

RSA®Conference2018

San Francisco | April 16 – 20 | Moscone Center

SESSION ID: DEV-R12

DEVSECOPS – USING CONTAINERS TO SPEED UP YOUR TESTING

Tim Chase

Director of Security – AppSec and Cloud
Nielsen



#RSAC

What is DevOps

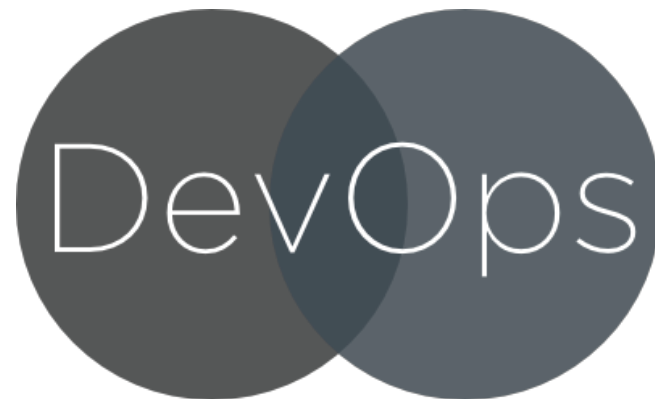


***DevOps** is the combination of cultural philosophies, practices, and tools that increases an organization's ability to deliver applications and services at high velocity – AWS Blog*

What is DevOps



- Brings Dev, Testing, Ops together
- Culture Change
- Goal is to reduce cycle time

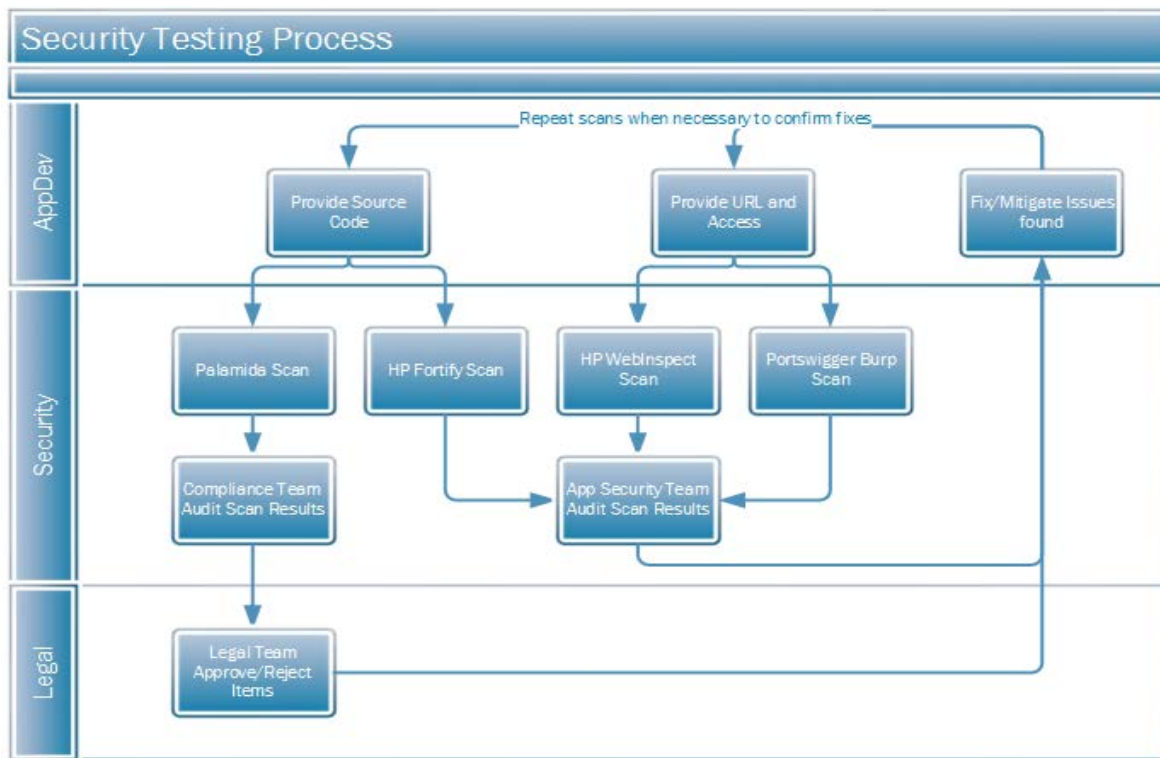


What is DevOps



“Until code is in production, no value is actually being generated, because it’s merely WIP stuck in the system.”— Gene Kim

Conventional AppSec Testing



Conventional AppSec testing is too slow

SLOW

Traditional AppSec Testing Doesn't Work



- Slow
- Too many people involved
- Manual
- Not flexible

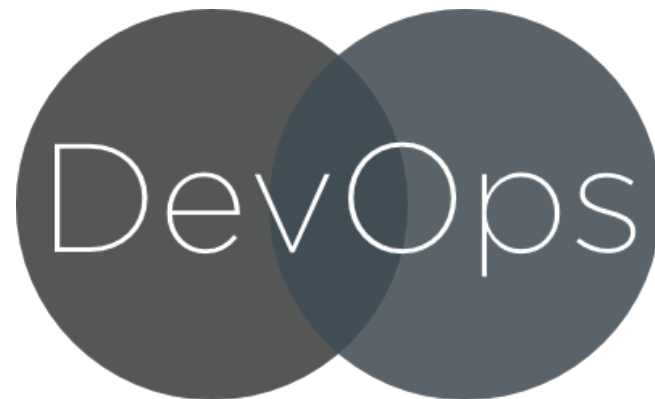


DevOps Changes Security



DevOps forces security to change

- Faster
- More Accurate
- Flexible
- Shift Responsibility



DevSecOps enters the picture



- Incorporate security principles into DevOps
- Make developers responsible for security
- Move security team to auditors/SMEs
- Shift in culture

What's the magic DevSecOps solution?



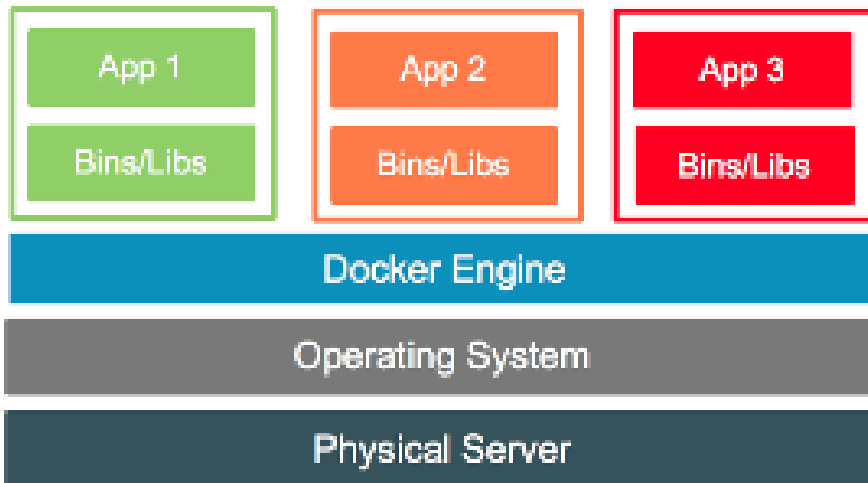
- No silver bullet
- Its about what works for you
- Keys
 - Increase Dev Responsibility
 - Automated
 - No PDFs!!
 - Flexible



One possible solution is containers



What's a container?



EXAMPLE OF A CONTAINER

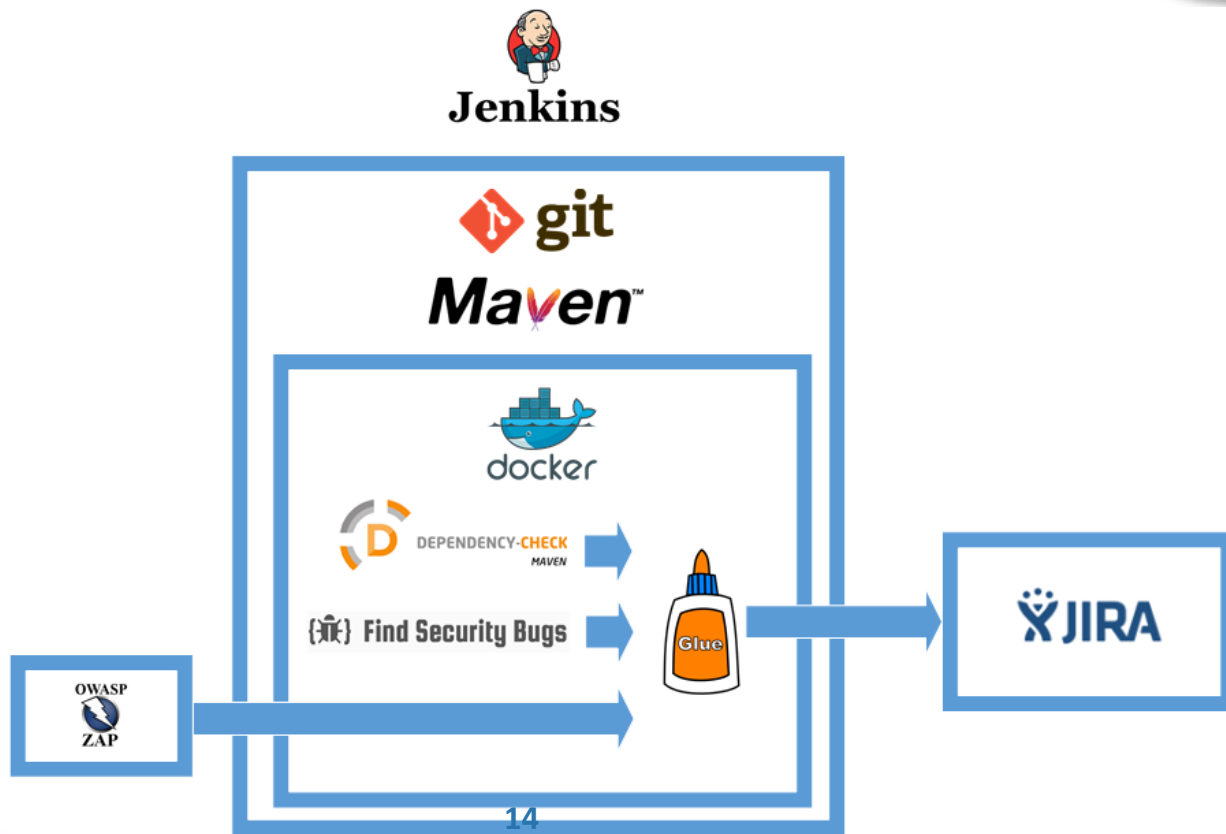
Packages apps into a single container for deployment

Containers + Security



- Determine application set
- Group all of your applications together
- Install in a Docker container
- Configure in build automation tool

Security Container Example



RSAConference2018



#RSAC

SIMPLE EXAMPLE

Tools Needed



- Jenkins
- Docker
- OWASP Glue
- Jira



Jenkins

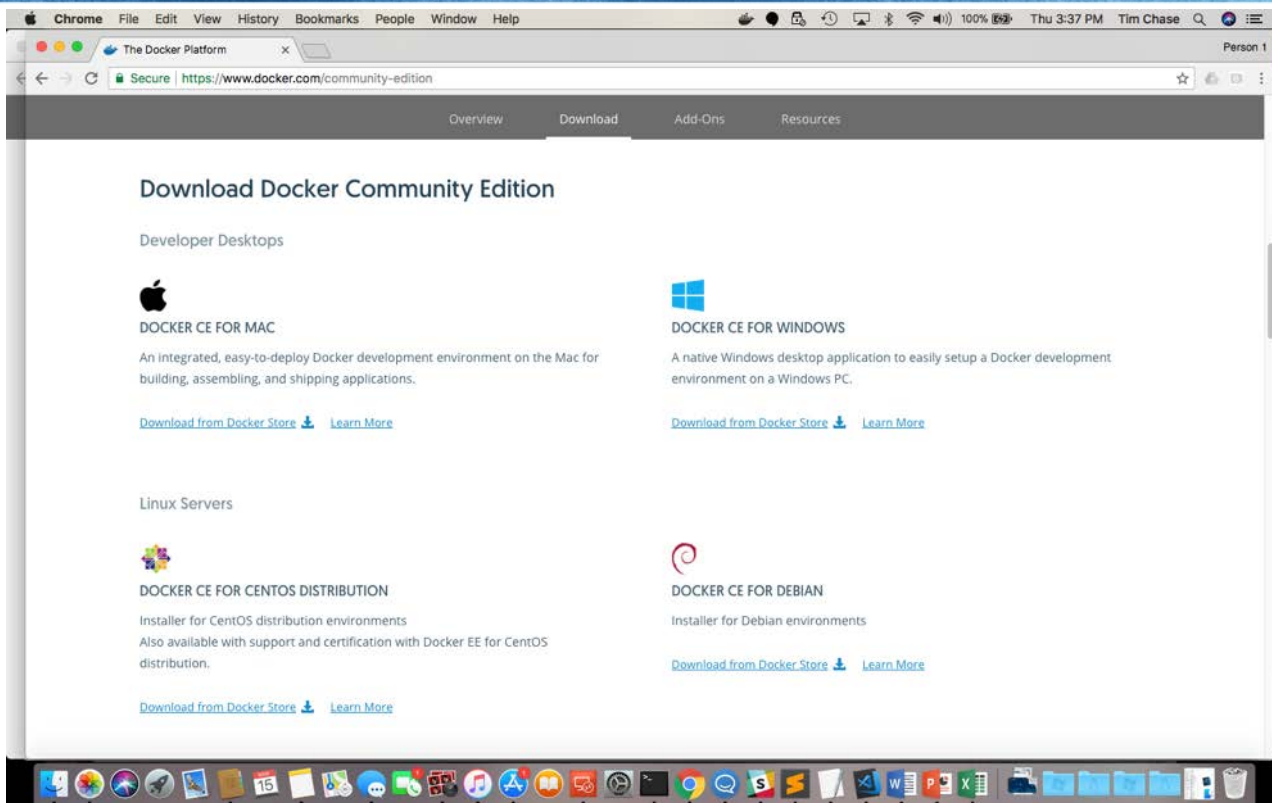


- Helpful for creating a pipeline of tools
- Docker container with security tools installed
- Easily extendable to new tools



- Examples of tools
 - Brakeman
 - FindSecBugs
 - NSP
 - Contrast (commercial)
 - Checkmarx (commercial) eslint
- Export
 - Jira
 - JSON
 - CSV/Text

Install Docker



Run Glue



- Decide what tools you want to use
- Decide how to export your data
- Build your command.....

```
docker run -v "${PWD}":/src/ --rm owasp/glue -d -t OWASPDdependencyCheck -d /src -f jira --jira-api-url https://adlm.company.com --jira-api-context "/jira" --jira-username "userID" --jira-password "Password123" --jira-project Project
```


Run Glue



```
test_services — ec2-user@ip-172-31-42-81:~ — -bash — 82x24
Tims-MBP:test_services timchase$ docker run -v "${PWD}":/src/ --rm owasp/glue -d -
t OWASPDdependencyCheck -d /src -f jira --jira-api-url https://a[REDACTED]/jir
a --jira-username [REDACTED] --jira-password [REDACTED] --jira-project BAPS --jira-co
mponent defect
Loading scanner...
Logfile nil?
calling scan
Running scanner
Mounting ... /src
Mounting target: /src
Checking about mounting /src with #<Glue::DockerMounter:0x000000022ef6d8>
In Docker mounter, target: /src became: ... wondering if it matched .docker
Checking about mounting /src with #<Glue::FileSystemMounter:0x000000022eeff8>
Mounting /src with #<Glue::FileSystemMounter:0x000000022eeff8>
Mounted /src with #<Glue::FileSystemMounter:0x000000022eeff8>
Processing target.../src
Running tasks in stage: wait
Running tasks in stage: mount
Running tasks in stage: file
Running tasks in stage: code
code - OWASPDdependencyCheck - #<Set:0x000000022b4948>
OWASP Dependency Check
Parsing report /src/dependency-check-report.xml
Fingerprint: CVE-2017-8806:postgresql-9.4.1208.jar
```

Push Glue to Jira



Browser window showing a Jira issue page for "CVE-2014-0085 in zookeeper-3.4.5-cdh5.5.2.jar". The page is titled "nielsen" and includes navigation tabs like Dashboards, Projects, Issues, Boards, Structure, Tests, Portfolio, Links, and Create. The issue details are as follows:

Details

Type:	Bug	Status:	TO DO (View Workflow)
Priority:	Low	Resolution:	Unresolved
Component/s:	None		
Labels:	None		
Automation Type:	Not Applicable		

Description

Description: CVE-2014-0085 in zookeeper-3.4.5-cdh5.5.2.jar
Timestamp: 2018-03-16 15:29:49 +0000
Source: zookeeper-3.4.5-cdh5.5.2.jar
https://bugzilla.redhat.com/show_bug.cgi?id=1067285, <http://rhn.redhat.com/errata/RHSA-2014-0400.html>
Severity: 2.1
Fingerprint: CVE-2014-0085:zookeeper-3.4.5-cdh5.5.2.jar
Detail: Apache Zookeeper logs cleartext admin passwords, which allows local users to obtain sensitive information by reading the log.
CWE-255 Credentials Management

Attachments

Drop files to attach, or browse.

Activity

All Comments Work Log History Activity Links Hierarchy Transitions Reopenings History SLA Overview

People

Assignee: Unassigned
Reporter: Tim Chase
Votes: 0
Watchers: 1 Stop watching this issue

Dates

Created: 16/Mar/18 10:33 AM
Updated: 16/Mar/18 10:33 AM

Development

Create branch

Agile

View on Board

HipChat discussions

Dedicated room: Create a room Choose a room
Other rooms: Issue mentioned in 0 rooms

Connect Glue to Jenkins



- To make truly DevOps, connect to automation
- In Jenkins, add a Build Step
- In the build step, execute a shell command that runs your docker command

Connect Glue to Jenkins



localhost:8080/job/Test%20Project/configure

Jenkins » Test Project »

General Source Code Management Build Triggers **Build Environment** Build Post-build Actions

☐ Use secret text(s) or file(s)
☐ Abort the build if it's stuck
☐ Add timestamps to the Console Output
☐ With Ant

Build

Execute shell

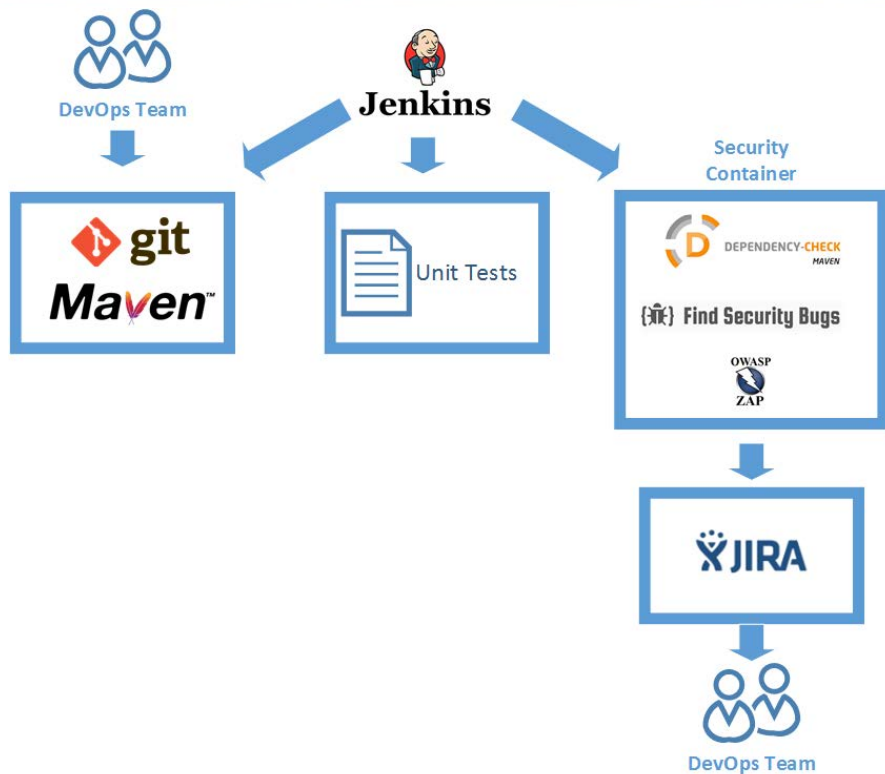
Command

```
echo $PWD  
mvn install -Dmaven.test.skip=true  
#docker pull owasp-glue  
echo "Starting Glue tool"  
echo "Script executed from ${PWD}"  
echo "${USER}"  
docker run -v "${PWD}":/src/ --rm owasp/glue -d -t OWASPDdependencyCheck -d /src -f jira --jira-a
```

See [the list of available environment variables](#)

Save Apply Advanced...

Security Container Example



Why a Security Container?



- Easy change of tools
- Easy rollout (i.e. prereq handled)
- Easy update
- Flexible for different environments
- Automated and integrated
- Cost

Where to Start



Start Easy

- One App to test
- Determine Tools for container
- Integrate with Dev Team

Where to Start



- Open source container: OWASP Glue
- Support out of box for many free tools
 - PMD
 - FindSecBugs
 - Brakeman
 - RetireJS
 - Dependency Check



Work to mature solution



- Add more tools
- Add different types of tools
 - Dependency Checks
 - Code quality checks
 - Dynamic scans
 - Gauntlt
- Fail the build



Keys to success



- DevOps mature
- Security champion on teams
- Really smart people
- Really technical people
- Flexibility
- Be OK to fail

Apply What You Have Learned Today



- Next Week
 - Try the solution with one application
- In the next 3 months
 - Determine standard toolset for one group of apps
 - Create and rollout container for similar apps
- In the next 6 months
 - Review success of initial container rollout
 - Determine plan for remaining applications

RSA®Conference2018



#RSAC

QUESTIONS