RSAConference2017
Singapore | 26–28 July | Marina Bay Sands

POWER OF OPPORTUNITY

SESSION ID: GPS-F02B

Safety and Speed—How Tenable Runs Swift and Sure in a DevOps World

Dave Cole
Chief Product Officer
Tenable
@mediafishy

Agenda

- The Problem
- Hypothesis
- What We Did
- Results
- Key Takeaways

tenable

RSA Conference 2017
Singapore

The Problem

1. Playing catch-up

Many advantages for building new platform w/ the latest tech

Better scaling

Responsiveness

Flexibility

Increased development velocity

Easier integration

1. Playing catch-up (cont.)

New platforms benefit from all your learnings, but they don't inherit all of your work– the old features often times, have to be re-created.

Unless you delay launching until you have everything, you're under time pressure from day 1. **Speed is crucial.**

2. Speed, the natural adversary of safety

The faster you go, the harder it is to control the outcome

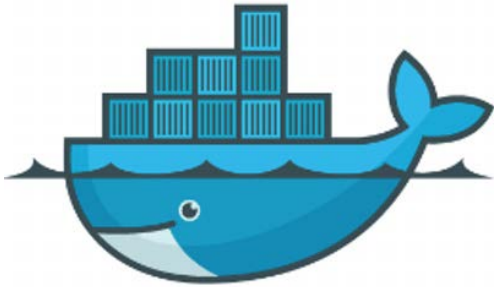
Especially true for security where even small lapses can introduce serious vulnerabilities

People are often skeptical of new platforms, let alone new vulnerability management platforms… with vulnerabilities!

3. Classic approach irrelevant

The new platform is based on Docker containers housing purpose-built micro services

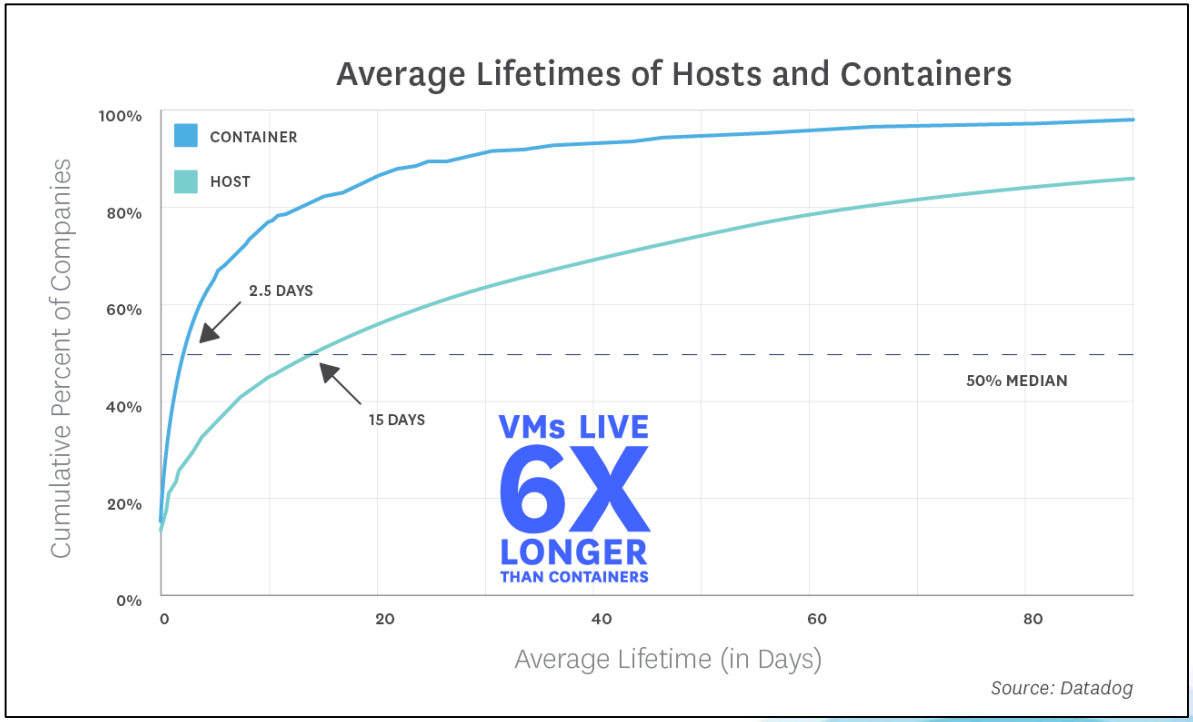
Using an agile approach with continuous integration & delivery (CI/CD), we can frequently update the platform



3. Classic approach irrelevant (cont.)

Containers are short-lived, average of 2.5 days.

Scans in production would be out of date before you act on them & patching makes little sense.



3. Classic approach irrelevant (cont.)

What about an agent in the container?

Still a slow scan & fix model. & heavy– container may not possess an OS, why would it have an agent?

RSA Conference 2017
Singapore

Hypothesis

Hypothesis

Security has to become part of the natural flow of the development pipeline for safe CI/CD.

To minimize the # of issues even an integrated assessment can handle, security must be ”baked in” to a disciplined design phase

Developers must be accountable for the security of their own code… & a dedicated person on their own team to help them.

RSA Conference 2017
Singapore

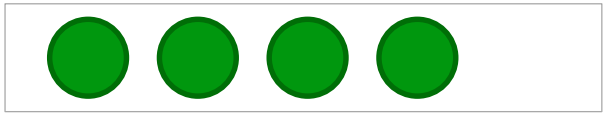
What We Did

Container Hardening

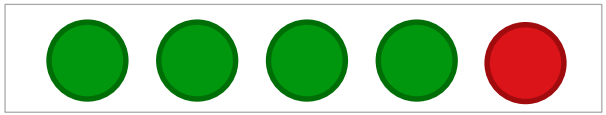
Start from known good – Docker base containers are hardened & actively maintained by the Ops team

Declared Ports on Container Images – additional ports are runtime are not accessible, blocked

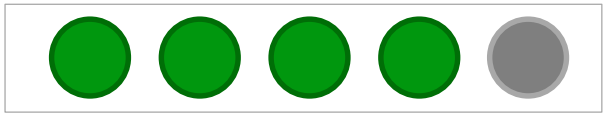
Healthy, Normal



Compromised, Add'l Port Open



Declared Ports Only; Blocked



Platform Hardening

- Configuration details loaded as a stream from a service at startup… instead of being stored as files on running machines
- Least-Privilege SELinux Policies on Servers
- Least-Privilege IAM Roles
- Deletes not allowed in AWS (via global IAM policy)
- Deep Session Validation (JWT on Backend Services)

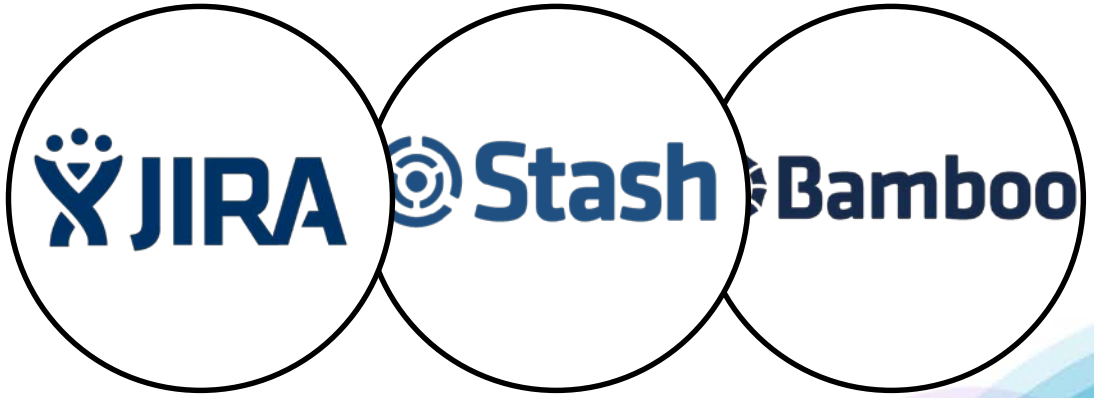
Designing for Safety & Speed

Created an explicit design phase w/ team–wide reviews

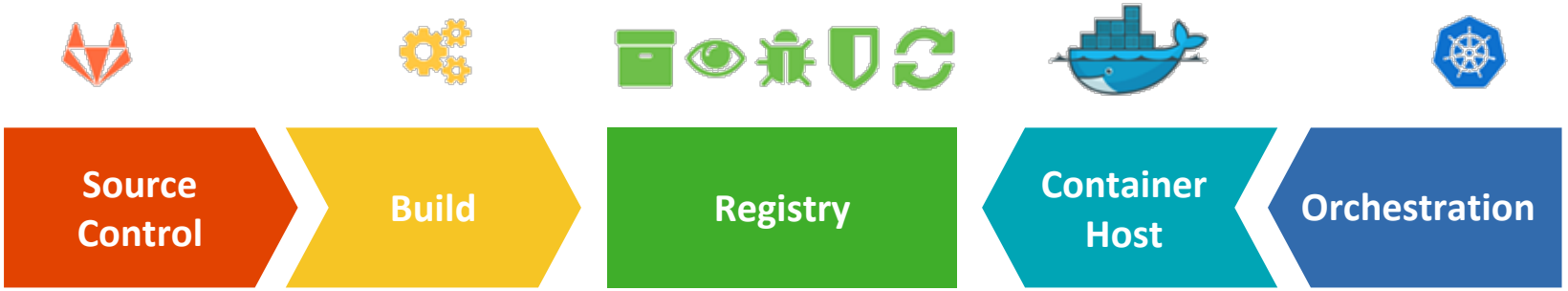
Properly “fund” design with the right people & time

Peer code reviews

End to end change tracking, starting from design (Jira) through commit (Stash) and build (Bamboo)



Security: a natural part of the pipeline



Build system integration (Bamboo) means container problems surface before production & in the same fashion as any other product defect

Scanning for vulnerabilities, malware & compliance happens inside a private registry at check-in & periodically thereafter

Nessus Agents used on the hosts themselves for periodic scanning

Making product security “native”

- Engineers must be accountable for their own code
- Accountability isn’t enough, someone has to own product security… and they can’t sit in the IT group
- A strong ops team is essential, but they have more to do than security
- We hired a seasoned security professional (former consultant, CISO & Developer) who reports into the VP of Engineering as a Sr. Director, Product Security

Pit stop: slowing down to speed up

- Amidst looming deadlines & urgent projects, we stopped nearly all feature development for a 2 week sprint
- We planned it for about 2 months
- We used the time to improve tooling, increase automation coverage, training & more
- Then we went straight back at it w/ true CI/CD

RSA Conference 2017
Singapore

Results

Results

Happier, more motivated engineers

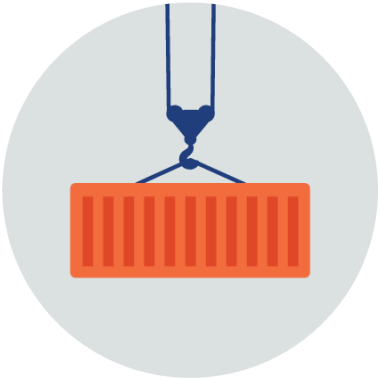
96.2% increase in amount of unique tests

20% drop in customer support tickets

0 known “escaped” security issues

Nice uptick in the # of releases

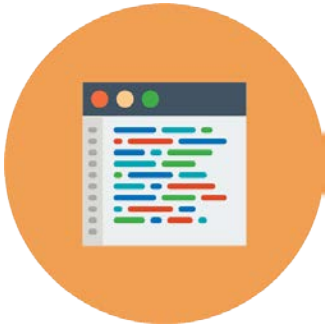
Key Takeaways



Hardening as essential as ever for both containers & platform

Safe CI/CD requires security pipeline integration

Key Takeaways Continued



Developers need to own the quality of their own code, ops can own platform health, prod sec needs to be native

Going fast, ironically requires going slower at the outset as you invest in process, integration & automation


tenable™