

RSA[®]Conference2019

San Francisco | March 4–8 | Moscone Center



BETTER.

SESSION ID: ASD-R02

Container Security at the Speed of CI/CD

Tim Chase

Director of Security
HealthStream



#RSAC

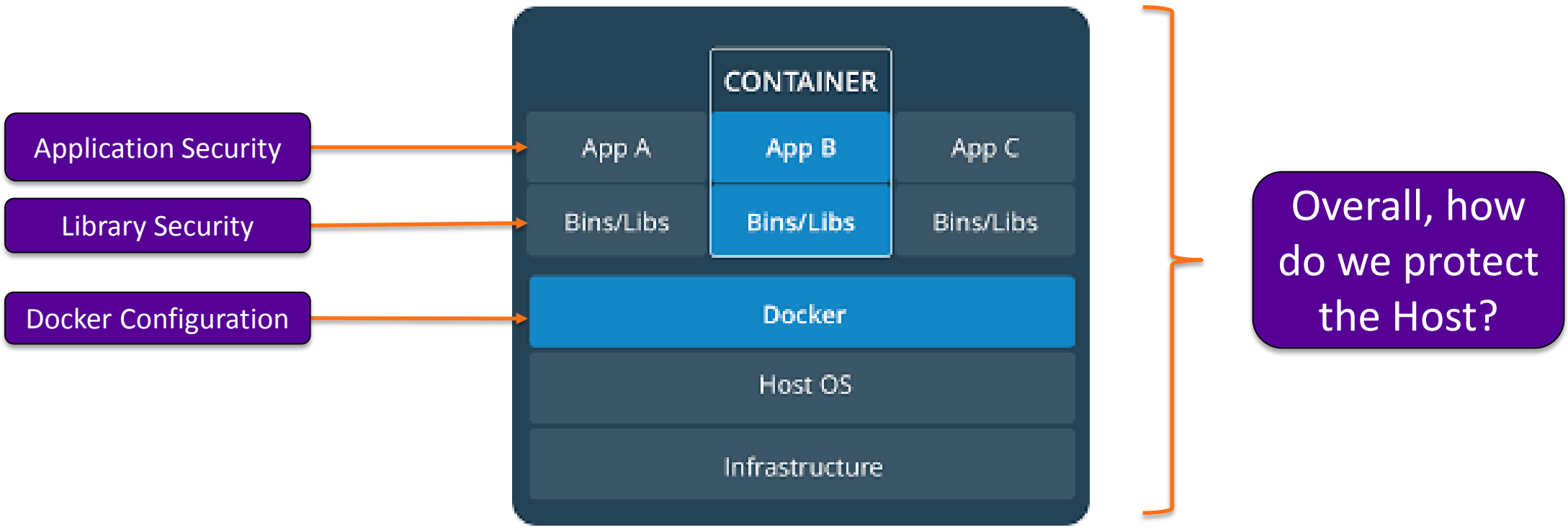
Intro To Tim

- Director of Security at HealthStream
- Been in security field for 15 years.
- Trainer on LinkedIn training
- Board advisor for C|ASE certification with EC-Council
- Focused on application security for many years
- Last few years spend a lot of time in cloud and containers

What's the problem?

- Containers are one package with everything
 - App Security/server security must combine
- Security thought must change
 - Be Faster
 - Must secure between containers

What's the Problem? – Container Example



EXAMPLE OF A CONTAINER

Packages apps into a single container for deployment

(image from docker.com)

What's the problem? – Library and AppSec

- OWASP 2013 broke out libraries into its own item (A-9)
- Equifax and Struts
- Easy to miss with containers
 - Containers are code
 - Traditional scans don't always work

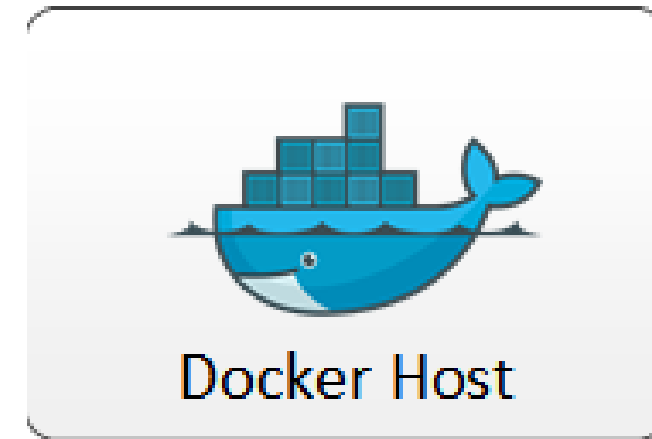
What's the problem? – Docker Configuration

- Docker has security holes
- Can fall to misconfiguration like anything (A6)
- CIS benchmarks for Docker



What's the problem? – Host Security

- Think of Docker like VMWare
- Be aware of Container Escape
- Docker uses ports like servers



What's the problem?

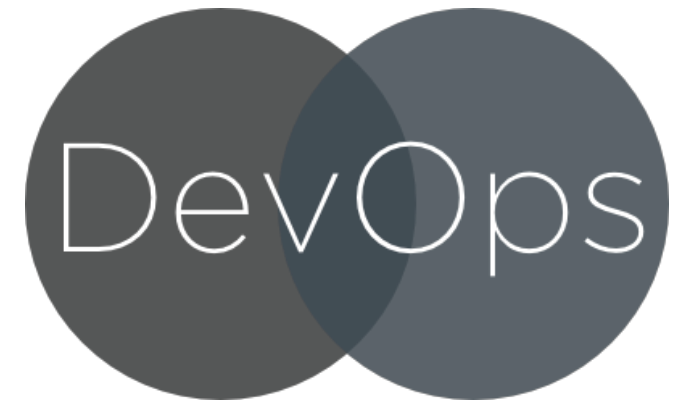
- Containers are one package with everything
 - App Security/server security must combine
- Security thought must change
 - **Be Faster**
 - Must secure between containers

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

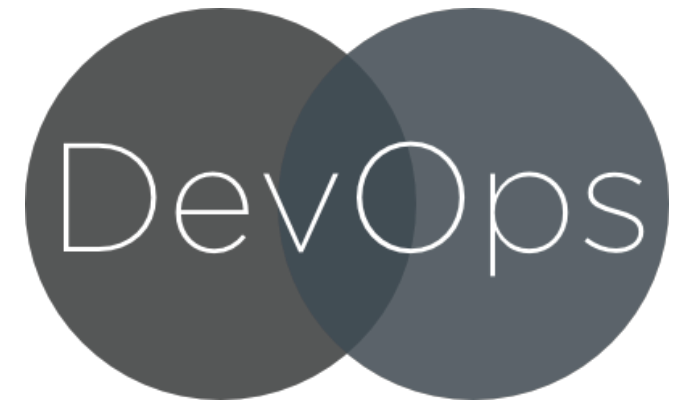
- Brings Dev, Testing, Ops together
- Culture Change
- Goal is to reduce cycle time



DevOps Changes Security

DevOps forces security to change

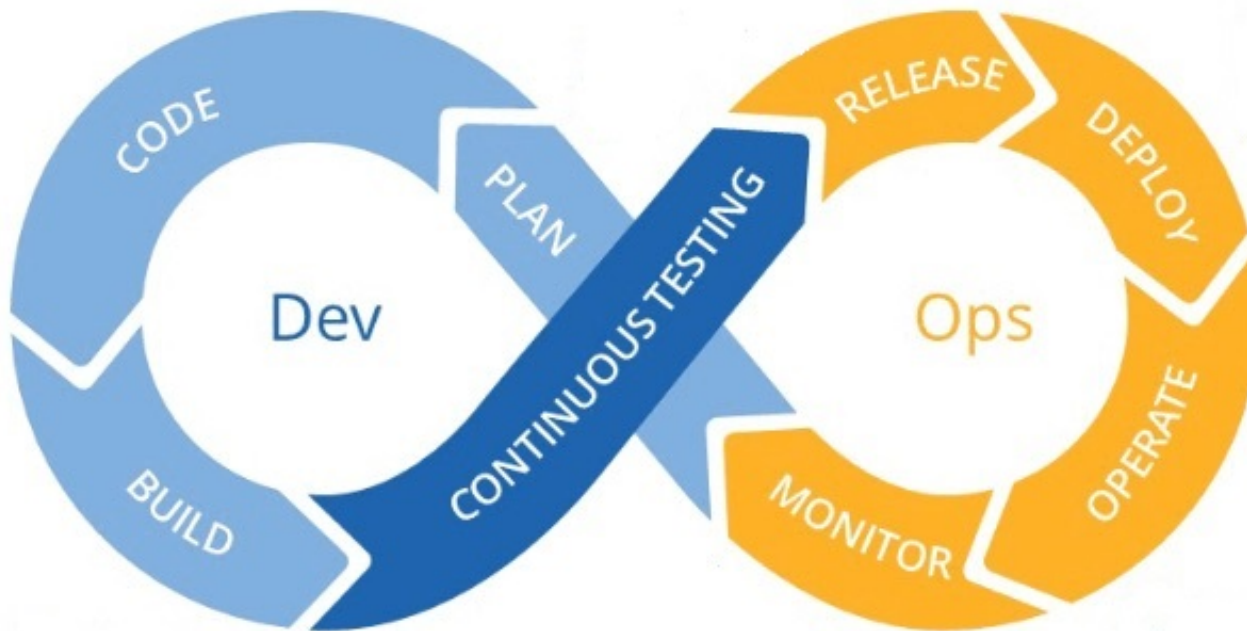
- Faster
- More Accurate
- Flexible
- Shift Responsibility



DevSecOps enters the picture

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

What is CI/CD?



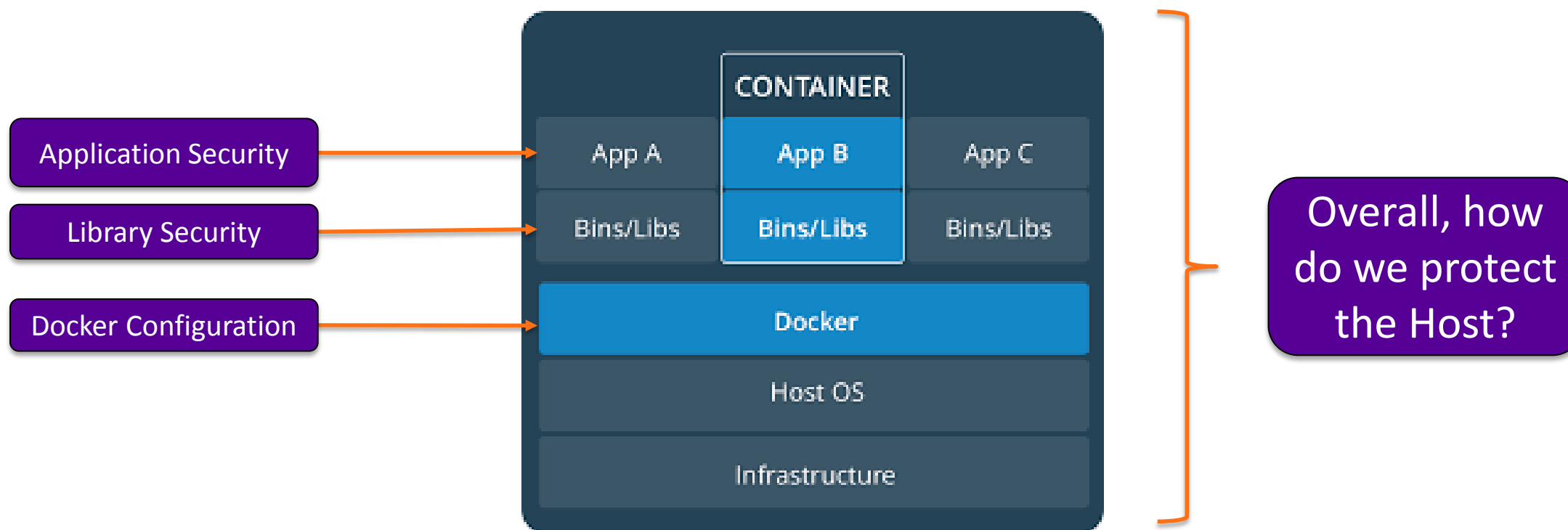
- Continuous Integration \ Continuous Deployment
- Build once a day or many times a day

Image from <https://www.mabl.com/blog/what-is-cicd>

What is CI/CD

- Continuous Integration
 - Automated developer check-in
 - After check-in, code is deployed
 - Automated tests usually are next
- Continuous Deployment
 - Automated release to production
 - Next step after CI passes checks
 - Usually goes together with CI

What's the Problem? – Container Example



EXAMPLE OF A CONTAINER

Packages apps into a single container for deployment

Container Security Parts

Vulnerabilities	Policies	Runtime Protection
<ul style="list-style-type: none">• What libraries are out of date• Are you using components with open CVEs	<ul style="list-style-type: none">• Compliance to container best practices• Example: Keys in container, SSH running in containers	<ul style="list-style-type: none">• Prevent container escape• Monitor for unusual activities on container

Examples

Twistlock



Monitor / Vulnerabilities

Vulnerability Explorer

Images

Hosts

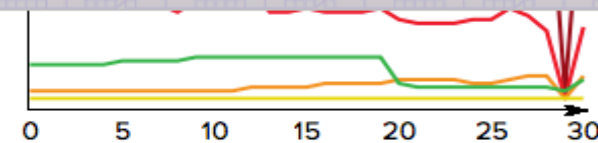
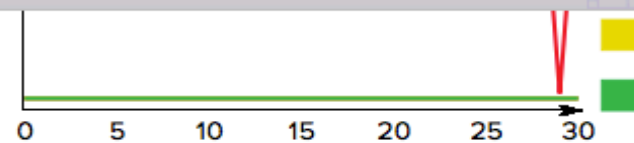
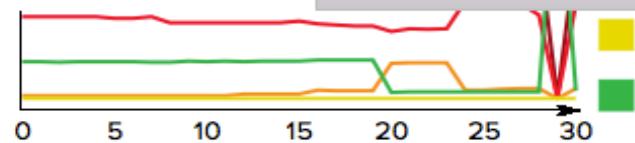
Registry

Serverless

Jenkins Jobs

Twistcli Scans

CVE Viewer



Top 10 most critical vulnerabilities (CVEs)

Images

Hosts

CSV

Search for a specific CVE in your environment

ID	Risk Score	Risk Factors	Impacted Packages	Impacted Images
CVE-2018-1270	0 <div><div></div></div> 1K	6	spring framework_spring-core:2.5.6	1
CVE-2018-7489	0 <div><div></div></div> 1K	5	com.fasterxml.jackson.core_jackson-databind:2.7.8, com.f...	9
CVE-2017-2519	0 <div><div></div></div> 1K	6	sqlite3:3.8.7.1-1+deb8u2	4
CVE-2018-1123	0 <div><div></div></div> 1K	7	procps-ng:3.3.10-10.el7, procps-ng:3.3.10-16.el7, procps:2:3...	14
CVE-2017-2518	0 <div><div></div></div> 1K	6	sqlite3:3.11.0-1ubuntu1, sqlite3:3.8.7.1-1+deb8u2	5
CVE-2017-7000	0 <div><div></div></div> 1K	6	sqlite:3.7.17-8.el7	7
CVE-2017-17485	0 <div><div></div></div> 1K	5	com.fasterxml.jackson.core_jackson-databind:2.8.5, com.f...	9
CVE-2017-2520	0 <div><div></div></div> 1K	6	sqlite3:3.11.0-1ubuntu1, sqlite3:3.8.7.1-1+deb8u2	5
CVE-2018-1000122	0 <div><div></div></div> 1K	6	curl:7.29.0-42.el7_4.1, curl:7.29.0-42.el7, curl:7.52.1-r1, curl:7...	2
CVE-2018-1000120	0 <div><div></div></div> 1K	6	curl:7.58.0-r0, curl:7.52.1-5+deb9u4, curl:7.47.0-1ubuntu2.6,...	2

Filter:

Updates

Available

Installed

Advanced

Install ↓

Name

Version

[Static Analysis Collector Plug-in](#)



This plug-in is an add-on for the plug-ins [Checkstyle](#), [Dry](#), [FindBugs](#), [PMD](#), [Task Scanner](#), and [Warnings](#): the plug-in collects the different analysis results and shows the results in a combined trend graph. Additionally, the plug-in provides health reporting and build stability based on these combined results.

1.46

[Static Analysis Utilities](#)



This plug-in provides utilities for the static code analysis plug-ins.

1.75

[Brakeman Plugin](#)



This plugin reads output from [Brakeman](#), a static analysis security vulnerability scanner for Ruby on Rails.

0.7

[Hudson Codescanner Plug-in](#)



This plugin generates the trend report for [Codescanner](#), a tool which uses static analysis to look for bugs, hints and other useful information in Symbian C++ source code.

0.11

[Coverity plugin](#)



This plugin integrates Jenkins with the [Coverity Connect](#) and [Coverity Static Analysis](#) tools.

1.7.1

[FindBugs Plug-in](#)



This plugin generates the trend report for [FindBugs](#), an open source program which uses static analysis to look for bugs in Java code.

4.63

[Kiuwan plugin](#)



This plugin allows you to Run [Kiuwan](#) static analysis of your code as part of your continuous integration process with Jenkins. You can update your code quality information in Kiuwan automatically.

1.3.5

Install without restart

Download now and install after restart

Update information obtained: 13 hr ago

Check now

Jenkins Integration

Twistlock

Address

Twistlock Console address, formatted as https://hostname:port

User

Twistlock account name used to authenticate to the Twistlock API

Password

Twistlock account's password

OK

Test Connection



Monitor / Vulnerabilities

- Vulnerability Explorer
- Images
- Hosts
- Registry
- Serverless
- Jenkins Jobs
- Twistcli Scans
- CVE Viewer

Dashboard

Defend

- Firewalls
- Runtime
- Vulnerabilities
- Compliance
- Access

Monitor

- Firewalls
- Runtime

Vulnerabilities

- Compliance
- Access

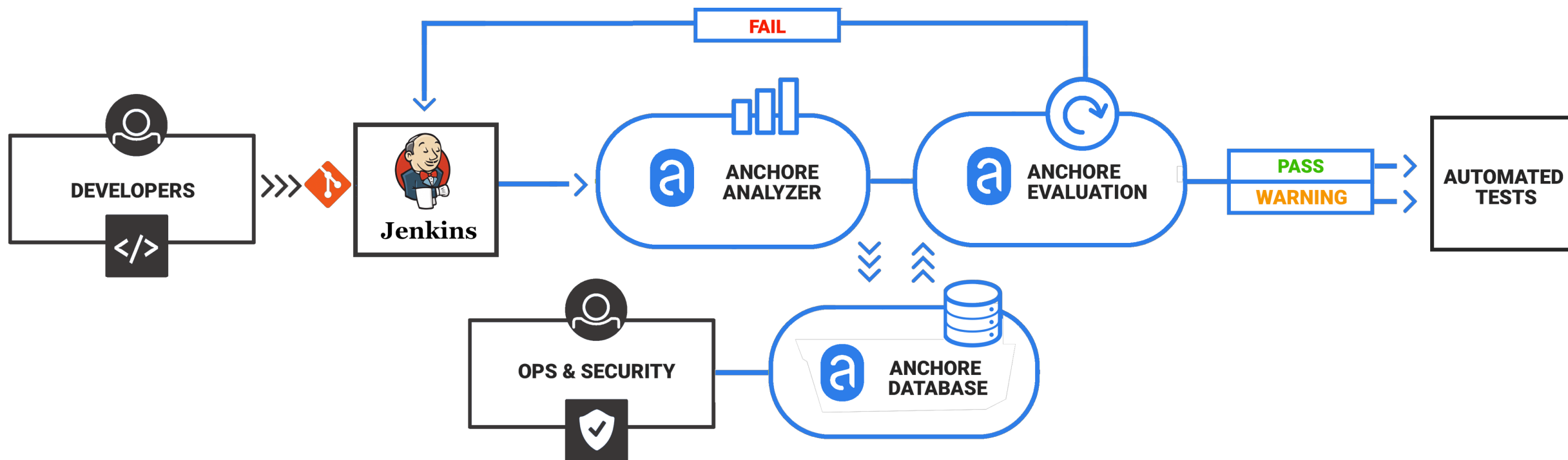
Manage

CSV

Search Jenkins jobs

Image	Node	Project	Build	Vulnerabilities	Risk Factors	Scan Time	Status
buy/centos7:7.5-2		bakerjg-Basel...	8	211 76 8	8	Aug 23, 2018 8:2	✓
buy/centos7:7.5-2		bakerjg-Basel...	7	211 76 8	8	Aug 23, 2018 7:3	✓
buy/centos7:7.5-2		bakerjg-Basel...	6	211 76 8	8	Aug 23, 2018 7:2	✓
buy/centos7:7.5-2		BaselImage_c...	52	211 76 8	8	Aug 23, 2018 6:3	✓
buy/centos7:7.5-3		bakerjg-Basel...	5	211 76 8	8	Aug 22, 2018 4:4	✓
buy/centos7-nginx:...		bakerjg-twistl...	3	240 115 12	9	Aug 22, 2018 3:5	✓
buy/centos7-nginx:...		bakerjg-twistl...	2	240 115 12	9	Aug 22, 2018 3:4	✓
buy/centos7-nginx:...		bakerjg-twistl...	1	240 115 12	9	Aug 22, 2018 3:4	✓
buy/centos7-tomca...		twistlock-scan	7	214 87 1711	9	Aug 22, 2018 2:2	✗

Container Security Flow



Container - Compliance

- Ensuring that docker images are setup with best practices
- Utilize standards like CIS benchmarks
- Continually monitor for updates

Demo Compliance rule

Compliance template ▼

1 Compliance actions

All types ▼

Set action on all

Ignore Alert Block

Search



All types	Severity ▼	Action	Description
Docker (CIS CE v1.1.0)	medium	Ignore Alert Block	Audit Docker files and directories - docker.service
container	medium	Ignore Alert Block	Create a separate partition for containers
image	medium	Ignore Alert Block	Audit Docker files and directories - docker.socket
host config	medium	Ignore Alert Block	Audit Docker files and directories - /etc/default/docker
daemon config	medium	Ignore Alert Block	Audit Docker files and directories - /etc/docker/daemon.json
daemon config files	medium	Ignore Alert Block	Audit Docker files and directories - /usr/bin/docker-containerd
security operations	medium	Ignore Alert Block	Audit Docker files and directories - /usr/bin/docker-runc
Kubernetes (CIS v1.2.0)	medium	Ignore Alert Block	Use the updated Linux Kernel
master	medium	Ignore Alert Block	Keep Docker up to date
worker	medium	Ignore Alert Block	Only allow trusted users to control Docker daemon
federation	high	Ignore Alert Block	
Twistlock Labs			
container			
image			
Linux (CIS v1.1.0)			
host			
Istio			
istio			
Custom			
image			

2

3

Customized error string (e.g., Please open a ticket at <http://helpdesk>)

Radar

Defend ▼

Firewalls

Runtime

Vulnerabilities

Compliance

Access

Monitor ▼

Firewalls

Runtime

Vulnerabilities

Compliance

Access

Manage ►

Container - Runtime

- Monitor the runtime security of docker containers on a host
- Look for specific items
 - Container escape
 - Unusual open ports
 - Data being exfiltrated

- Radar
- Defend
 - Firewalls
 - Runtime
 - Vulnerabilities
 - Compliance
 - Access
- Monitor
 - Firewalls
 - Runtime
 - Vulnerabilities
 - Compliance
 - Access
- Manage

Active Archived

Search incidents



Collections

Category	Type	Host	Impacted	Date	Actions	Collections
Hijacked process	Container	demo-neil-lab-twistlock-com	neilcar/struts2_demo:latest	Dec 6, 2018 9:12:56 AM		
Data exfiltration	Container	demo-neil-lab-twistlock-com	neilcar/struts2_demo:latest	Dec 6, 2018 9:12:56 AM		
Port scanning	Container	demo-neil-lab-twistlock-com	neilcar/struts2_demo:latest	Dec 6, 2018 9:12:51 AM		
Lateral movement	Container	demo-neil-lab-twistlock-com	morello/httpd:latest	Dec 6, 2018 9:11:34 AM		

First << Prev 1 2 Next >> Last
Pg 1 of 2

Incident Hijacked process

This incident category indicates that an allowed process has been used in ways that are inconsistent with its expected behavior. This type of incident could be a sign that a process has been used to compromise a container

[Learn more](#)

View forensic data

Host name demo-neil-lab-twistlock-com

Container name /strutsserver

Image name neilcar/struts2_demo:latest

Time 2018-12-06 09:12:56

Total 2 audit items in incident

csv

Dec 6, 2018 9:12:56 AM

PROCESSES

Dec 6, 2018 9:12:56 AM

FILESYSTEM

Details

/bin/bash launched from /usr/lib/jvm/java-7-openjdk-amd64/jre/bin/java but is not found in the runtime model MD5:33135f5a1fb45f5dff915ec1193c0dc7. Full command: /bin/bash -c /usr/bin/git clone https://github.com/huntergregal/mimipenguin.git

Rule Default - alert on suspicious runtime behavior

Response

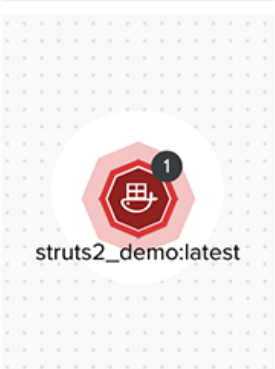
Show model

Report

Relearn

Collections

Radar view of incident



Examples

Aqua





aqua



Dashboard

Images

Containers

Services

Audit

ADMINISTRATION

Policies

Secrets

Enforcers

Compliance

System

Images

Show repositories from:

All Registries

Show repositories with:

All

Filter repositories by name:



SCAN QUEUE >



HOST IMAGES



+ ADD IMAGES

<input type="checkbox"/> Repository ^	Security Issues	Image Profile	Disallowed	Registry
> alpine	<div><div></div></div>	None	1 / 6	Host Images
> alpine	<div><div></div></div>	None	0 / 1	k8s.gcr.io
> alpine/postgres	<div><div></div></div>	None	0 / 1	jfrog2
> ashex/pokemongo-map	<div><div></div></div>	None	0 / 1	Docker Hub
> busybox	<div><div></div></div>	None	0 / 1	k8s.gcr.io
> centos	<div><div></div></div>	None	0 / 1	Host Images
> confluentinc/cp-zookeeper	<div><div></div></div>	None	0 / 1	Docker Hub
> golang	<div><div></div></div>	None	0 / 1	Host Images
> jboss/wildfly	<div><div></div></div>	None	0 / 1	k8s.gcr.io
> mongo	<div><div></div></div>	mongo-host-images	1 / 3	Host Images
> mongo	<div><div></div></div>	None	0 / 1	k8s.gcr.io
> mosho	<div><div></div></div>	None	0 / 1	Host Images
> mymongo	<div><div></div></div>	None	0 / 1	Host Images
> nginx	<div><div></div></div>	Nginx	0 / 9	Host Images

[Back to Dashboard](#)
[Status](#)
[Changes](#)
[Build Now](#)
[Build scheduled](#)
[Configure](#)
[Full Stage View](#)
[Rename](#)
[Pipeline Syntax](#)


Pipeline pipeline






[add description](#)
[Disable Project](#)



 [Last Successful Artifacts](#)
 [scanout.html](#) 20.52 KB [view](#)


 [Recent Changes](#)

Stage View

 **Build History**
[trend](#)

	#5	Jun 8, 2018 10:44 AM
	#4	Jun 7, 2018 11:08 AM
	#3	Jun 7, 2018 11:07 AM
	#2	Jun 7, 2018 11:05 AM
	#1	Jun 7, 2018 8:48 AM

 [RSS for all](#)
 [RSS for failures](#)

				Build	Aqua Scanner	Integration Tests	Push Image	Deploy
Average stage times: (Average full run time: ~16s)				473ms	8s	500ms	483ms	464ms
#5	Jun 08 13:44	No Changes		429ms	9s	434ms	382ms	408ms
#4	Jun 07 14:08	No Changes		500ms	11s	638ms	609ms	586ms
#3	Jun 07 14:07	No Changes		437ms	8s	475ms	486ms	449ms

CIS Benchmarks

Docker Hosts

Kubernetes Nodes

Docker CIS



HOST ^

LAST CHECK

FAIL

WARN

PASS

INFO

devAJcos14b377-

vm0.vx5foawd15wetkxf0dpxscxowmf.ax.internal.cloudapp.net.devAJcos14b377-vm0

2018-09-14 | 10:45:07 AM

44

45

17

0

> 1. Host Configuration

10

3

0

0

> 2. Docker daemon configuration

9

2

7

0

> 3. Docker daemon configuration files

8

6

6

0

3.1

Ensure that docker.service file ownership is set to root:root (Scored)

Step 1: Find out the file location: `systemctl show -p FragmentPath docker.service` Step 2: If the file does not exist, this recommendation is not applicable. If the file exists, execute the below command with the correct file path to set the ownership and group ownership for the file to root . For example, `chown root:root /usr/lib/systemd/system/docker.service`

pass

3.2

Ensure that docker.service file permissions are set to 644 or more restrictive (Scored)

Step 1: Find out the file location: `systemctl show -p FragmentPath docker.service` Step 2: If the file does not exist, this recommendation is not applicable. If the file exists, execute the below command with the correct file path to set the file permissions to 644 . For example, `chmod 644 /usr/lib/systemd/system/docker.service`

pass

Docker CIS

Failed Warn Pass

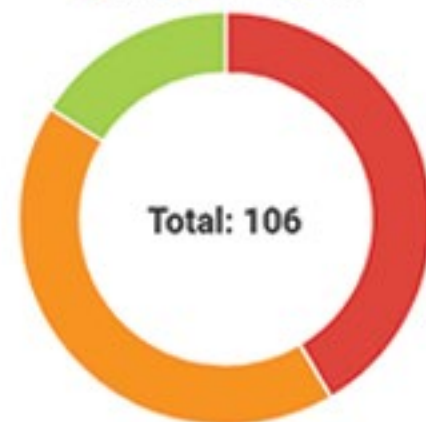




Image Profiles > MongoDB

* Name

MongoDB

Description

MongoDB document databases provide high availability and easy scalability.

Enforcement
Mode

Enforce

Audit Only

Read-Only Directories and Files



Allowed Executables



Container Engine Controls Linux only



The following controls will be enforced with any container execution. Note: these controls will also be enforced on audit-only hosts.

☒ Read-only root filesystem ⓘ

☒ No new privileges ⓘ

Seccomp profile:

Enter seccomp profile here...

Available Profile Controls

To add security controls to the image profile, click the + button or drag and drop the control to the profile area.

Network



Blacklisted Executables



Identity Inside The Container



Drift Prevention



Volumes



Limits



Environment Variables



Restricted Volumes



Allowed System Calls



Container Firewall Policies

Name	Description	Update Time	Author
Default Firewall Policy	Network Firewall Default Policy	2017-01-30 02:39:37 PM	system
block inbound		2018-07-02 07:00:14 PM	administrator
no-google		2018-08-23 04:19:15 PM	administrator

Container Firewall Policies > default

* Name: default

Description: Network Firewall Default Policy

Outbound Network Rules

Inbound Network Rules

Port Range

e.g. "80", "0-65535"

Destination

IP Address / CIDR

e.g. "190.1.2.3/12"

Allow

Deny

Priority

Destination IP/CIDR

Port Range

Allow/Deny

1

Anywhere

0-65535

Allow

Deny

Save Changes

Cancel

Apply What You Have Learned Today

- Next week you should:
 - Identify a team using a container within your organization
- In the first three months following this presentation you should:
 - Identify a tool that you want to use to test container security
 - Work to define a process to integrate container security into the CI/CD
- Within six months you should:
 - Rollout container security to the team in the CI/CD process
 - Continue the rollout to include other projects and