How "Shifting Left" with Secure DevOps Can Reduce Your Cyber Exposure

Corey Bodzin
VP of Product Operations, Tenable

Gene Kim
DevOps Pioneer, Author, Researcher and Entrepreneur

tenable

@RealGeneKim

Agenda

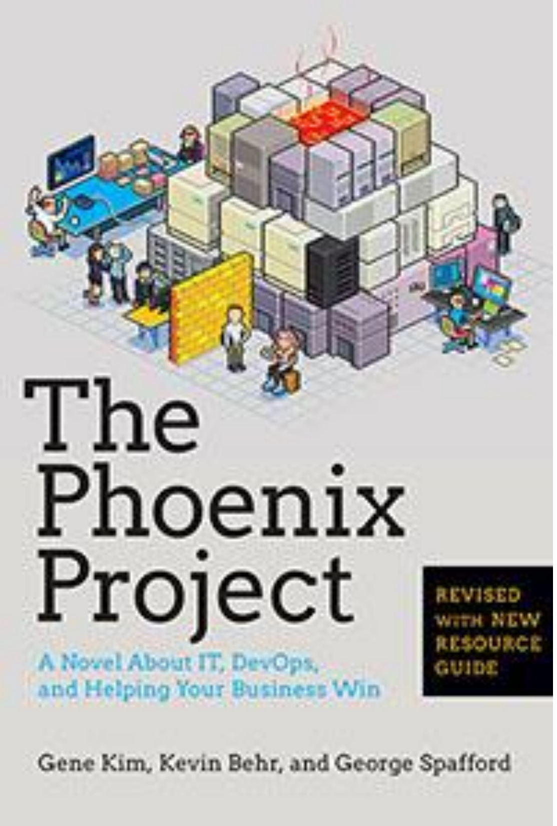
- The Downward Spiral
- DevOps Is Awesome for InfoSec
- Three Ways of Secure DevOps
- Secure DevOps Example: Containers
- Next Steps

Poll Question #1

To what extent do InfoSec and DevOps collaborate in your organization?

1. Rarely or never
2. Occasionally as issues emerge
3. Periodically on a monthly basis
4. Routinely on a weekly basis
5. Continuously as part of the same team

Phoenix Project (2013)

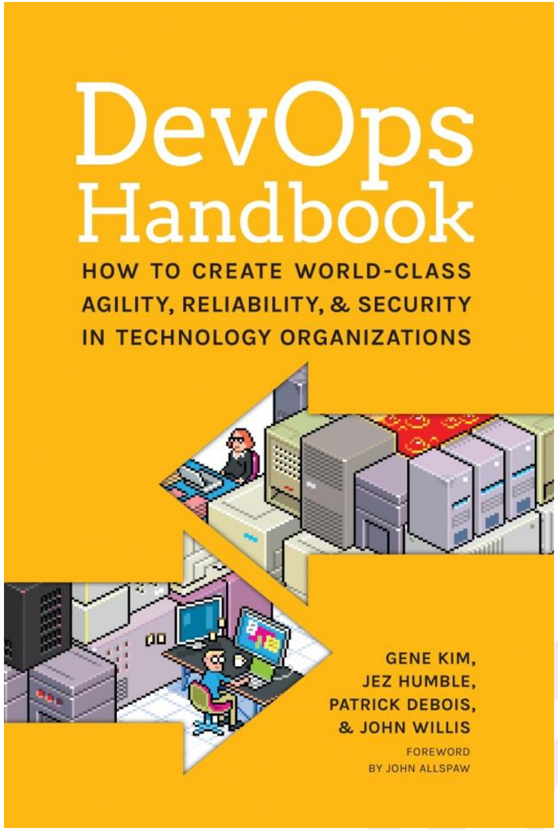


The Phoenix Project

A Novel About IT, DevOps, and Helping Your Business Win

REVISED WITH NEW RESOURCE GUIDE

Gene Kim, Kevin Behr, and George Spafford



DevOps Handbook

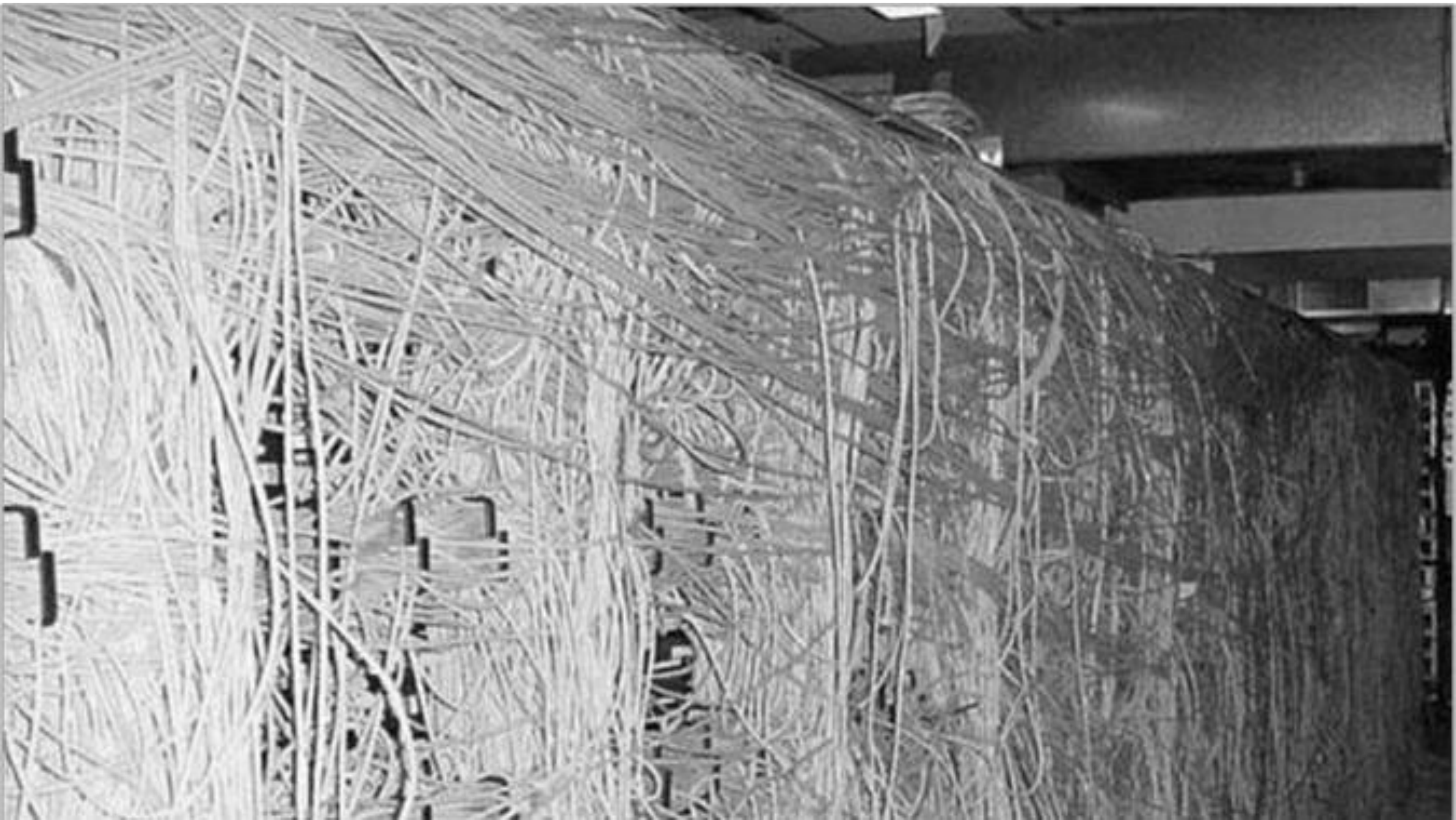
HOW TO CREATE WORLD-CLASS AGILITY, RELIABILITY, & SECURITY IN TECHNOLOGY ORGANIZATIONS

GENE KIM, JEZ HUMBLE, PATRICK DEBOIS, & JOHN WILLIS

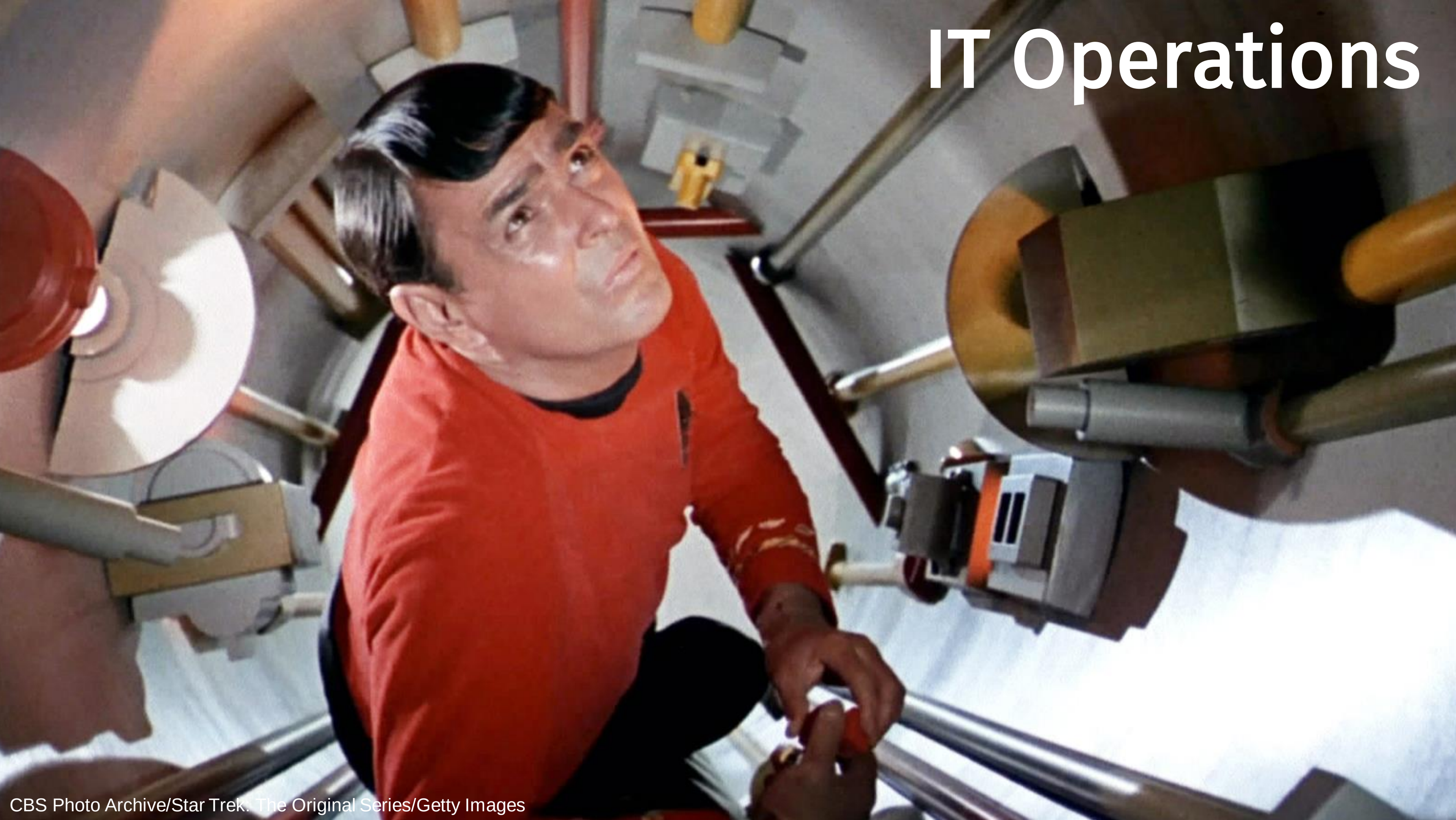
FOREWORD BY JOHN ALLSPAW

DevOps Handbook (2016)

The Downward Spiral



IT Operations



CBS Photo Archive/Star Trek: The Original Series/Getty Images

The Developers

The Product Managers

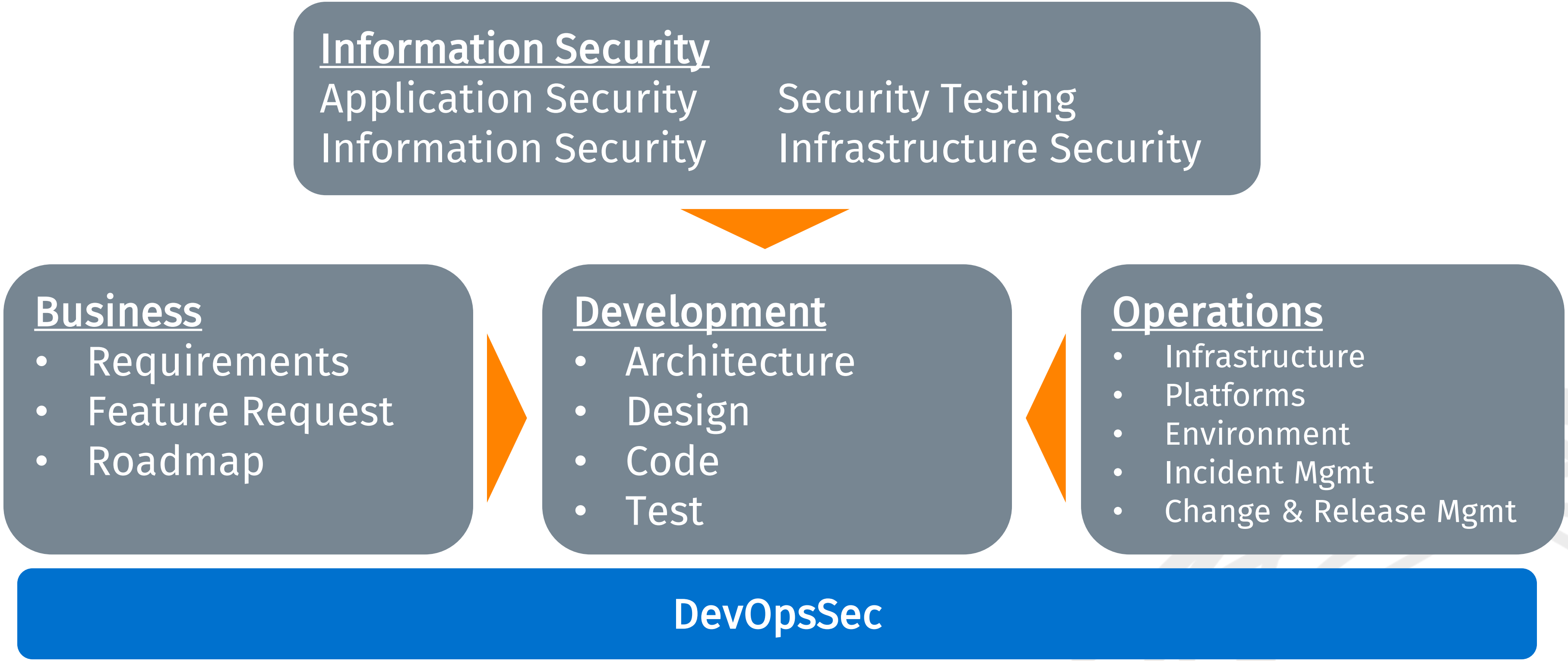
Source: Flickr: birdsandanchors

BIG COPS. SMALL TOWN. MODERATE VIOLENCE.
SIMON PEGG NICK FROST
HOT FUZZ
A NEW COMEDY FROM THE MAKERS OF
SHAUN OF THE DEAD
POLICE

“Hot Fuzz”: Rogue Pictures

DevOps Is Awesome For Infosec

Capital One: DevOpsSec



Information Security

Application Security

Information Security

Security Testing

Infrastructure Security

Business

- Requirements
- Feature Request
- Roadmap

Development

- Architecture
- Design
- Code
- Test

Operations

- Infrastructure
- Platforms
- Environment
- Incident Mgmt
- Change & Release Mgmt

DevOpsSec

Source: Tapabrata Pal, Capital One

The Business Value Of DevOps Is Even Higher Than We Thought

High Performers Are More Agile

46x

more frequent deployments

440x

faster lead times than their peers

tenable

Source: Puppet/DORA: 2017 State Of DevOps Report: https://puppet.com/resources/whitepaper/state-of-devops-report

High Performers Are More Reliable

5x

lower change failure rate

96x

faster mean time to recover (MTTR)

tenable™

Source: Puppet/DORA: 2017 State Of DevOps Report: https://puppet.com/resources/whitepaper/state-of-devops-report

High Performers Are More Secure And Controlled *

2x

less time spent remediating security issues

29%

more time spent on new work

tenable

Source: Puppet Labs 2016 State Of DevOps Report: https://puppet.com/resources/white-paper/2016-state-of-devops-report

@RealGeneKim

High Performers Win In The Marketplace

2x

more likely to exceed profitability, market share & productivity goals

2x

more likely to achieve organizational and mission goals, customer satisfaction, quantity & quality goals

tenable

Source: Puppet/DORA: 2017 State Of DevOps Report: https://puppet.com/resources/whitepaper/state-of-devops-report

High Performers Win In The Marketplace

2.2x

higher employee
Net Promoter Score

50%

higher market
capitalization growth
over 3 years*

tenable™

Source: Puppet Labs 2016 State Of DevOps Report: https://puppet.com/resources/white-paper/2016-state-of-devops-report

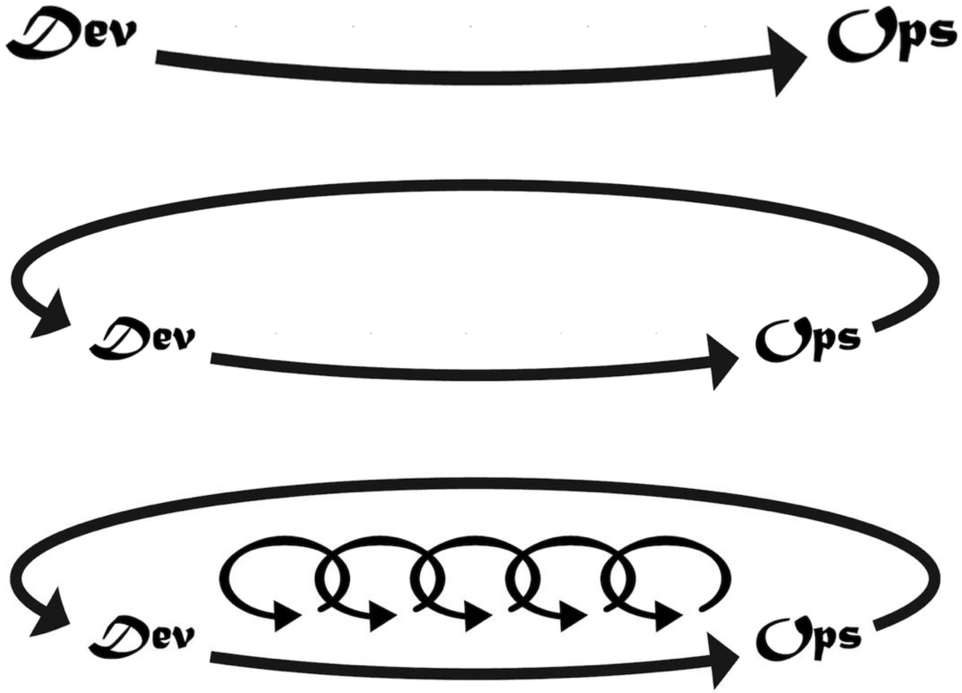
@RealGeneKim

The Opposite Of Technical Debt Is…

When we can safely, quickly, reliably, securely achieve all the goals, dreams and aspirations of our business…

tenable™

The Three Ways



The First Way: Flow

- Creating single repository for code and environments
- All Ops artifacts in version control
- Determinism in the release process
- Consistent Dev, Test and Production environments, all properly built before deployment begins
- Developers checking in code daily, being productive
- Automated regression testing
- Features being deployed daily without catastrophic failures
- Decreased lead time
- Faster cycle time and release cadence

Google Dev And Ops (2013)

- 15,000 engineers, working on 4,000+ projects
- All code is checked into one source tree (billions of files!)
- 5,500 code commits/day
- 75 million test cases are run daily

"Automated tests transform fear into boredom."
-- Eran Messeri, Google

The First Way: Infosec Controls

- Integrate Infosec into Development iteration demonstrations
- Integrate peer reviews into all production change deployments
- Integrate Infosec into our deployment pipeline
- Including vulnerability scanning, static code analysis
- Ensure correctness and security of our applications
- Ensure correctness and security of our environments
- Ensure correctness and security of our software supply chain
- Ensure correctness and security of our deployment pipeline

The Second Way: Feedback

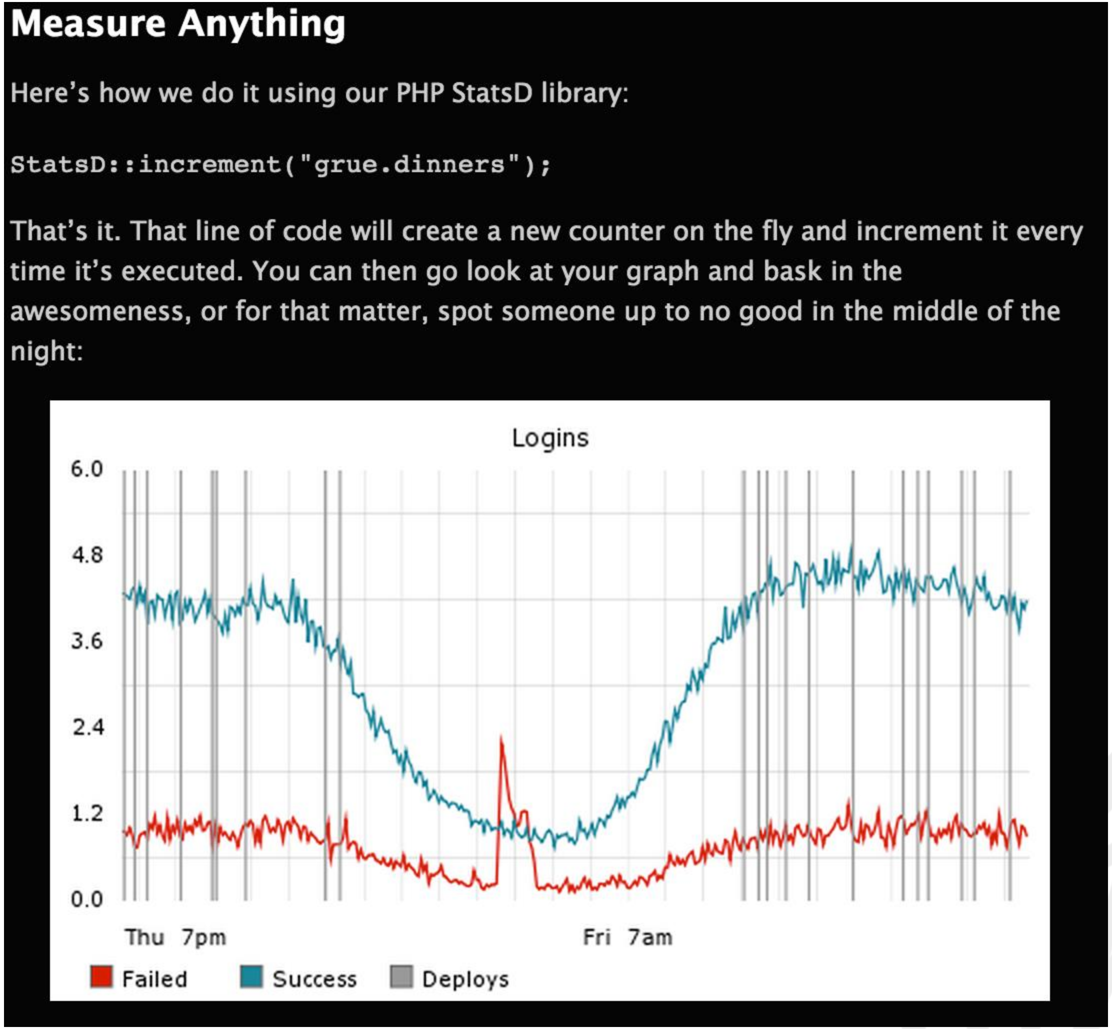
- Peer review of code and environment changes
- Disciplined automated testing enabling many simultaneous small, agile teams to work productively
- Proactive monitoring of the production environment
- Defects and security issues getting fixed faster than ever
- High trust culture
- All groups communicating and coordinating better
- Everybody is getting more work done

Pervasive Production Telemetry

- Etsy engineering culture: anything in production requires telemetry:

  Ian Malpass: “If it moves, we graph it. Even if it doesn’t move, we graph it, just in case it makes a run for it.”

- 2011: 200,000 production metrics
- 2015: 800,000 production metrics

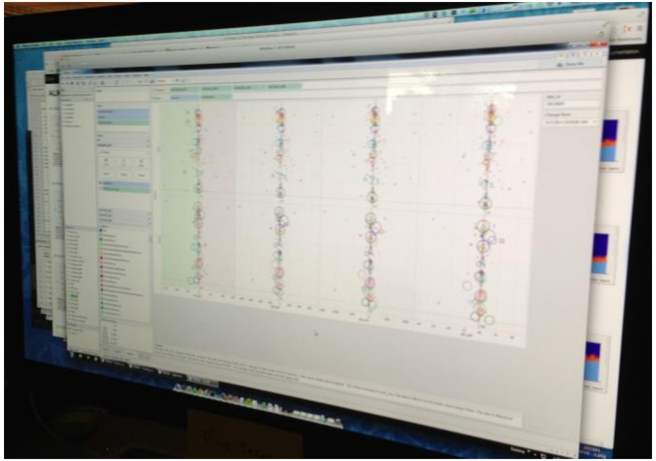


Measure Anything

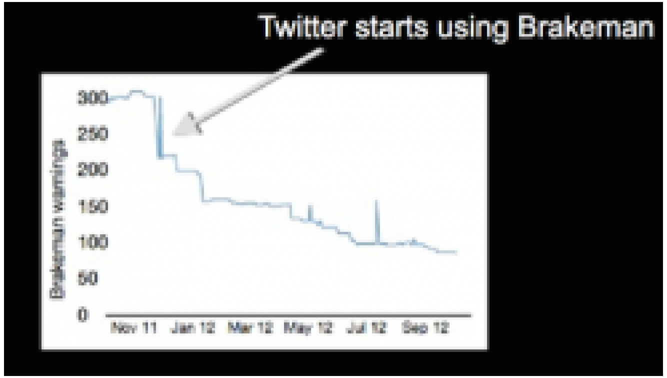
Here’s how we do it using our PHP StatsD library:

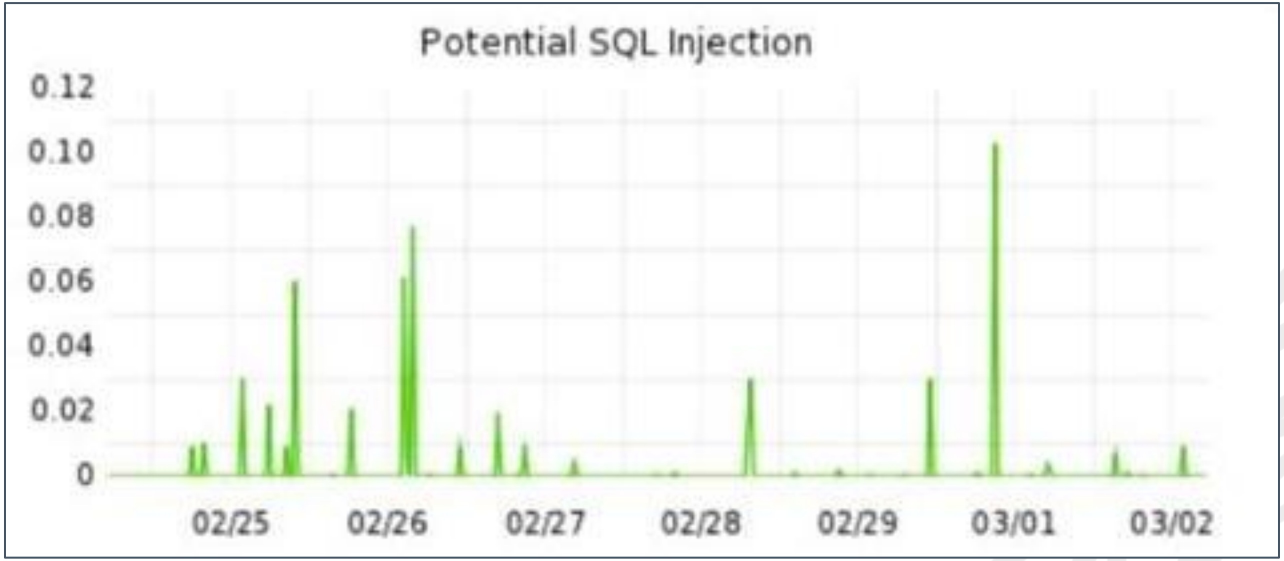
```
StatsD::increment("grue.dinners");
```

That’s it. That line of code will create a new counter on the fly and increment it every time it’s executed. You can then go look at your graph and bask in the awesomeness, or for that matter, spot someone up to no good in the middle of the night:



People actually look at the logs!
(Mention Verizon PCI Data Breach Study)





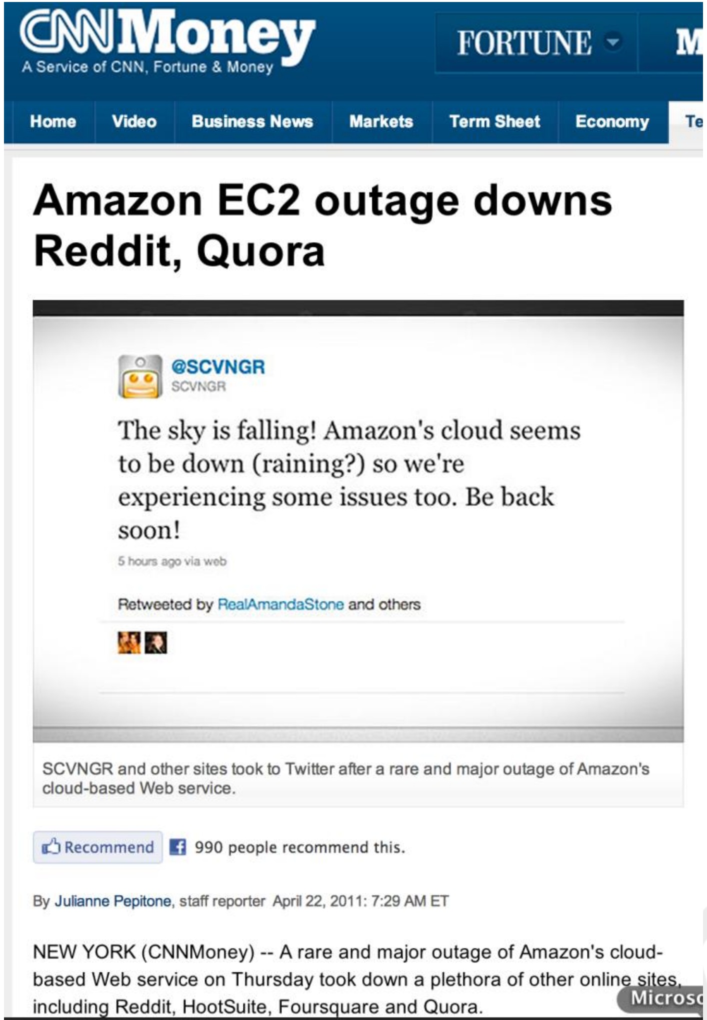
Source: The DevOps Handbook (Courtesy of Justin Collins, Twitter; Nick Galbreath, Etsy)

The Second Way: Infosec Controls

- Integrate dynamic testing and other security metrics in production
- Integrate Infosec into defect tracking tools
- Integrate Infosec into blameless post-mortems
- Integrate Infosec into all production telemetry
  - Applications
  - Environments
  - Deployment pipeline

The Third Way: Organizational Learning

- Reserve 20% of all Dev and Ops cycles for paying down technical debt
- Fearlessly inject faults into the production environment to gain assurance of our resilience
- Do everything we can to enable developer productivity
- Create organizational learning from our successes and failures, so we can win in the marketplace



Amazon EC2 outage downs Reddit, Quora

@SCVNGR
SCVNGR

The sky is falling! Amazon's cloud seems to be down (raining?) so we're experiencing some issues too. Be back soon!

5 hours ago via web

Retweeted by RealAmandaStone and others

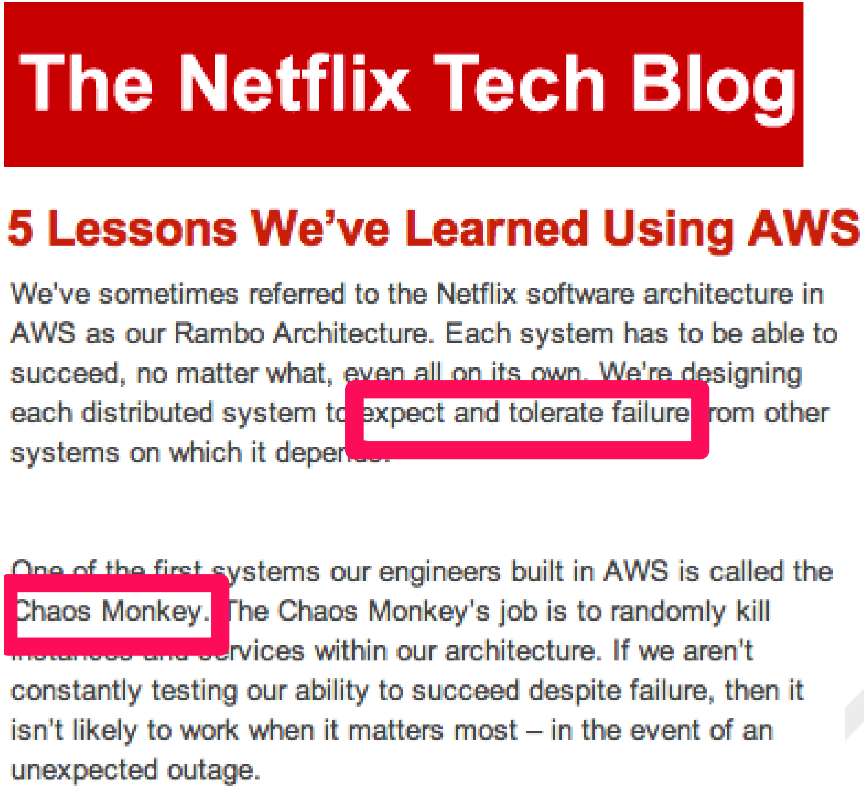
SCVNGR and other sites took to Twitter after a rare and major outage of Amazon's cloud-based Web service.

Recommend 990 people recommend this.

By Julianne Pepitone, staff reporter April 22, 2011: 7:29 AM ET

NEW YORK (CNNMoney) -- A rare and major outage of Amazon's cloud-based Web service on Thursday took down a plethora of other online sites, including Reddit, HootSuite, Foursquare and Quora.

Inject Failures Often



The Netflix Tech Blog

5 Lessons We've Learned Using AWS

We've sometimes referred to the Netflix software architecture in AWS as our Rambo Architecture. Each system has to be able to succeed, no matter what, even all on its own. We're designing each distributed system to expect and tolerate failure from other systems on which it depends.

One of the first systems our engineers built in AWS is called the Chaos Monkey. The Chaos Monkey's job is to randomly kill instances and services within our architecture. If we aren't constantly testing our ability to succeed despite failure, then it isn't likely to work when it matters most – in the event of an unexpected outage.

tenable

@RealGeneKim

You Don’t Choose Chaos Monkey…
Chaos Monkey Chooses You

The Third Way: Infosec Controls*

- Integrate preventive security controls into a shared source code repository
- Integrate Infosec controls into our shared services
- Integrate penetration testing (and rebooting) into our daily work

DevOps Is For The Unicorns…
…And The Horses, Too

DevOps Enterprise: Lessons Learned

- On Nov. 7-9, we held the third DevOps Enterprise Summit, a conference for horses, by horses
- Speakers included fifty leaders from:
  - Barclays, ING Bank, UK HMRC, Hiscox, Zurich Insurance, LV, UK GDS, iTV, Unilever, SAP, Macy's, Disney, Target, GE Capital, Western Union, Sherwin Williams, Blackboard, Nordstrom, Telstra, US Department of Homeland Security, CSG, Raytheon, IBM, Ticketmaster, MITRE, Marks and Spencer, Barclays Capital, Microsoft, Nationwide Insurance, Capital One, Gov.UK, Fidelity, Rally Software, Neustar, Walmart, PNC, ADP, ...

Observations

- They were using the same technical practices and getting the same sort of metrics as the unicorns
  - Target: 100+ deploys per week, < 10 incidents per month, enabled 53 business initiatives
  - Capital One: 100s of deploys per day, lead time of minutes
  - Macy’s: 1,500 manual tests every 10 days, now 100Ks automated tests run daily
  - Disney: Has embedded nearly 100 Ops engineers into LOB teams across the enterprise
  - Nationwide Insurance: Retirement Plans app (COBOL on mainframe)
  - Raytheon: testing and certification from months to a day
  - Key Bank: rebuilt consumer online banking in containers and Kubernetes in 1 year
  - Nordstrom: 20% lead time reduction into executive bonuses

Why Do I Think This Is Important?

tenable™

@RealGeneKim

The Downward Spiral…

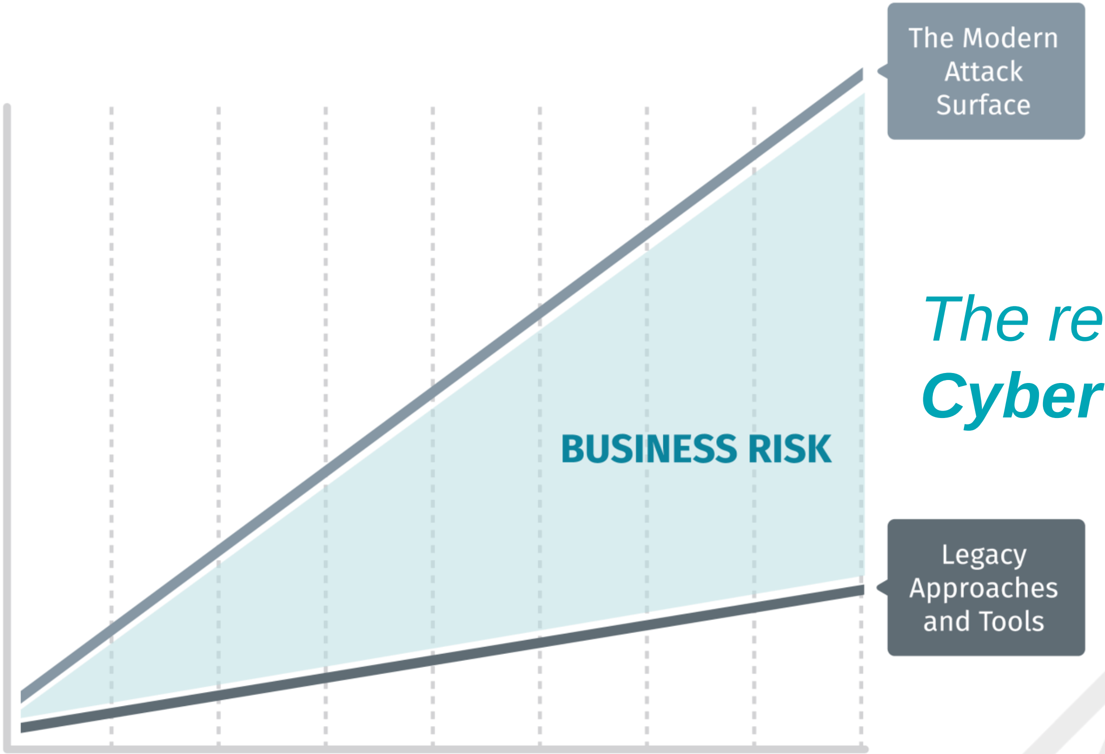
BIG COPS. SMALL TOWN. MODERATE VIOLENCE.
SIMON PEGG NICK FROST
HOT FUZZ
FROM THE MAKERS OF "SHAUN OF THE DEAD"

Poll Question #2

To what extent is your organization application containers like Docker or rkt?

1. What the heck is a container?
2. I think we may have some containers
3. We are dabbling with containers
4. Containers are part of our pre-prod environments
5. Containers are part of our production workloads

Legacy approaches cannot keep pace with an expanding attack surface



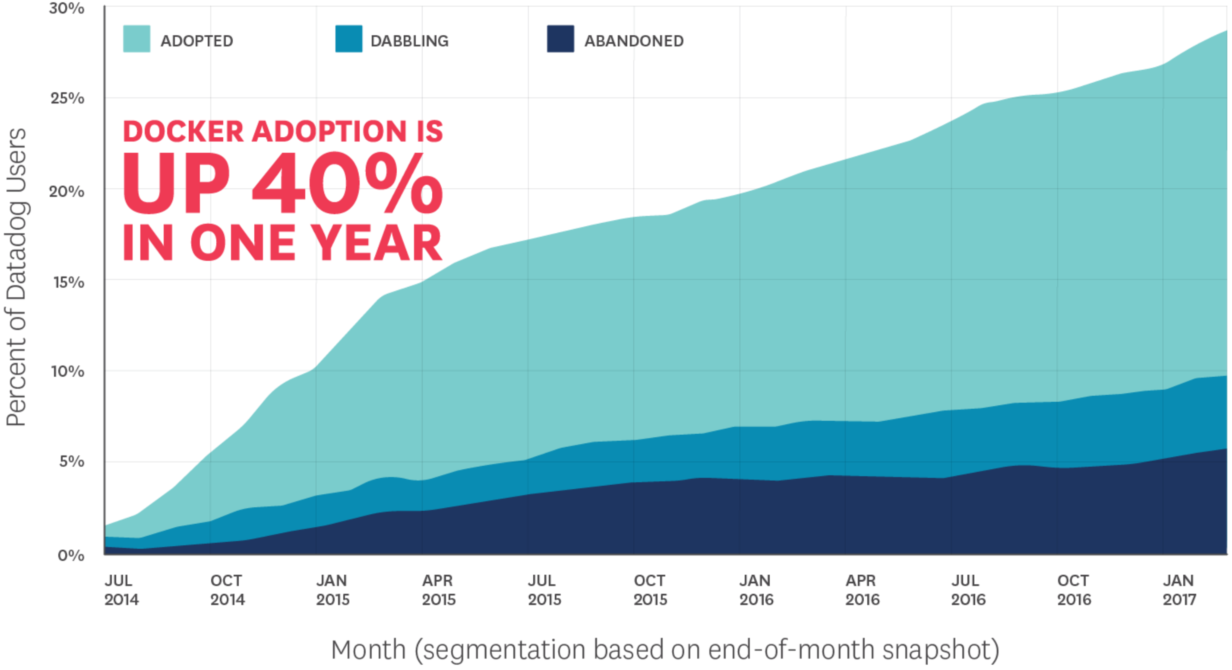
Cloud

Containers

The result is a
Cyber Exposure gap

Containers are exploding in adoption…

Docker Adoption[1]



500,000+

Dockerized apps in Docker Hub[2]

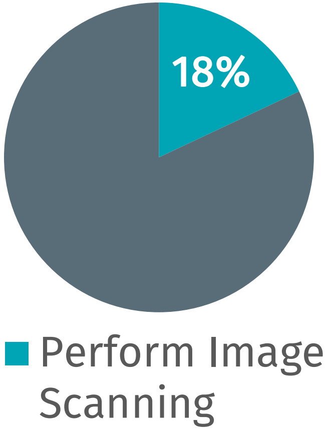
8 Billion+

Docker Container Downloads[2]

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

…and have become a massive blind spot to InfoSec

Of organizations with containers in production[1]



Risk Assessment Index[2] Organization's ability to assess cybersecurity risks

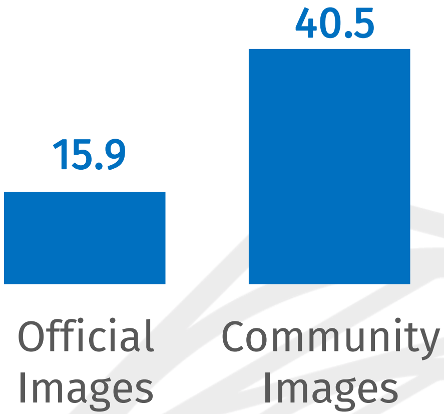
Score: **52%**
Grade: **F**

Containerization Platforms

Score: **57%**
Grade: **F**

DevOps Environments

Average number of vulnerabilities in Docker Hub[3]



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

tenable

DevOps scale and speed requires a new approach to container security

Mutable

OR

Immutable

Automated inspection of container images

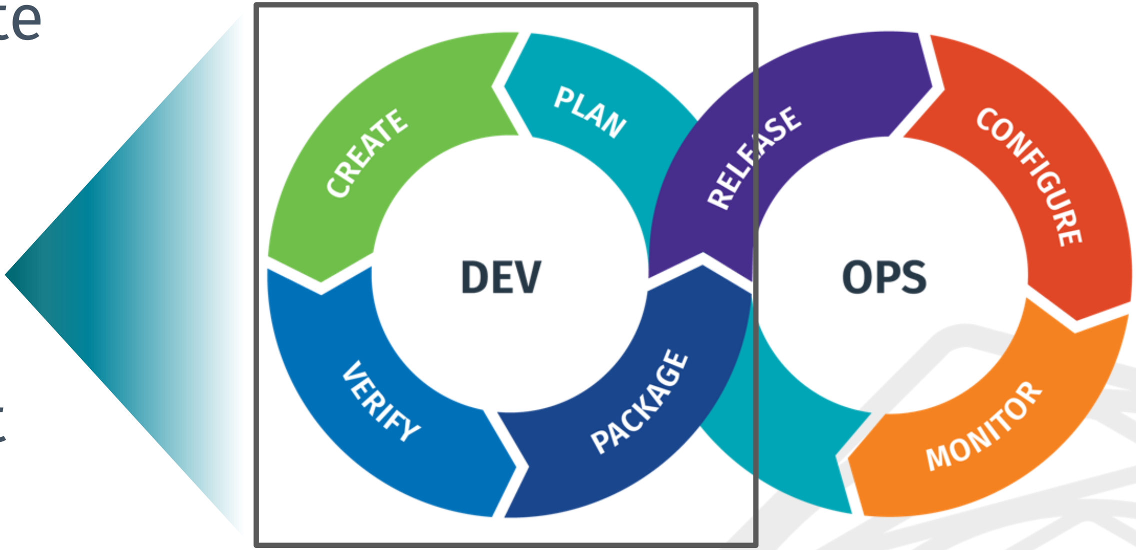
Fast, in-depth assessment of container images for vulnerabilities and malware

Layer hierarchy intelligence to understand when vulnerabilities are mitigated in higher layers

Prevent vulnerabilities by securing assets prior to deployment

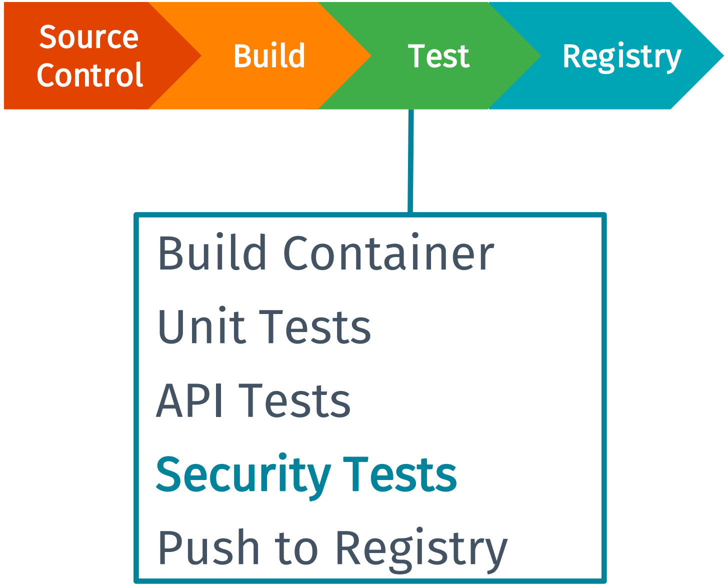
Identify and remediate vulnerabilities before they are exploitable

Ensure all assets are secure and compliant before production



tenable™

“Shift left” with security in the software development lifecycle



Source Control

Build

Test

Registry

Build Container

Unit Tests

API Tests

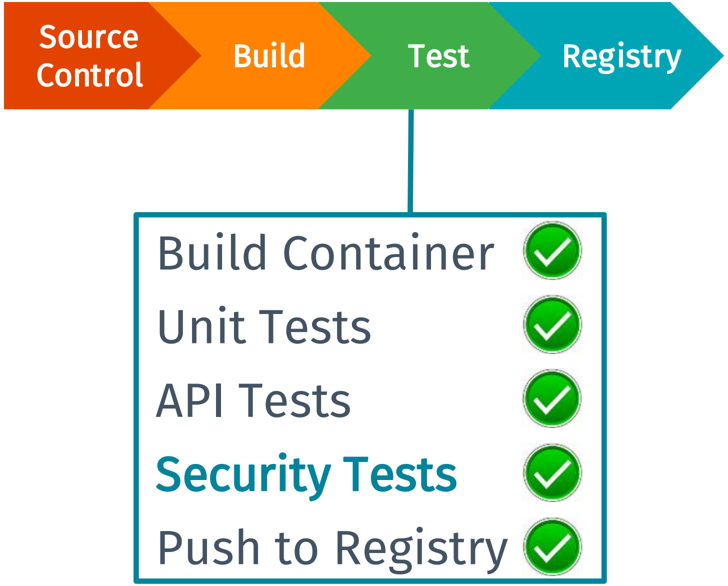
Security Tests

Push to Registry

Vulnerability and malware detection testing within the DevOps toolchain

Integrate with CI/CD build systems and container registries

Ensure containers in production are compliant with policy



Source Control → Build → Test → Registry

- Build Container ✓
- Unit Tests ✓
- API Tests ✓
- **Security Tests** ✓
- Push to Registry ✓

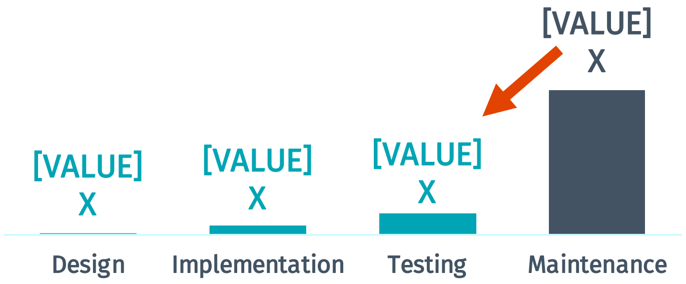
Notify developers immediately when images exceed organization risk thresholds

Allow developers to take direct action with specific remediation advice

“Shifting left” provides value to both InfoSec and DevOps

Reduce Costs

Cost of Fixing Defects in SLDC[1]



Eliminate Blind Spots

Comprehensive Insight Across Modern Assets

Enterprise IT

Cloud

Containers

Applications

Mobile

Accelerate DevOps

Time to Complete Security Test

< 30 Seconds

[1] Source: Computer Business Review, ”The cost of fixing bugs throughout the SDLC,” March 2017

Are you new to DevOps?
Go to where the developers are

AWS re:Invent

dockercon

O'REILLY®
Velocity
CONFERENCE

DEVOPSDAYS

Jenkins World
A global DevOps event
2017

DEVOPS ENTERPRISE SUMMIT
San Francisco
November 13–15, 2017

Do you get DevOps?
Try out Tenable.io Container Security for free

60 Day Trial

tenable.com/try-container

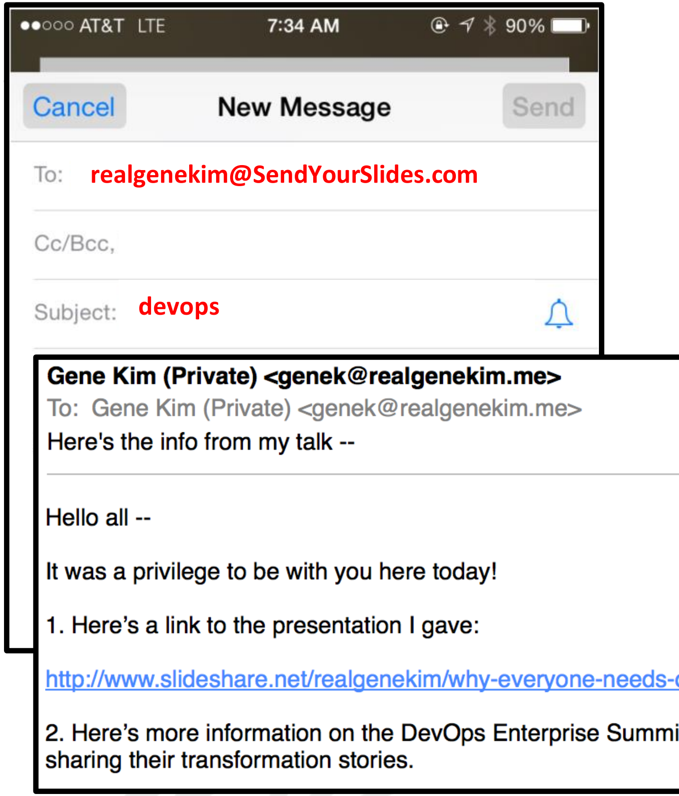
Want to learn more?

To receive the following:

- A copy of this presentation
- The 140 page excerpt of *The DevOps Handbook*
- The 140 page excerpt of *The Phoenix Project*
- Videos and slides from DevOps Enterprise 2014-2016
- Link to the DevOps Audit Defense Toolkit
- One hour excerpt of *The Phoenix Project* audiobook

Just pick up your phone, and send an email:

To: realgenekim@SendYourSlides.com
Subject: **devops**



To: realgenekim@SendYourSlides.com

Cc/Bcc,

Subject: devops

Gene Kim (Private) <genek@realgenekim.me>
To: Gene Kim (Private) <genek@realgenekim.me>
Here's the info from my talk --

Hello all --

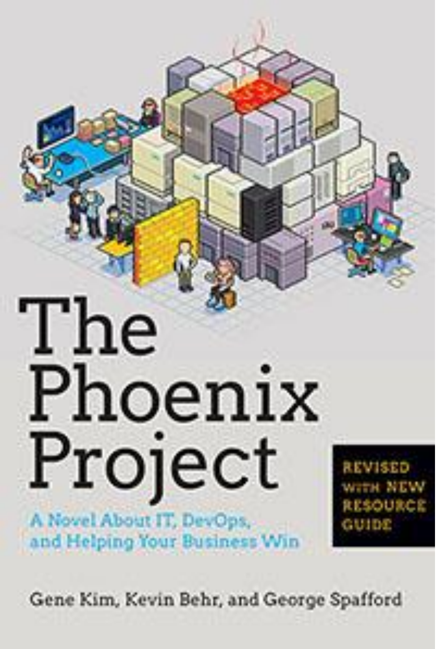
It was a privilege to be with you here today!

1. Here’s a link to the presentation I gave:

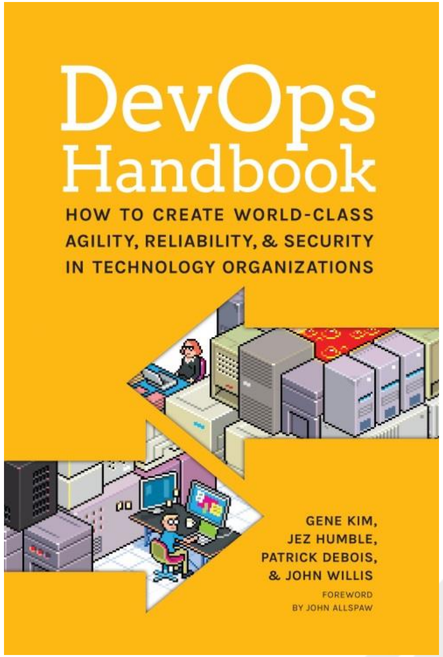
http://www.slideshare.net/realgenekim/why-everyone-needs-

2. Here’s more information on the DevOps Enterprise Summi
sharing their transformation stories.

Live attendees have been entered in a Sweepstakes to win a copy of one of Gene's books.


The Phoenix Project
A Novel About IT, DevOps, and Helping Your Business Win
REVISED WITH NEW RESOURCE GUIDE
Gene Kim, Kevin Behr, and George Spafford

100x


DevOps Handbook
HOW TO CREATE WORLD-CLASS AGILITY, RELIABILITY, & SECURITY IN TECHNOLOGY ORGANIZATIONS
GENE KIM, JEZ HUMBLE, PATRICK DEBOIS, & JOHN WILLIS
FOREWORD BY JOHN ALLSPAW

100x

tenable™