



Red Hat
OpenShift
Container Platform

OPENShift CONTAINER PLATFORM

DEVSECOPS OVERVIEW

Joshua Smith
Cloud Specialist SA
joshua.smith@redhat.com

Laine Vyvyan
Channel SA, North Central
laine.vyvyan@redhat.com

AGENDA

INTRODUCTION: Today's Business Needs

KEY CONCEPTS: Digital Transformation, DevSecOps, etc

HOLISTIC VIEW: The Technology of the Solution

STARTER PACK: DevSecOps CI/CD Pipeline

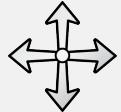
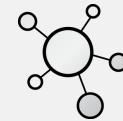
DIGITAL TRANSFORMATION NEEDS



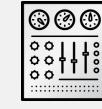
Speed / Security



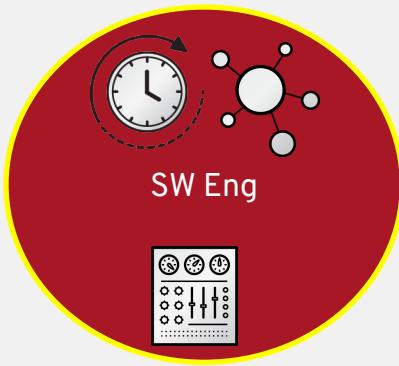
IT Optimization / App Modernization



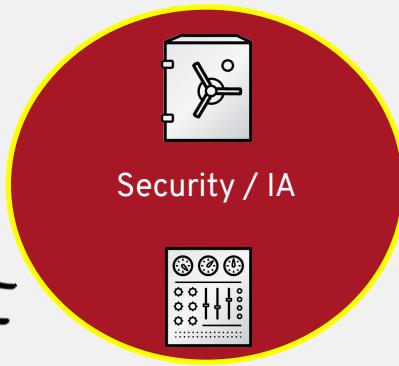
Path to the Cloud / Cloud First



THE CULTURAL CHALLENGE



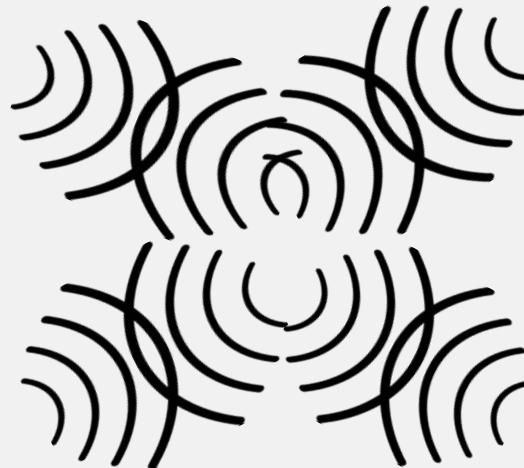
SW Eng



Security / IA



IT Ops

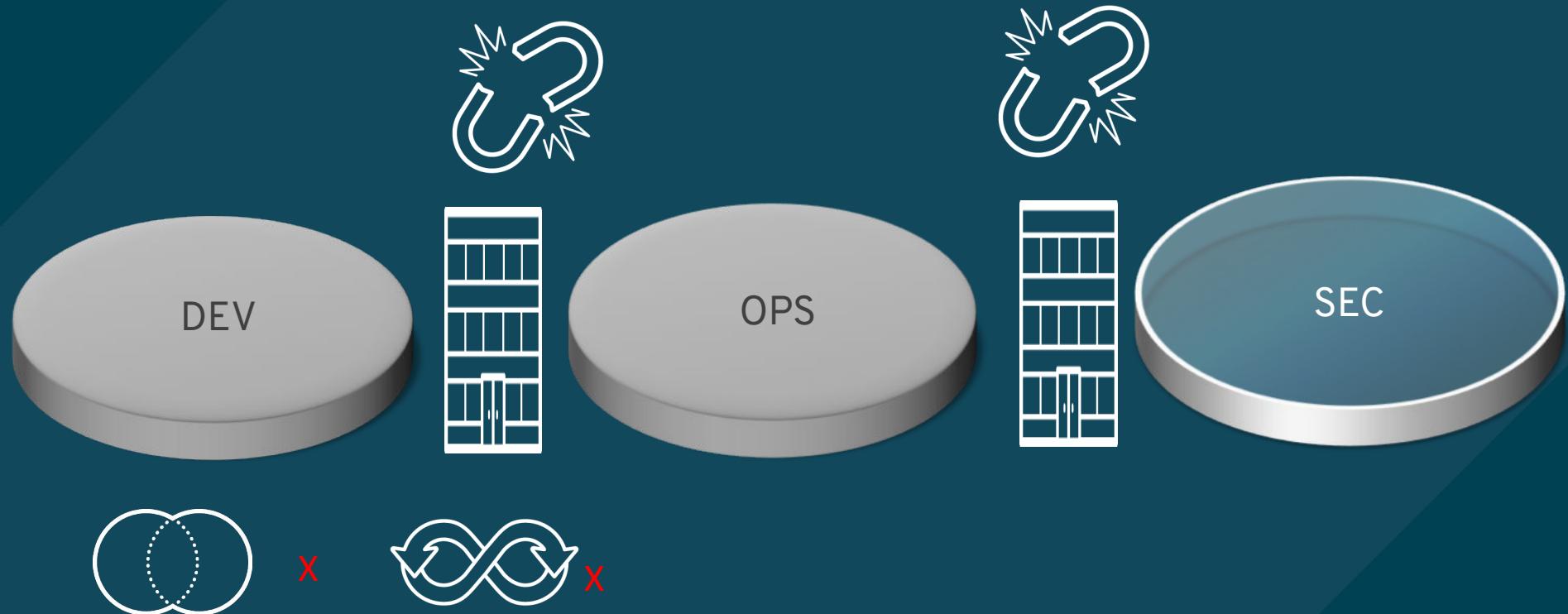


Biz Analyst / QA

THE CULTURAL CHALLENGE (CONT.)

Developers	IT Ops	QA/BA	Security / IA
<ul style="list-style-type: none">• Features• Quality• Attributes• Efficiency• Performance• Users• Authentication• Authorization• New Technology	<ul style="list-style-type: none">• Deployment• Maintenance• Updates• Change policy• Failure• Data loss• Risk prevention• Authentication• Authorization	<ul style="list-style-type: none">• Testable• Issue tracking• Bug Reports• Usability• Performance• Load• Help Desk	<ul style="list-style-type: none">• Data Privacy• Intrusion detection• Threat vectors• CWEs & CVEs• Package/Artifact security• Authentication• Authorization• Security Standards• Compliance

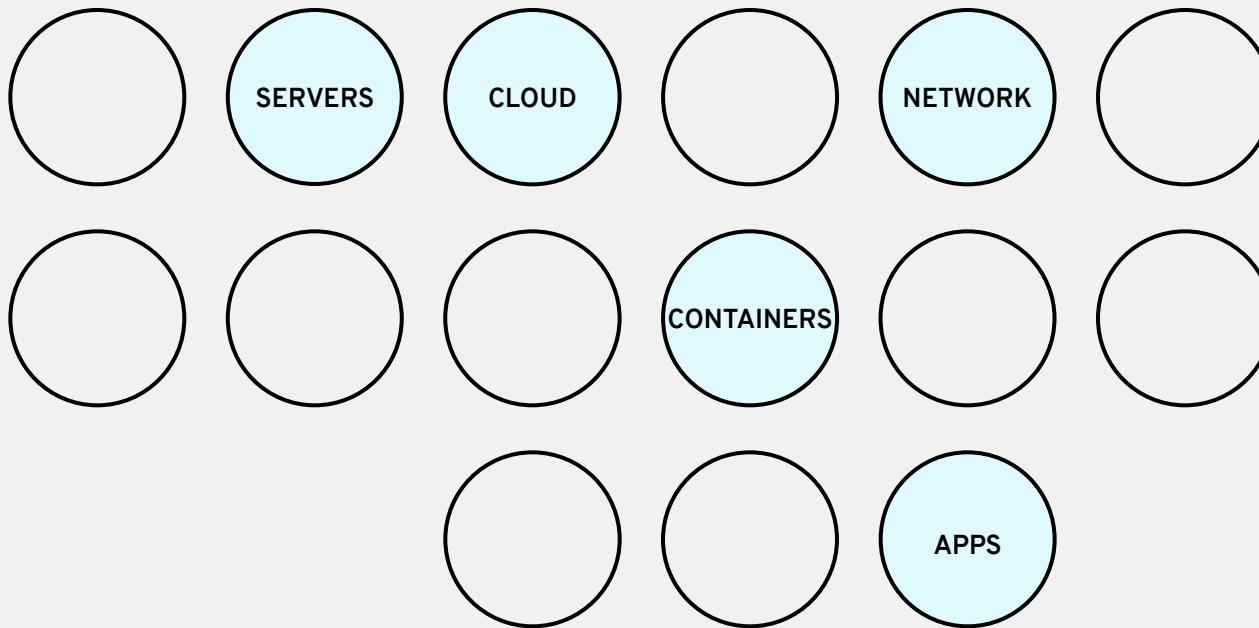
WHAT DOES THAT LOOK LIKE?



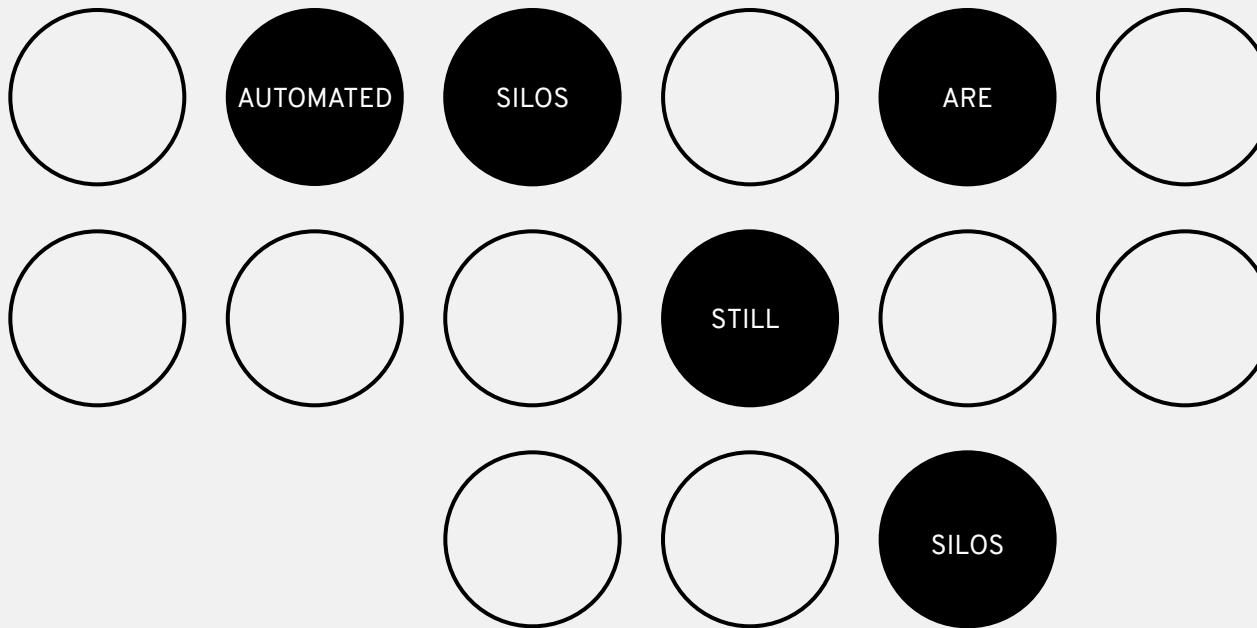
MAYBE SOMETHING LIKE THIS?



THE OPERATIONAL CHALLENGE



THE OPERATIONAL CHALLENGE (CONT.)



THE OPERATIONAL CHALLENGE (CONT.)

1

PEOPLE PROBLEMS

Skills gaps & org charts
get in the way

2

POINT TOOLS

Proliferation of point solutions
and vendor-specific tools

3

PACE OF INNOVATION

Automation requires integration
across domains

THE TECHNICAL CHALLENGE

Applications require complicated installation, verification/validation and integration every time they are deployed.



SOLUTION REQUIRES AN EVOLUTION IN...



Applications
New ways of developing,
delivering, and
integrating applications



Platform
Modernize existing and
build new cloud-based
infrastructure

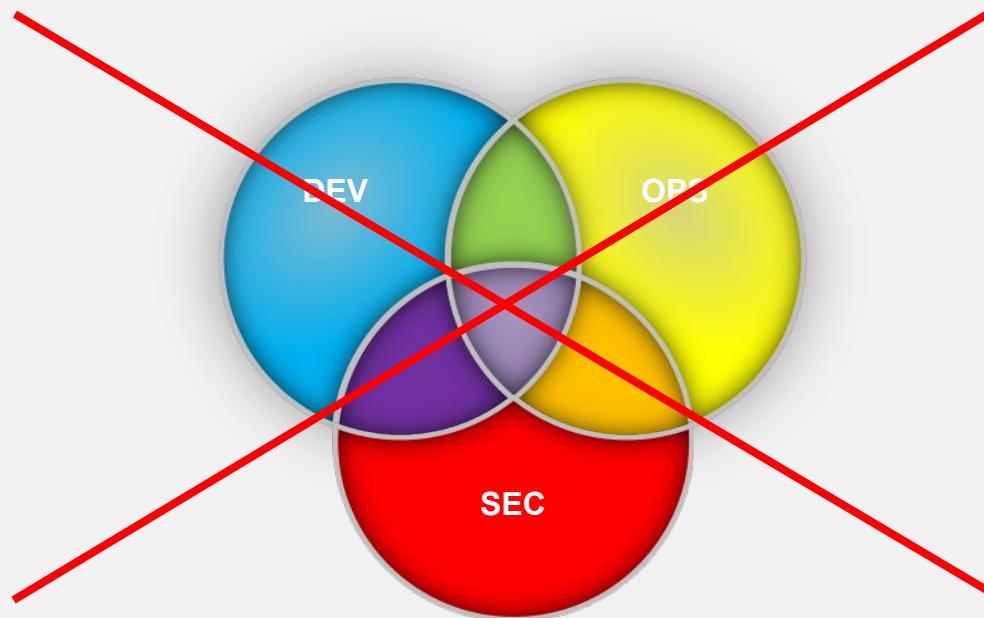


Process
More agile process
across Security, IT and
Engineering

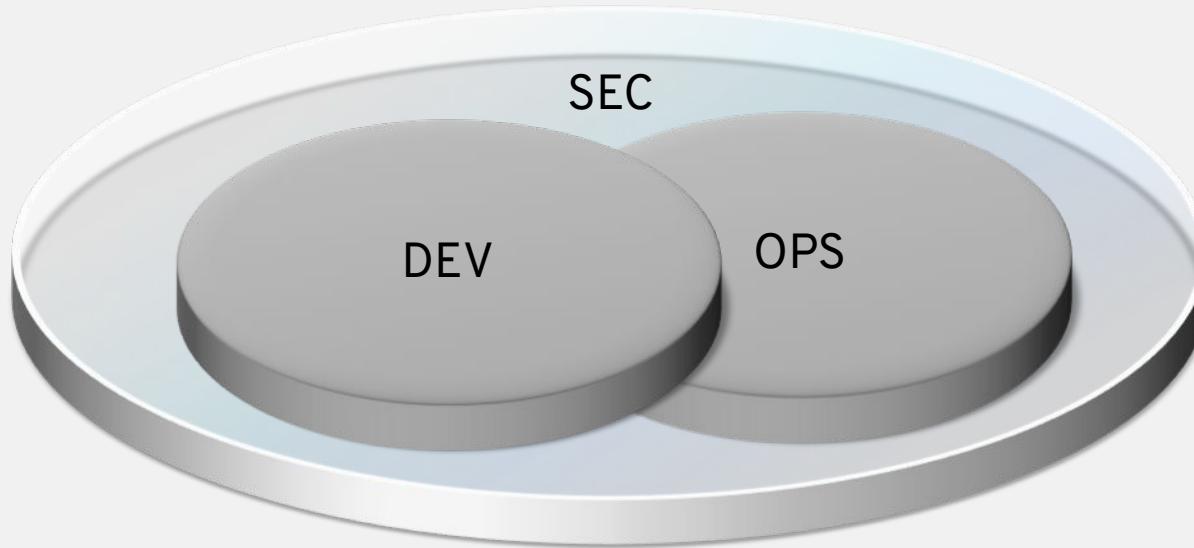
IF YOU WANT SOMETHING NEW,
YOU HAVE TO STOP DOING SOMETHING
OLD.

-Peter Drucker

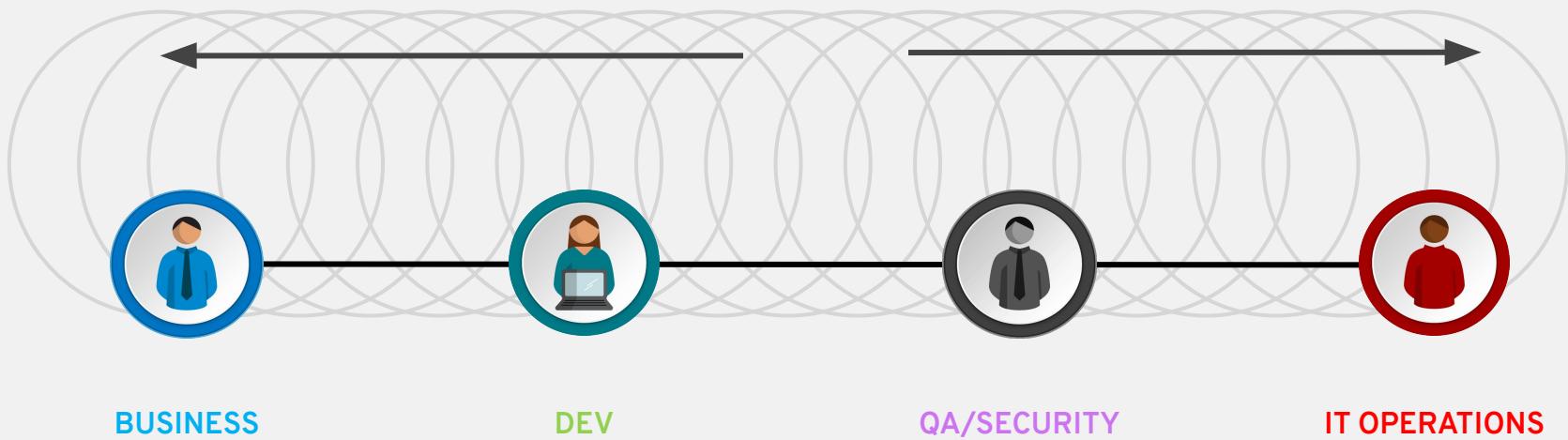
LETS FIRST DISPEL SOME MYTHS



SECURITY ENCOMPASSES NOT INTERSECTS



ADDRESSING THE OPERATIONAL CHALLENGE

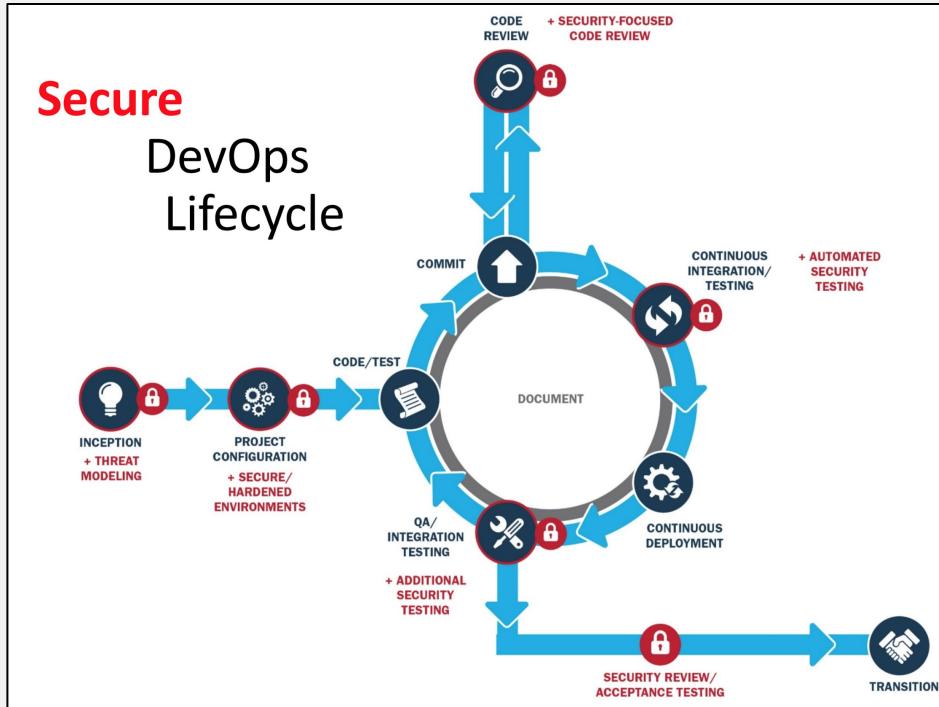


ADDRESSING THE TECHNICAL CHALLENGE

Adopting a container platform strategy will allow applications to be easily shared, managed, secured and deployed.

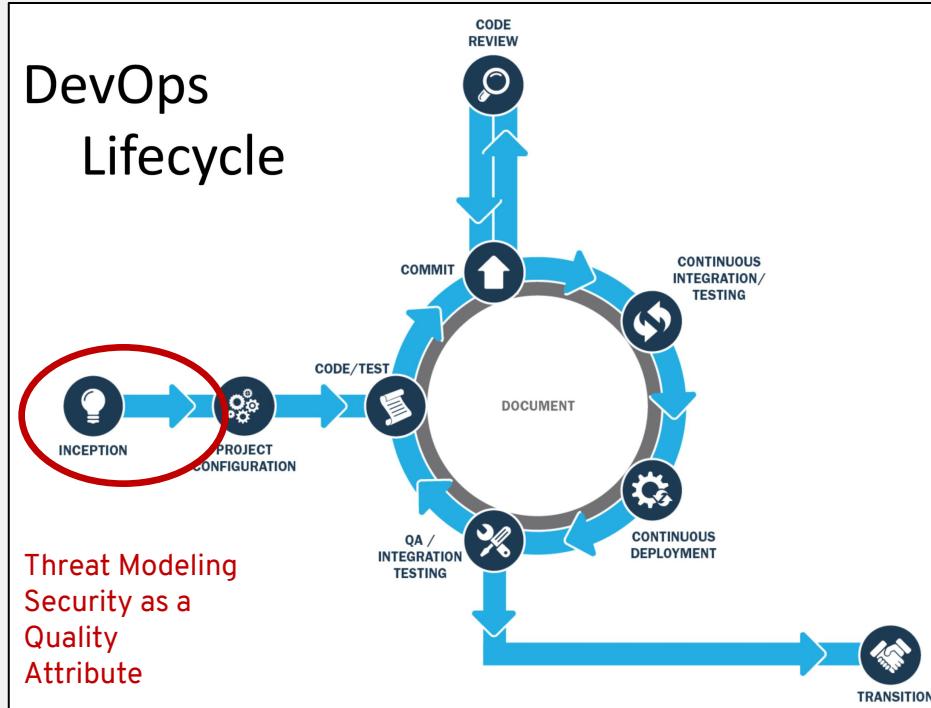


SO WHAT DOES THAT LOOK LIKE?



From All Day DevOps Webinar Nov 2016, Content distributable from Carnegie Mellon

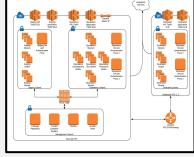
“SHIFT LEFT” WITH SECURITY/IA



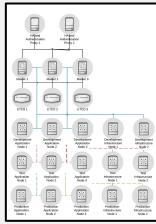
WHAT DOES SECURE MEAN TO YOU?

Global																		
	ISO 27001	ISO 27018	ISO 27017	ISO 22301	ISO 9001	SOC 1 Type 2	SOC 2 Type 2	SOC 3	CSA STAR Self-Assessment	CSA STAR Certification	CSA STAR Attestation							
U.S. Gov																		
	Moderate JAB P-ATO	High JAB P-ATO	DoE 10 CRF 810	DoD DISA SRG Level 2	DoD DISA SRG Level 4	DoD DISA SRG Level 5	DFARS	SP 800-171	FIPS 140-2	Section 508 VPAT	ITAR	CJIS	IRS 1075					
Industry																		
	NEN 7510	PCI DSS Level 1	CDSA	MPAA	FACT UK	Shared Assessments	FIEC	FISC Japan	HIPAA / HITECH Act	HITRUST	GxP 21 CFR Part 11	MARS-E	IG Toolkit UK	FERPA	GLBA	FFIEC		
Regional																		
	BIR 2012	Argentinian PDPA	EU Model Clauses	UK G-Cloud	China DJCP	China GB 18030	China TRUCS	Singapore MTCS	Australia IRAP/CCSL	New Zealand GCIO	Japan My Number Act	ENISA IAF	Japan CS Mark Gold	Spain ENS	Spain DPA	India MeitY	Canada Privacy Laws	Germany IT Grundschutz workbook

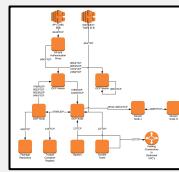
DON'T START FROM SCRATCH



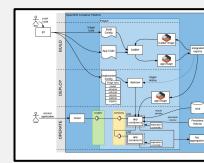
LOGICAL COMPONENT
BLOCK DIAGRAM



CONTROLLED
INTERFACE
DIAGRAM



PHYSICAL
CONNECTIVITY
DIAGRAM



ROLE
BASED
ACTIVITY
DIAGRAM



ROLE TO
COMPONENT
ALLOCATION

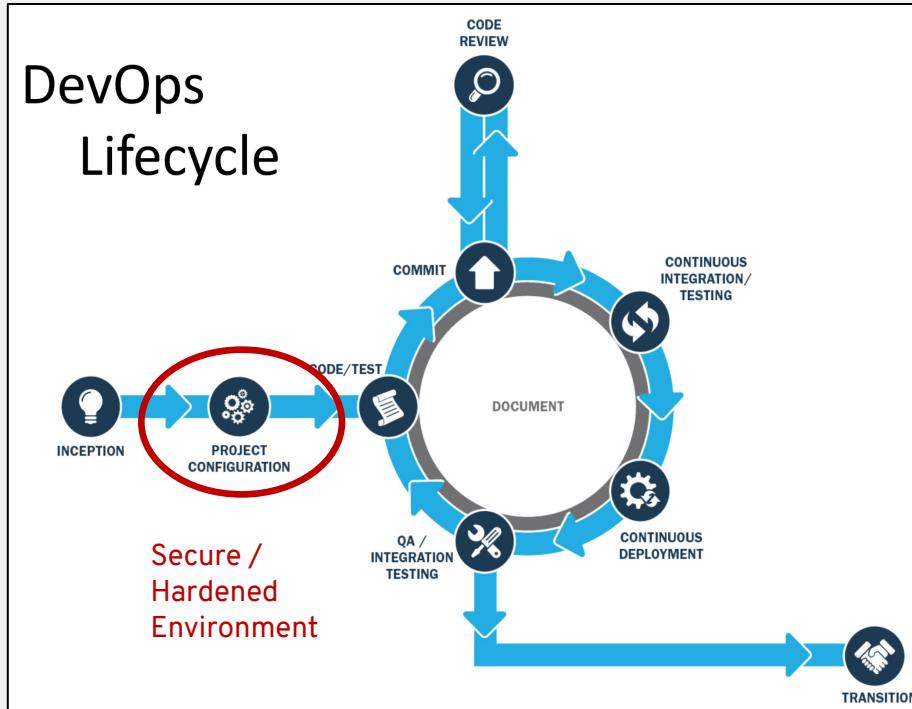


CUSTOM
ANSIBLE
ROLES



CENTRALIZED
ARTIFACTS

ADOPT A SECURITY INHERITANCE MODEL



DEPLOYING A SECURE SOFTWARE FACTORY



REPOSITORIES



RED HAT[®]
ANSIBLE[®]
Automation

UBIQUITOUS AUTOMATION

DEPLOYING A SECURE SOFTWARE FACTORY



REPOSITORIES



RED HAT[®]
OPENSTACK[®]
PLATFORM

RED HAT[®]
ENTERPRISE
VIRTUALIZATION

RED HAT[®]
GLUSTER STORAGE

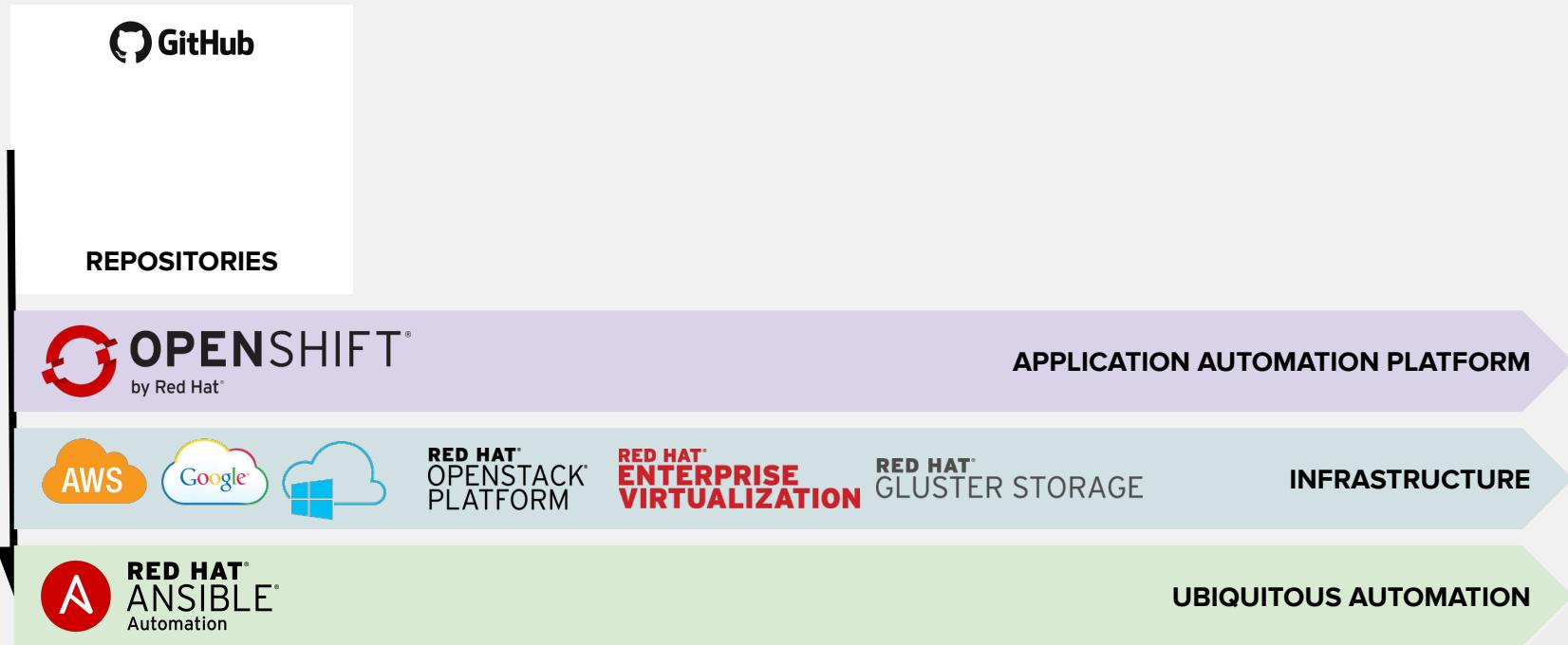
INFRASTRUCTURE



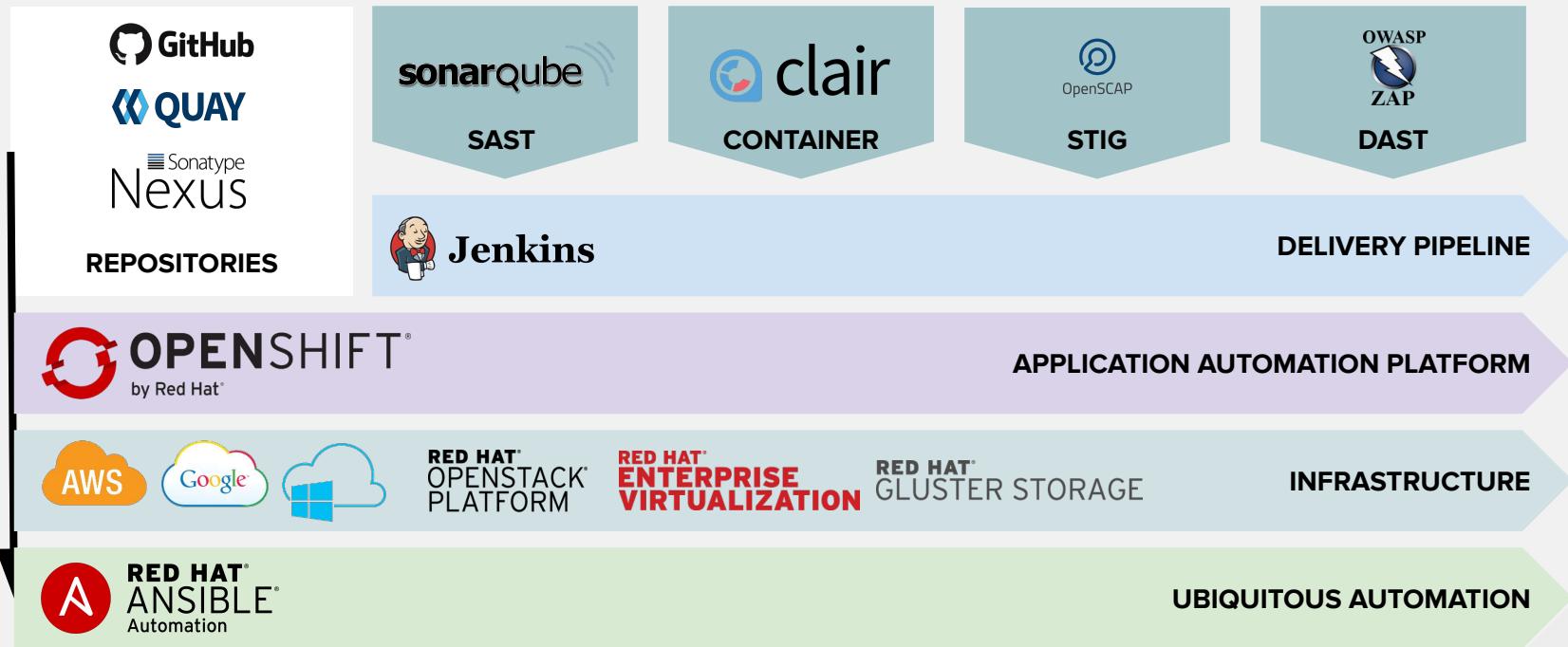
RED HAT[®]
ANSIBLE[®]
Automation

UBIQUITOUS AUTOMATION

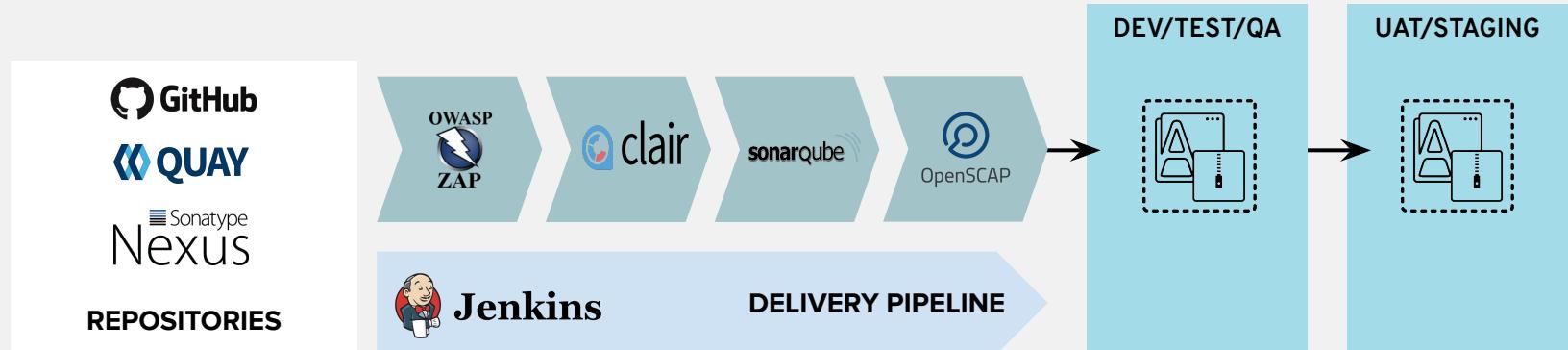
DEPLOYING A SECURE SOFTWARE FACTORY



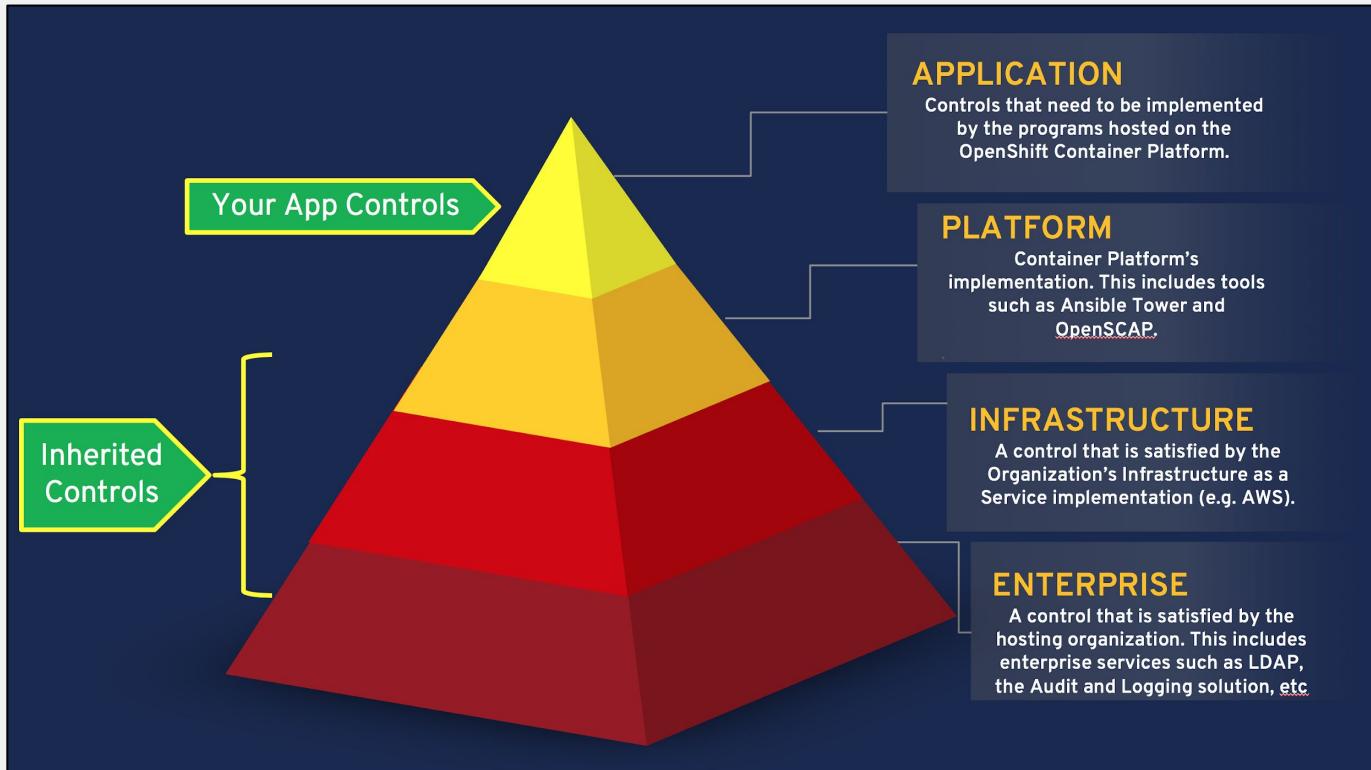
DEPLOYING A SECURE SOFTWARE FACTORY

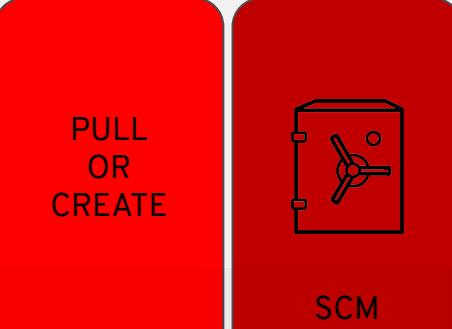
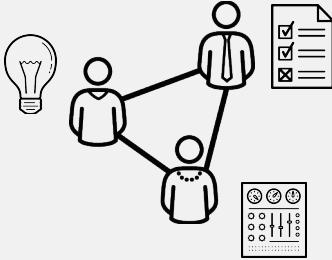


EXERCISING A SECURE SOFTWARE FACTORY



SECURITY INHERITANCE MODEL





BUILD

LOAD

SCAN

SIGN



DEV

INSPECT

BUILD

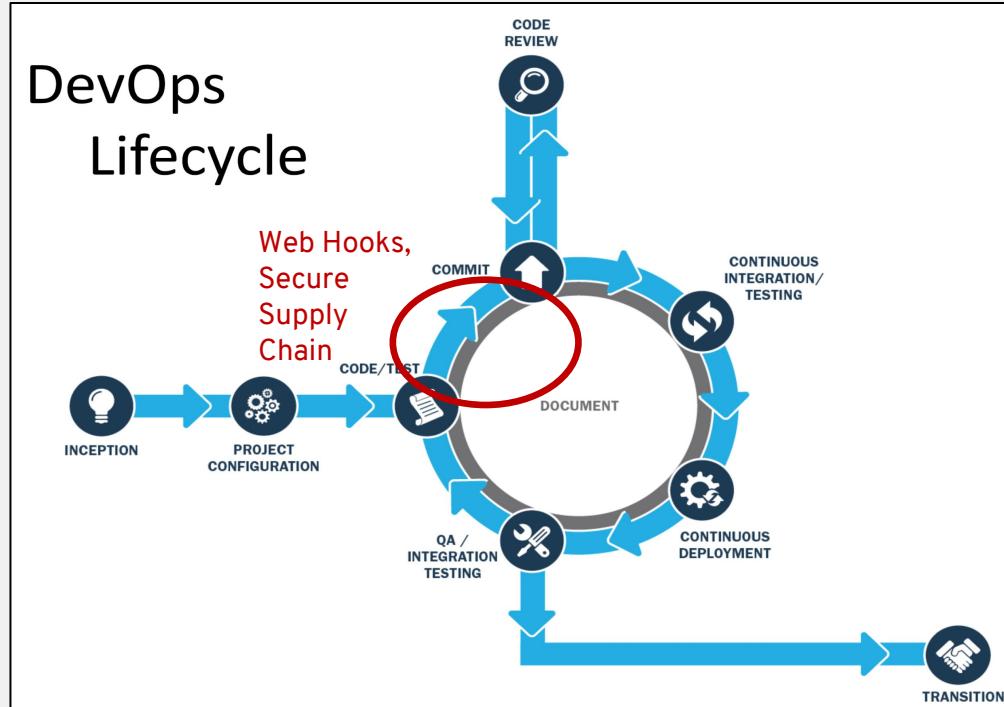
SCAN

TEST

DEPLOY

MONITOR

ONLY INTRODUCE "APPROVED" ELEMENTS



CONTAINERS START WITH QUALITY PARTS

What goes into your secure software supply chain? Red Hat provides:

- Manual inspection
- Automated inspection
- Packaging Guidelines
- Build Roots
- Quality Assurance
- Certifications
- Signing
- Distribution
- Response
- Support
- Security Updates

The image shows two screenshots of Red Hat's container management tools. The top screenshot is the 'Red Hat Container Catalog' displaying 'Java Applications'. It shows a timeline from March to April 2017 with three tags: 1.0-2 (RHEA-2017-029), 1.0-3 (RHBA-2017-168), and 1.0-2 (RHEA-2017-0291). The 1.0-3 tag is highlighted. To the right is a 'Health Index A' grid with six columns labeled A through F. The bottom screenshot is the 'RED HAT CONTAINER REGISTRY' showing 'Images pushed recently'. It lists several images across different projects, each with a timestamp of '24 days ago'.

Red Hat Container Catalog

Java Applications

by Red Hat, Inc. | in Product Red Hat OpenShift Container Platform

registry.access.redhat.com/redhat-openjdk-18/openjdk18-openshift Updated 7 days ago 1.0-3 : Health Index A

Tag Name Date Pushed Image Advisory Health Index Docker Image ID

1.0-2 7 days ago RHBA-2017-168 A af2b44054a5d

1.0-2 2 months ago RHEA-2017-0291 C 0e4b6c3a7491

RED HAT CONTAINER REGISTRY

Images by project

default

dumb

kube-system

logging

management-infra

openshift

openshift-infra

Images pushed recently

domestic-image-policy-check 24 days ago

default-registry-console 24 days ago

openshift/rhel7-180-openshift 24 days ago

openshift/rhoss-amp42 24 days ago

openshift/rhoss-amp42 24 days ago

openshift/rhoss-datavirt3-openshift 24 days ago

openshift/rhoss-datavirt3-openshift 24 days ago

openshift/rhoss-processserver83-openshift 24 days ago

openshift/rhoss-processserver83-openshift 24 days ago

OPENSHIFT SECURE REGISTRY

THE VALUE OF TRUSTED CONTENT

Red Hat Registry Stats

- 227 repositories
- 2,169 images
- 1+ TB storage



Red Hat Security Statistics 2016

- 97 critical RHSA
- 286 important RHSA
- 100% fixed in <1d



Red Hat Customer Portal Stats 2016

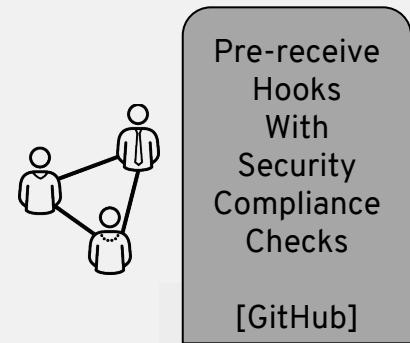
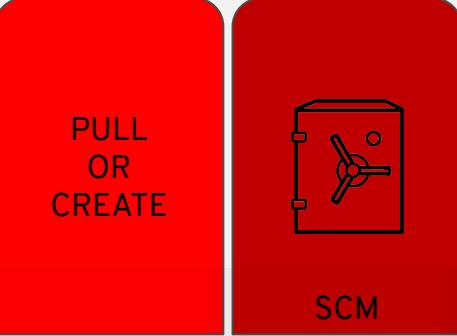
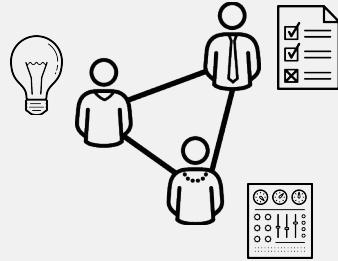
- 13,100,000 visitors
- 2,400,000 searches
- 108,300,000 views



- Image Documentation
- Image Advisories

- Container Health Index
- Extensive Image Metadata

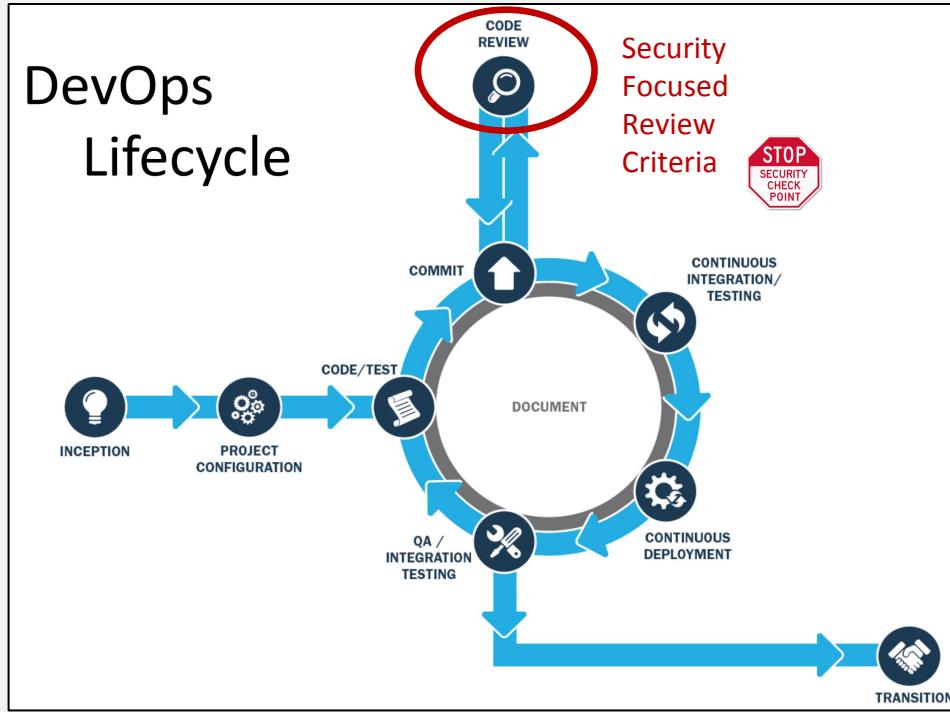
**RED HAT®
CONTAINER
CATALOG**

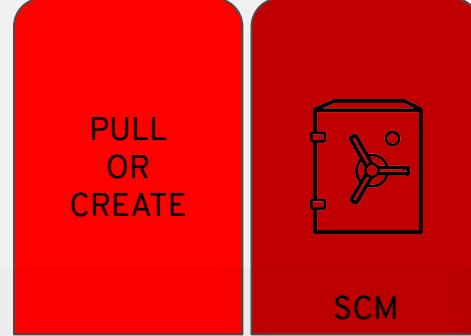
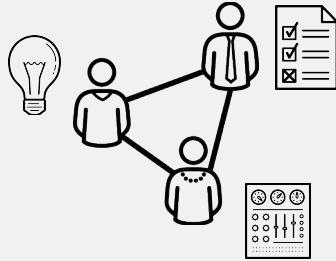


Pre-receive
Hooks
With
Security
Compliance
Checks
[GitHub]

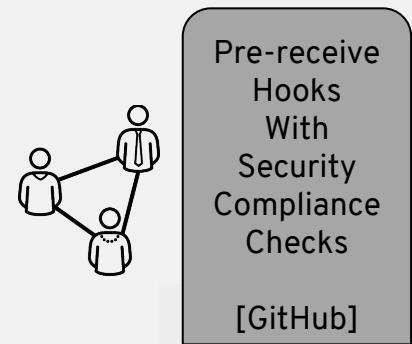


AUTOMATE WHAT YOU CAN & BUILD TRUST





BUILD LOAD SCAN SIGN



Code Review

DEV INSPECT BUILD SCAN TEST DEPLOY MONITOR

DEMO OUTPUT FOR PIPELINE INVOCATION POST CODE REVIEW

OPENShift CONTAINER PLATFORM

Labs CI/CD Pipelines [Learn More](#)

[ci-for-labs-ci-cd-pipeline](#) created a month ago

Source Repository: <https://github.com/posip-redhat/labs-ci-cd.git>
No pipeline builds have run for ci-for-labs-ci-cd-pipeline. View the file [Jenkinsfile](#) in the source repository to see what stages will run.

[Start Pipeline](#)

[java-app-pipeline](#) created a month ago

Source Repository: <https://github.com/c2c24/sampleJavaApp>

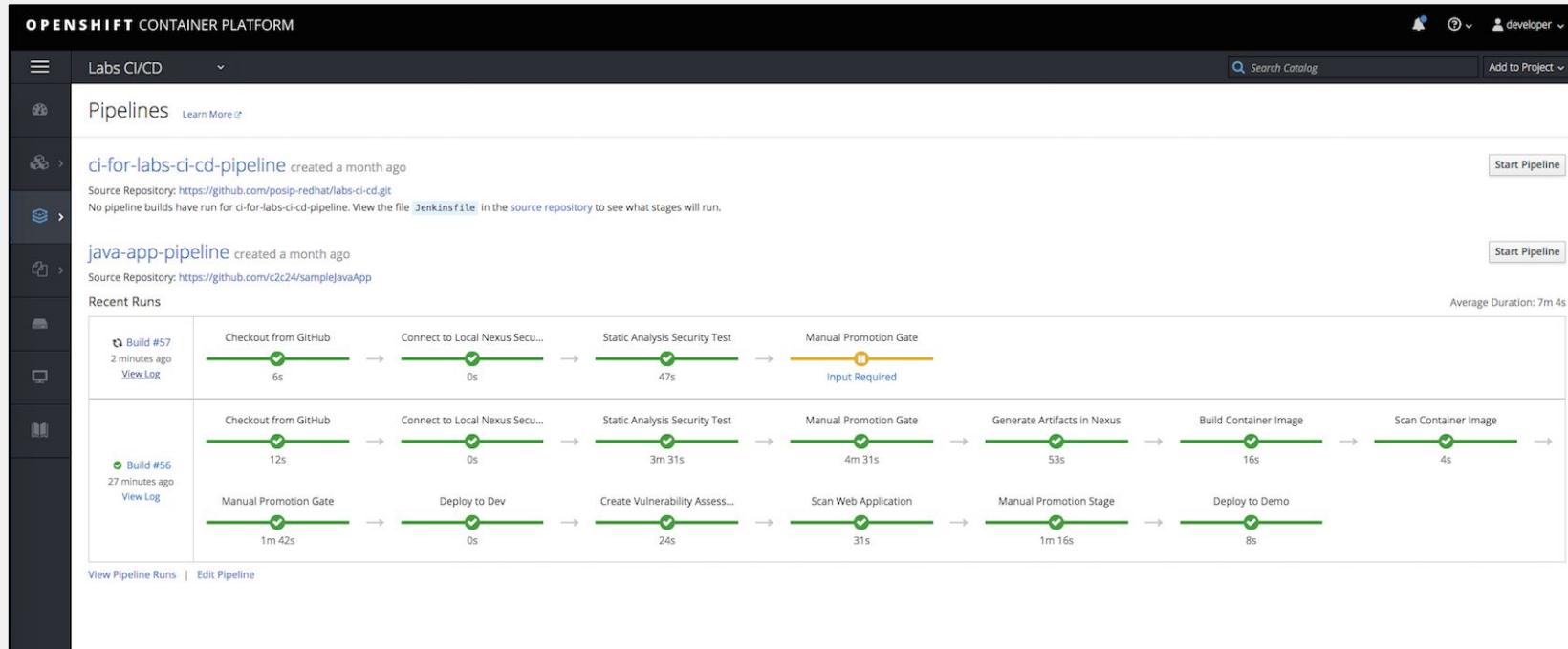
Average Duration: 7m 4s

Recent Runs

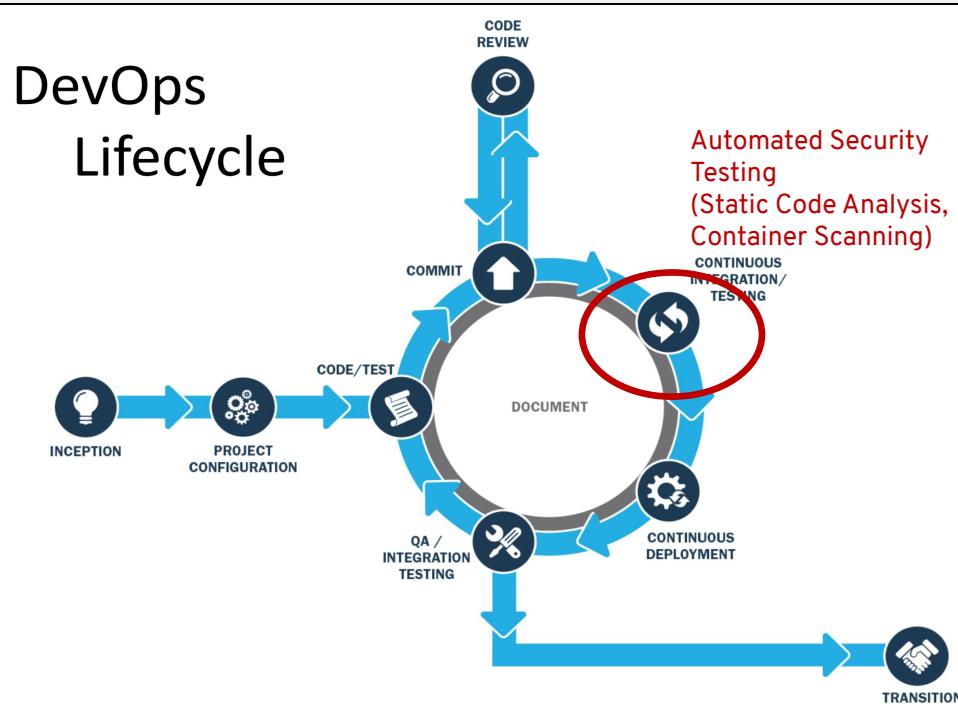
Build #57	Checkout from GitHub	Connect to Local Nexus Secu...	Static Analysis Security Test	Manual Promotion Gate
2 minutes ago View Log	6s	0s	47s	Input Required

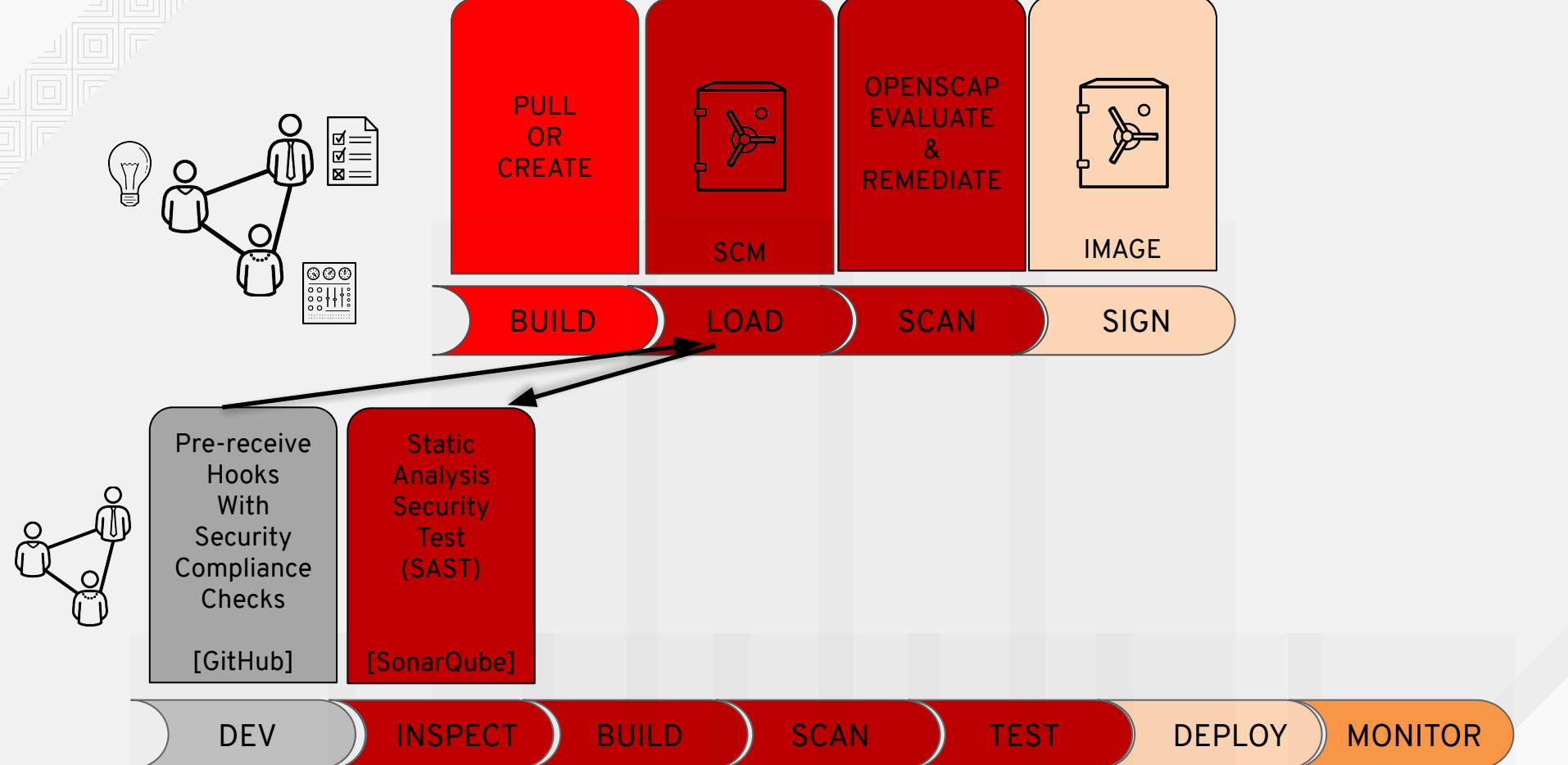
Build #56	Checkout from GitHub	Connect to Local Nexus Secu...	Static Analysis Security Test	Manual Promotion Gate	Generate Artifacts in Nexus	Build Container Image	Scan Container Image
27 minutes ago View Log	12s	0s	3m 31s	4m 31s	53s	16s	4s
Manual Promotion Gate	Deploy to Dev	Create Vulnerability Assess...	Scan Web Application	Manual Promotion Stage	Deploy to Demo		
1m 42s	0s	24s	31s	1m 16s	8s		

[View Pipeline Runs](#) | [Edit Pipeline](#)



DON'T WASTE COMPUTE OR TIME





OUTPUT FOR STATIC ANALYSIS ([LINK](#))

SonarQube Projects Issues Rules Quality Profiles Quality Gates Administration

Search for projects, sub-projects and files... A

automation-api master

Overview Issues Measures Code Activity Administration

Quality Gate Passed

Bugs 0 A Vulnerabilities 0 A Leak Period: since previous version started last month

0 Bugs 0 Vulnerabilities 0 New Bugs 0 New Vulnerabilities

Code Smells 0 A Debt 0 Code Smells 0 A New Debt 0 New Code Smells

started last month

Coverage 0.0% Coverage on New Code

0.0% Coverage

Duplications 2.4% Duplicated Blocks 6 Duplications on 0.0% New Lines 0.0% Duplication on 5 New Lines

Parent pom providing dependency and plugin management for applications built with Maven

8 3.7k Java 3.5k Lines of Code XML 197

No tags

Activity

May 15, 2018 0.4-SNAPSHOT Quality Gate: Green (was Orange)

May 15, 2018 Quality Gate: Orange (was Red)

May 15, 2018 Quality Gate: Red (was Orange)

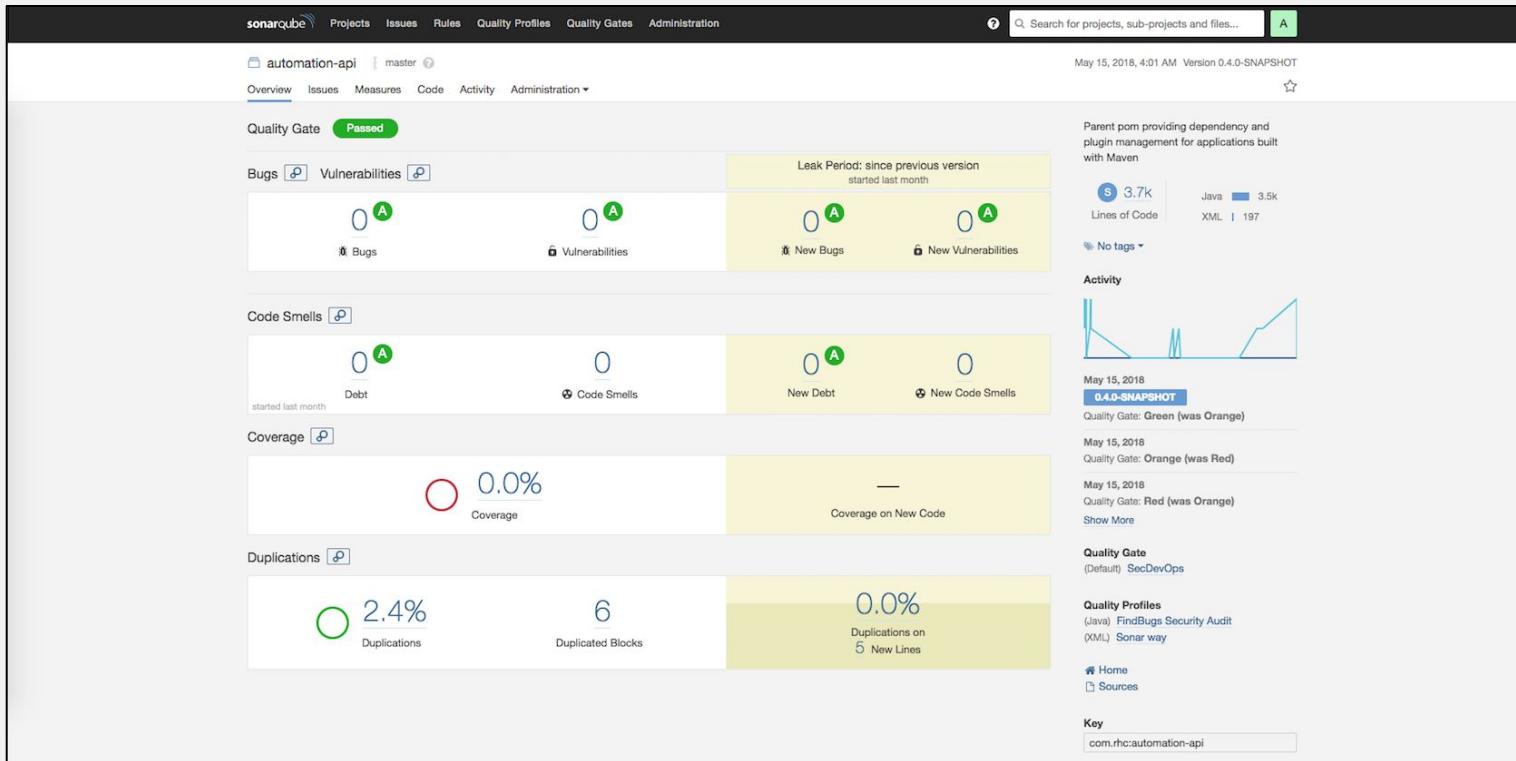
Show More

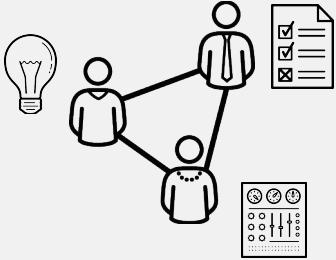
Quality Gate (Default) SecDevOps

Quality Profiles (Java) FindBugs Security Audit (XML) Sonar way

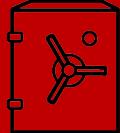
Home Sources

Key com.rhc:automation-api



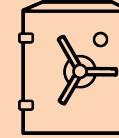


PULL
OR
CREATE



SCM

OPENSCLP
EVALUATE
&
REMEDIATE



IMAGE

BUILD

LOAD

SCAN

SIGN

Pre-receive
Hooks
With
Security
Compliance
Checks
[GitHub]

Static
Analysis
Security
Test
(SAST)
[SonarQube]

Policy
Enforcement
For
Build
Artifacts
& Images
[OCP]

DEV

INSPECT

BUILD

SCAN

TEST

DEPLOY

MONITOR

OUTPUT FOR OPENSCAP IMAGE SCAN FROM PIPELINE ([LINK](#))

OPENSHIFT CONTAINER PLATFORM

Labs CI/CD

Pipelines [Learn More](#)

ci-for-labs-ci-cd-pipeline created a month ago

Source Repository: <https://github.com/posip-redhat/labs-ci-cd.git>

No pipeline builds have run for ci-for-labs-ci-cd-pipeline. View the file [Jenkinsfile](#) in the source repository to see what stages will run.

Start Pipeline

java-app-pipeline created a month ago

Source Repository: <https://github.com/c2c24/sampleJavaApp>

Start Pipeline

Average Duration: 7m 0s

Recent Runs

Build #58 3 minutes ago View Log	Checkout from GitHub 6s	Connect to Local Nexus Secu... 0s	Static Analysis Security Test 48s	Manual Promotion Gate 59s	Generate Artifacts in Nexus 25s	Build Container Image 14s	Scan Container Image 4s

Build #57
9 minutes ago
[View Log](#)

Checkout from GitHub
6s

Connect to Local Nexus Secu...
0s

Static Analysis Security Test
47s

Manual Promotion Gate
2m 11s

Input Required

[View Pipeline Runs](#) | [Edit Pipeline](#)

DEMO OUTPUT FOR OPENSCAP IMAGE SCAN

Score

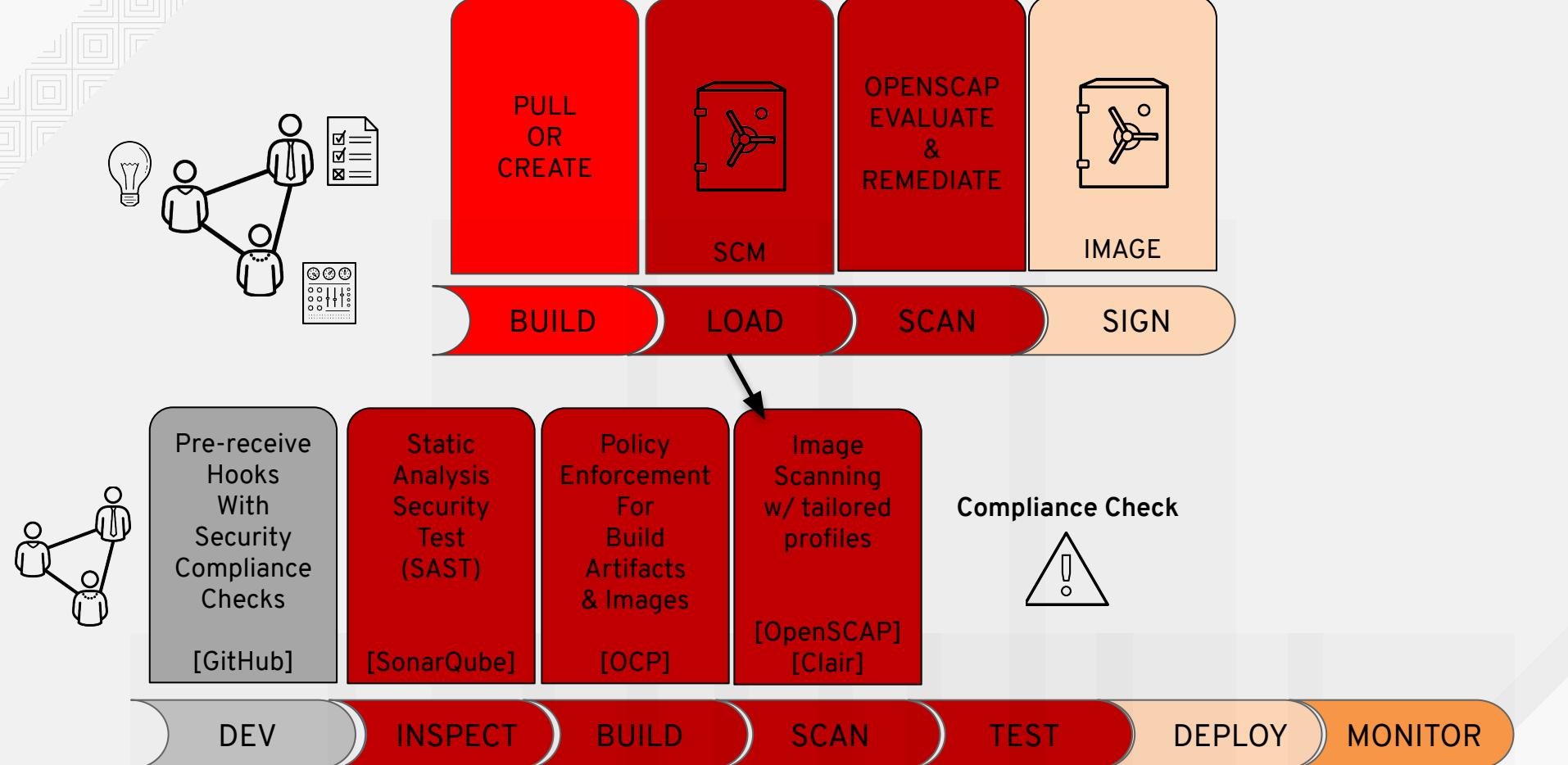
Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	98.067635	100.000000	98.07%

Rule Overview

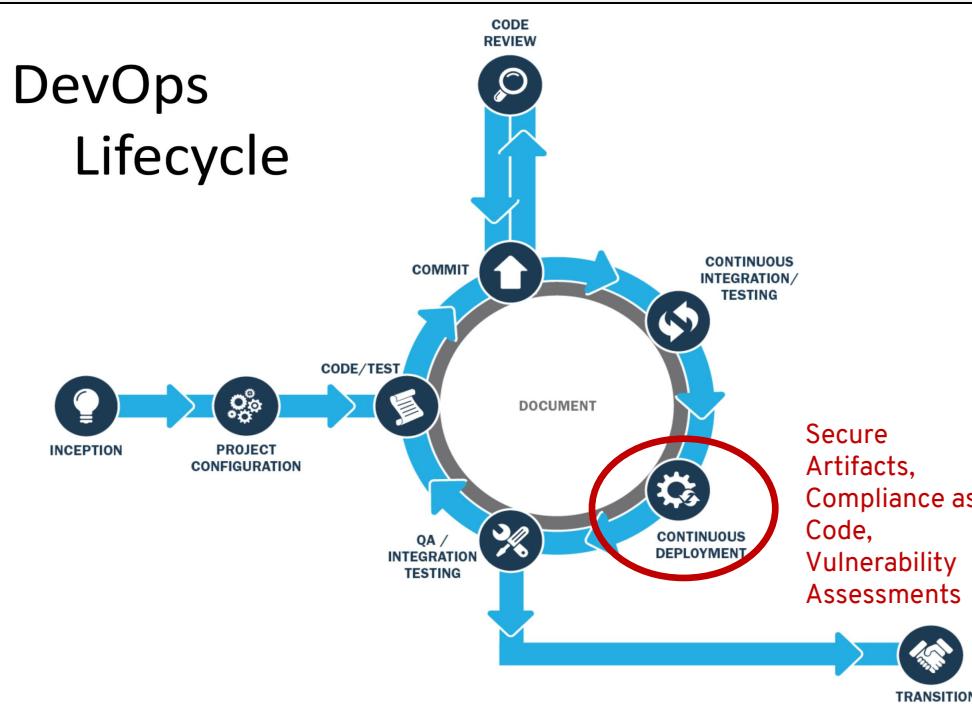
pass fail notchecked
 fixed error notapplicable
 informational unknown

Search through XCCDF rules Search
Group rules by: Default

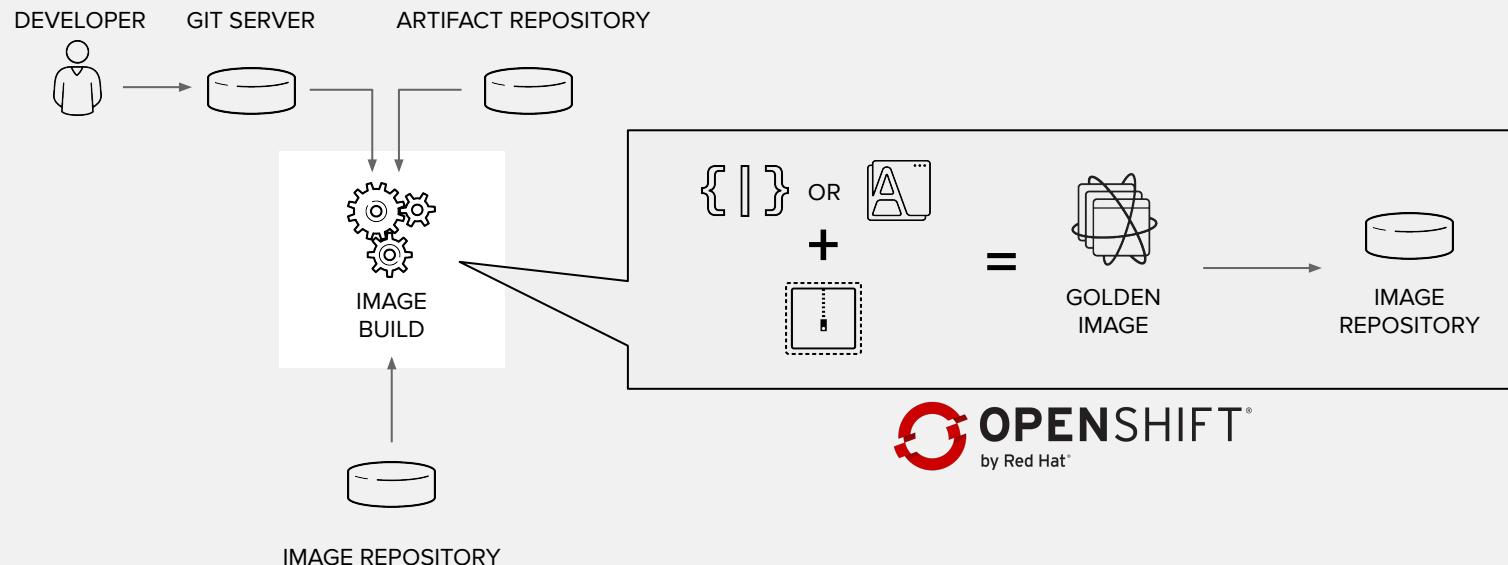
Title	Severity	Result
Automatically generated XCCDF from OVAL file: com.redhat.rhsa-RHEL7.xml 12x fail		
RHSA-2014:0675: java-1.7.0-openjdk security update (Critical)	high	pass
RHSA-2014:0678: kernel security update (Important)	high	pass
RHSA-2014:0679: openssl security update (Important)	high	pass
RHSA-2014:0680: openssl098e security update (Important)	high	pass
RHSA-2014:0684: gnutls security update (Important)	high	pass
RHSA-2014:0685: java-1.6.0-openjdk security update (Important)	high	pass
RHSA-2014:0686: tomcat security update (Important)	high	pass
RHSA-2014:0687: libtasn1 security update (Moderate)	medium	pass
RHSA-2014:0702: mariadb security update (Moderate)	medium	pass
RHSA-2014:0703: json-c security update (Moderate)	medium	pass



POLICY DRIVEN DEPLOY AND COMPLIANCE



BUILDING APPLICATION ON OPENSHIFT



VULNERABILITY ASSESSMENT FROM PIPELINE ([LINK](#))

OPENShift CONTAINER PLATFORM

Labs CI/CD

Pipelines Learn More ↗

ci-for-labs-ci-cd-pipeline created a month ago

Source Repository: <https://github.com/posip-redhat/labs-ci-cd.git>

No pipeline builds have run for ci-for-labs-ci-cd-pipeline. View the file `Jenkinsfile` in the source repository to see what stages will run.

[Start Pipeline](#)

java-app-pipeline created a month ago

Source Repository: <https://github.com/c2c24/sampleJavaApp>

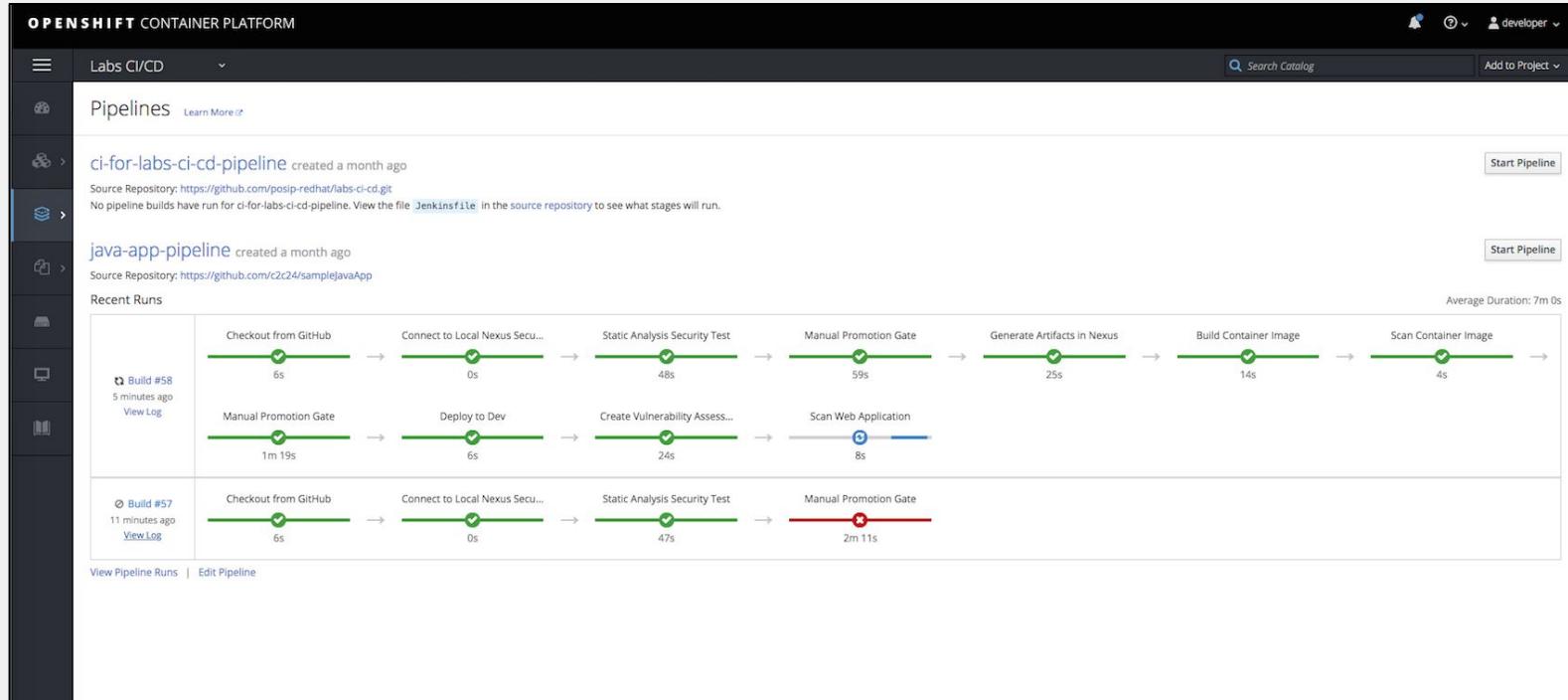
Average Duration: 7m 0s

Recent Runs

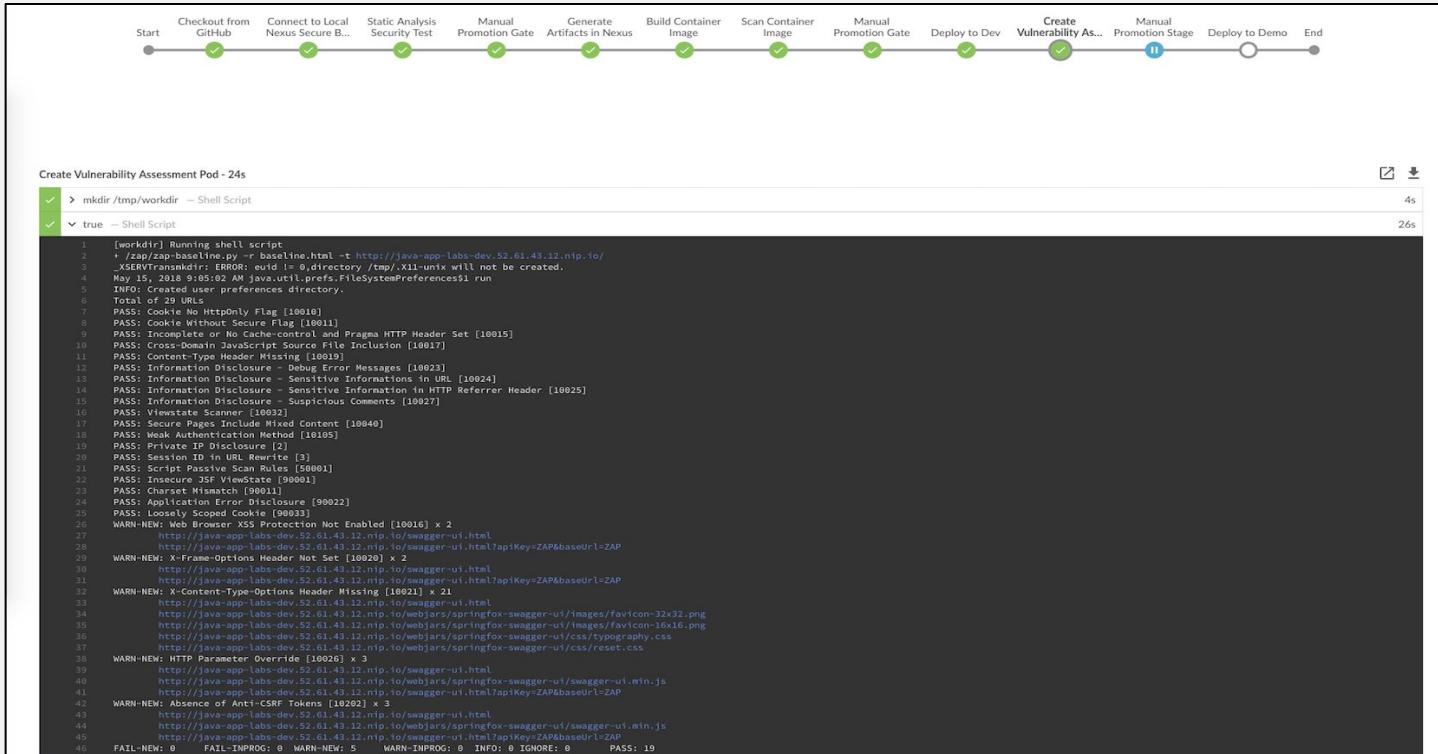
	Checkout from GitHub	Connect to Local Nexus Secu...	Static Analysis Security Test	Manual Promotion Gate	Generate Artifacts in Nexus	Build Container Image	Scan Container Image
Build #58 5 minutes ago View Log	6s	0s	48s	59s	25s	14s	4s
	Manual Promotion Gate	Deploy to Dev	Create Vulnerability Assess...	Scan Web Application			
	1m 19s	6s	24s	8s			

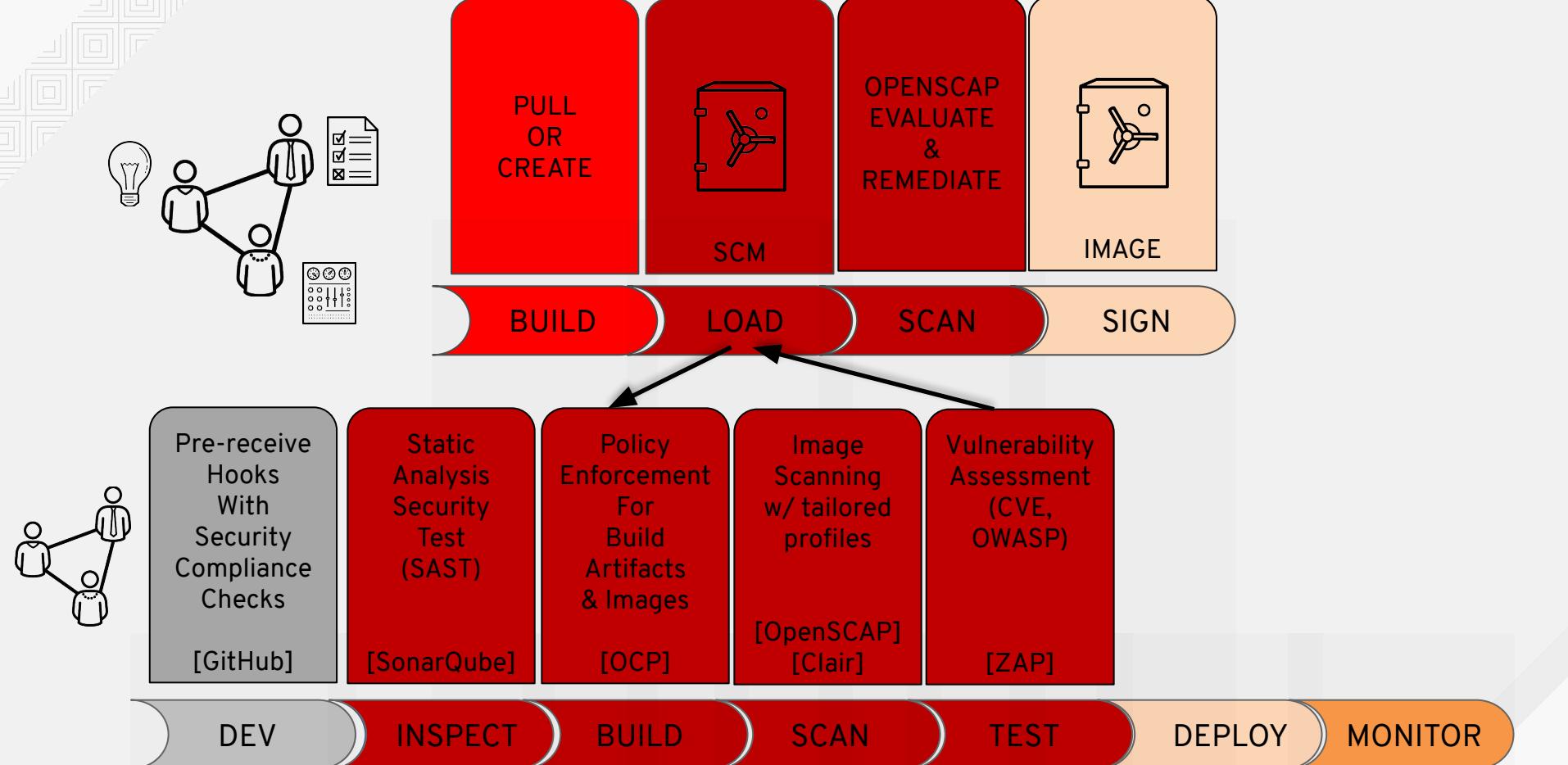
	Checkout from GitHub	Connect to Local Nexus Secu...	Static Analysis Security Test	Manual Promotion Gate
Build #57 11 minutes ago View Log	6s	0s	47s	2m 11s

[View Pipeline Runs](#) | [Edit Pipeline](#)

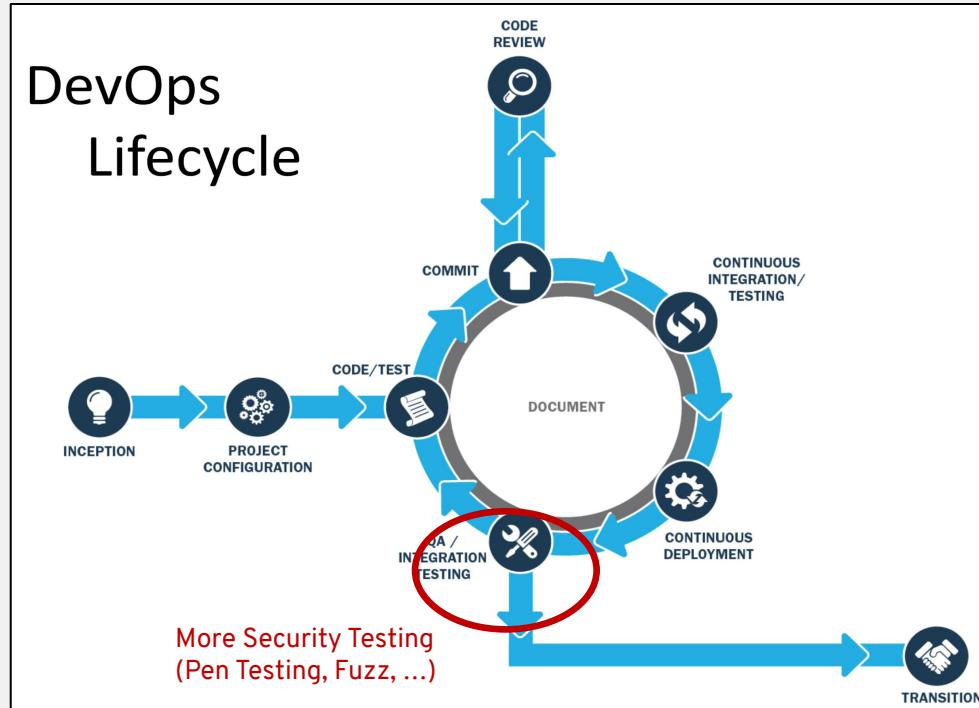


DEMO OUTPUT FOR VULNERABILITY ASSESSMENT

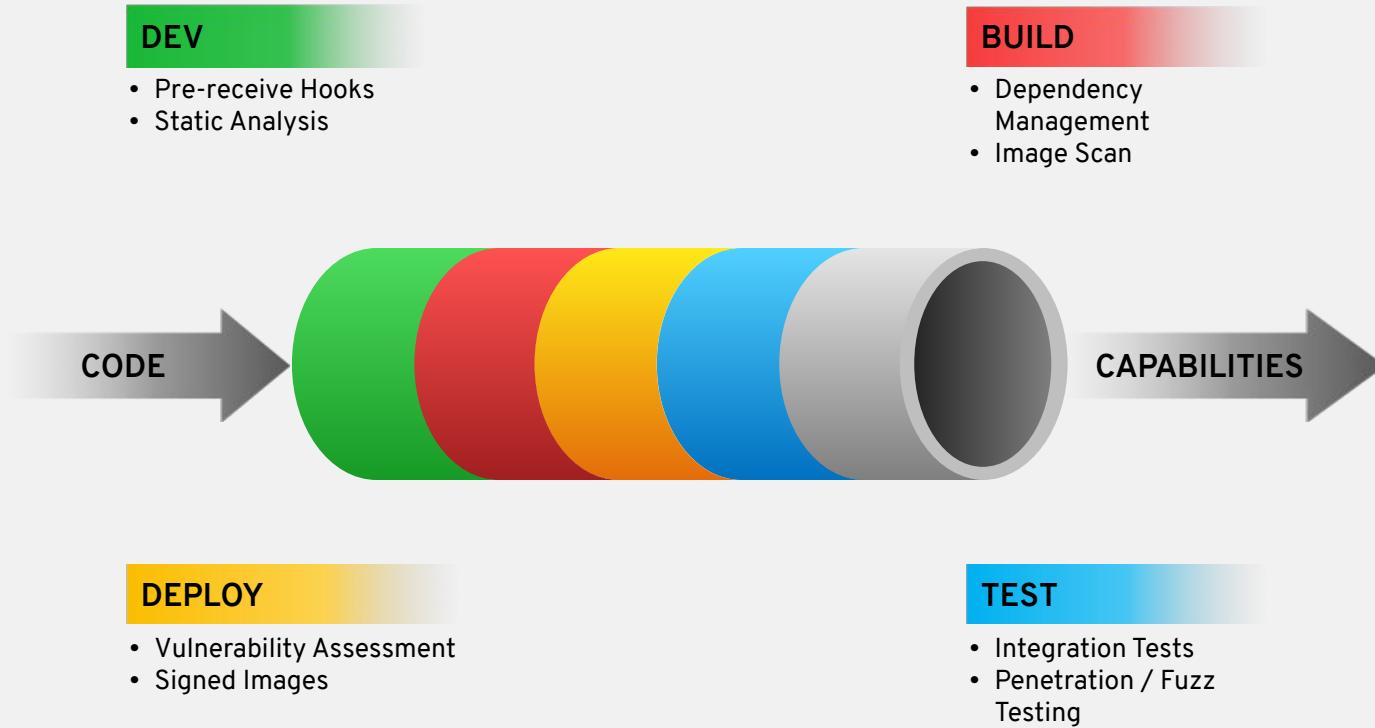




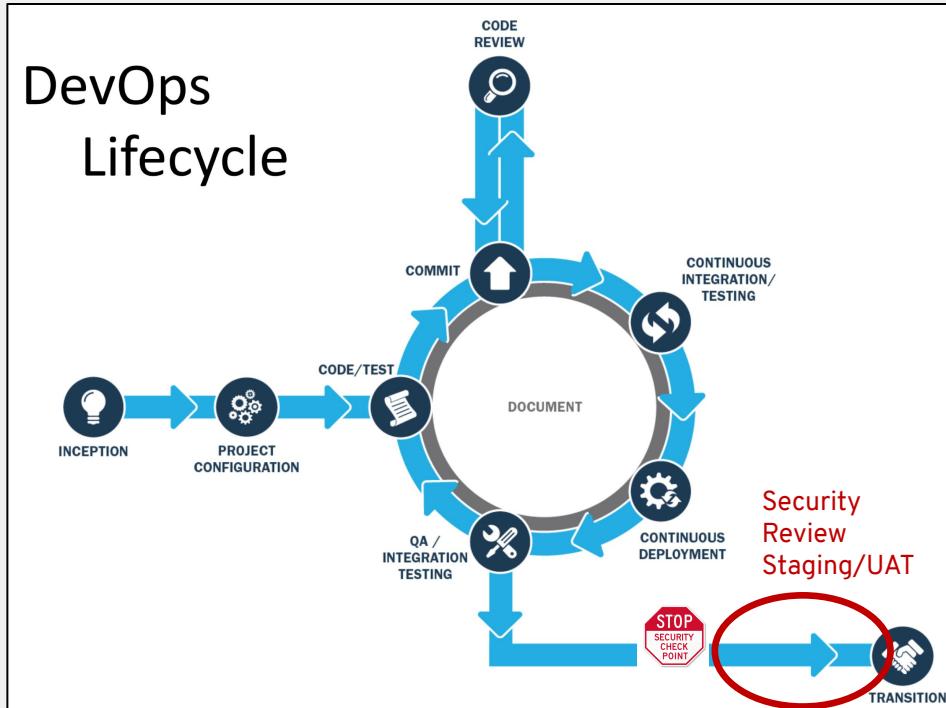
WHAT GETS MEASURED GETS IMPROVED



FROM CODE TO CAPABILITIES



CONTINUE TO BUILD TRUST AND AUTOMATE



From All Day DevOps Webinar Nov 2016, Content distributable from Carnegie Mellon

OUTPUT OF COMPLETED PIPELINE ([LINK](#))

OPENSOURCE CONTAINER PLATFORM

Labs CI/CD

Pipelines [Learn More ↗](#)

ci-for-labs-ci-cd-pipeline created a month ago

Source Repository: <https://github.com/posip-redhat/labs-ci-cd.git>

No pipeline builds have run for ci-for-labs-ci-cd-pipeline. View the file `Jenkinsfile` in the source repository to see what stages will run.

[Start Pipeline](#)

java-app-pipeline created a month ago

Source Repository: <https://github.com/c2c24/sampleJavaApp>

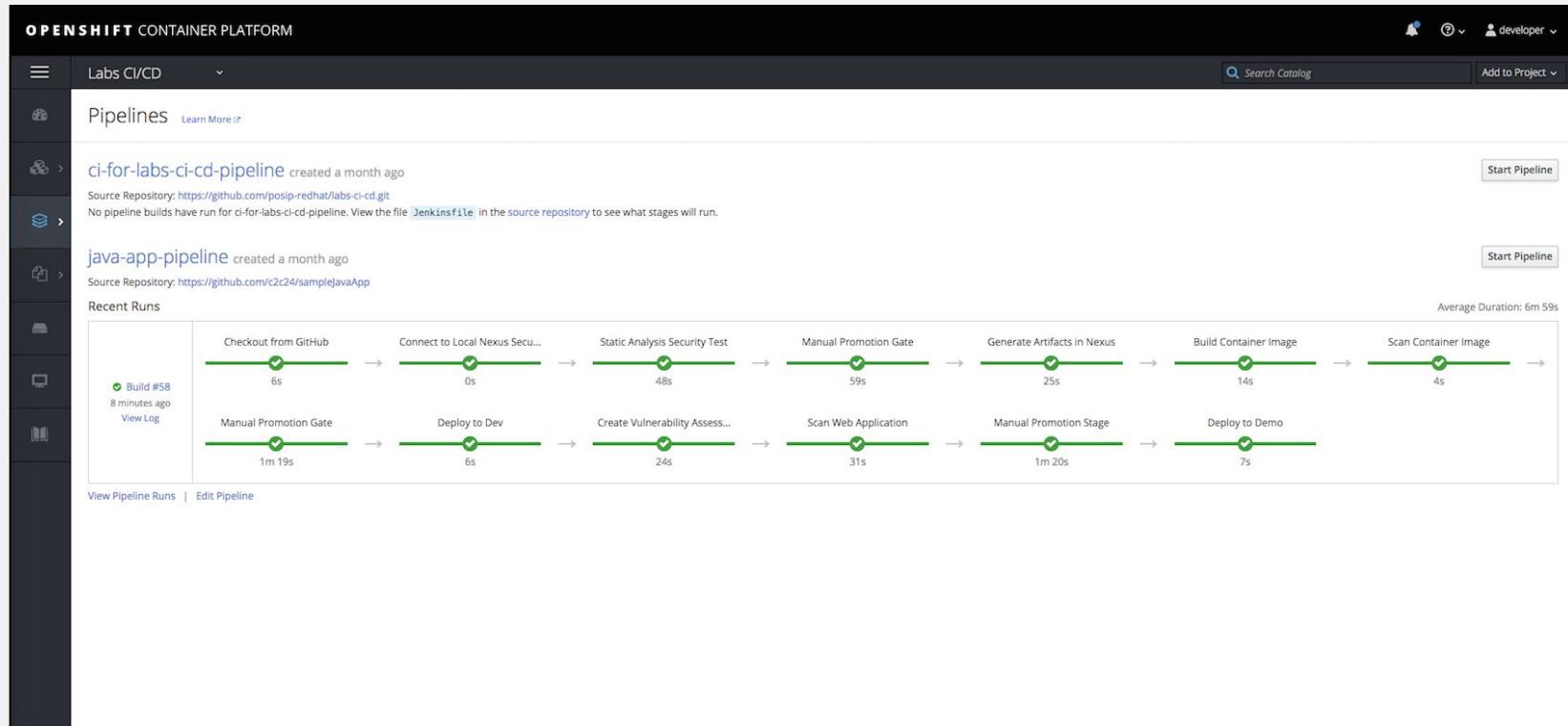
[Start Pipeline](#)

Average Duration: 6m 59s

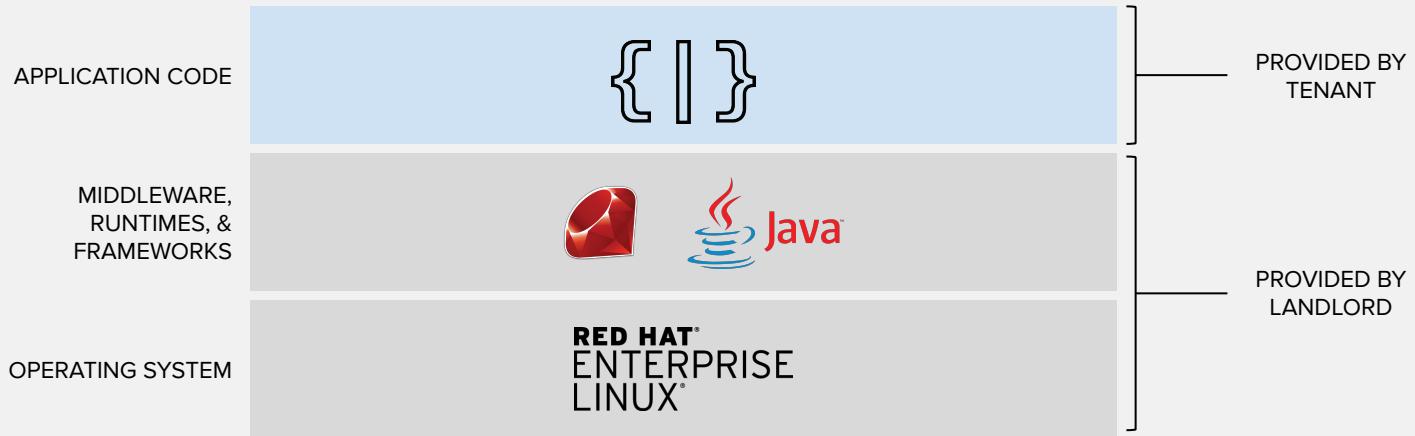
Recent Runs

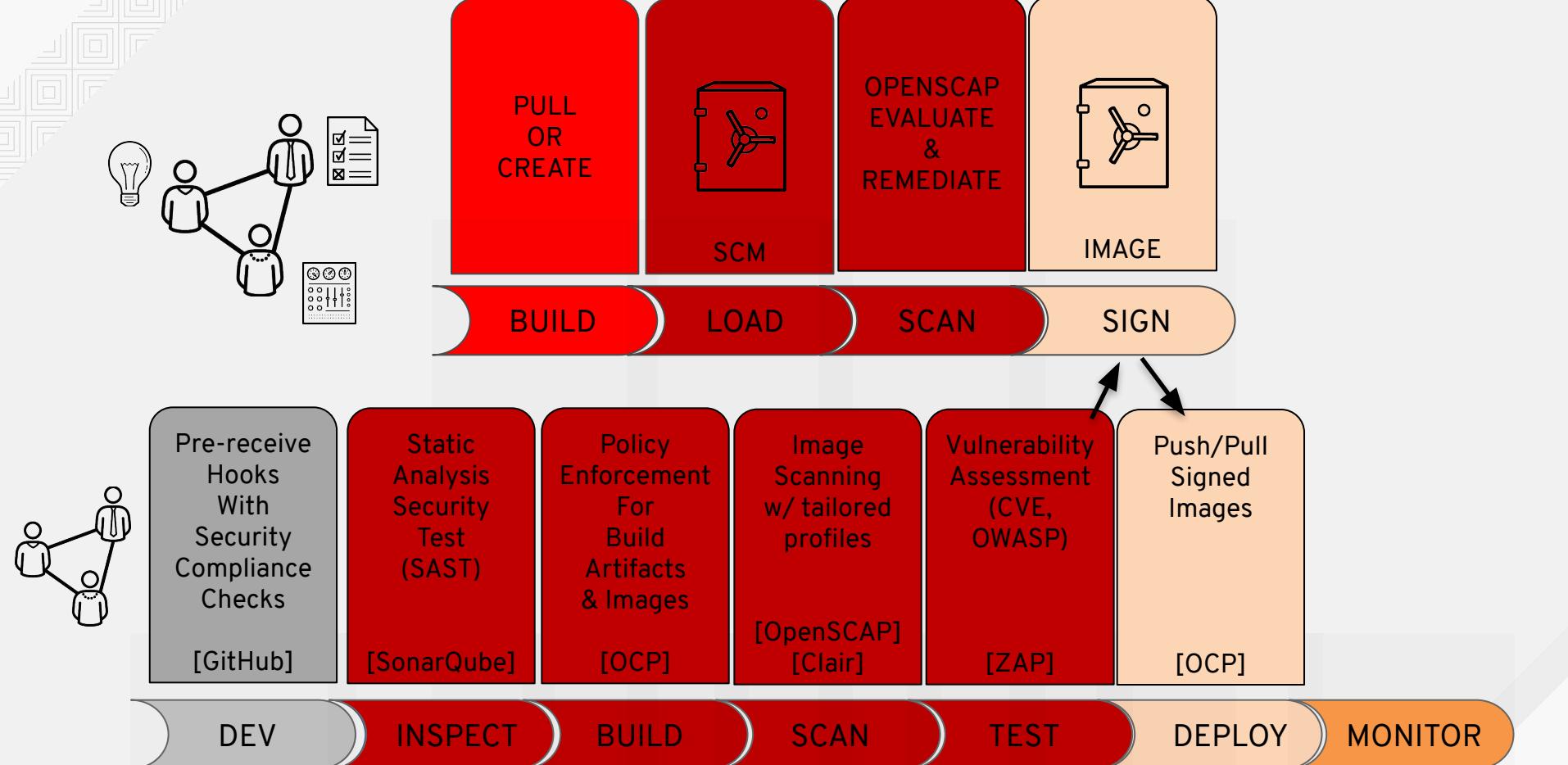
	Checkout from GitHub	Connect to Local Nexus Secu...	Static Analysis Security Test	Manual Promotion Gate	Generate Artifacts in Nexus	Build Container Image	Scan Container Image
Build #58 8 minutes ago View Log	6s	0s	48s	59s	25s	14s	4s
	Manual Promotion Gate	Deploy to Dev	Create Vulnerability Assess...	Scan Web Application	Manual Promotion Stage	Deploy to Demo	
	1m 19s	6s	24s	31s	1m 20s	7s	

[View Pipeline Runs](#) | [Edit Pipeline](#)

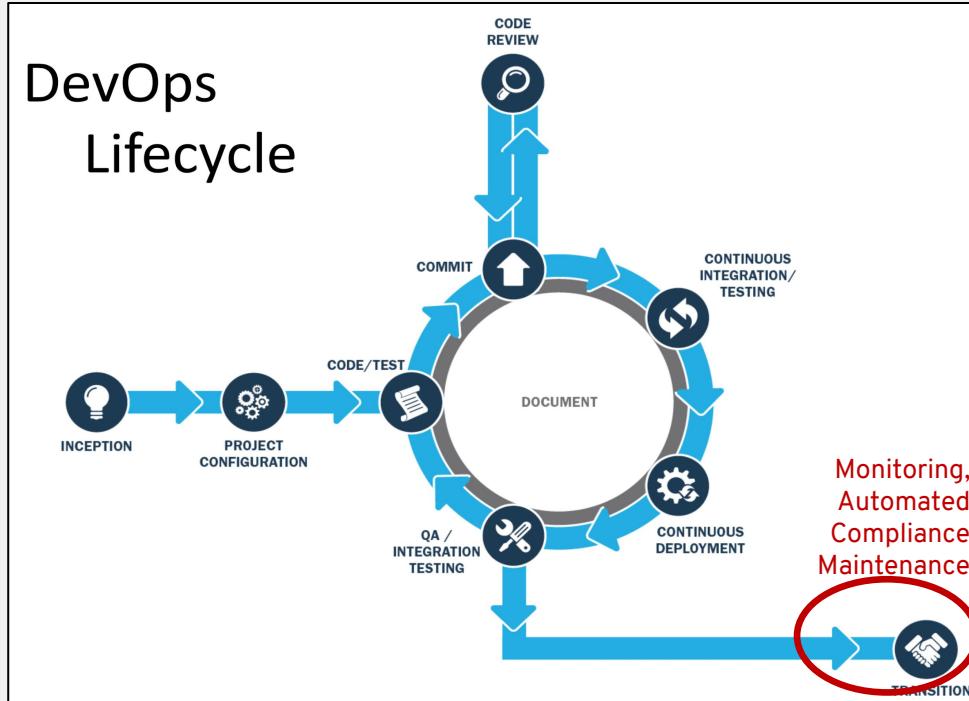


THE GOLDEN IMAGE

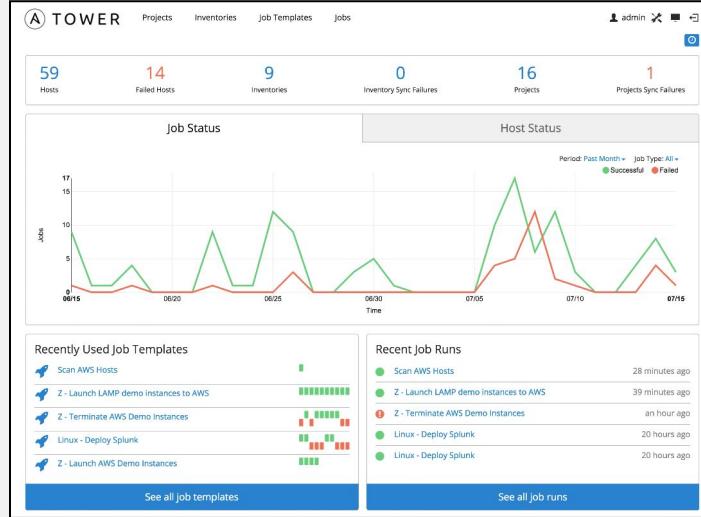




ITERATIVE SECURE DEPLOYMENTS

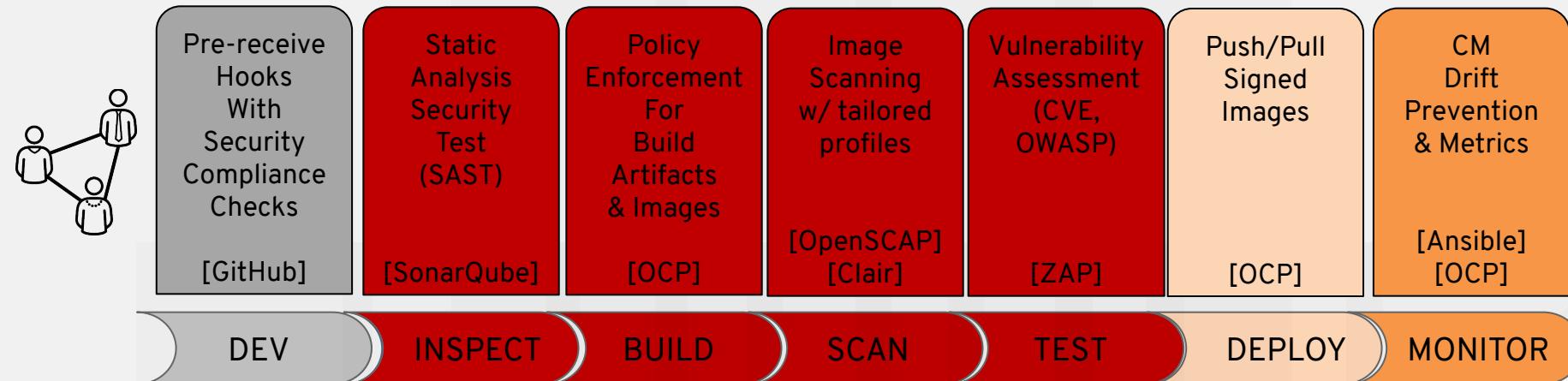
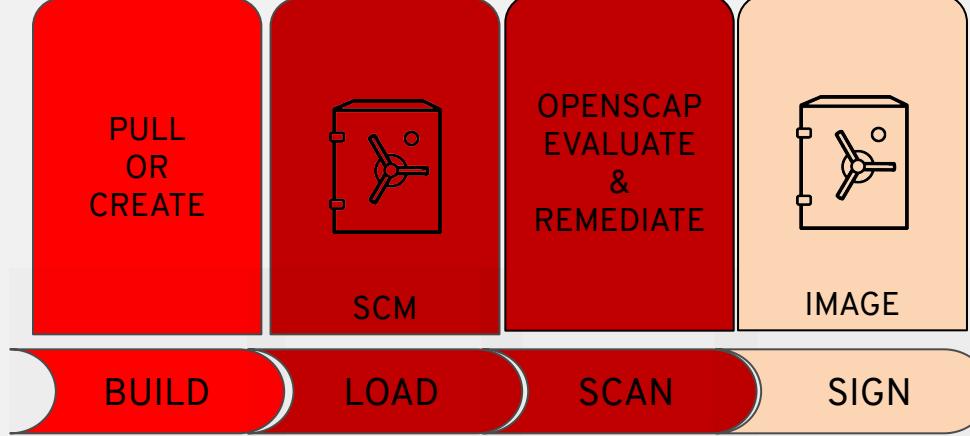
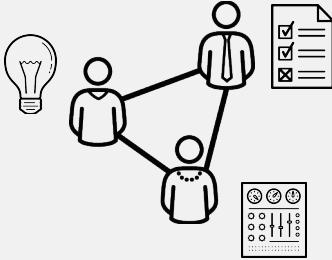


DAY-2 OPERATIONS SAMPLE VIEW FROM ANSIBLE TOWER

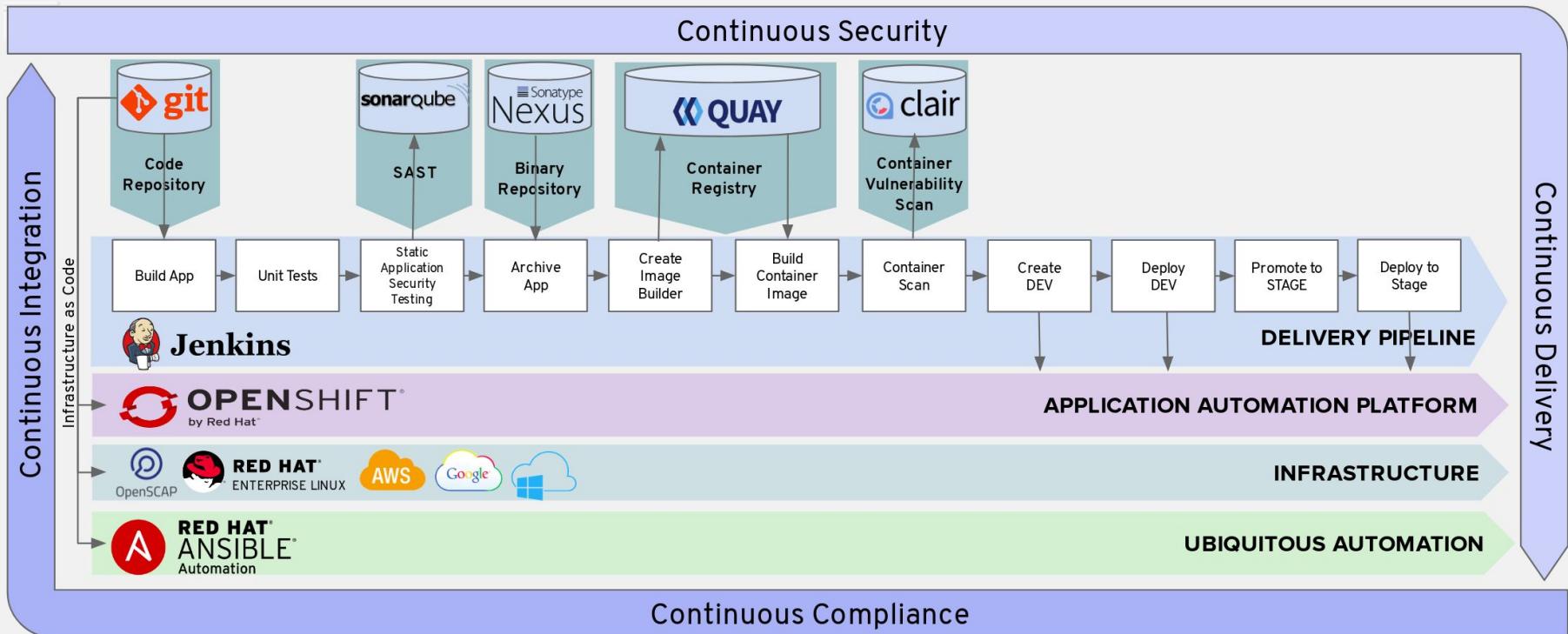


ENSURES SOFTWARE SYSTEMS WORK AS ADVERTISED

- Automate compliance with Ansible
- Red Hat Gov GitHub has an 800-53 role that you can use to apply STIG settings
- <https://github.com/RedHatGov/ansible-role-800-53>
- **Configuration Drift?** No problem. Rerun the playbook for continuous compliance



THE SECURE SOFTWARE FACTORY





redhat.

THANK YOU



plus.google.com/+RedHat



linkedin.com/company/red-hat



youtube.com/user/RedHatVideos



facebook.com/redhatinc



twitter.com/RedHatNews