
# 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

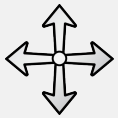
HOLISTIC VIEW: The Technology of the Solution

STARTER PACK: DevSecOps CI/CD Pipeline

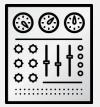
# DIGITAL TRANSFORMATION NEEDS

Speed / Security

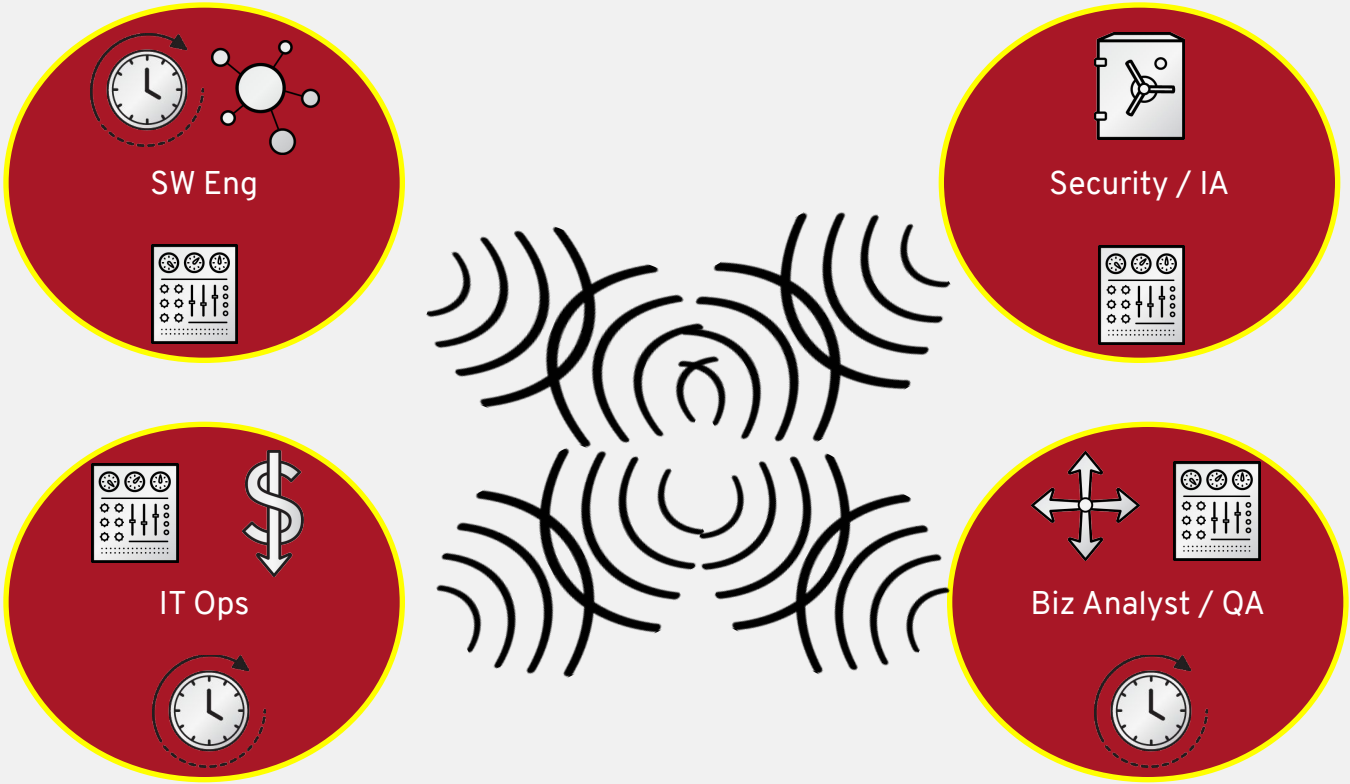
IT Optimization / App Modernization



Path to the Cloud / Cloud First



# THE CULTURAL CHALLENGE



# THE CULTURAL CHALLENGE (CONT.)

## Developers

- Features
- Quality
- Attributes
- Efficiency
- Performance
- Users
- Authentication
- Authorization
- New Technology

## IT Ops

- Deployment
- Maintenance
- Updates
- Change policy
- Failure
- Data loss
- Risk prevention
- Authentication
- Authorization

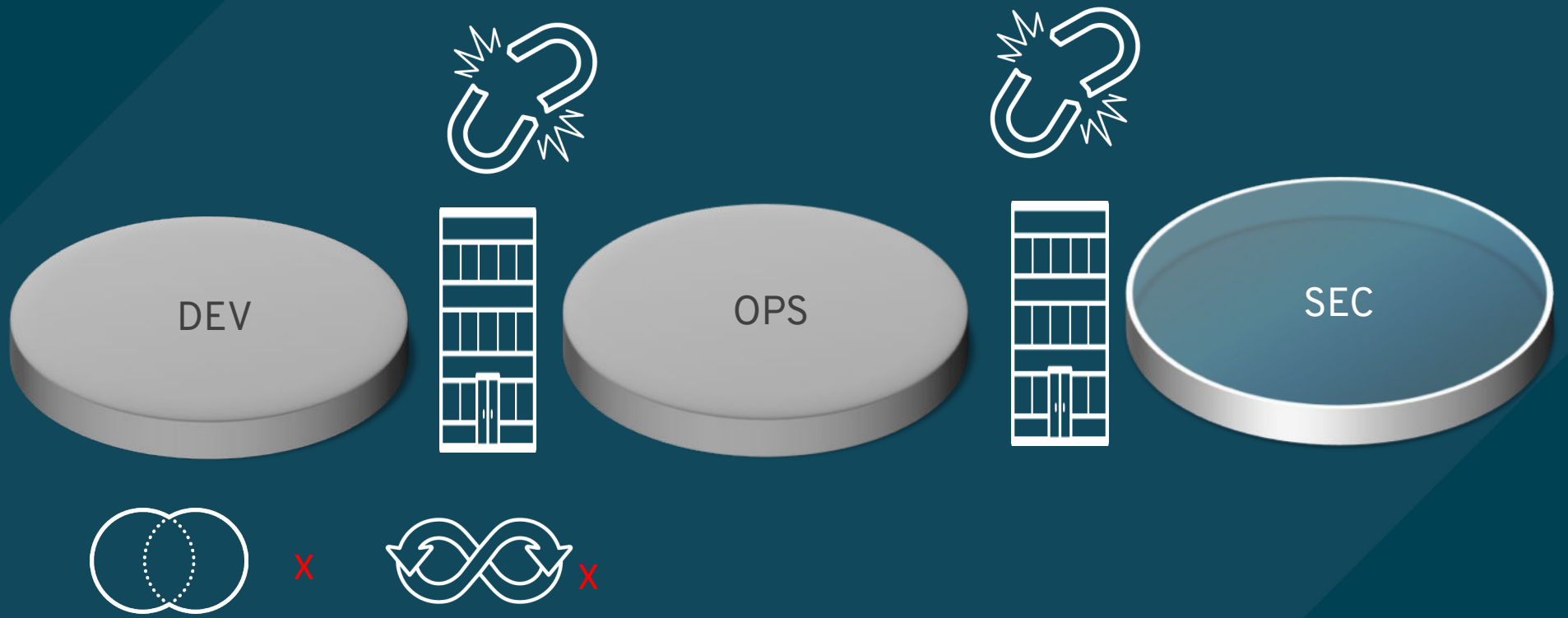
## QA/BA

- Testable
- Issue tracking
- Bug Reports
- Usability
- Performance
- Load
- Help Desk

## Security / IA

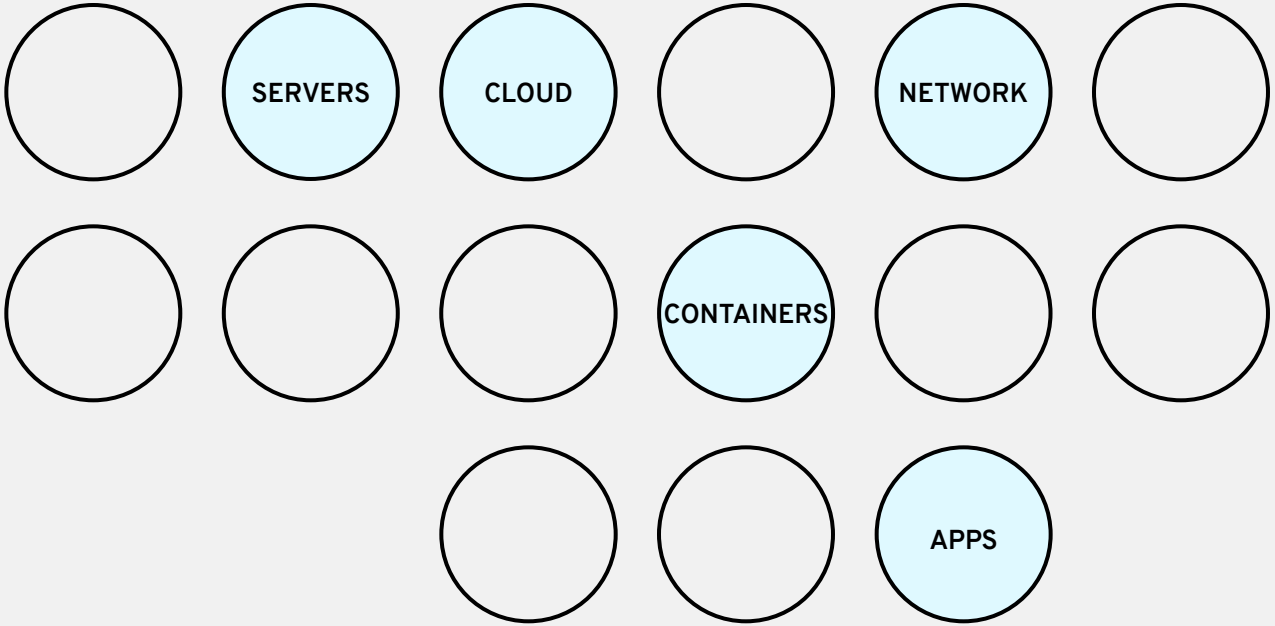
- Data Privacy
- Intrusion detection
- Threat vectors
- CWEs & CVEs
- Package/Artifact security
- Authentication
- Authorization
- Security Standards
- Compliance

# WHAT DOES THAT LOOK LIKE?

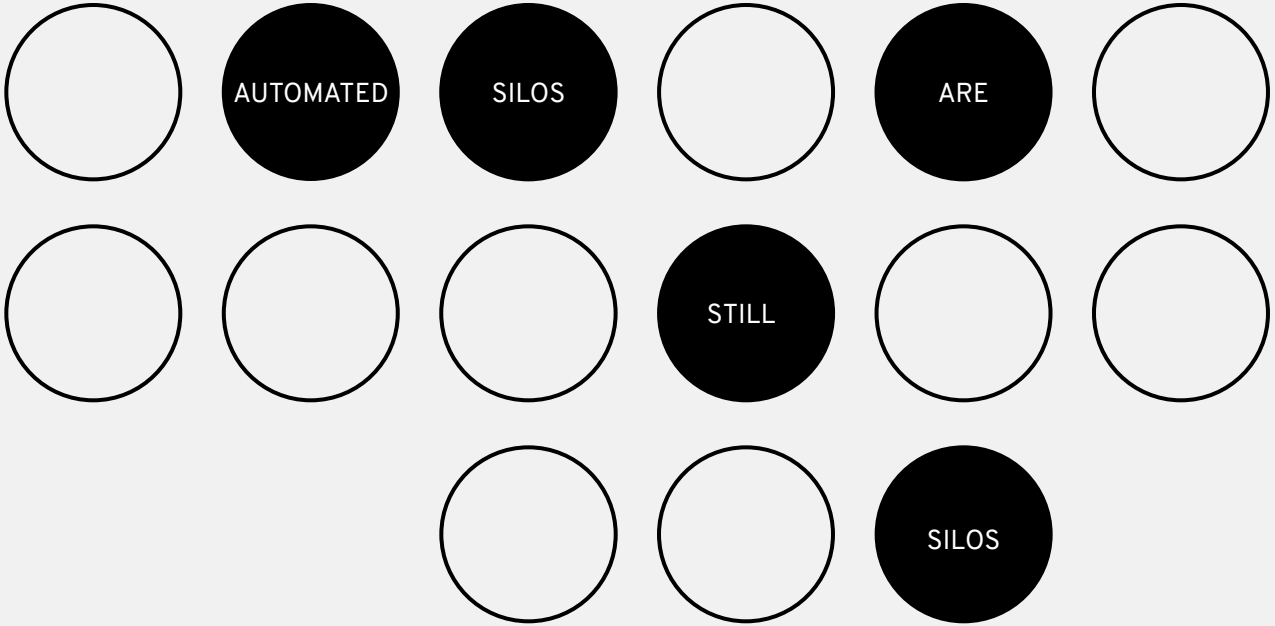


# MAYBE SOMETHING LIKE THIS?

# 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

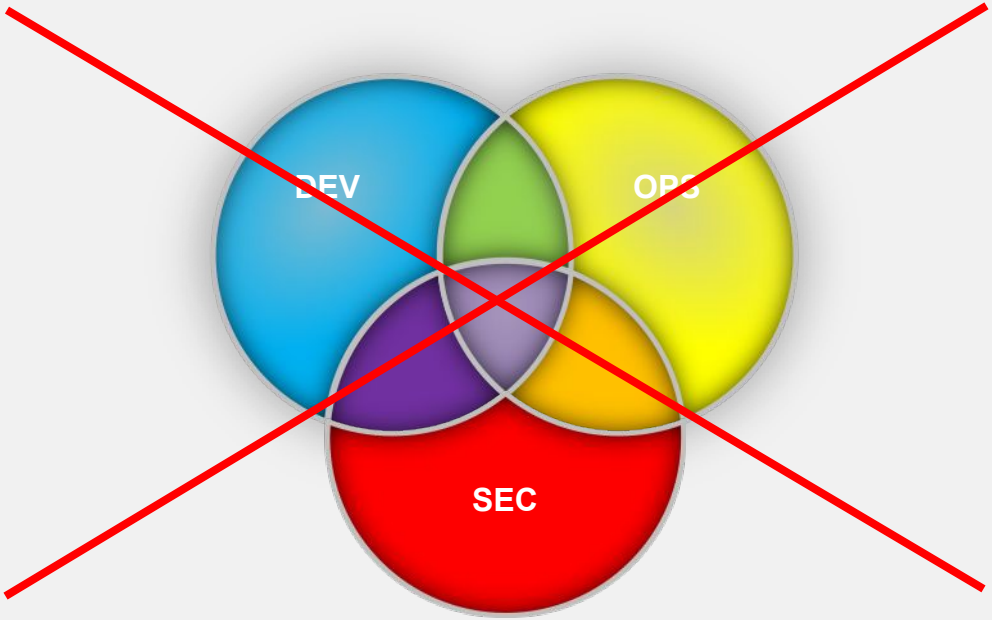
**Platform**
Modernize existing and build new cloud-based infrastructure

**Process**
More agile process across Security, IT and Engineering

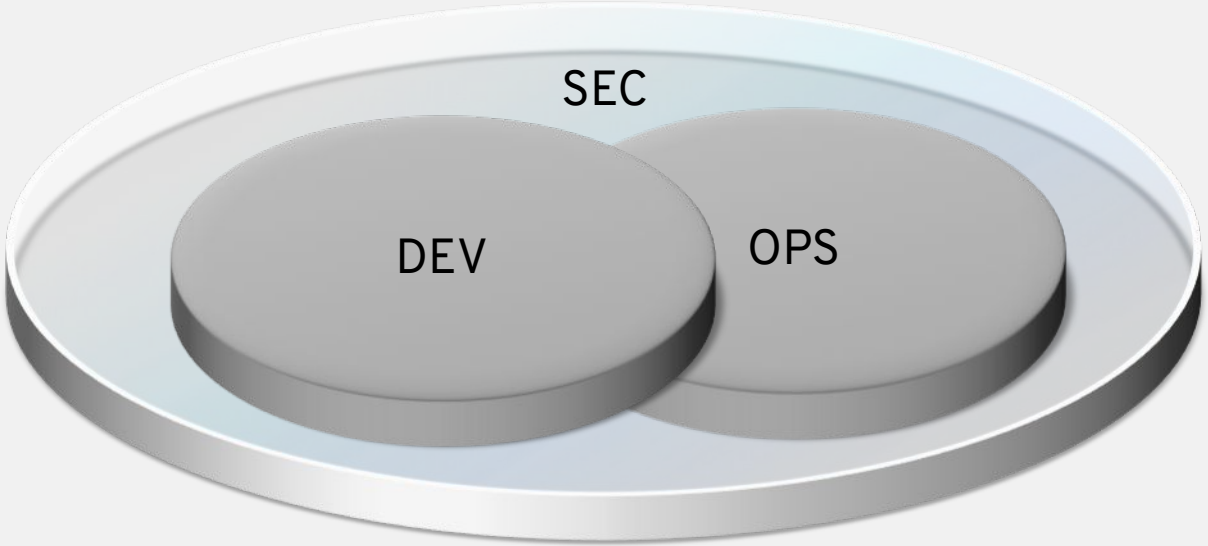
IF YOU WANT SOMETHING NEW,
YOU HAVE TO STOP DOING SOMETHING OLD.

–Peter Drucker

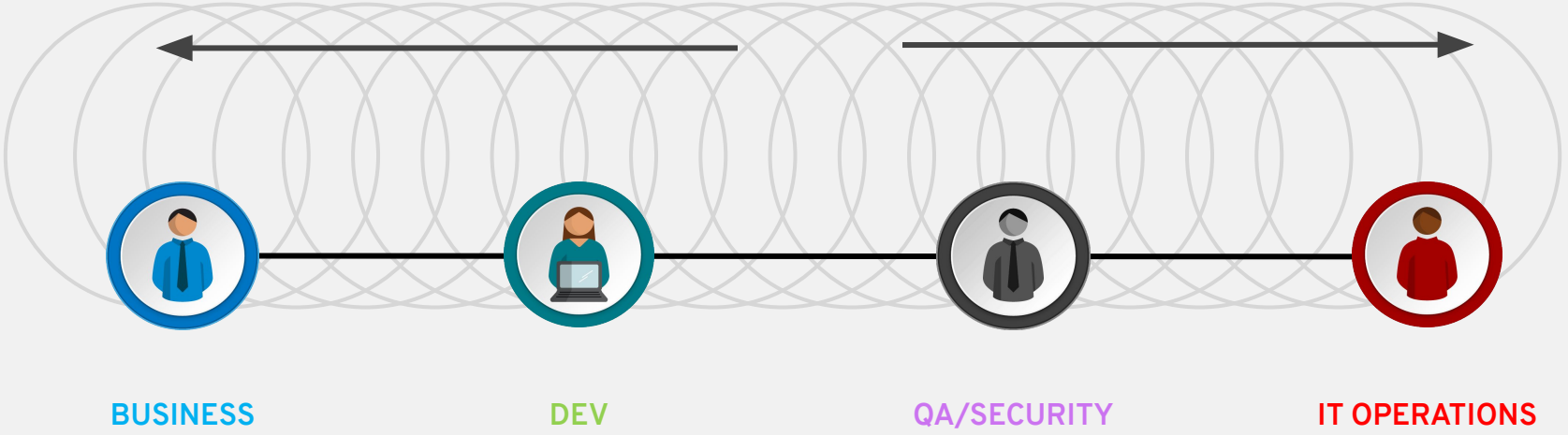
# LETS FIRST DISPEL SOME MYTHS



# SECURITY ENCOMPASSES NOT INTERSECTS



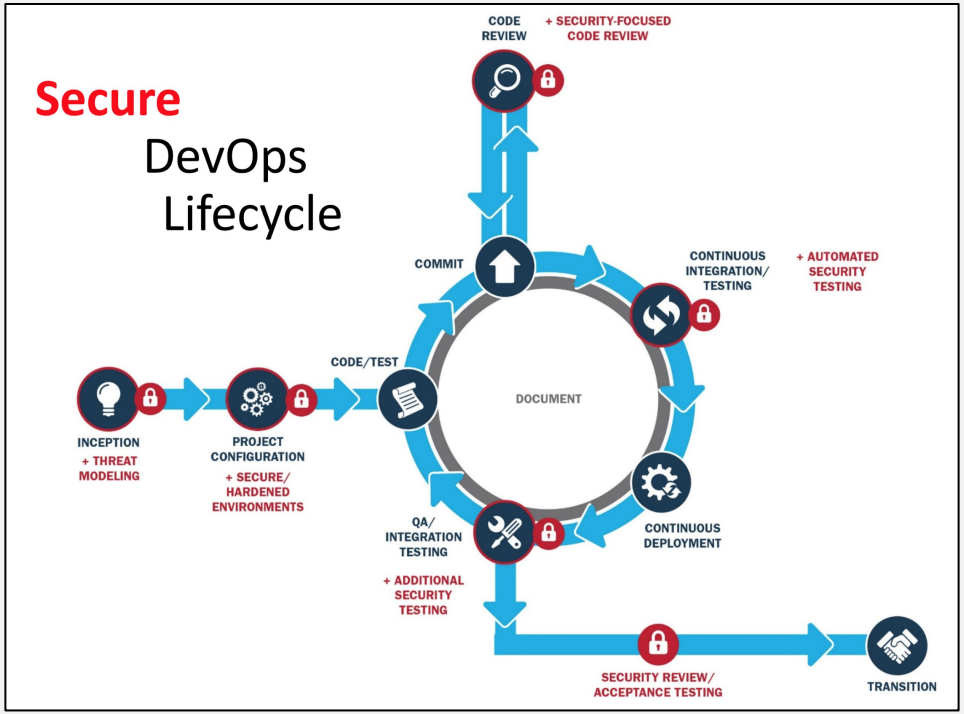
# ADDRESSING THE OPERATIONAL CHALLENGE



# ADDRESSING THE TECHNICAL CHALLENGE

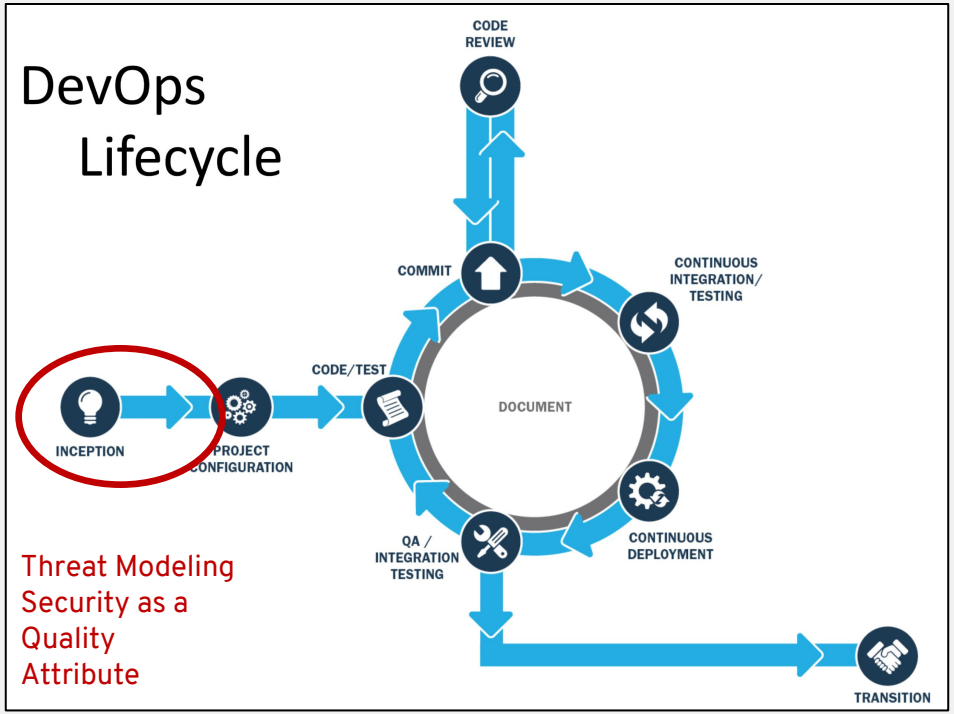
Adopting a container platform strategy will allow applications to be easily shared, managed, secured and deployed.

# SO WHAT DOES THAT LOOK LIKE?



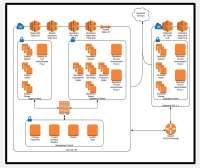

From All Day DevOps Webinar Nov 2016, Content distributable from Carnegie Mellon

# “SHIFT LEFT” WITH SECURITY/IA

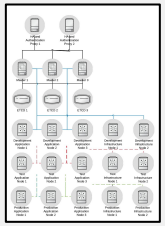


# WHAT DOES SECURE MEAN TO YOU?

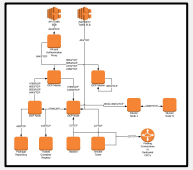
# DON’T START FROM SCRATCH



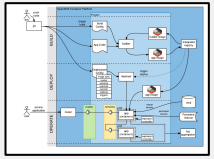
LOGICAL COMPONENT BLOCK DIAGRAM



CONTROLLED INTERFACE DIAGRAM



PHYSICAL CONNECTIVITY DIAGRAM



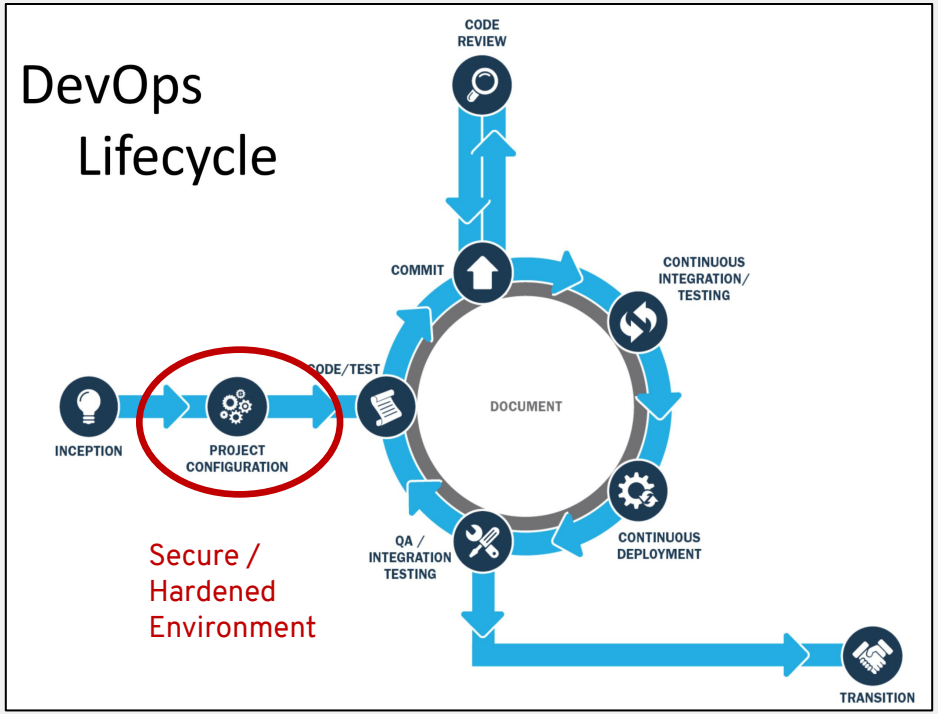
ROLE BASED ACTIVITY DIAGRAM

ROLE TO COMPONENT ALLOCATION

CUSTOM ANSIBLE ROLES

CENTRALIZED ARTIFACTS

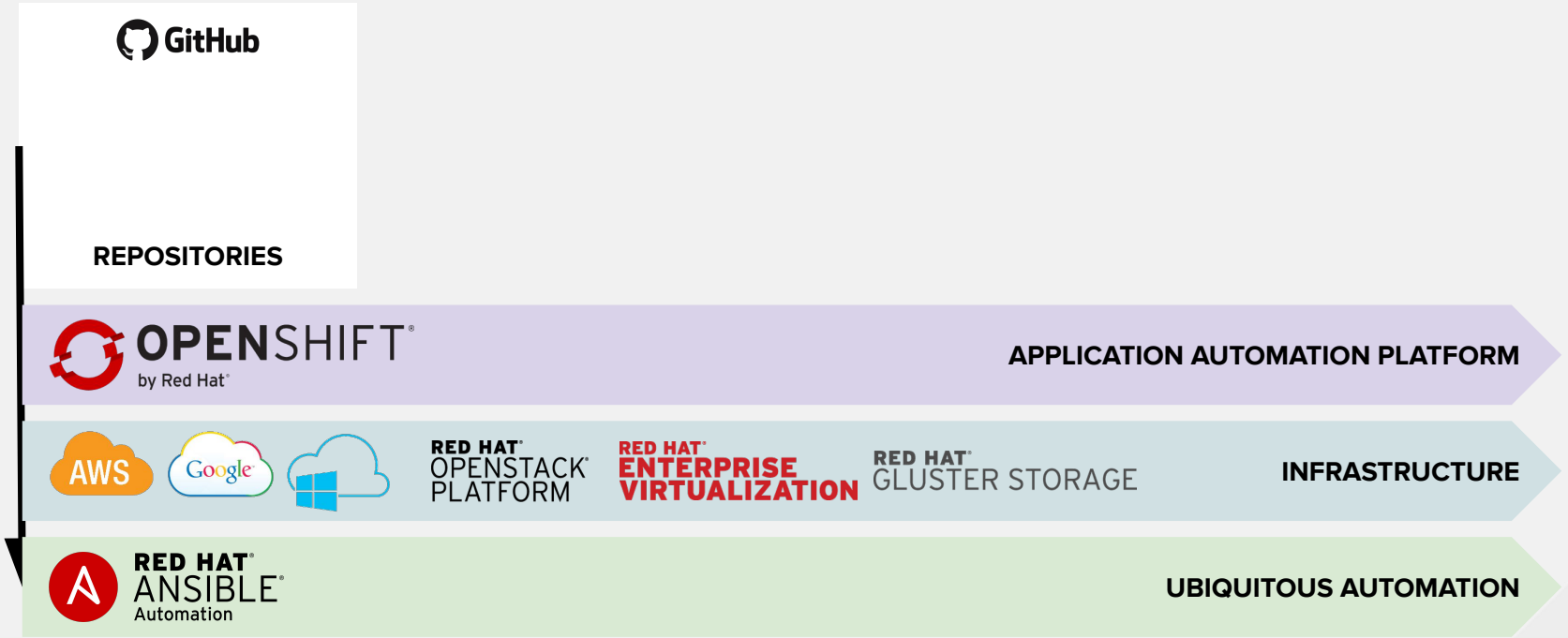
# ADOPT A SECURITY INHERITANCE MODEL



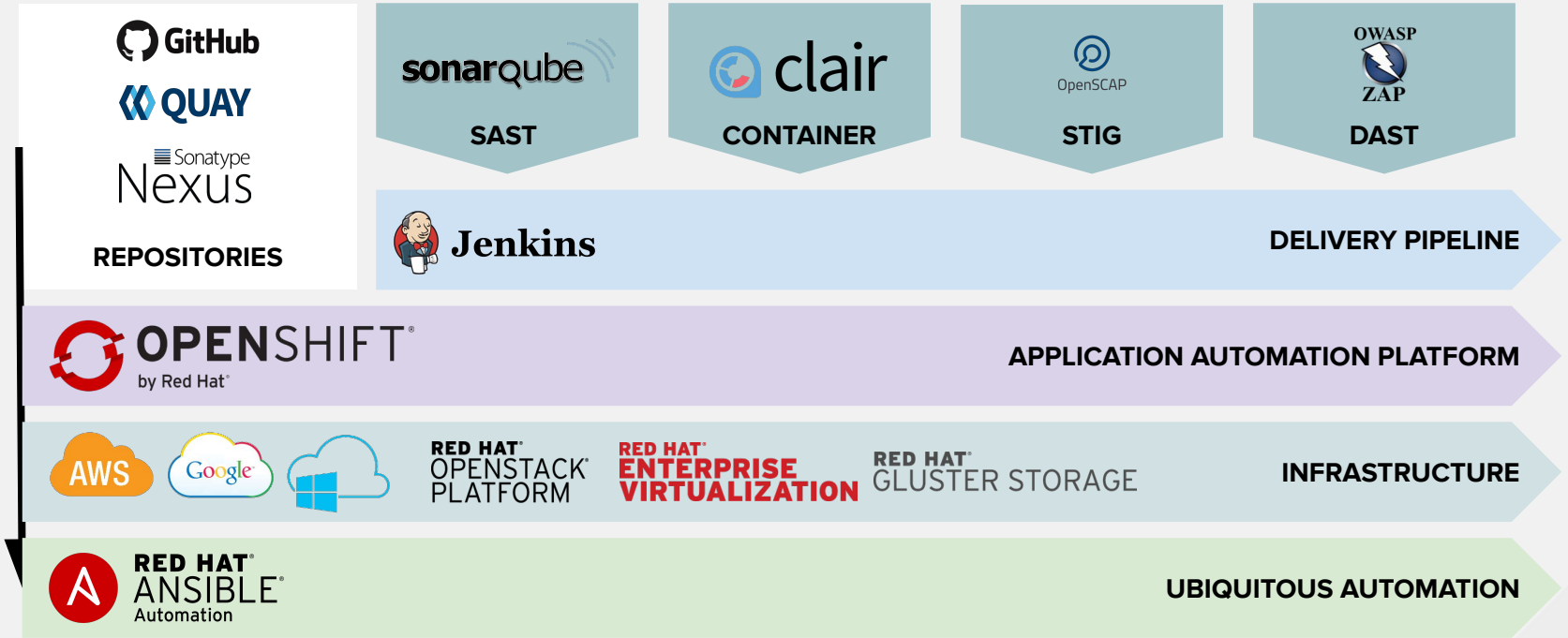
# DEPLOYING A SECURE SOFTWARE FACTORY

# DEPLOYING A SECURE SOFTWARE FACTORY

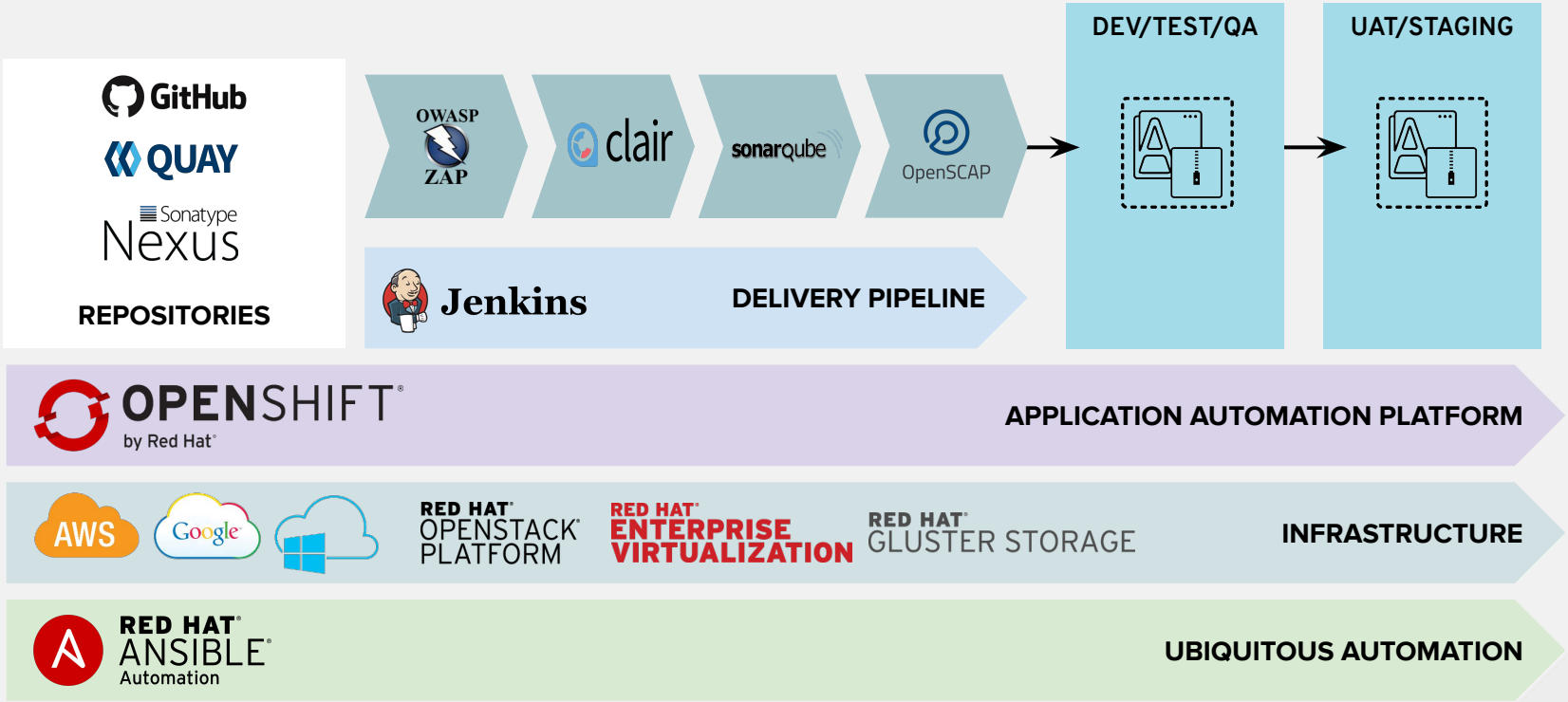
# DEPLOYING A SECURE SOFTWARE FACTORY



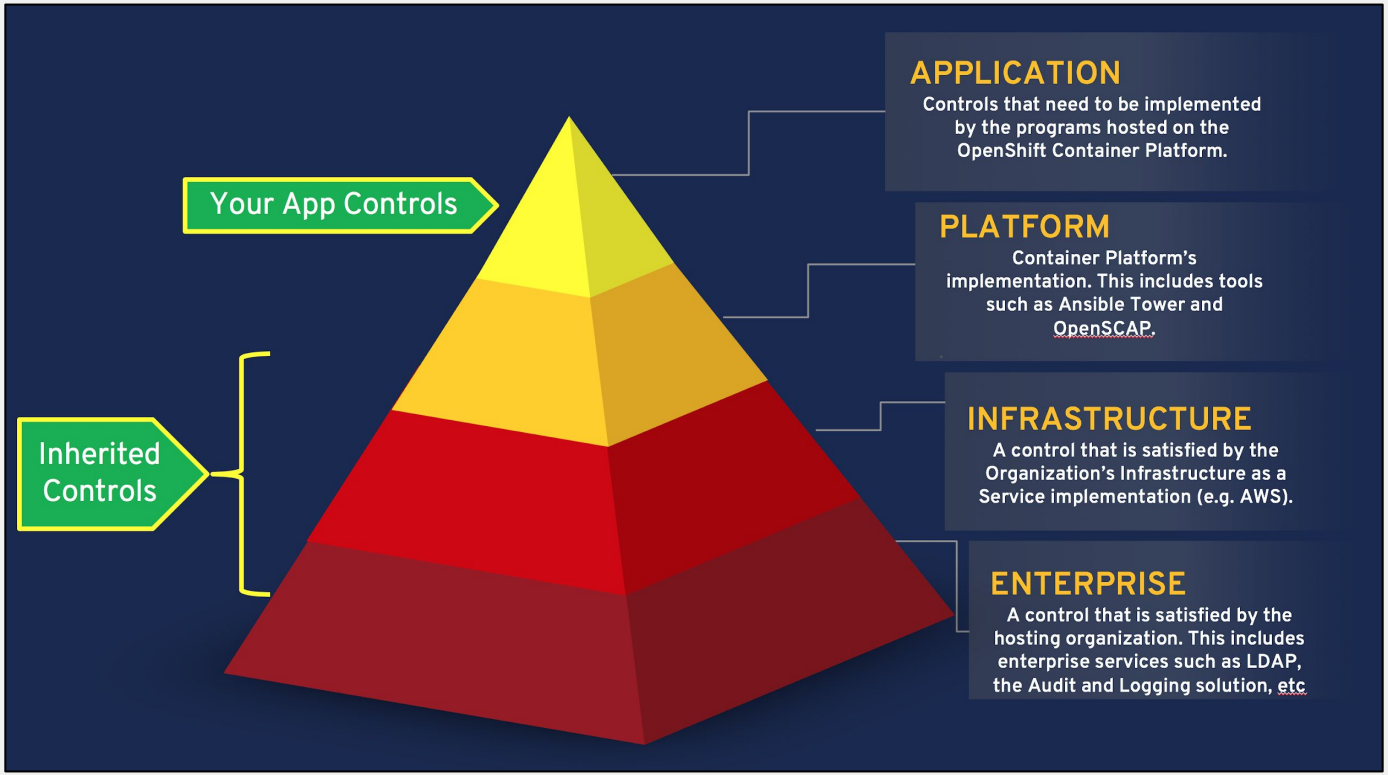
# DEPLOYING A SECURE SOFTWARE FACTORY

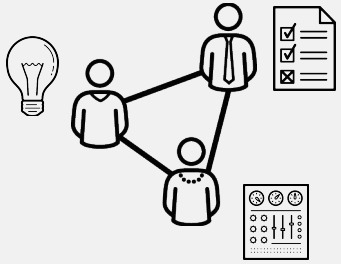


# EXERCISING A SECURE SOFTWARE FACTORY



# SECURITY INHERITANCE MODEL

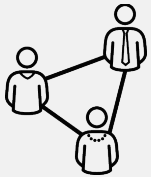




PULL OR CREATE

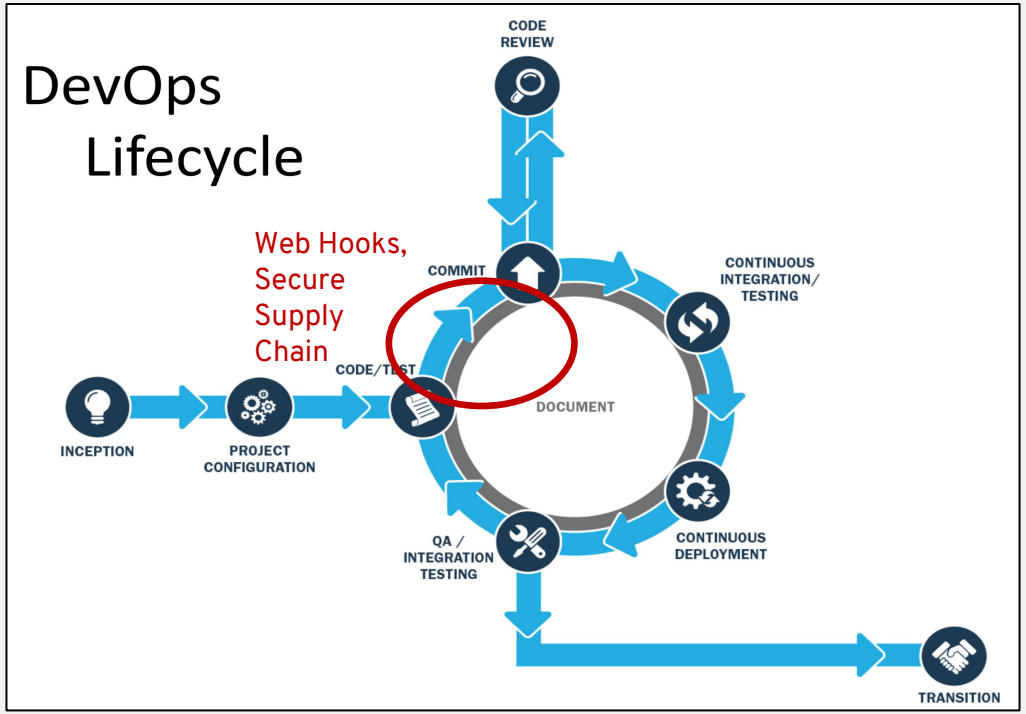
SCM

BUILD LOAD SCAN SIGN



DEV INSPECT BUILD SCAN TEST DEPLOY MONITOR

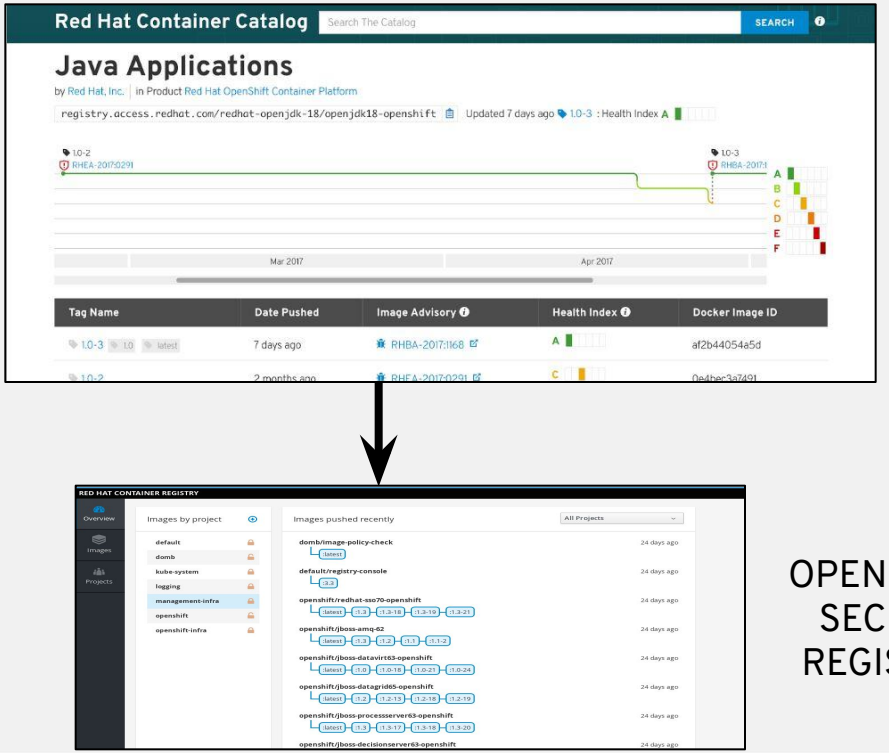
# ONLY INTRODUCE ”APPROVED” ELEMENTS



# 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




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

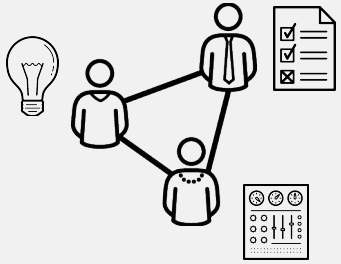
**Red Hat Customer Portal Stats 2016**

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

- Image Documentation
- Image Advisories

RED HAT® CONTAINER CATALOG

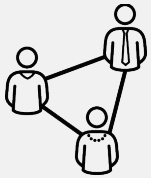
- Container Health Index
- Extensive Image Metadata



PULL OR CREATE

SCM

BUILD | LOAD | SCAN | SIGN

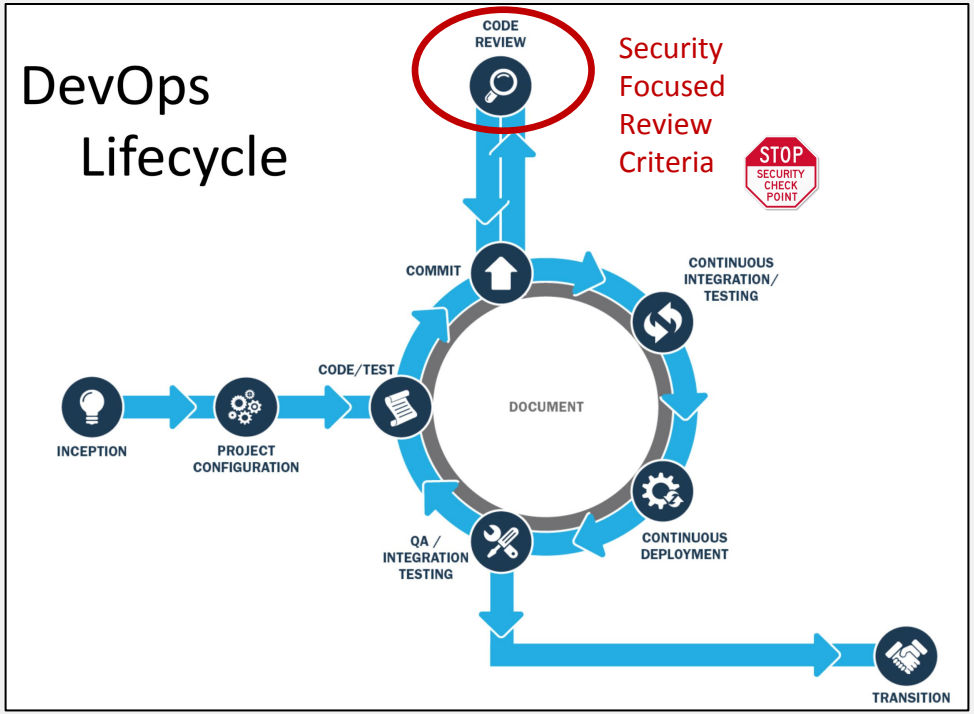


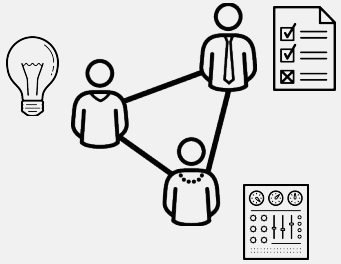
Pre-receive Hooks With Security Compliance Checks

[GitHub]

DEV | INSPECT | BUILD | SCAN | TEST | DEPLOY | MONITOR

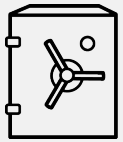
# AUTOMATE WHAT YOU CAN & BUILD TRUST



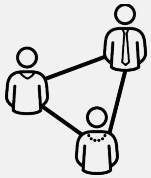


PULL
OR
CREATE

SCM



BUILD | LOAD | SCAN | SIGN



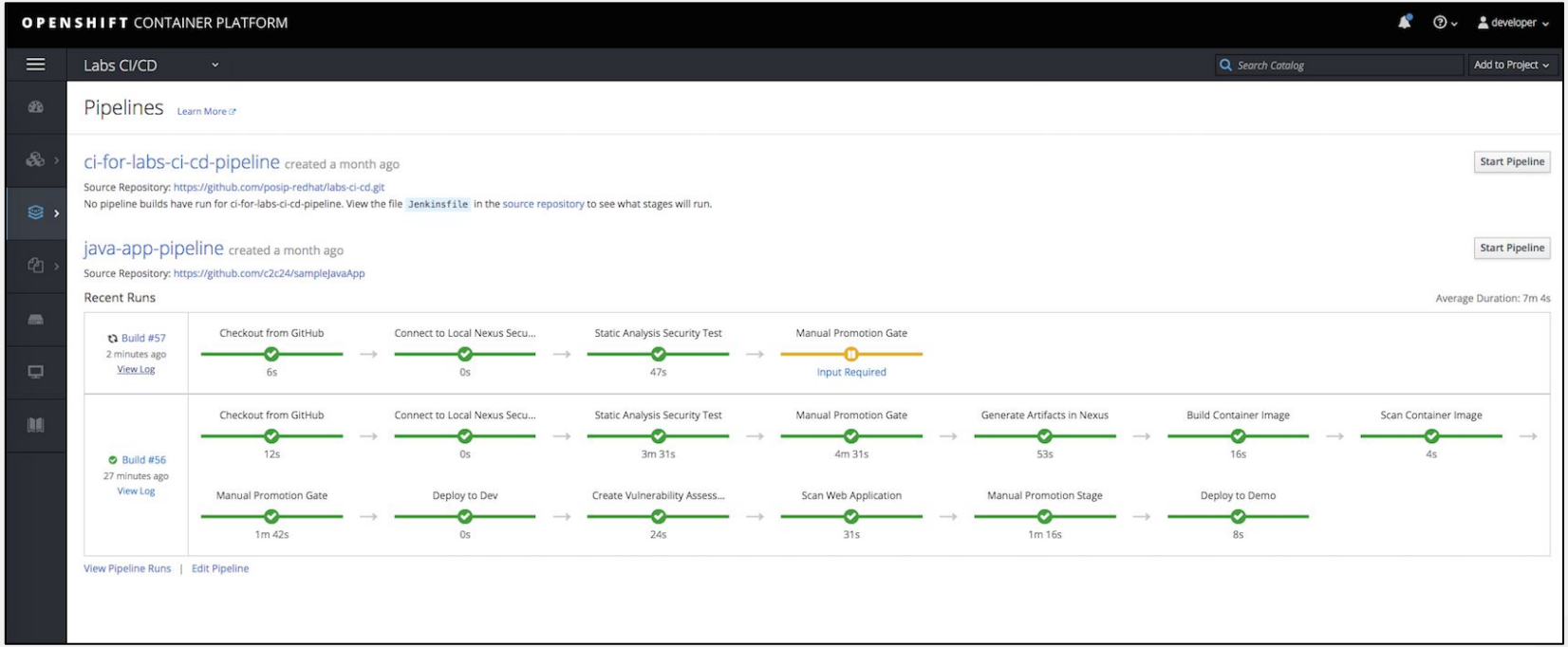
Pre-receive
Hooks
With
Security
Compliance
Checks

[GitHub]

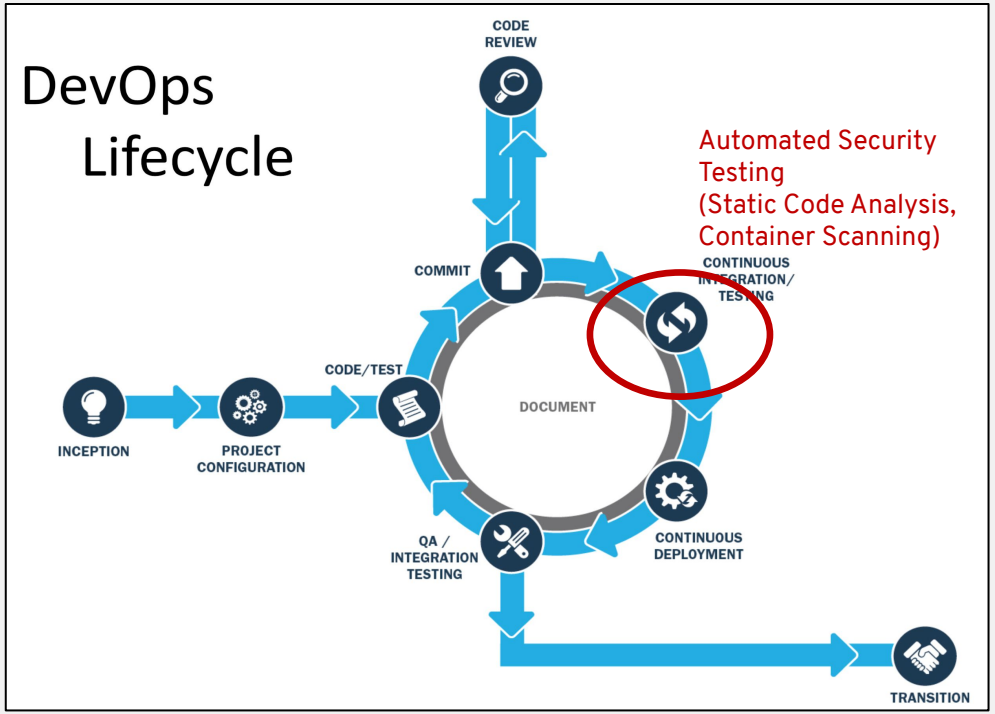
**Code Review**

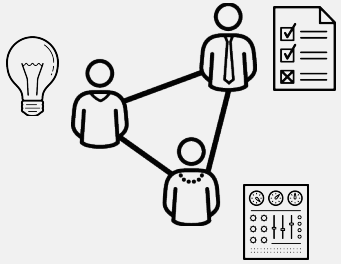
DEV | INSPECT | BUILD | SCAN | TEST | DEPLOY | MONITOR

# DEMO OUTPUT FOR PIPELINE INVOCATION POST CODE REVIEW



# DON’T WASTE COMPUTE OR TIME





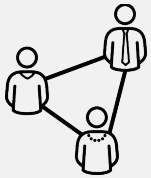
PULL OR CREATE

SCM

OPENSCAP EVALUATE & REMEDIATE

IMAGE

BUILD | LOAD | SCAN | SIGN



Pre-receive Hooks With Security Compliance Checks

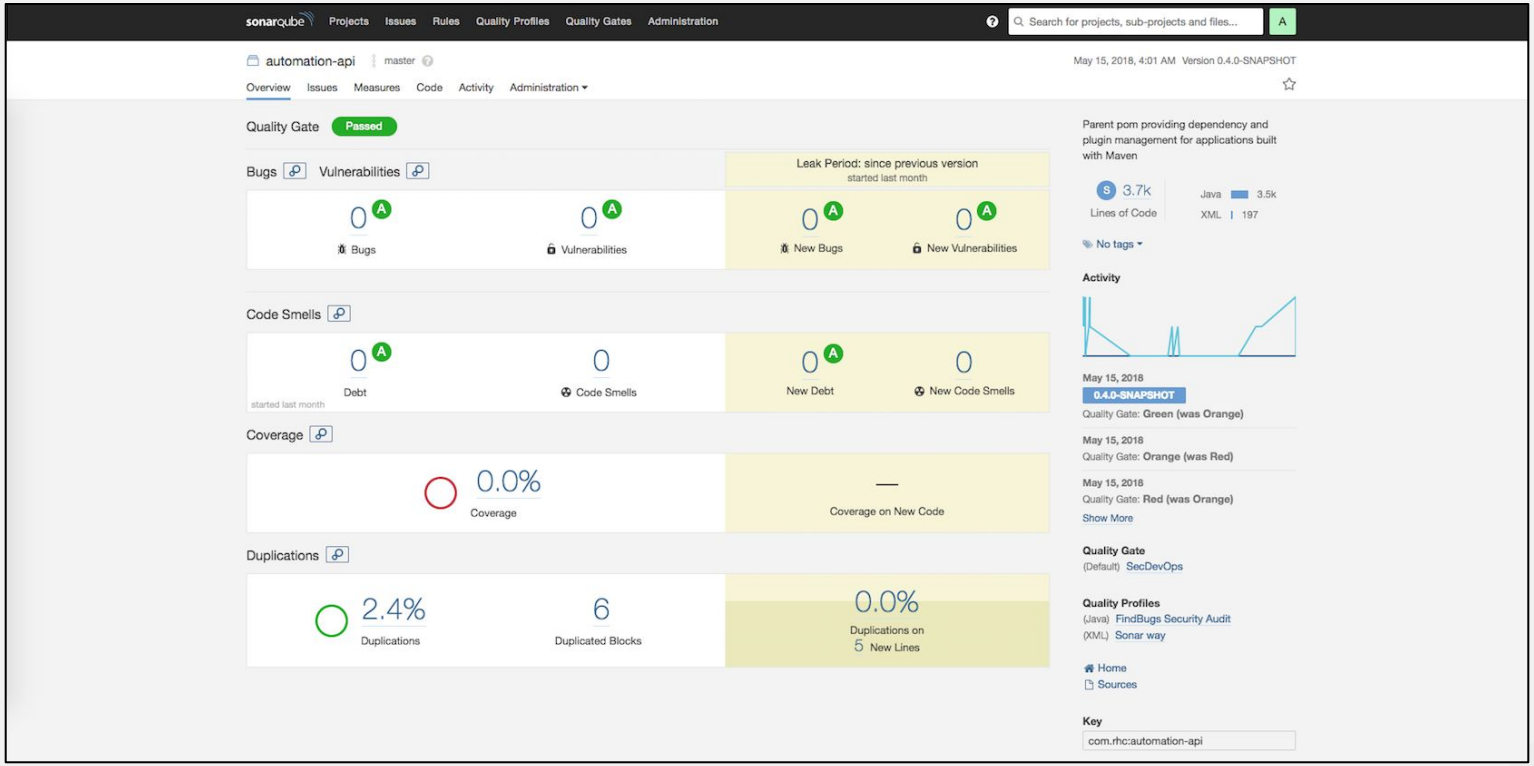
[GitHub]

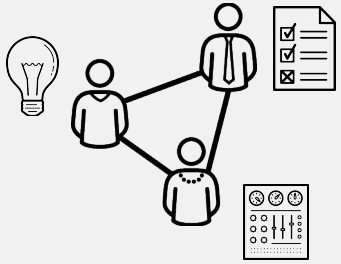
Static Analysis Security Test (SAST)

[SonarQube]

DEV | INSPECT | BUILD | SCAN | TEST | DEPLOY | MONITOR

# OUTPUT FOR STATIC ANALYSIS (LINK)





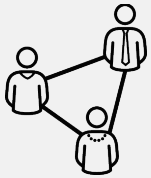
PULL OR CREATE

SCM

OPENSCAP EVALUATE & REMEDIATE

IMAGE

BUILD | LOAD | SCAN | SIGN



Pre-receive Hooks With Security Compliance Checks

[GitHub]

Static Analysis Security Test (SAST)

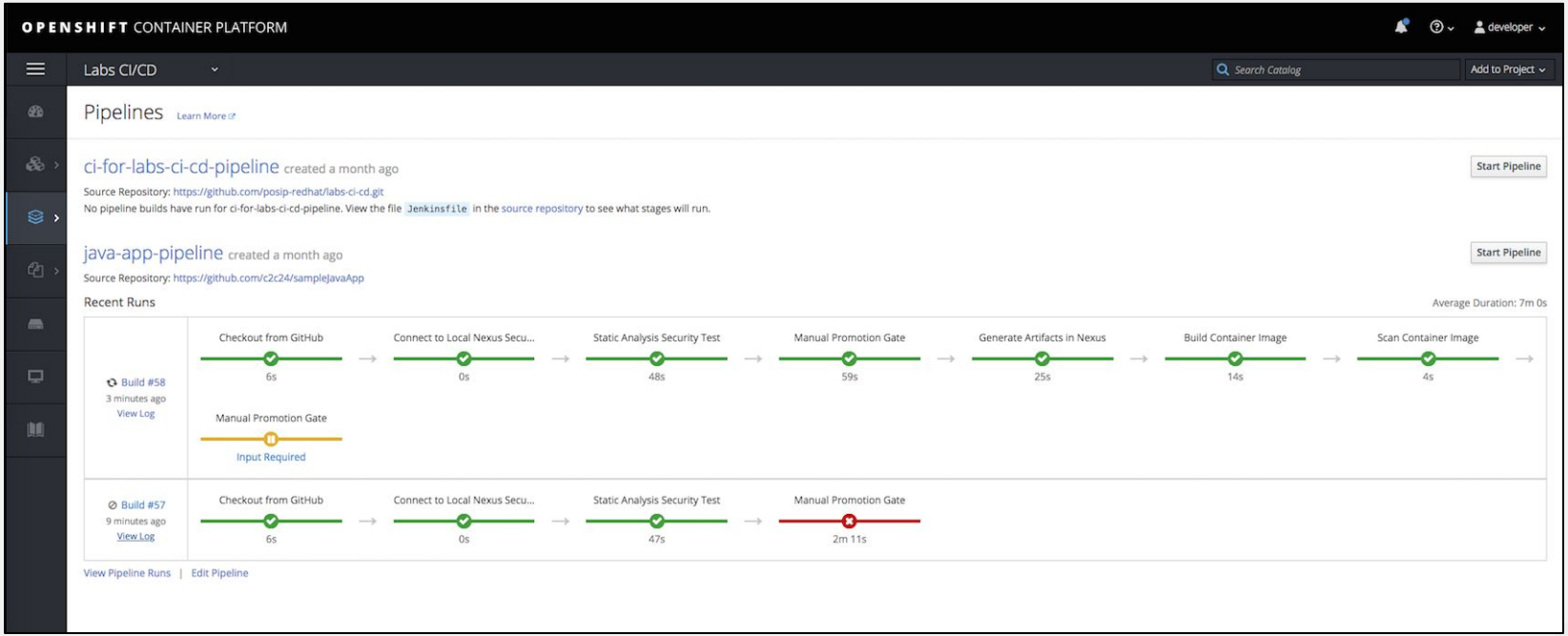
[SonarQube]

Policy Enforcement For Build Artifacts & Images

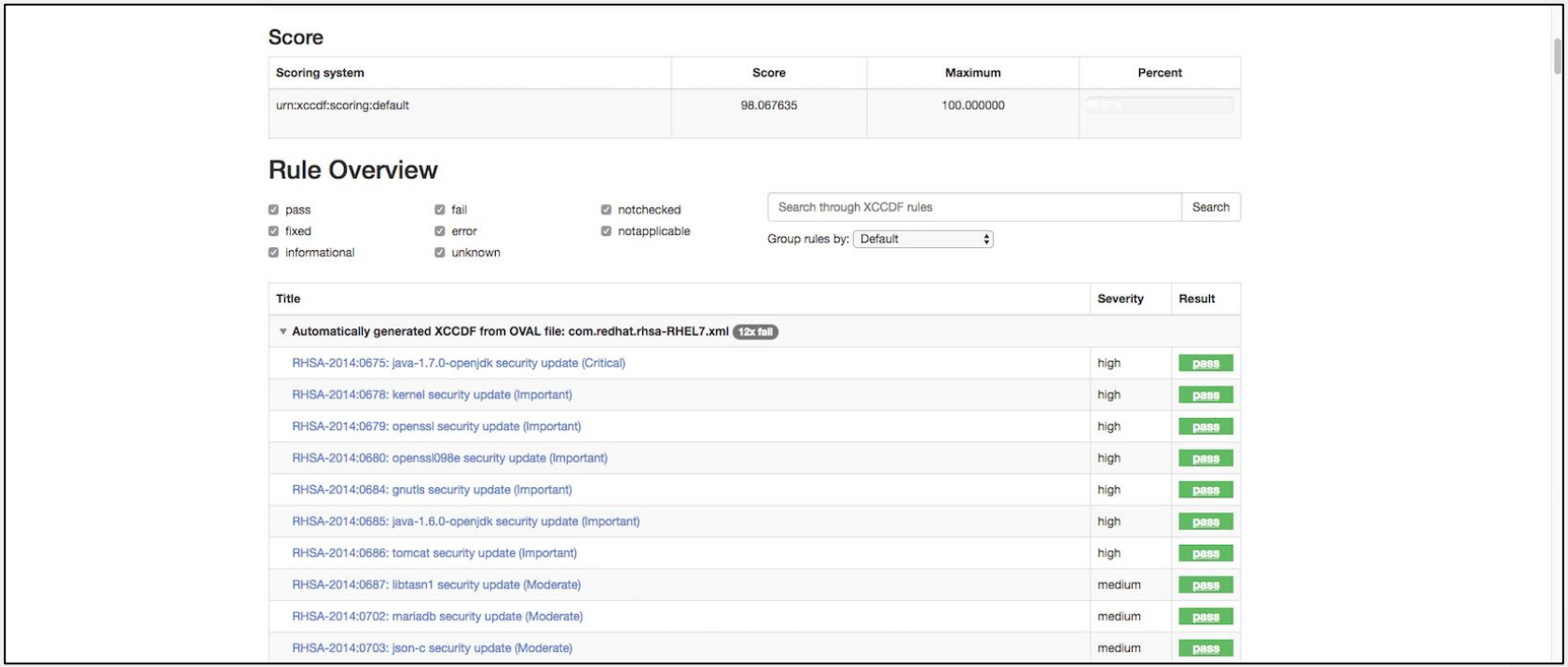
[OCP]

DEV | INSPECT | BUILD | SCAN | TEST | DEPLOY | MONITOR

# OUTPUT FOR OPENSCAP IMAGE SCAN FROM PIPELINE (LINK)



# DEMO OUTPUT FOR OPENSCAP IMAGE SCAN



## Score

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

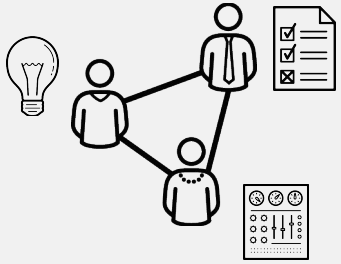
## Rule Overview

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 |



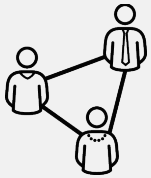
PULL OR CREATE

SCM

OPENSCAP 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]

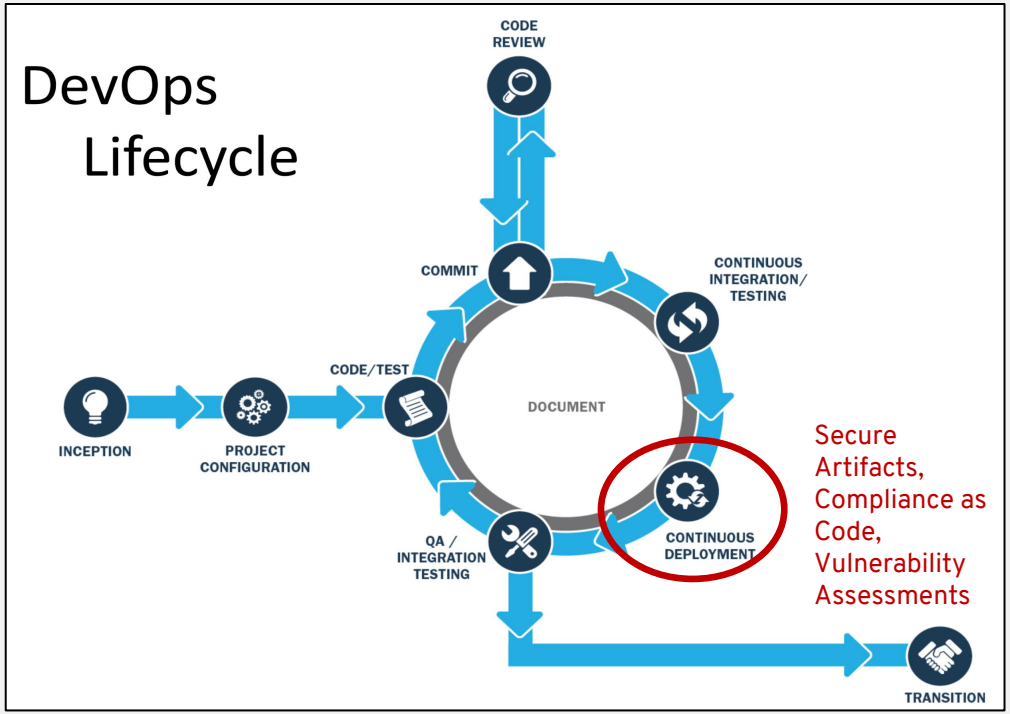
Image Scanning w/ tailored profiles

[OpenSCAP] [Clair]

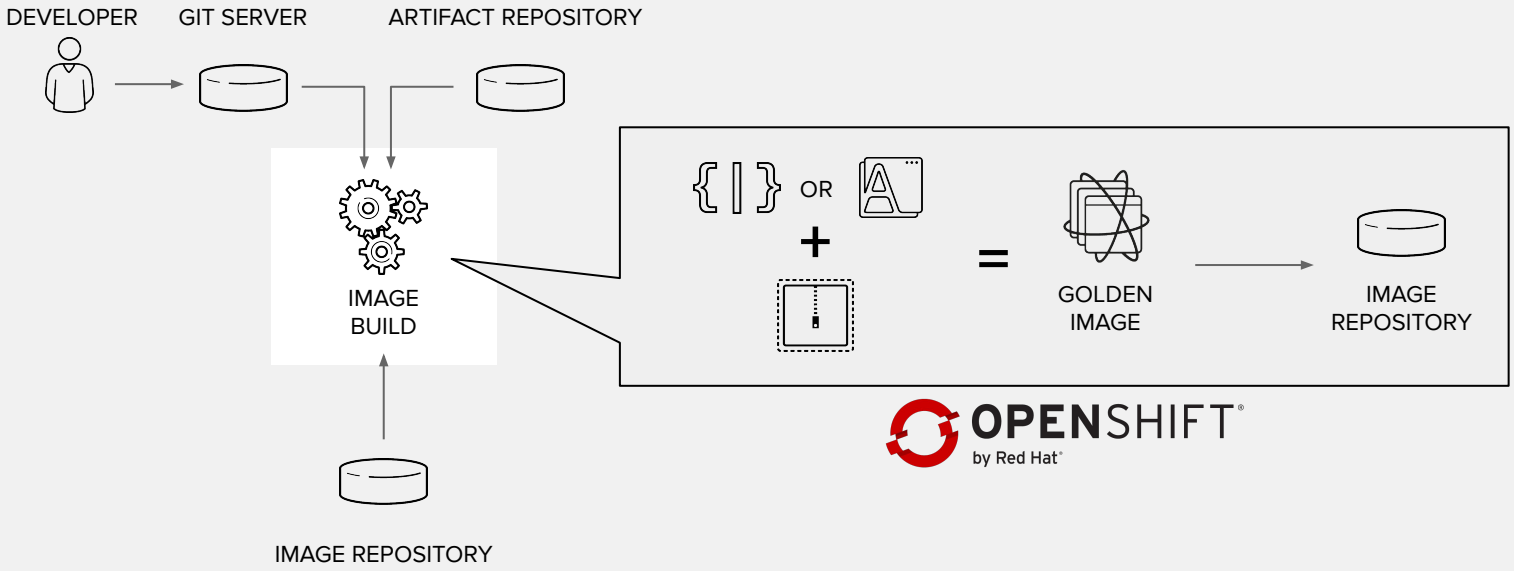
**Compliance Check**

DEV | INSPECT | BUILD | SCAN | TEST | DEPLOY | MONITOR

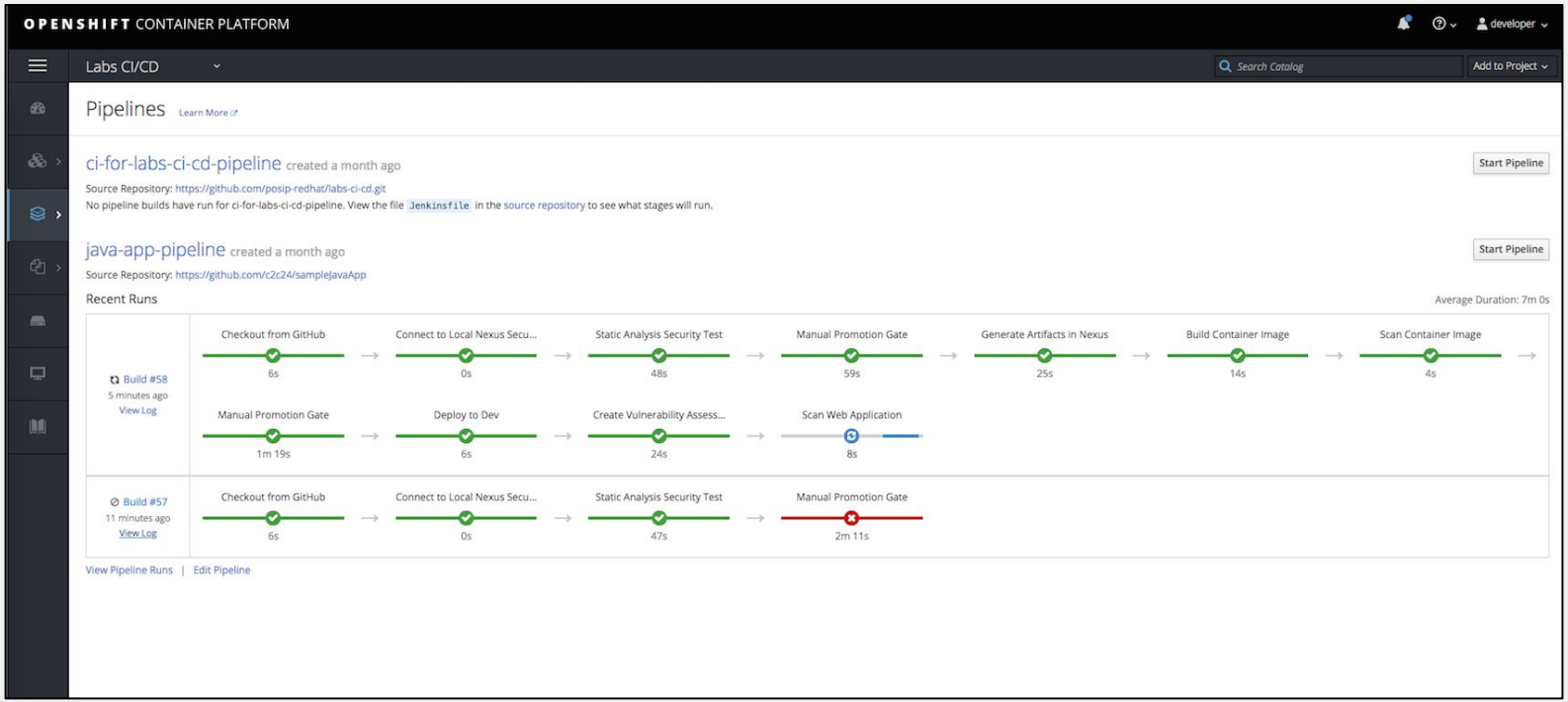
# POLICY DRIVEN DEPLOY AND COMPLIANCE



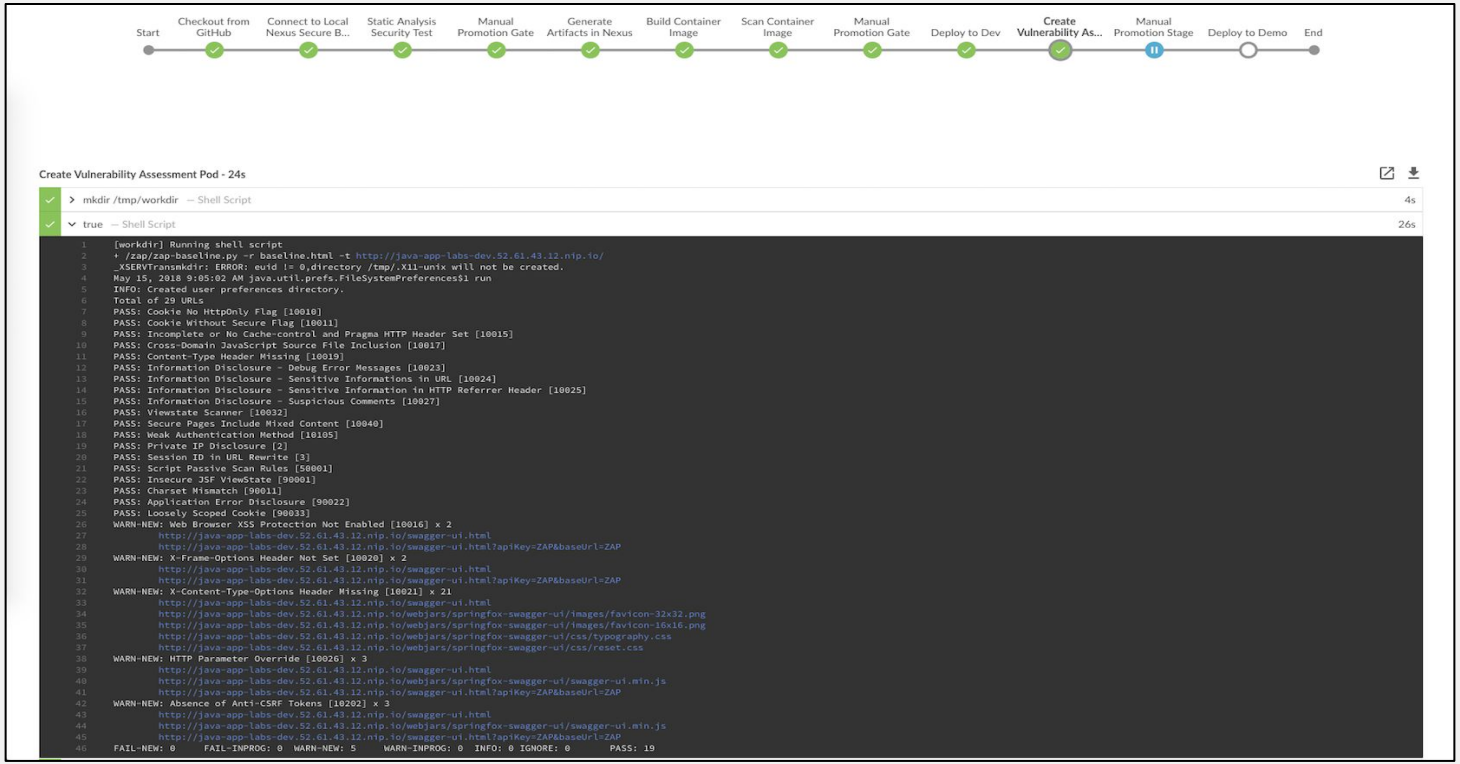
# BUILDING APPLICATION ON OPENSHIFT

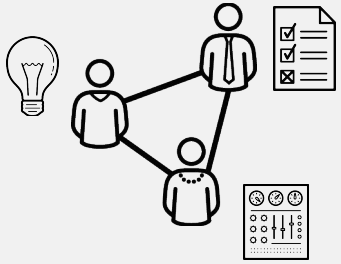


# VULNERABILITY ASSESSMENT FROM PIPELINE (LINK)



# DEMO OUTPUT FOR VULNERABILITY ASSESSMENT





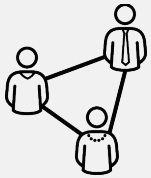
PULL OR CREATE

SCM

OPENSCAP EVALUATE & REMEDIATE

IMAGE

BUILD | LOAD | SCAN | SIGN



Pre-receive Hooks With Security Compliance Checks [GitHub]

Static Analysis Security Test (SAST) [SonarQube]

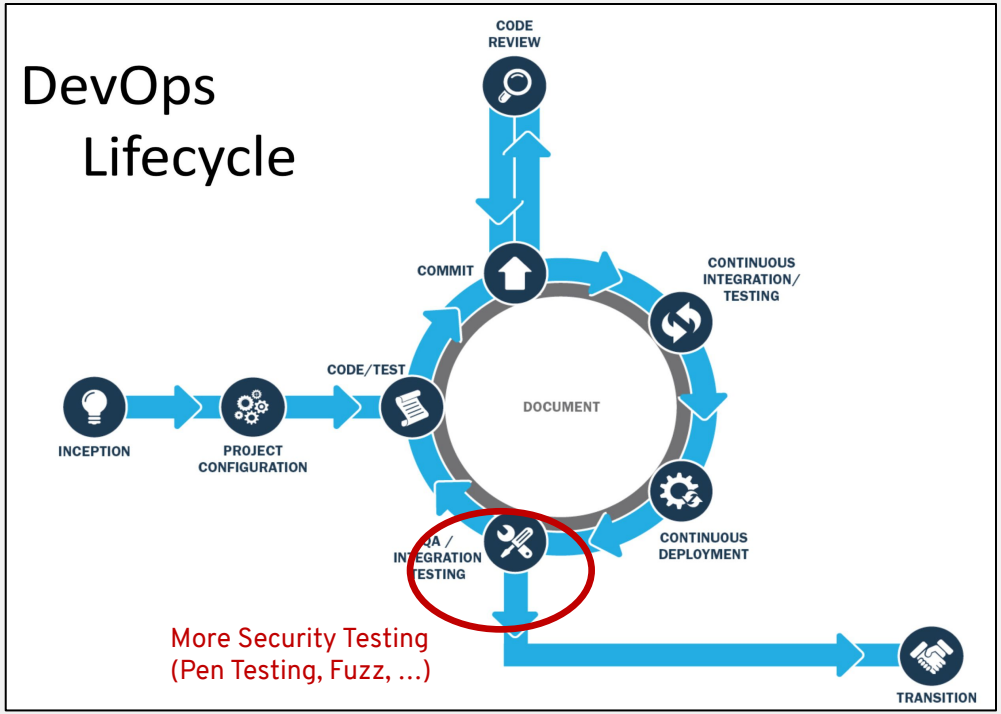
Policy Enforcement For Build Artifacts & Images [OCP]

Image Scanning w/ tailored profiles [OpenSCAP] [Clair]

Vulnerability Assessment (CVE, OWASP) [ZAP]

DEV | INSPECT | BUILD | SCAN | TEST | DEPLOY | MONITOR

# WHAT GETS MEASURED GETS IMPROVED



# FROM CODE TO CAPABILITIES

**DEV**

- Pre-receive Hooks
- Static Analysis

**BUILD**

- Dependency Management
- Image Scan

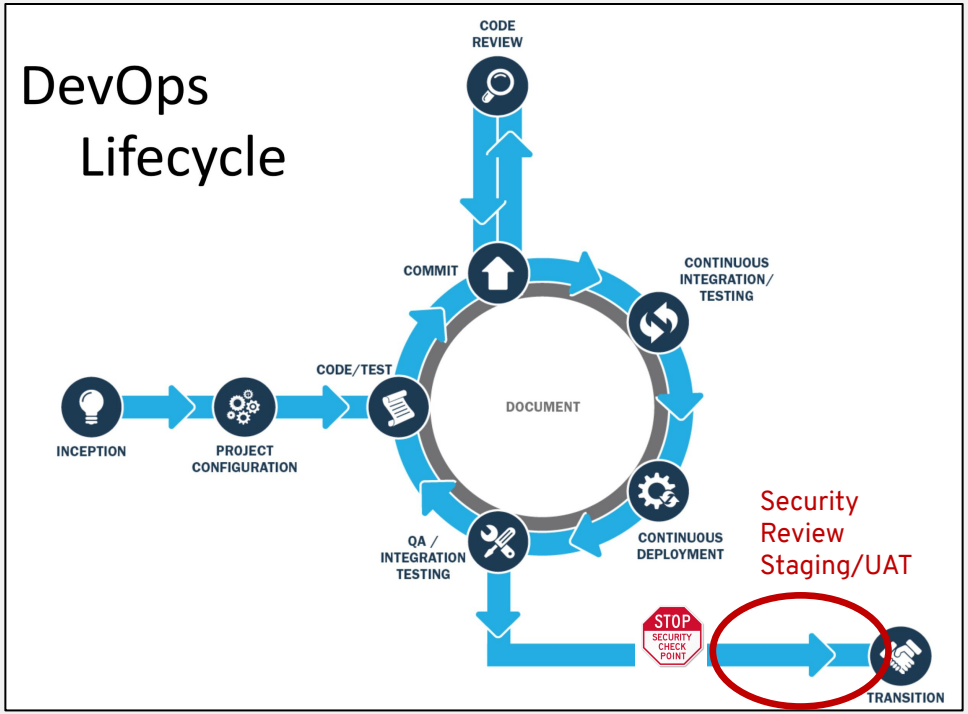

**DEPLOY**

- Vulnerability Assessment
- Signed Images

**TEST**

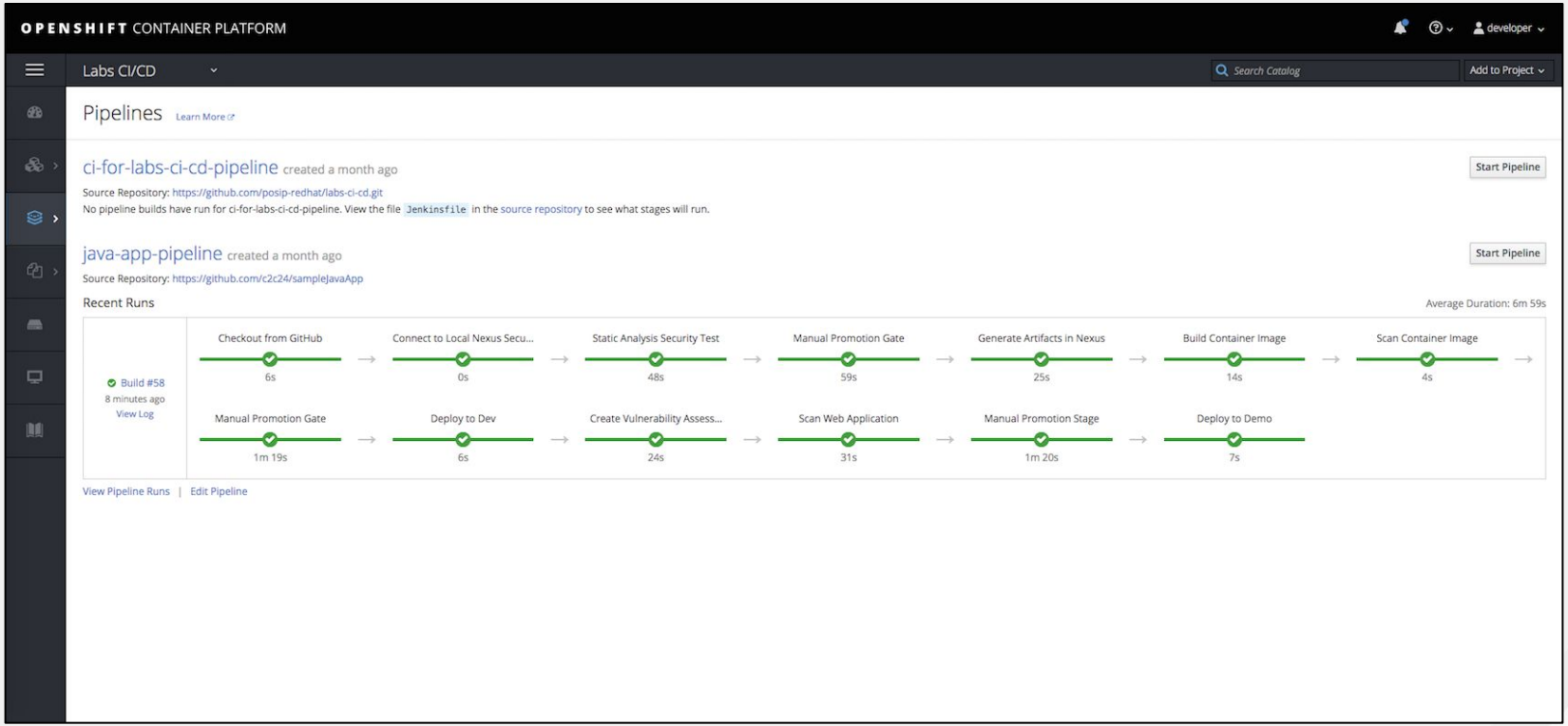
- Integration Tests
- Penetration / Fuzz Testing

# CONTINUE TO BUILD TRUST AND AUTOMATE

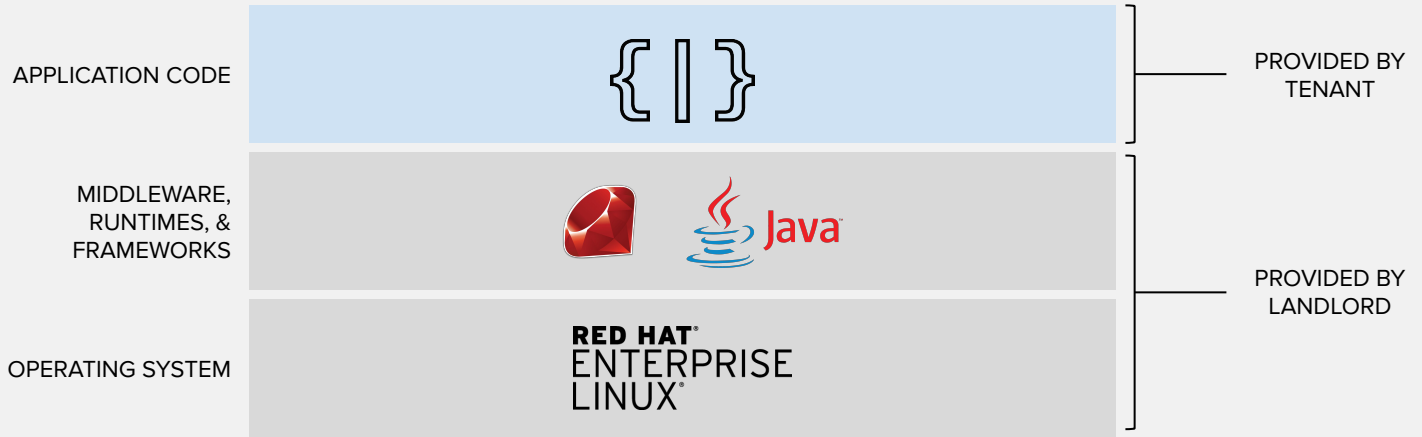


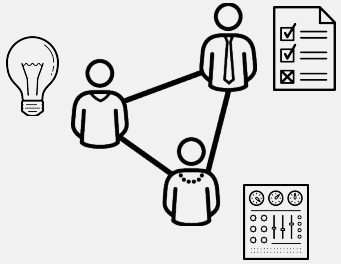

From All Day DevOps Webinar Nov 2016, Content distributable from Carnegie Mellon

# OUTPUT OF COMPLETED PIPELINE (LINK)



# THE GOLDEN IMAGE





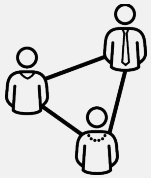
PULL OR CREATE

SCM

OPENSCAP 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]

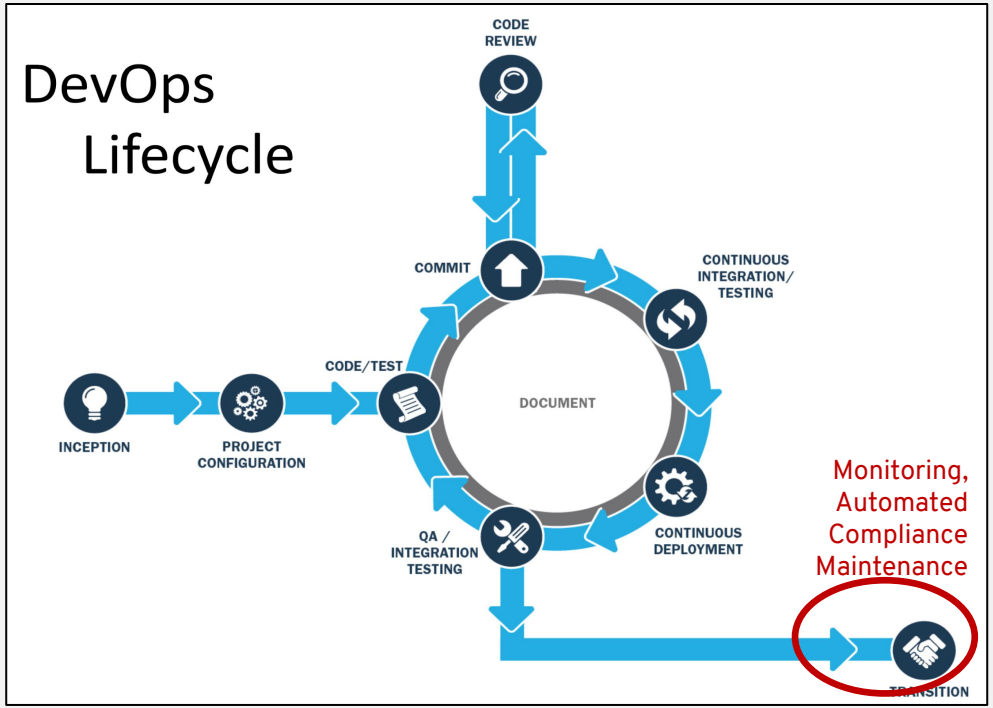
Image Scanning w/ tailored profiles [OpenSCAP] [Clair]

Vulnerability Assessment (CVE, OWASP) [ZAP]

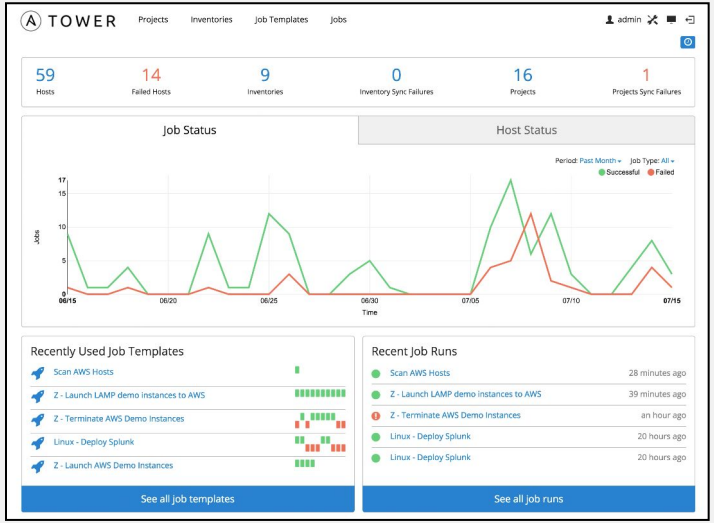
Push/Pull Signed Images [OCP]

DEV | INSPECT | BUILD | SCAN | TEST | DEPLOY | MONITOR

# ITERATIVE SECURE DEPLOYMENTS

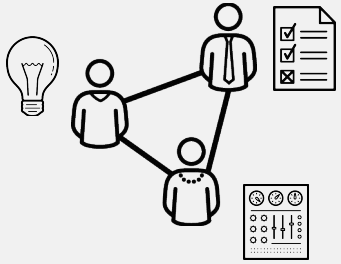


# DAY-2 OPERATIONS SAMPLE VIEW FROM ANSIBLE TOWER




## 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



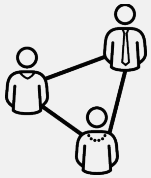
PULL OR CREATE

SCM

OPENSCAP EVALUATE & REMEDIATE

IMAGE

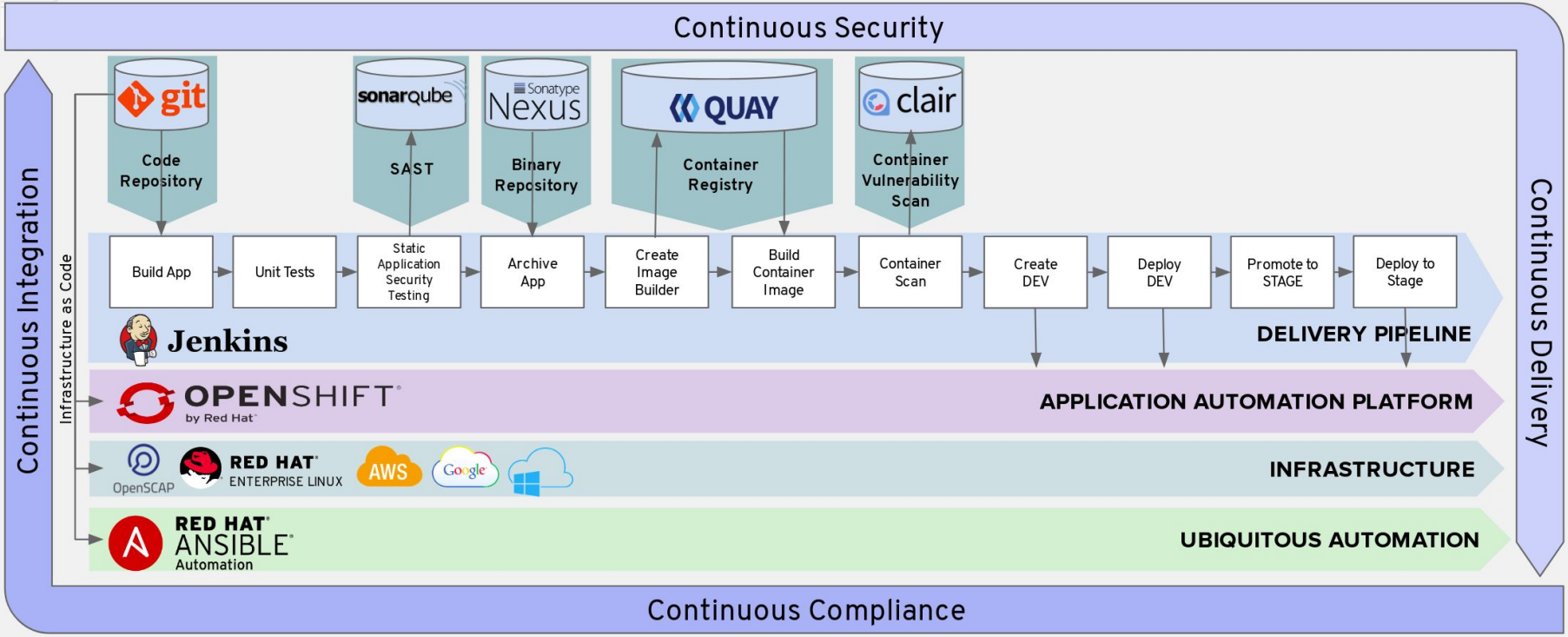
BUILD | LOAD | SCAN | SIGN



| Pre-receive Hooks With Security Compliance Checks | Static Analysis Security Test (SAST) | Policy Enforcement For Build Artifacts & Images | Image Scanning w/ tailored profiles | Vulnerability Assessment (CVE, OWASP) | Push/Pull Signed Images | CM Drift Prevention & Metrics |
|---|---|---|---|---|---|---|
| [GitHub] | [SonarQube] | [OCP] | [OpenSCAP] [Clair] | [ZAP] | [OCP] | [Ansible] [OCP] |

DEV | INSPECT | BUILD | SCAN | TEST | DEPLOY | MONITOR

# THE SECURE SOFTWARE FACTORY



redhat.

# THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos