RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

Challenge today's security thinking

SESSION ID: ASD-W02

Is DevOps Breaking Your Company?

Elizabeth Lawler

CEO & Co-Founder

Conjur, Inc.

@elizabethlawler

#RSAC

Agenda

I. **Security + DevOps Overview**

Unstoppable Force vs Immovable Object

Aligning Goals

II. **SecDevOps: Take 1**

Automation Workflow

Gaps in the System

III. **SecDevOps : Take 2**

Security as Code

IAM for Machines

Secrets Management

User Management

IV. **What is Next?**

V. **Conclusion and Q&A**

Thank you!

Top Takeaways

1) Start conversations with all the stakeholders to address current security and compliance challenges
2) Map security and compliance best practice and principles into continuous delivery
3) Expect this to be iterative and evolving process

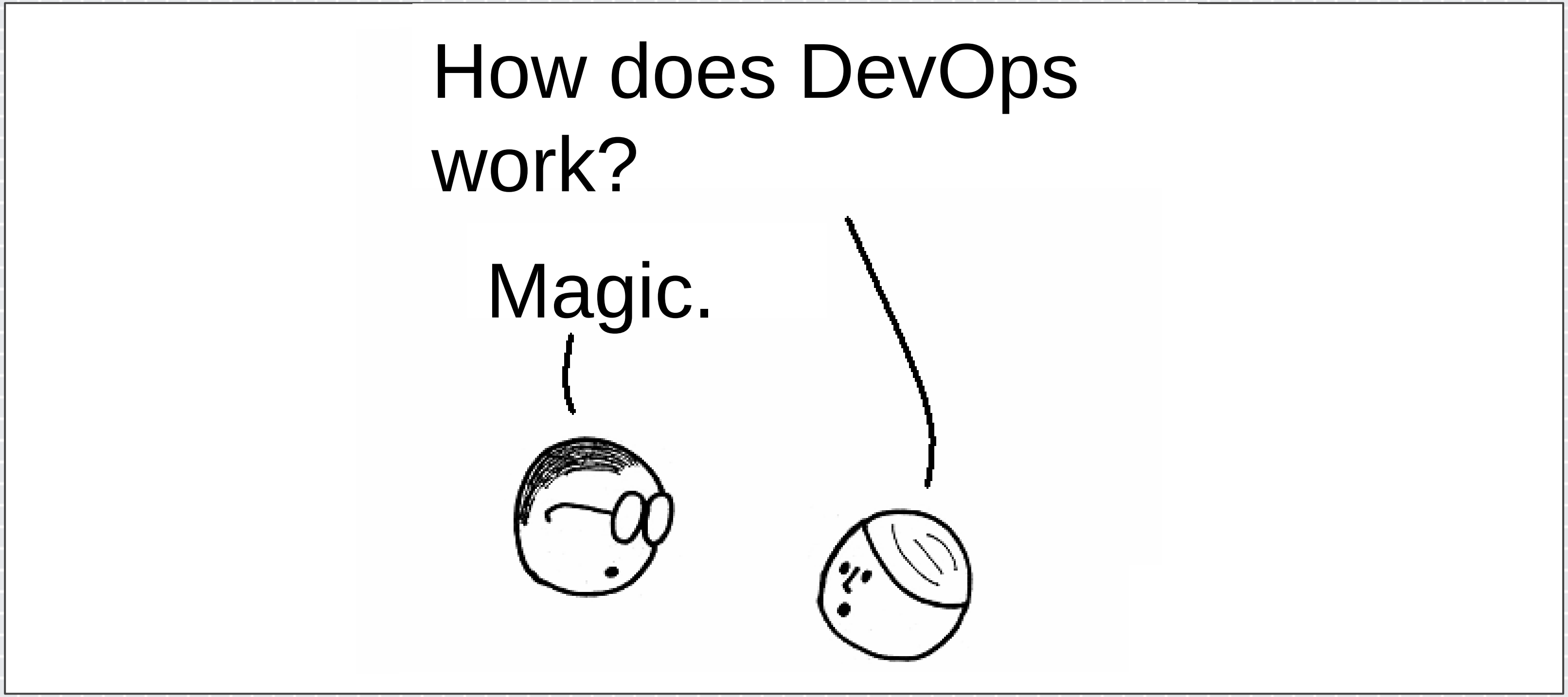
RSAConference2015

San Francisco | April 20-24 | Moscone Center

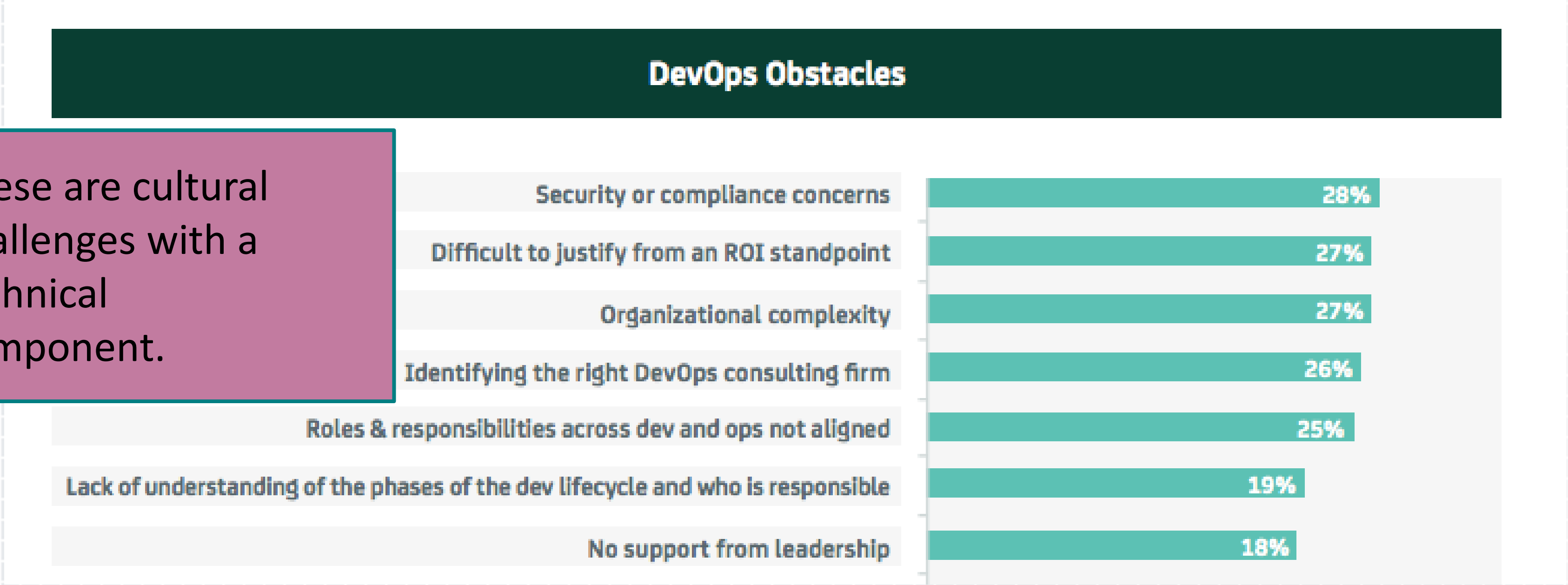
#RSAC

I. Security + DevOps Recap

DevOps: Powerful, But Hard To Understand



Security And Compliance Concerns Slow The Adoption Of DevOps



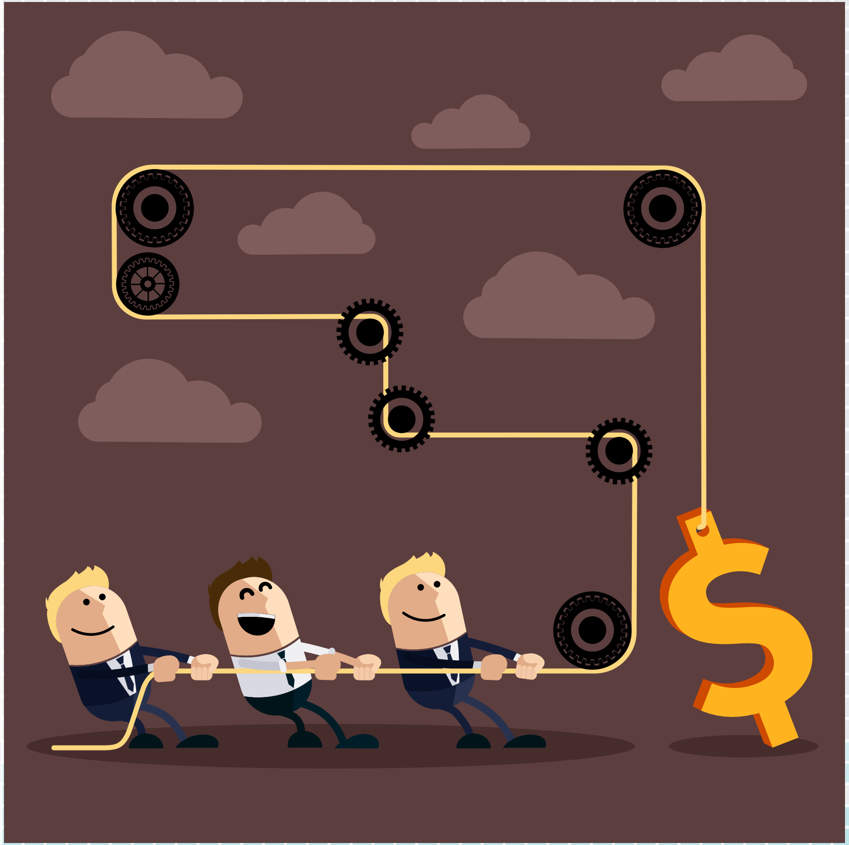
These are cultural challenges with a technical component.

Source: *DevOps: The Worst-Kept Secret to Winning in the Application Economy* by CA Technologies, October 2014 (http://rewrite.ca.com/us/~/media/rewrite/pdfs/white-papers/devops-winning-in-application-economy.pdf)

Cultural Challenges

We’re All In It Together

SEC



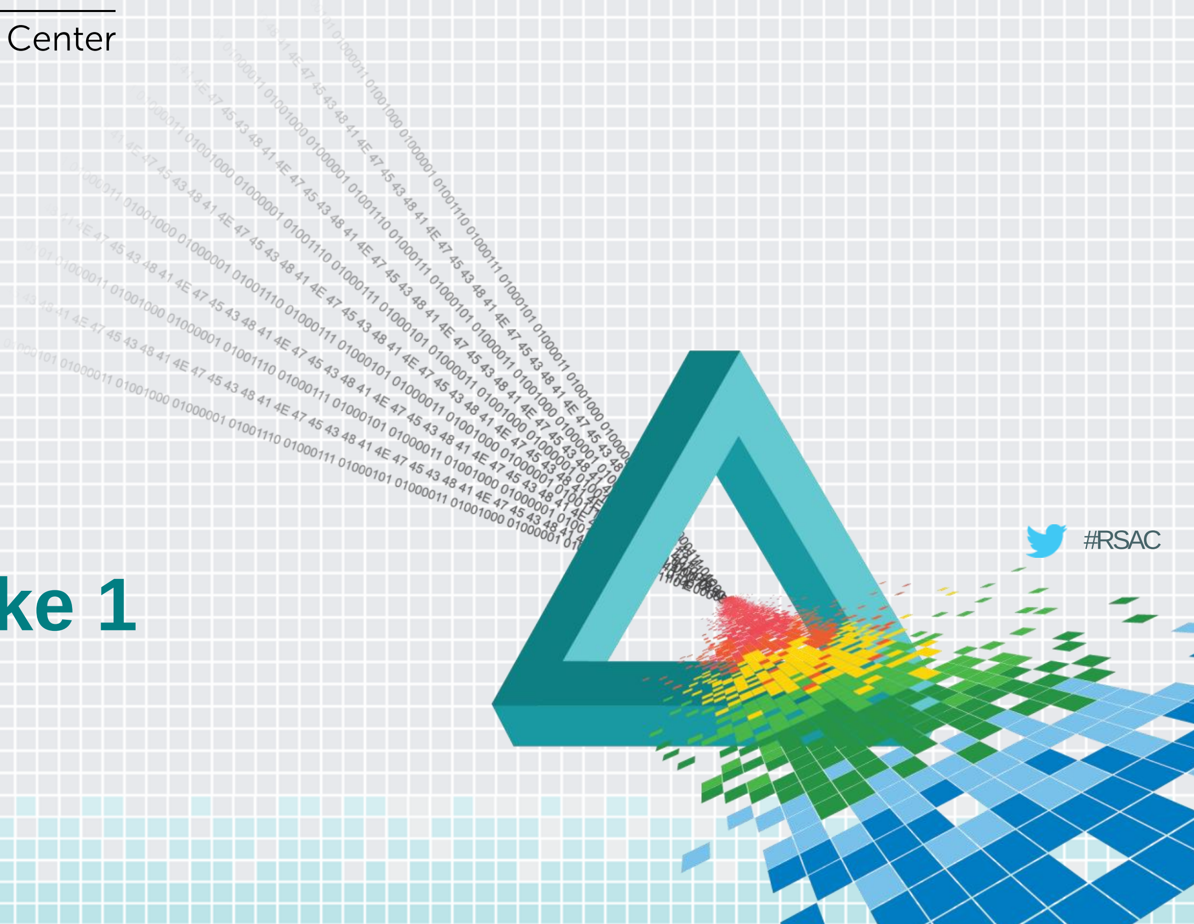
Q: Is DevOps Breaking Your Company?

A: No, but security may break (or brake) your DevOps!

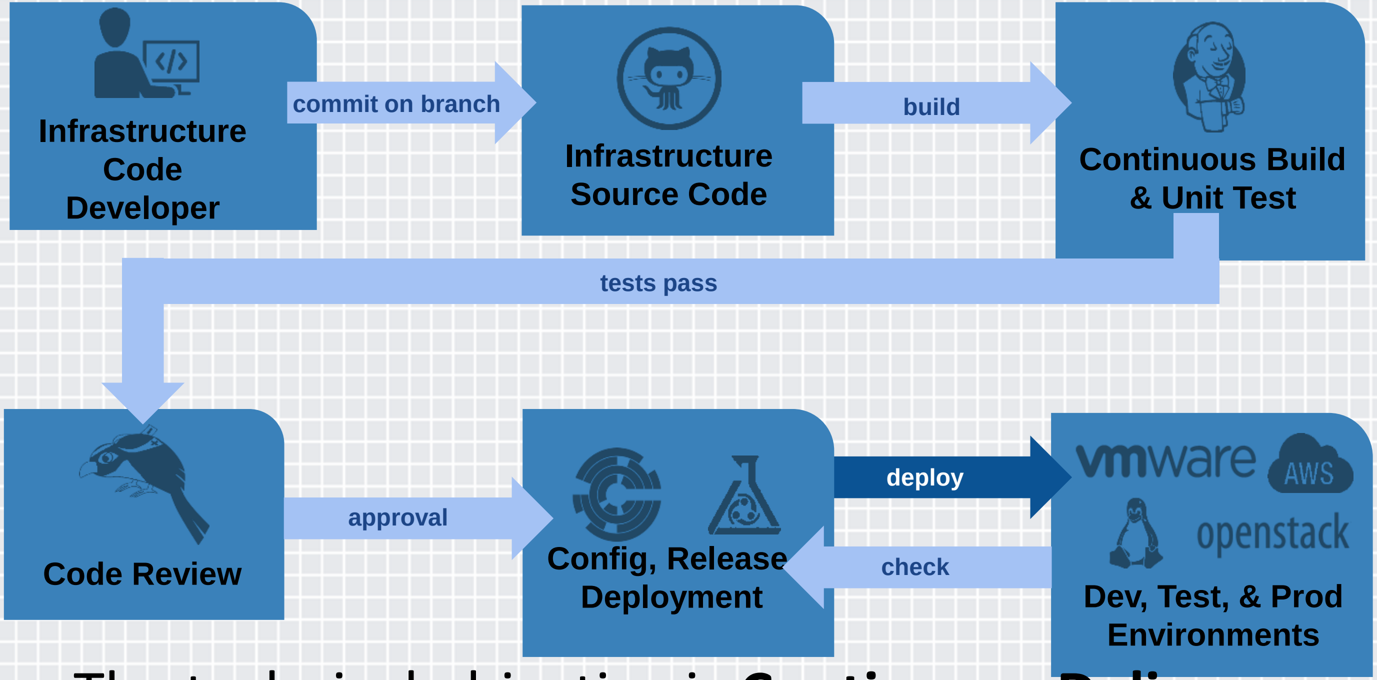
DevOps leverages a set of tools and processes that are constantly striving to go **faster**.

Some of these tools and processes don't easily lend themselves to information security best practices.

II. SecDevOps: Take 1



Holistic, Automated Processes To Build And Deliver Software/IT Infrastructure


Infrastructure Code Developer
commit on branch
Infrastructure Source Code
build
Continuous Build & Unit Test
tests pass
Code Review
approval
Config, Release Deployment
deploy
check
vmware
AWS
openstack
Dev, Test, & Prod Environments

The technical objective is **Continuous Delivery**

SecDevOps 1.0: Where Are We Today?

Source Control

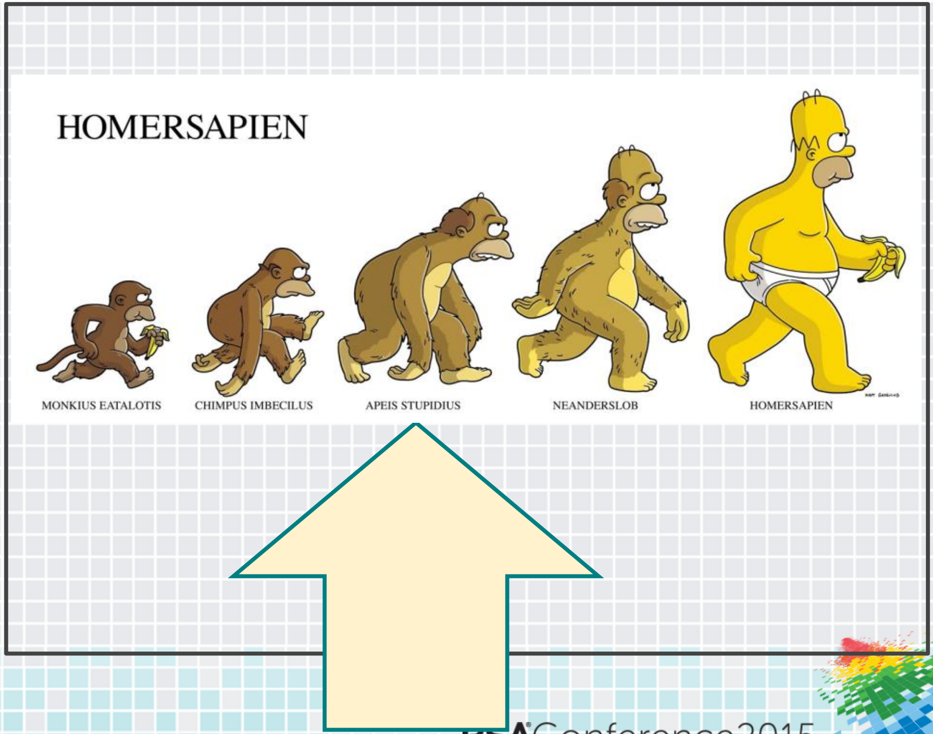
Automated Build and Test

Configuration Management

Orchestration

Software-Defined Networking

Monitoring

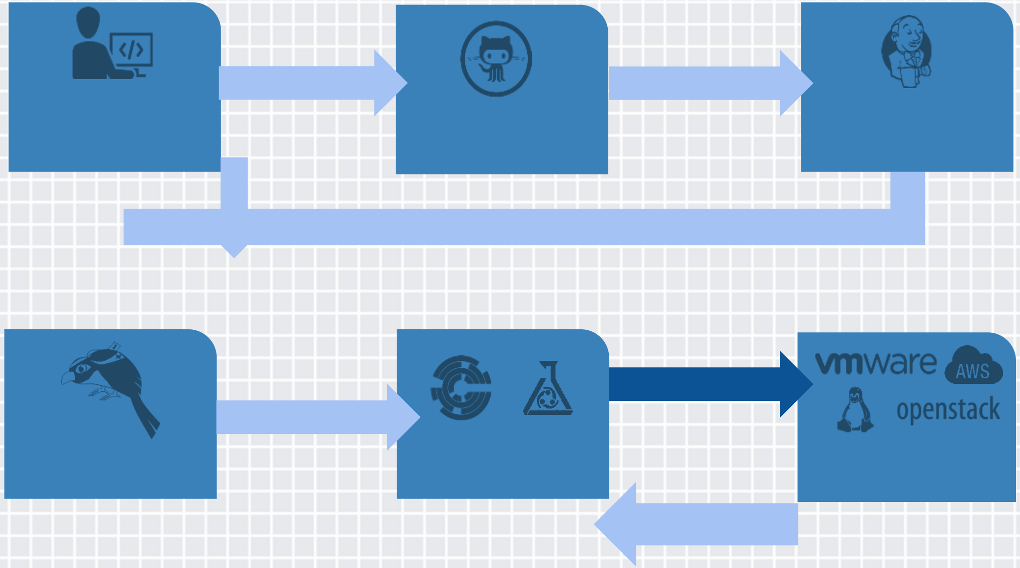


Let's Create : Continuous Compliance

- Robust security and compliance controls

  … with

- Full support for automation



SecDevOps 1.0: Security Challenges

Code is the sys and security admin

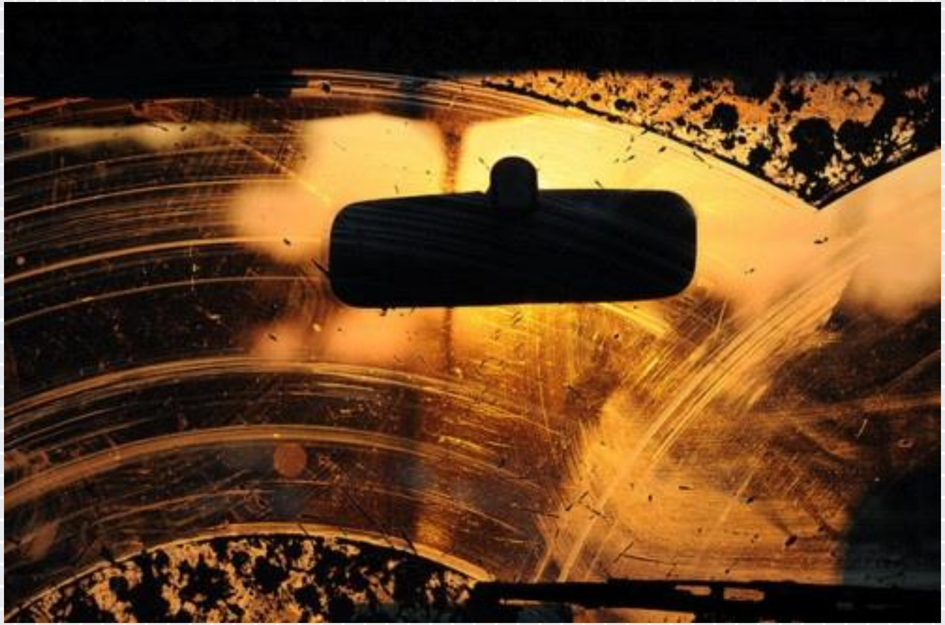
Automation is a Force Multiplier

SecDevOps 1.0: Missing Transparency

“Automated and traceable authorizations of promotion”

“RBAC (for) access to production systems with documentation”

“Encryption and logical access controls that lock out unauthorized access”



Adapted from Brightline https://www.brightline.com/2012/12/auditing-devops-developers-with-access-to-production/

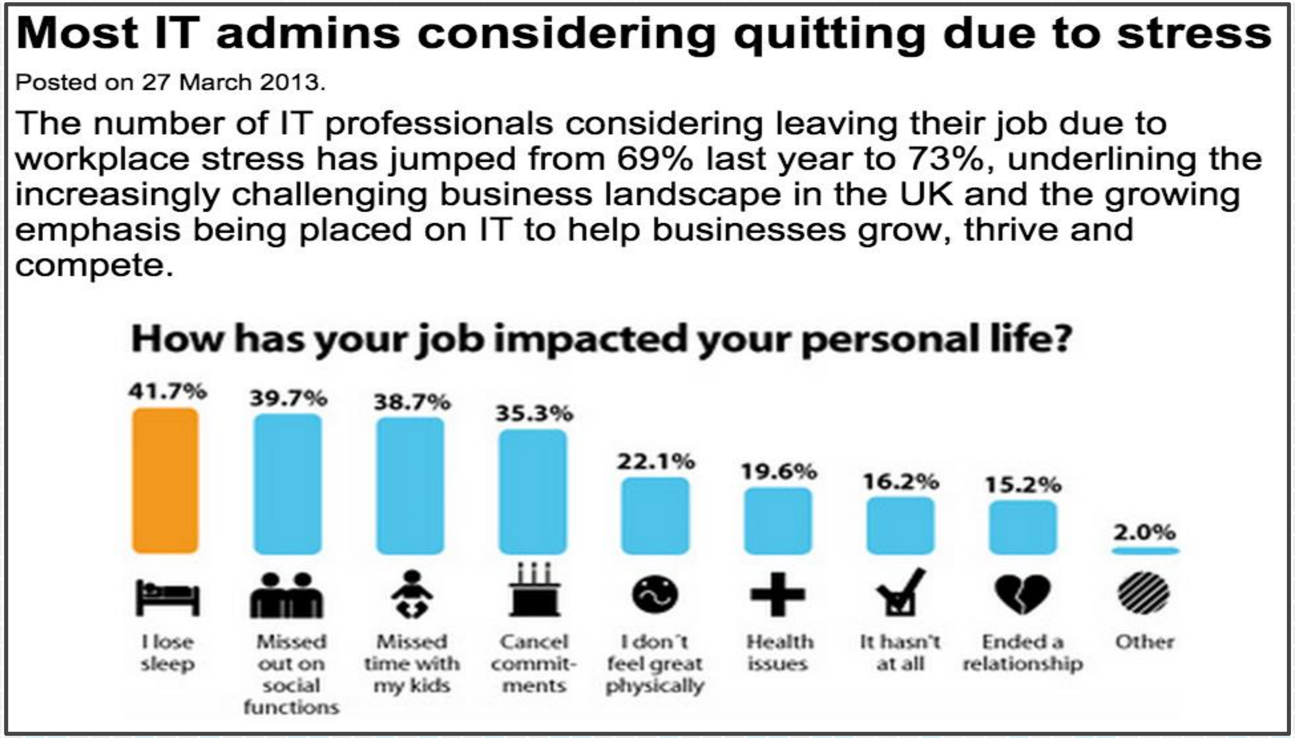
Wrong Tools For The Job

Anti-Pattern: Production-only Workflows

Problem: security controls that developers cannot replicate locally

Result: Speed-killer

Anti-Pattern: Human Bottlenecks



Most IT admins considering quitting due to stress

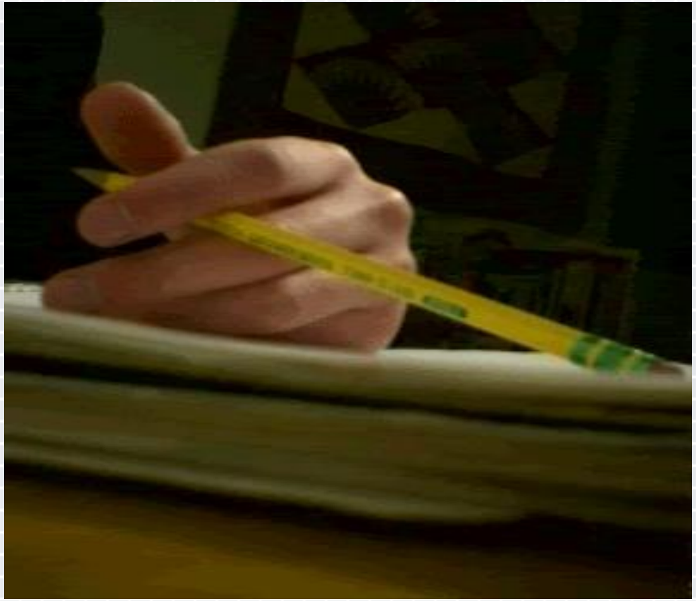
Posted on 27 March 2013.

The number of IT professionals considering leaving their job due to workplace stress has jumped from 69% last year to 73%, underlining the increasingly challenging business landscape in the UK and the growing emphasis being placed on IT to help businesses grow, thrive and compete.

Anti-Pattern: Conflation of Concerns

Config Management as a DIY Security System

Anti-patterns create "Security Debt"

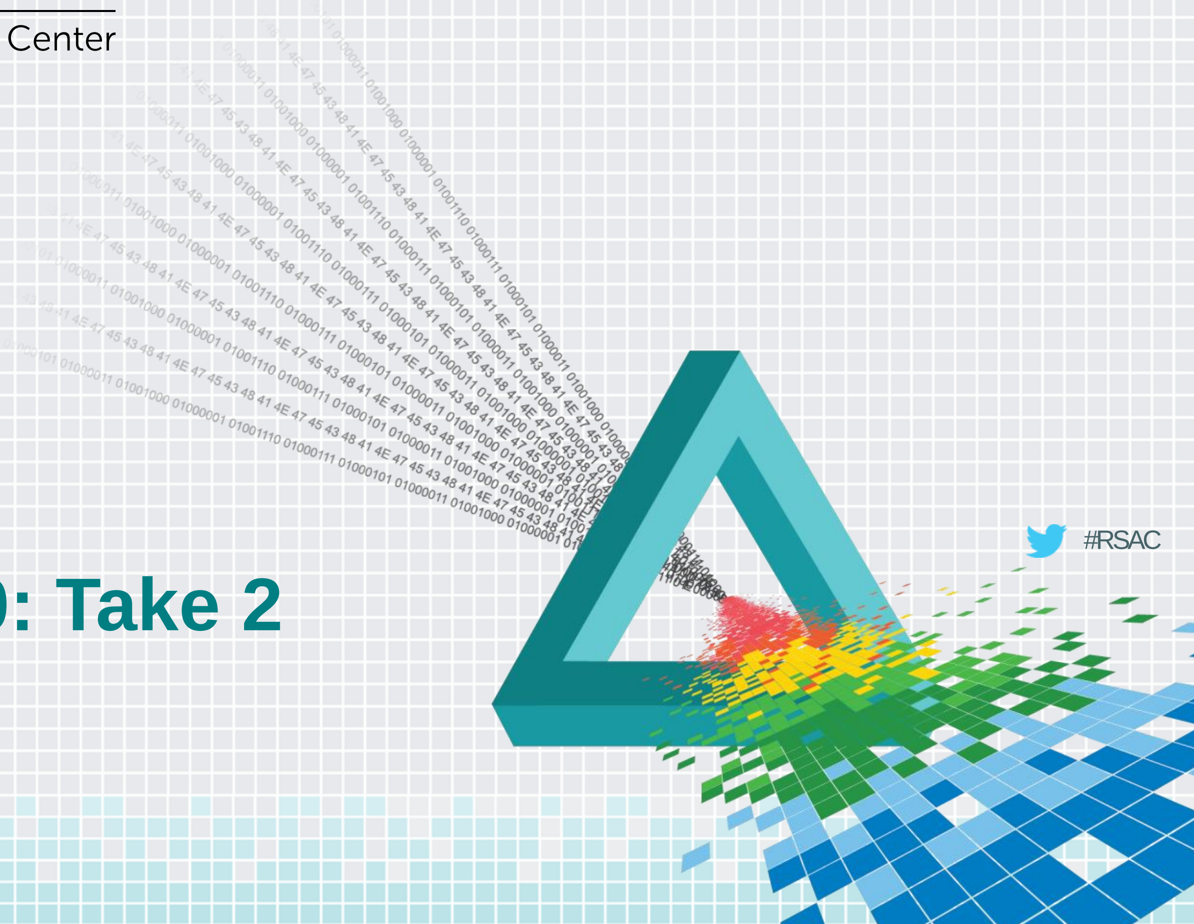
New Product Feature	New Security Feature
	

Addressing security bottlenecks and issues are often deferred, until...

Worst-Case Scenario?

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

III. SecDevOps 2.0: Take 2

SecDevOps 2.0: High-Level Goals

1. Enforce principles of least privilege and access control in the “coded” workflow

1. Reduce security misadventures and “whoops” moments

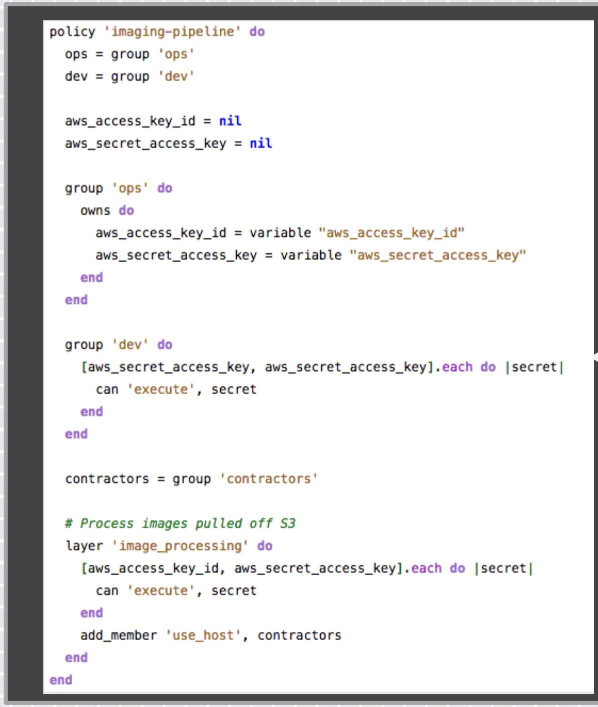
1. Highly durable and scalable - like the cloud itself

2. Audit everything, including automation exceptions (one-off builds)

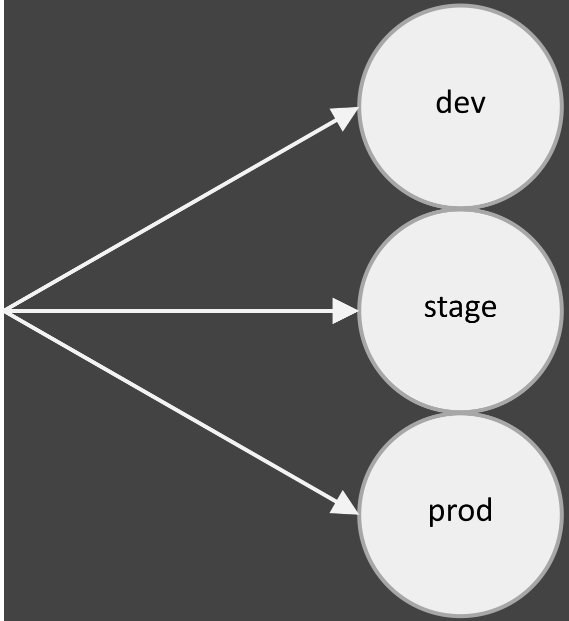
We Need To Rethink How We Define Policies, Identities And Networks In A Way That...

- *Works with automation*
- *Supports agile development and continuous delivery*
- *Intuitive to compliance teams and stakeholders*

SecDevOps 2.0: Security Policy As Code

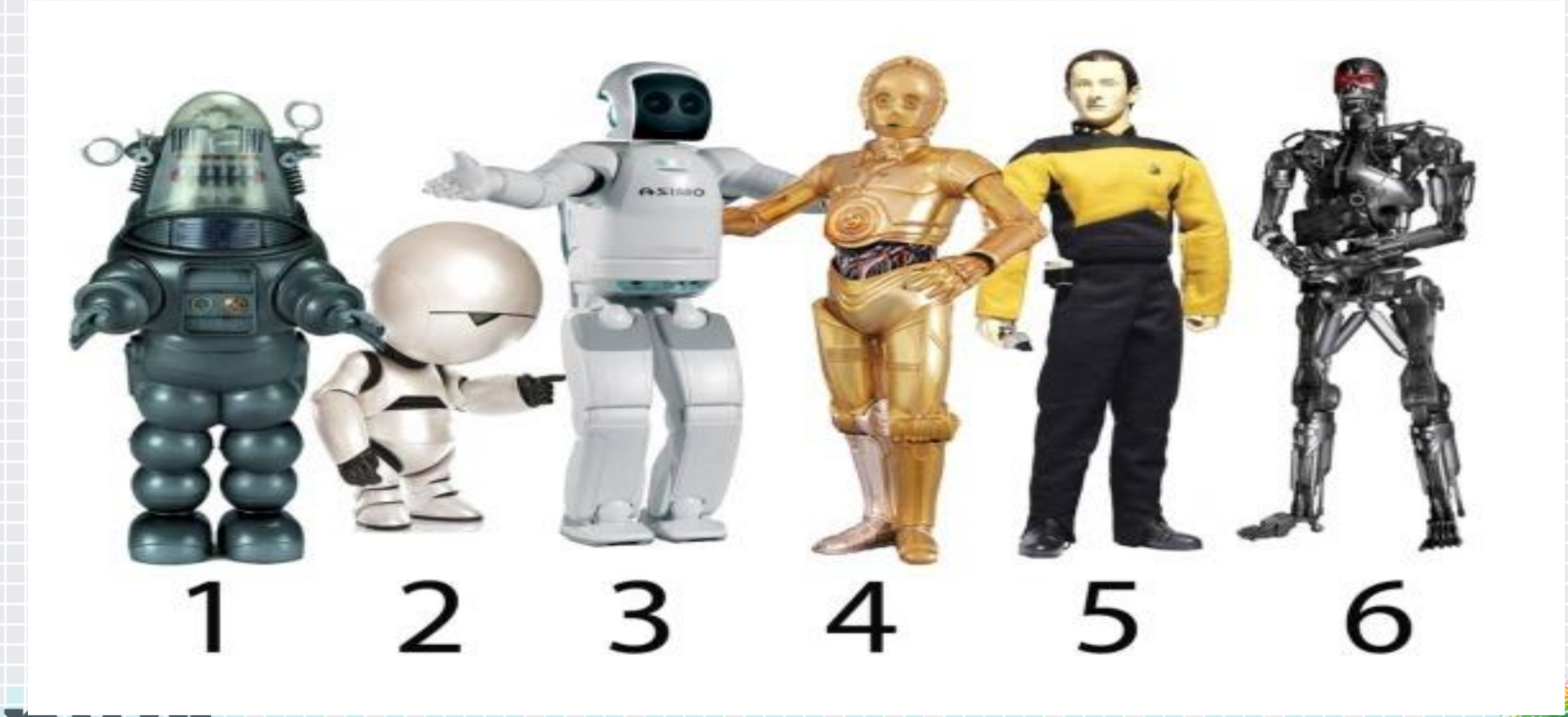


```
policy 'imaging-pipeline' do
  ops = group 'ops'
  dev = group 'dev'

  aws_access_key_id = nil
  aws_secret_access_key = nil

  group 'ops' do
    owns do
      aws_access_key_id = variable "aws_access_key_id"
      aws_secret_access_key = variable "aws_secret_access_key"
    end
  end

  group 'dev' do
    [aws_secret_access_key, aws_secret_access_key].each do |secret|
      can 'execute', secret
    end
  end

  contractors = group 'contractors'

  # Process images pulled off S3
  layer 'image_processing' do
    [aws_access_key_id, aws_secret_access_key].each do |secret|
      can 'execute', secret
    end
    add_member 'use_host', contractors
  end
end
```

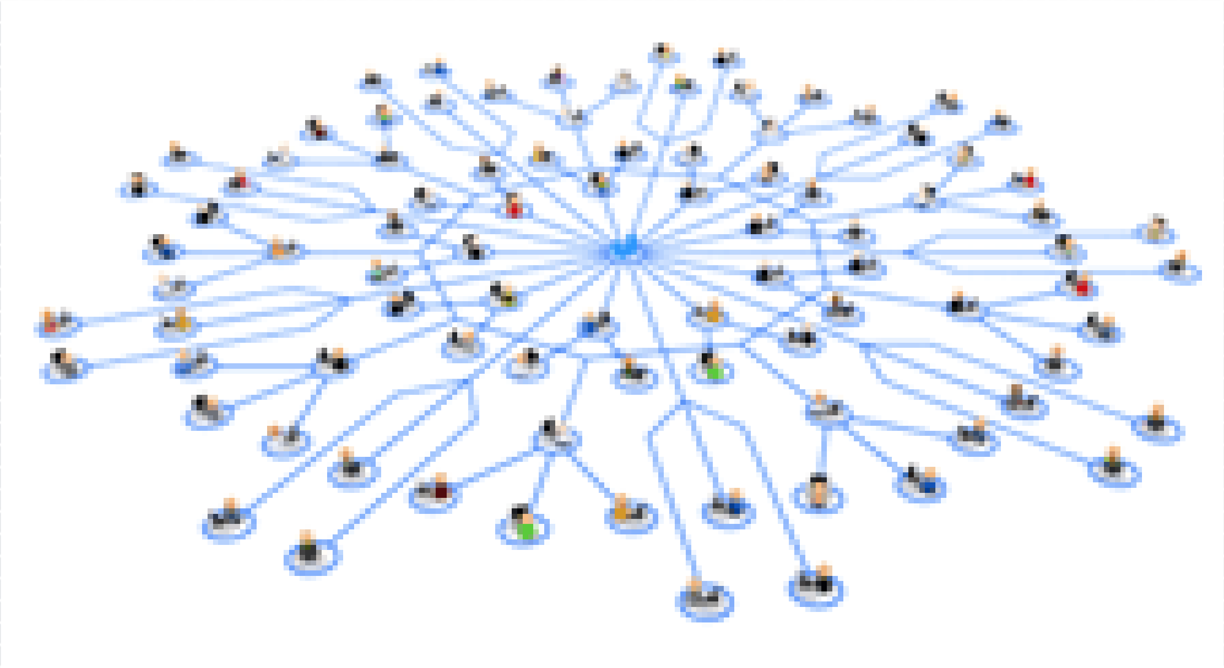


Conjur Policy DSL

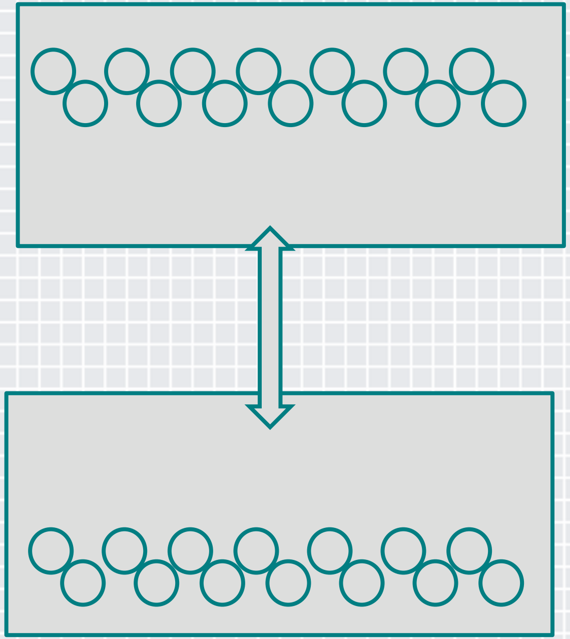
SecDevOps 2.0: IAM For Machines At Scale



SecDevOps 2.0: IAM For Machines At Scale

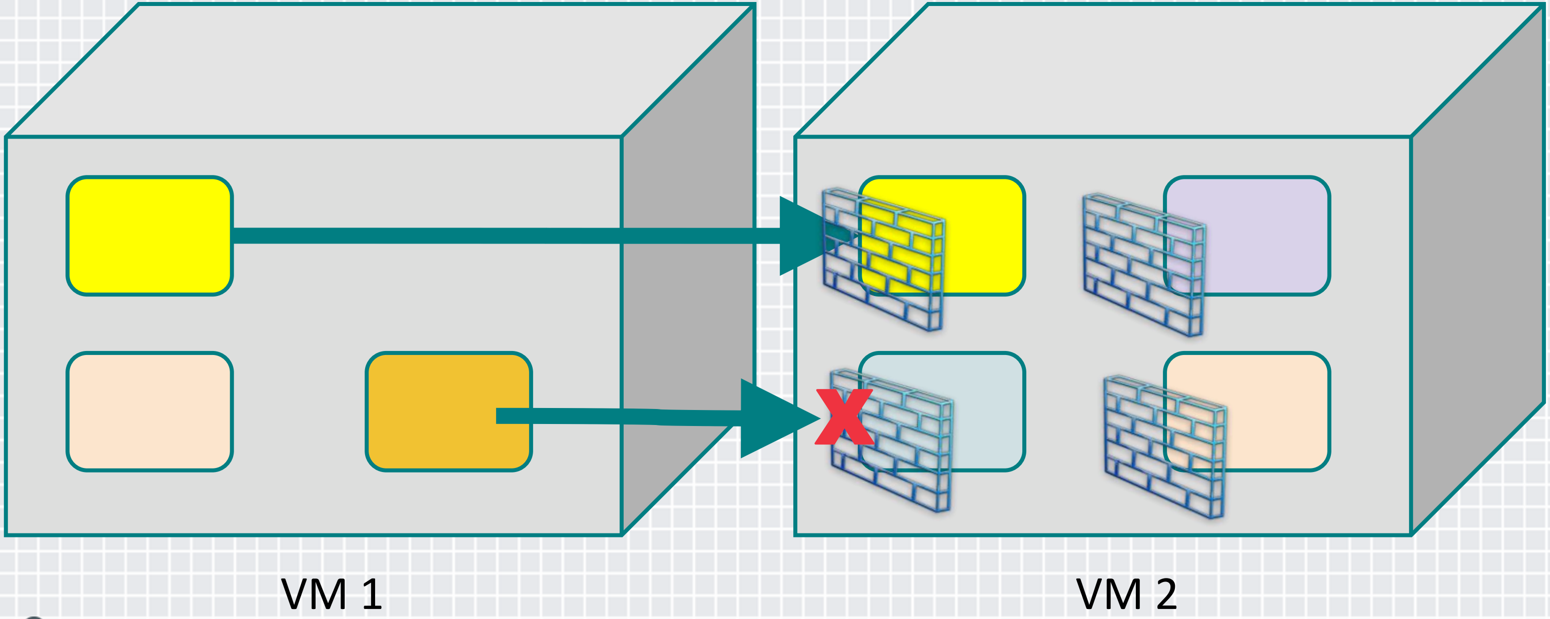


SecDevOps 2.0: Software-Defined Firewall

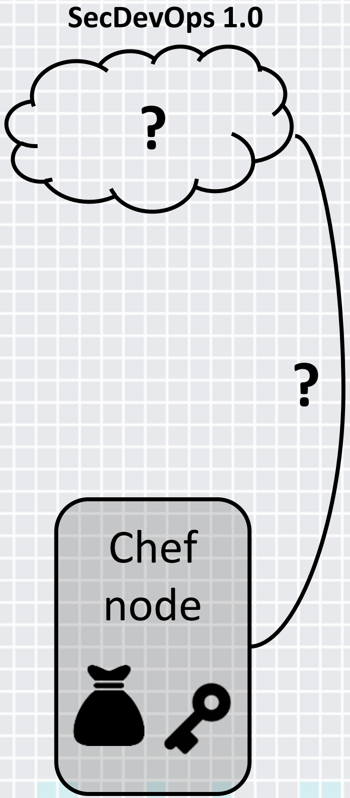


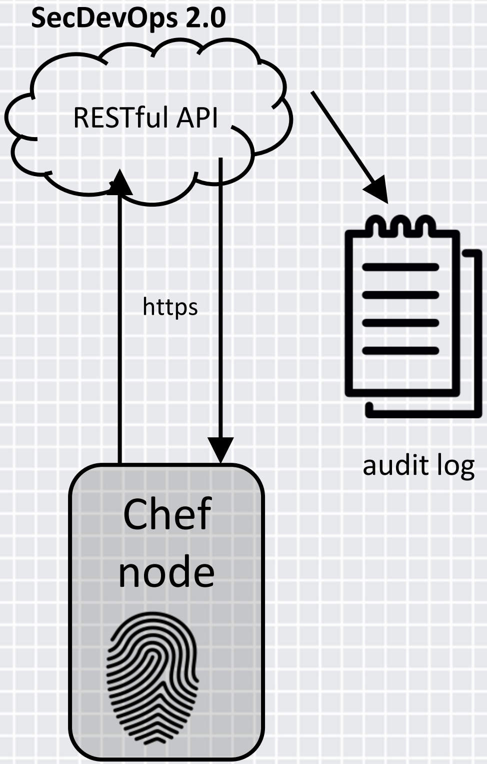
- Use Foundation/Golden Images to "bake in" trust in core services, such as identity management, configuration management, secrets-as-a-service and audit
- Providing secrets to docker containers
- Security Gates

SecDevOps 2.0: Software-Defined Firewall

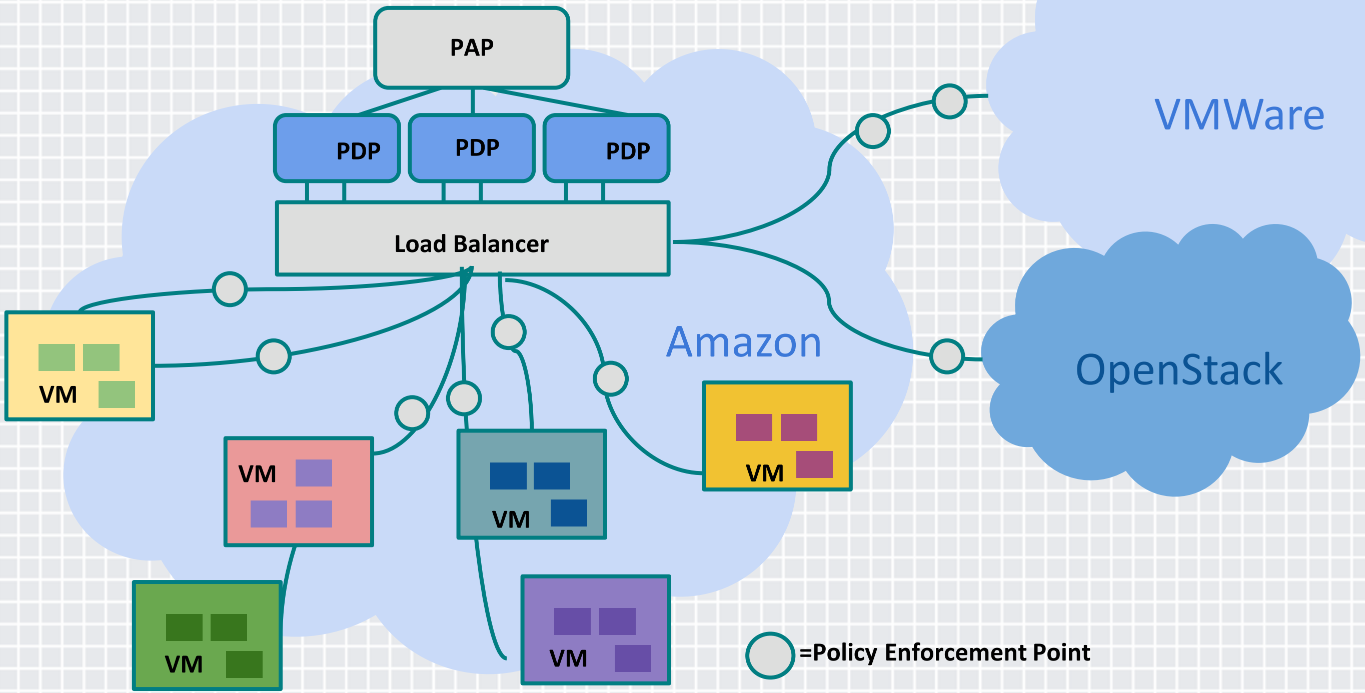


SecDevOps 2.0 Secrets Service

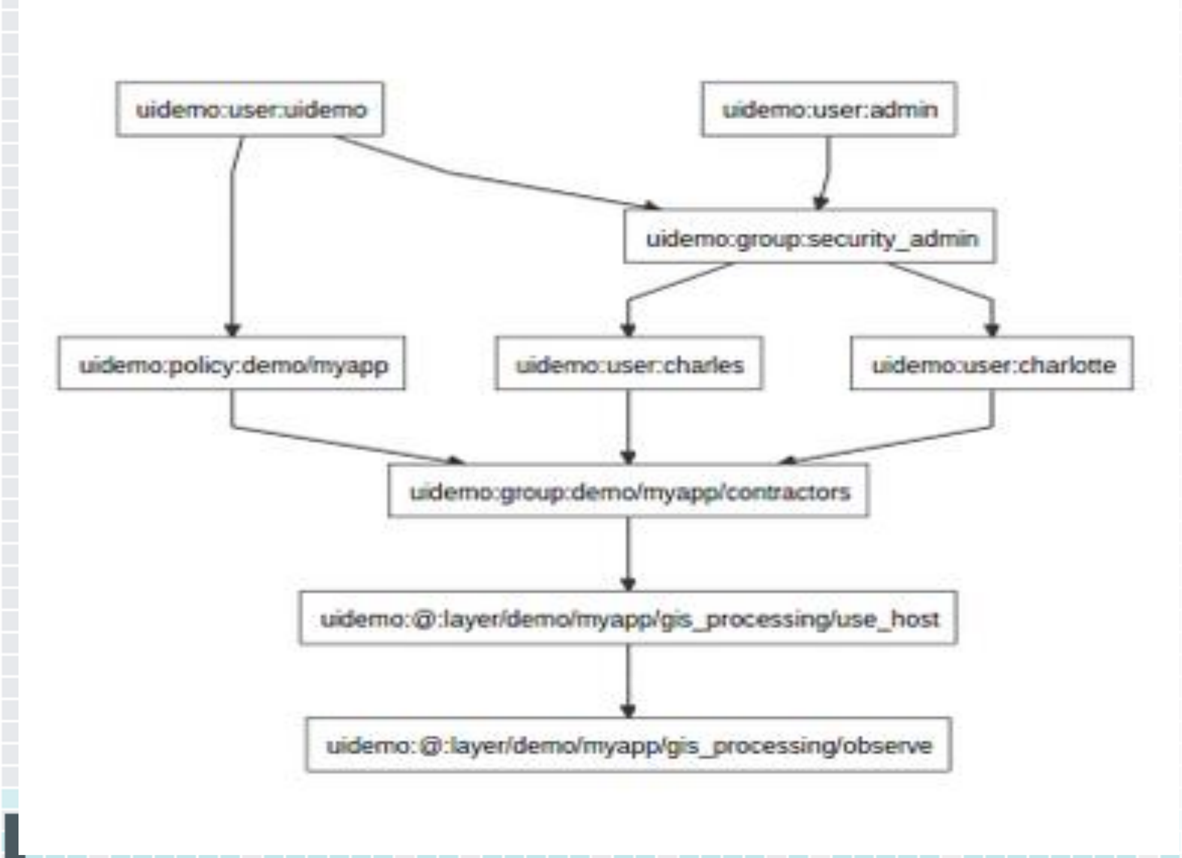




SecDevOps 2.0: Software-Defined Firewall

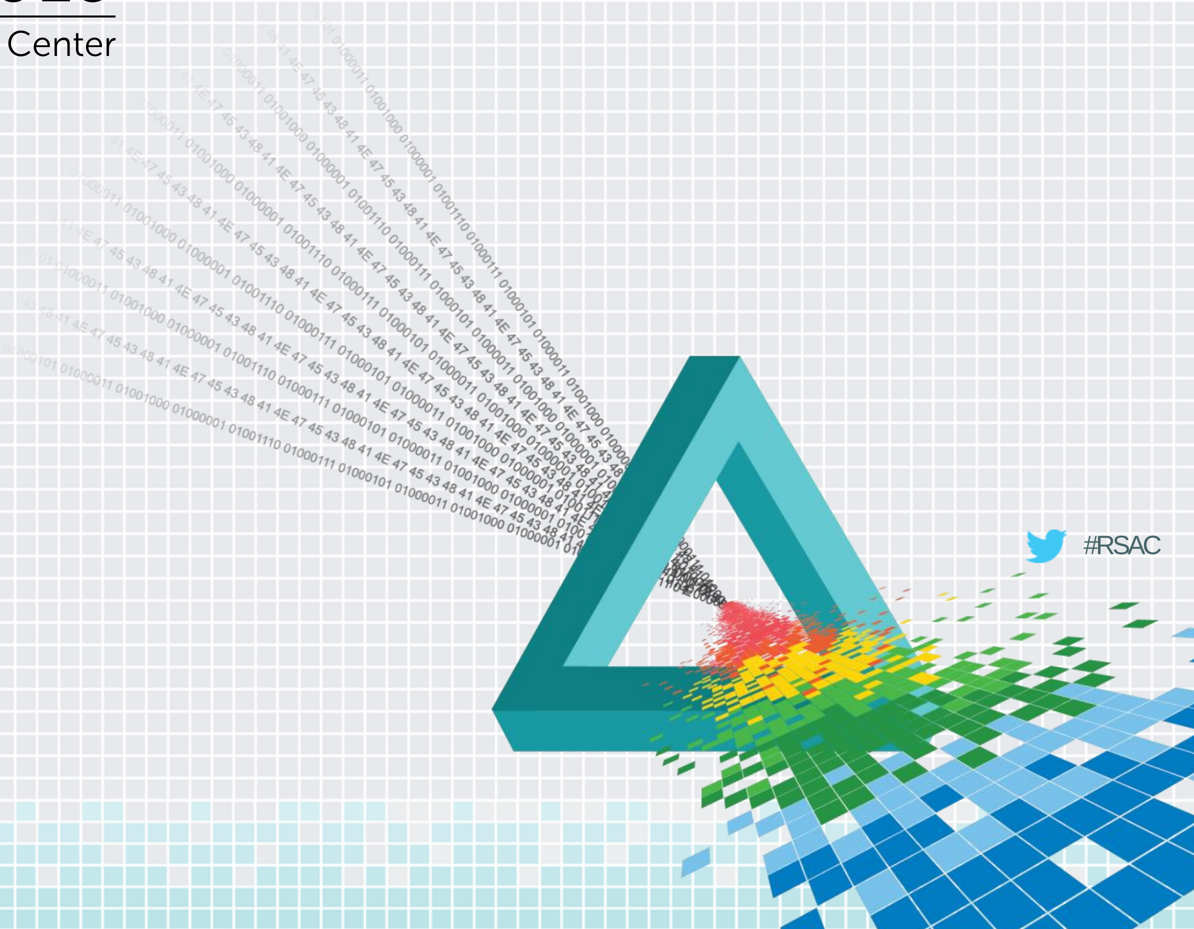


Result: Clear Controls And Processes


uidemo:user:uidemo
uidemo:user:admin
uidemo:group:security_admin
uidemo:policy:demo/myapp
uidemo:user:charles
uidemo:user:charlotte
uidemo:group:demo/myapp/contractors
uidemo:@:layer/demo/myapp/gis_processing/use_host
uidemo:@:layer/demo/myapp/gis_processing/observe

RSAConference2015

San Francisco | April 20-24 | Moscone Center



#RSAC

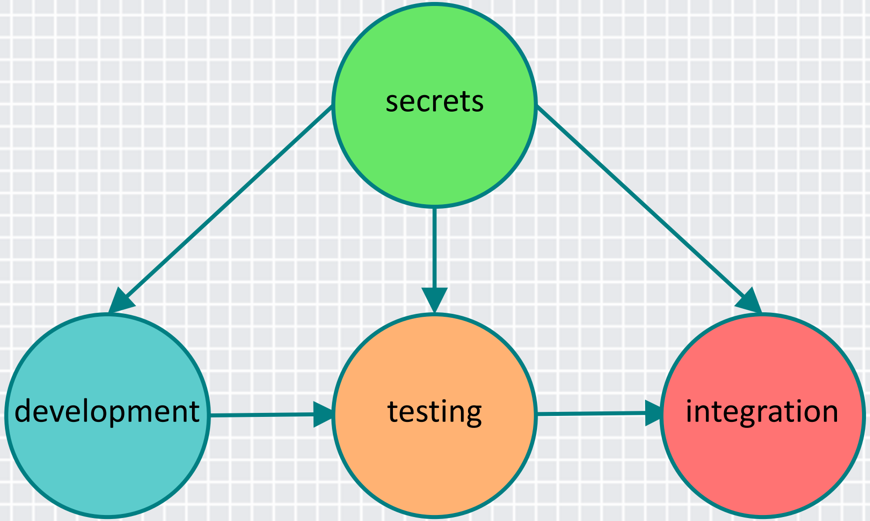
I. What is Next?

Opportunities To Improve DevOps Practices

- Provide a facility outside of operational tools to access/include sensitive information.
- Create multiple environments organized by risk.
- Audit everything, including automation exceptions (one-off builds).

Development Centric Security

Key is securing the developer in their natural workflow, not forcing a flow that can lead to errors & omissions

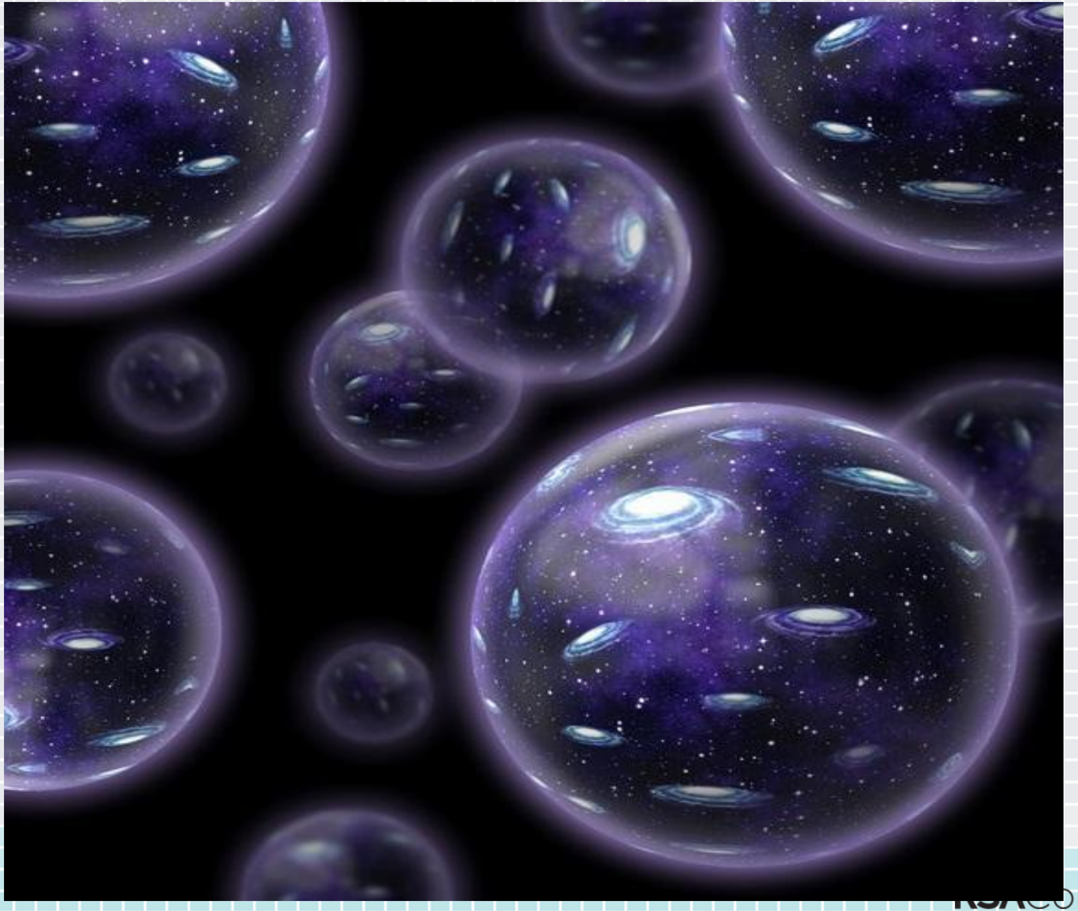


New Tools : Control Plane Microservices

- Delegate routine tasks to trusted microservices that are governed by highly limited access control policies and continuously audited

- Use Foundation/Golden Images to "bake in" trust in core services, such as identity management, configuration management, secrets-as-a-service and audit

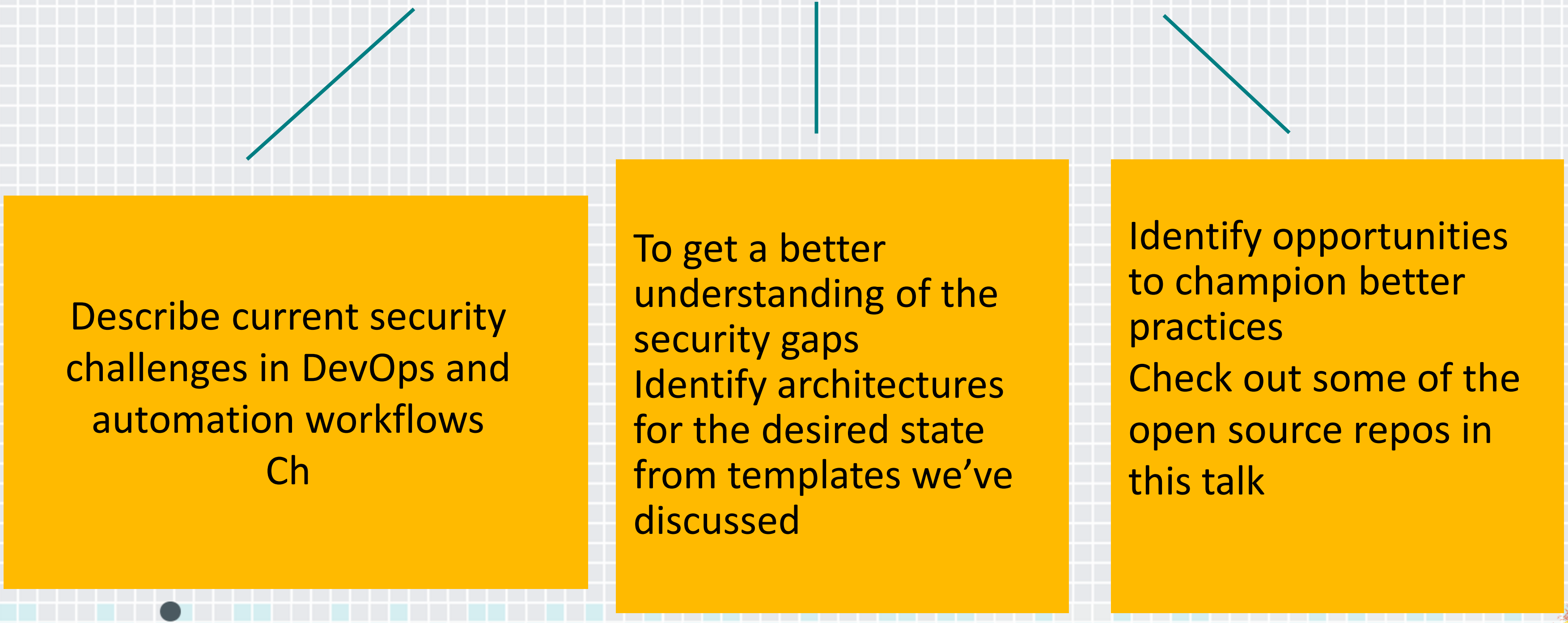
New Approaches: Microdev environments?



Top Takeaways

1) Start conversations with all the stakeholders to address current security and compliance challenges
2) Map security and compliance best practice and principles into continuous delivery
3) Expect this to be iterative and evolving process

Educate + Learn = Apply

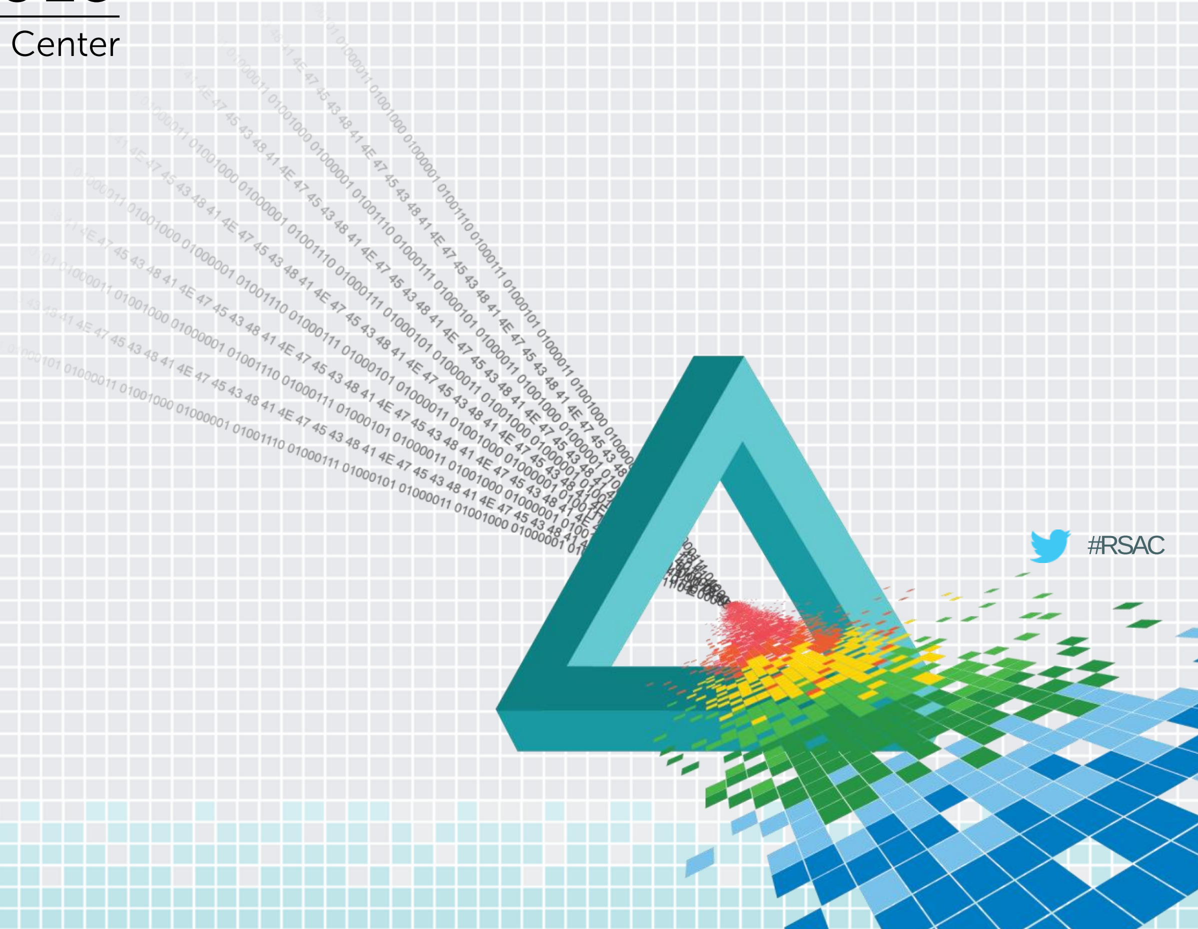


Describe current security challenges in DevOps and automation workflows
Ch

To get a better understanding of the security gaps
Identify architectures for the desired state from templates we've discussed

Identify opportunities to champion better practices
Check out some of the open source repos in this talk

IV. Q & A



Thank You!

Additional Questions? Let’s Connect…

Elizabeth Lawler

- email: elawler@conjur.net
- phone: (617) 906-8216
- web: www.conjur.net
- twitter: @elizabethlawler /@conjurinc