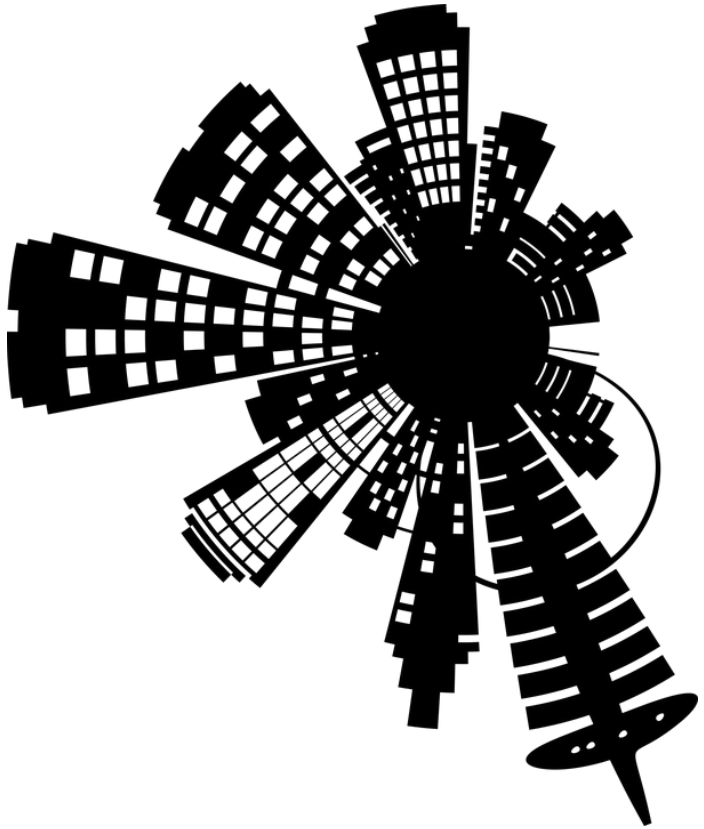
SACON International 2017

India | Bangalore | November 10 – 11 | Hotel Lalit Ashok



Integrating Container Vulnerability Management into DevOps

Richard Bussiere
Tenable
Technical Director

Agenda

- ✓ What's the Security Risk Introduced through Containers?
- ✓ What can we do about it?
- ✓ Short Demo
- ✓ Conclusions

Whack a Mole??

How can you understand the vulnerabilities & risk dynamic assets expose you to when the asset is here now then gone?

Can you answer these questions?

Every organization, no matter how large or small,
should be able to answer these **three fundamental questions** at all times:

How Secure Are We?

How Exposed Are We?

How Do We Proactively Reduce Our Exposure?

Measuring Cyber Exposure Leverages Vulnerability Management

Live Discovery

Continuous Visibility

Prioritize Exposure

Communicate Cyber Risk

Cyber Exposure Metric

Live Discovery of every modern asset across any computing environment

Continuous Visibility into where an asset is secure, or exposed, and to what extent

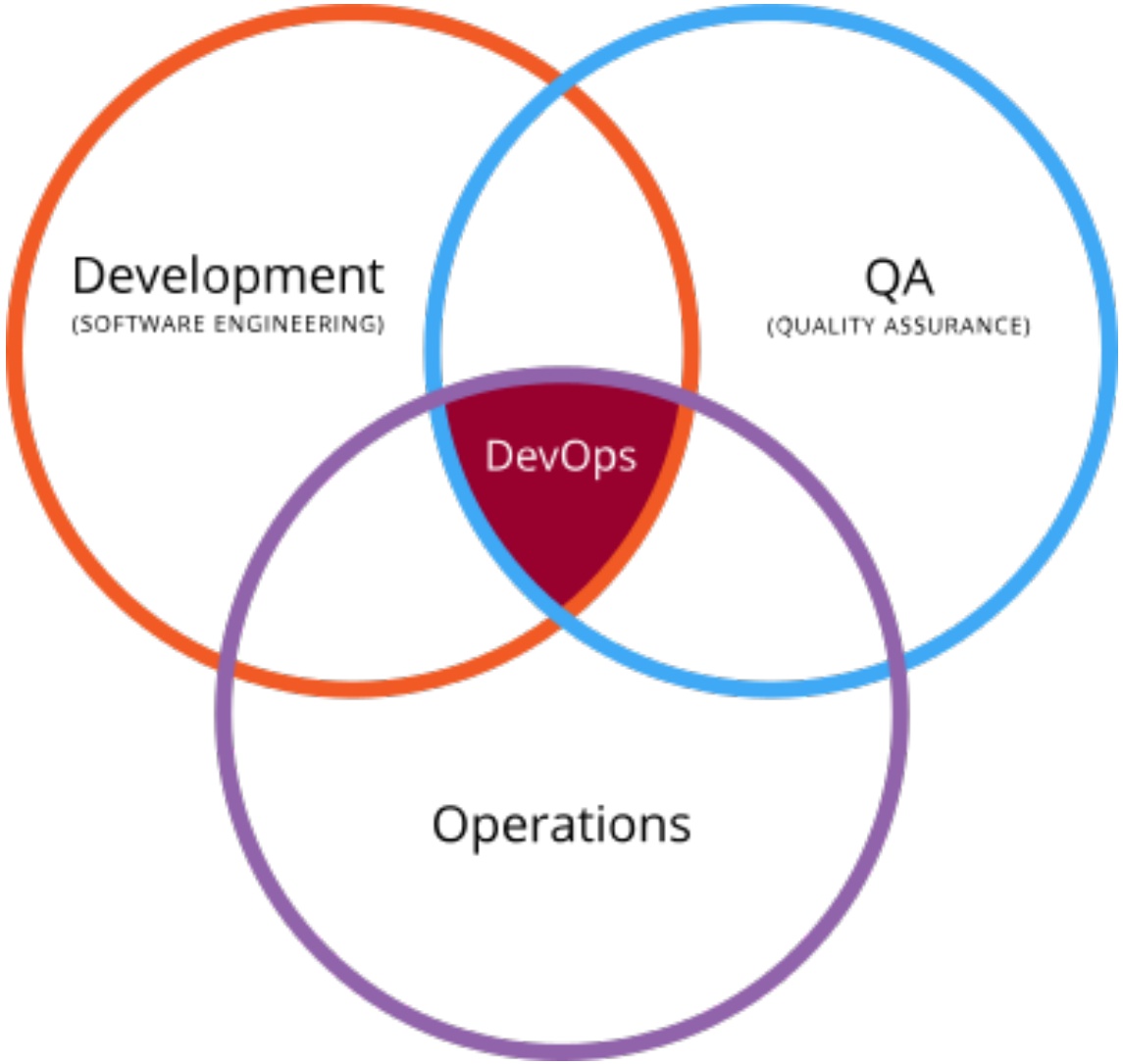
Add context to the exposure to prioritize and select the appropriate remediation technique

Accurately represent and communicate cyber risk to the business – in business terms

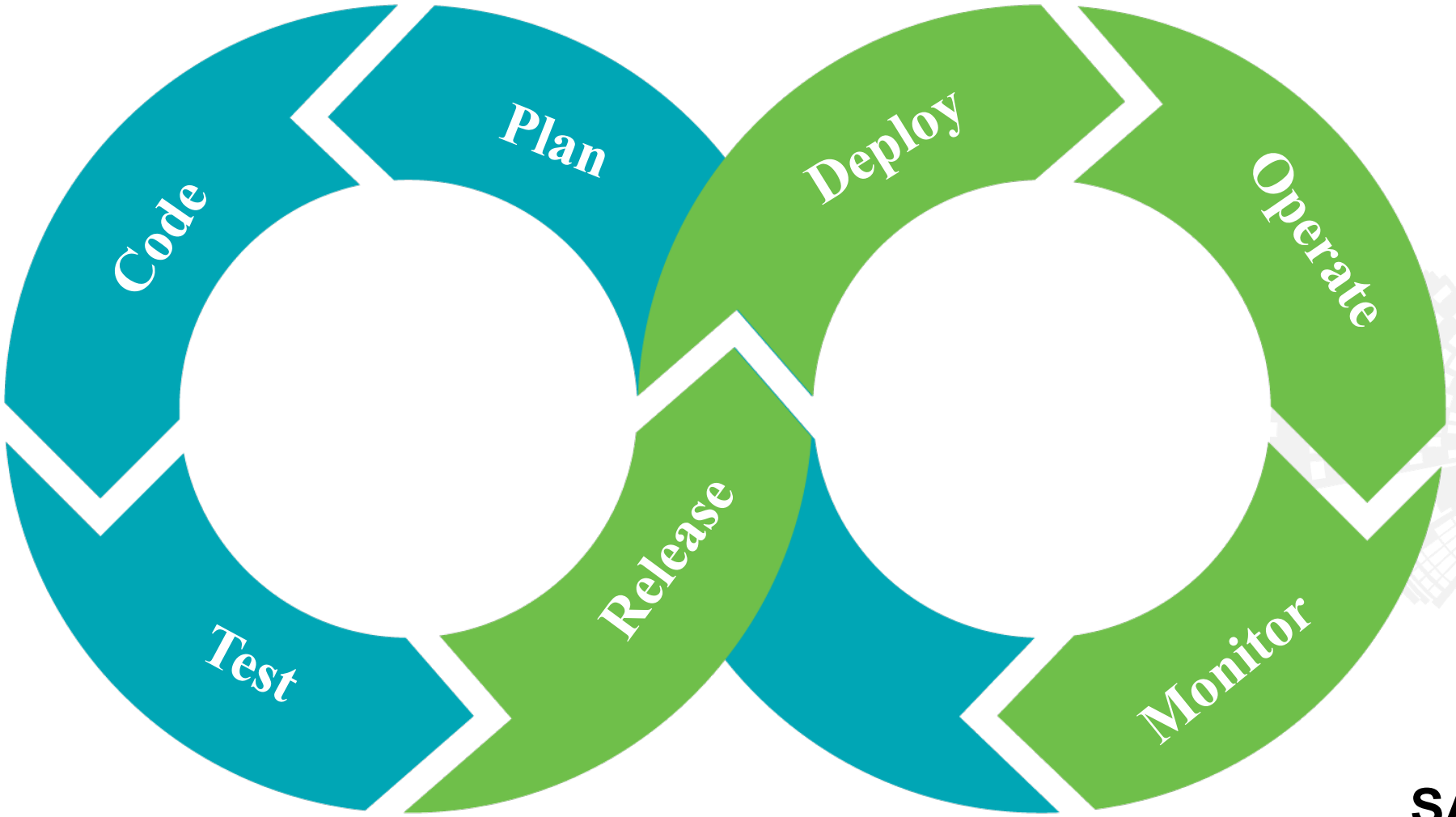
Apply Cyber Exposure data as a key risk metric for strategic decision support


SHARMAN
DEV
SHARMAN
OPS

Intersecting 3 Domains



Agile = Continuous Change



DevOps & Security - Disconnected?

Asked two different CISOs of two different major Indian telcos "What's your container strategy"?

- Answer: "What's a container?"

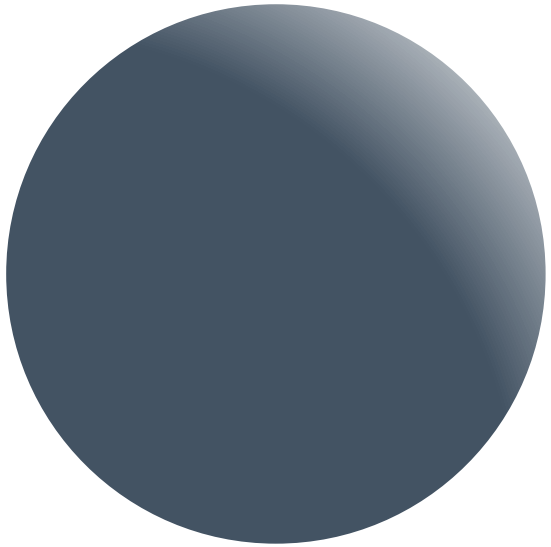
Singapore

- Considering using DevOps in the near future…
- Most not sure if this stuff is actually present in their environments

Can security keep up with the pace?

DevOps is driving changes in IT architecture

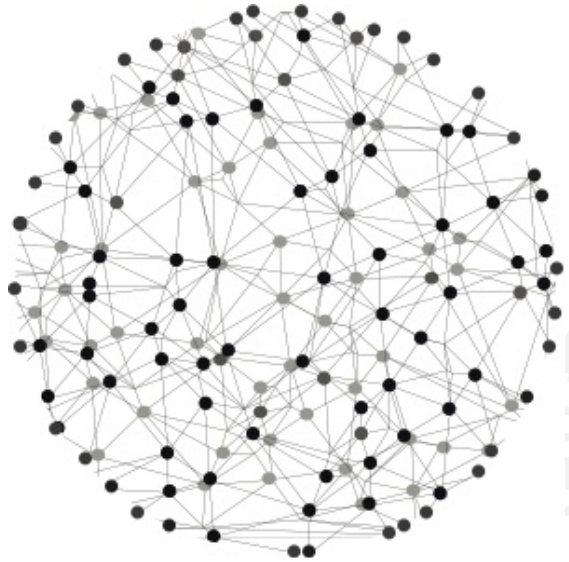
Monolithic



Built as a **single, self-contained** unit

Components are **interconnected** and **interdependent**

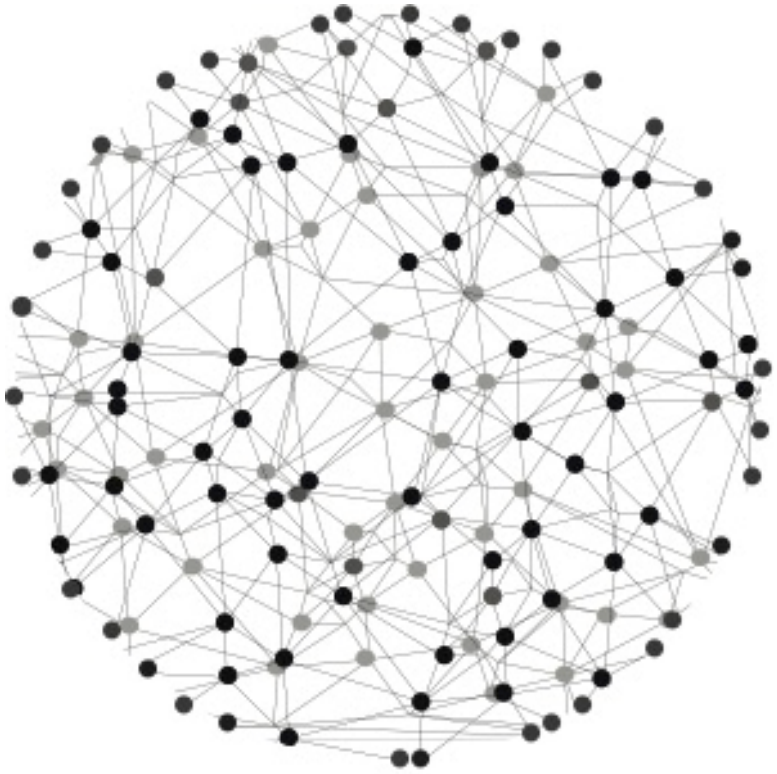
Microservices



Built as a **suite of modular** services

Components are **loosely coupled** and **highly cohesive**

Application containers enable infrastructure modernization with microservices



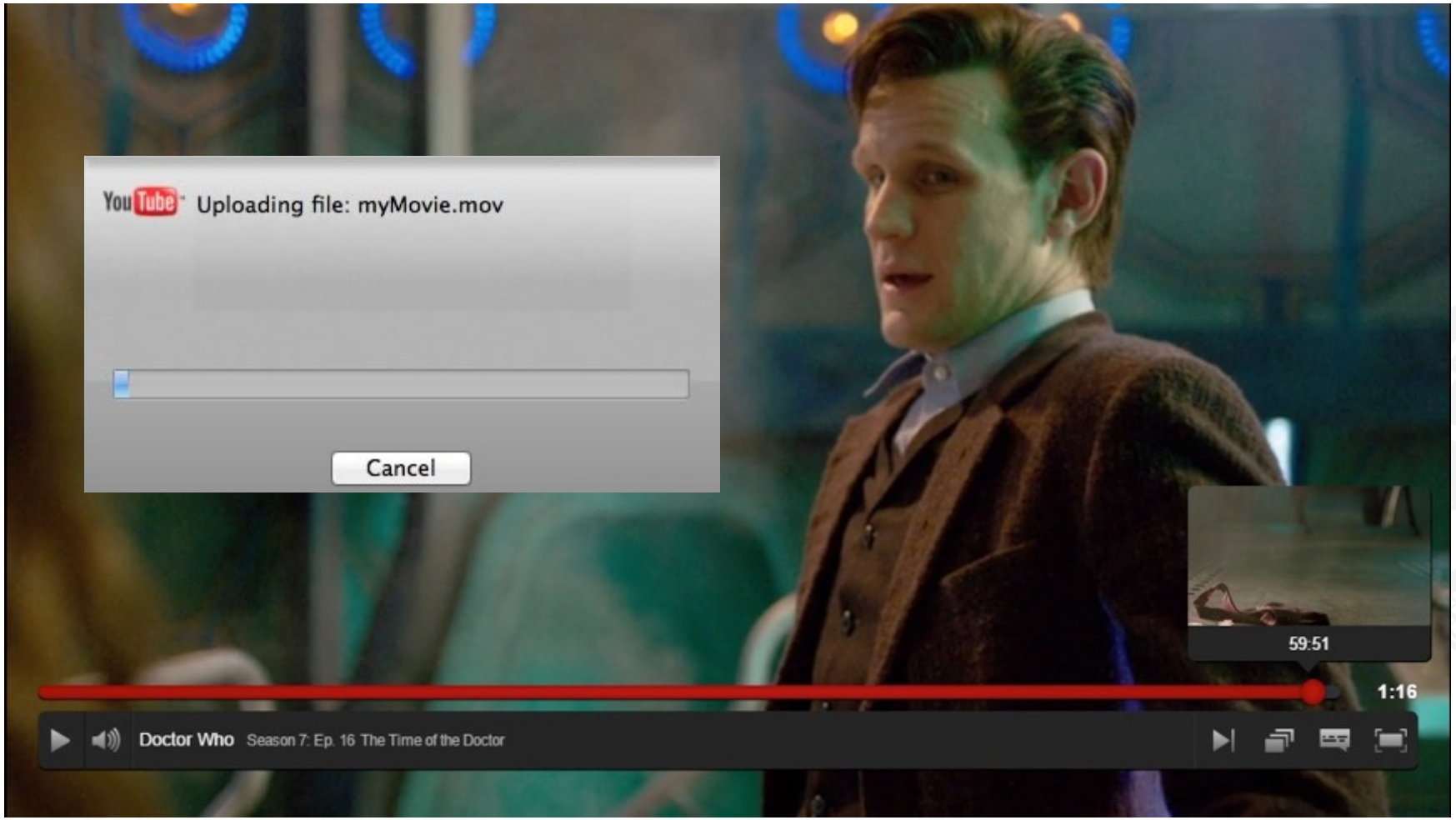
Each microservice is hosted in a container and connected via APIs

Containers encapsulate a lightweight runtime environment for the application

Microservices on containers provide:

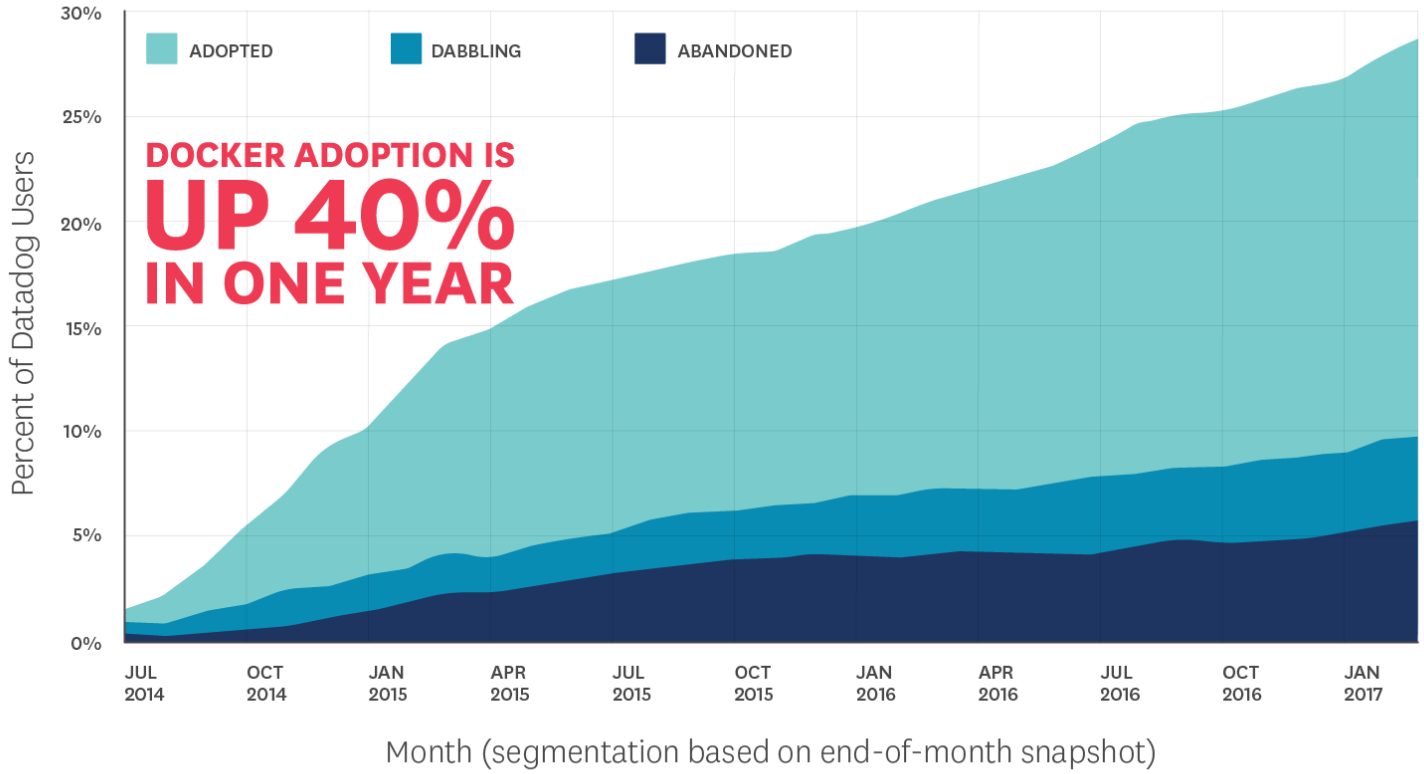
- Faster development and deployment velocity
- Greater scalability to quickly create and destroy
- Increased operational efficiency and responsiveness

YouTube example: microservices and containers



Application containers are exploding in adoption…

Docker Adoption[1]



500,000+

Dockerized apps in Docker Hub[2]

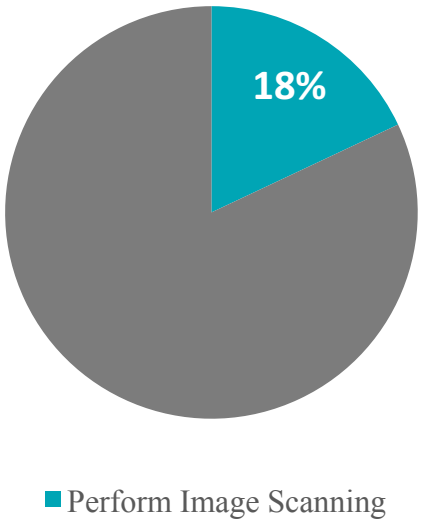
8 Billion+

Docker Container Downloads[2]

Sources:
1) Datadog, 2017
2) Docker, 2017

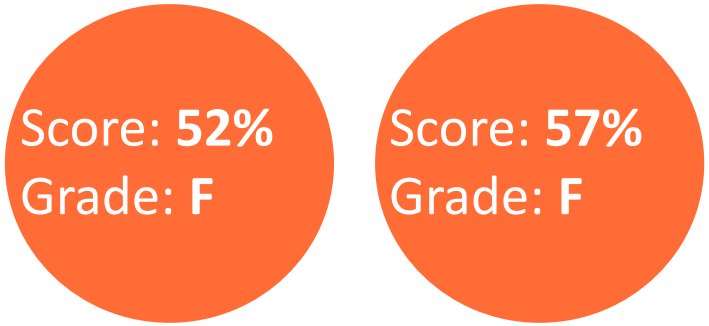
Major Cyber Exposure gap

Of organizations with containers in production[1]

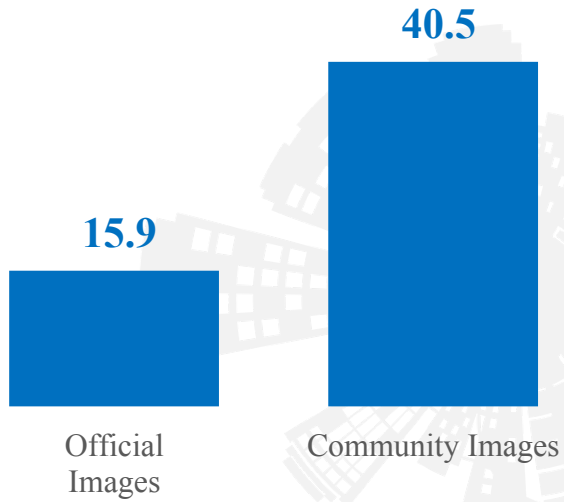


Risk Assessment Index[2]

Organization's ability to assess cybersecurity risks



Average number of vulnerabilities in Docker Hub[3]



Sources:
1) Anchore, "Snapshot of the Container Ecosystem," 2017
2) Tenable, "2017 Global Cybersecurity Assurance Report Card," 2017
3) Tenable, "Sourcing Container Images from Docker Hosts," 2017

Modern applications raise the stakes with risk

"Modern applications are **largely assembled**, not developed, and developers often download and use **known vulnerable open-source** components and frameworks."

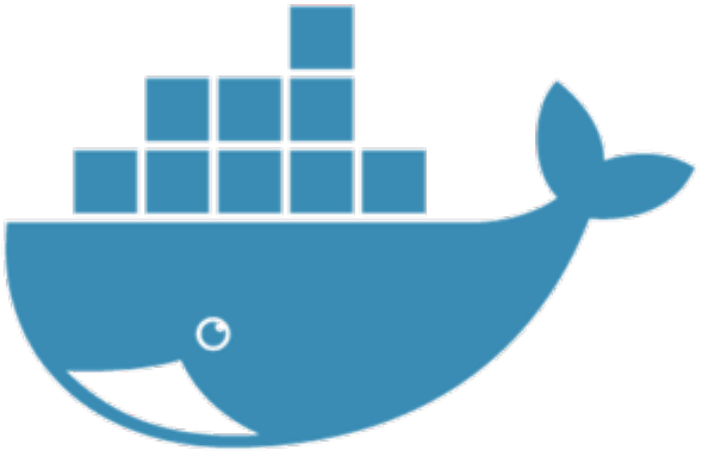
-Gartner

And organizations have taken notice

"Even if Docker certifies an app as being safe and effective, I'm not **risking $11 billion** on Docker telling me it's safe. We need **extra assurance** and to prove it to ourselves."

– James Ford, Chief Strategic Architect, ADP

Sharing Images: Docker Hub … Safe?



nginx	official	5.7K STARS	10M+ PULLS	DETAILS
redis	official	3.6K STARS	10M+ PULLS	DETAILS
busybox	official	969 STARS	10M+ PULLS	DETAILS
ubuntu	official	5.8K STARS	10M+ PULLS	DETAILS
registry	official	1.4K STARS	10M+ PULLS	DETAILS
alpine	official	2.0K STARS	10M+ PULLS	DETAILS
mysql	official	4.1K STARS	10M+ PULLS	DETAILS
mongo	official	3.1K STARS	10M+ PULLS	DETAILS

Traditional security approaches do not work with containers

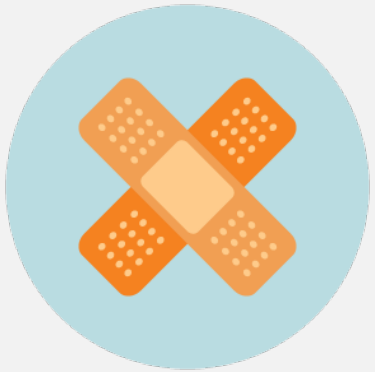
1

Short Lifespan

2

Inability to Use Traditional VM Techniques

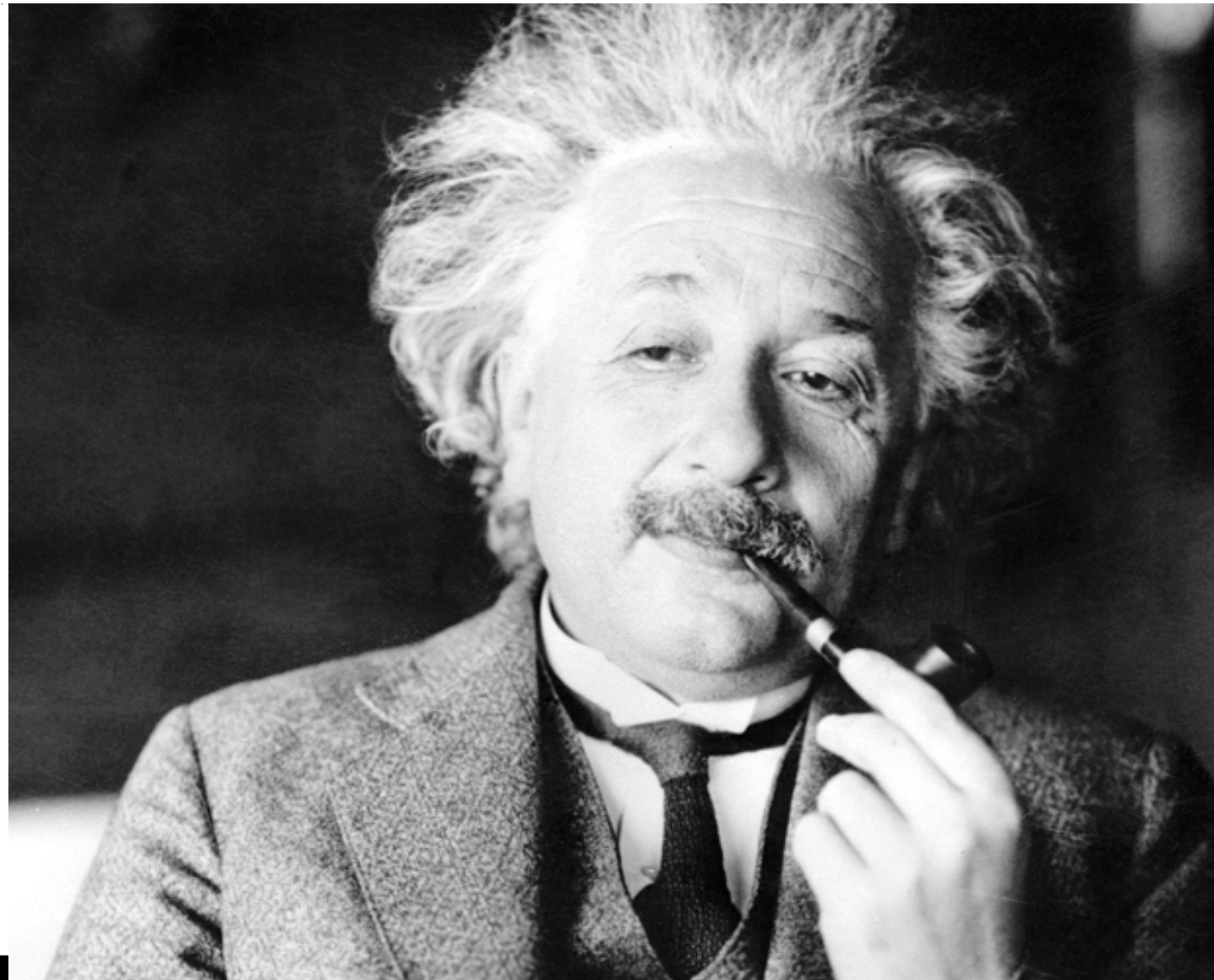
3



Inability to Remediate Vulnerabilities

Think differently about protecting modern assets

Insanity: *Doing the same thing over and over again and expecting a different result*

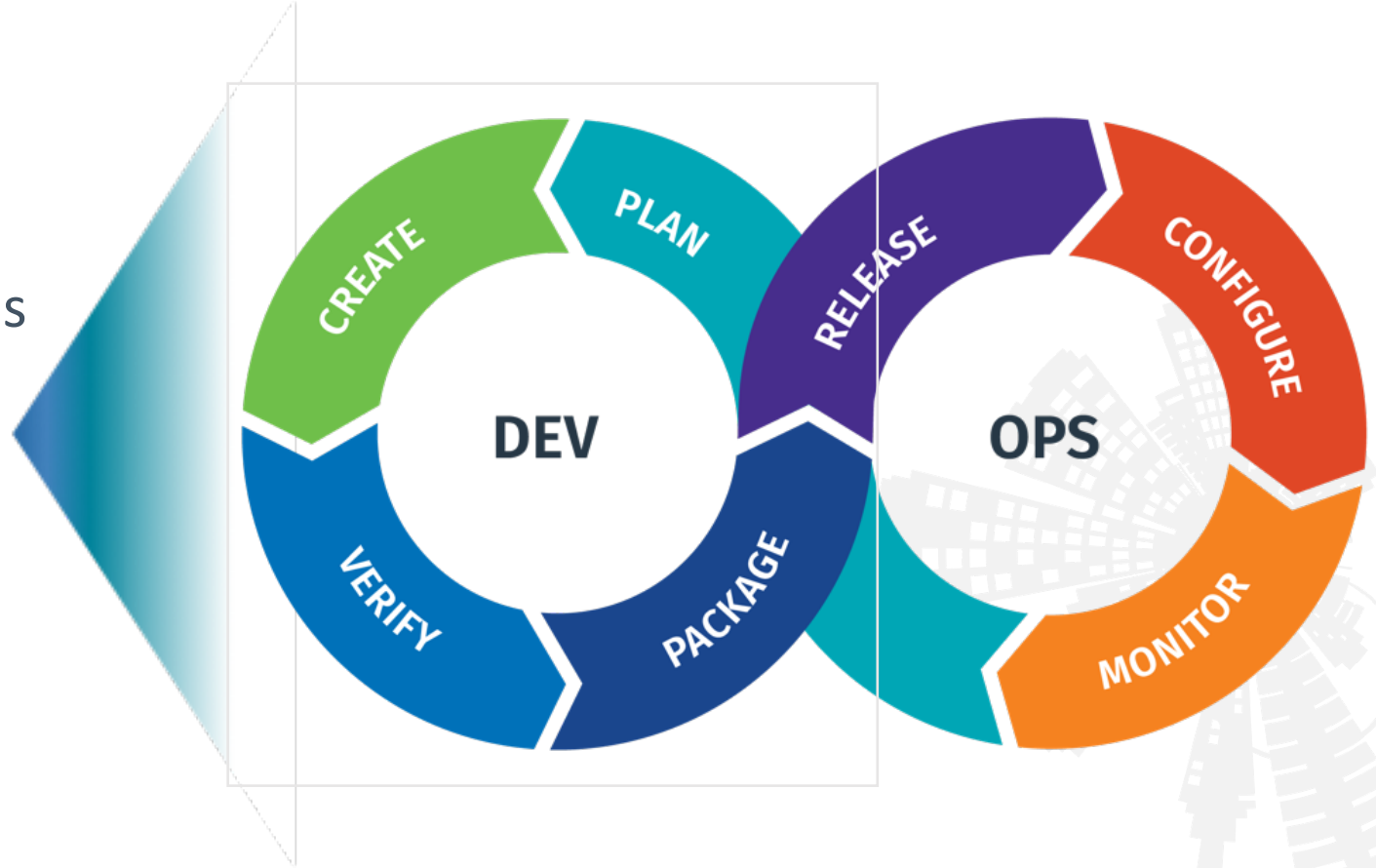


Prevent container vulnerabilities by securing images prior to deployment

Integrate container security into the DevOps toolchain

Identify and remediate vulnerabilities before they are exploitable

Ensure all container images are secure and compliant before production



What does this mean to Security and DevOps?

Enterprise Security

Ensure containers are part of a holistic Cyber Exposure program

Reduce risk across a growing modern attack surface

Identify and remediate vulnerabilities as early in the SDLC as possible

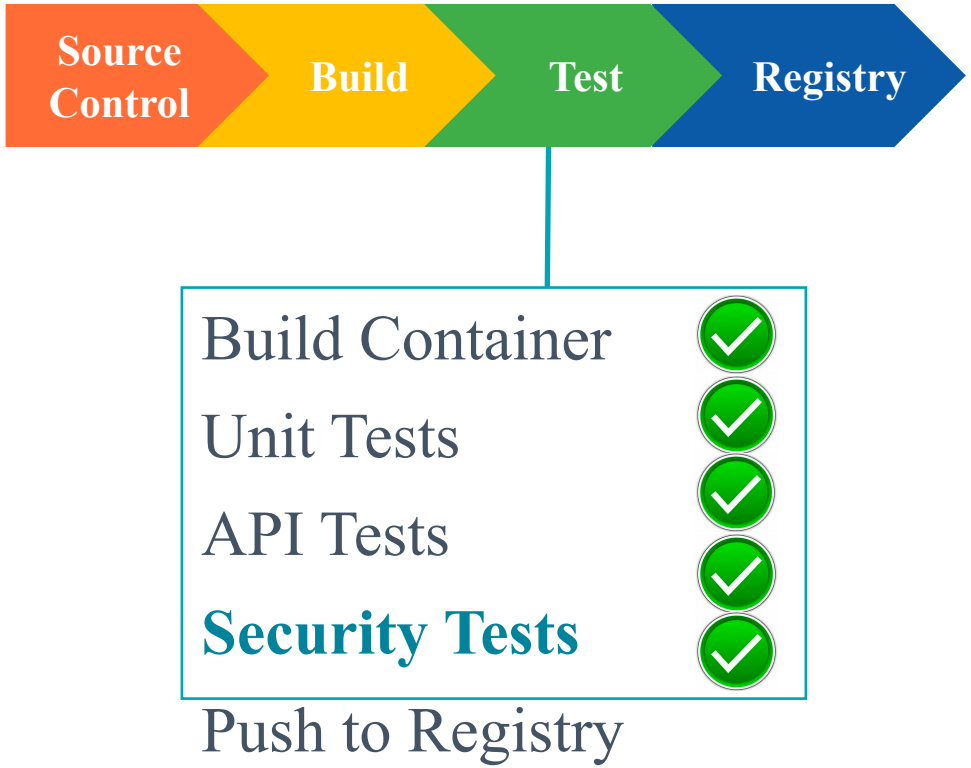
DevOps

Deliver quality, well-tested code at high velocity and scale

Integrate security into the DevOps toolchain, without sacrificing speed

Identify and remediate vulnerabilities as early in the SDLC as possible

“Shift left” with security in the software development lifecycle

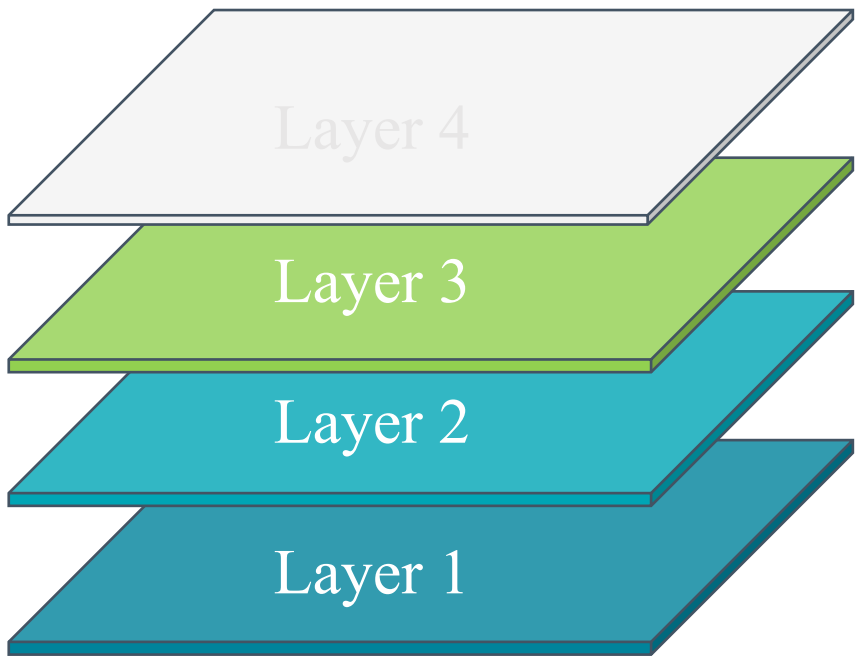


Perform rapid vulnerability and malware detection testing within the DevOps toolchain

Out of the box integrations with CI/CD build systems

- Jenkins, Bamboo, Shippable, Travis CI and more
- Import across container images registries
- Fully documented RESTful API for custom integrations

Know what is inside a container before deployment



Produce a detailed bill of materials covering all layers and components

- Libraries / binaries
- Configuration files
- Dependencies
- Applications

“At-a-glance visibility” into both container image inventory and security

Deep assessment of container images

Assessment of container images by layer

Detect the presence of malware in the layers

Apply layer hierarchy intelligence to understand when vulnerabilities are mitigated in higher layers

Continuously protect containers from newly identified threats

Continuously monitor in production containers for new vulnerabilities

Automatically re-test as new vulnerabilities are identified

Respond to newly emerging risks to encsure ontinuous protection

Policy - Ensure containers in production are compliant with policy

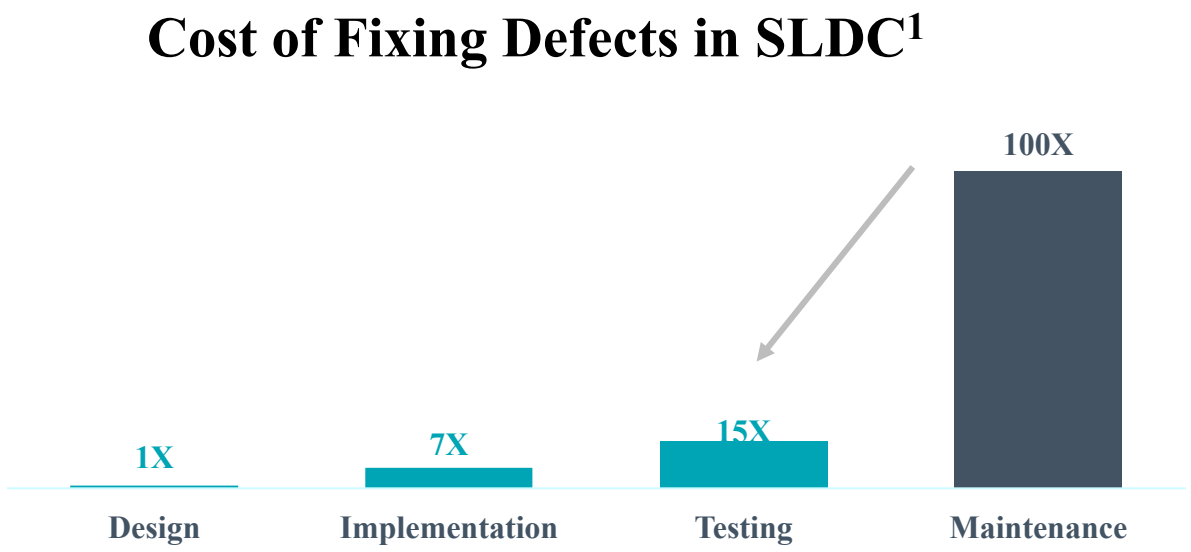
Write container security policies that align to security goals and objectives

Notify developers immediately when container images exceed organization risk thresholds

Allow developers to take direct action with specific remediation advice

Reduce costs by catching container vulnerabilities earlier

Reduce Costs

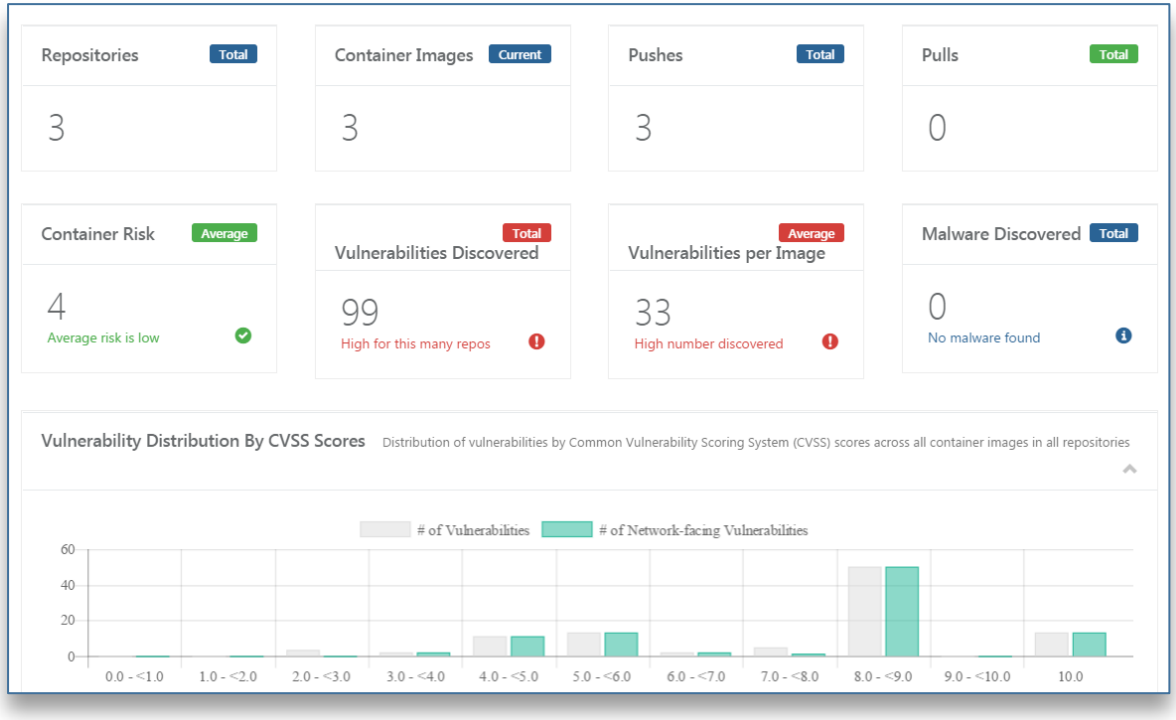


Reduce costs by >85%
by remediating vulnerabilities before deployment

Reduce false positives
and ensure developers do not waste time fixing non-vulns

1) Source: Computer Business Review, "The cost of fixing bugs throughout the SDLC," March 2017

Eliminate Blind Spots

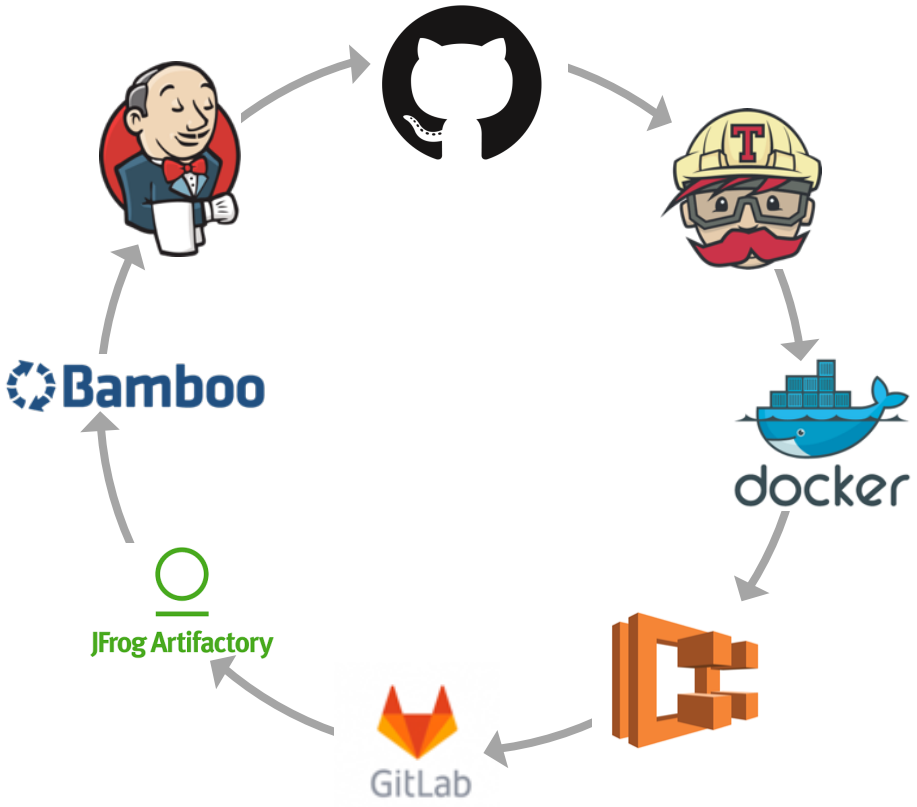


Comprehensive insight into:

- Container image inventory
- Summary of vulnerabilities and malware
- Distribution of vulnerabilities by CVSS score and risk level

Avoid slowing down existing DevOps processes and workflows

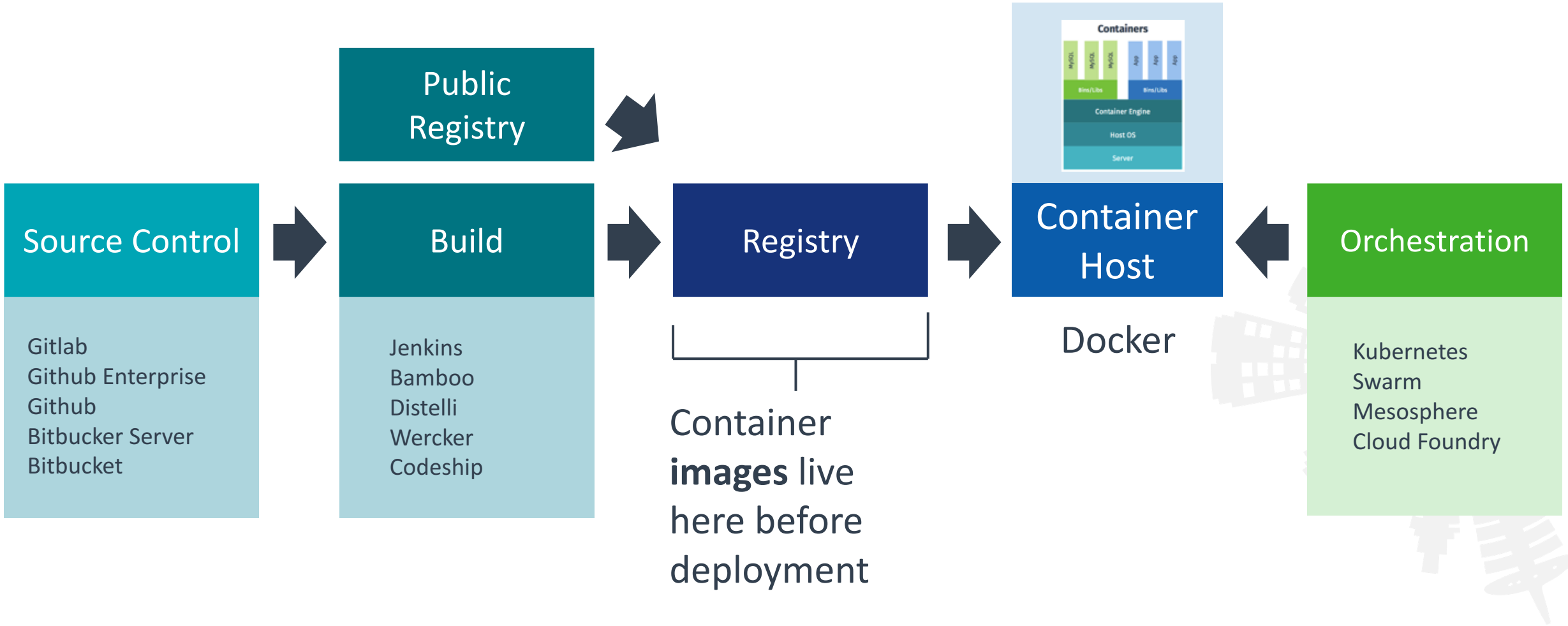
Accelerate DevOps



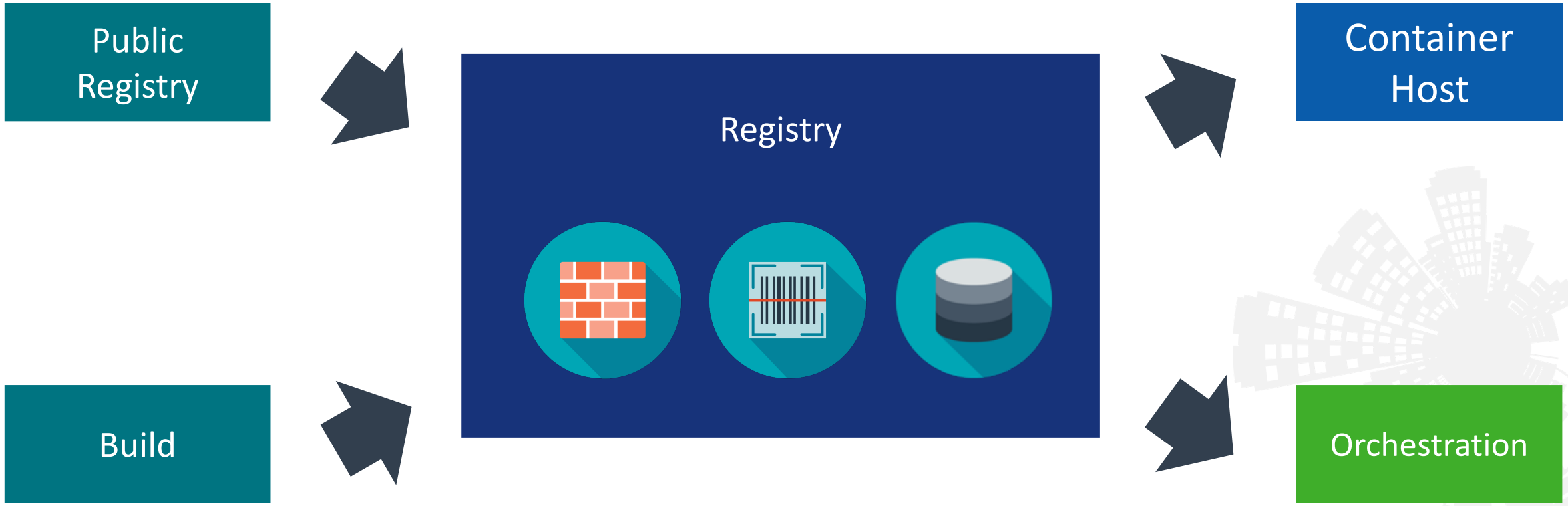
<30 second security test
within the DevOps toolchain

Out of the box integration
with common CI/CD systems and container registries

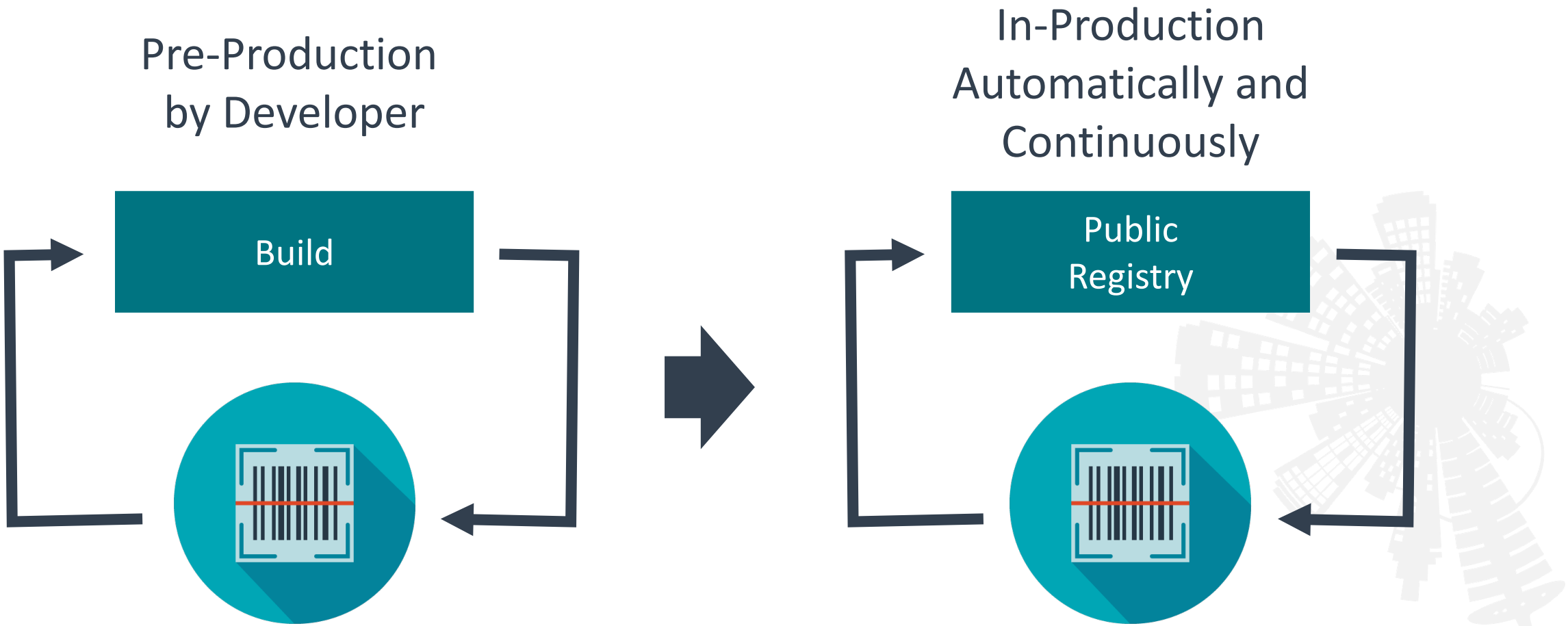
The Entire Process Laid Out…



Injecting Security into DevOps Workflow



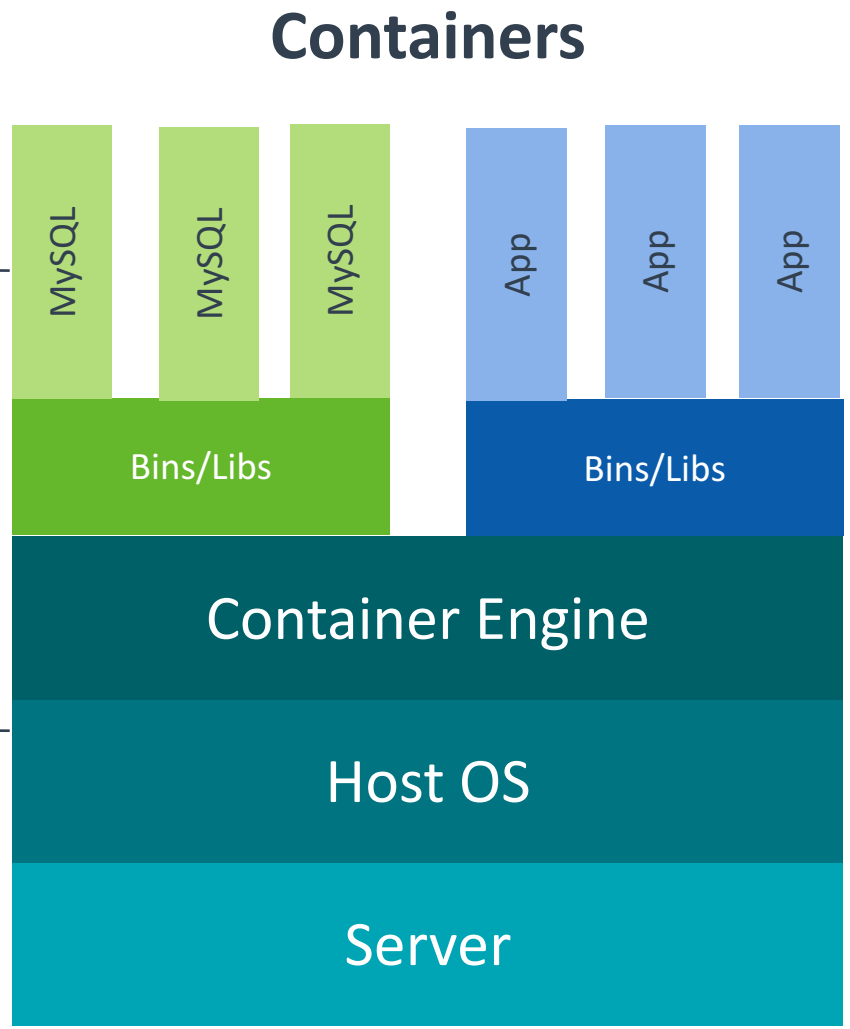
When to Scan Container Images?



Vulnerability Scanning with Modern Stacks

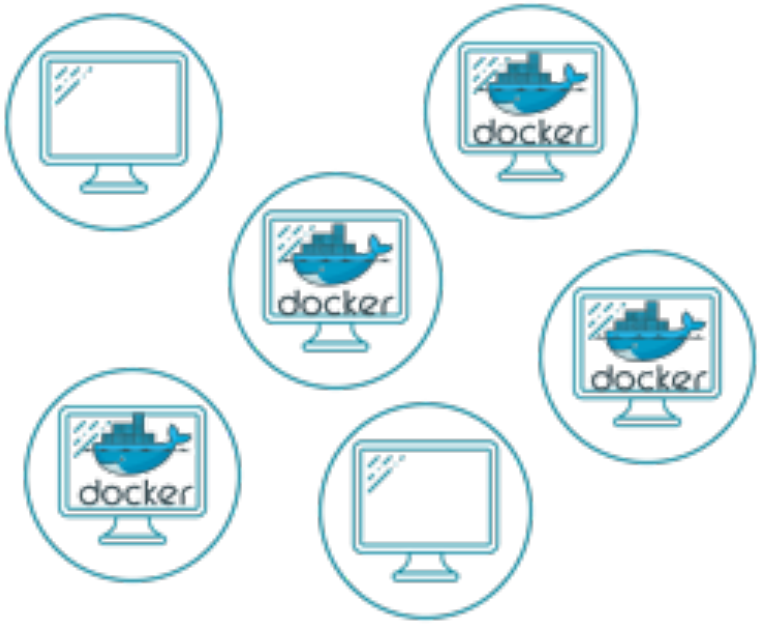
Scan for vulns by scanning container images

Scan for vulns using "traditional" approaches



External Web App Scanning

Identify running container hosts…



tenable.io™ Vulnerability Management

SecurityCenter SC™

Nessus N™

INFO **Docker Service Detection**

Description

The Docker service is running on the remote host. Docker is an open-source project that automates the deployment of applications inside software containers.

See Also

https://www.docker.com/

Output

```
The following containers were detected running on the remote Docker host:

Name  :/centos7.1
Image :centos

ID    :75621b2f15e4c909ba8860b88761d54ab98c6cbd1bf70414b5647c5719060759
Ports :n/a

Name  :/centos_7.2.1511
Image :centos
```

…and harden hosts with the CIS Docker benchmark

CIS Center for Internet Security®

- Configuration
- Patching
- Permissions
- Access
- Sprawl

WARNING	6.4 Backup container data
WARNING	6.5 Use a centralized and remote log collection service
WARNING	6.6 Avoid image sprawl
PASSED	1.2 Use the updated Linux Kernel
PASSED	1.5 Remove all non-essential services from the host - RPM
PASSED	1.5 Remove all non-essential services from the host - running processes
PASSED	1.5 Remove all non-essential services from the host - sockets
PASSED	1.6 Keep Docker up to date
PASSED	2.1 Do not use lxc execution driver
PASSED	2.4 Allow Docker to make changes to iptables
PASSED	2.5 Do not use insecure registries
PASSED	2.7 Do not use the aufs storage driver
PASSED	3.1 Verify that docker.service file ownership is set to root:root
PASSED	3.15 Verify that /etc/docker directory ownership is set to root:root

Try Tenable.io Container Security today

tenable.com/try-container

60 Day Fully Operational Trial for FREE!!


tenable™