

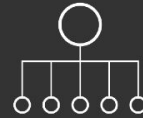
# DevOpsSec: Building CI/CD with Security Teams

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





# SORENSEN'S LESSONS



**STANDARD  
PARTS**

**STANDARD  
PROCESS**

**STANDARD  
INFRASTRUCTURE**

**BUILD  
FOR CHANGE**



## STANDARD PARTS

- Standardized
- Interoperable
- Multi-vendor

STANDARD PROCESS

STANDARD INFRASTRUCTURE

BUILD FOR CHANGE



STANDARD  
PARTS

**STANDARD  
PROCESS**

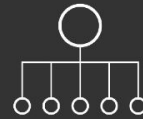
STANDARD  
INFRASTRUCTURE

BUILD  
FOR CHANGE

Eliminate redundancy

Encourage flexibility

Drive modularity



STANDARD  
PARTS

STANDARD  
PROCESS

**STANDARD  
INFRASTRUCTURE**

BUILD  
FOR CHANGE

Process drives tools.  
Not the other way around.



STANDARD  
PARTS

STANDARD  
PROCESS

STANDARD  
INFRASTRUCTURE

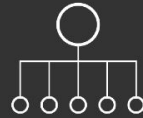
**BUILD  
FOR CHANGE**

Turn craftwork  
into commodities.

Design for improvement,  
not function.



# SORENSEN'S LESSONS



**STANDARD  
PARTS**

**STANDARD  
PROCESS**

**STANDARD  
INFRASTRUCTURE**

**BUILD  
FOR CHANGE**

**RELEASES PER YEAR**

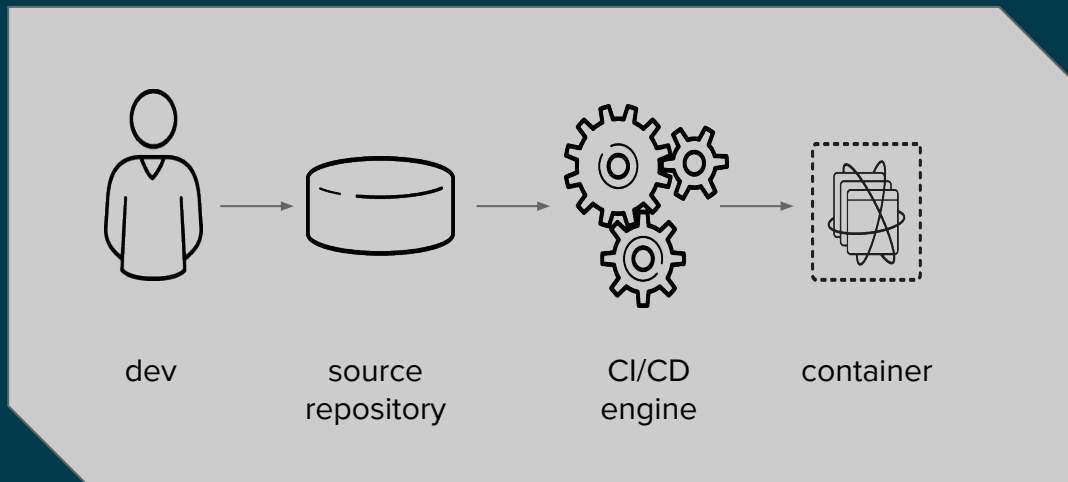
**1/day**



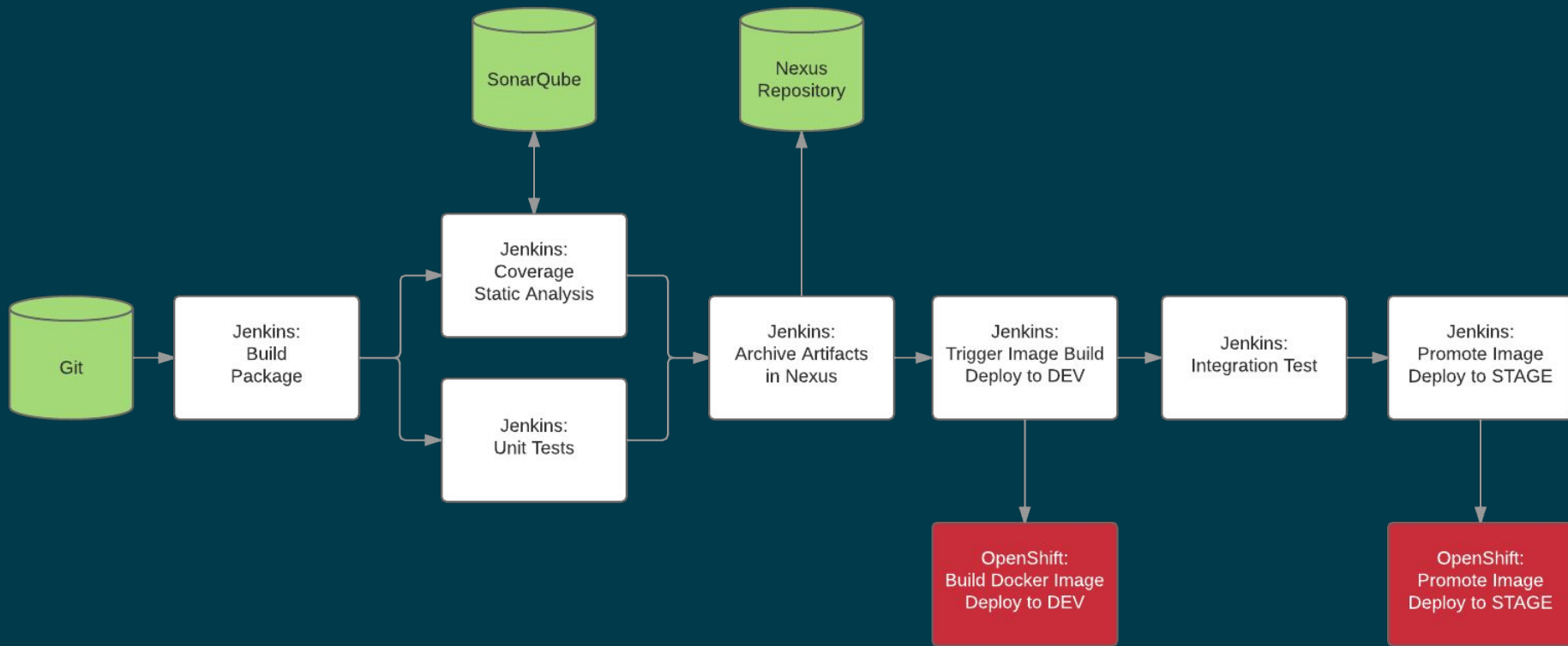
**1/hour**



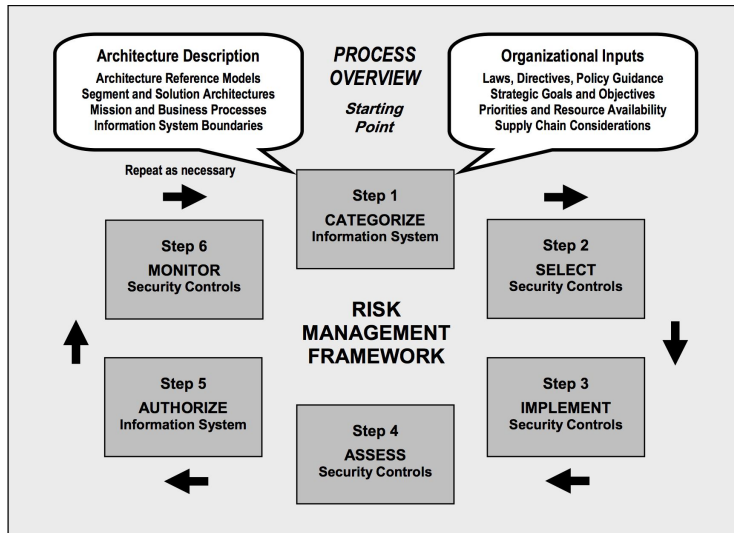
# INTRO TO CI/CD



# INTRO TO CI/CD


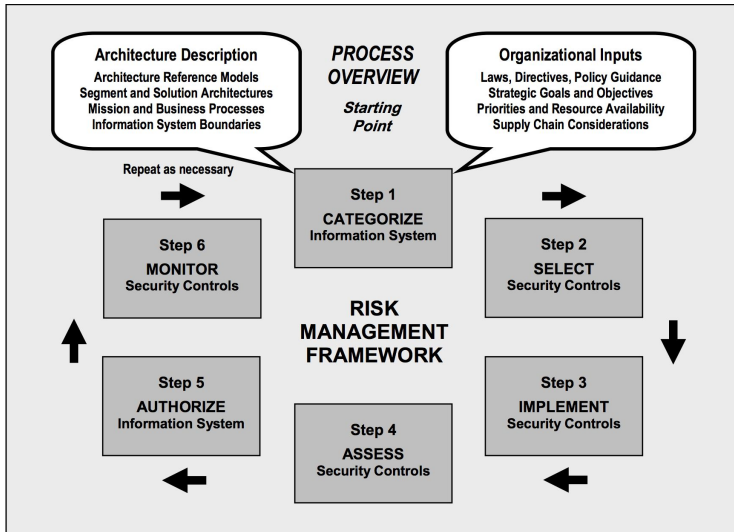


# Meanwhile, in Government: FISMA from an earlier era



- 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



## Xacta<sup>®</sup>, featuring the AWS Enterprise Accelerator for Compliance

*AWS and Telos<sup>®</sup> – Accelerating secure and compliant cloud deployments.*

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

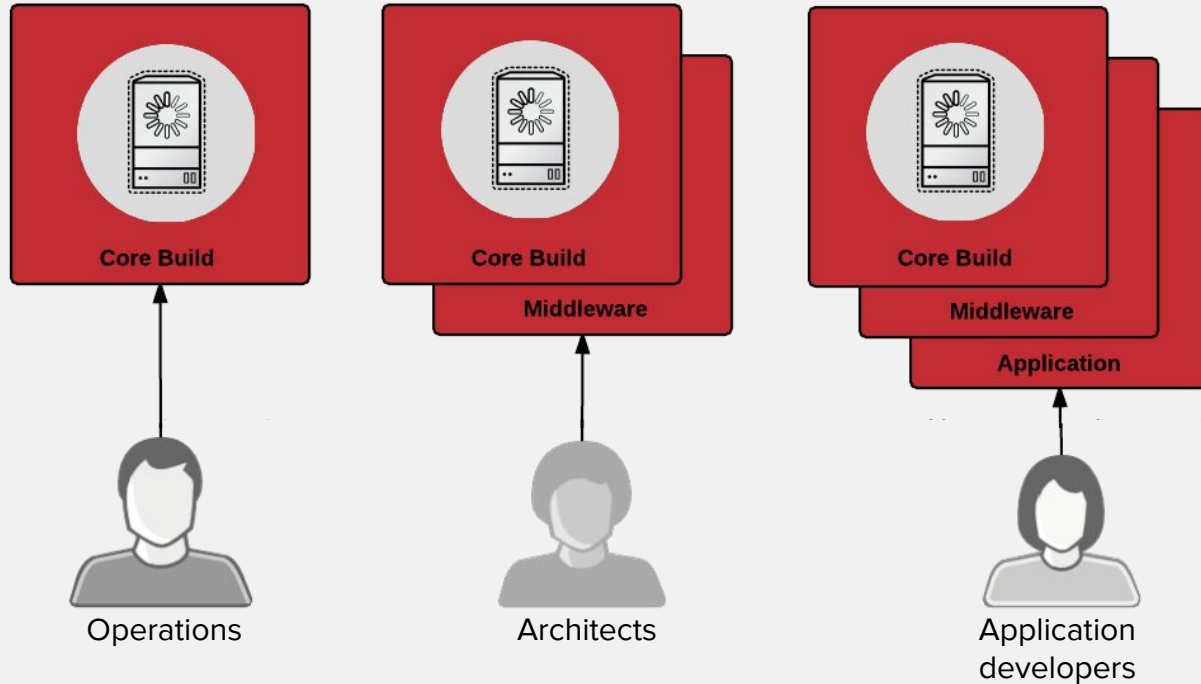
The key to AWS and Xacta saving you time and effort is the ability to inherit common security controls and automate key compliance processes. According to an analysis conducted by Telos:

- 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>

# DevOps + Security

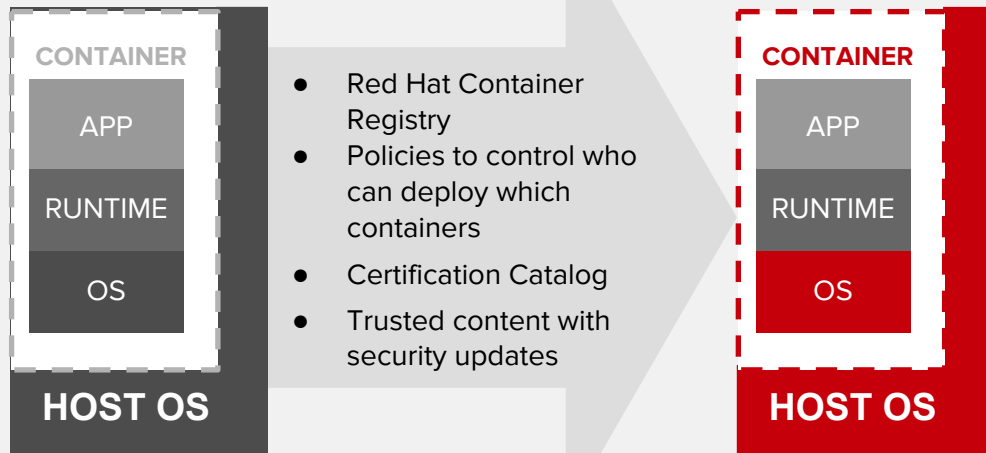
# Layered Packaging: Separation of Concerns



# Registries: Where do you get your containers?

## Public and Private Registries

- What security meta-data is available for your images?
- Are the images updated regularly?
- Are there access controls in the registry? How strong are they?

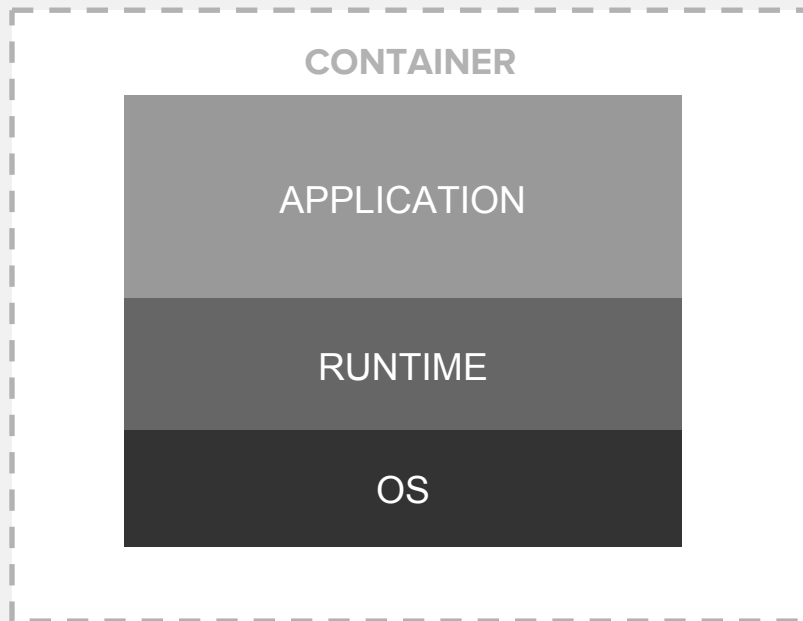


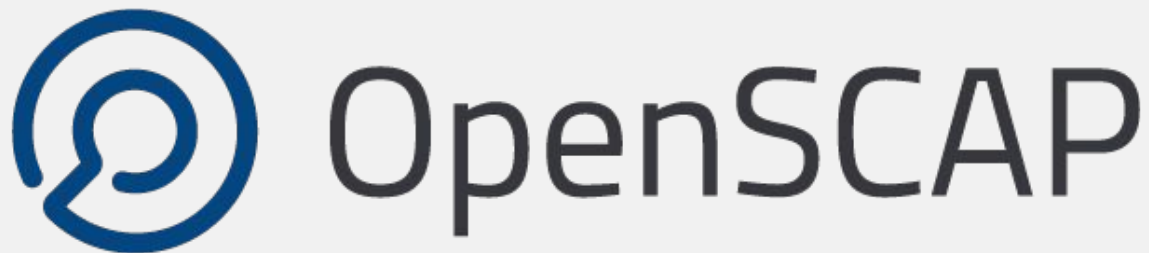


# Container Contents Matter

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?





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**  
NSA.gov

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>





# 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

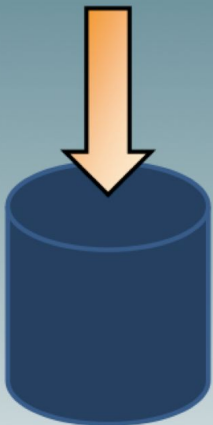
“Security Button” RHEL7 Installer:

- 6 people, 90 days

Shipping in RHEL 7:

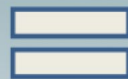
- **Intelligence Community:** C2S and CS2
- **DoD:** RHEL7 Vendor STIG
- **Civilian:** USGCB/OSPP
- **Justice:** FBI Criminal Justice Info. Systems (FBI CJIS)

Known-Provence  
Whitelist Software  
Measurements



Pre-  
established  
Reference  
Image

SCAP-derived  
Configuration  
Settings



Defined and  
Verified  
Configuration  
Settings

SCAP-derived  
Vulnerability  
Testing



Threat  
Intelligence  
Feeds



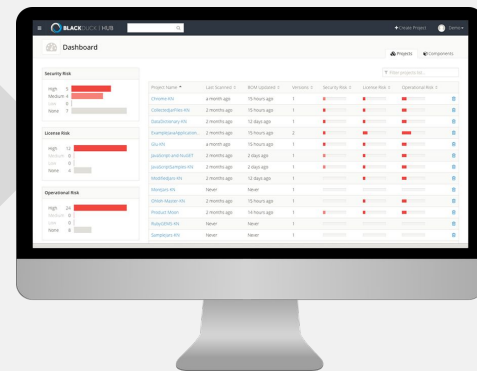
More Secure, Reliable IT on a  
Continuously Monitored  
basis = **Unprecedented  
Operational Readiness**

# Atomic Scan

Enables multiple container scanners



RED HAT  
CONTAINER  
SCANNING  
INTERFACE



# Example Pipeline

The screenshot shows the Jenkins web interface for a pipeline named 'demo-application-pipeline'. The top navigation bar includes the Jenkins logo and a search field. The left sidebar contains navigation links: 'Back to Dashboard', 'Status', 'Changes', 'Build with Parameters', 'Delete Pipeline', 'Configure', 'Move', and 'Full Stage View'. The main content area is titled 'Pipeline demo-application-pipeline' and includes a 'Recent Changes' link. Below this is the 'Stage View' section, which displays a table of pipeline stages and their execution history.

**Stage View**

Average stage times:  
(Average full run time: ~1min 18s)

	Checkout	Build Application	SonarQube analysis	OpenShift Build	Container Scan	OpenShift Dev Deploy	Automated Acceptance Test	Deploy to Production
<b>#7</b> Nov 01 16:11 No Changes	5s	20s	6s	21s	10s	5s	5s	0ms (paused for 41s) aborted
<b>#6</b> Nov 01 16:07 No Changes	5s	20s	6s	21s	10s failed			
<b>#5</b> Nov 01 16:04 No Changes	5s	20s	6s	21s	10s	5s	5s	4s (paused for 0s)

**Build History** [trend](#)

find

- #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!**



**Thank You**

# Contact Info

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

E-Mail: [shawn@redhat.com](mailto: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>