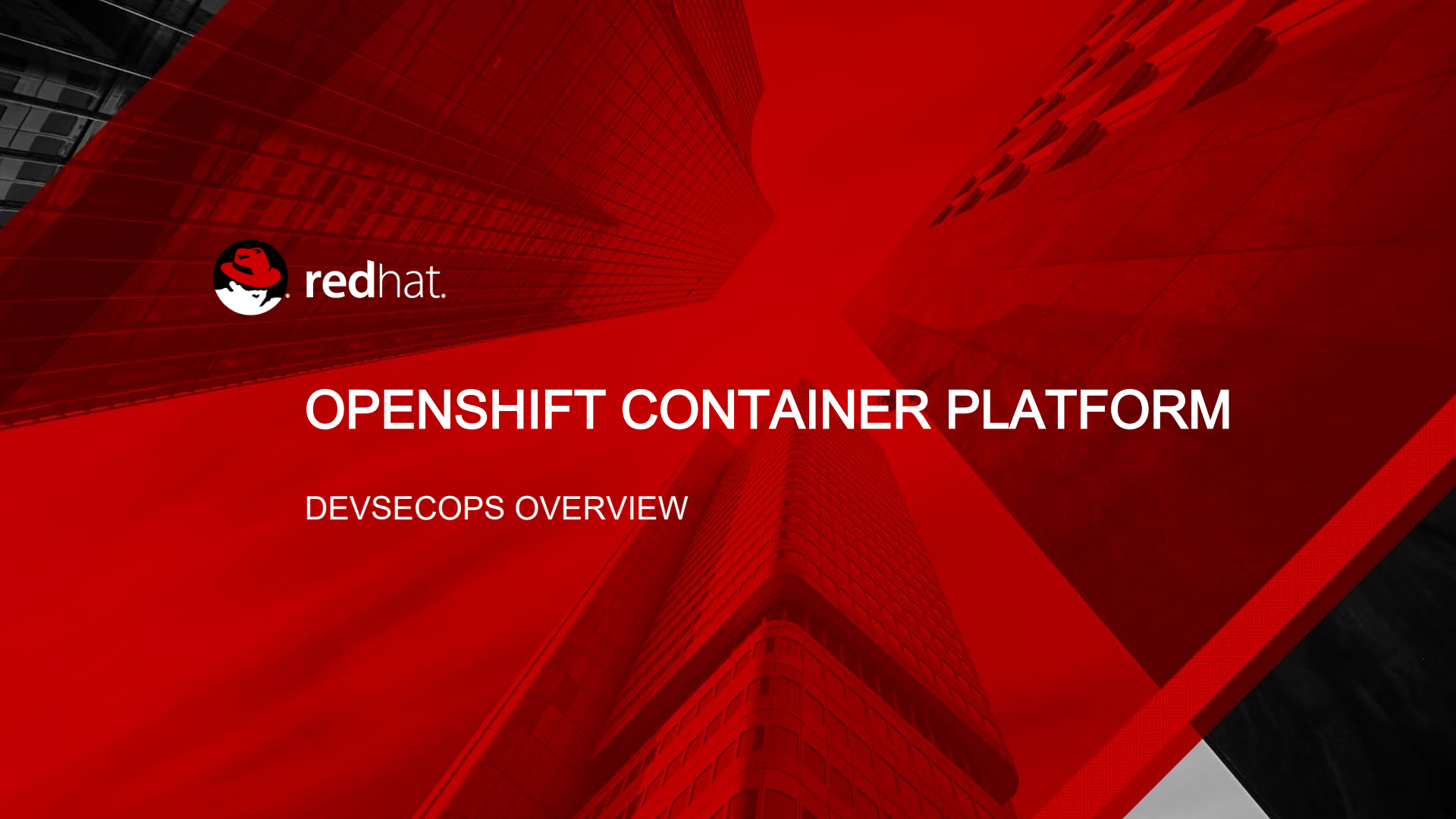


OPENSHIFT CONTAINER PLATFORM

DEVSECOPS OVERVIEW

AGENDA

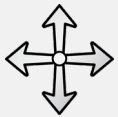
INTRODUCTION	Today’s Business Need
KEY CONCEPTS	Digital Transformation, DevSecOps, etc.
HOLISTIC VIEW	Technology Solution
STARTER PACK	DevSecOps CI/CD Pipeline

GENERAL DISTRIBUTION
redhat.

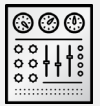
DIGITAL TRANSFORMATION NEEDS

Speed / Security

IT Optimization / App Modernization



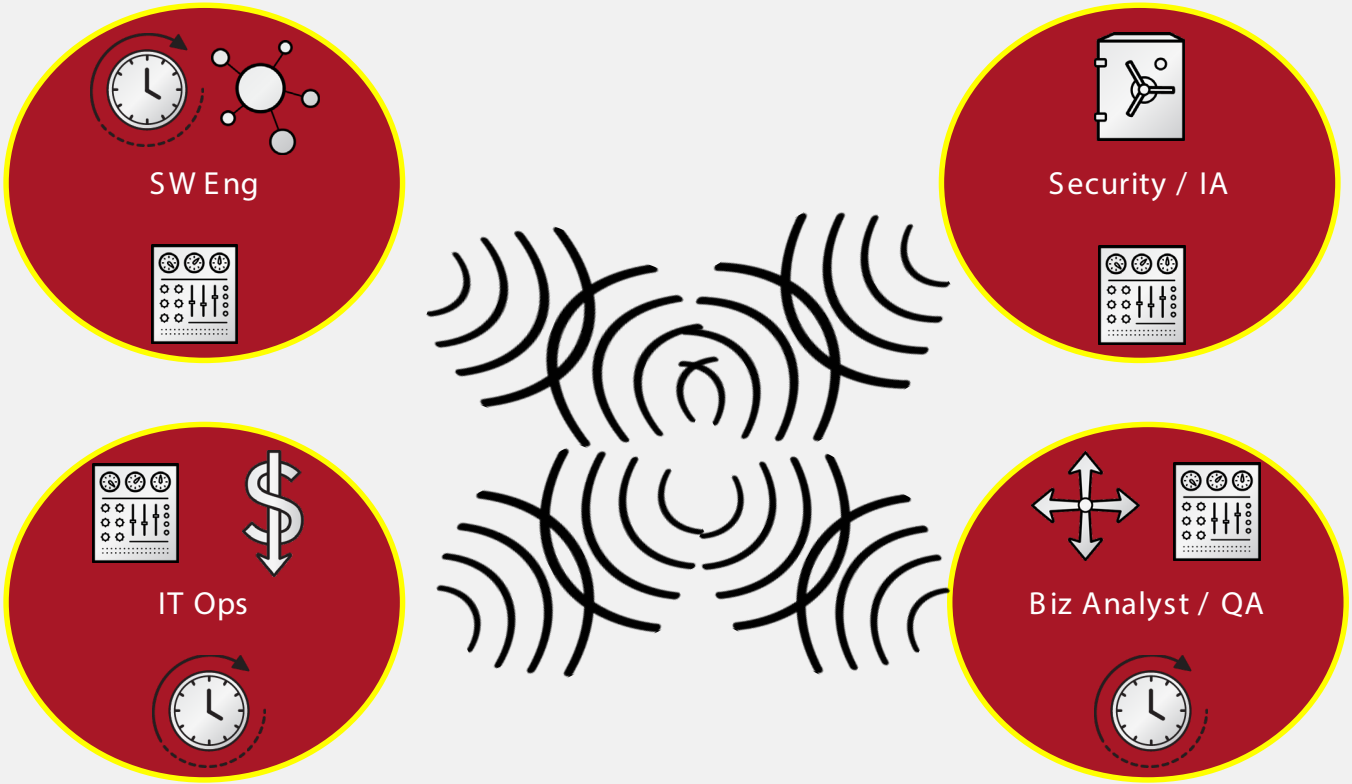
Path to the Cloud / Cloud First



GENERAL DISTRIBUTION

redhat.

THE CULTURAL CHALLENGE



GENERAL DISTRIBUTION

redhat.

THE CULTURAL CHALLENGE (CONT.)

Developers

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

IT Ops

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

QA/BA

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

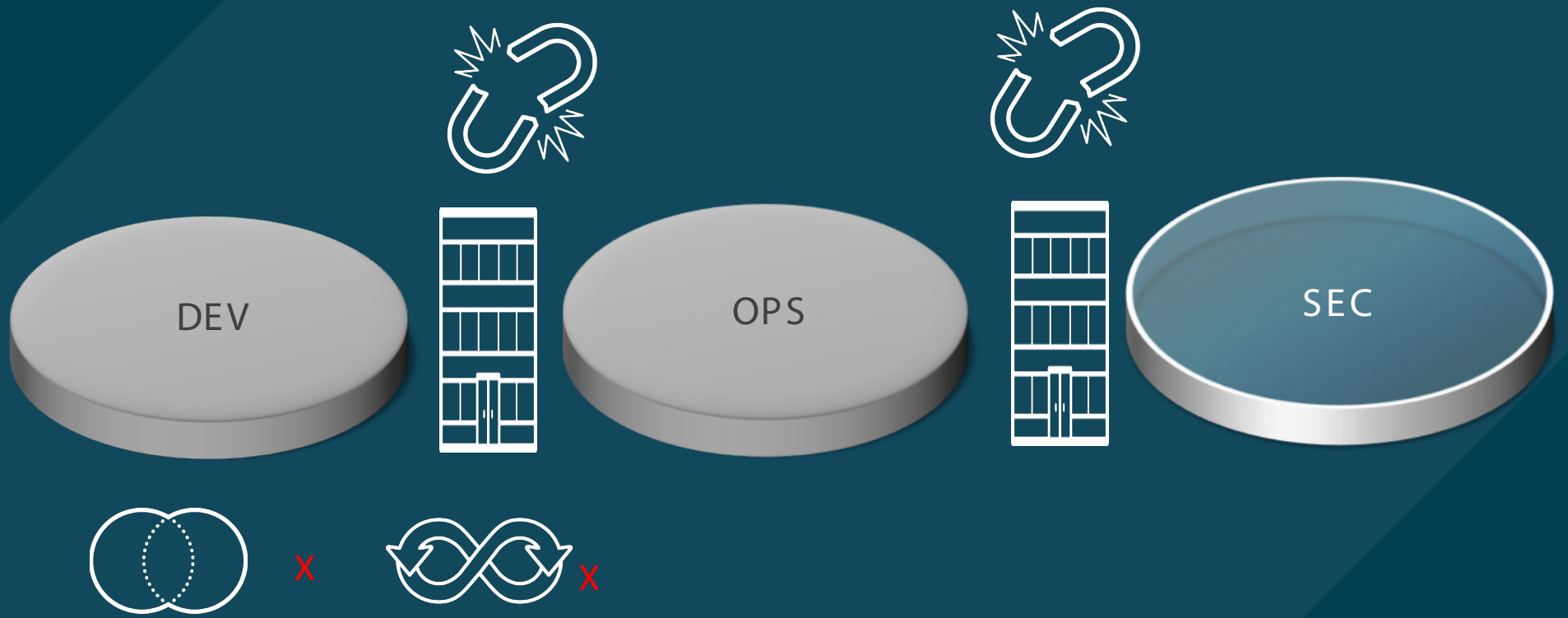
Security / IA

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

GENERAL DISTRIBUTION

redhat.

WHAT DOES THAT LOOK LIKE?

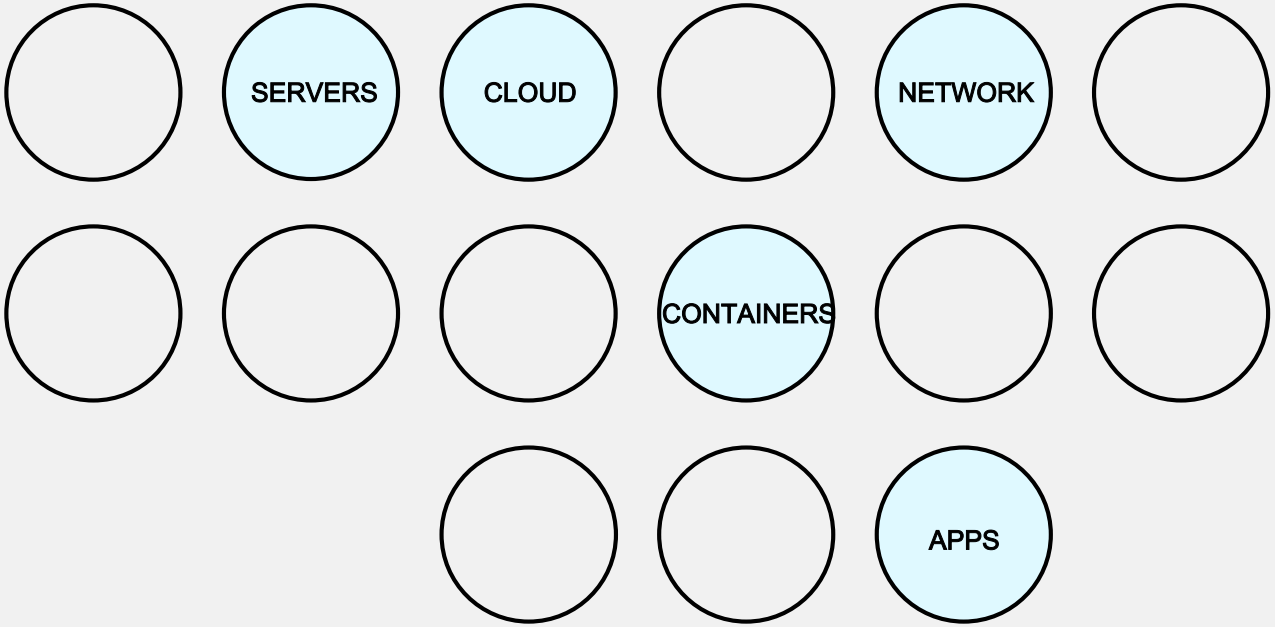


redhat.

MAYBE SOMETHING LIKE THIS?

redhat.

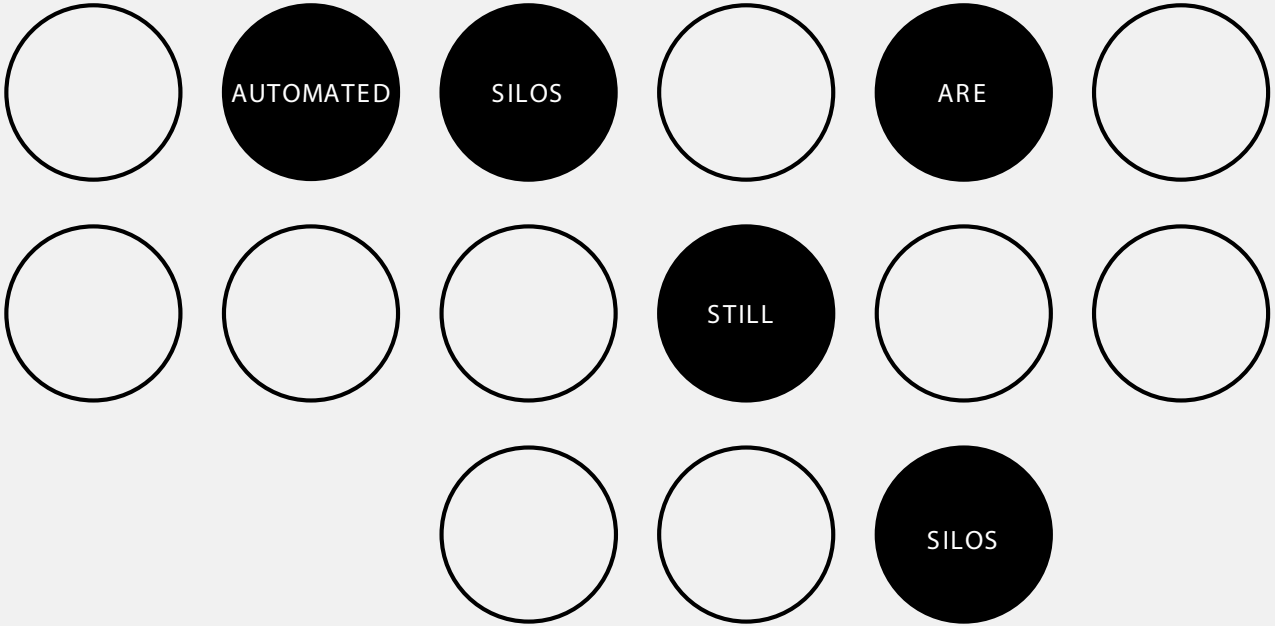
THE OPERATIONAL CHALLENGE



GENERAL DISTRIBUTION

redhat.

THE OPERATIONAL CHALLENGE (CONT.)



GENERAL DISTRIBUTION

redhat.

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

GENERAL DISTRIBUTION

THE TECHNICAL CHALLENGE

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

GENERAL DISTRIBUTION

redhat.

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

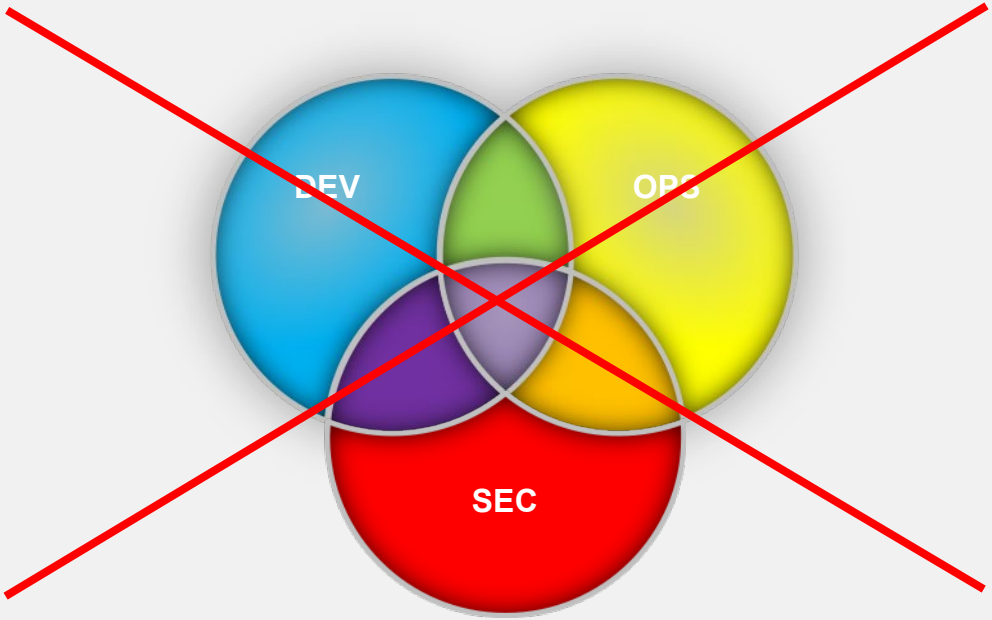
GENERAL DISTRIBUTION

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

–Peter Drucker

redhat.

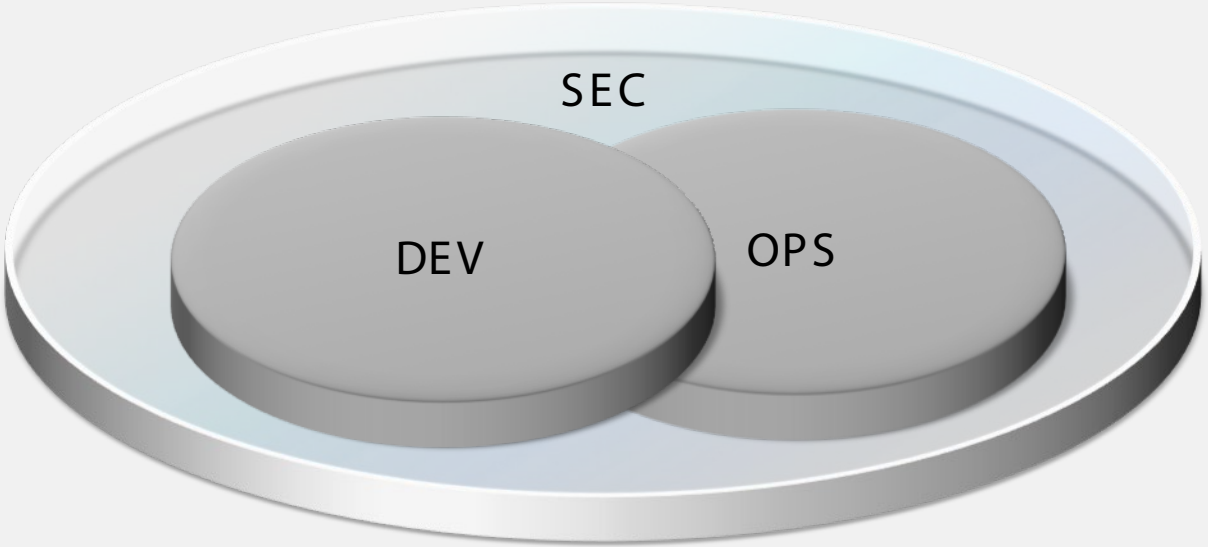
LETS FIRST DISPEL SOME MYTHS



GENERAL DISTRIBUTION

redhat.

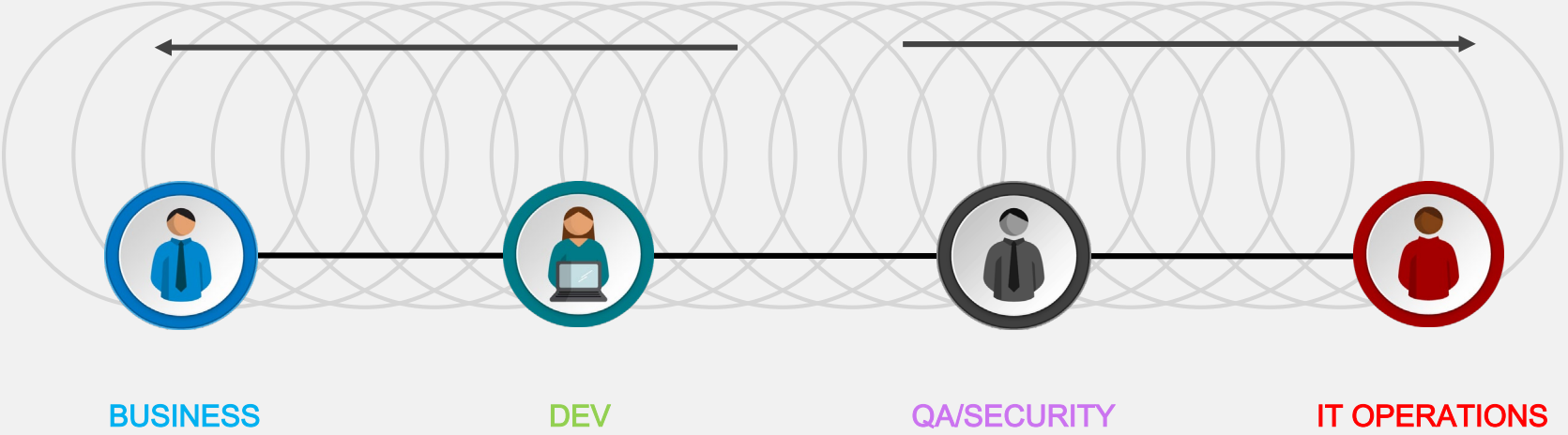
SECURITY ENCOMPASSES NOT INTERSECTS



GENERAL DISTRIBUTION

redhat.

ADDRESSING THE OPERATIONAL CHALLENGE



GENERAL DISTRIBUTION

redhat.

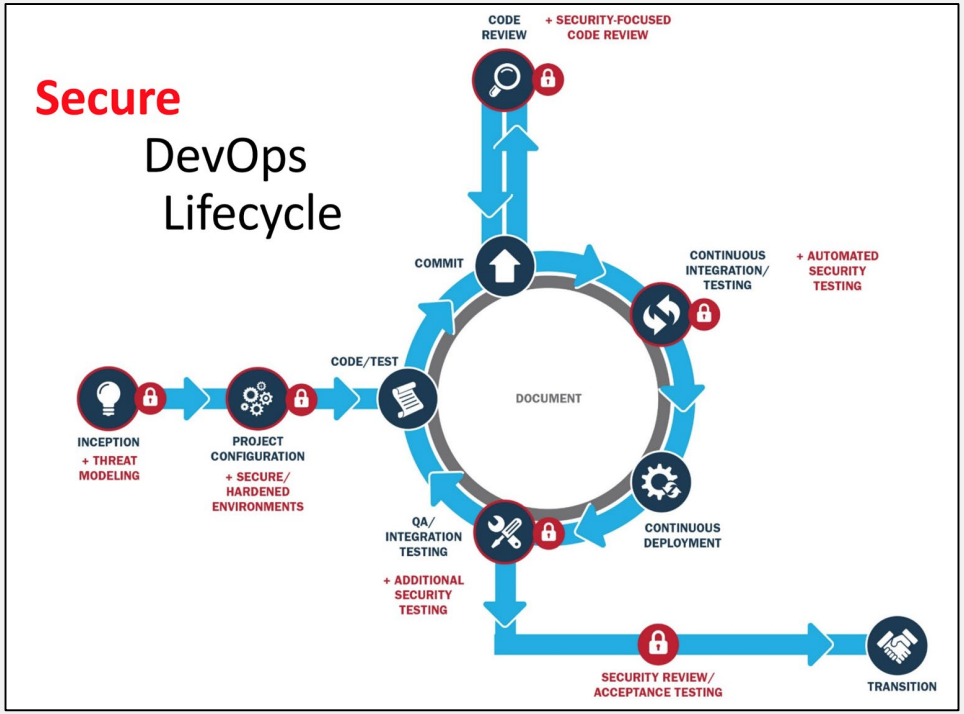
ADDRESSING THE TECHNICAL CHALLENGE

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

GENERAL DISTRIBUTION

redhat.

SO WHAT DOES THAT LOOK LIKE?

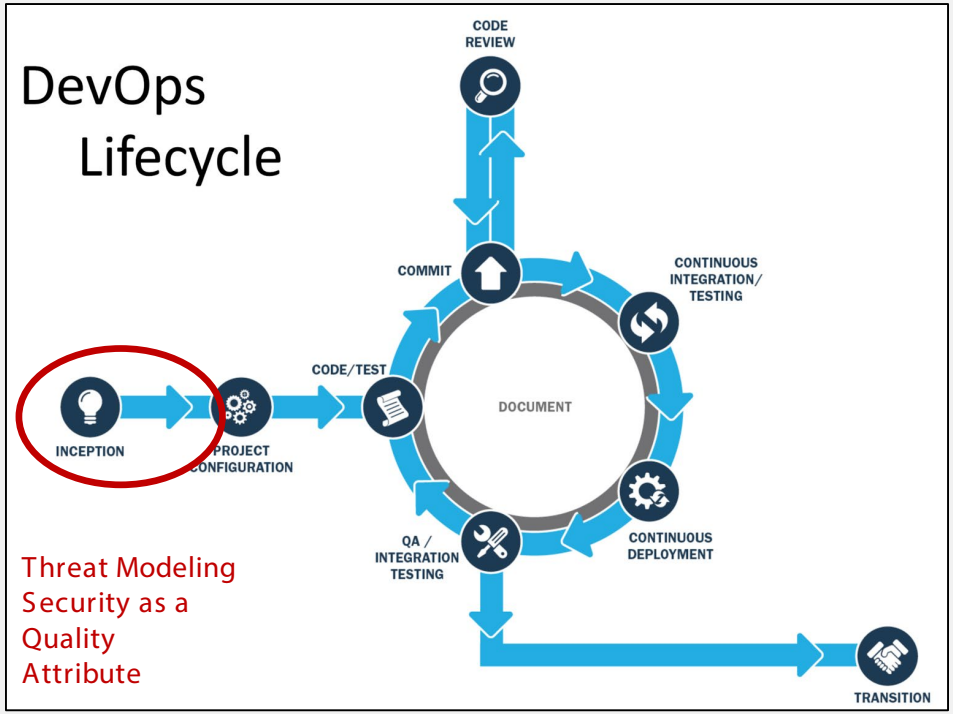


From All Day DevOps Webinar Nov 2016, Content distributable from Carnegie Mellon

GENERAL DISTRIBUTION

redhat.

“SHIFT LEFT” WITH SECURITY/IA



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

GENERAL DISTRIBUTION

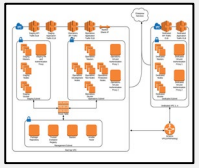
redhat.

WHAT DOES SECURE MEAN TO YOU?

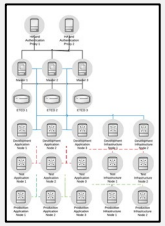
GENERAL DISTRIBUTION

redhat.

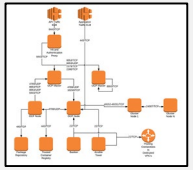
DON'T START FROM SCRATCH



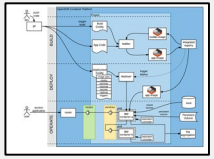
LOGICAL COMPONENT BLOCK DIAGRAM



CONTROLLED INTERFACE DIAGRAM

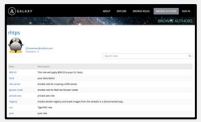


PHYSICAL CONNECTIVITY DIAGRAM



ROLE BASED ACTIVITY DIAGRAM

ROLE TO COMPONENT ALLOCATION



CUSTOM ANSIBLE ROLES

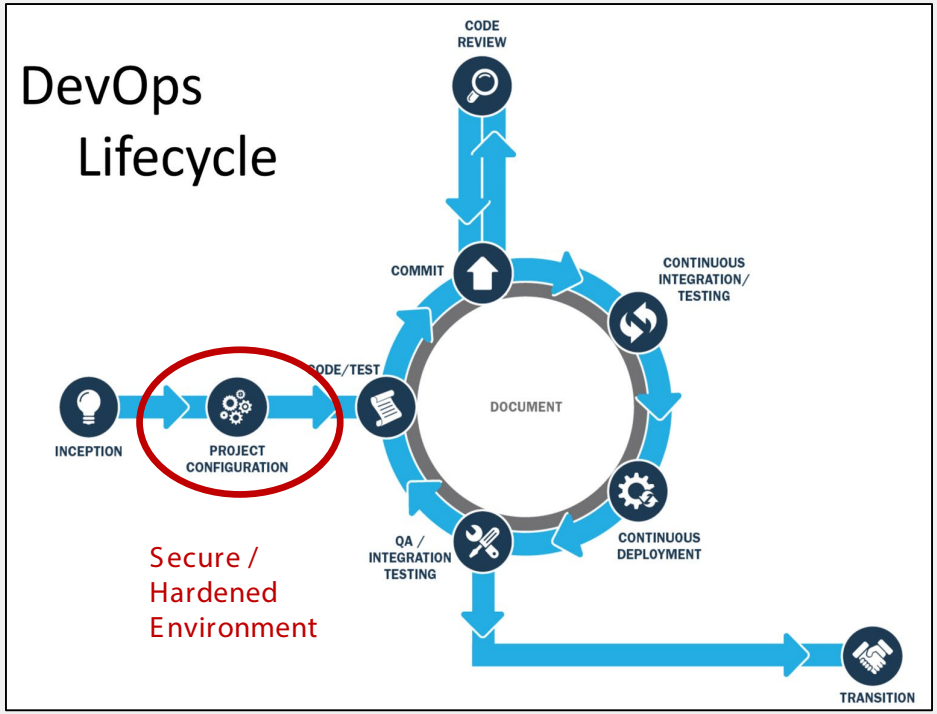
CENTRALIZED ARTIFACTS

Generic published reference architectures at https://goo.gl/Hz1gEJ

GENERAL DISTRIBUTION

redhat.

ADOPT A SECURITY INHERITANCE MODEL

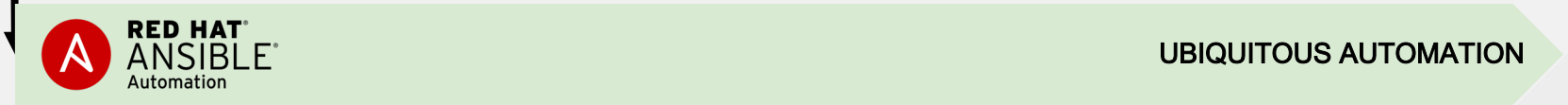


From All Day DevOps Webinar Nov 2016, Content distributable from Carnegie Mellon

GENERAL DISTRIBUTION

redhat.

DEPLOYING A SECURE SOFTWARE FACTORY



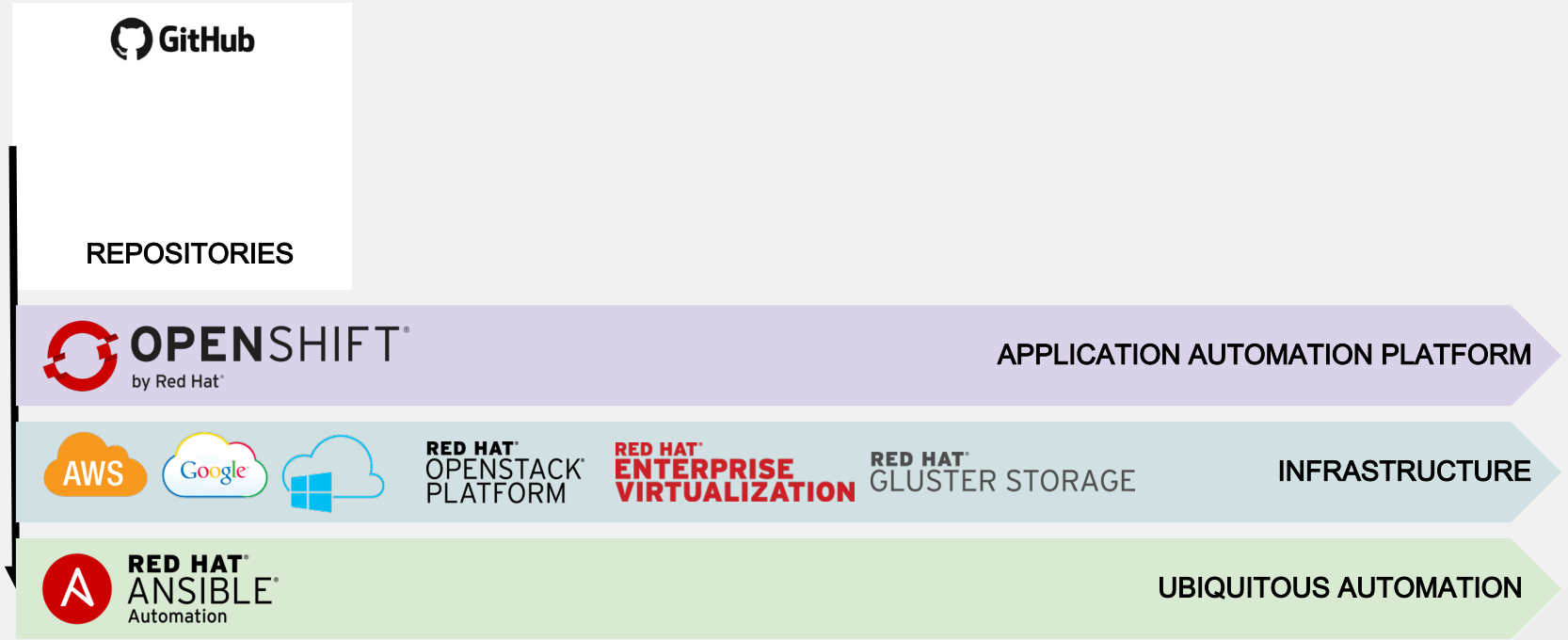
GENERAL DISTRIBUTION

redhat.

DEPLOYING A SECURE SOFTWARE FACTORY

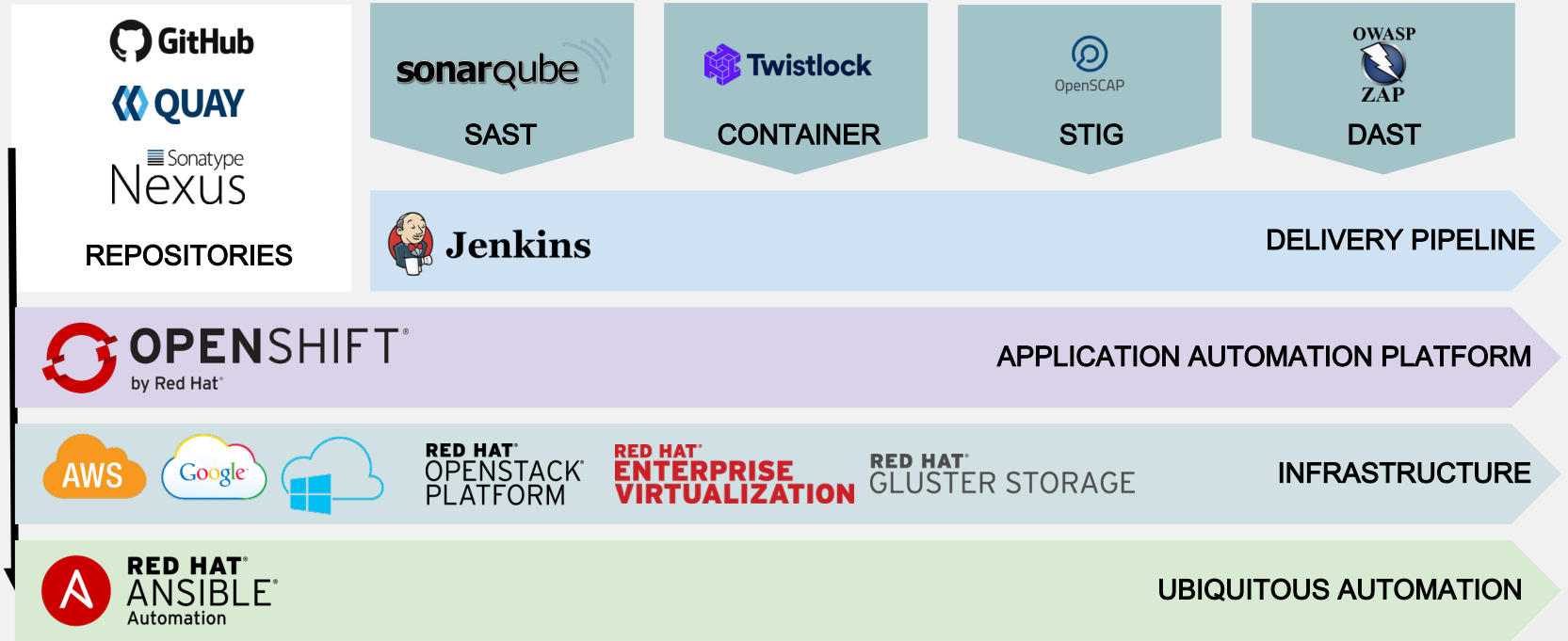
GENERAL DISTRIBUTION

DEPLOYING A SECURE SOFTWARE FACTORY



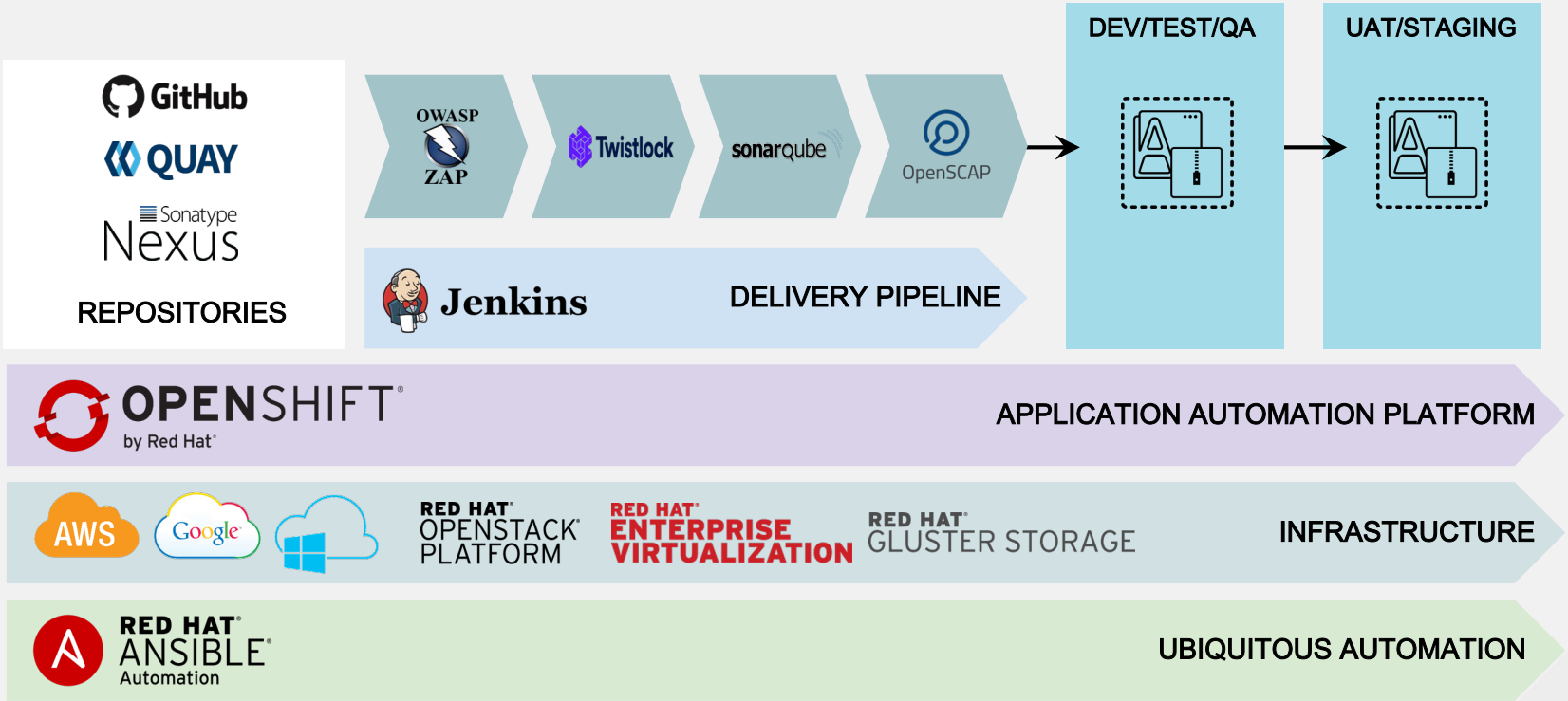
GENERAL DISTRIBUTION

DEPLOYING A SECURE SOFTWARE FACTORY



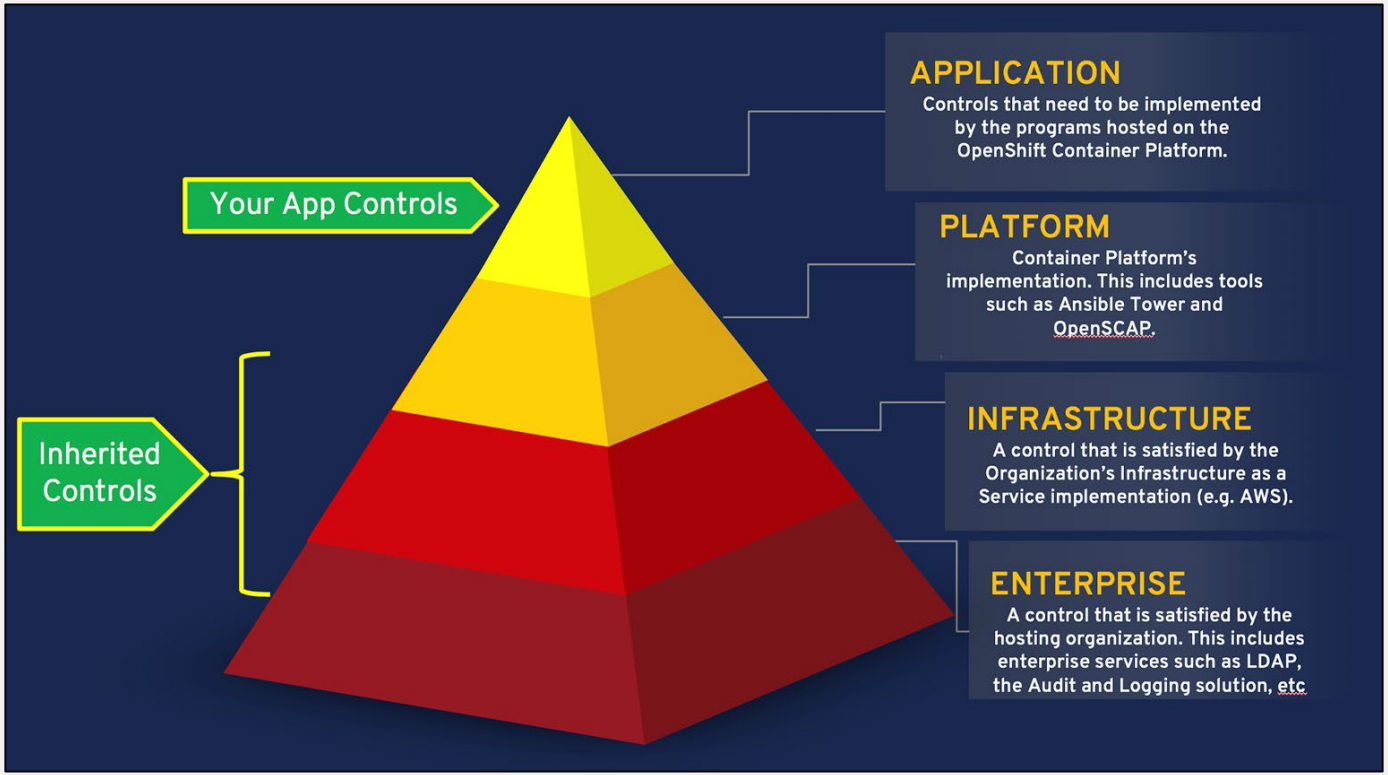
GENERAL DISTRIBUTION

EXERCISING A SECURE SOFTWARE FACTORY



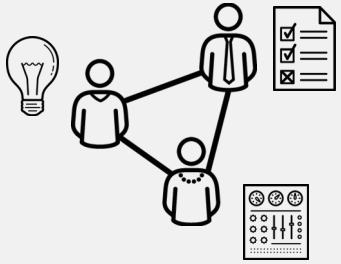
GENERAL DISTRIBUTION

SECURITY INHERITANCE MODEL



GENERAL DISTRIBUTION

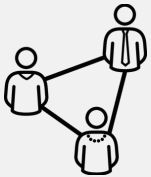
redhat.



PULL OR CREATE

SCM

BUILD LOAD SCAN SIGN

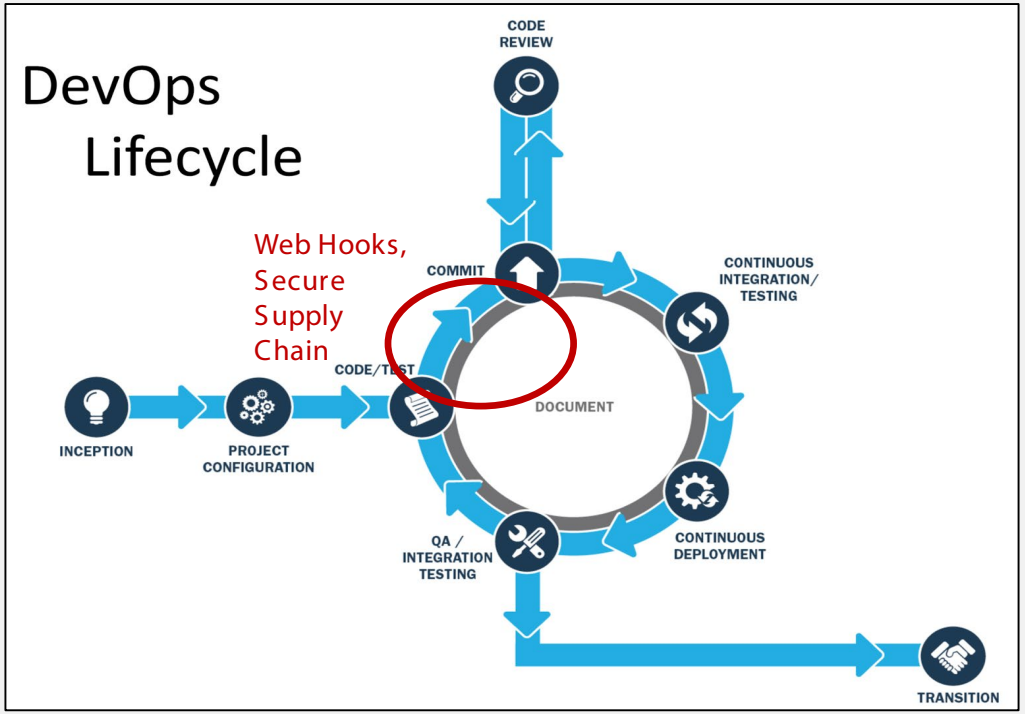


DEV INSPECT BUILD SCAN TEST DEPLOY MONITOR

GENERAL DISTRIBUTION

redhat.

ONLY INTRODUCE "APPROVED" ELEMENTS



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

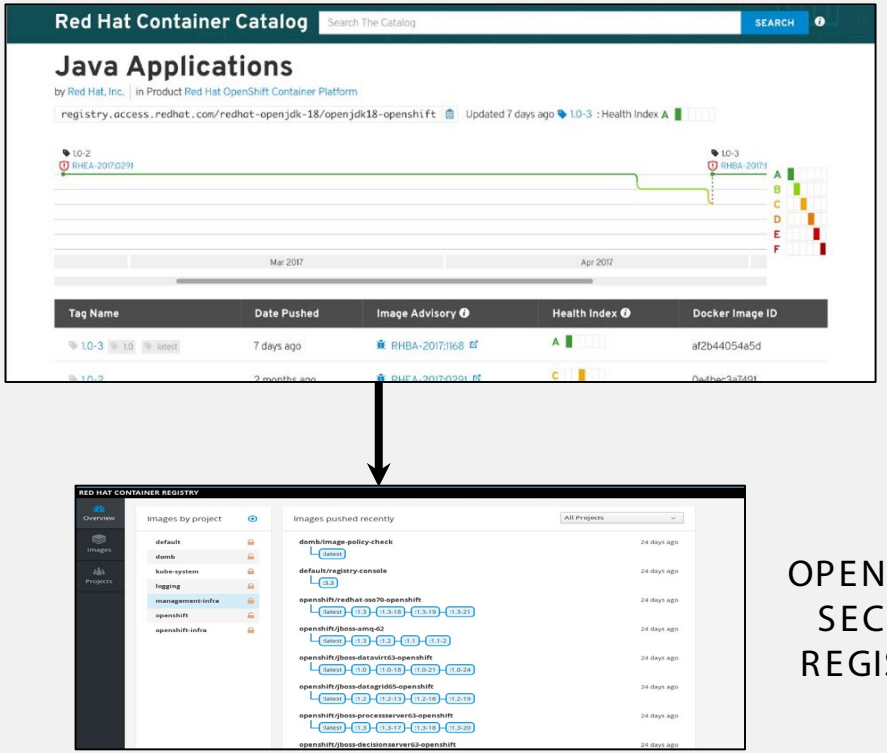
GENERAL DISTRIBUTION

redhat.

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

GENERAL DISTRIBUTION

redhat.

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

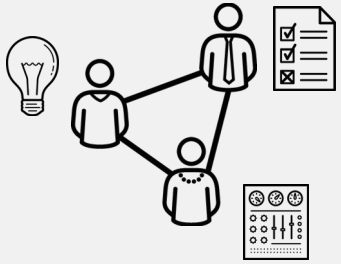
- Image Documentation
- Image Advisories

RED HAT® CONTAINER CATALOG

- Container Health Index
- Extensive Image Metadata

GENERAL DISTRIBUTION

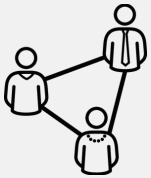
redhat.



PULL OR CREATE

SCM

BUILD | LOAD | SCAN | SIGN



Pre-receive Hooks With Security Compliance Checks

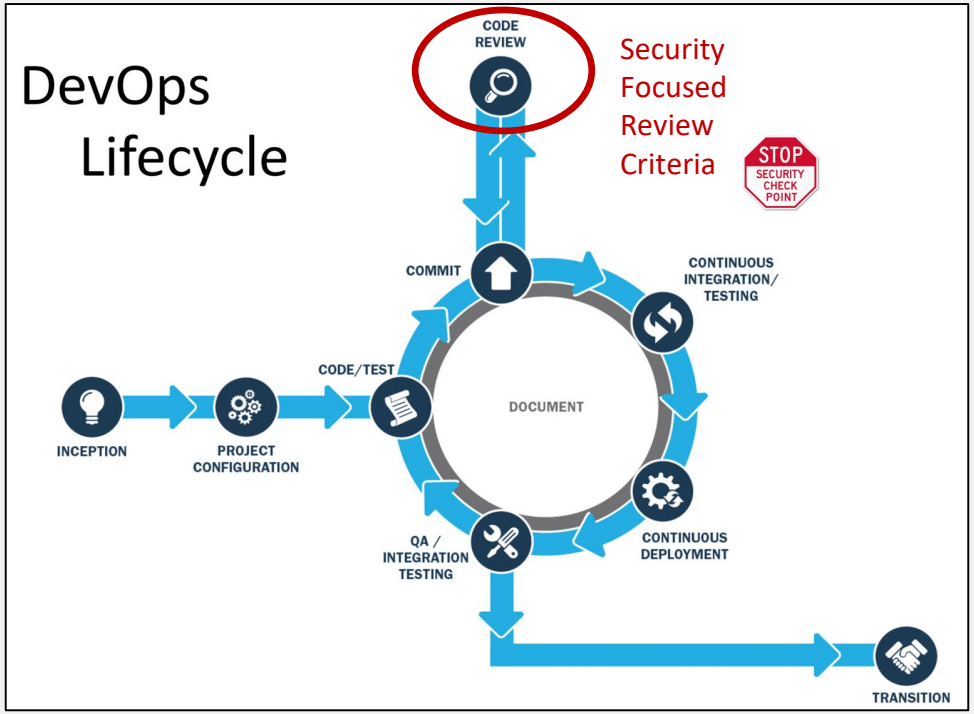
[GitHub]

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

GENERAL DISTRIBUTION

redhat.

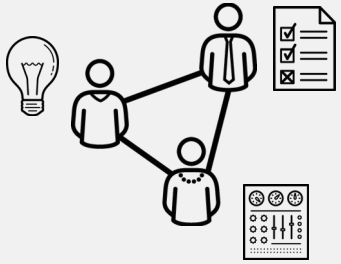
AUTOMATE WHAT YOU CAN & BUILD TRUST



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

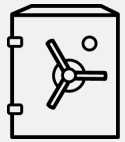
GENERAL DISTRIBUTION

redhat.

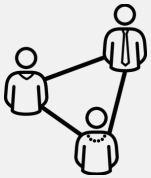


PULL OR CREATE

SCM



BUILD LOAD SCAN SIGN



Pre-receive Hooks With Security Compliance Checks

[GitHub]

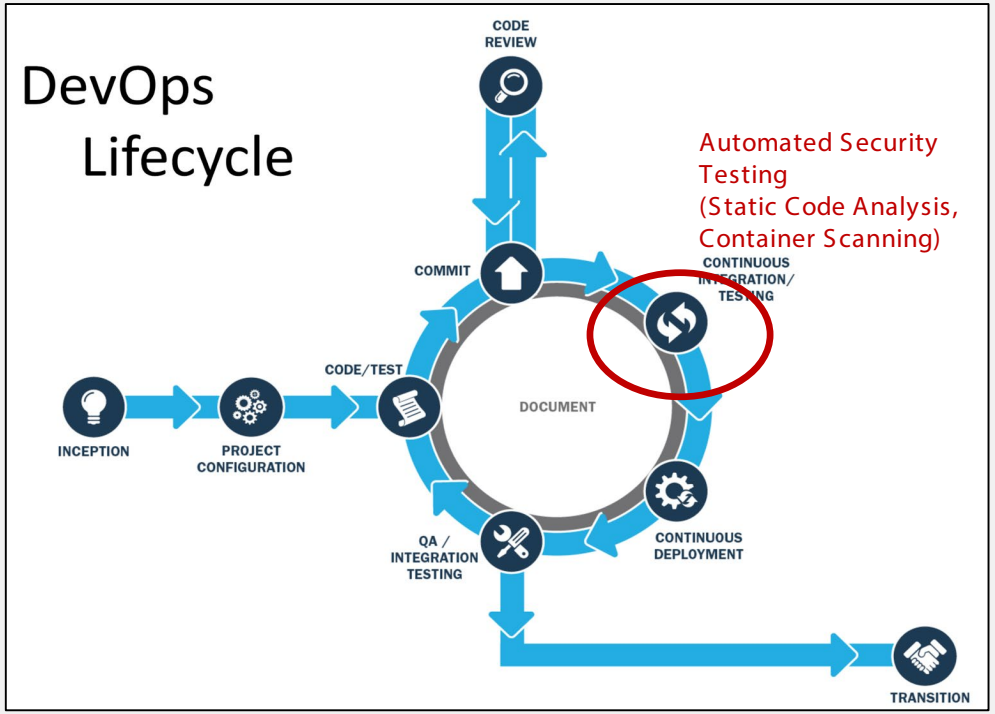
Code Review

DEV INSPECT BUILD SCAN TEST DEPLOY MONITOR

GENERAL DISTRIBUTION

redhat.

DON'T WASTE COMPUTE OR TIME

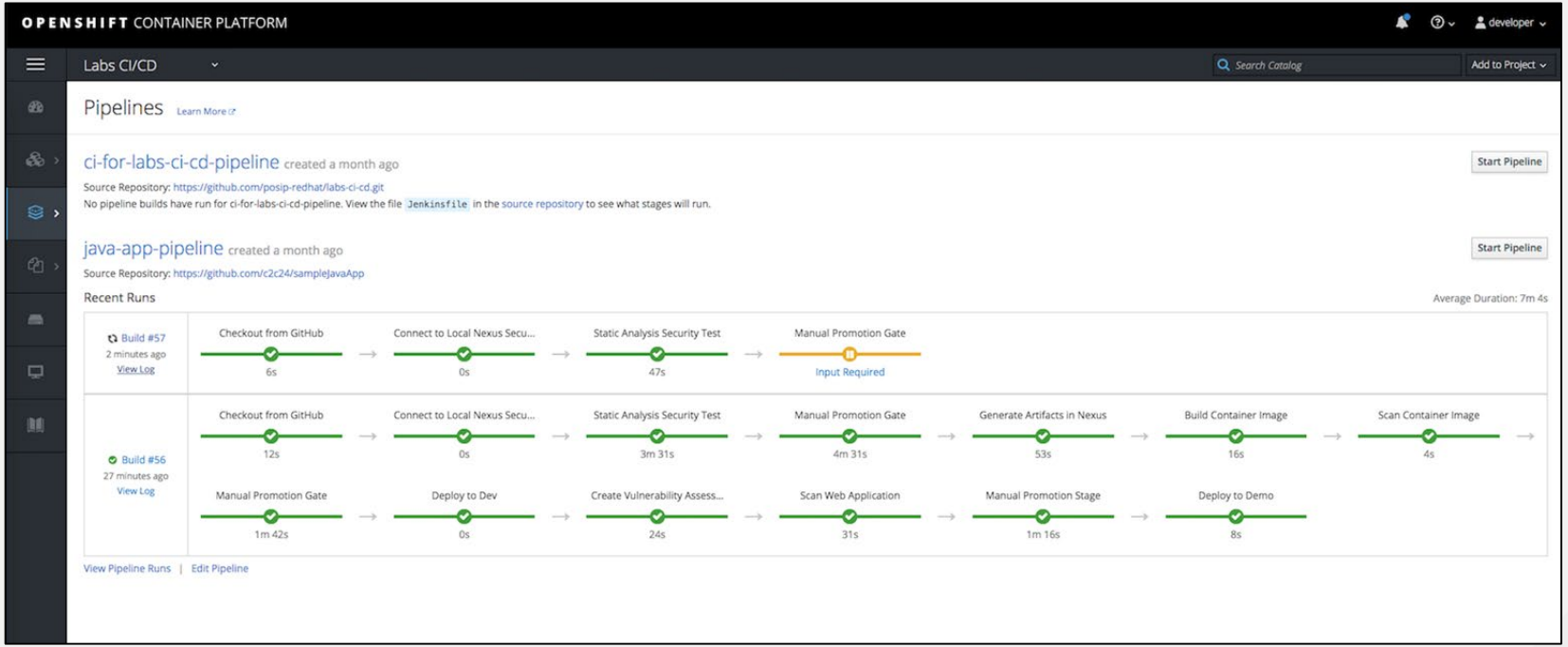


From All Day DevOps Webinar Nov 2016, Content distributable from Carnegie Mellon

GENERAL DISTRIBUTION

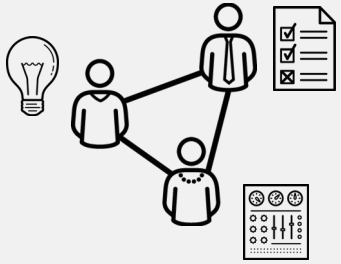
redhat.

DEMO OUTPUT FOR PIPELINE INVOCATION POST CODE REVIEW



GENERAL DISTRIBUTION

redhat.



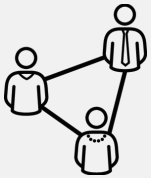
PULL OR CREATE

SCM

OPENSCAP EVALUATE & REMEDIATE

IMAGE

BUILD | LOAD | SCAN | SIGN



Pre-receive Hooks With Security Compliance Checks

[GitHub]

Static Analysis Security Test (SAST)

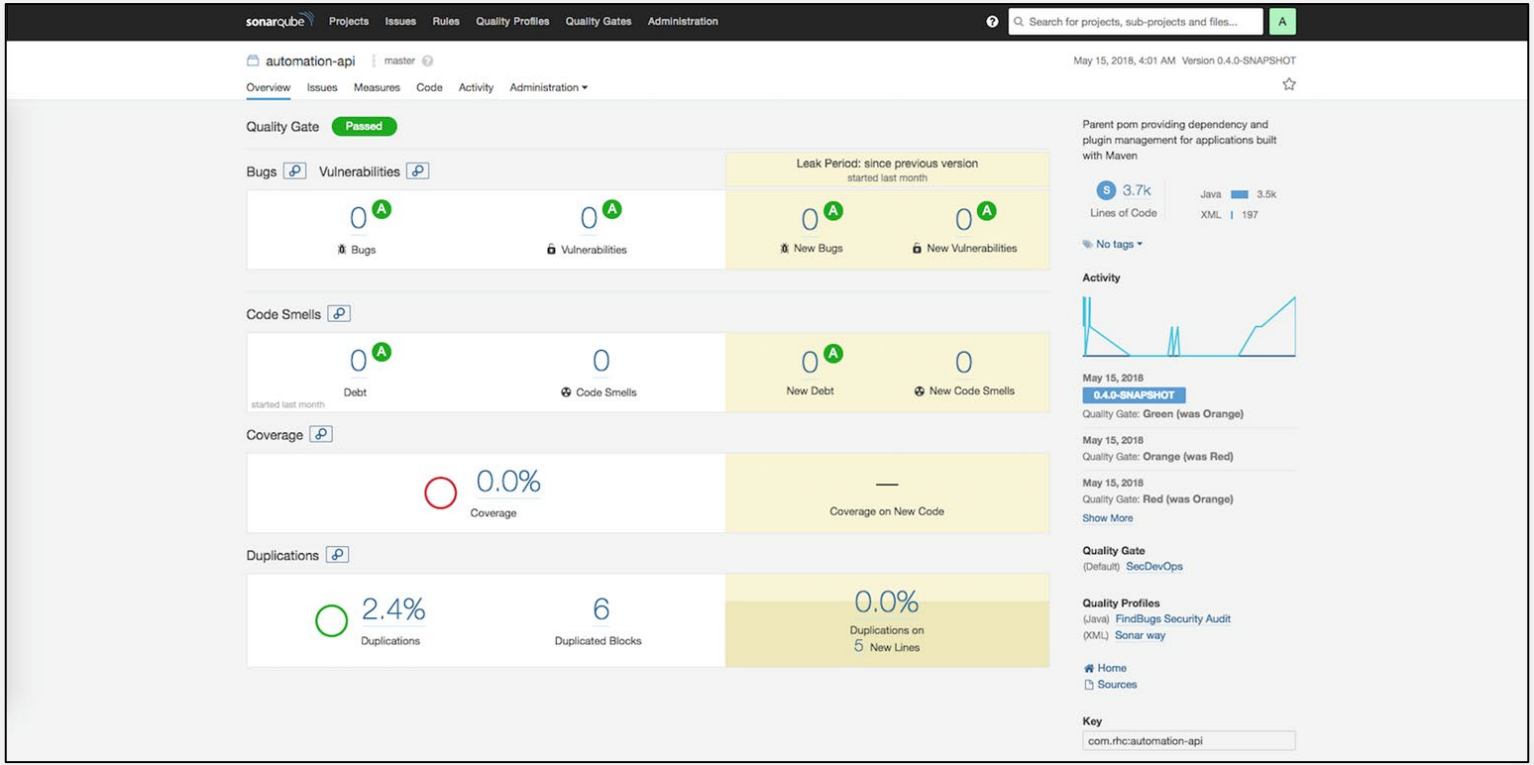
[SonarQube]

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

GENERAL DISTRIBUTION

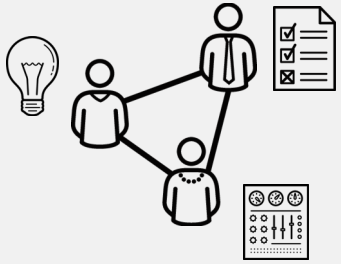
redhat.

DEMO OUTPUT FOR STATIC ANALYSIS SECURITY TEST



GENERAL DISTRIBUTION

redhat.



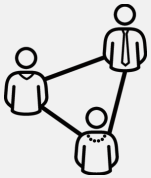
PULL OR CREATE

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

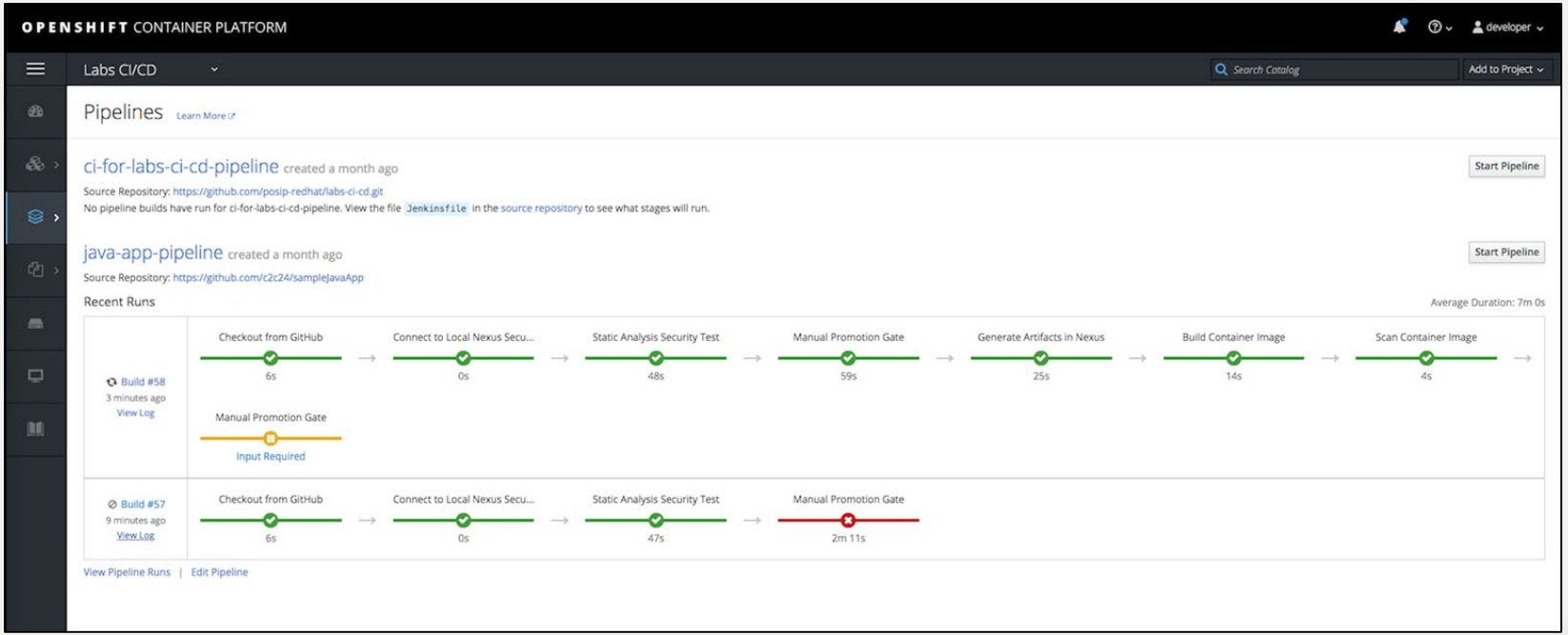
[OCP]

DEV INSPECT BUILD SCAN TEST DEPLOY MONITOR

GENERAL DISTRIBUTION

redhat.

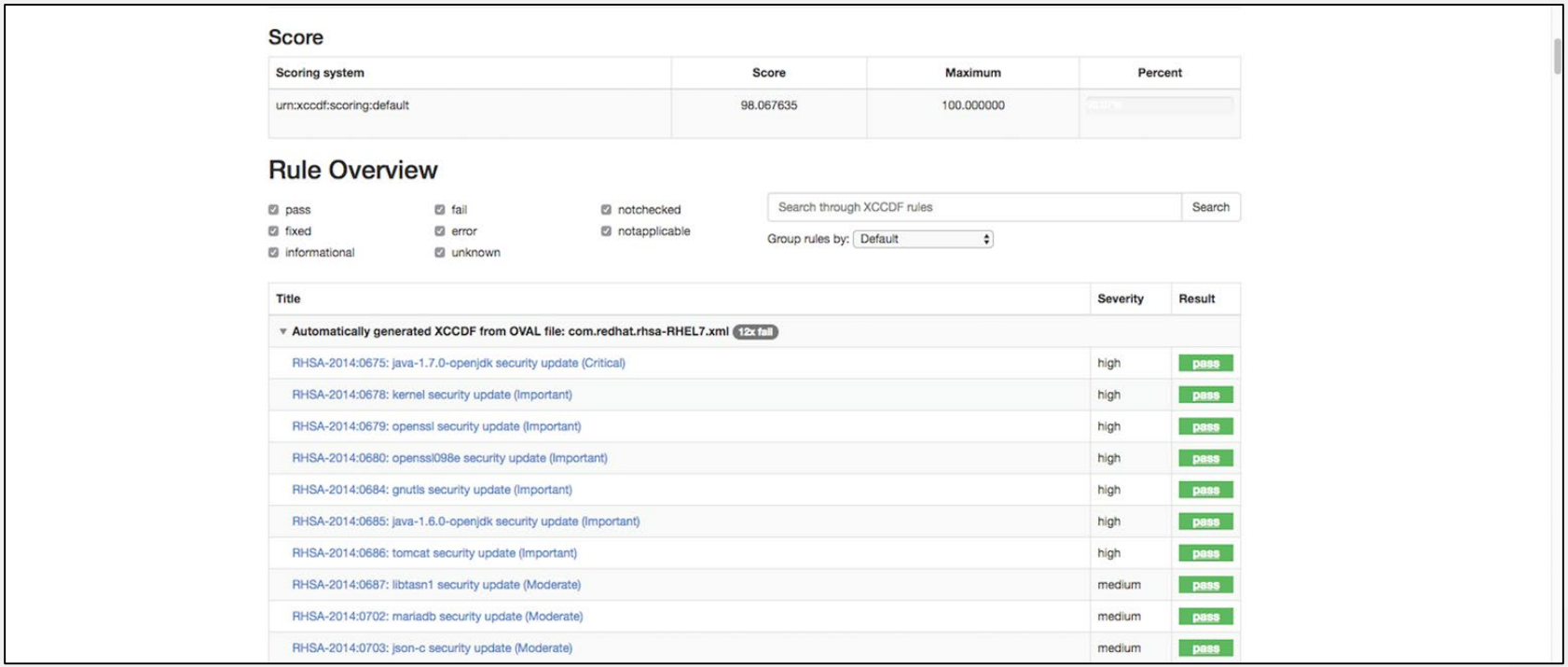
DEMO OUTPUT FOR OPENSCAP IMAGE SCAN FROM PIPELINE



GENERAL DISTRIBUTION

redhat.

DEMO OUTPUT FOR OPENSCAP IMAGE SCAN



Score

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

Rule Overview

pass fail notchecked
fixed error notapplicable
informational unknown

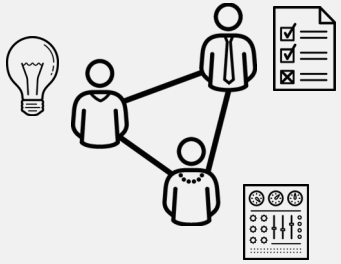
Search through XCCDF rules Search

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

GENERAL DISTRIBUTION

redhat.



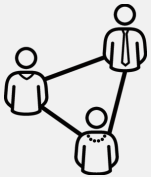
PULL OR CREATE

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]

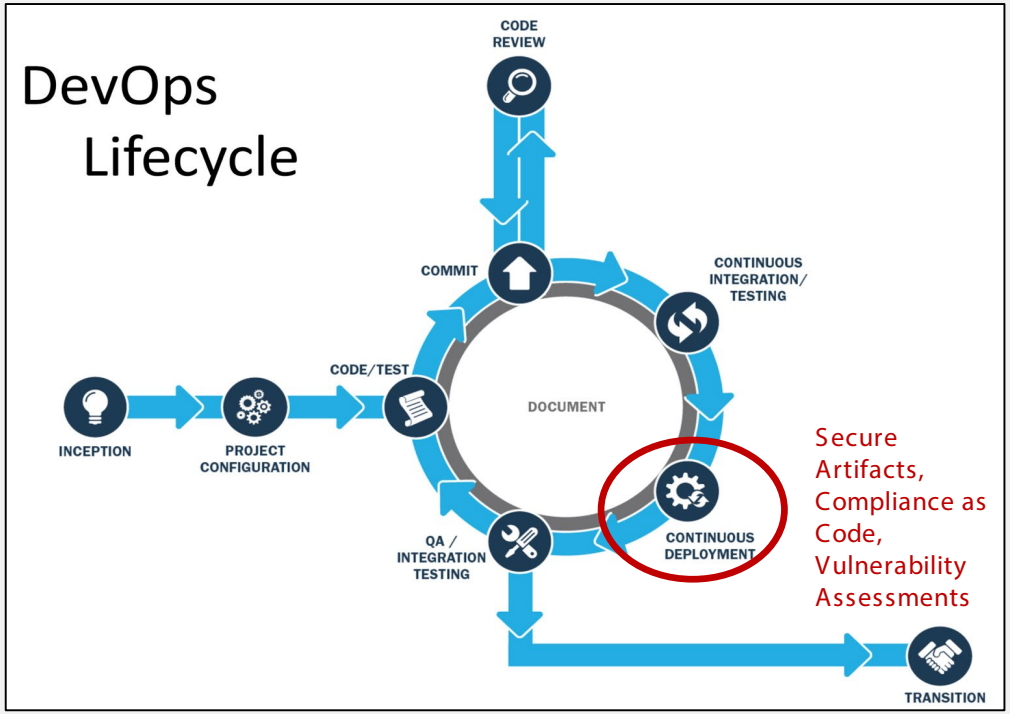
Compliance Check

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

GENERAL DISTRIBUTION

redhat.

POLICY DRIVEN DEPLOY AND COMPLIANCE

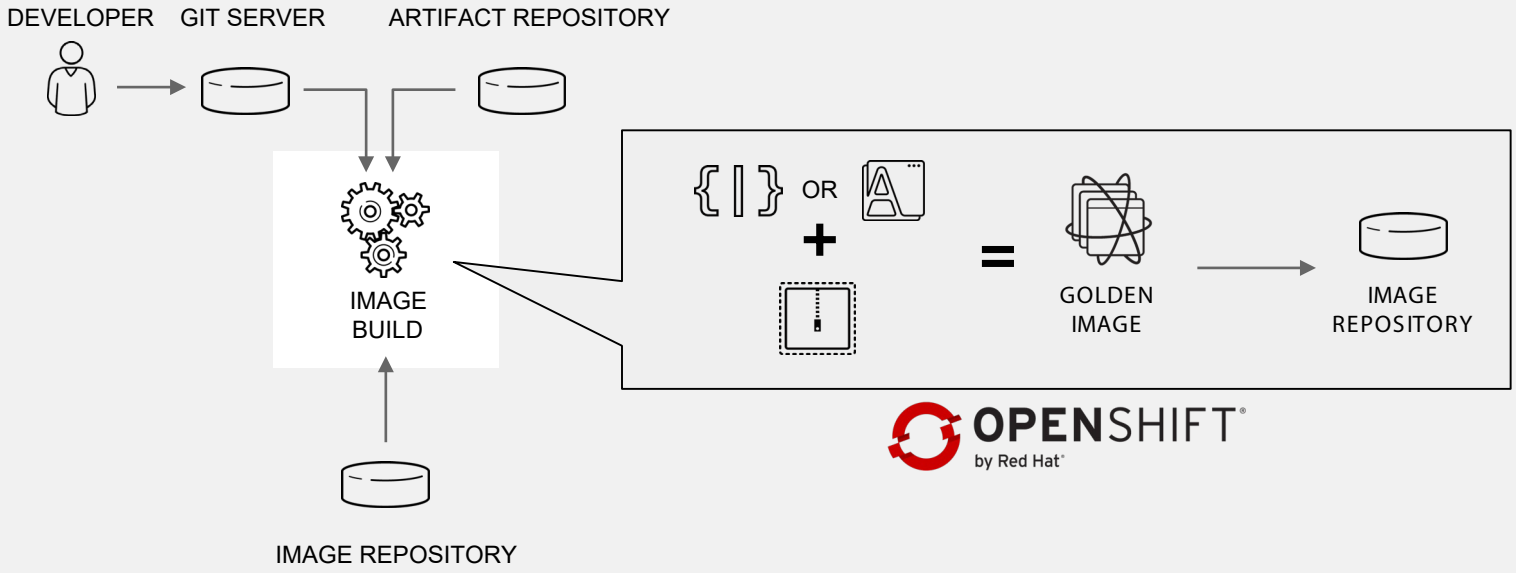


From All Day DevOps Webinar Nov 2016, Content distributable from Carnegie Mellon

GENERAL DISTRIBUTION

redhat.

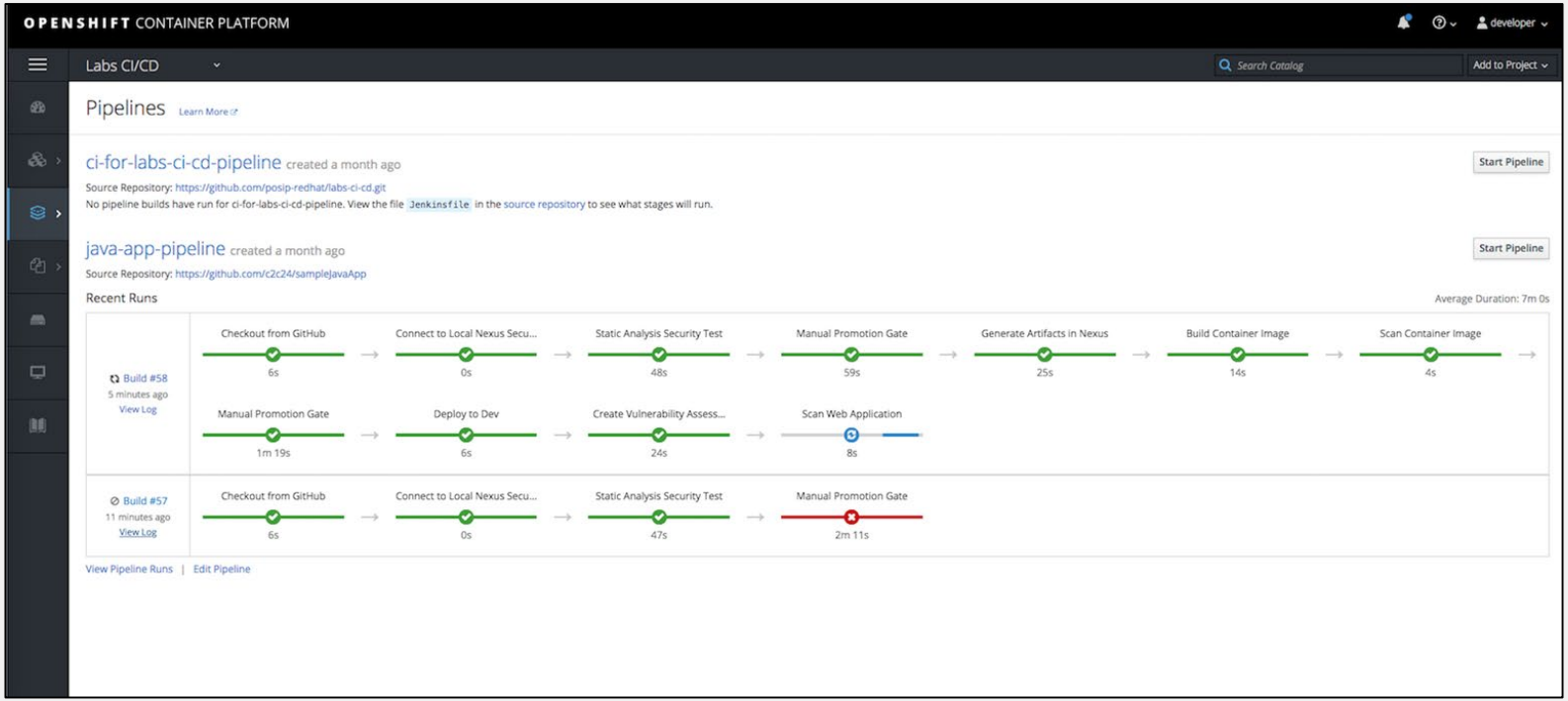
BUILDING APPLICATION ON OPENSHIFT



GENERAL DISTRIBUTION

redhat.

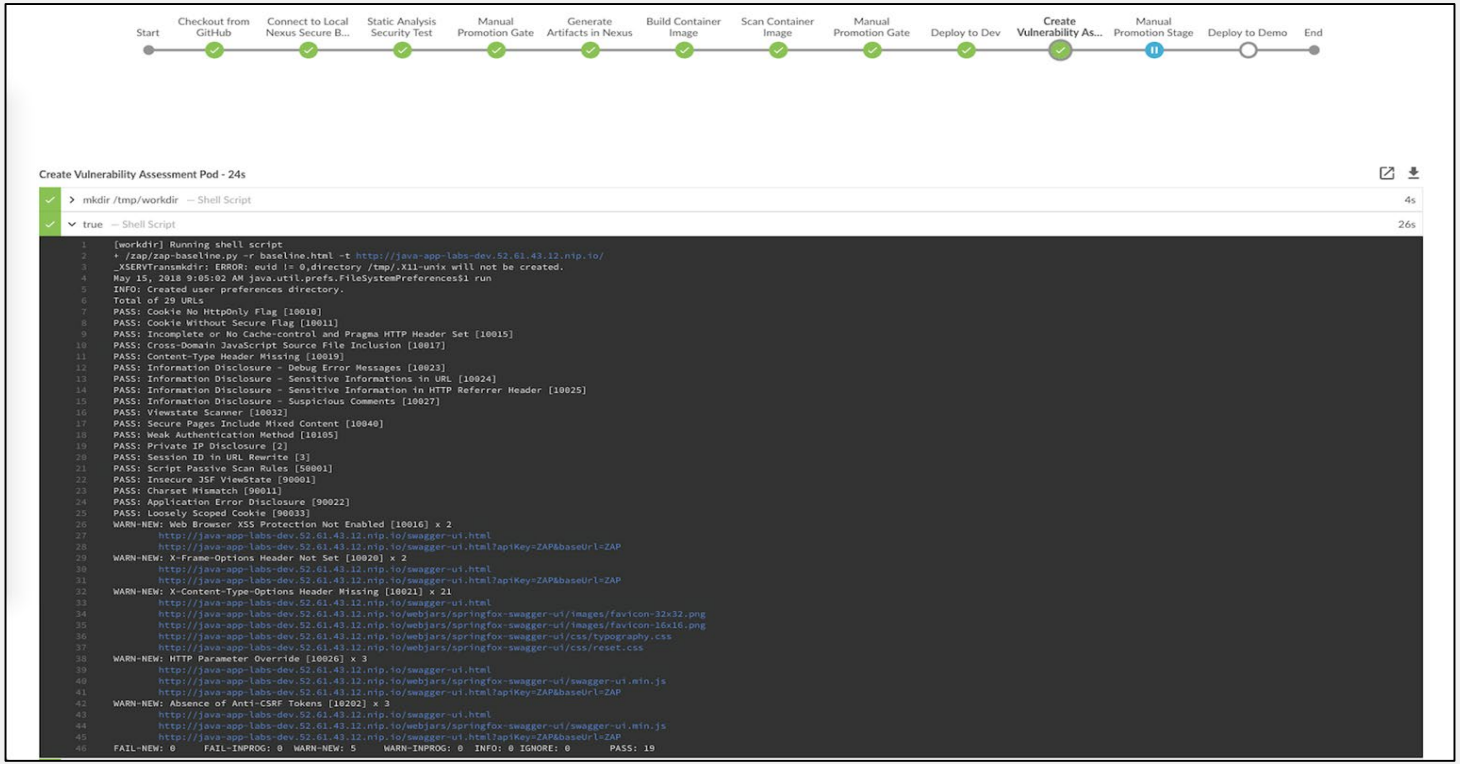
DEMO VULNERABILITY ASSESSMENT FROM PIPELINE



GENERAL DISTRIBUTION

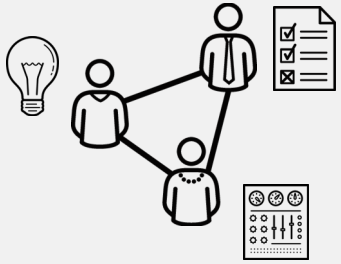
redhat.

DEMO OUTPUT FOR VULNERABILITY ASSESSMENT



GENERAL DISTRIBUTION

redhat.



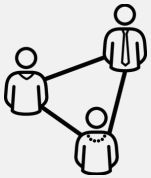
PULL OR CREATE

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)

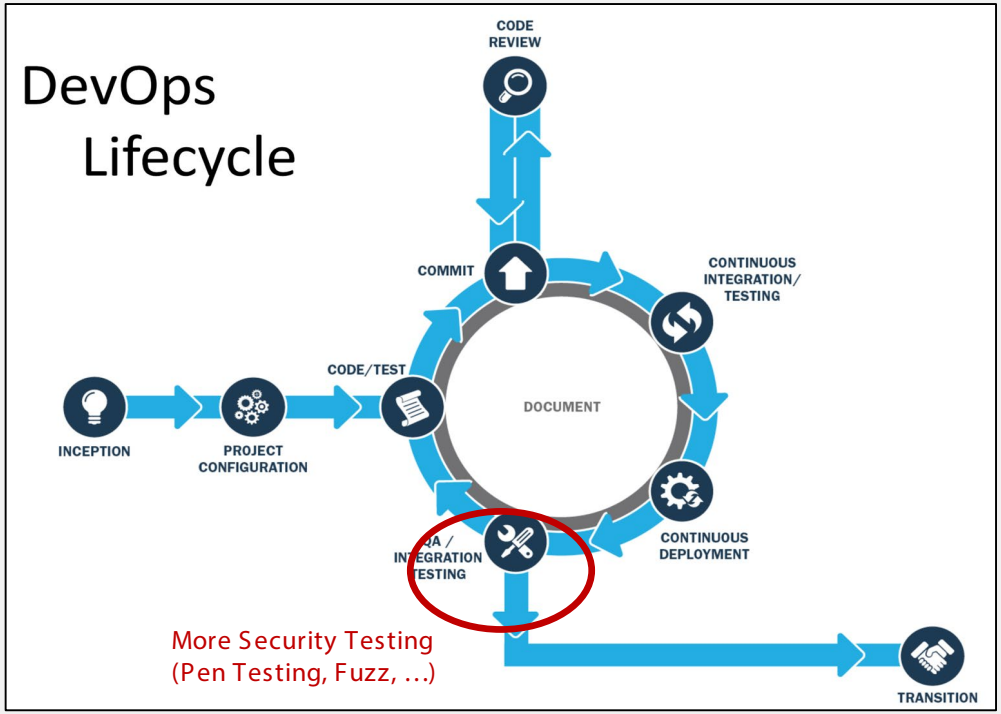
[ZAP]

DEV INSPECT BUILD SCAN TEST DEPLOY MONITOR

GENERAL DISTRIBUTION

redhat.

WHAT GETS MEASURED GETS IMPROVED



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

GENERAL DISTRIBUTION

redhat.

FROM CODE TO CAPABILITIES

DEV

- Pre-receive Hooks
- Static Analysis

BUILD

- Dependency Management
- Image Scan

DEPLOY

- Vulnerability Assessment
- Signed Images

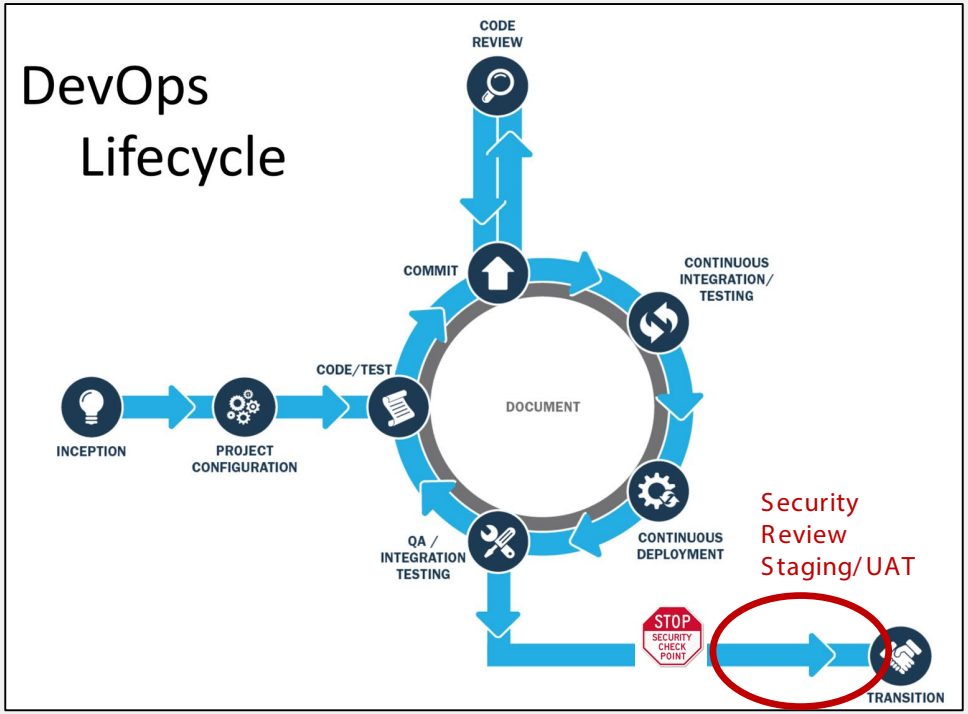
TEST

- Integration Tests
- Penetration / Fuzz Testing

GENERAL DISTRIBUTION

redhat.

CONTINUE TO BUILD TRUST AND AUTOMATE

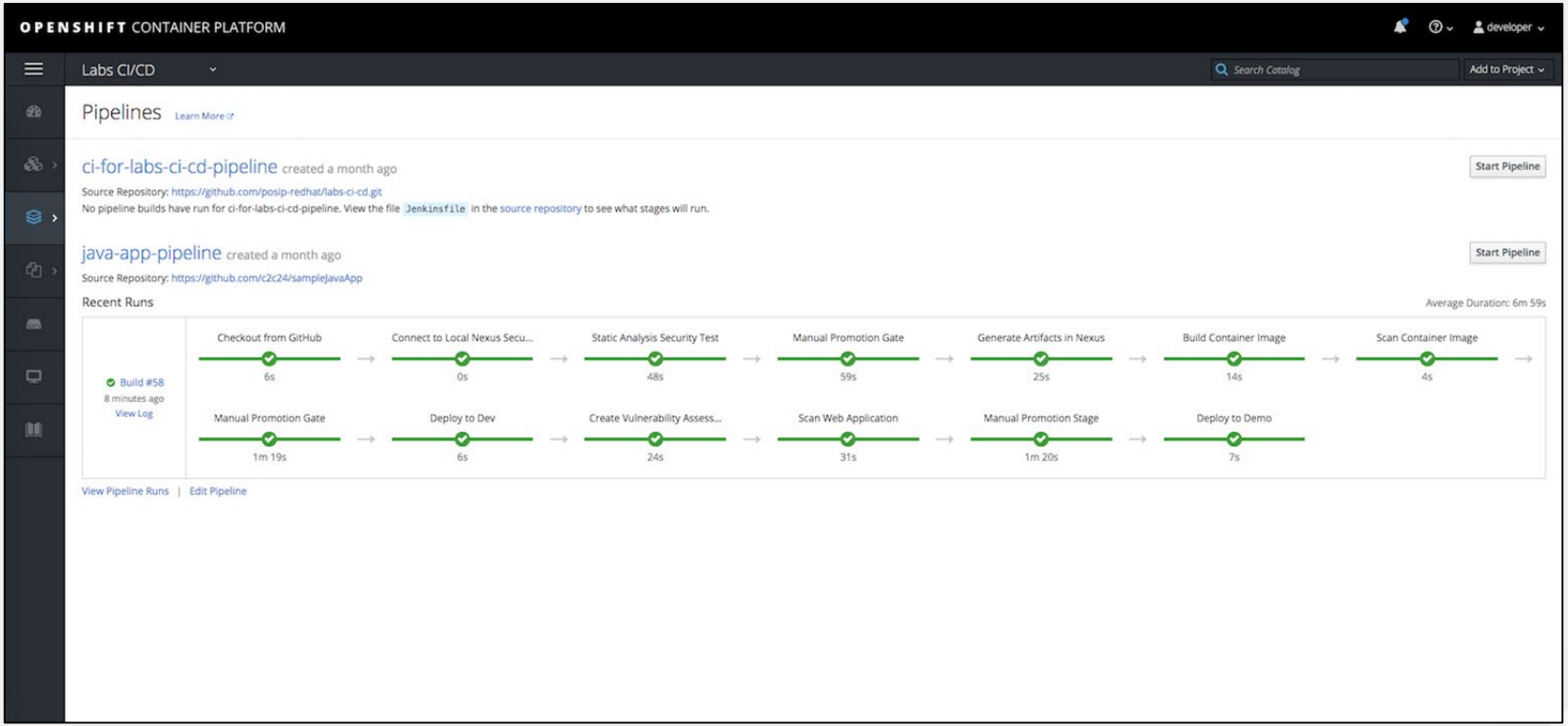


From All Day DevOps Webinar Nov 2016, Content distributable from Carnegie Mellon

GENERAL DISTRIBUTION

redhat.

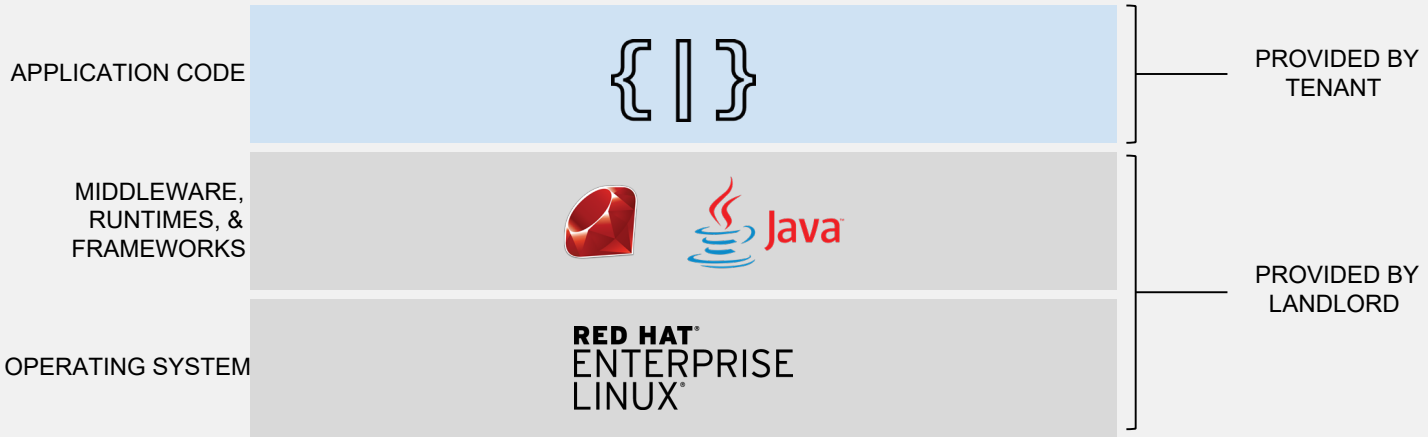
DEMO OUTPUT OF COMPLETED PIPELINE



GENERAL DISTRIBUTION

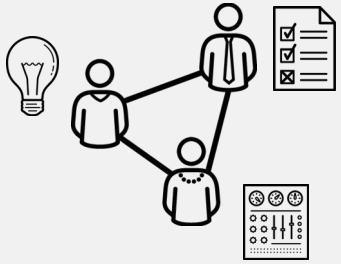
redhat.

THE GOLDEN IMAGE



GENERAL DISTRIBUTION

redhat.



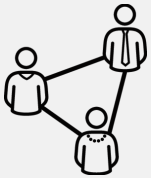
PULL OR CREATE

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]

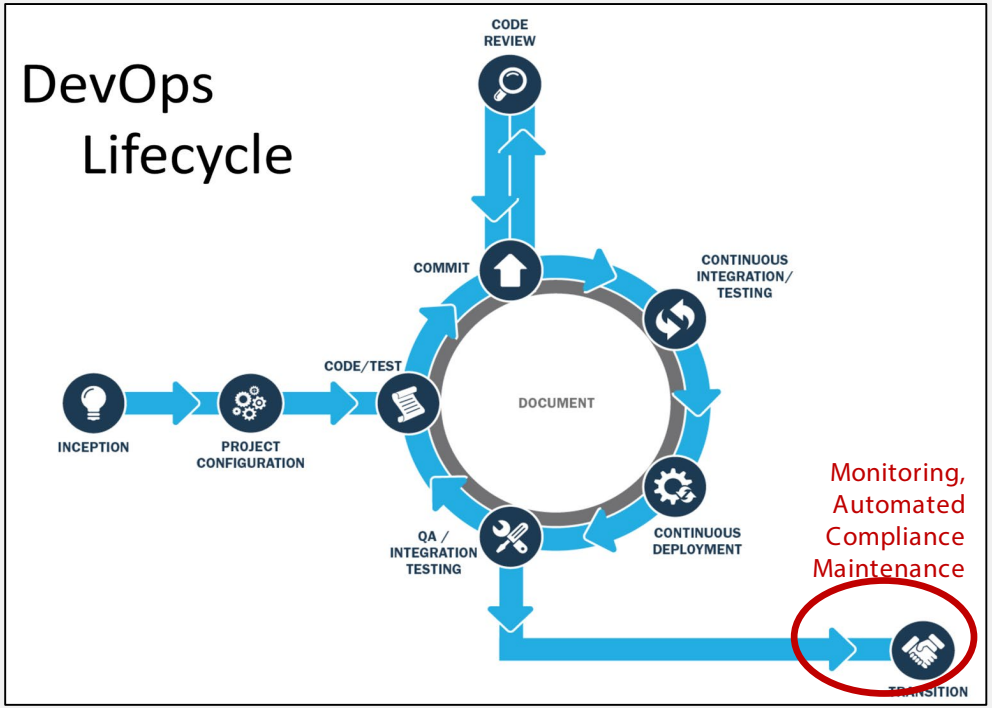
Push/Pull Signed Images [OCP]

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

GENERAL DISTRIBUTION

redhat.

ITERATIVE SECURE DEPLOYMENTS

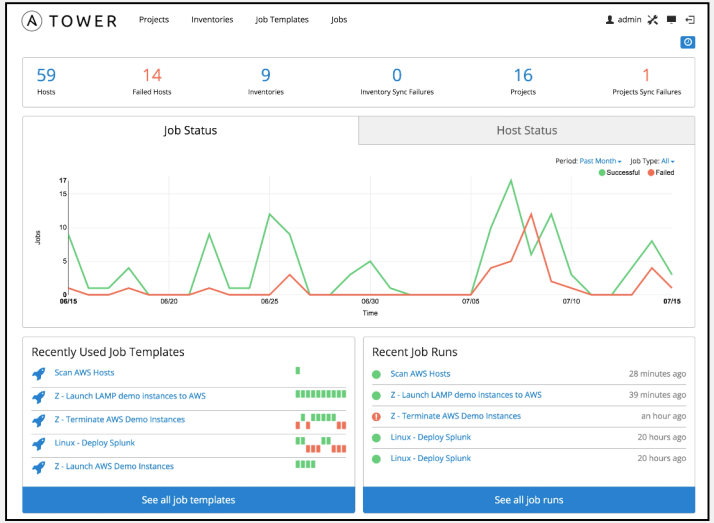


From All Day DevOps Webinar Nov 2016, Content distributable from Carnegie Mellon

GENERAL DISTRIBUTION

redhat.

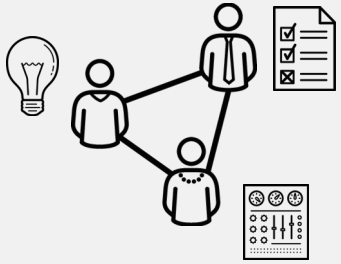
DAY-2 OPERATIONS SAMPLE VIEW FROM ANSIBLE TOWER



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

GENERAL DISTRIBUTION
redhat.



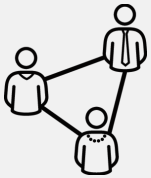
PULL OR CREATE

SCM

OPENSCAP EVALUATE & REMEDIATE

IMAGE

BUILD | LOAD | SCAN | SIGN



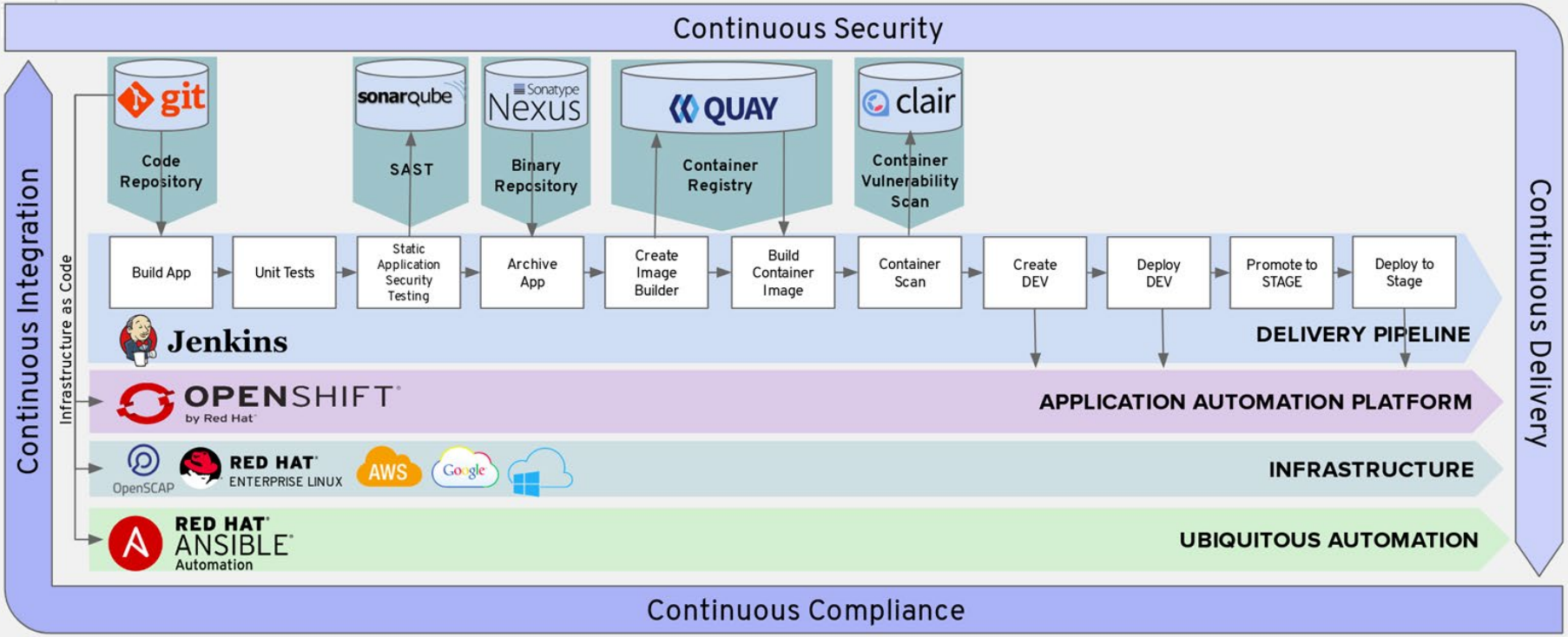
Pre-receive Hooks With Security Compliance Checks [GitHub]	Static Analysis Security Test (SAST) [SonarQube]	Policy Enforcement For Build Artifacts & Images [OCP]	Image Scanning w/ tailored profiles [OpenSCAP] [Clair]	Vulnerability Assessment (CVE, OWASP) [ZAP]	Push/Pull Signed Images [OCP]	CM Drift Prevention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

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

GENERAL DISTRIBUTION

redhat.

THE SECURE SOFTWARE FACTORY



GENERAL DISTRIBUTION

redhat.

redhat.

THANK YOU

plus.google.com/+RedHat

facebook.com/redhatinc

linkedin.com/company/red-hat

twitter.com/RedHatNews

youtube.com/user/RedHatVideos