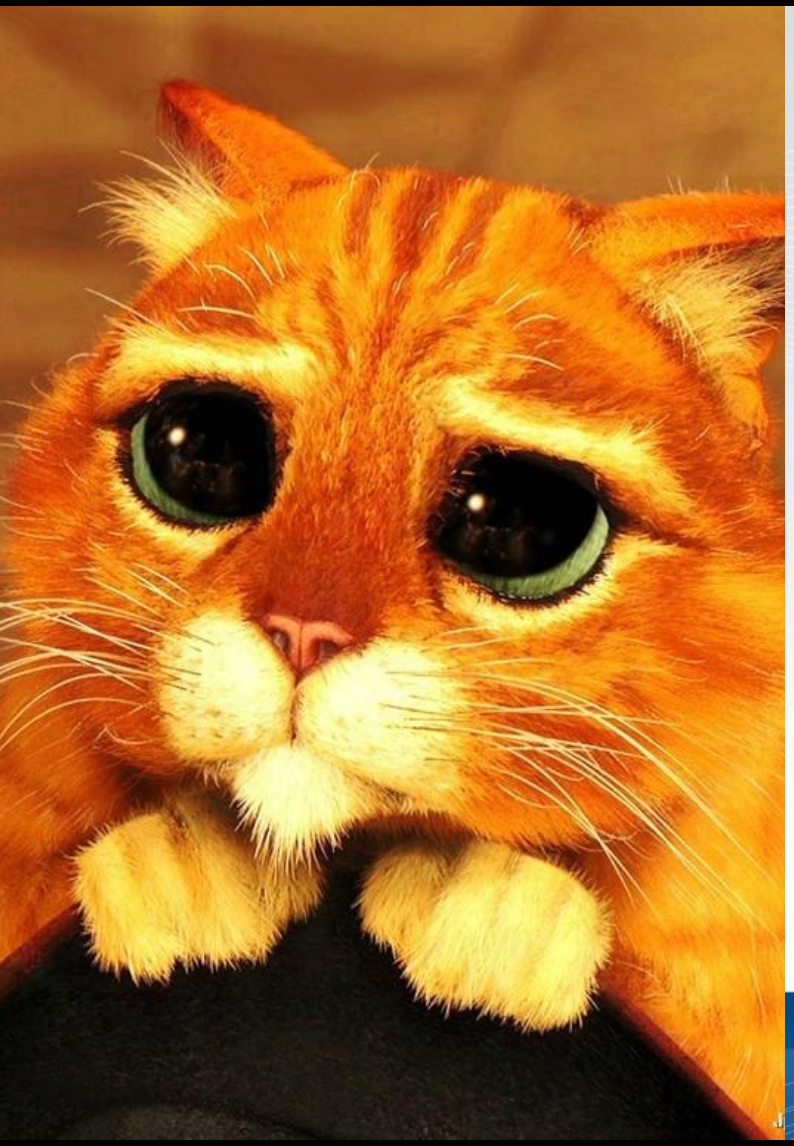
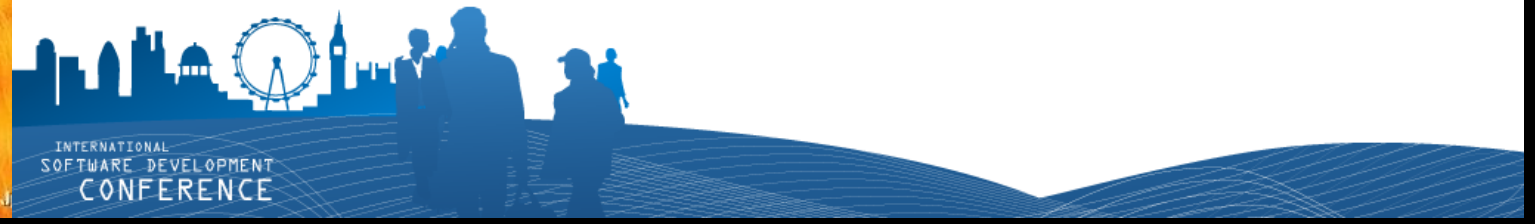


QCon

Please evaluate my talk via the mobile app!



Help, my Security Officer is allergic to DevOps…!

DevOps and Security, a match made in heaven or a forced marriage from hell?

Pop quiz: What is the acronym for...

HyperText Transfer Protocol

Pop quiz: What is the acronym for...

Internet

Mail Access

Protocol

Pop quiz: What is the acronym for...

Secure Hyper Text Transfer Protocol

Pop quiz: What is the acronym for...

Secure**d** Internet Mail **A**ccess Protocol

Pop quiz: What is the acronym for...

Development & Operations

Pop quiz: What is the acronym for...

Secure Development & Operations

Image: Portrait taken by Arthur van Schendel

> whoami

» Frank Breedijk

- Security Officer at Schuberg Philis
- Author of Seccubus
- Blogger for CupFigther.net

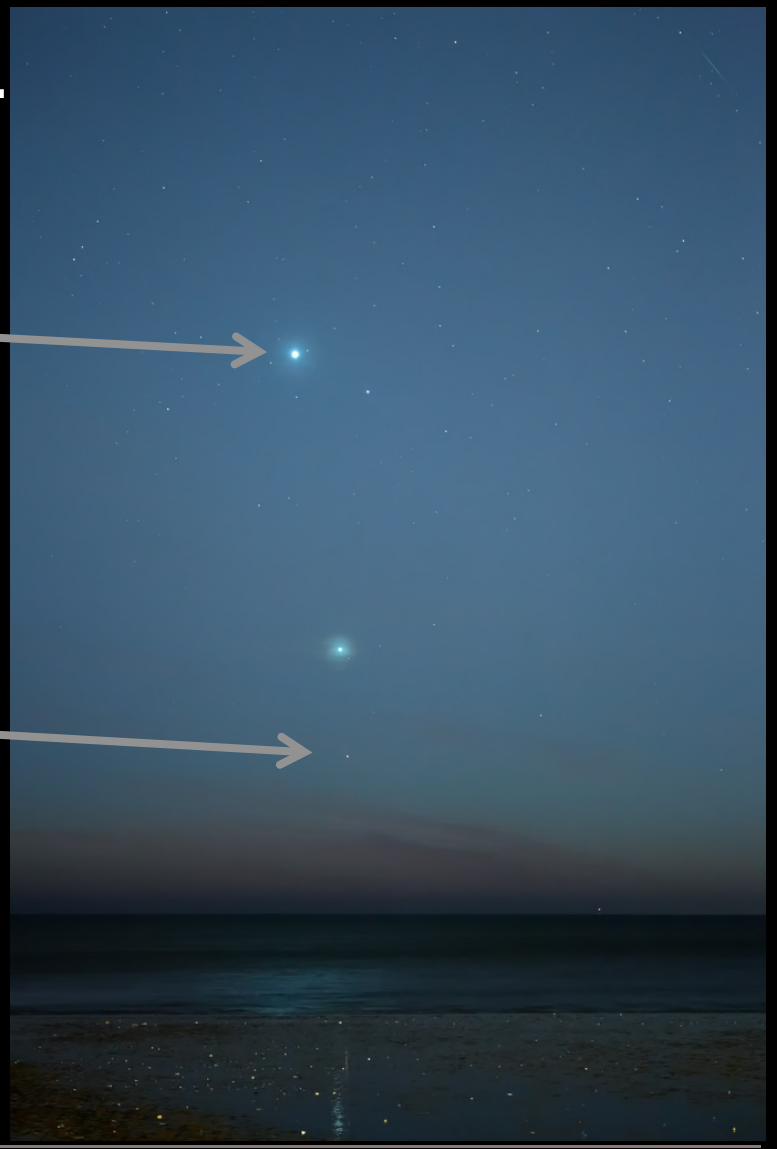
Email:	fbreedijk@schubergphilis.com
Twitter:	@Seccubus
Blog:	http://cupfighter.net
Project:	http://www.seccubus.com
Company:	http://www.schubergphilis.com

Image: http://devopsreactions.tumblr.com/post/47939884113/blue-screen-after-patching-production-server

Typical security officer reaction when you propose DevOp

Image: Conjunction CC NC by lrargerich http://www.flickr.com/photos/29638083@N00/5707310636/

We need to understand where we come from…



» DevOp

» Security

What is CENSOREDop?

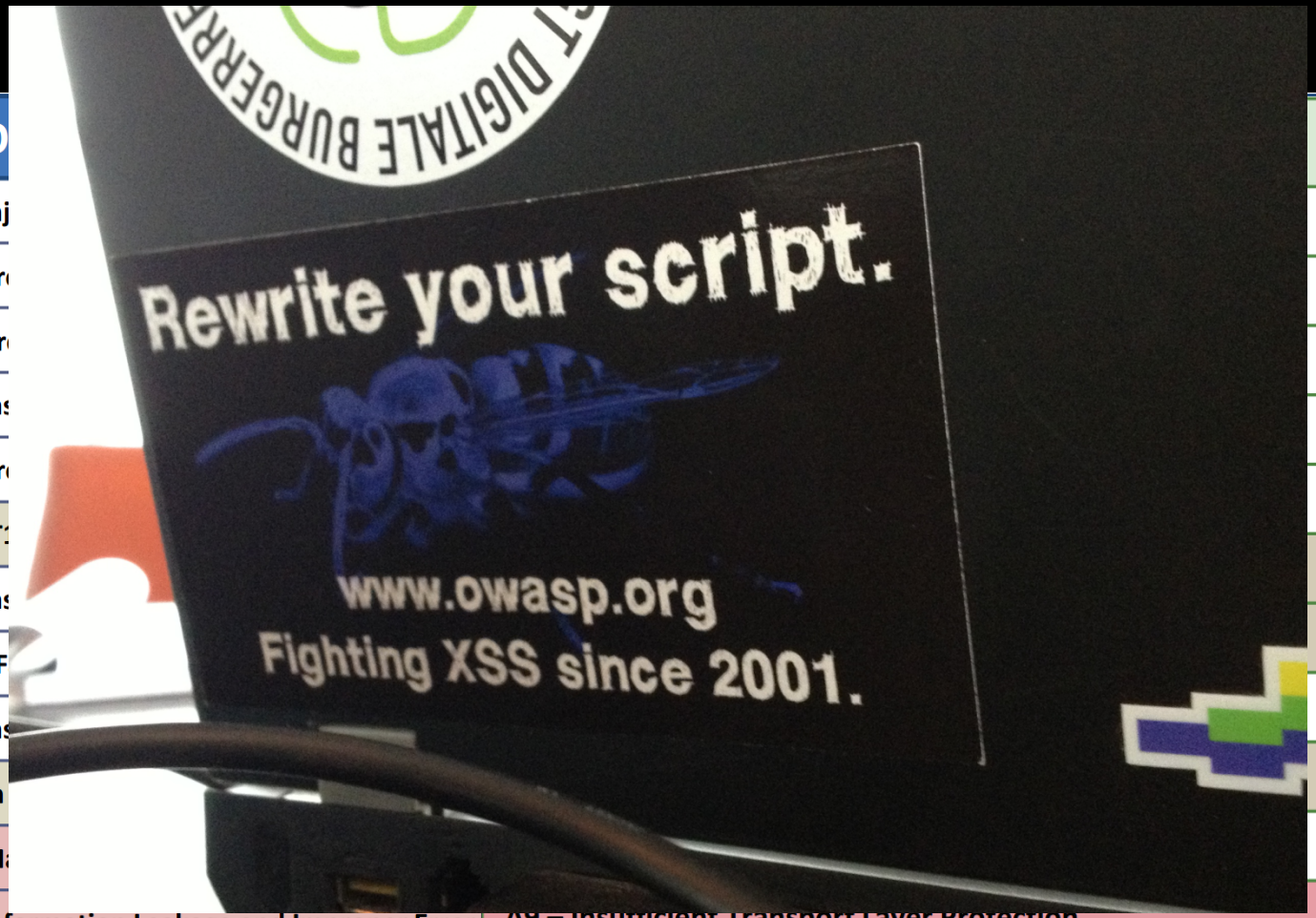
- » CENSOREDop is a methodology where Development and Operations jointly work together to enable faster delivery of software or services to the production environment.
- » CENSOREDop enables faster release cycles (up to and above ten releases a day)
- » With CENSOREDop software can be automatically built, tested and deployed, ideally without the involvement operations resources
- » CENSOREDop is often supported by Agile development processes

Source: http://devopsreactions.tumblr.com/post/41776196984/first-test

Faster delivery cycles…
How is this going to affect my security posture?

Image: @akaasjagers desktop by Frank Breedijk

Developers do not have a great reputation with security



O
A2 – Inj
A1 – Cr
A7 – Br
A4 – Ins
A5 – Cr
<was T1
A8 – Ins
A10 – F
A9 – Ins
<not in
A3 – Ma
A6 – Information Leakage and Improper Error

	OWASP Top 10 – 2013 (New)
	A1 – Injection
	A2 – Broken Authentication and Session Management
	A3 – Cross-Site Scripting (XSS)
	A4 – Insecure Direct Object References
	A5 – Security Misconfiguration
	A6 – Sensitive Data Exposure
	A7 – Missing Function Level Access Control
	A8 – Cross-Site Request Forgery (CSRF)
	A9 – Using Known Vulnerable Components
	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

Source: http://testerreactions.tumblr.com/post/50489315537/new-implementation-first-verification

Faster delivery cycles…
What security worries about

» Poorly tested code…

» How can it be mitigated? (aka Your answer) ☺

- Automated testing
  - Functionali☺☺☺
  - Security
    - Foritfy, VeraCode, WhiteHat Sentinel
    - Gauntlt (https://github.com/gauntlt)
    - BDD-Security (http://www.continuumsecurity.net/bdd-intro.html)
    - Chaos Monkey (https://github.com/Netflix/SimianArmy)
    - Seccubus (www.secubus.com)

Source: http://devopsreactions.tumblr.com/post/46061575774/surviving-a-ddos-attack

Faster delivery cycles…
What security worries about

» No more room for to patch

» How can it be mitigated? (aka Your answer)
- Patches become just another release
- If we miss a patch window, there will be plenty more
- We didn't miss our single shot to get it right

Source: http://en.wikipedia.org/wiki/Separation_of_duties

Joint cooperation
Automated deployment

» What about separation of duties?

Application in information systems [edit]

The accounting profession has invested significantly in separation of duties because of the understood risks accumulated over hundreds of years of accounting practice.

By contrast, many corporations in the United States found that an unexpectedly high proportion of their Sarbanes-Oxley internal control issues came from IT. Separation of duties is commonly used in large IT organizations so that no single person is in a position to introduce fraudulent or malicious code or data without detection. Role based access control is frequently used in IT systems where SoD is required. Strict control of software and data changes will require that the same person or organizations performs only one of the following roles:

- Identification of a requirement (or change request); e.g. a business person
- Authorization and approval; e.g. an IT governance board or manager
- Design and development; e.g. a developer
- Review, inspection and approval; e.g. another developer or architect.
- Implementation in production; typically a software change or system administrator.

This is not an exhaustive presentation of the software development life cycle, but a list of critical development functions applicable to separation of duties.

To successfully implement separation of duties in information systems a number of concerns need to be addressed:

- The process used to ensure a person's authorization rights in the system is in line with his role in the organization.
- The authentication method used such as knowledge of a password, possession of an object (key, token) or a biometrical characteristic.
- Circumvention of rights in the system can occur through database administration access, user administration access, tools which provide back-door access or supplier installed user accounts. Specific controls such as a review of an activity log may be required to address this specific concern.

Source: http://devopsreactions.tumblr.com/post/50566447542/another-pci-dss-audit

Another PCI DSS audit

Source: http://securityreactions.tumblr.com/post/31398166073/when-someone-says-their-company-is-secure-because-they

When someone says their company is secure because they run PCI-DSS Scans

Source: http://devopsreactions.tumblr.com/post/48511362536/i-dont-need-to-test-that-what-can-possibly-go-wrong

Segregation of duties…
What does security worry about?

» Mistakes by incompetence

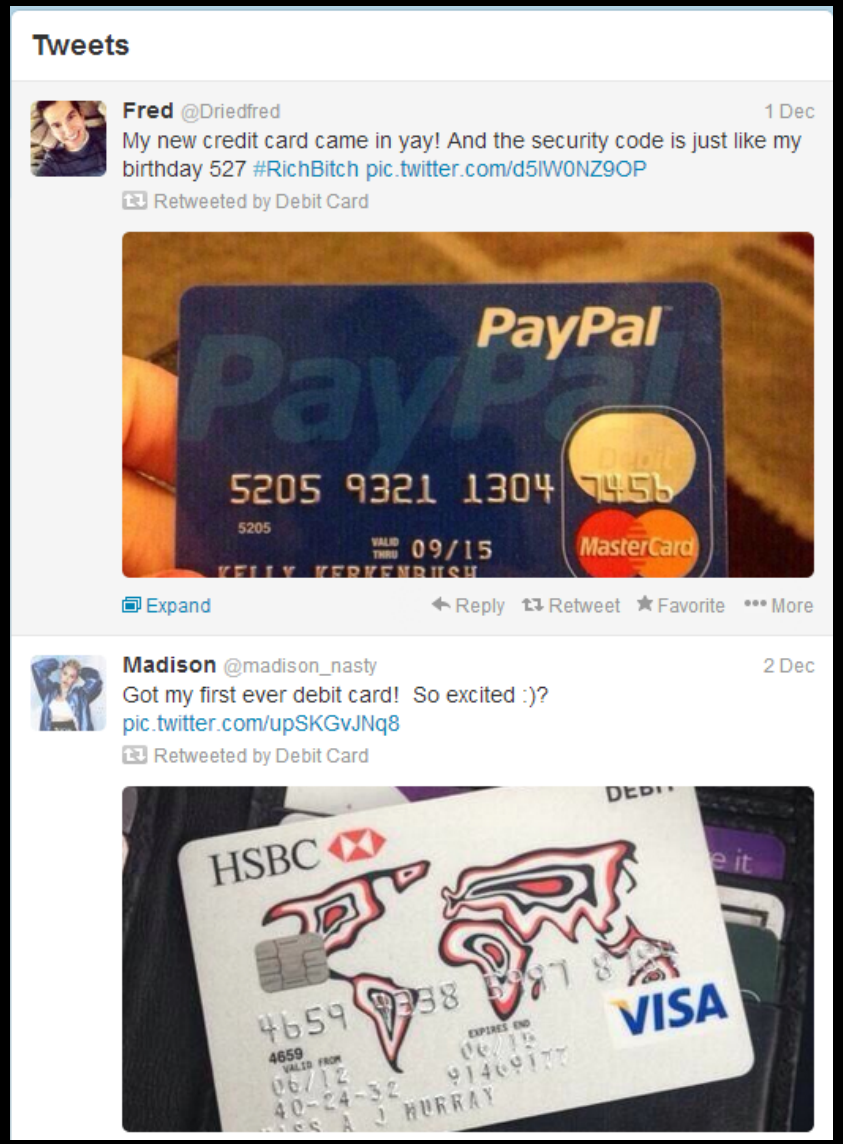
» How can it be mitigated? (aka Your answer) ☺
- Culture
  - Make sure people know and respect their own limits ☺
- Transparency
  - Make sure all changes are visible to everyone
  - Peer review
  - Changes are small and can be understood
- Not every part of the system is in scope of PCI DSS/SOX ☺
  - Work with approvals for components in scope

Source: https://twitter.com/NeedADebitCard

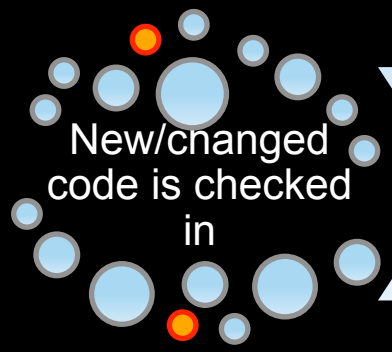
Segregation of duties…
What does security worry about?

» Fraud
  – There may be actual financial losses
  – Failed PCI DSS/ SOX
  – Auditors want us to have this

» How can it be mitigated? (aka Your answer)
  – Transparency
    • Make sure all changes are visible to everyone
    • Peer review
    • Changes are small and can be understood
  – Not every part of the system is in scope of PCI DSS/SOX
    • Work with approvals for components in scope



Putting signatures on critical code…



New/changed code is checked in

Critical code does NOT match signature

Security team reviews critical code and signs it

Build ok!

Source: http://doit.creighton.edu/faculty-staff-services/cab

10 or more releases a day…

Change Advisory Board (CAB)

Overview

The change advisory board (CAB) helps to ensure that changes to IT systems are managed in a rational and predictable manner. CAB is responsible for enforcing change management policies within IT and for overseeing and approving request for changes (RFCs). The security team manages the operations, policies, and procedures of the change advisory board. The CISO acts as the meeting chair, and a member of the security team serves as a voting member.

- DoIT CAB meets every Thursday (while university is open), 1:00 pm, in the Old Gym 4th floor conference room
- Request for Changes (RFC's) should be submitted at least 2 weeks before implementation
- Attendance is necessary to represent your RFC

Source: http://dilbert.com/strips/comic/2006-08-17/

Security says NO…

Source: http://securityreactions.tumblr.com/post/67562914945/java-source-code-review

Change advisory board…
Why security says noooo…

» Are changes reviewed for security?

» How can it be mitigated? (aka Your answer)

– It will happen anyway…

– There will be at least 50 changes a week

- Security doesn't have the capacity to review everything
- Let us help you to deal with this
- Ask for guidance on what needs a review
- Implement signatures for critical functionality
- Add automated security testing

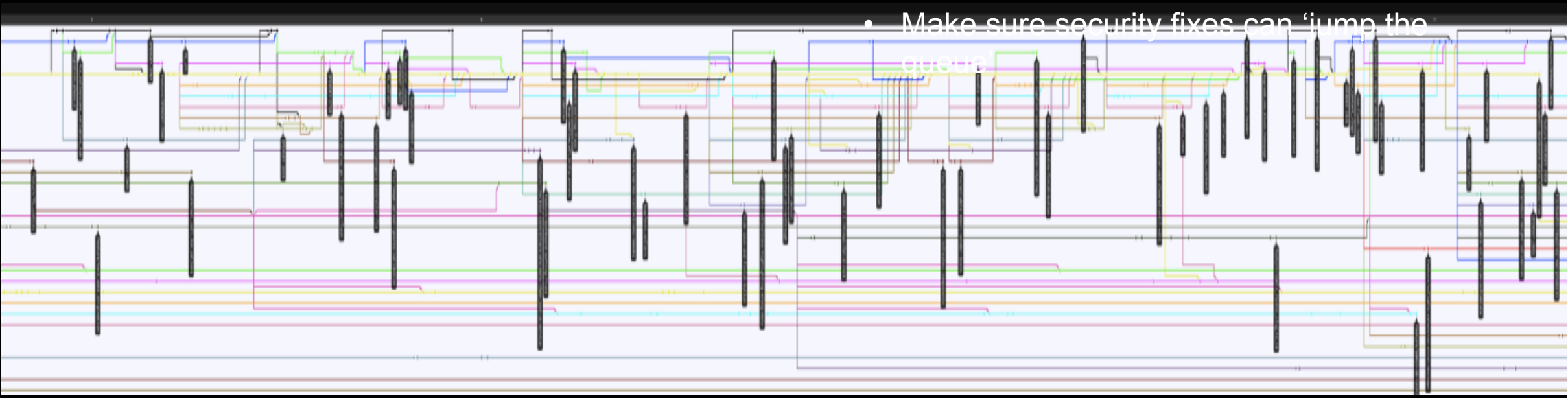
Change advisory board…
Why security says noooo…

» Changes must have a role back plan

» How can it be mitigated? (aka Your answer)

– Role back cannot exist

- But fix forward does (multiple times a day)
- Make sure security fixes can ‘jump the queue’



Source: http://securityreactions.tumblr.com/post/64390760807/when-the-client-asks-me-to-verify-their-fix

Change advisory board…
Why security says noooo…

» We are afraid of uncontrolled change

» The CAB was our only point of influence

» How can it be mitigated? (aka Your answer)

– Enable security to become the immune system

- Give insight into all changes
- Allow security to test / verify changes
- Whenever, whatever, however
- Automate security tests

» Pulling the Andon cord is not saying no…

» Remind security that survival isn't mandatory

Image: Planning Poker, CC NC SA by 2nk - http://www.flickr.com/photos/53023503@N00/3947006171/

Agile development
My objections

- » Product owner owns the backlog to delivery functionality to the user
- » Complexity of stories is measured in story points
- » You don't get points for fixing defects

Security

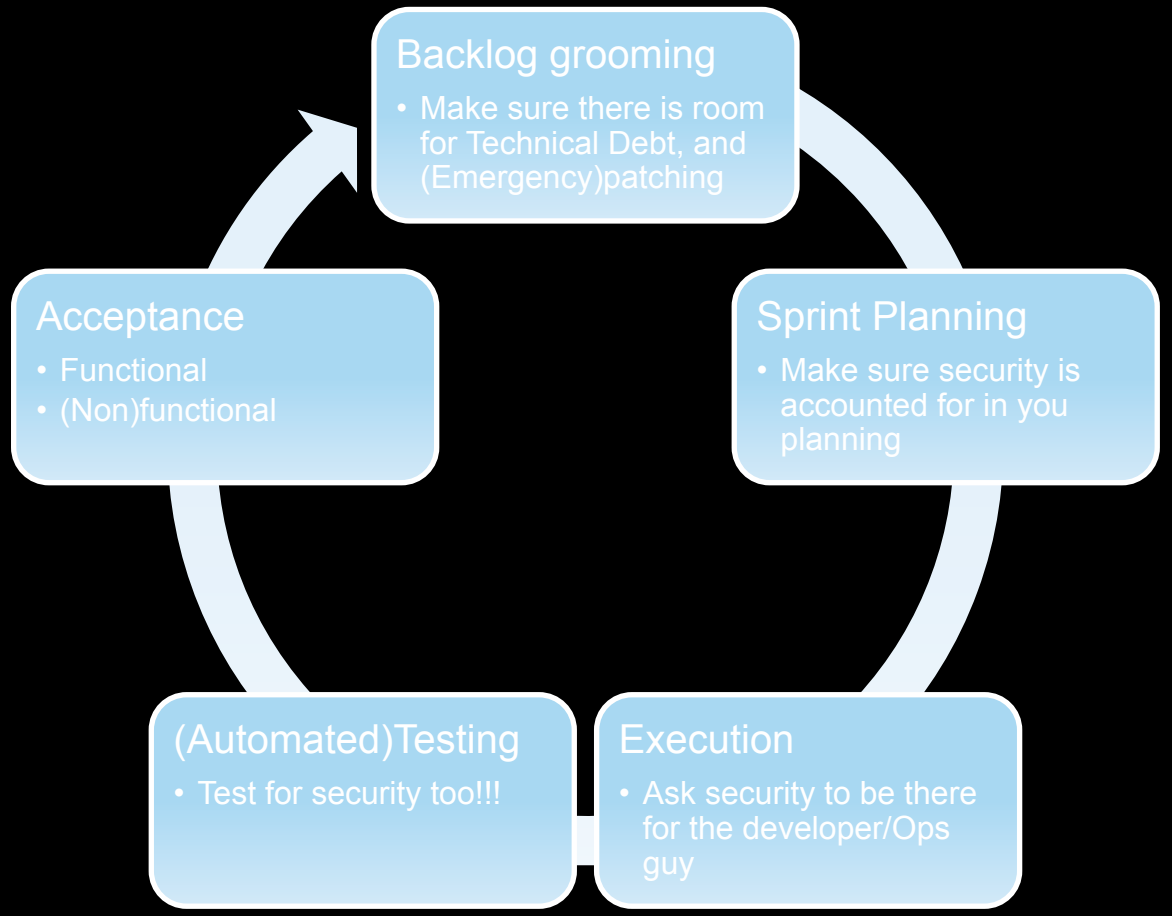
- » Is often a "non-functional" requirement
- » Making sure security is part of a story increases complexity (cost) of a story
- » Devs are not rewarded for fixing security issues
- » Result: Security seems to make you less agile

Image: Post-It Fun, CC by zerojay - http://www.flickr.com/photos/15969266@N04/3238168719/

Agile development
Your answer

- Security and product owner should cooperate
- Non-functional requirements are requirements too
- Dealing with NFRs from the start is more effective/efficient then dealing with them later
- We will plan for unplanned work
- Make sure the team is rewarded for reducing technical debt
  - There is security debt in technical debt

Where Security needs to be fit into Agile

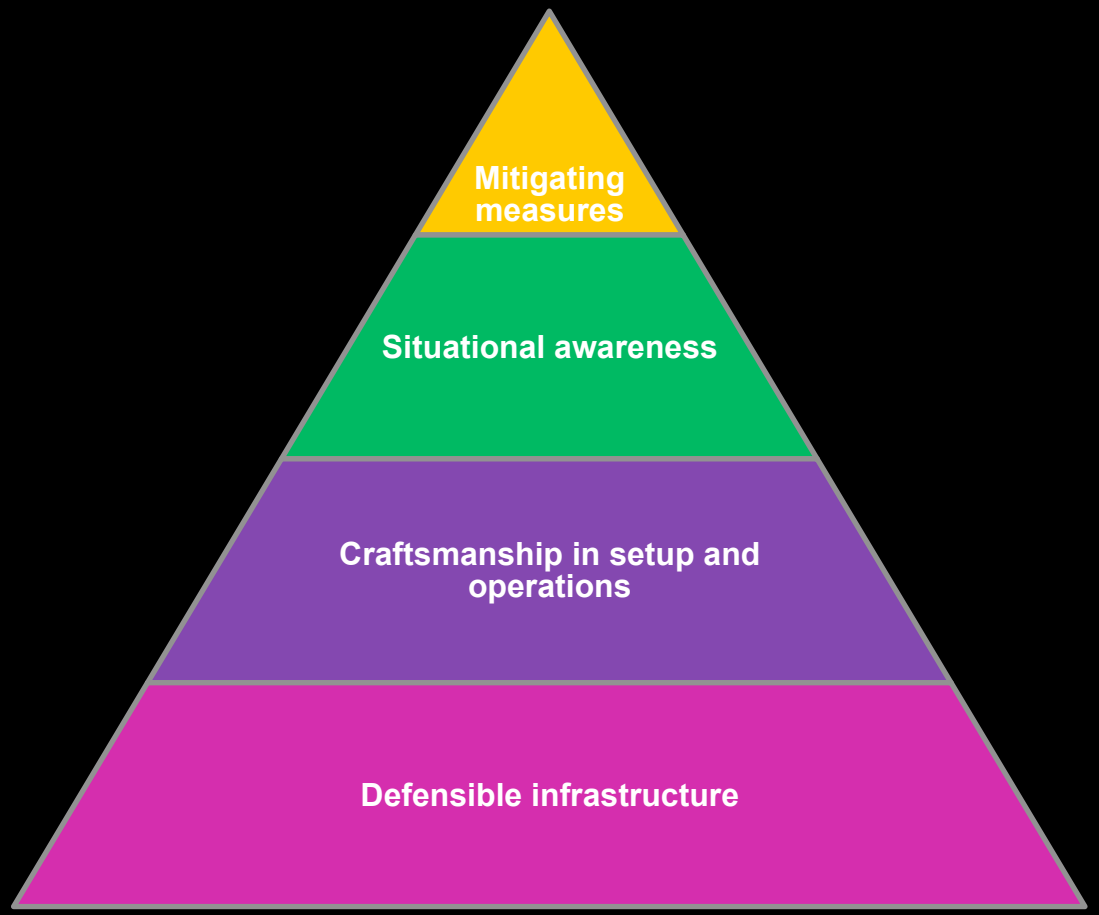


Source: http://securityreactions.tumblr.com/post/59198452899/crypto-implementation-in-whistle-im

Security is misguided too…

- Security people are obsessed with controls/locks…
- We don't often spend time/money where it has the most effect on security

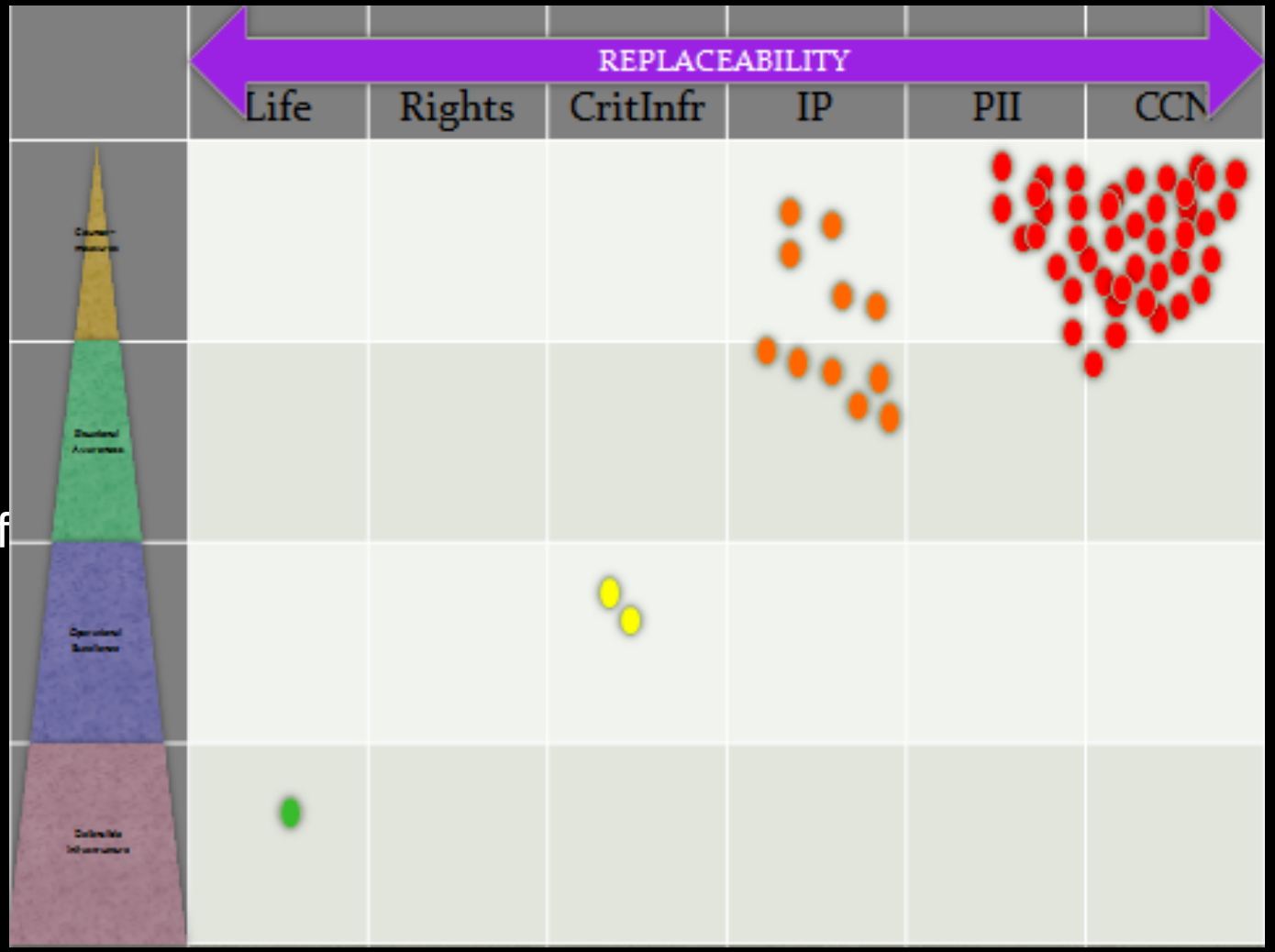
Where do we get the most bang for buck?



- Specific security technologies
  - IDS, IPS
  - Next generation firewall
  - Data loss preventions
- What is happening now?
  - Who is attacking?
  - What are they doing
- How well are your systems maintained?
  - Patch levels up to date?
  - Security holes patched?
  - Passwords hashed and salted?
  - AV up to date?
- How well can you defend your infrastructure?
  - Layers of defense?
  - Access control in order?
  - Dual factor authentication?
  - Stepping stones?

What the industry talks about

- » Conference talks are centered around attack and technical measures
- » Most infosec spending is around mitigating measures, not defensible infrastructures of quality of software / infrastructure operation



Example: using automation to build system imag

» At Schuberg Phils we automated OS builds

» Wins for security
- Systems are no longer like snowflakes
- Every system that is installed at least starts secure
- Insecure images break the build
- Tested against the CIS benchmarks

» Wins for Dev/Ops
- Software is tested against secure builds
- Works on my laptop becomes irrelevant
- No need to wait 2 hours for all windows patches to install

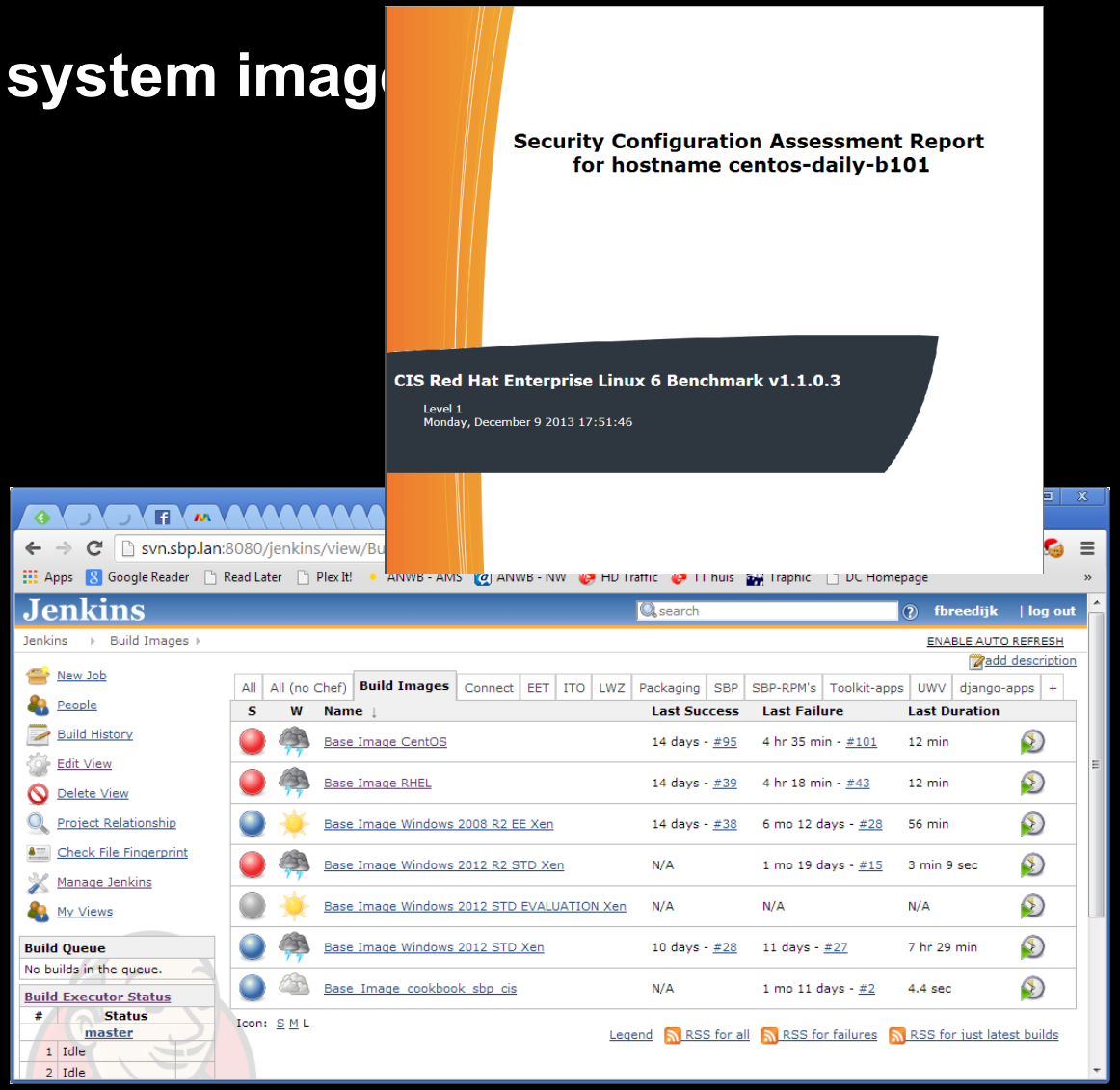


Image: http://devopsreactions.tumblr.com/post/49168088989/backup-and-dr-testing

Rugged DevOpS

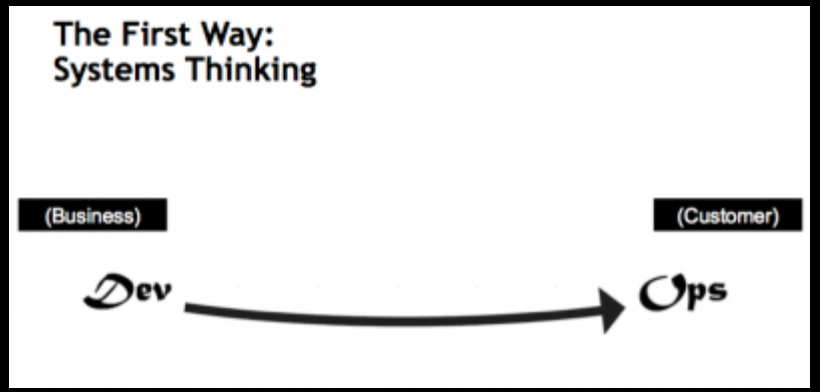
DevOpS benefits

- Infrastructure has become code too
  - Can be unit tested
  - Security can be built in
- DevOpS has lots of small changes that take place often
  - Changes are small so impact of missing a window is small
  - Emergency changes can skip the queue
  - Environments should be rebuilt often
    - Makes DR test implicit
    - Enables easy patching
- DevOpS is quality driven
  - Security is a quality

Security is part of all the ways of DevOp

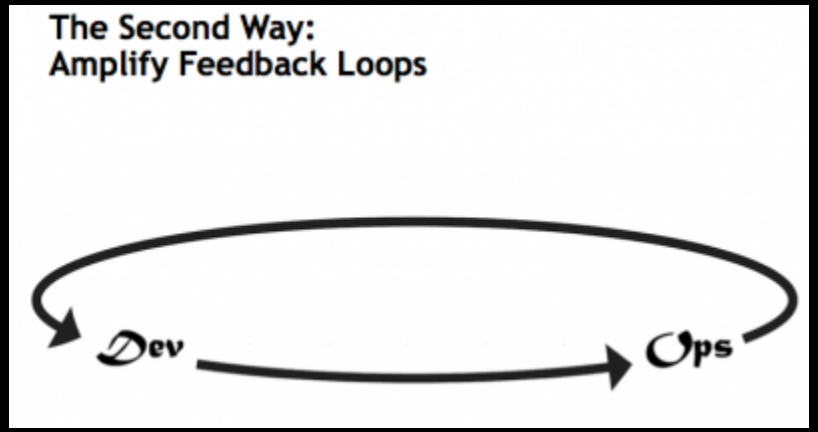
» System thinking
  – Code not in production isn't code
  – Code that isn't secure isn't code

» Stop treating security as a silo…



Allow security to provide a strong feedback signal

- The shorter the feedback loops are, the better the learning effect
  - Automated security testing
  - Signed code
  - Allow security to pull the Andon cord
  - Have Nagios tests for security?



Allow for experimentation???

- DevOps is THE change to security to finally get it right
- Defensible infrastructure

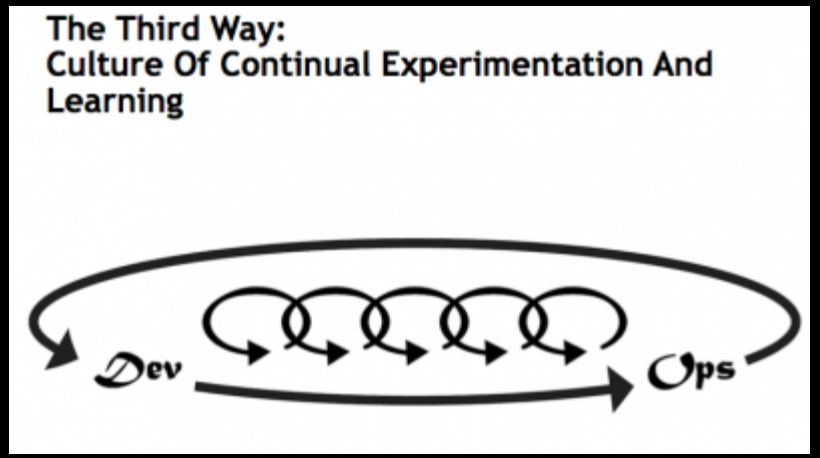


Image: http://securityreactions.tumblr.com/post/65138818960/got-my-5th-animated-gif-published-in-securityreactions

Conclusion…

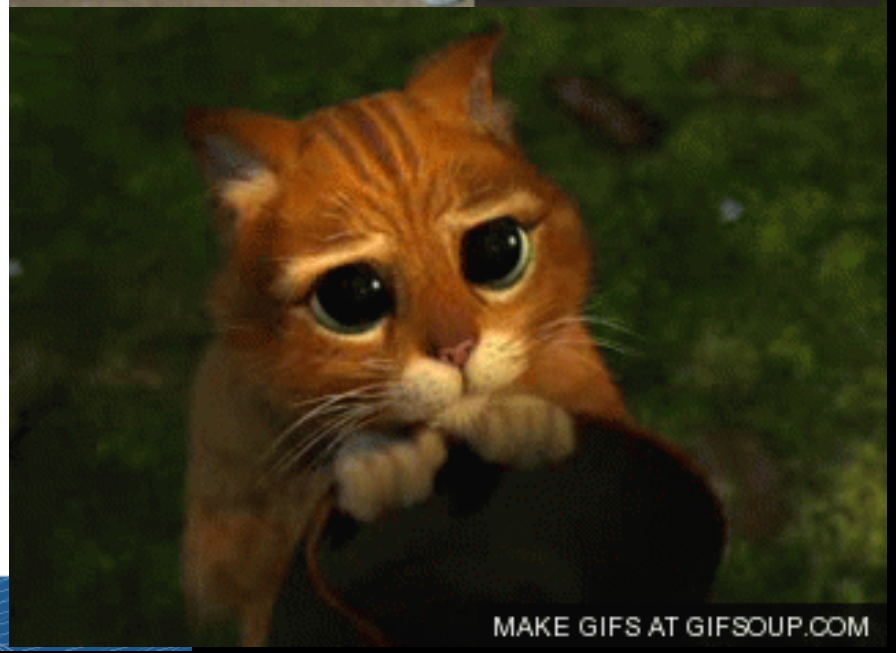
» DevOpS is full of win!

» If we listen to each other we can all benefit

@seccubus
fbreedijk@schubergphilis.com

QC

Please evaluate my talk via the mobile app!



INTERNATIONAL SOFTWARE DEVELOPMENT CONFERENCE