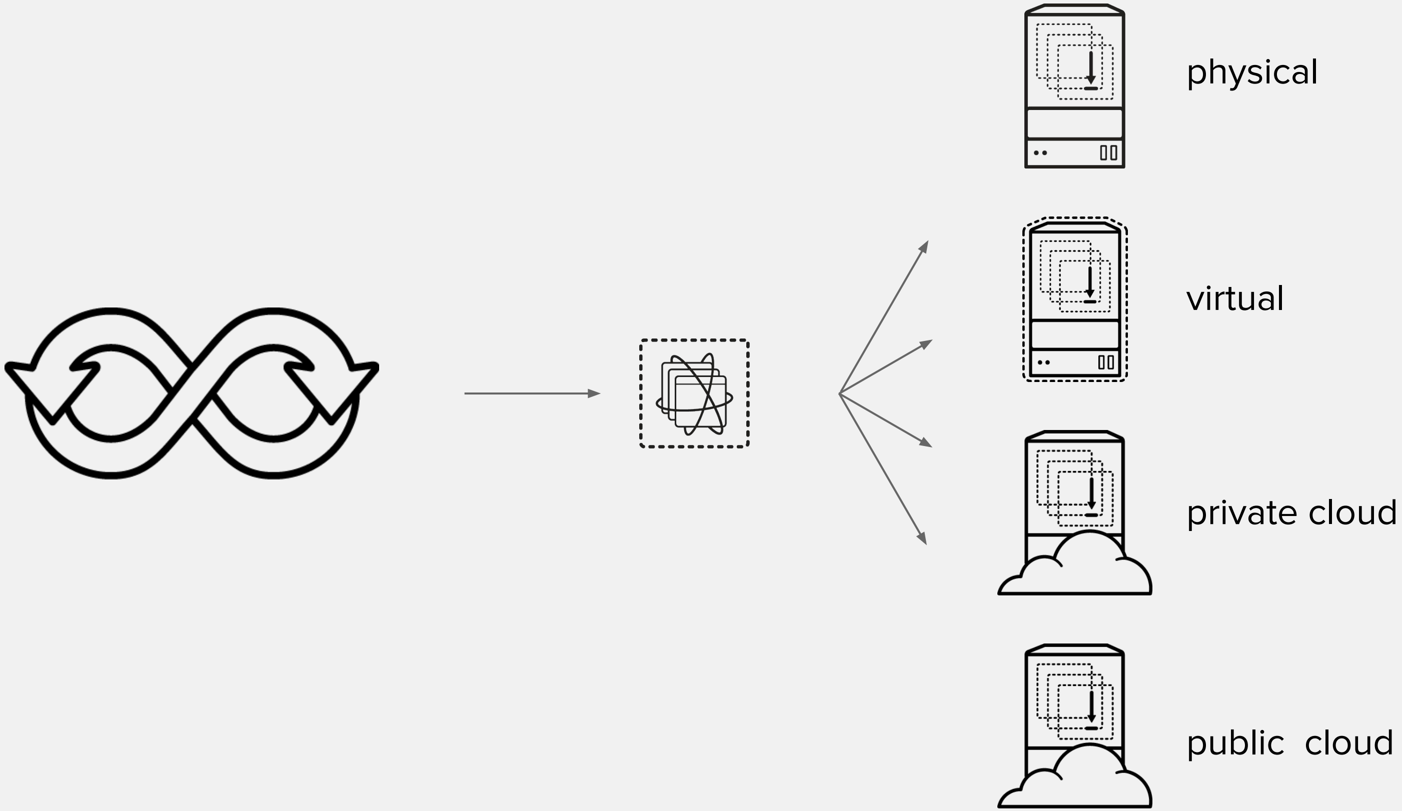

Container
App
Operating System
Virtual Machine
Hardware
Controlled by Developers
Controlled by IT Operations

A SOLUTION



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

$ docker run app:v1
```



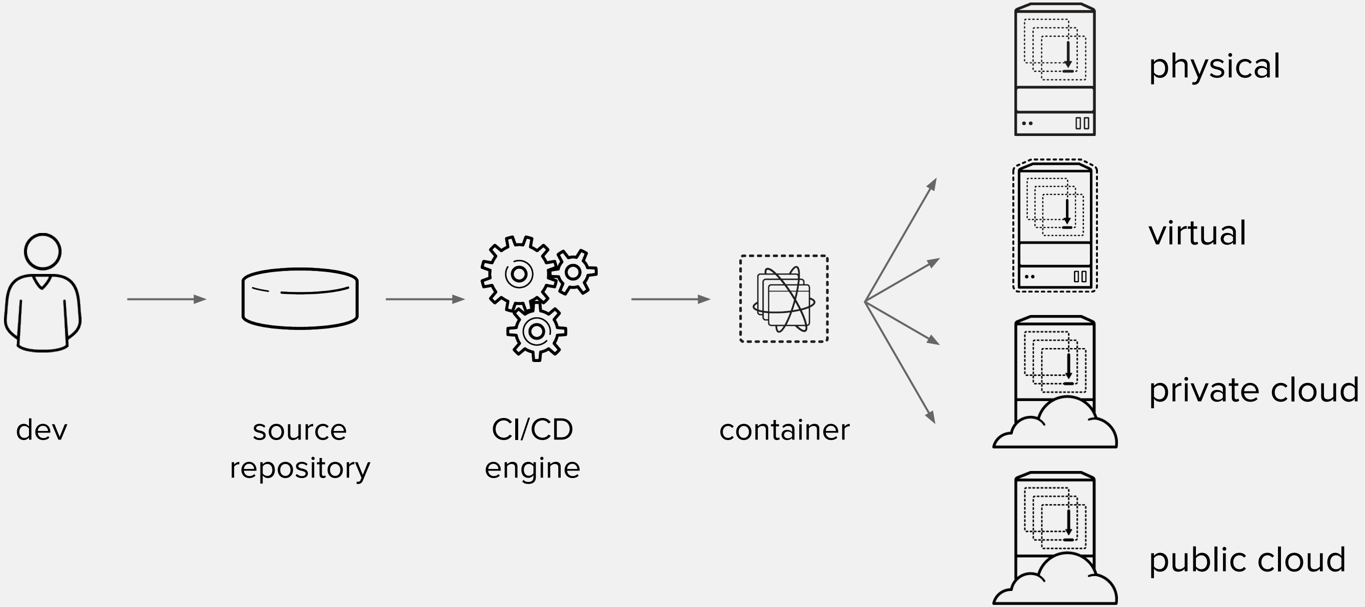
physical

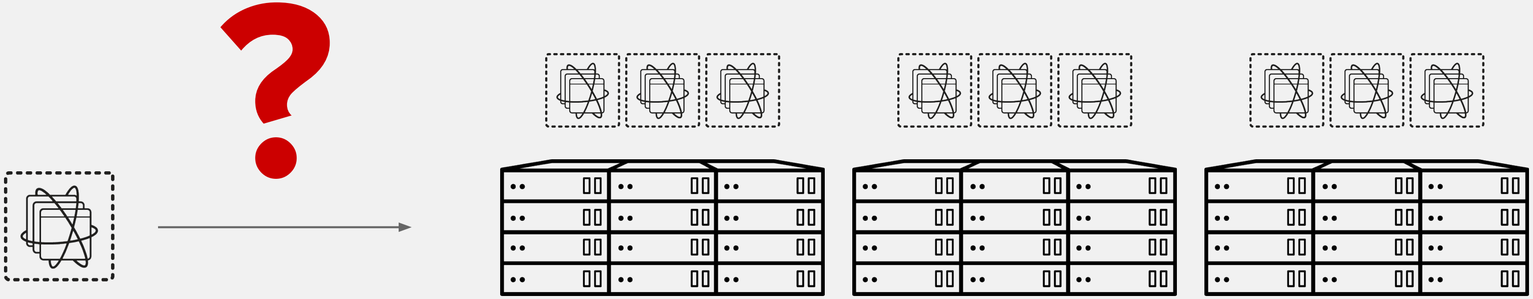
virtual

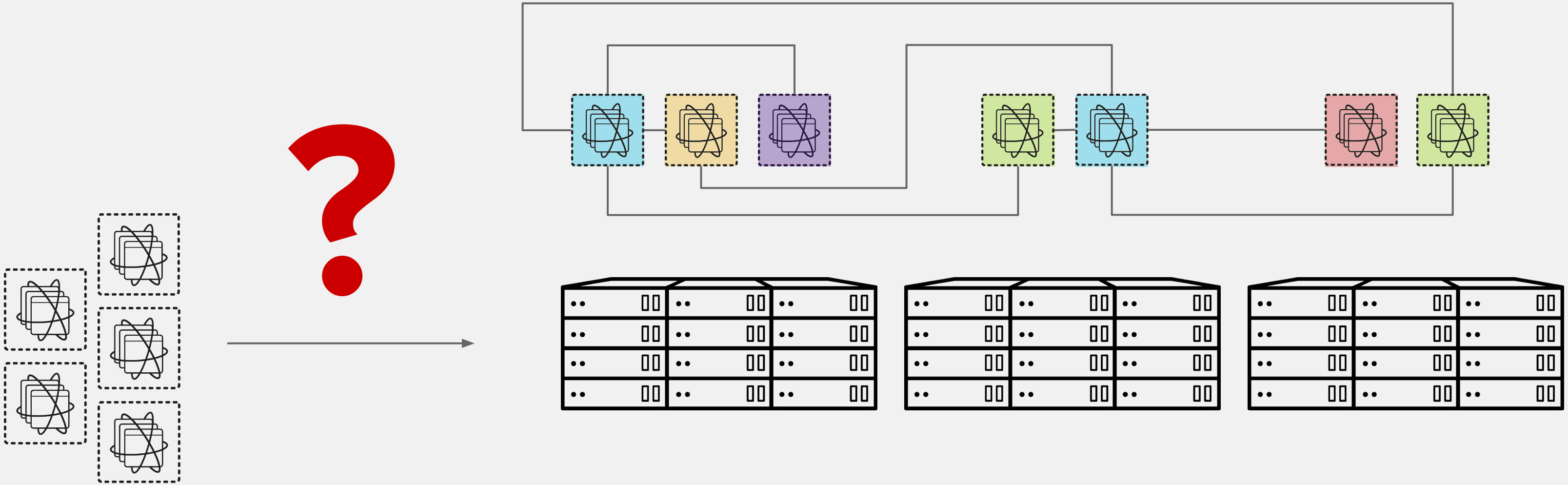
private cloud

public cloud

DEVOPS WITH CONTAINERS







WE NEED MORE THAN JUST CONTAINERS

Scheduling
Decide where to deploy containers

Lifecycle and health
Keep containers running despite failures

Discovery
Find other containers on the network

Monitoring
Visibility into running containers

Security
Control who can do what

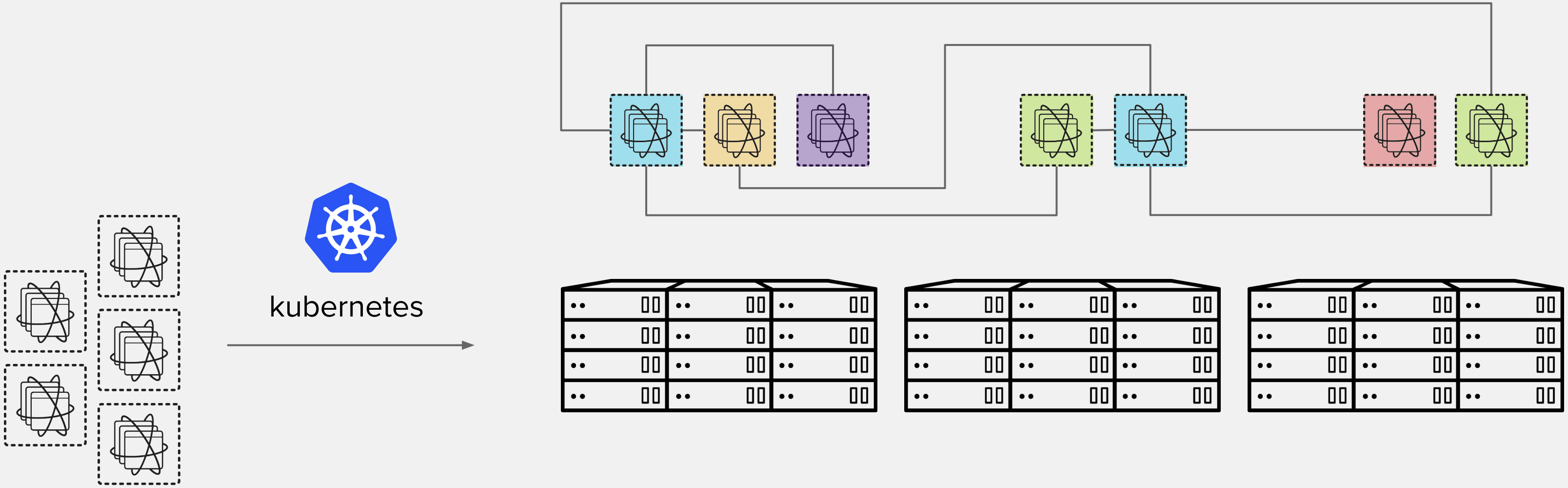
Scaling
Scale containers up and down

Persistence
Survive data beyond container lifecycle

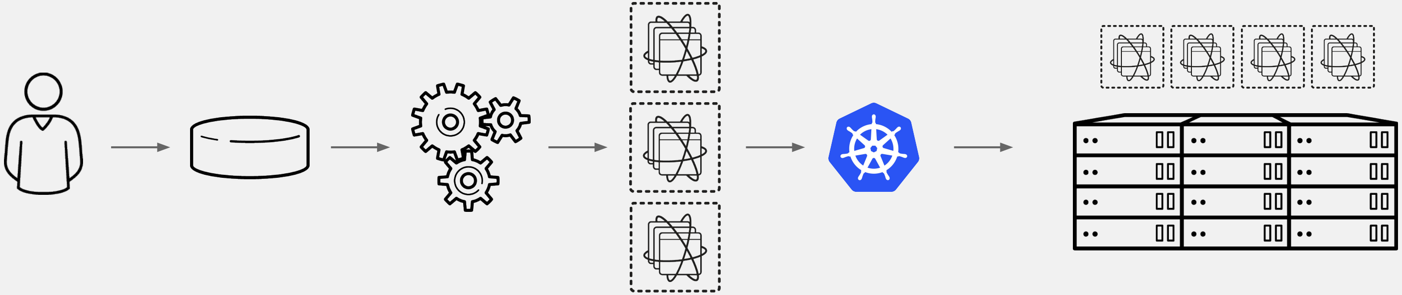
Aggregation
Compose apps from multiple containers

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

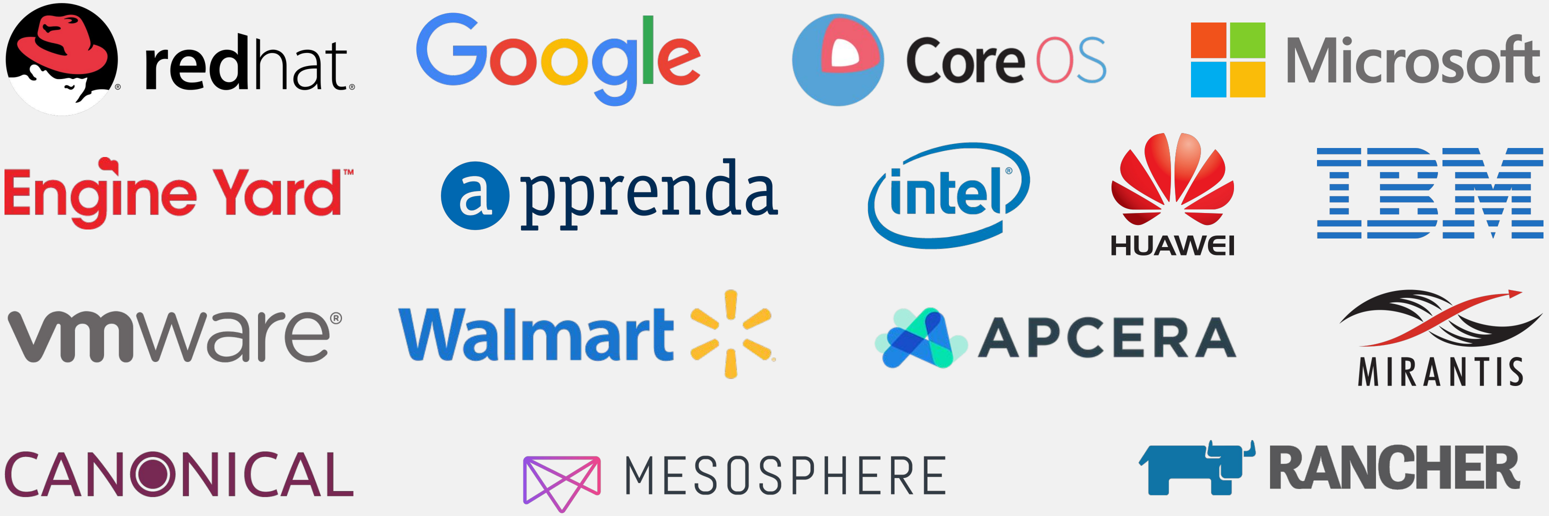
kubernetes


kubernetes

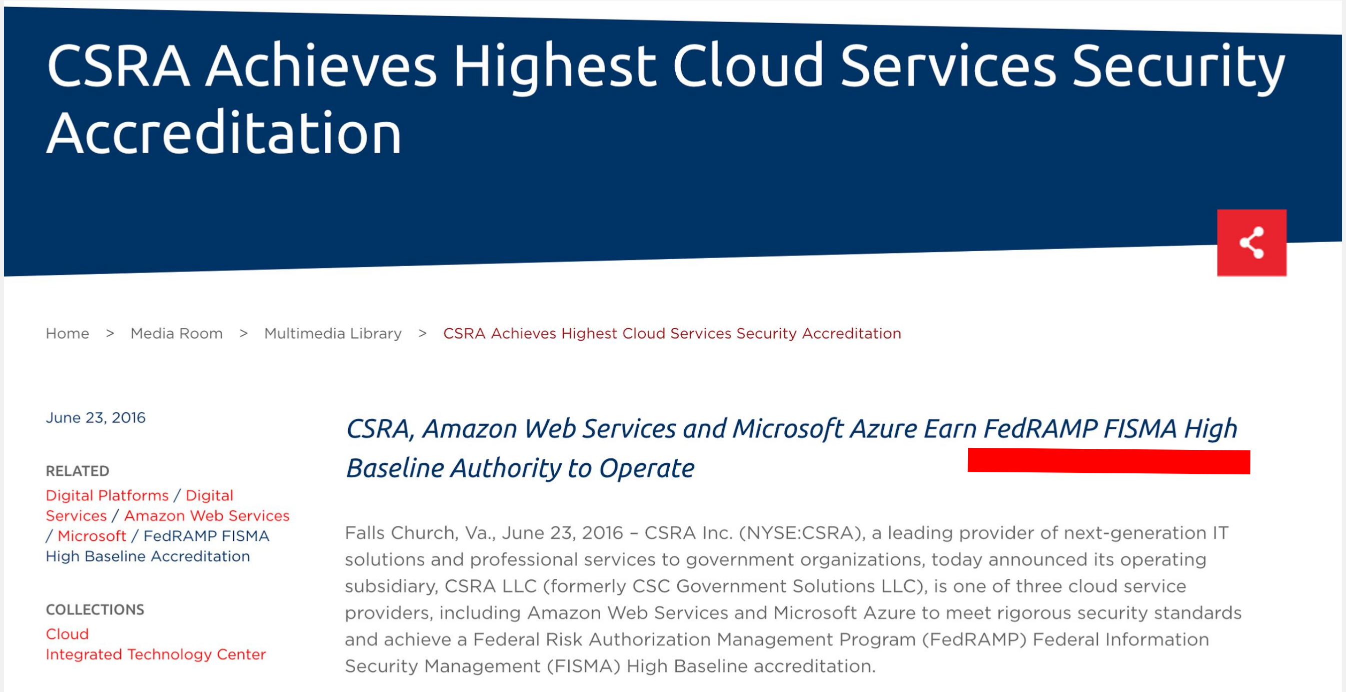
DEVOPS WITH CONTAINERS AND KUBERNETES



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

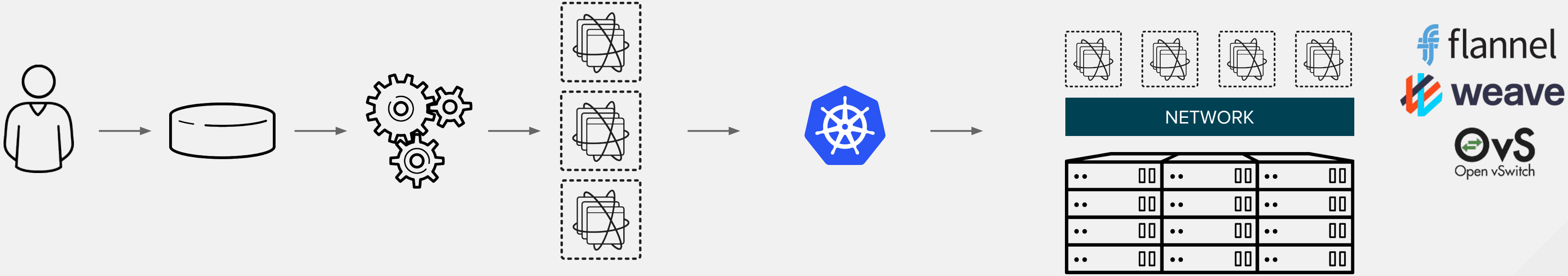
Cloud

Integrated Technology Center

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

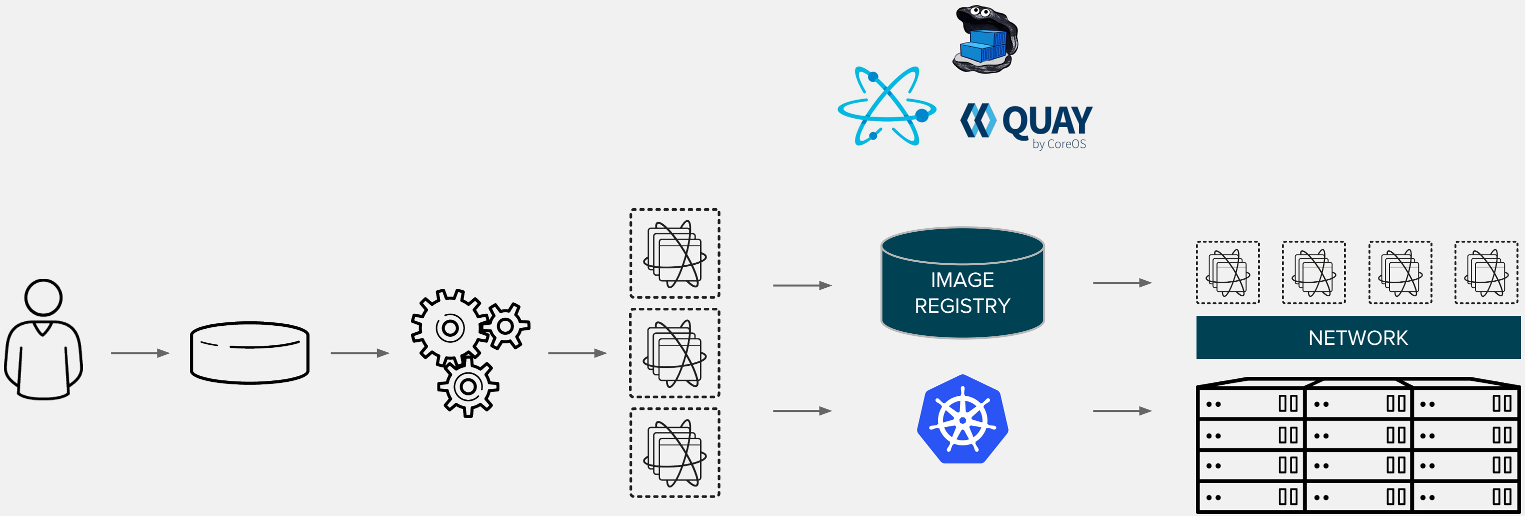
Falls Church, Va., June 23, 2016 – CSRA Inc. (NYSE:CSRA), a leading provider of next-generation IT solutions and professional services to government organizations, today announced its operating subsidiary, CSRA LLC (formerly CSC Government Solutions LLC), is one of three cloud service providers, including 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



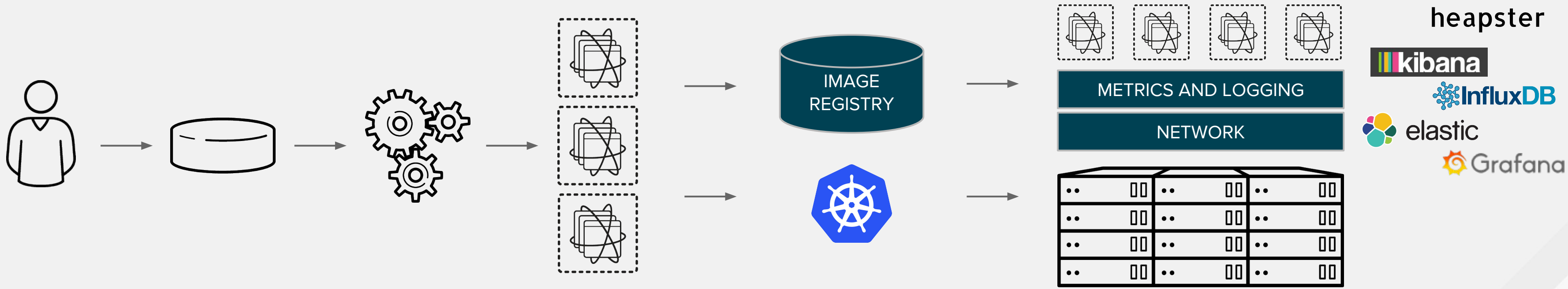
Not enough! Need networking

DEVOPS WITH CONTAINERS AND KUBERNETES



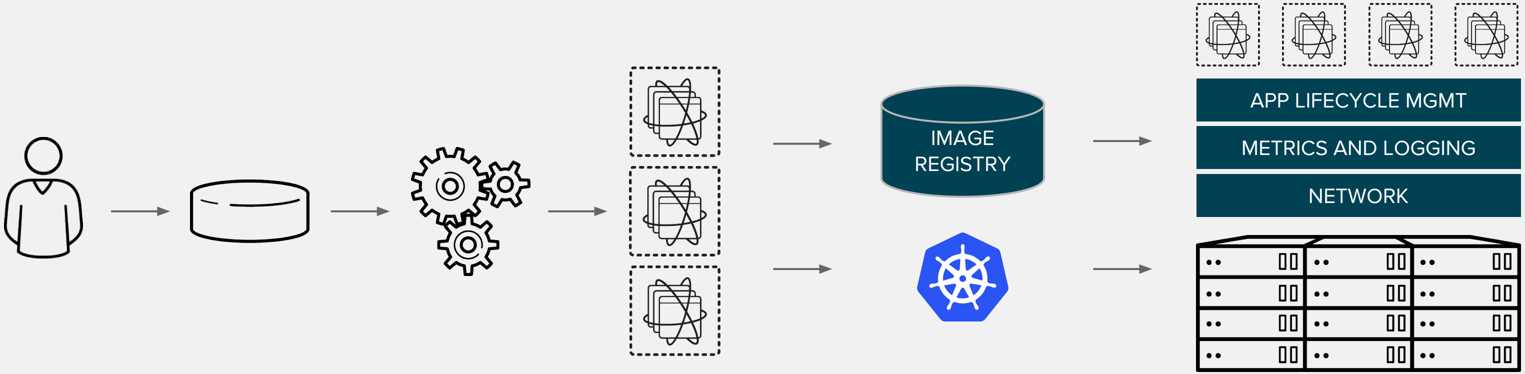
Not enough! Need an image registry

DEVOPS WITH CONTAINERS AND KUBERNETES



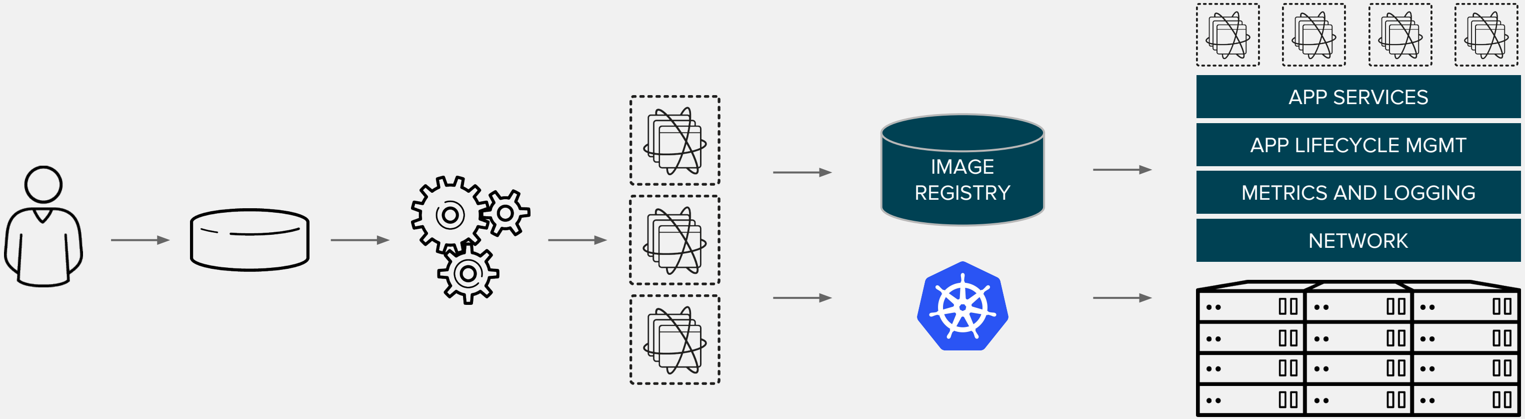
Not enough! Need metrics and logging

DEVOPS WITH CONTAINERS AND KUBERNETES



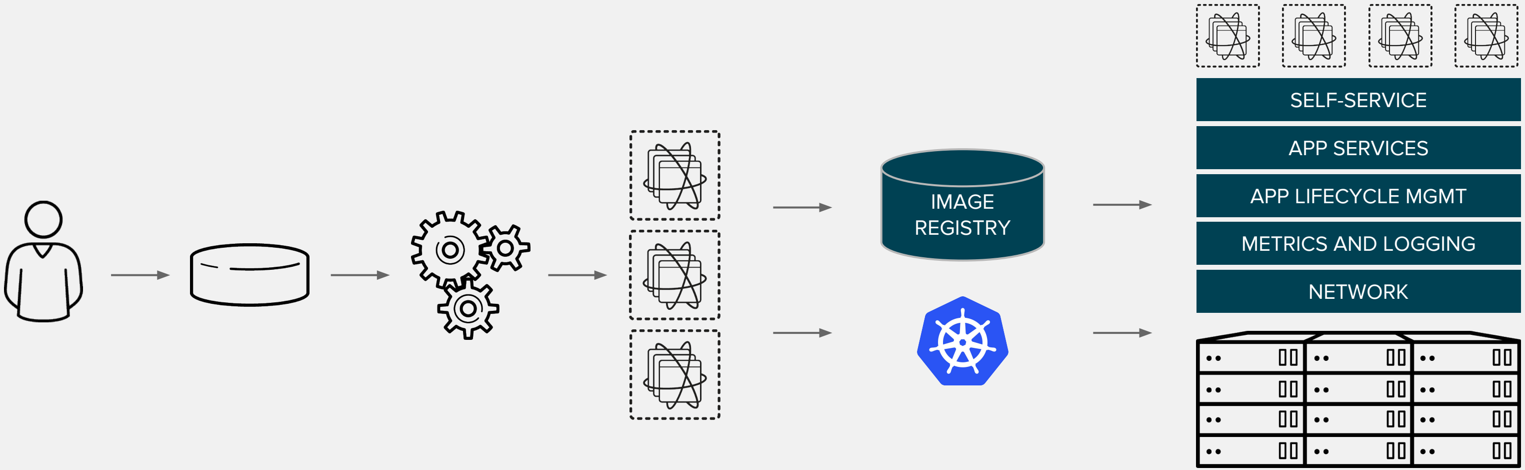
Not enough! Need application lifecycle management

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

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

RED HAT® OPENSHIFT

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

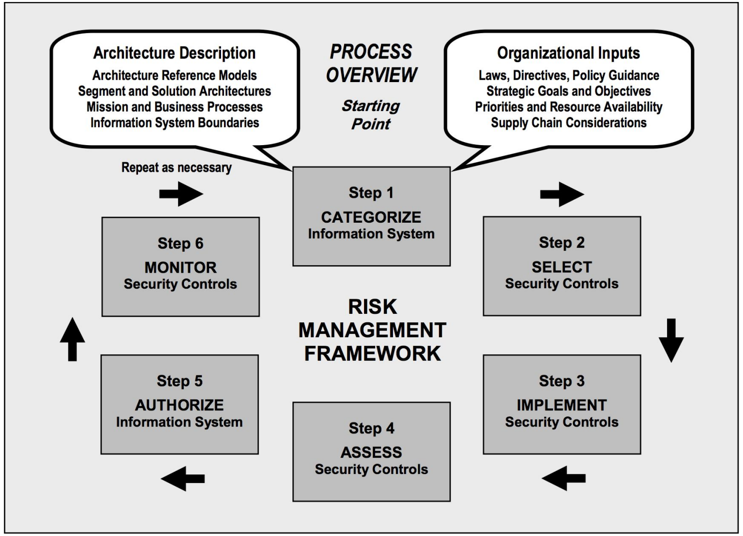
MARCH 2017

INDUSTRY FIRST: NIST CERTIFIED CONFIGURATION AND VULNERABILITY SCANNER FOR CONTAINER

JUNE 2017

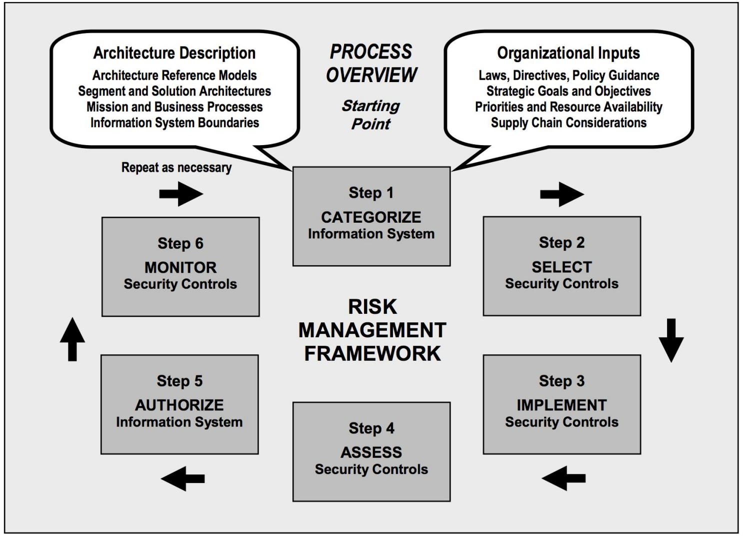
OPENSHIFT BLUEPRINT FOR AZURE
(FedRAMP MODERATE)

Meanwhile, in Government: FISMA from an earlier era


Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries
PROCESS OVERVIEW
Starting Point
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Repeat as necessary
Step 1 CATEGORIZE Information System
Step 2 SELECT Security Controls
Step 3 IMPLEMENT Security Controls
Step 4 ASSESS Security Controls
Step 5 AUTHORIZE Information System
Step 6 MONITOR Security Controls
RISK MANAGEMENT FRAMEWORK

- 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



Architecture Description
Architecture Reference Models
Segment and Solution Architectures
Mission and Business Processes
Information System Boundaries

PROCESS OVERVIEW

Starting Point

Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations

Repeat as necessary

Step 1
CATEGORIZE
Information System

Step 2
SELECT
Security Controls

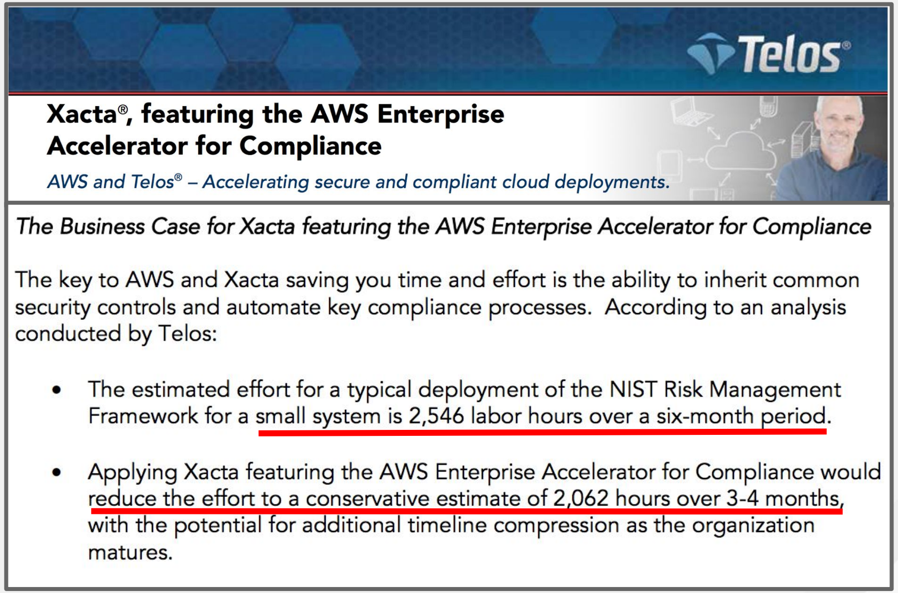
Step 3
IMPLEMENT
Security Controls

Step 4
ASSESS
Security Controls

Step 5
AUTHORIZE
Information System

Step 6
MONITOR
Security Controls

RISK MANAGEMENT FRAMEWORK



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:

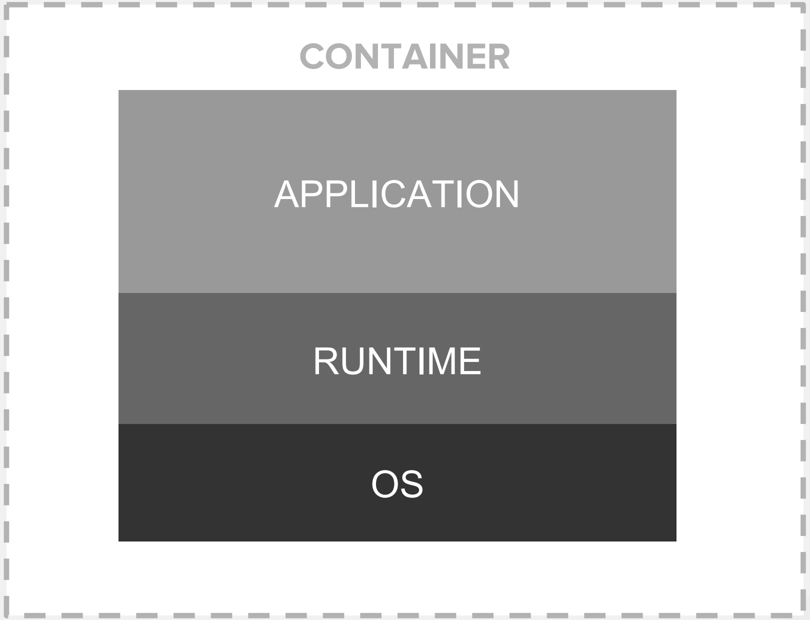
- The estimated effort for a typical deployment of the NIST Risk Management Framework for a small system is 2,546 labor hours over a six-month period.
- Applying Xacta featuring the AWS Enterprise Accelerator for Compliance would reduce the effort to a conservative estimate of 2,062 hours over 3-4 months,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

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

Container Contents Matter

You need to know . . .

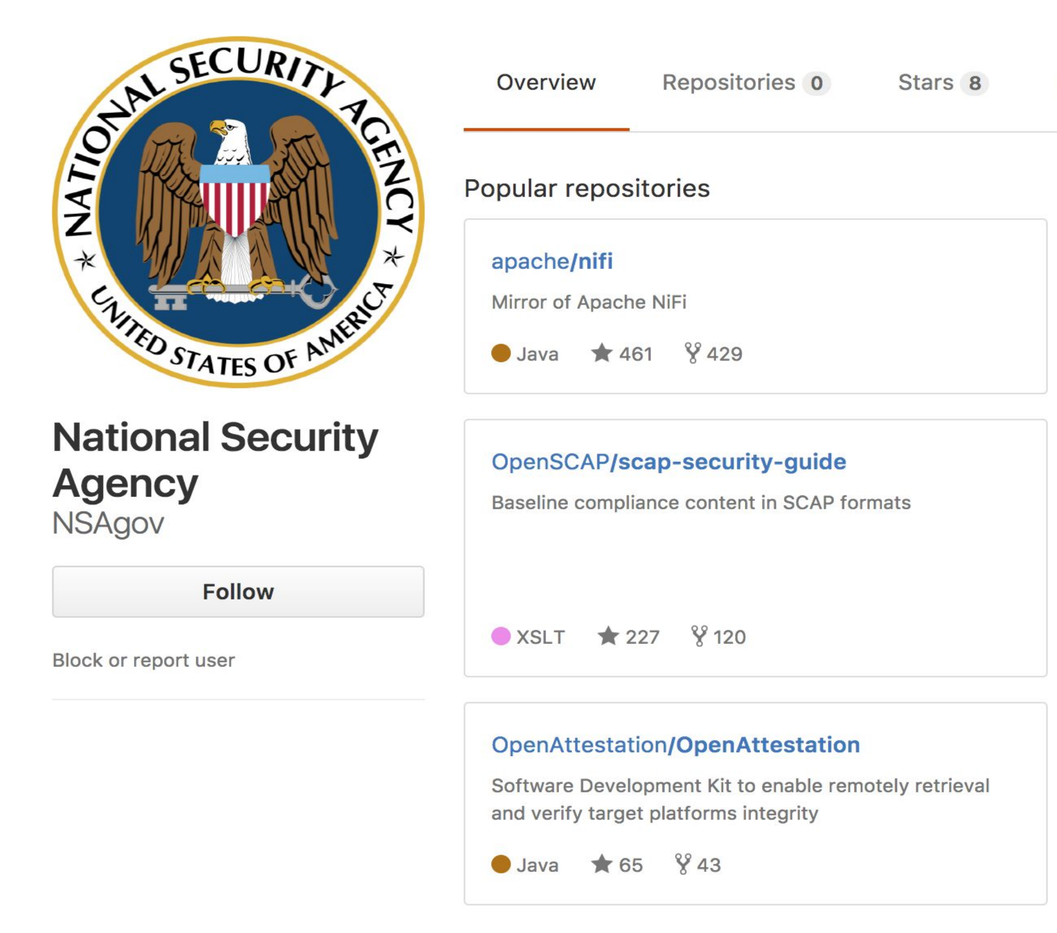
- Will what’s inside your container compromise your infrastructure?
- Are there known vulnerabilities in the application layer?
- Are the runtime and operating system layers up to date?



OpenSCAP

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

https://github.com/NSAgov
Or direct: 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

Department of Justice Federal Bureau of Investigation

Central Intelligence Agency United States of America

LOCKHEED MARTIN

Defense Information Systems Agency

TRESYS TECHNOLOGY

ARL U.S. Army Research Laboratory

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

HARRIS®

OpenSCAP

RHEL7 STIG content, rebased in RHEL 7.3:

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

OpenSCAP interpreter contains:

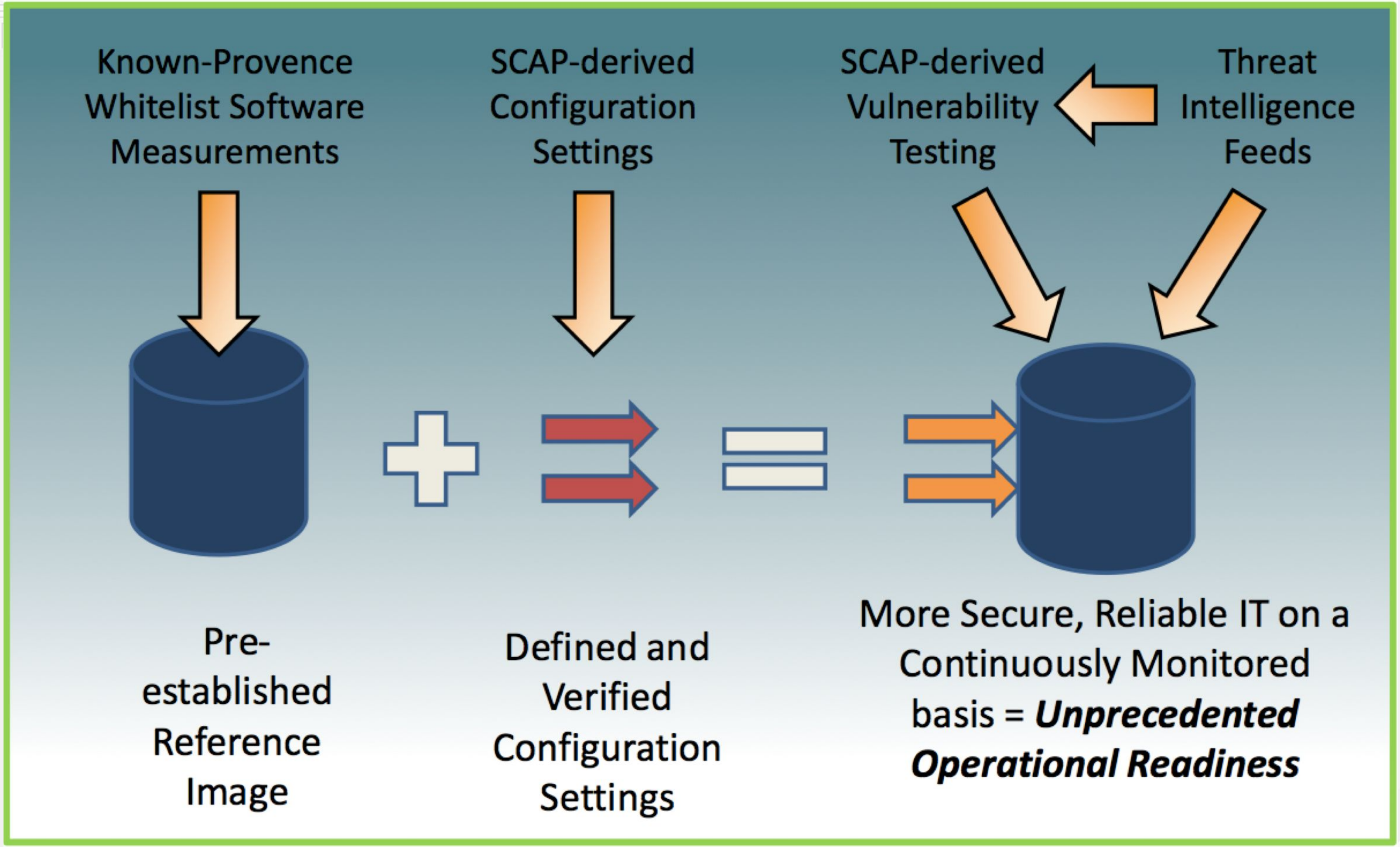
- 6,811 commits from 74 people
- 157,775 lines of code

“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

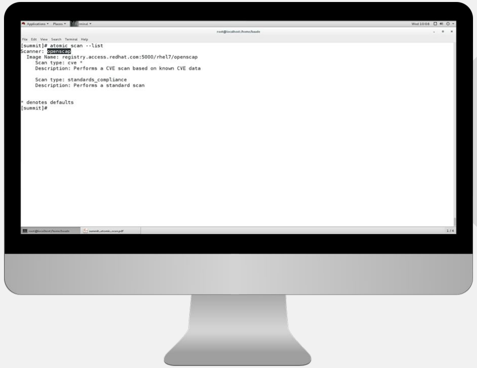
Defined and Verified Configuration Settings

More Secure, Reliable IT on a Continuously Monitored basis = ***Unprecedented Operational Readiness***

Atomic Scan

Enables multiple container scanners

OpenSCAP



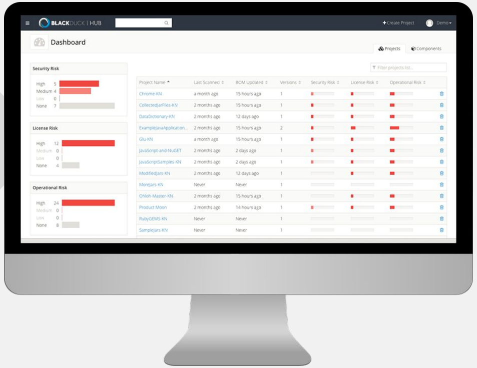
```
[summit]# atomic scan --list
Scanner: openscap
  Image Name: registry.access.redhat.com:5000/rhel7/openscap
     Scan type: cve *
     Description: Performs a CVE scan based on known CVE data

     Scan type: standards_compliance
     Description: Performs a standard scan


* denotes defaults
[summit]#
```

RED HAT
CONTAINER
SCANNING
INTERFACE

BLACKDUCK



Dashboard

Security Risk

High	5	🟥
Medium	4	🟥
Low	0	
None	7	

License Risk

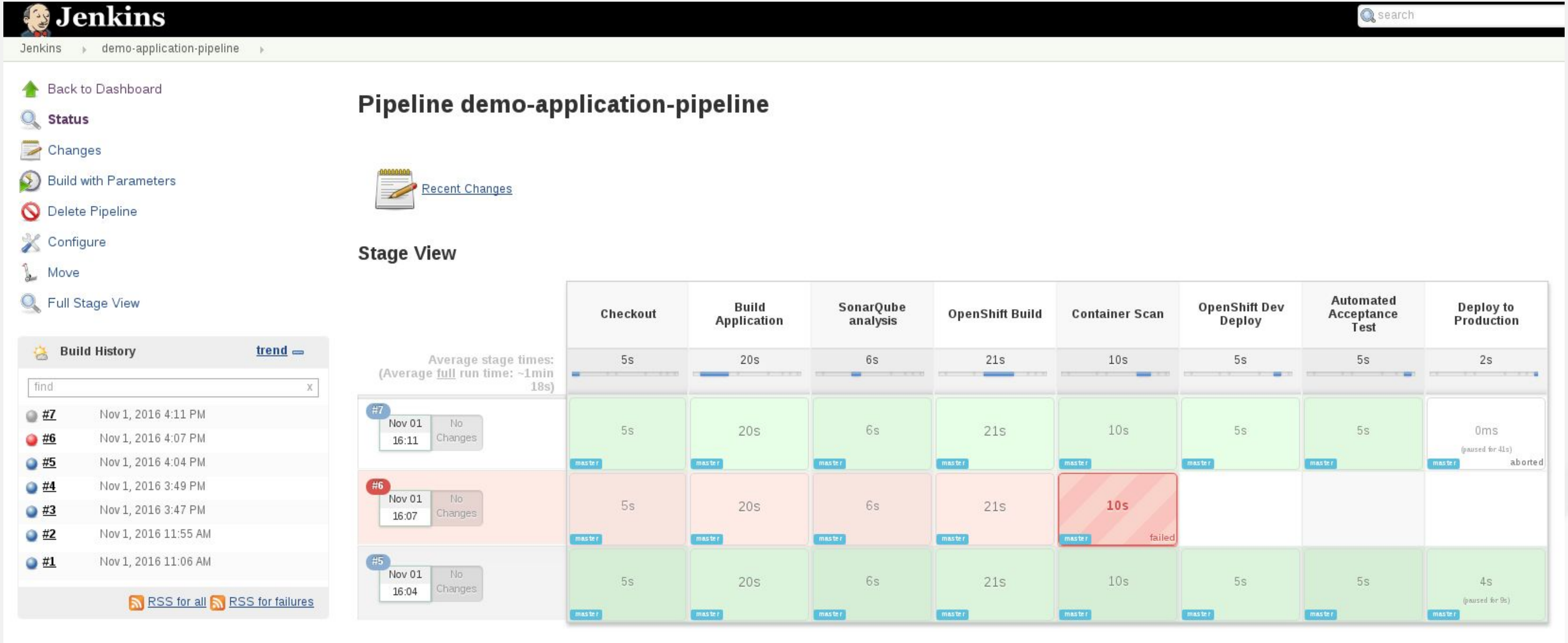
High	12	🟥
Medium	0	
Low	0	
None	4	

Operational Risk

High	24	🟥
Medium	0	
Low	0	
None	8	

Project Name	Last Scanned	BOM Updated	Versions	Security Risk	License Risk	Operational Risk
Chrome-KN	a month ago	15 hours ago	1	🟥	🟥	🟥
CollectedJarFiles-KN	2 months ago	15 hours ago	1	🟥	🟥	🟥
DataDictionary-KN	2 months ago	12 days ago	1	🟥	🟥	🟥
ExampleJavaApplication...	2 months ago	15 hours ago	2	🟥	🟥	🟥
Glu-KN	a month ago	15 hours ago	1	🟥	🟥	🟥
JavaScript-and-NuGET	2 months ago	2 days ago	1	🟥	🟥	🟥
JavaScriptSamples-KN	2 months ago	2 days ago	1	🟥	🟥	🟥
ModifiedJars-KN	2 months ago	12 days ago	1		🟥	🟥
MoreJars-KN	Never	Never	1			
Ohloh-Master-KN	2 months ago	15 hours ago	1		🟥	🟥
Product Moon	2 months ago	14 hours ago	1	🟥	🟥	🟥
RubyGEMS-KN	Never	Never	1			
SampleJars-KN	Never	Never	1			

Example Pipeline



Pipeline demo-application-pipeline

Recent Changes

Stage View

	Checkout	Build Application	SonarQube analysis	OpenShift Build	Container Scan	OpenShift Dev Deploy	Automated Acceptance Test	Deploy to Production
Average stage times: (Average full run time: ~1min 18s)	5s	20s	6s	21s	10s	5s	5s	2s
#7 Nov 01 16:11 No Changes	5s master	20s master	6s master	21s master	10s master	5s master	5s master	0ms (paused for 41s) master aborted
#6 Nov 01 16:07 No Changes	5s master	20s master	6s master	21s master	10s master failed			
#5 Nov 01 16:04 No Changes	5s master	20s master	6s master	21s master	10s master	5s master	5s master	4s (paused for 9s) master

Build History trend

find x

#7	Nov 1, 2016 4:11 PM
#6	Nov 1, 2016 4:07 PM
#5	Nov 1, 2016 4:04 PM
#4	Nov 1, 2016 3:49 PM
#3	Nov 1, 2016 3:47 PM
#2	Nov 1, 2016 11:55 AM
#1	Nov 1, 2016 11:06 AM

RSS for all RSS for failures

demos!

Contact Info

LinkedIn:	https://www.linkedin.com/in/shawndwells/
EMail:	shawn@redhat.com
Cell:	443-534-0130 (US EST)
Blog:	https://shawnwells.io

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

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