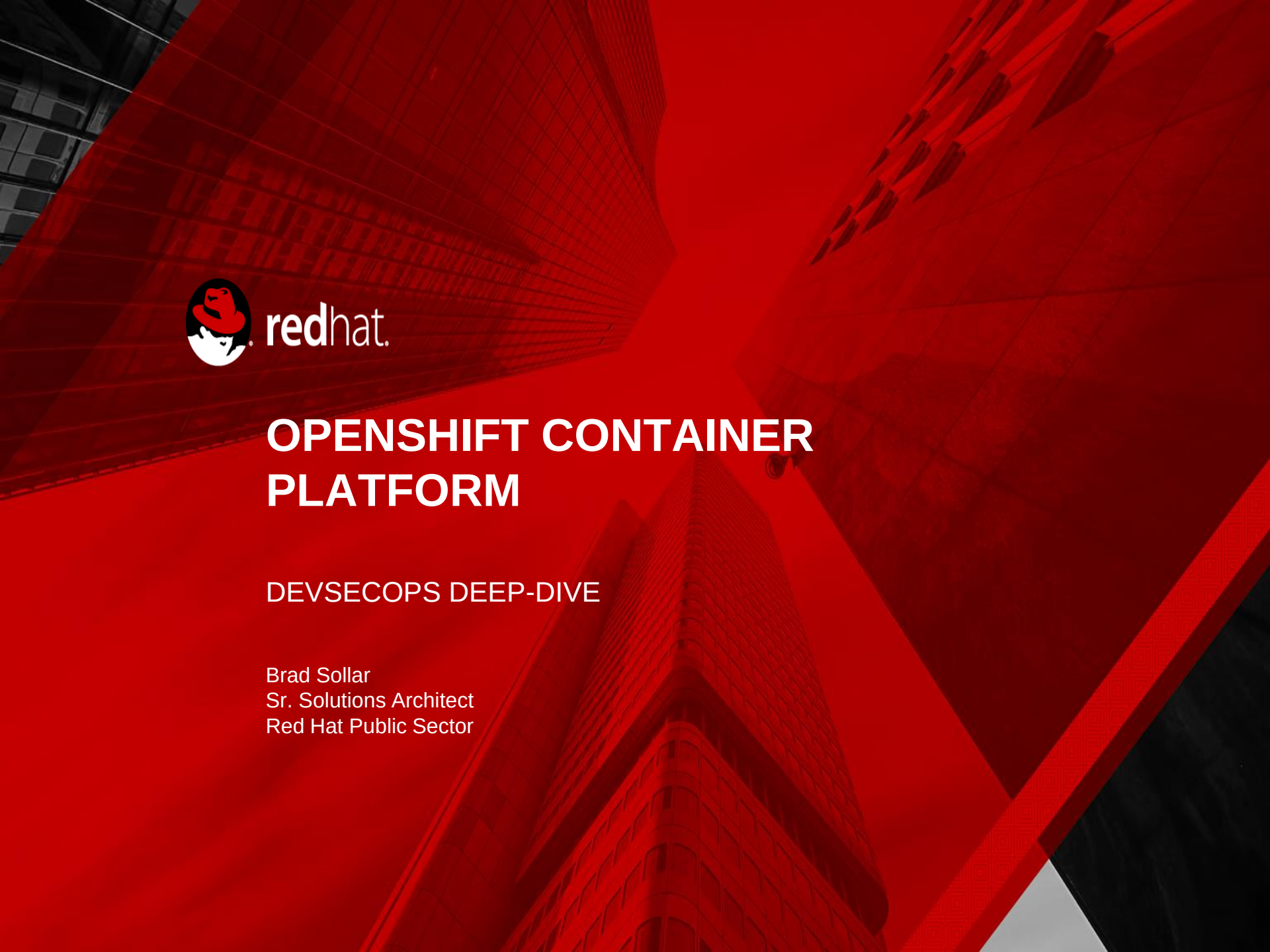
Virginia Information Technologies Agency

Welcome and Opening Remarks

Michael Watson

November 7, 2018



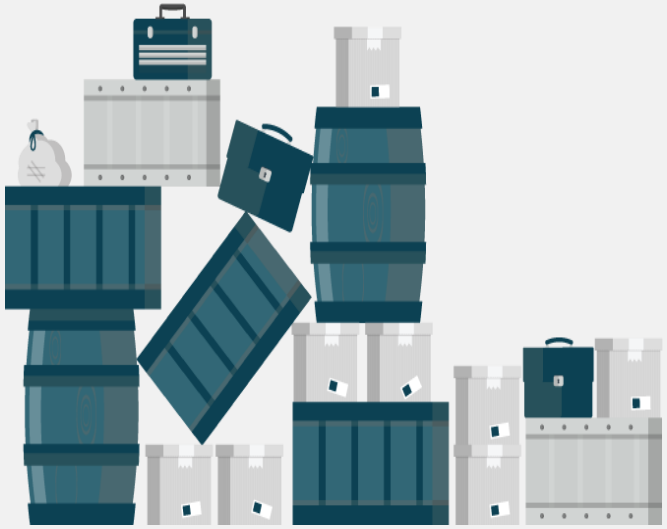
OPENSHIFT CONTAINER PLATFORM

DEVSECOPS DEEP-DIVE

Brad Sollar
Sr. Solutions Architect
Red Hat Public Sector

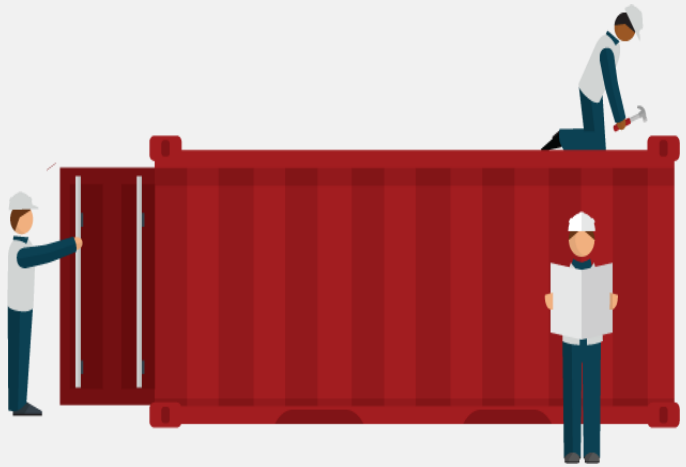
THE PROBLEM

Applications require complicated installation and integration every time they are deployed.

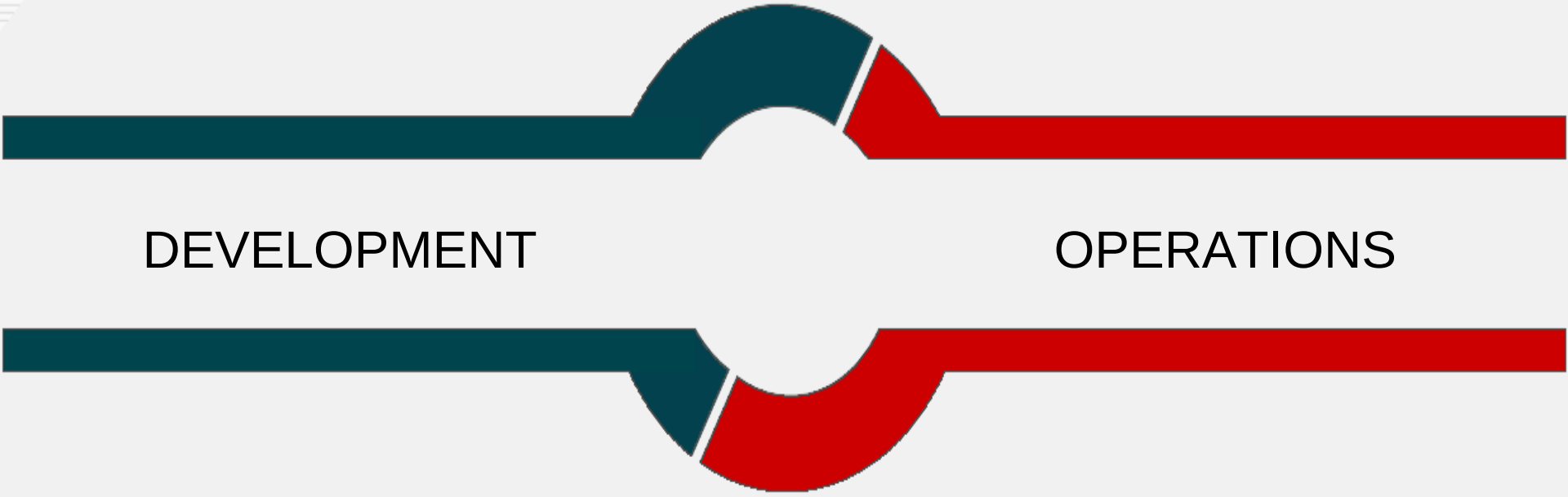


THE SOLUTION

Adopt a container strategy in order to allow applications to be easily shared and deployed.



WHAT ARE CONTAINERS?

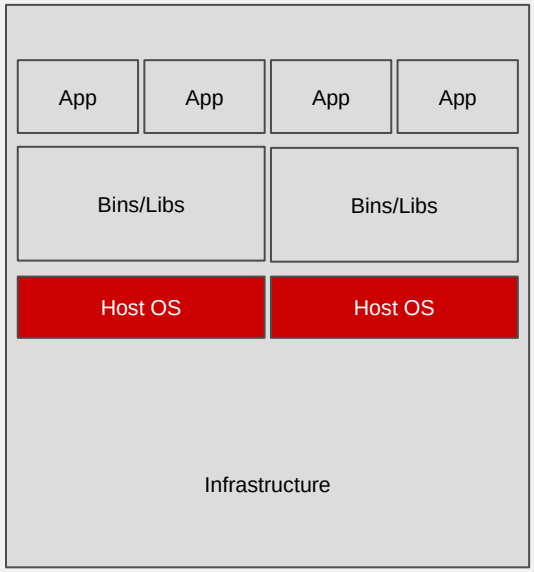


- Packaged app runtime environment
- Enables cross platform deployment
- Decouple and share components

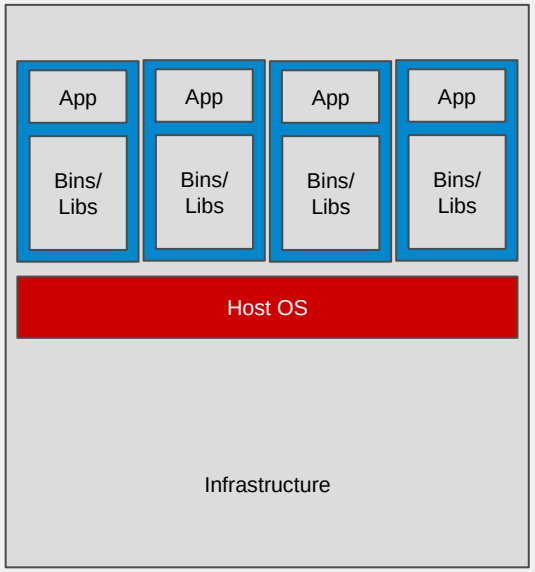
- Sandboxed processes on shared kernel
- Complementary to Virtual Machines
- Simpler, lighter, and denser than VMs

CONTAINERS ARE COMPLEMENTARY TO VMs

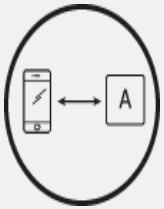
Virtual Machines



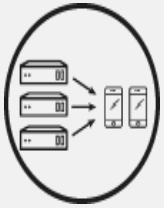
Containers



CONTAINERS EFFECT



Monolith



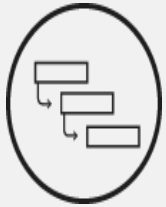
N-Tier

Microservices

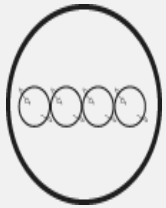
Datacenter

Hosted

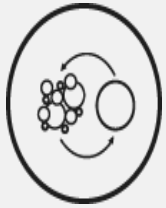
Hybrid Cloud



Waterfall

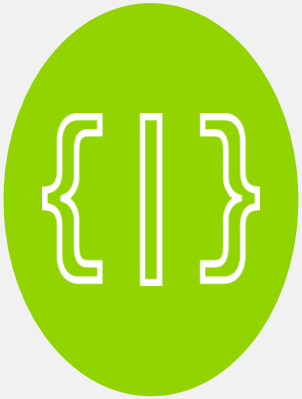


Agile



DevOps

BUILD AND DEPLOY CONTAINER IMAGES

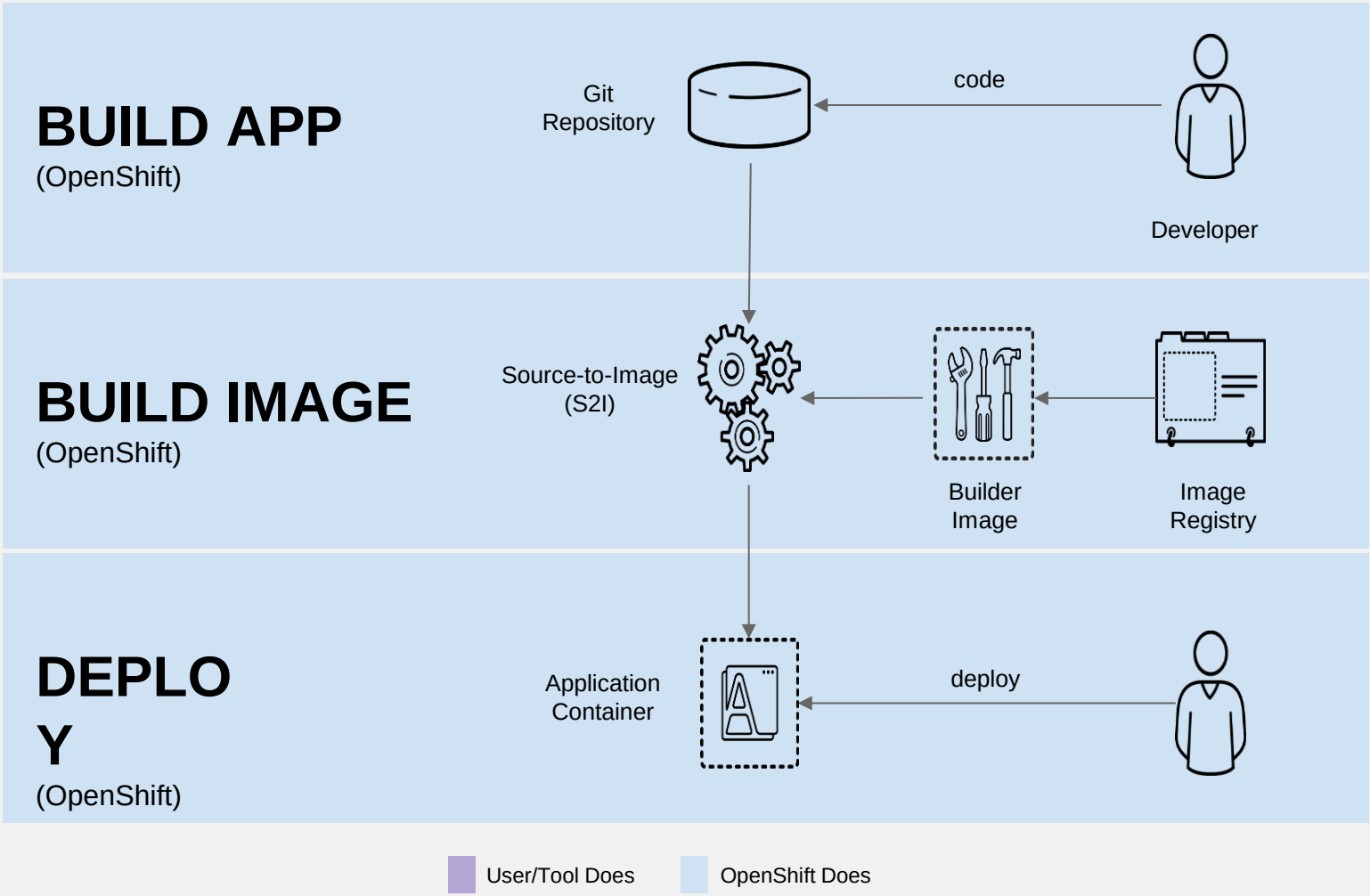


DEPLOY YOUR SOURCE CODE

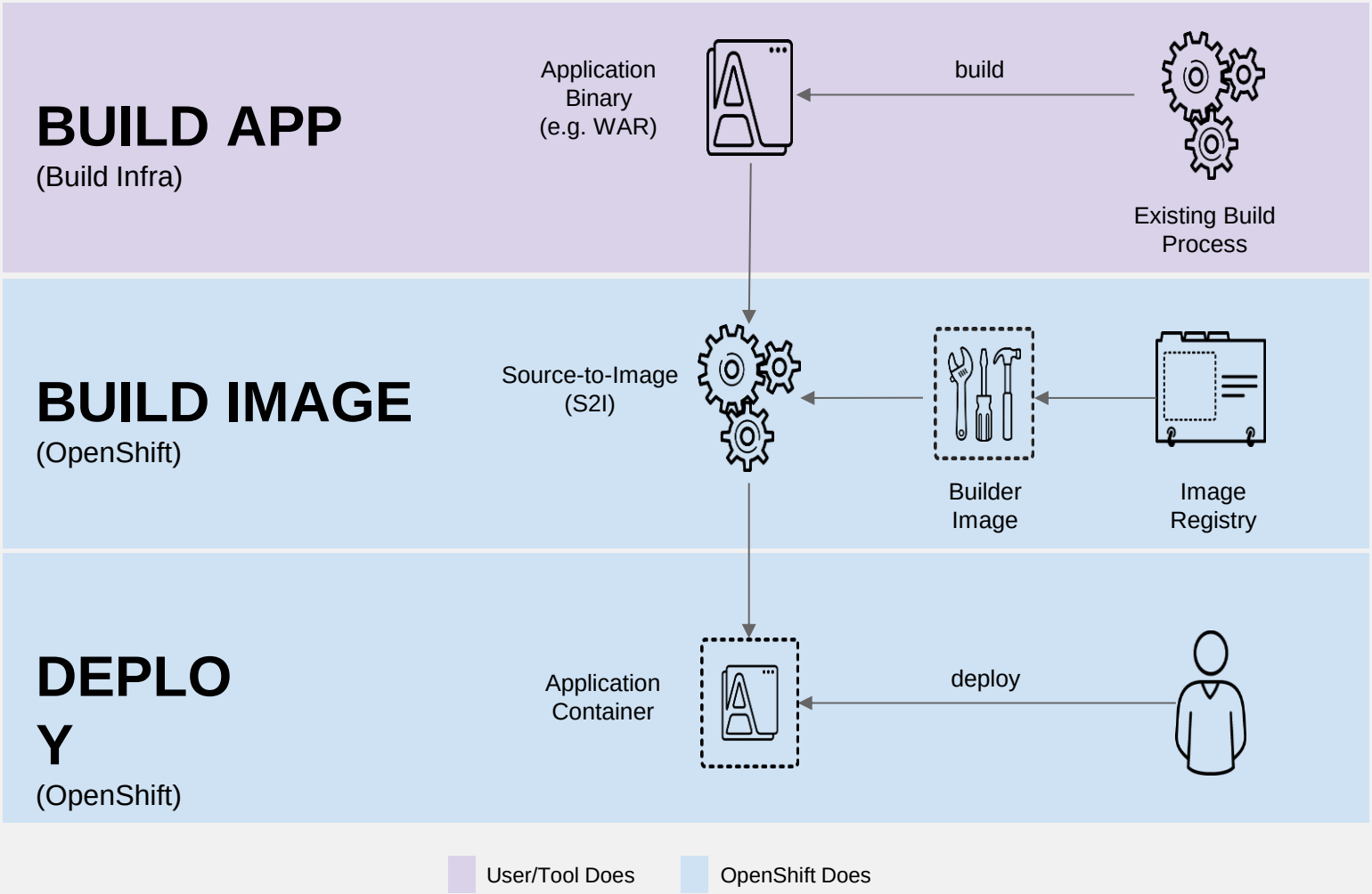
DEPLOY YOUR APP BINARY

DEPLOY YOUR CONTAINER IMAGE

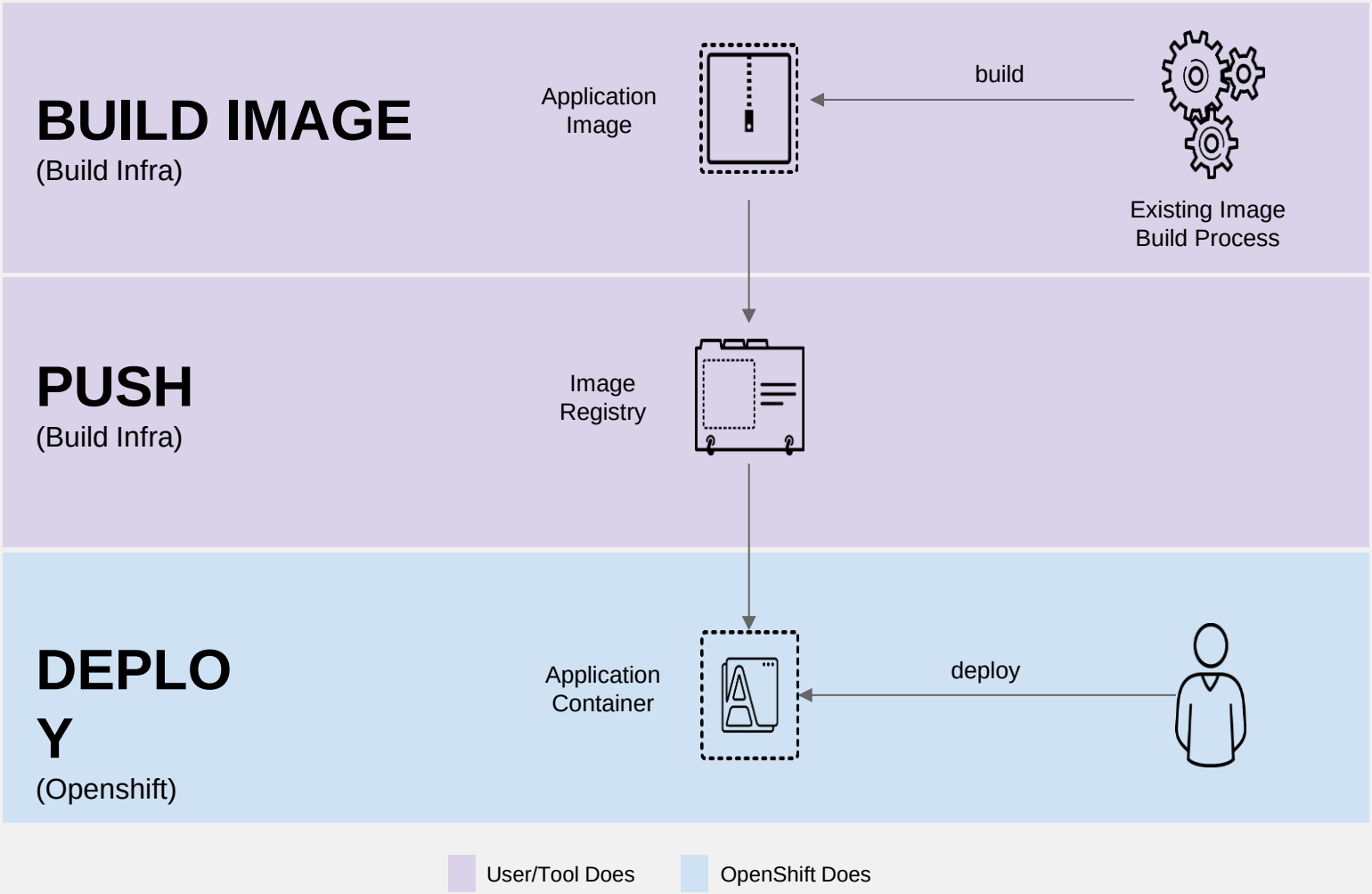
SOURCE CODE DEPLOYMENT



APP BINARY DEPLOYMENT

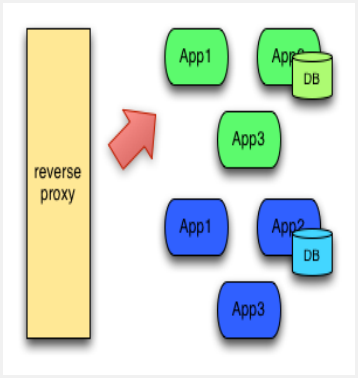


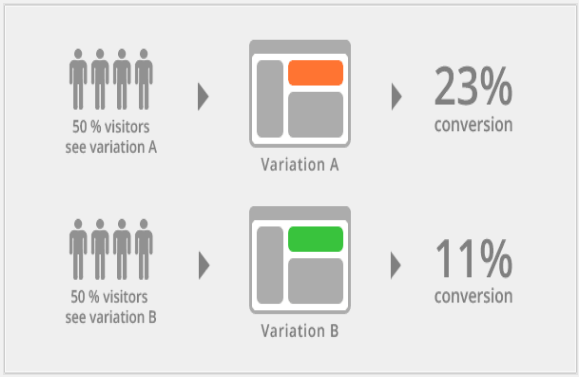
CONTAINER IMAGE DEPLOYMENT



OPENSHIFT DEPLOYMENT STRATEGIES

Painless deployments with zero/reduced downtime through automation





ROLLING DEPLOYMENTS

A rolling deployment slowly replaces instances of the previous version of an application with instances of the new version of the application.

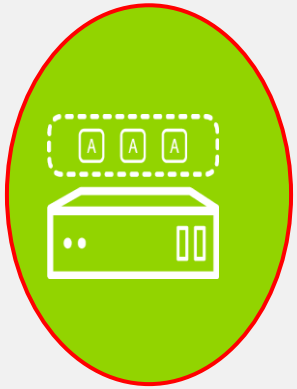
BLUE/GREEN DEPLOYMENTS

A blue/green deployment is a software deployment strategy that relies on two identical production configurations that alternate between active and inactive.

A/B DEPLOYMENTS

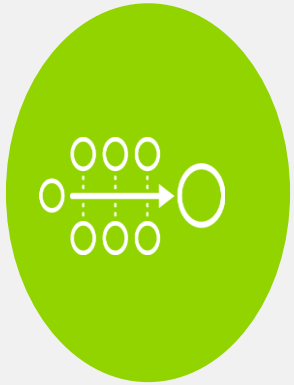
A/B testing (sometimes called split testing) is comparing two versions of a web page to see which one performs better.

OPENSHIFT LOVES CI/CD



JENKINS-AS-A SERVICE ON OPENSHIFT

HYBRID JENKINS INFRA WITH OPENSHIFT

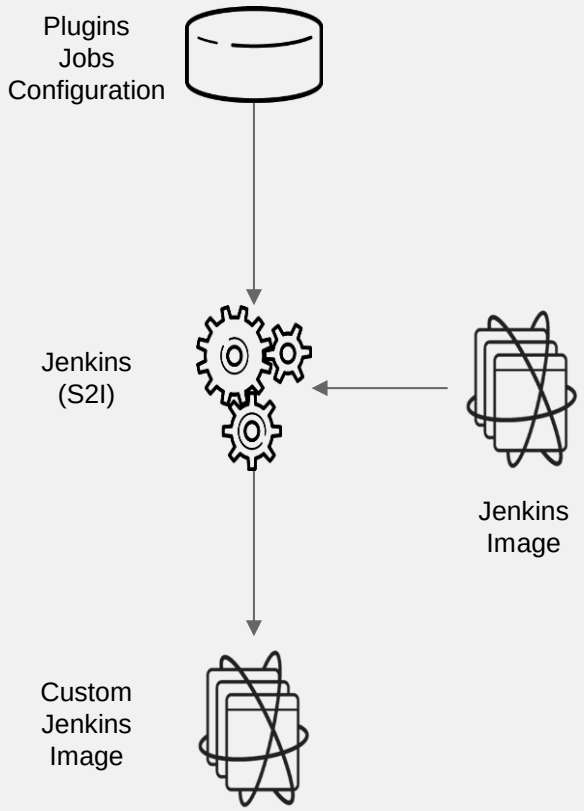


EXISTING CI/CD DEPLOY TO OPENSHIFT

JENKINS-AS-A-SERVICE ON OPENSHIFT

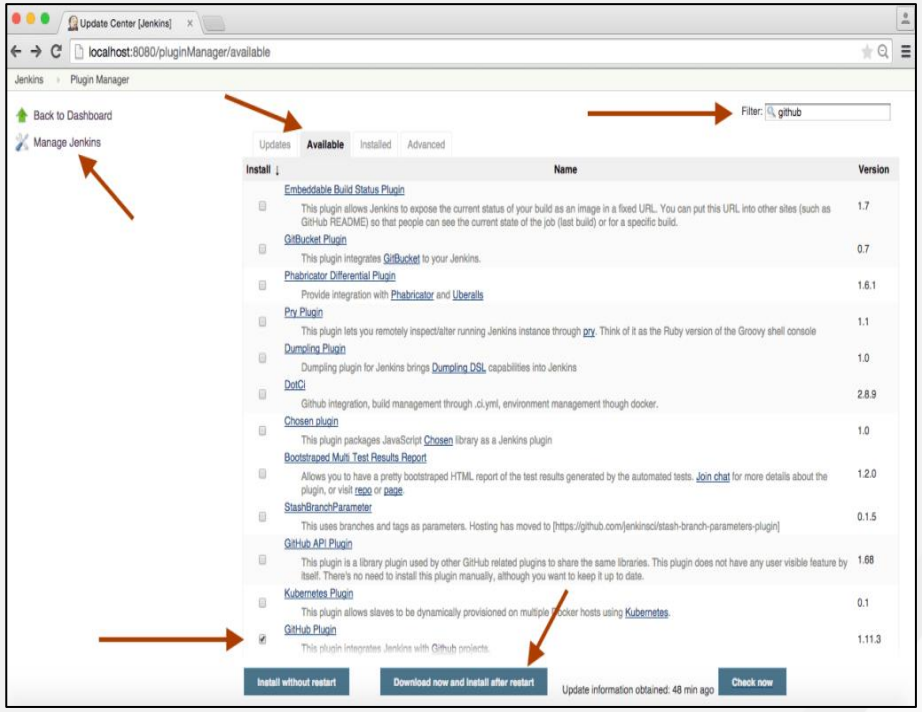
- Certified Jenkins images with pre-configured plugins
  - Provided out-of-the-box
  - Follows Jenkins 1.x and 2.x LTS versions

- Jenkins S2I Builder for customizing the image
  - Install plugins, configure Jenkins, configure build jobs

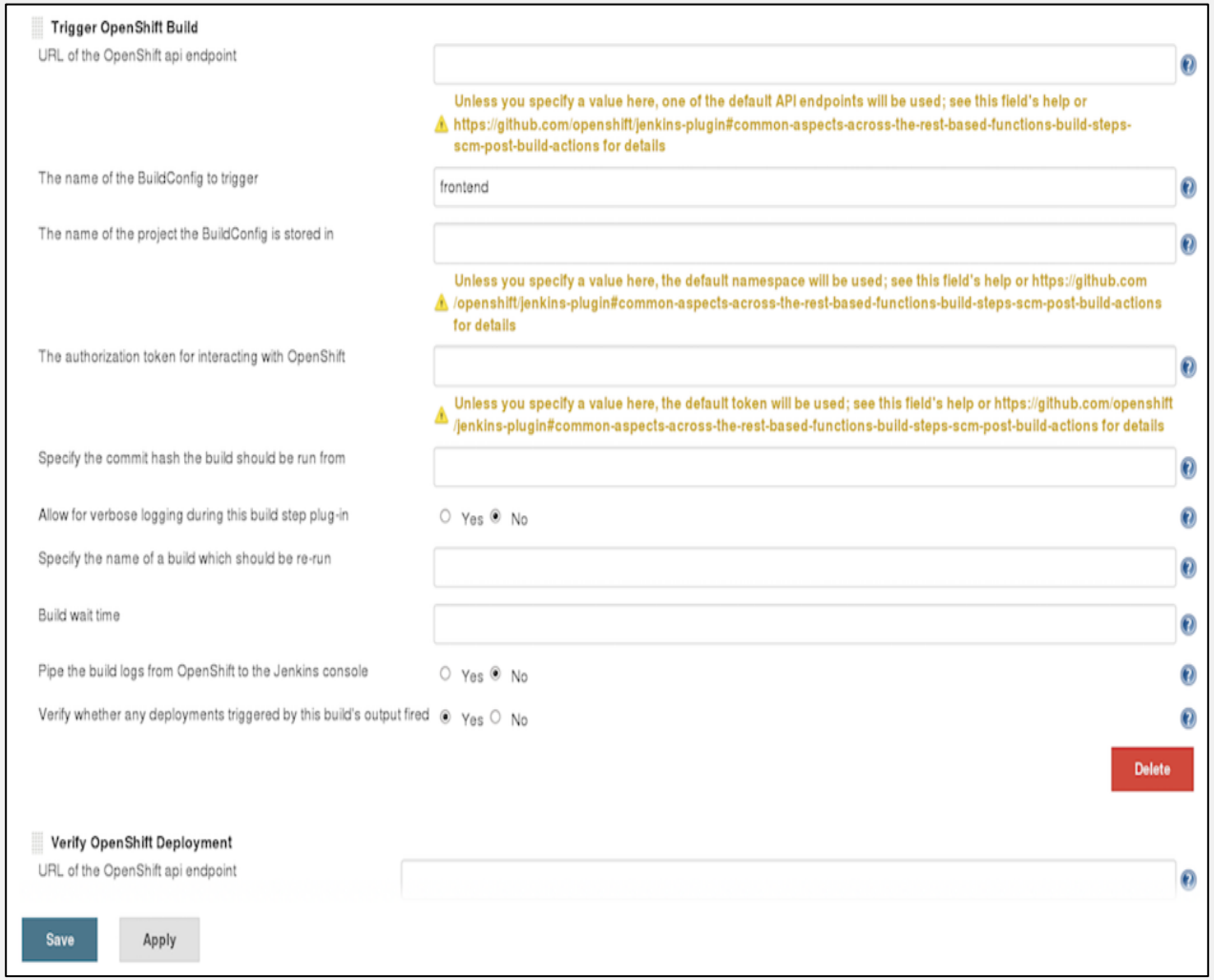


JENKINS PLUGIN

- The most fundamental part of a Pipeline
- Tell Jenkins *what* to do, and serve as the basic building block for both Declarative and Scripted Pipeline syntax

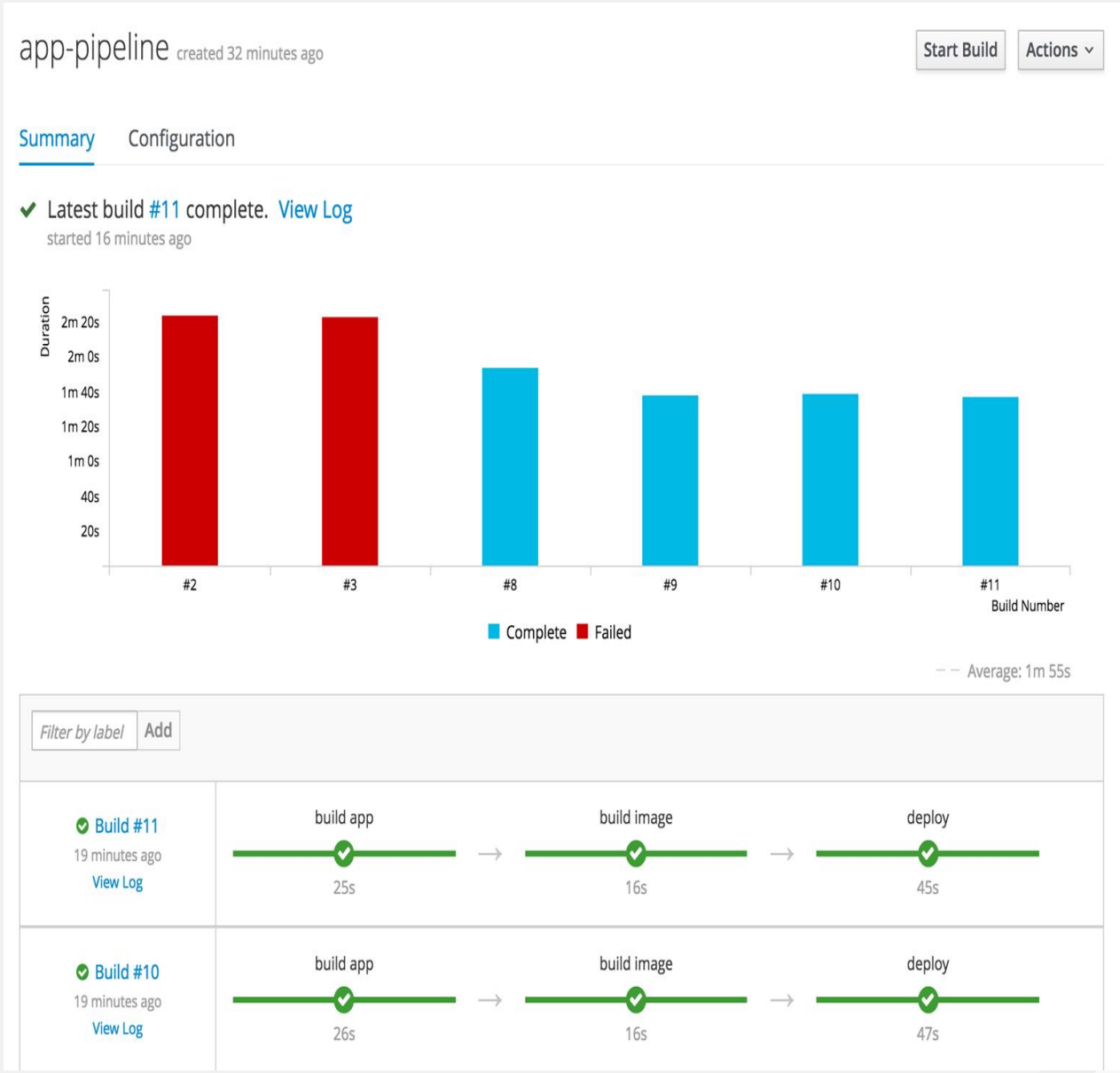


OPENSHIFT JENKINS PLUGIN

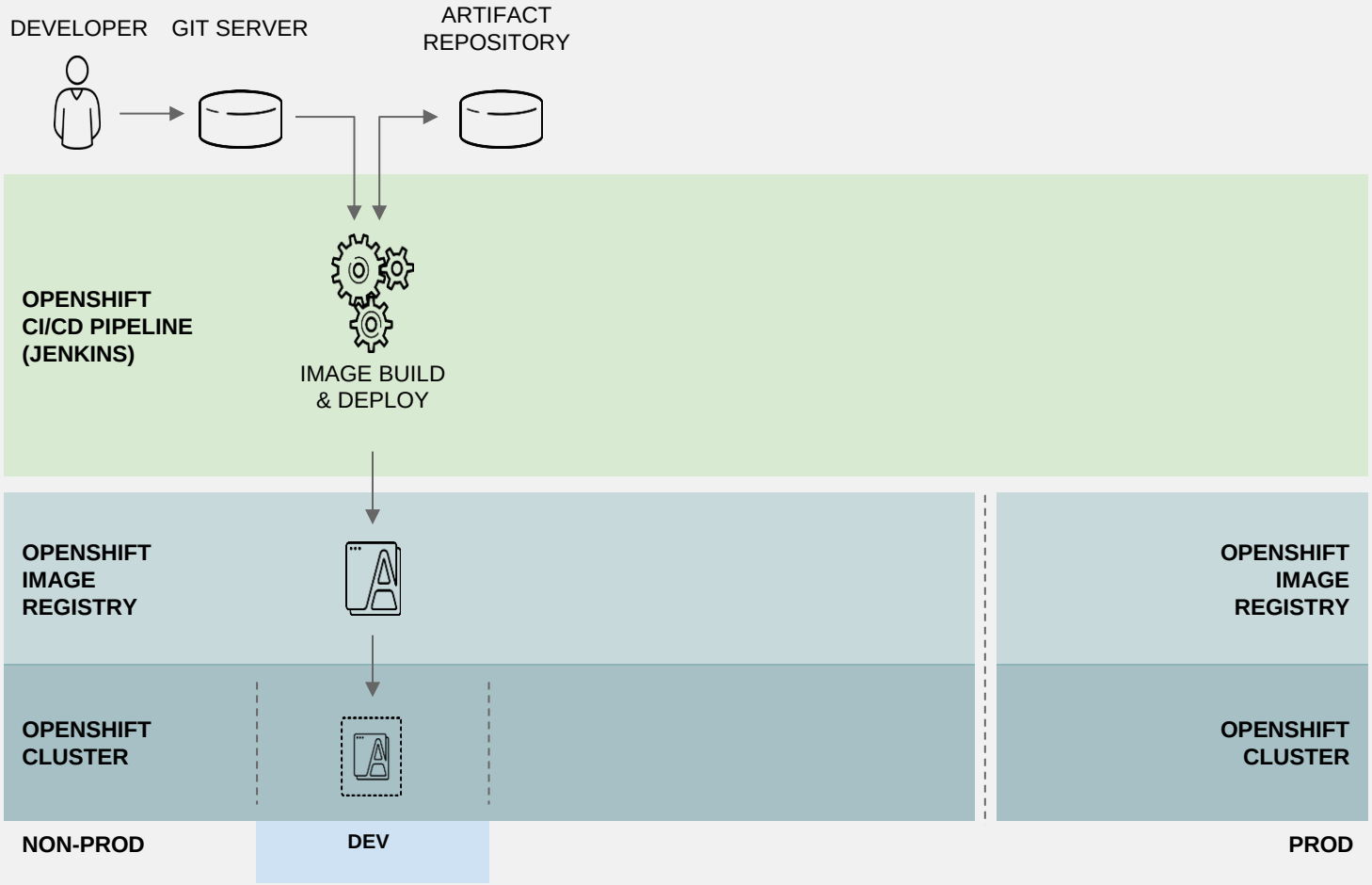


```
kind: BuildConfig
apiVersion: v1
metadata:
  name: sample-pipeline
  labels:
    Name: sample-pipeline
spec:
  triggers:
  - type: GitHub
    github:
      secret: secret101
  - type: Generic
    generic:
      secret: secret101
strategy:
  type: JenkinsPipeline
  jenkinsPipelineStrategy:
    jenkinsfile: |-
      node('maven') {
      stage 'build'
            openshiftBuild(buildConfig: 'ruby-sample-build', showBuildLogs:'true')
            stage 'deploy'
            openshiftDeploy(deploymentConfig: 'frontend')
      }
```

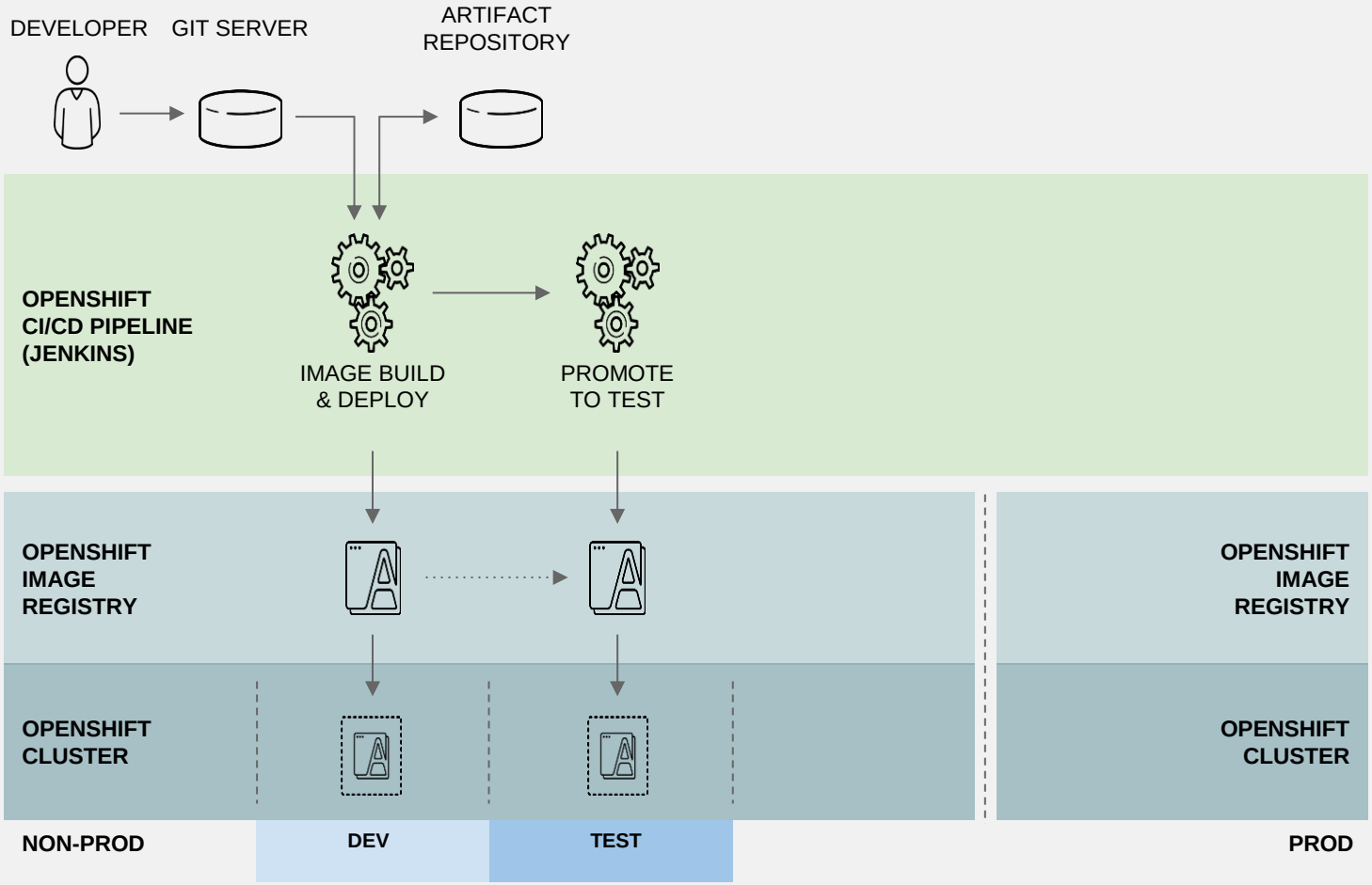
OPENSHIFT PIPELINES IN WEB CONSOLE



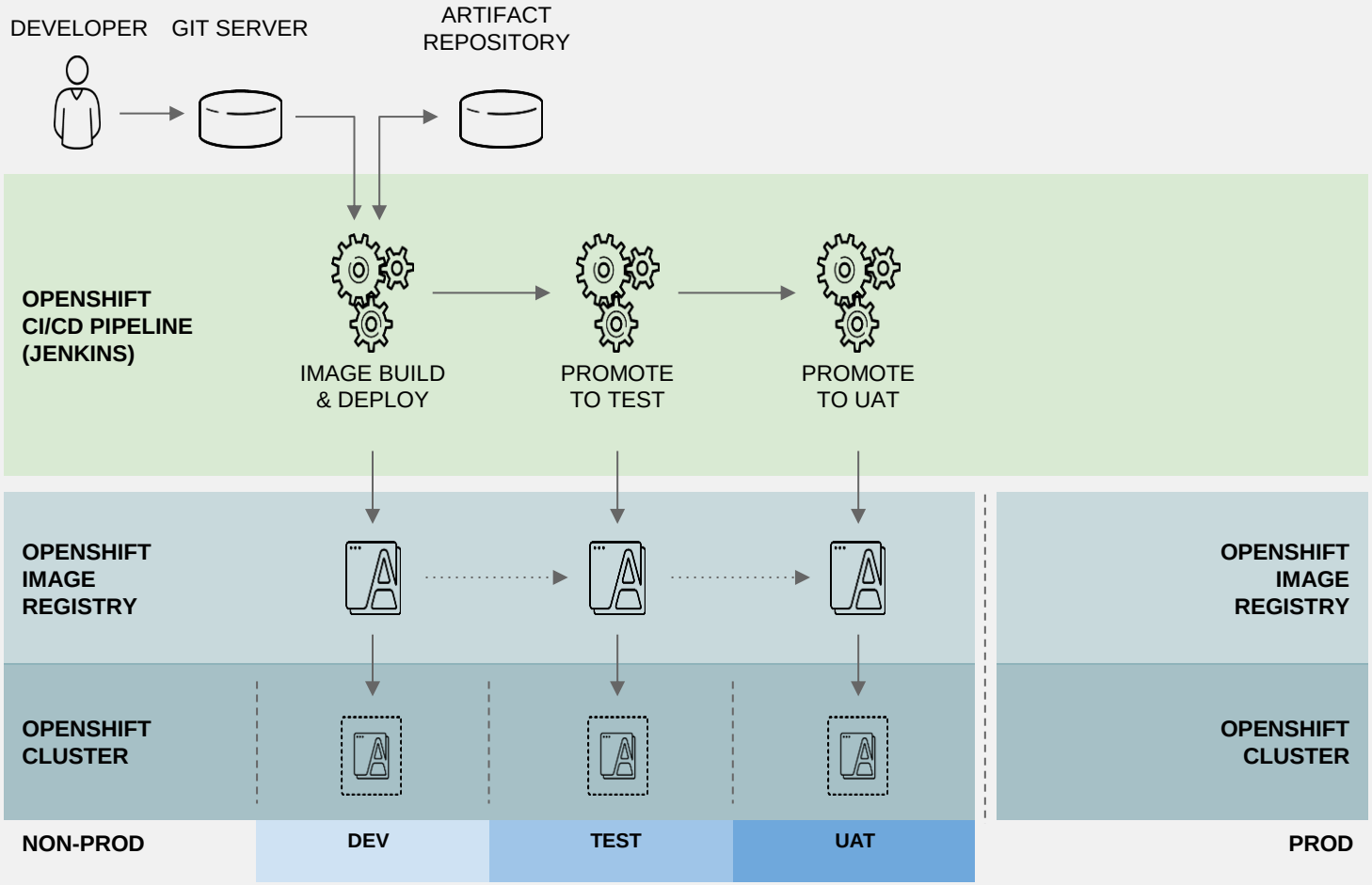
CONTINUOUS DELIVERY PIPELINE



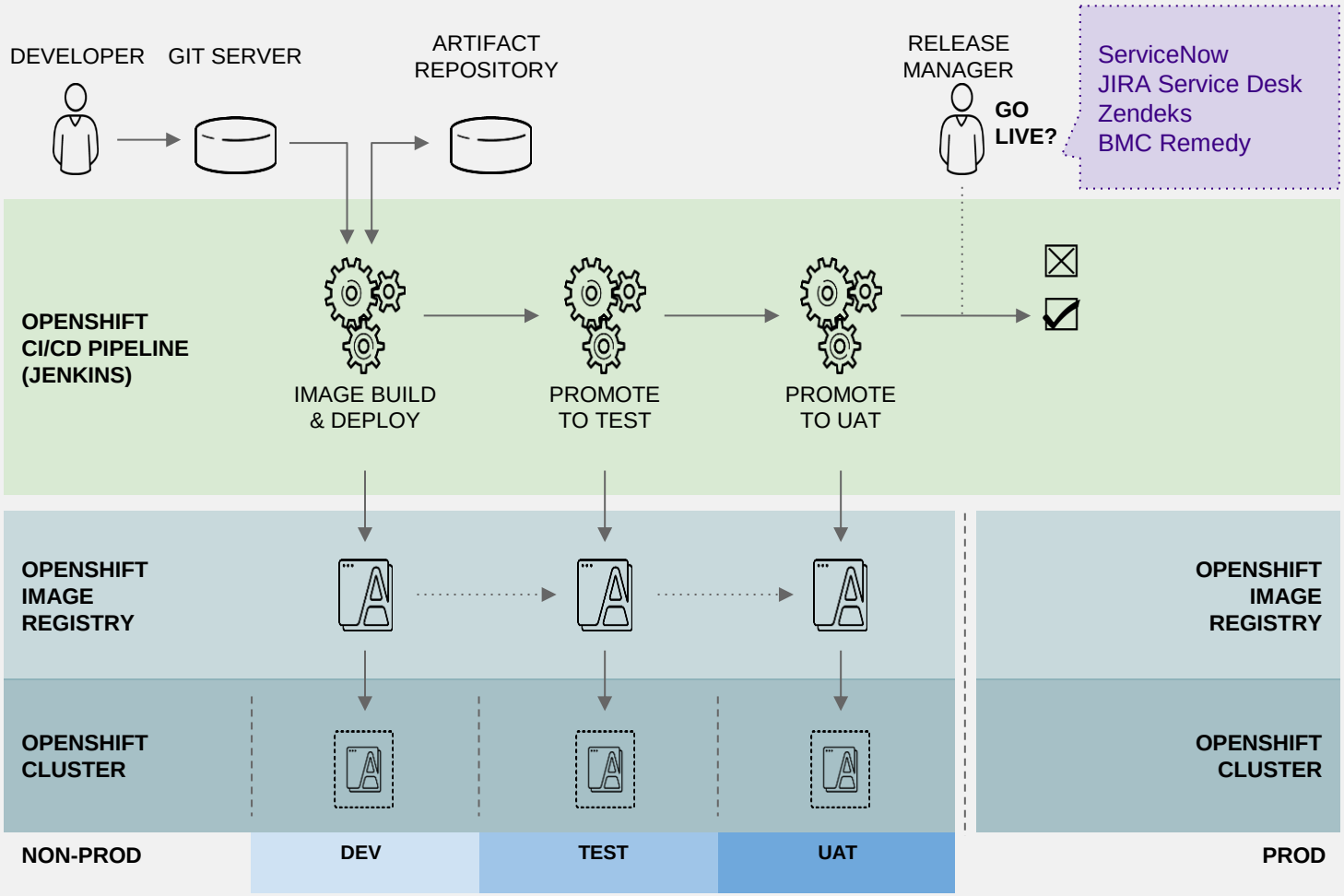
CONTINUOUS DELIVERY PIPELINE



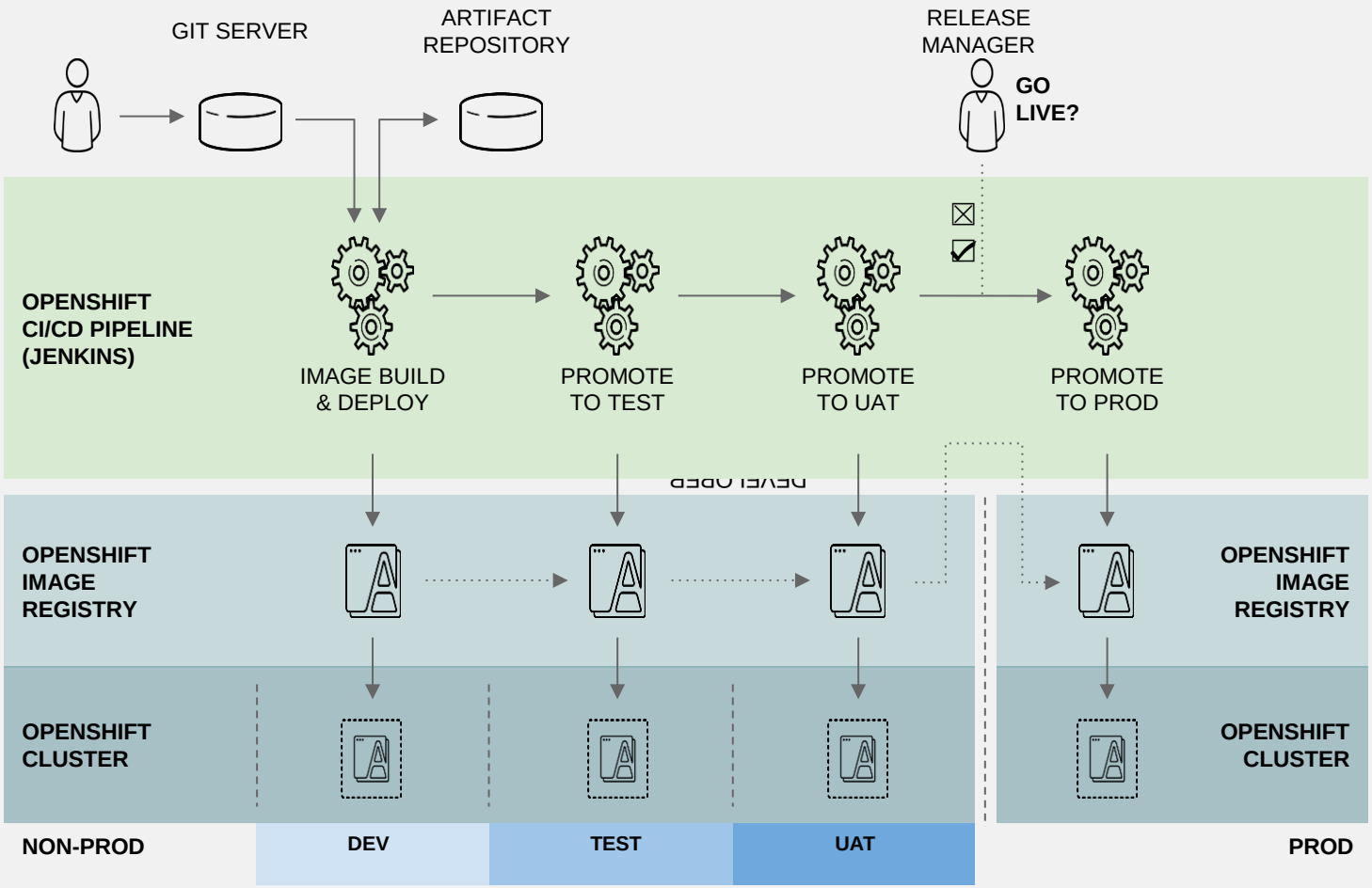
CONTINUOUS DELIVERY PIPELINE



CONTINUOUS DELIVERY PIPELINE

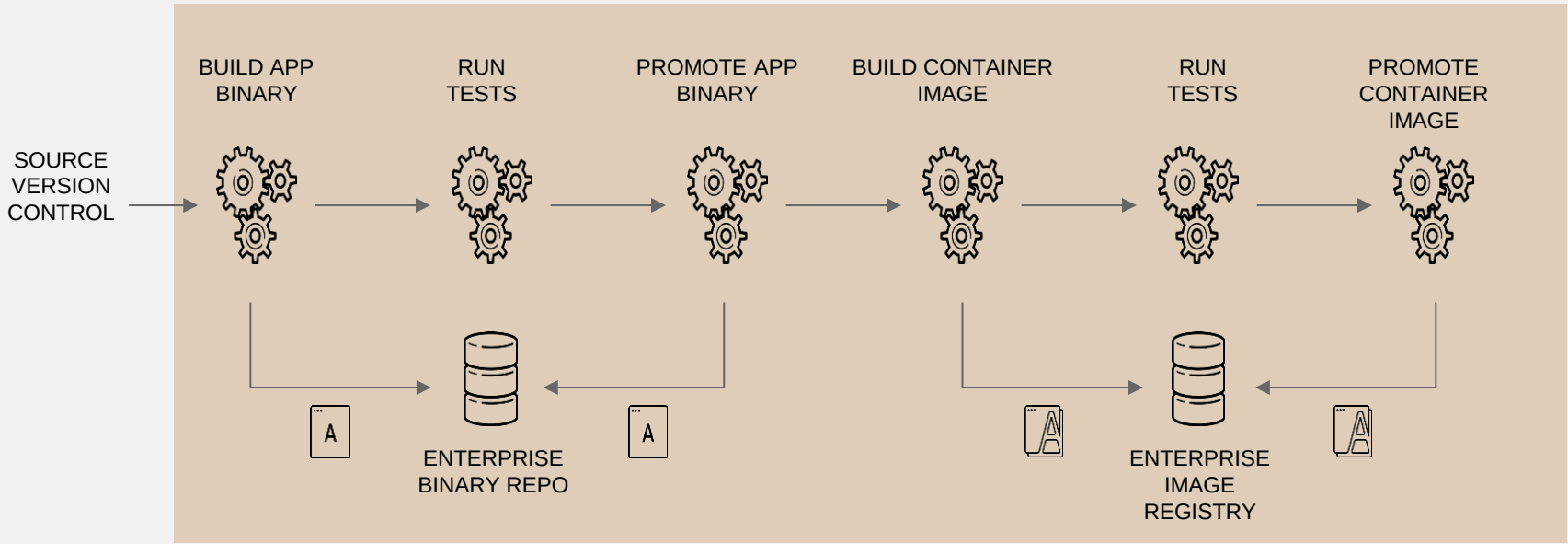


CONTINUOUS DELIVERY PIPELINE

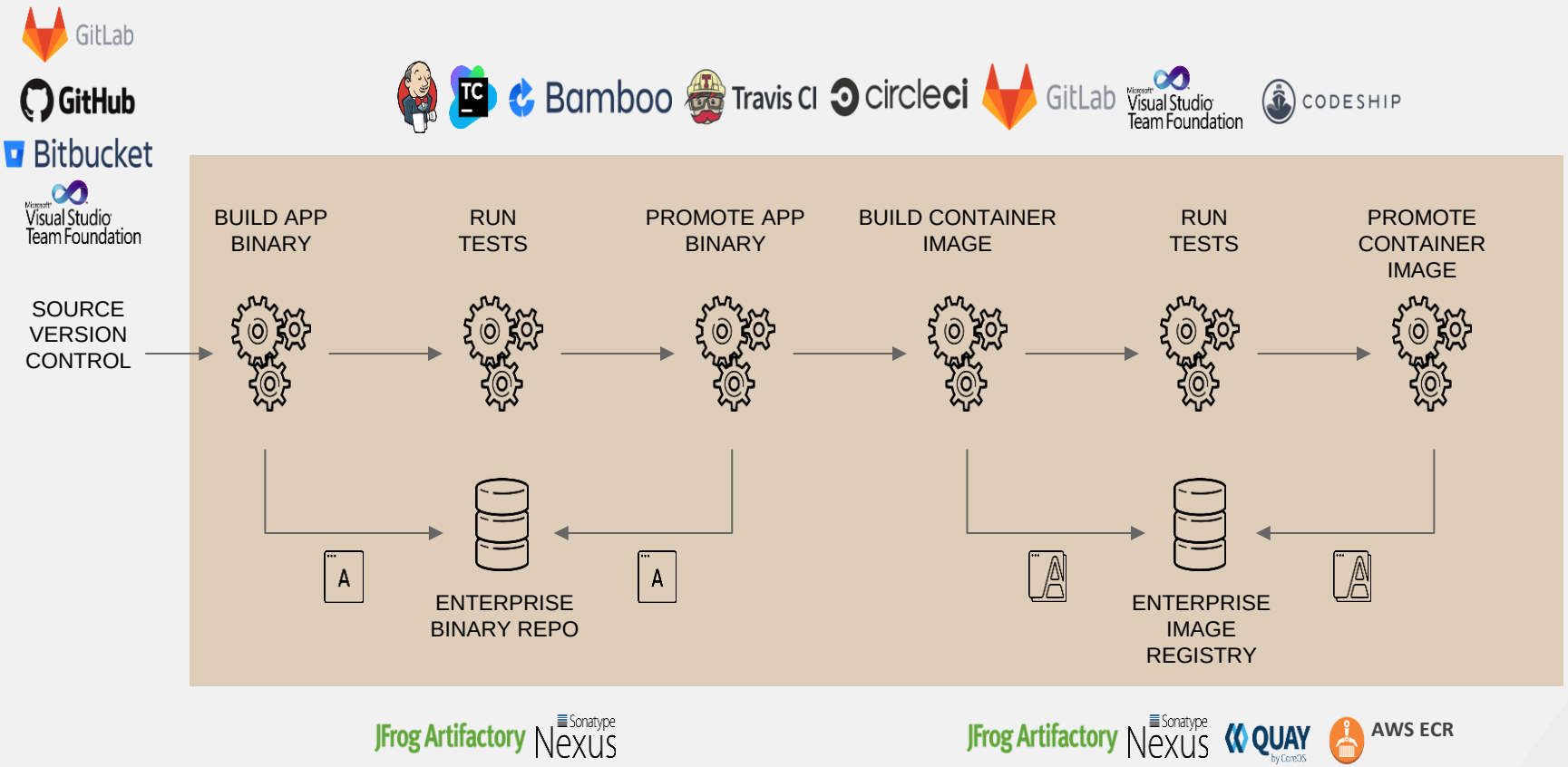


BUT…
SOME TEAMS ALREADY HAVE AUTOMATED DELIVERY PIPELINES

WHAT IF THERE ARE EXISTING DELIVERY PROCESSES?

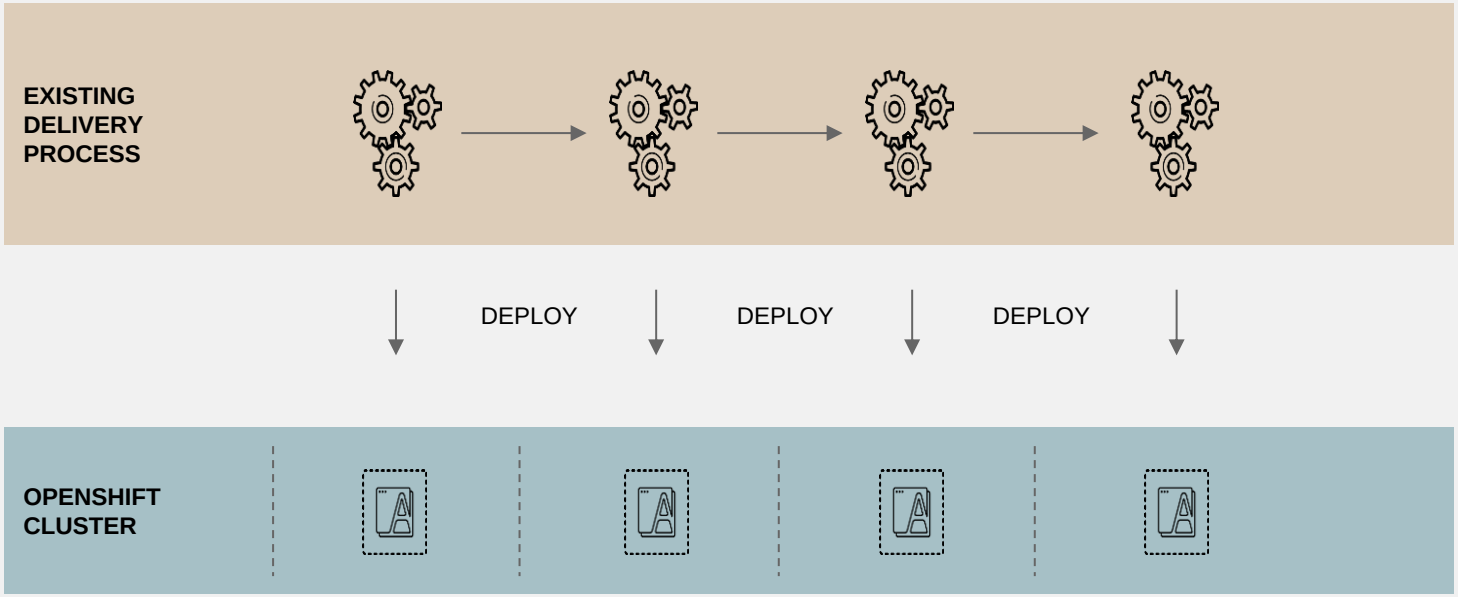


WHAT IF THERE ARE EXISTING DELIVERY PROCESSES?

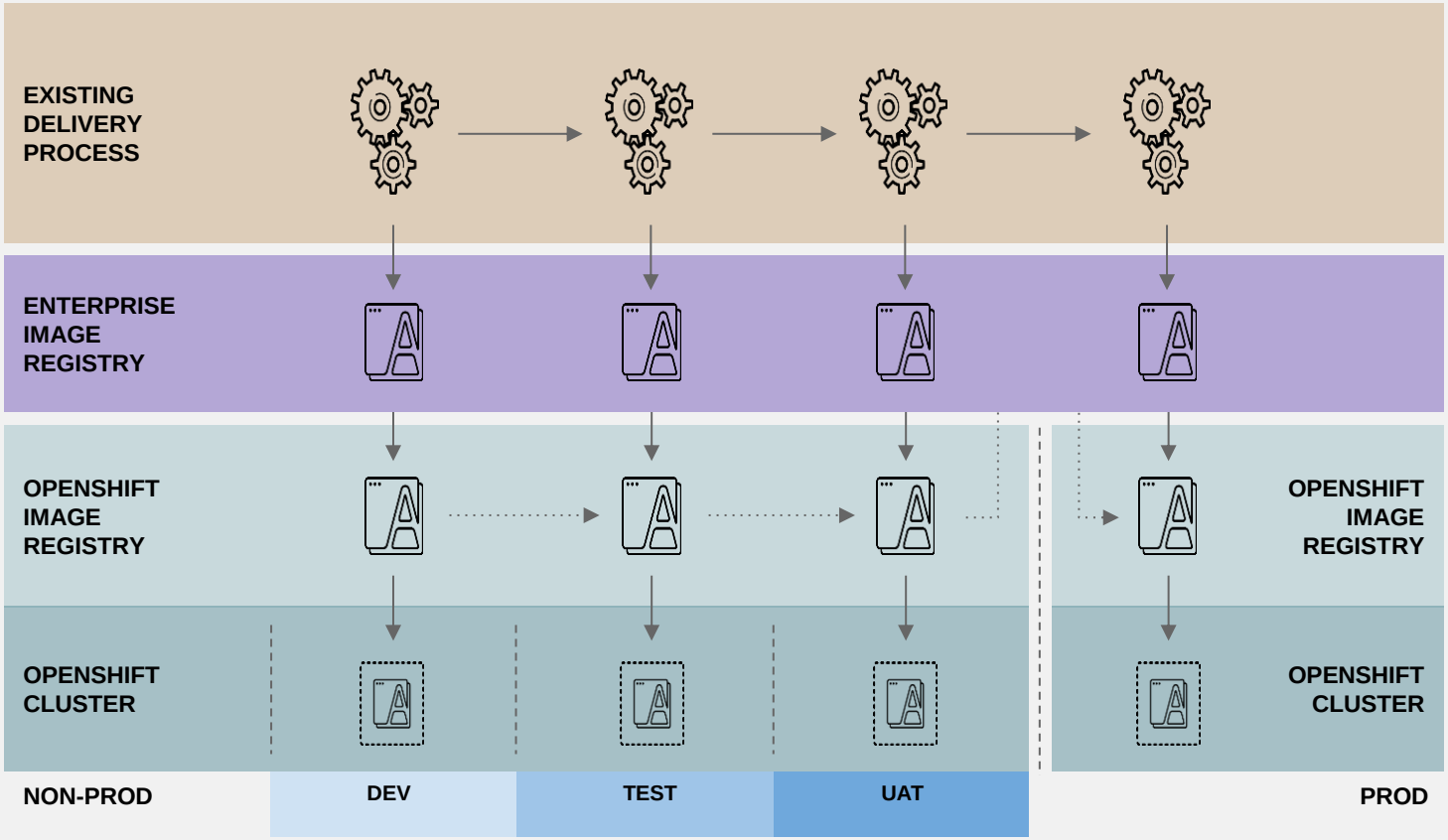


redhat.

ENRICHING EXISTING DELIVERY PROCESSES WITH OPENSHIFT



ENRICHING EXISTING DELIVERY PROCESSES WITH OPENSHIFT



THANK YOU


plus.google.com/+RedHat


facebook.com/redhatinc


linkedin.com/company/red-hat


twitter.com/RedHatNews


youtube.com/user/RedHatVideos

HOW DO YOU USE THIS CONCEPT?

- Have your team rank themselves in the order of their strengths.
- Use the criteria as an ongoing framework for performance discussions.
- All of these virtues can be developed.

Virginia Information Technologies Agency

MSI Security Update

Grayson Walters
Information Security Manager / ISO
SAIC MSI

November 7th 2018

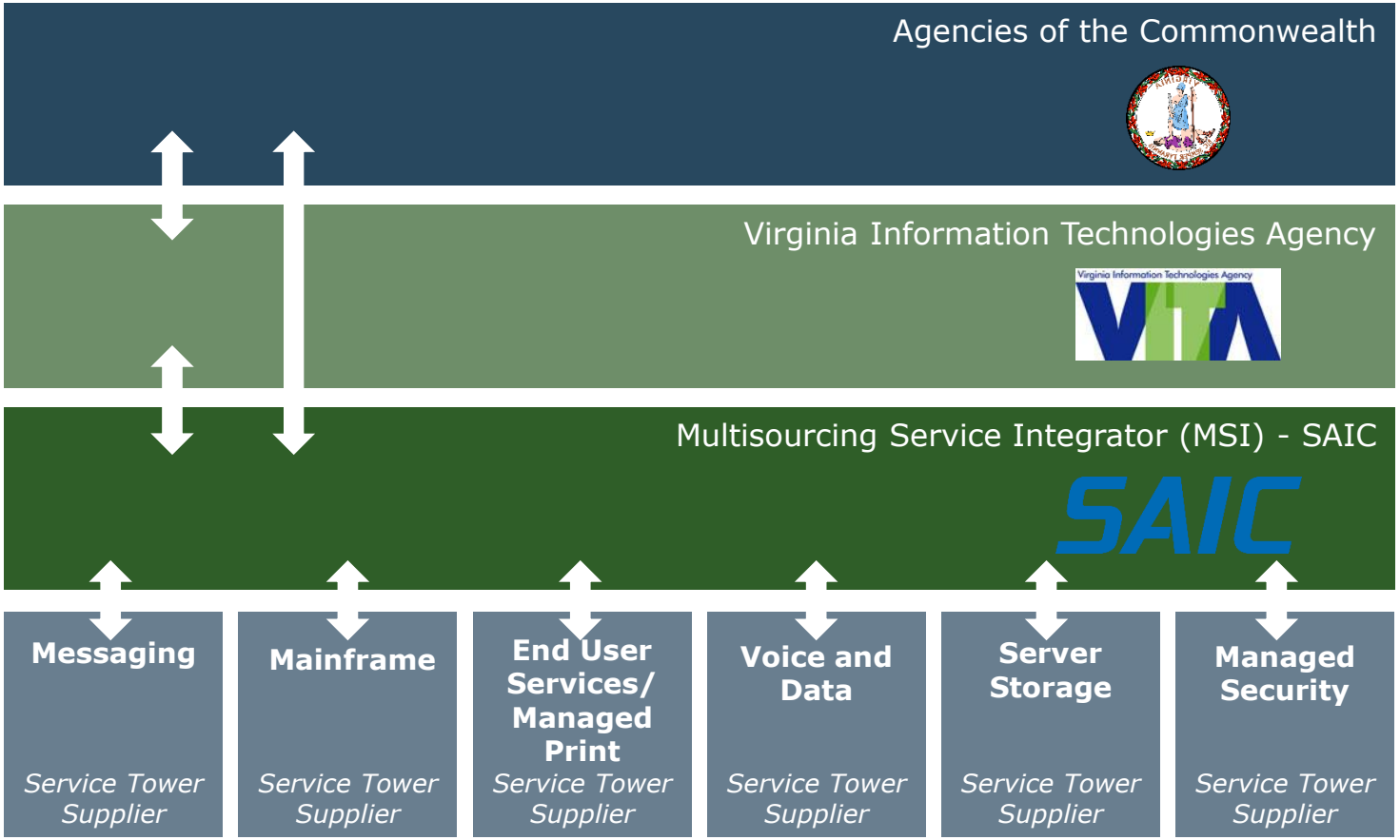
Introductions

Grayson Walters | CISSP®
Information Security Manager & ISO | Federal Civilian Agencies
tel: 804/273-8522

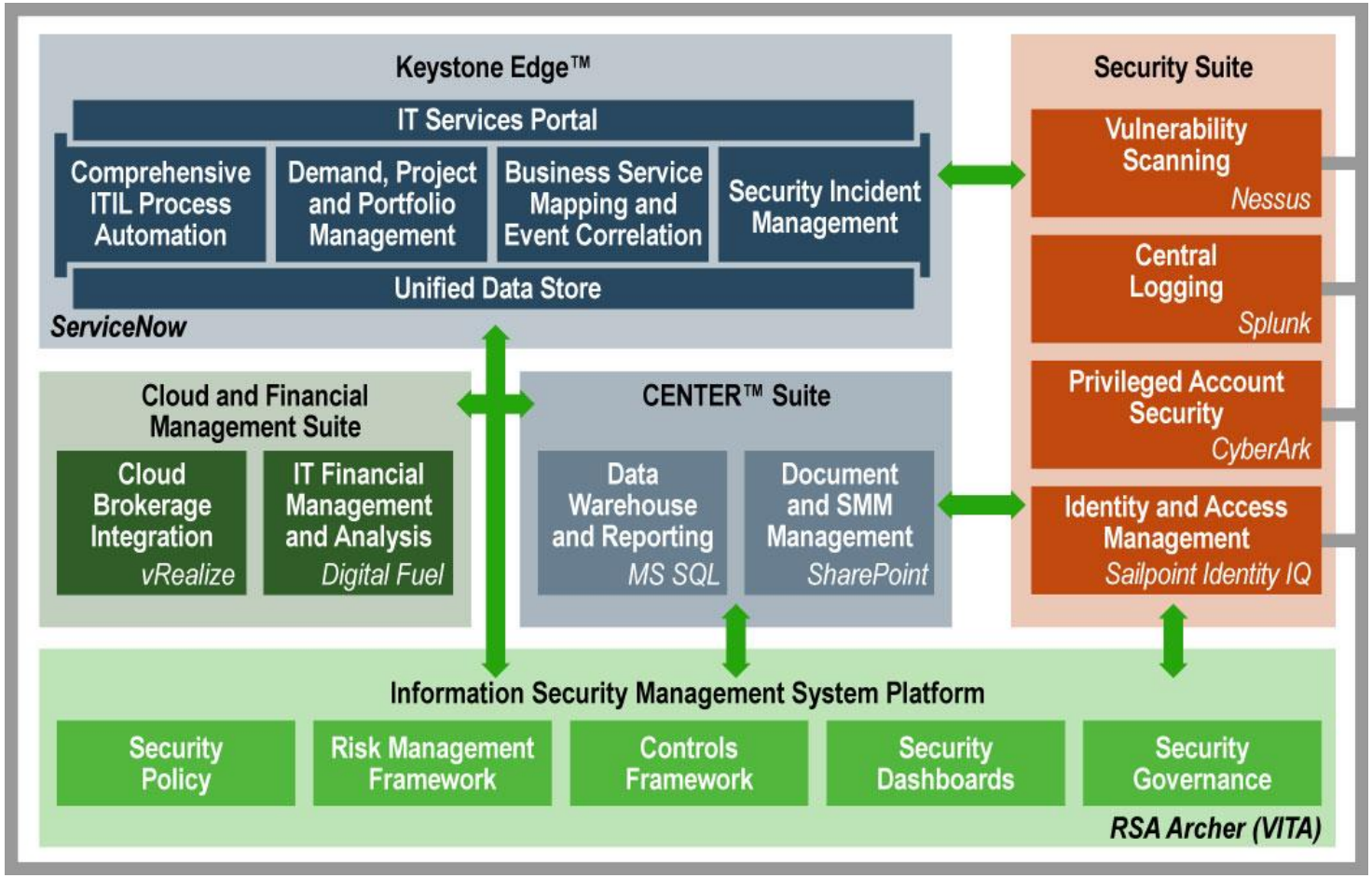
Agenda

- Introductions
- MSI Overview
- MSI Security Operations Overview
- Additional MSI Security Benefits
- MSI Security Calendar

MSI Overview – Model



MSI Overview – Technology



MSI Security Operations Overview

Security Incident Management

- **Change:** View more information about your security incidents including status updates, who is working, and next steps
- **Tool:** RSA Archer and Keystone Edge
- **Coming:** Dec. 15, 2018

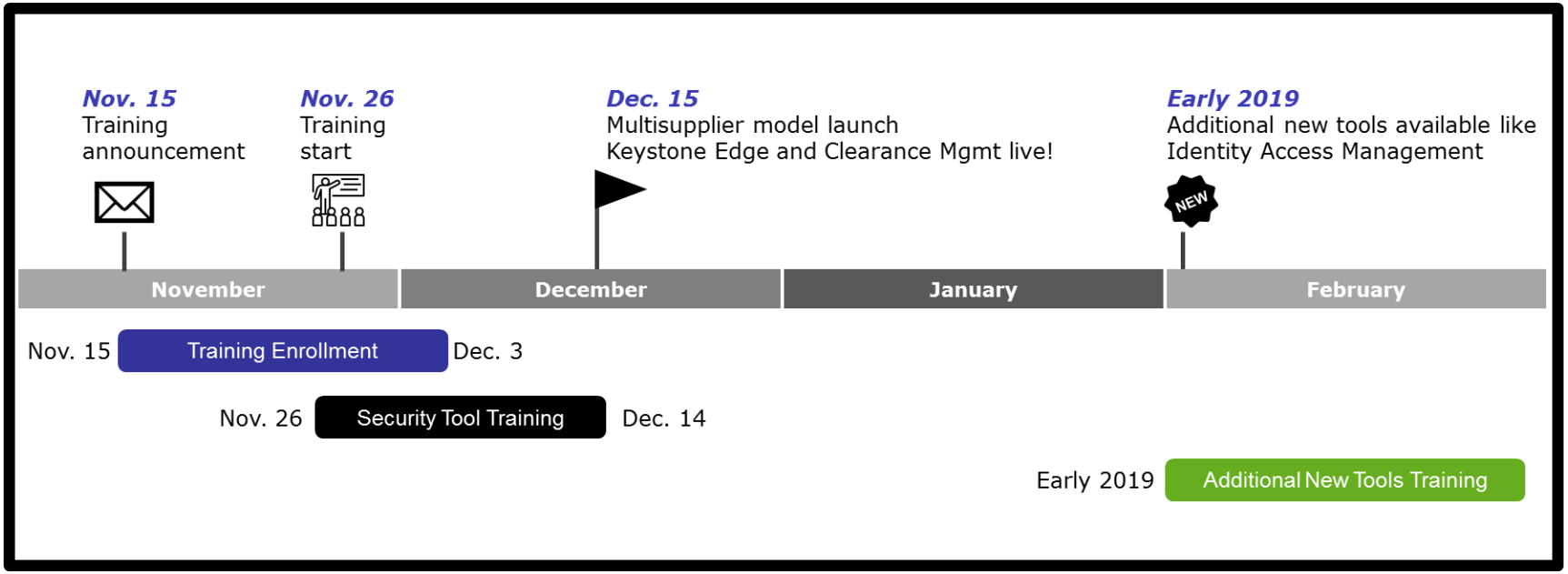
Identity & Access Management

- **Change:** New tool to manage system access
- **Tool:** Sailpoint Identity IQ
- **Coming:** Early 2019

Security Clearance

- **Change:** View STS Supplier personnel clearances
- **Tool:** Keystone Edge – Security Clearance Tracking Database
- **Coming:** Dec. 15, 2018

MSI Security Calendar



Thank you!

For further information please contact:

Grayson Walters | CISSP®

Information Security Manager & ISO | Federal Civilian Agencies

tel: 804/273-8522

SAIC
Redefining Ingenuity™

How to Spot Ideal Team Players

Stephanie Williams-Hayes
VDH Information Security Officer
ISO Information Sharing
November 7, 2018


T E A M
TOGETHER EVERYONE ACHIEVES MORE

How do you use teams to accomplish your work in the world of Information Security?

5 STAGES OF TEAM DEVELOPMENT

Source: Bruce Tuckman –Forming-Norming-Storming-Performing-Adjourning Model

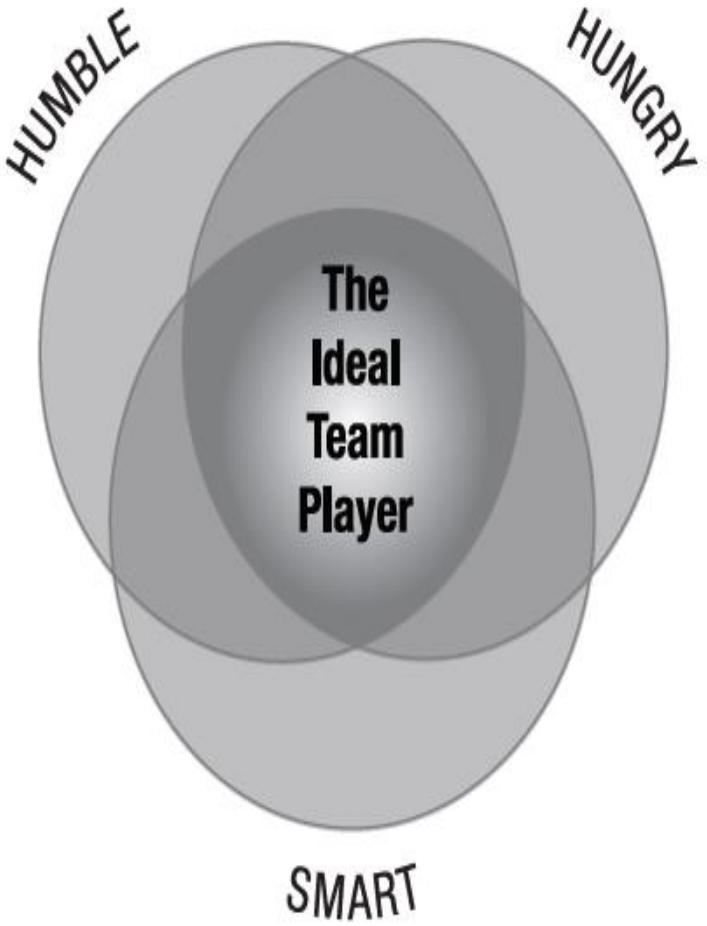

Teamwork can make a Dreamwork

Selecting the right staff for the right job.

First Who...Then What

Source: Jim Collins – Good to Great

IDEAL TEAM PLAYER MODEL



Source: Patrick Lenionci –Ideal Team Player

HUMBLE

MOST IMPORTANT VIRTUE

- Interested in others
- Focused on the greater good
- Recognition of that which is true (aka, not thinking highly of oneself)
- Not arrogant

Source: Patrick Lenionci –Ideal Team Player

HUNGER

- Work ethic
- Goes above and beyond
- Never a slacker
- Passionate
- Will do whatever it takes

Source: Patrick Lenionci –Ideal Team Player

SMART

- Emotionally Smart
- Common sense around people
- Practices emotiona intelligence in behaviors

Source: Patrick Lenionci –Ideal Team Player

IDEAL Team Players....

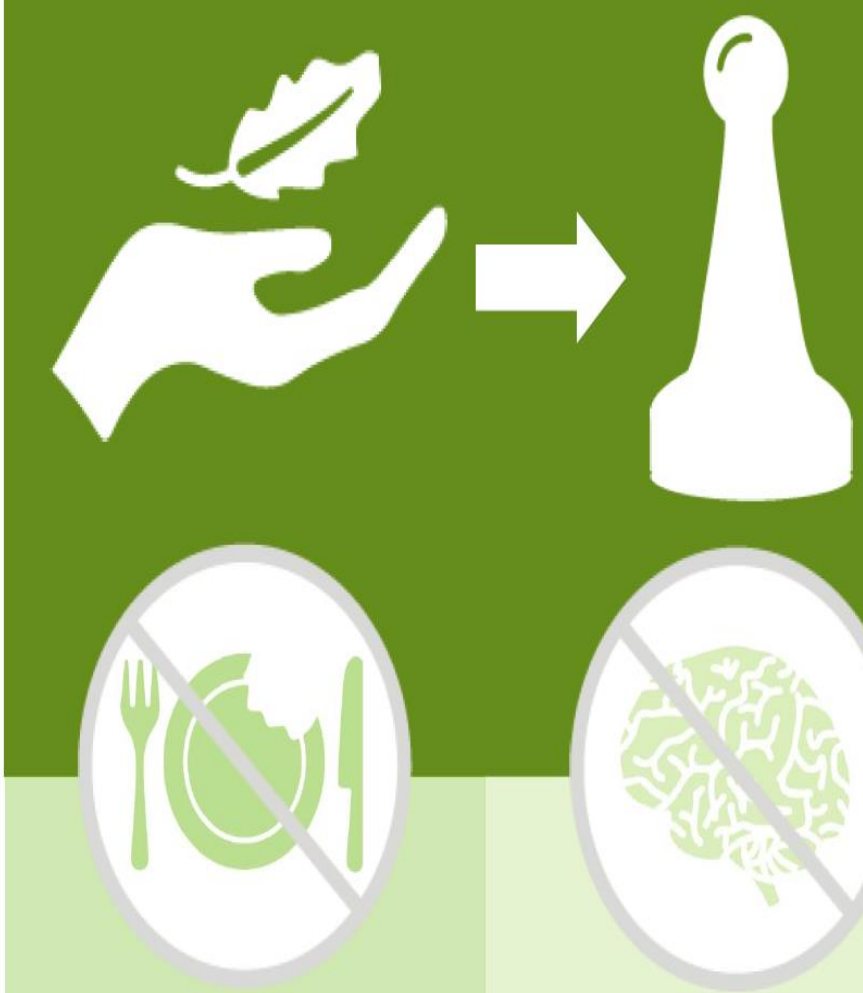
Source: Patrick Lenionci – 5 Dysfunctions of a Team and Ideal Team Player

WHAT HAPPENS WHEN PEOPLE ARE STRONG IN JUST ONE OF THOSE AREAS?

JUST HUMBLE

Nice, but doesn't get anything done.

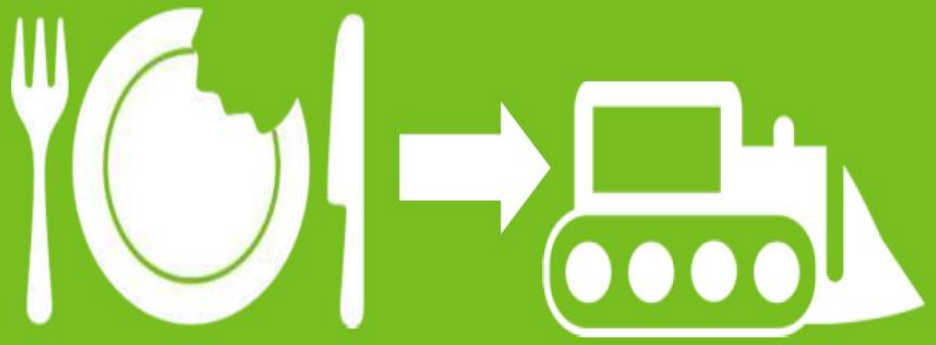
AKA, THE PAWN



JUST HUNGRY

It's all about them and
leaves a trail of hurt behind.

AKA, THE BULLDOZER



JUST SMART

Not hard working and doesn't get much done.

AKA, THE CHARMER

WHAT HAPPENS WHEN PEOPLE ARE STRONG IN TWO OF THESE AREAS?

HUMBLE

&

HUNGRY

Accidental mess maker but with good intentions.

HUMBLE

&

SMART

A loveable slacker who doesn't want to do too much.

HUNGRY

&

SMART

The most dangerous combination.

A skillful politician who is not humble and people get hurt.

HOW DO YOU USE THIS CONCEPT?

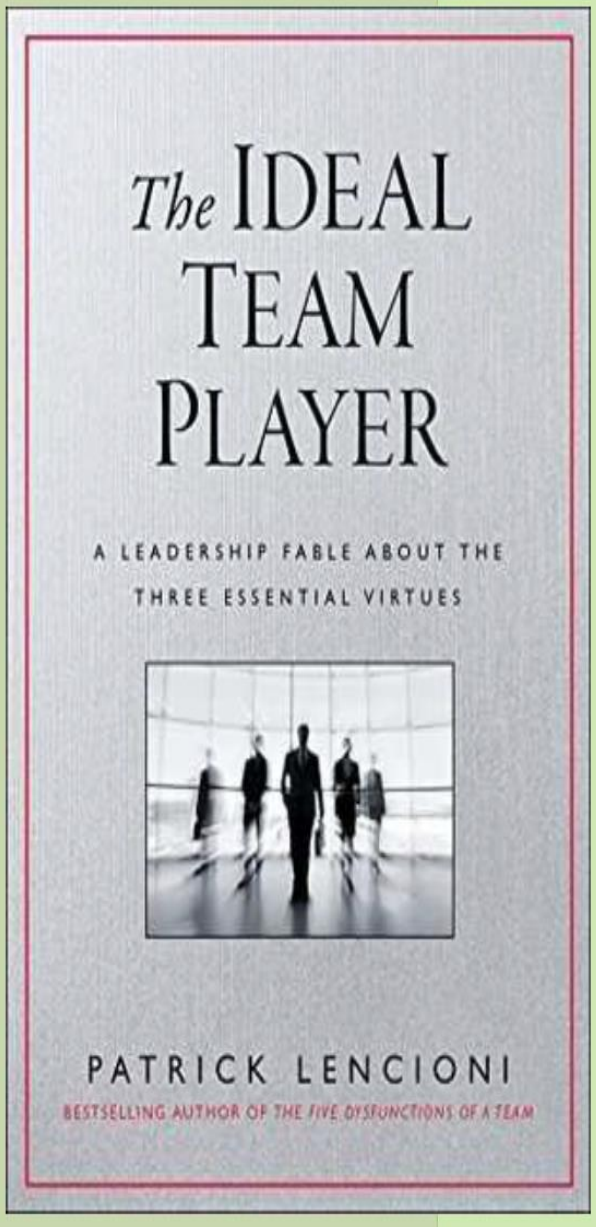
- Have your team rank themselves in the order of their strengths.
- Use the criteria as an ongoing framework for performance discussions.
- All of these virtues can be developed.

TEAM BUILDING
A

TEAM BUILDING ACTIVITY

Take-Aways

- Strategy
- Leadership & Teamwork
- Problem Solving Skills
- Communication Skills



Read the book to dig in and take your management to the next level.

QUESTIONS

Stephanie Williams-Hayes
VDH Information Security Officer
Stephanie Williams-Hayes@vdh.Virginia.gov
804-864-7111

Virginia Information Technologies Agency

Web Application Vulnerability Scanning Update

VITA
Commonwealth Security & Risk Management

November 7, 2018

COV Web Application Vulnerability Scanning Program

- History
  - 2009 Incident scans to paid service to legislative support for all systems in FY2017. Running for 2 years
- Status
  - 98% compliance, with a 40% reduction in critical vulnerabilities, footprint reduction, partnering with agencies to reduce risks. You receive quarterly scans and reports
- Future
  - Integrating internal sensitive applications into the program, further reduction. Vulnerable High risk applications apparent
- How you can help
  - Review reports & remediate, ask for assistance if needed

Results and Archer

- High and medium alerts in Archer
  - Volume is overwhelming
  - We hope to develop a dynamic solution at some point
- Agency Role
  - Ensure each scan has a matching application
  - Review repeat high and medium findings
  - Become familiar with this in Archer; Once we have our part set, agencies will be tasked with updating these in Archer

Alert Trends & Alert Reduction

- We scan 1500 unique URLs per quarter
  - Alerts are being remediated across the board
    - Virginia won national honors with DGIF # 1 400 websites
  - Repeat high & medium alerts are visible
  - Low's are not always low risk
  - You can test these as we do
- ISO role – Guide application developers and web masters to strive for a culture that creates secure resilient applications to reduce alerts

A Great Tool to help with that

OWASP

OWASP Top 10 - 2017

The Ten Most Critical Web Application Security Risks

(Open Web Application Security Project)

Why the OWASP Top Ten ?

- Adopting the OWASP Top 10 will foster a culture within your organization into one that produces secure code

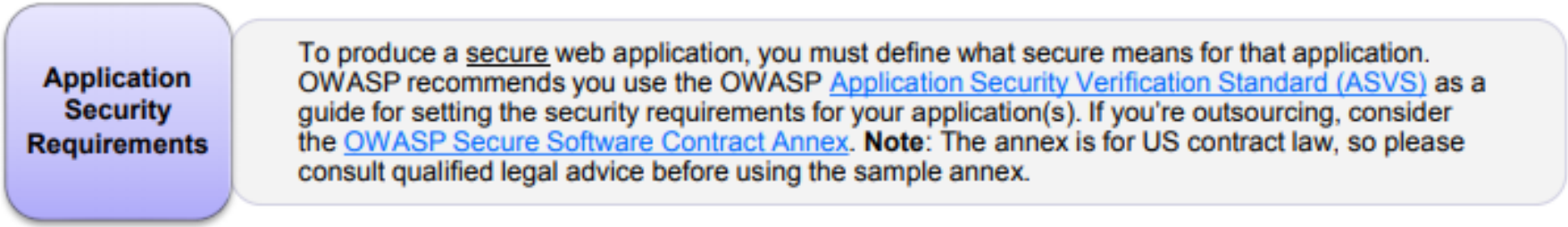
- Establish & Use Repeatable Security Processes and Standard Security Controls

  – https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=Main

Sections for Job function Roles

- What's next for Developers
- What's Next for Security Testers
- What's Next for Organizations
  - which is suitable for CIOs and CISOs, and
- What's Next for Application Managers
  - which is suitable for application managers or anyone responsible for the lifecycle of the application

Each Section has links to resources



- The OWASP Application Security Verification Standard (ASVS) Project provides a basis for testing web application technical security controls and also provides developers with a list of requirements for secure development

OWASP Application Security Verification Standard (ASVS) Project

OWASP ASVS 3.1 (early access)

- ASVS V1 Architecture
- ASVS V2 Authentication
- ASVS V3 Session Management
- ASVS V4 Access Control
- ASVS V5 Input validation and output encoding
- ASVS V7 Cryptography
- ASVS V8 Error Handling
- ASVS V9 Data Protection
- ASVS V10 Communications
- ASVS V13 Malicious Code
- ASVS V15 Business Logic Flaws
- ASVS V16 Files and Resources
- ASVS V17 Mobile
- ASVS V18 API
- ASVS V19 Configuration
- ASVS V20 Internet of Things

Application Security Architecture

Application Security Architecture

Rather than retrofitting security into your applications and APIs, it is far more cost effective to design the security in from the start. OWASP recommends the OWASP Prevention Cheat Sheets as a good starting point for guidance on how to design security in from the beginning.

OWASP Cheat Sheets

V · T · E	Cheat Sheets [Collapse]
Developer / Builder	3rd Party Javascript Management · Access Control · AJAX Security Cheat Sheet · Authentication (ES) · Bean Validation Cheat Sheet · Choosing and Using Security Questions · Clickjacking Defense · Credential Stuffing Prevention Cheat Sheet · Cross-Site Request Forgery (CSRF) Prevention · Cryptographic Storage · C-Based Toolchain Hardening · Deserialization · DOM based XSS Prevention · Forgot Password · HTML5 Security · HTTP Strict Transport Security · Injection Prevention Cheat Sheet · Injection Prevention Cheat Sheet in Java · JSON Web Token (JWT) Cheat Sheet for Java · Input Validation · Insecure Direct Object Reference Prevention · JAAS · Key Management · LDAP Injection Prevention · Logging · Mass Assignment Cheat Sheet · .NET Security · OS Command Injection Defense Cheat Sheet · OWASP Top Ten · Password Storage · Pinning · Query Parameterization · REST Security · Ruby on Rails · Session Management · SAML Security · SQL Injection Prevention · Transaction Authorization · Transport Layer Protection · TLS Cipher String Configuration · Unvalidated Redirects and Forwards · User Privacy Protection · Web Service Security · XSS (Cross Site Scripting) Prevention · XML External Entity (XXE) Prevention Cheat Sheet
Assessment / Breaker	Attack Surface Analysis · REST Assessment · Web Application Security Testing · XML Security Cheat Sheet · XSS Filter Evasion
Mobile	Android Testing · IOS Developer · Mobile Jailbreaking
OpSec / Defender	Virtual Patching · Vulnerability Disclosure
Draft and Beta	Application Security Architecture · Business Logic Security · Content Security Policy · Denial of Service Cheat Sheet · Grails Secure Code Review · IOS Application Security Testing · PHP Security · Regular Expression Security Cheatsheet · Secure Coding · Secure SDLC · Threat Modeling
	All Pages In This Category

Standard Security Controls

Standard Security Controls

Building strong and usable security controls is difficult. Using a set of standard security controls radically simplifies the development of secure applications and APIs. The OWASP Proactive Controls is a good starting point for developers, and many modern frameworks now come with standard and effective security controls for authorization, validation, CSRF prevention, etc.

- https://www.owasp.org/index.php/OWASP_Proactive_Controls

OWASP Top 10 Proactive Controls 2018

- The OWASP Top Ten Proactive Controls 2018 is a list of security techniques that should be included in every software development project. They are ordered by order of importance, with control number 1 being the most important. This document was written by developers for developers to assist those new to secure development.

Proactive Controls ...

1. Define Security Requirements
2. Leverage Security Frameworks and Libraries
3. Secure Database Access
4. Encode and Escape Data
5. Validate All Inputs
6. Implement Digital Identity
7. Enforce Access Controls
8. Protect Data Everywhere
9. Implement Security Logging and Monitoring
10. Handle All Errors and Exceptions

Secure Development Lifecycle

Secure Development Lifecycle

To improve the process your organization follows when building applications and APIs, OWASP recommends the OWASP Software Assurance Maturity Model (SAMM). This model helps organizations formulate and implement a strategy for software security that is tailored to the specific risks facing their organization.

- Great model to help create a secure development program
- Quick start guide helps assess the current status and move through stages to a mature risk based model
- Scanning is a small component

Application Security Education

Application Security Education

The OWASP Education Project provides training materials to help educate developers on web application security. For hands-on learning about vulnerabilities, try OWASP WebGoat, WebGoat.NET, OWASP NodeJS Goat, OWASP Juice Shop Project or the OWASP Broken Web Applications Project. To stay current, come to an OWASP AppSec Conference, OWASP Conference Training, or local OWASP Chapter meetings.

- SANS Role Based Training and Application Developer Security Awareness Training

Just sending Gobbledygook

- Something that looks like garbage is likely an encoded attack
- Evasion techniques
- Escape, validate and limit encoding

It's public data anyway.

- Let's not make our visitors use SQL injection to get the data
- Applications should be secure so they are not used to pivot
- It brings more scrutiny from evil doers
- SQL Injection is easy to detect and easy to fix
  - OWASP Top 10 – A1

It's False Positive

- By far the most common comment across the board
- The scanner software is not intelligent but typically accurate in the context of the test
- The HTTP request and response tells the story
- You can see this with a simple tool
- A false negative is worse

The scans caused X

- Crashed our site
- Corrupted the database
- Sent 50,000 emails

- Investigate and resolve
- Any of these issues are vulnerable from a third party as well

  – A6:2017-Security Misconfiguration

We can't patch

- Too busy
- We'll have to recreate what we've done
- Patches fix problems and plug exploits
- Scans identified most vulnerabilities related to successful exploits before they were executed
- This is the number one cause of successful exploits
  - A9:2017-Using Components with Known Vulnerabilities

WAF and IPS are adequate protection

- Blocks scans & automated testing
- Cannot block
  - Tamper scripts
  - Proxy Tools
  - Evasion Techniques
  - Persistent People
  - Incidents
- We must fix the applications in addition to the use of WAF and IPS technologies
  - Defense in depth

WordPress

!	WordPress username enumeration	1
!	WordPress XML-RPC authentication brute force	1
!	Insecure transition from HTTPS to HTTP in form post	32
!	Possible sensitive directories	1
!	WordPress admin accessible without HTTP authentication	1
!	WordPress default administrator account	1

- Wpscan, Burp Suite Pro
- Logon page, Patch
- WPMain
- A9:2017-Using Components with Known Vulnerabilities

Summary

- Work with web scanner team or the incident handlers
- Keep Archer current
- Read your quarterly reports, test and remediate vulnerabilities, review each alert, ask for help
- Use the OWASP Top 10 to help create a secure development culture
- Implement a defense in depth strategy

Questions?

Upcoming Events

Miscellaneous Announcements

Ed Miller
Director IT Security Governance

Miscellaneous Announcements

- The new IT Risk Management Standard is on ORCA now. Please review & comment.

- The NCSR Survey is online in Archer. Please review it & complete by December 15. (it's at the top of the "Agency Workspace" in Archer.)

- Quarterly Updates: When submitting your QU's, be sure to include Risk Treatment Plan Updates.

SAVE THE DATE

COV Security Conference

Date: April 11&12

Location: Altria Theater

Cost: $175

If you are interested in presenting:

Email: covsecurityconference@vita.virginia.gov

For more information.

More information on registration will be coming soon……

IS Orientation

The last IS Orientation for 2018 will be held on:

December 13, 2018 @1:00 PM

CESC - Room 1221

ISO Certification Contacts

If you still have questions about your certification, contact:

Edward.Miller@vita.virginia.gov

Tina Harris-Cunningham@vita.virginia.gov

Future ISOAG

December 5 , 2018 @ CESC 1:00-4:00

Panel Discussion on Ransomware

Panelists: Tim McBride, NIST
Gregory Bell, DBHDS
Samuel "Gene" Fishel, OAG
Wes Kleene, VITA

Tier III Data Centers
Chris Boswell, VITA

ISOAG meets the 1st Wednesday of each month in 2018

ADJOURN

THANK YOU FOR ATTENDING

Picture courtesy of www.v3.co.uk