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

Tool Chain AKA Dev Ops Workflow

Wrong Tools for the Job

II. **SecDevOps 2.0: Defined**

Motivation and Requirements

Policy, Identity and Network 2.0

Best Practices

III. **SecDevOps 2.0: In Practice**

New Tools

Case Study

Takeaways

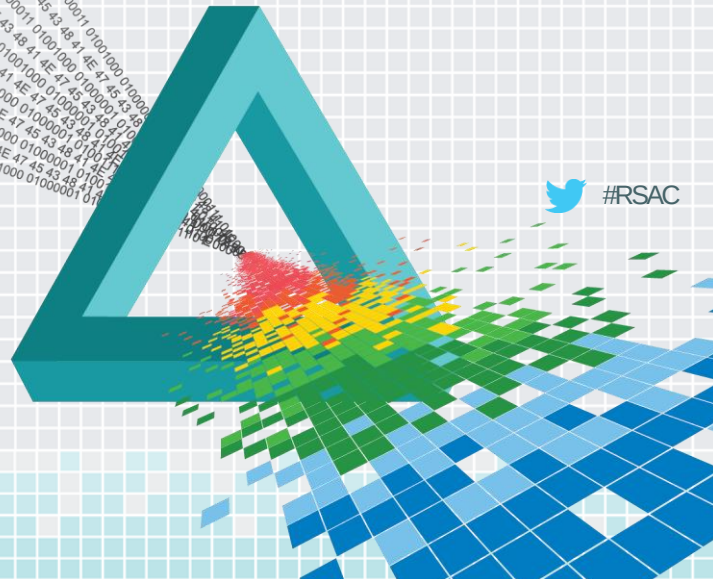
IV. **Q&A**

Thank you!

RSAConference2015

San Francisco | April 20-24 | Moscone Center

I. Security + DevOps Overview



#RSAC

Adoption of DevOps Is Driven By Business Concerns

- High-performing organizations are deploying code 30 times more often with 50% fewer failures
- High IT performance correlates with strong business performance, helping to boost 2x an enterprise's productivity, profitability, and market share

https://puppetlabs.com/2014-devops-report

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**.

These tools and processes don’t easily lend themselves to *some* existing information security best practices.

Security And Compliance Concerns Slow The Adoption Of DevOps

#RSAC

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

This Needs To **Stop!**

We're All In It Together

Your business *needs* DevOps to succeed in order to thrive and survive.

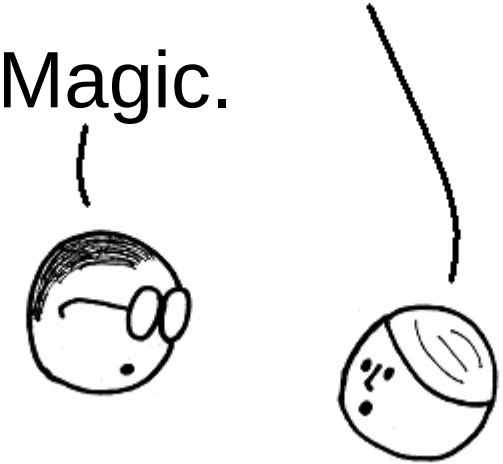
Security and **Compliance** *need* transparency and to participate in building out a safe and secure DevOps process.

Dev and **Ops** *need* buy-in on the transformative potential of agility and automation from Security and Compliance.

DevOps: Powerful, But Hard To Understand

How does DevOps work?

Magic.

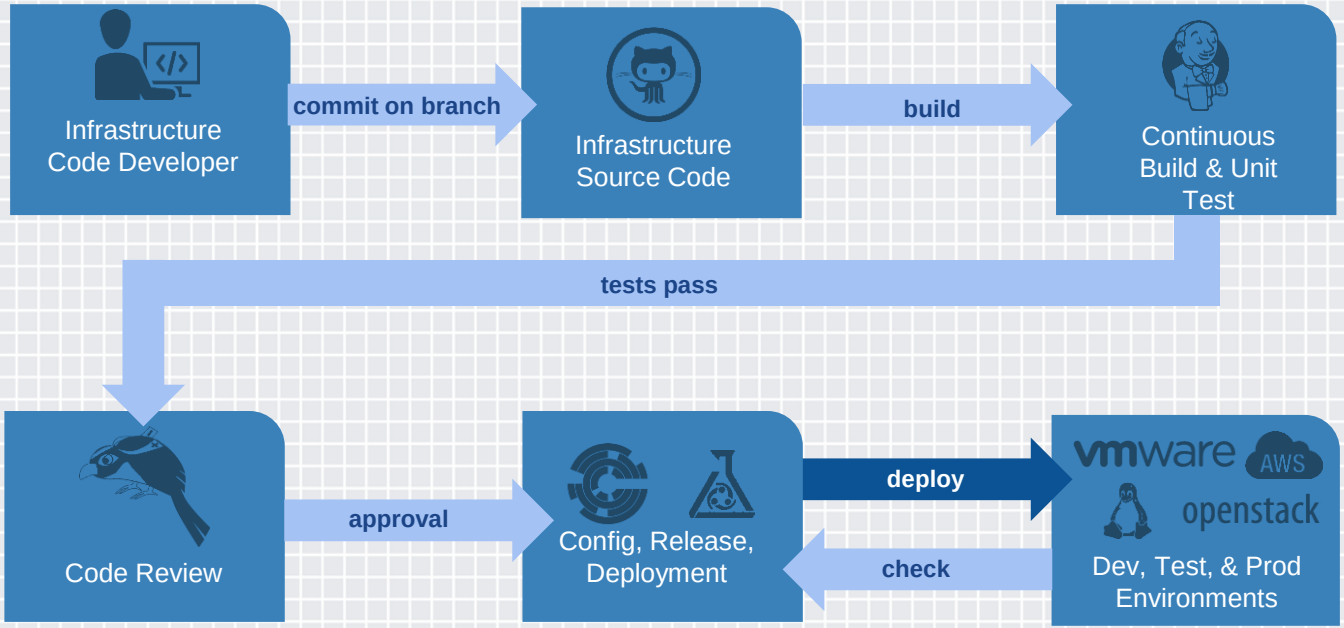


Start The Conversation!

- Security, Compliance, Developers, and Operations need personal relationships and mutual understanding.
- Differences in language: The way that security, compliance, developers and ops talk about the same problem can be bridged.
- Everyone has a right to transparency and clear understanding of how things work.

II. SecDevOps 2.0: Defined

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



The technical objective is **Continuous Delivery**

DevOps: Not Your Old Architecture

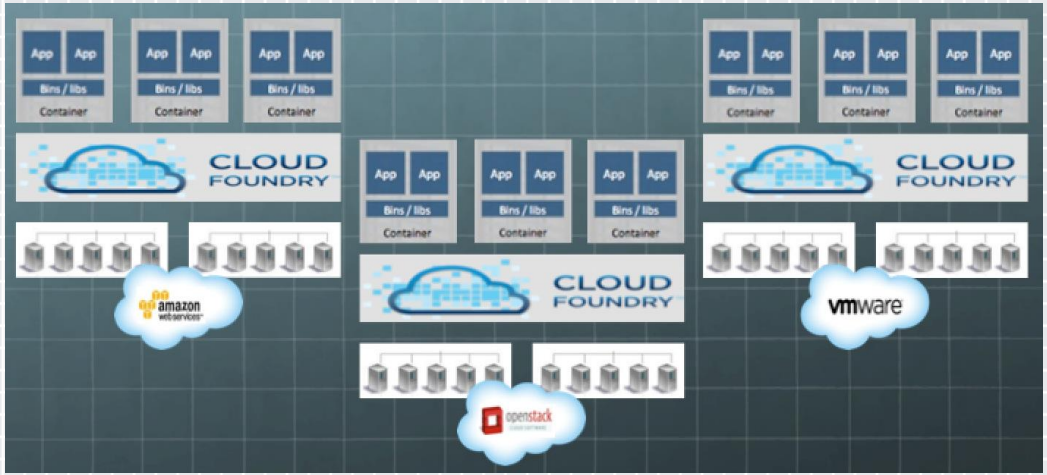
- Same packages
- Same configuration

  … and…

- Same security and compliance controls

  … with …

- Full support for automation



Continuous Delivery: Security Standpoint

Code is the new privileged user/sys admin

- Who and what can touch the code is critical to security
- Fewer people → more trusted services
- Machine identity and trust is critical

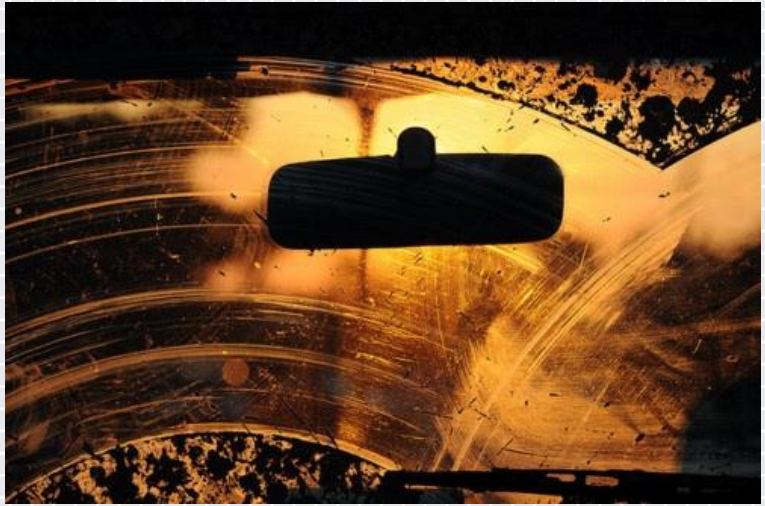
Automation is a Force Multiplier and a Double- Edged Sword

- Good: Patch management
- Bad: Introduce vulnerability “globally” with a push of button
- Ugly: Catastrophic failure

Continuous Delivery: Compliance Standpoint

Lack of transparency is the #1 obstacle to compliance

- Policies are buried in code
- Lack of well-defined management tools makes change controls hard to define
- Little to no visual reporting of access controls and system activity



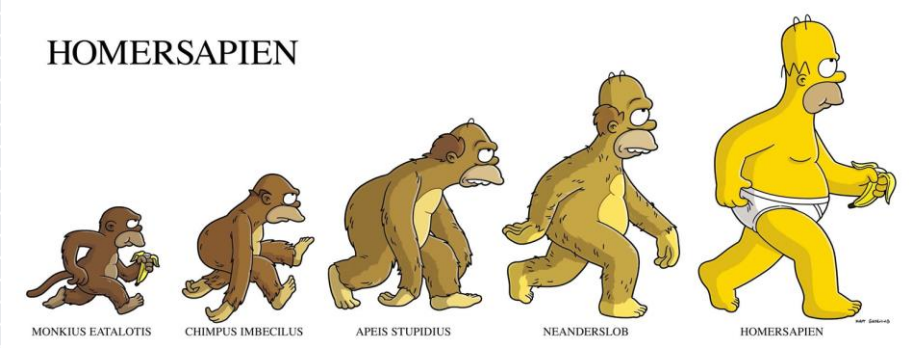
SecDevOps 1.0: Security Challenges That Have Already Been Well-Addressed

Source Control

- Audit and provenance of source code Cloud APIs
- Network isolation / security groups
- Machine inventory

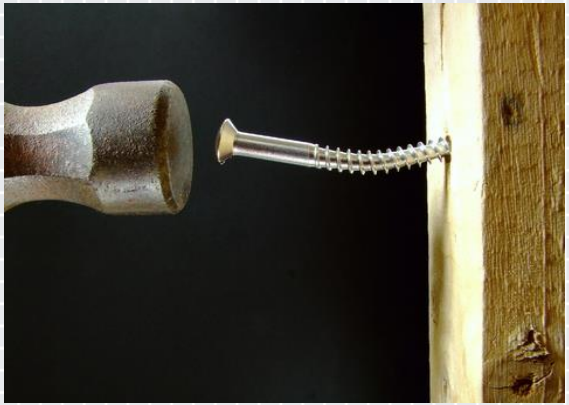
Configuration Management

- Reproducible images and application deployment
- Patch management
- Build and test automation
- Software validation



Wrong Tools For The Job

"Sometimes when all you have is a hammer, everything looks like a nail."



- SCM: Collaboration, not least privilege
- CI: Powerful system accounts
- Configuration Management (Puppet/Chef): not secrets management

Anti-Pattern: Production-only Workflows

Problem: security controls that developers cannot replicate locally

Result: Speed-killer

Anti-Pattern: Human Bottlenecks

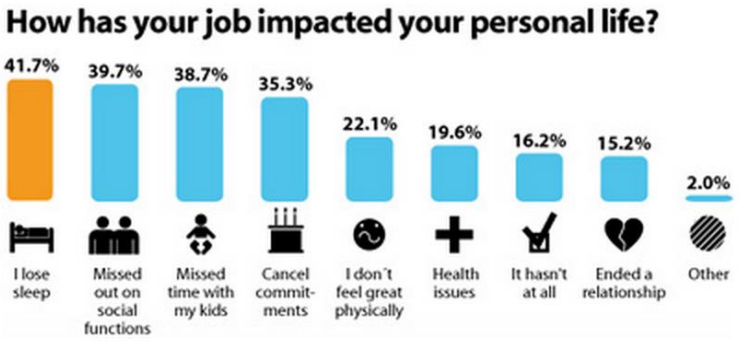
Problem: Security controls that require manual intervention for routine tasks

Result: Tech resources are wasted on trivial tasks, unclear organizational ownership of tasks, throughput suffers, and so does morale.

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.



"Cool" DIY security projects become albatrosses

Anti-Pattern: Conflation of Concerns

Problem: Security controls embedded in systems that weren't designed with security as their primary purpose.

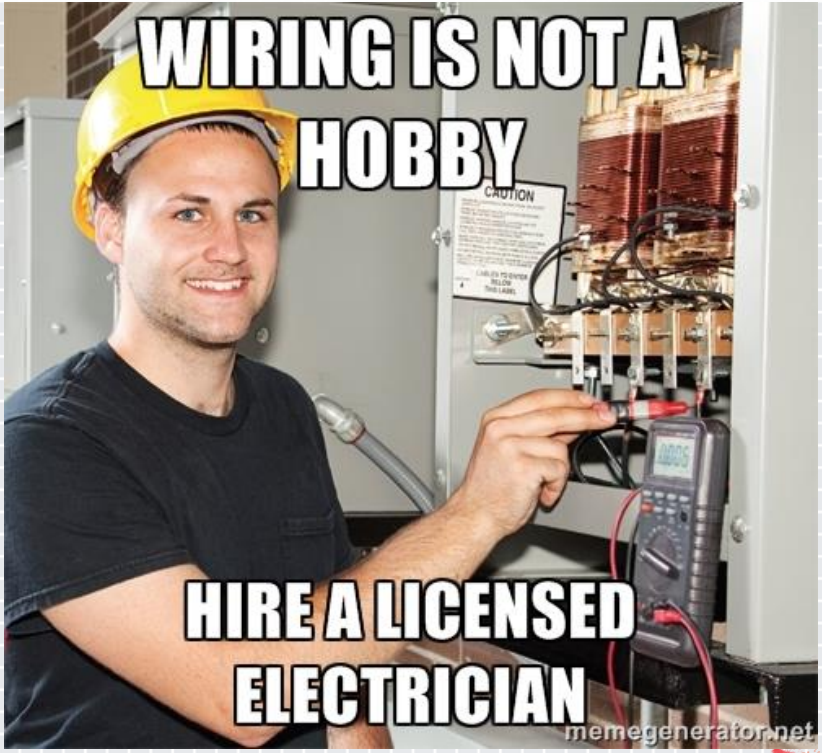
Result: Agility is sacrificed.

Configuration Management Is Not For Secrets

Two orthogonal concerns:

1. Install packages and establish configuration settings.
2. “Wire up” the system with identity and secrets.

System “wiring” should **not** be in the domain of configuration management.



Anti-patterns create “Security Debt”

New Product Feature	New Security Feature
	

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

Worst-Case Scenario? Full Stop

- Regulated Workloads Aren't Brought into the DevOps arena
- Security Incident
  - Breach or unauthorized access because of workflow challenges in getting the job done
- Static Workflow Caps Velocity
  - Changing is too hard or too risky

Mind The Gap: The Access Control Automation Gap

Challenges in mapping the organization to dynamic infrastructure:

- Practical Separation of Duties
- Least Privilege Access via Role-Based Access Control
- Audit and Reporting

Firewall
Application Auth
Systems Access
Control Plane
Internal Network
Physical Infrastructure

III. SecDevOps 2.0: In Practice

SecDevOps 2.0: High-Level Goals

1. Enforce principles of least privilege in the workflow
1. “Separation of duties” for automated systems & DevOps personnel
1. Reduce misadventures and “whoops” moments
1. Highly durable and scalable - like the cloud itself

This Is More Than A “Nice To Have”

- Organizational understanding of the Trust Model of the Infrastructure requires demonstrable controls
- Building a scalable trust model requires drilling into the details of each Sec + Dev + Ops concern and addressing the cultural, technical and tooling gaps.
- From who, or what, does the right to perform each privileged action flow?

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

- *Works with automation*
- *Supports agile development and continuous delivery*
- *Is intuitive to security and compliance teams*

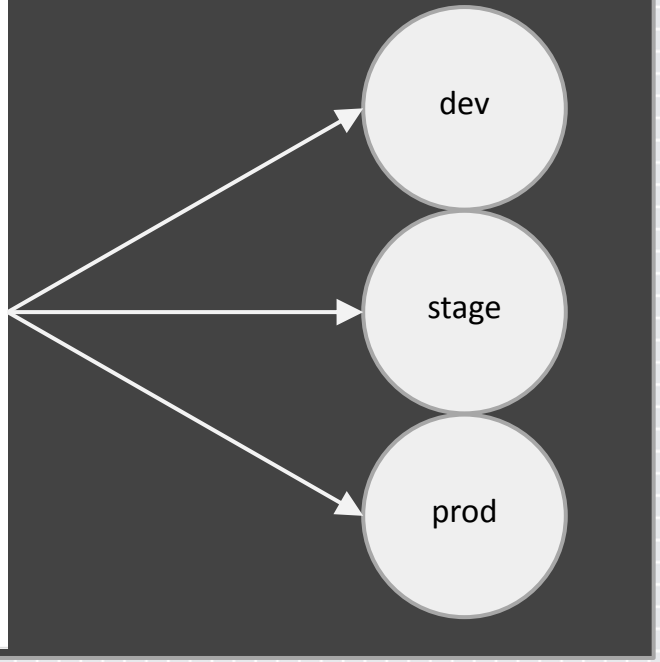
DevOps = Code = Security In Source Control

Security setup should be checked into source control. This doesn't mean checking your secrets into source. The setup of your security topology is ***in source***. Secrets are populated ***into it***.

1. Visible to all teams that depend on security.
2. Resolves confusion around where things are, what they are named, who/what has access to what.
3. Changes to topology are versioned and can be reviewed.

SecDevOps 2.0: Security Policy As Code

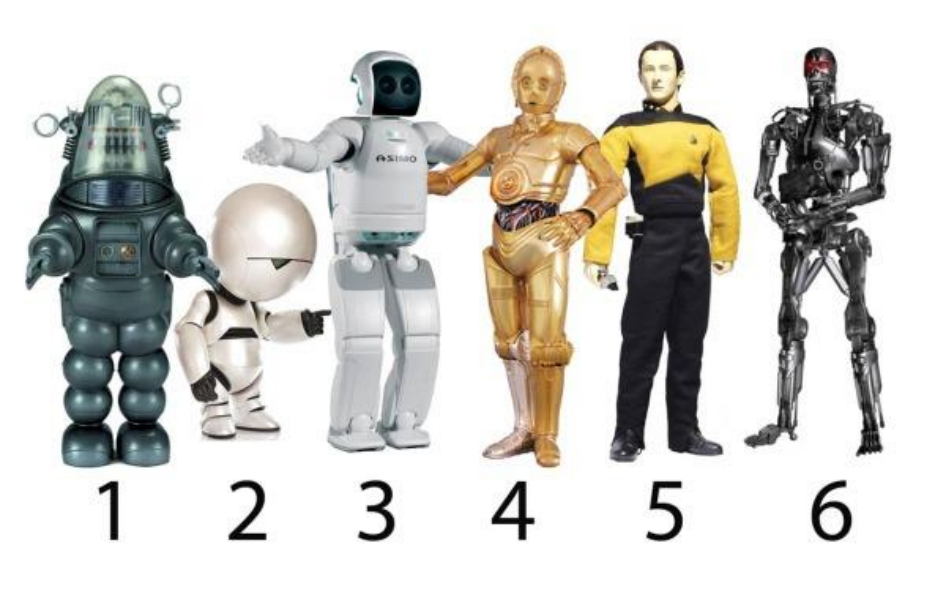
```
policy 'imaging-pipeline' do
  ops = group 'ops'
  dev = group 'dev'

  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: Identity For Machines At Scale

- Each Server (VM), Container (Docker, LXC) and Service needs to have an identity for access control to be meaningful
- Provisioning of these identities needs to be automated and included in SecDevOps workflow
- Machine-to-machine trust

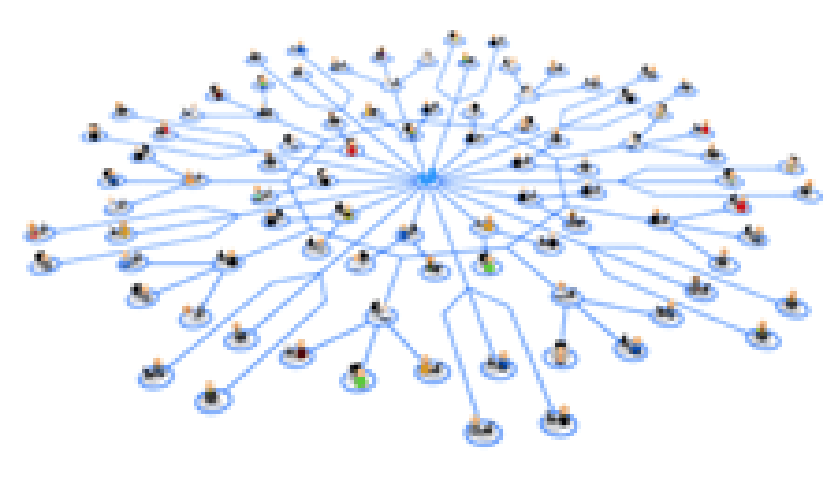


New Tools: Identity Management For Robots

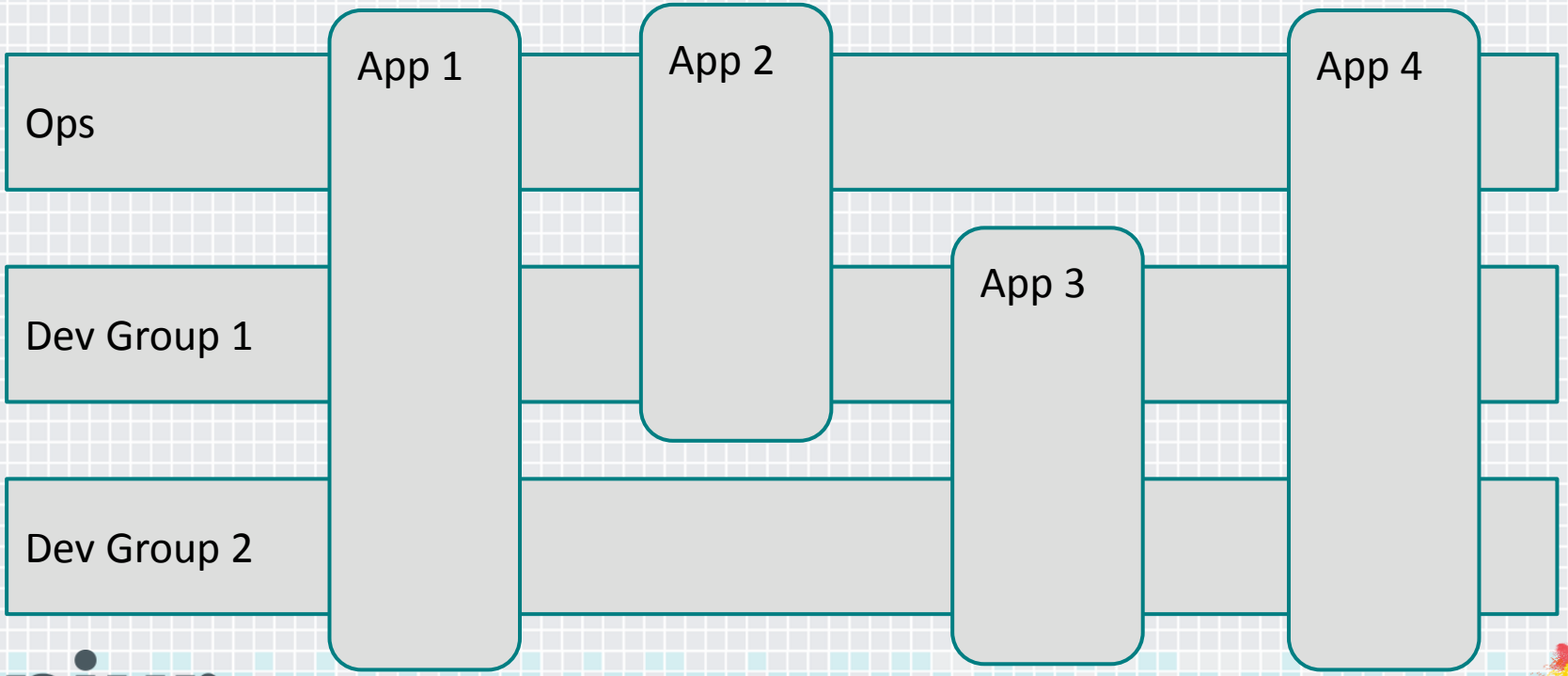
Machine trust and identity that works for servers, VMs, containers, and IOT.

Apply known tools and techniques from traditional identity management to robots

Example: Segregation of regulated applications/cloud into distinct application layers using policies that govern each service



Identity: Benefits For Access Control



SecDevOps 2.0: Perimeterless Network

- A collection/cluster of micro services all running on the same machine CAN’T rely on Hypervisor virtual networking for basic access control

- Applications span multiple machines and cloud providers

New Tools: Software-Defined Firewall

- Traffic “gates” that will work with clustered architecture
- Identity-based authorization of traffic
- Auditing and detection of unauthorized services

Example: Kubernetes / CoreOS Cluster

Opportunities To Improve 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).

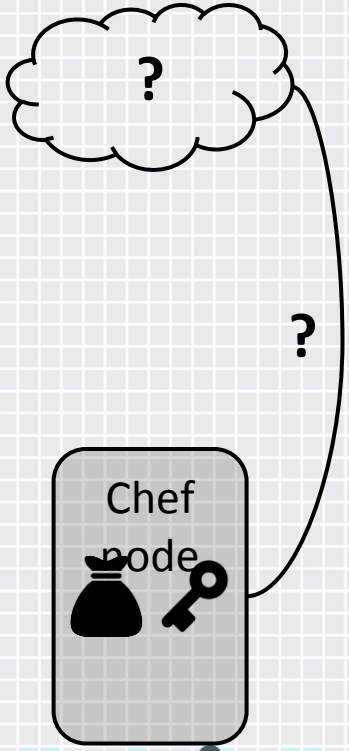
Tooling: “Secrets-As-A-Service”

- Trusted secrets server
- Identity-based access to secrets- (for people *and* machines)
- Thorough audit of all secrets-related activity
- Secrets distribution rooted in machine trust and strong cryptography
- Enables human administrators to “delegate” their authority to code and scripts

Example: Providing secrets to docker containers.

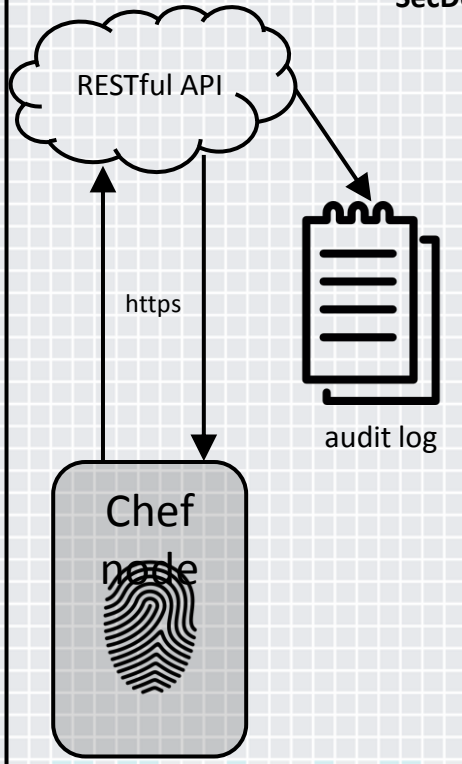
Secrets Service: Benefits

SecDevOps 1.0



- decryption keys are secrets themselves
- key storage and retrieval is complicated
- one decryption key per node
- access logs difficult to search and manage
- chef-vault makes key distribution easier at the expense of auto-scaling

SecDevOps 2.0



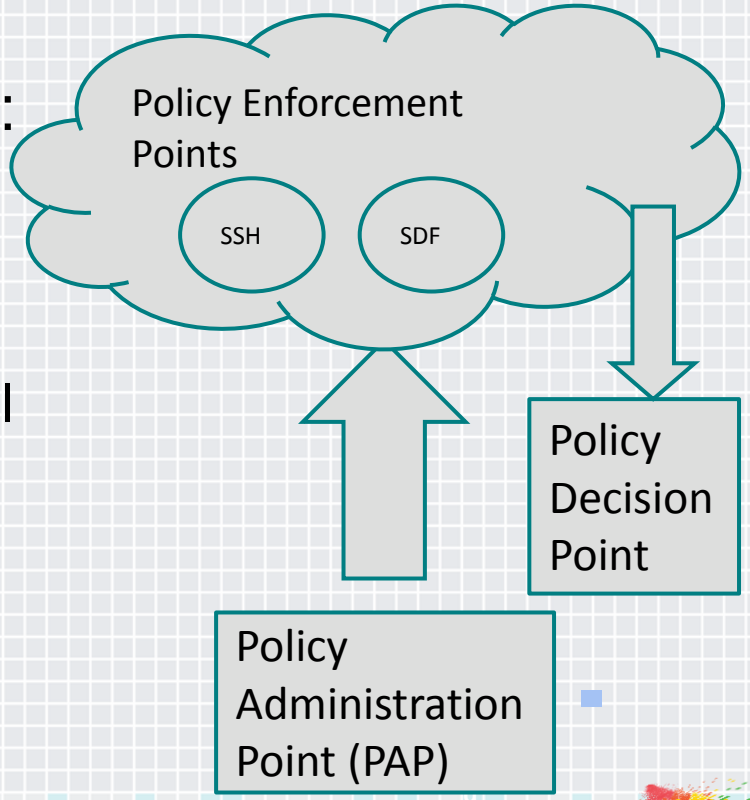
- Nodes have an identity, use that to fetch secrets. Easily given and revoked
- Permissions are role-based, applied to layers not hosts
- Chef library encapsulates authenticated HTTPS call
- full audit log of changes

Improving Practices

- 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

Logical Architecture

- **Policy Administration Point** (PAP): Policies created by DevOps and pushed through Workflow
- **Distributed Policy Enforcement Points** (PEP): Software-Defined Firewall (SDF), SSH, Secrets
- **Centralized Policy Decision Point (PDP):** Managed and controlled by Ops



Result: Clear Controls And Processes

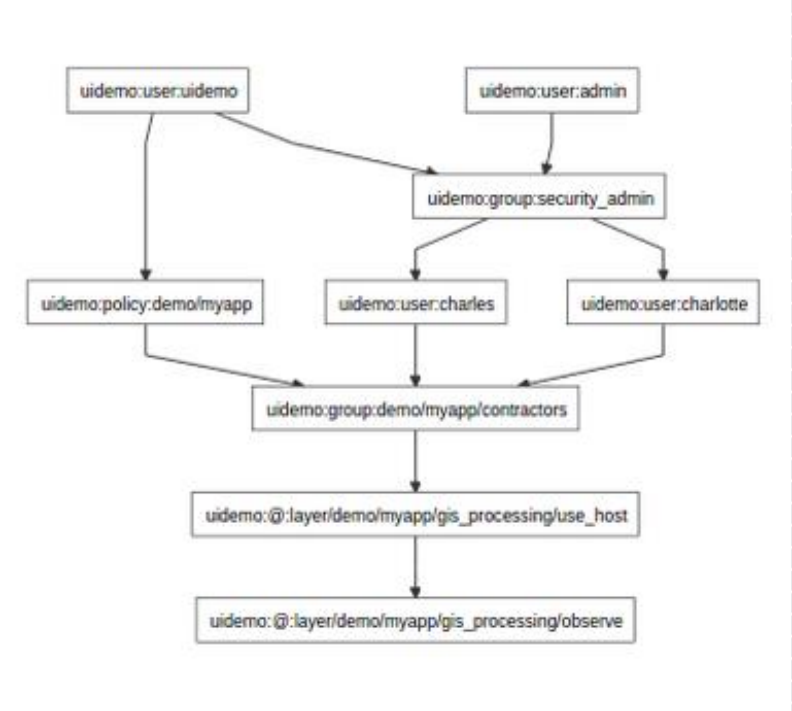
Problem:

Warnings

a day ago dustin was **denied permission** to *execute* on variable:build-0.1.0/s3/website/identity/access_key

Solution:

a day ago	dustin	performed *execute* on variable:build-0.1.0/s3/website/identity/access_key
a day ago	attic	gave variable:build-0.1.0/s3/website/identity/access_key to group:v4/ops



Takeaways

- Start the conversation with the DevOps team -- address ‘baked in’ cultural component to challenges
- Full incorporation of security and compliance into DevOps is possible
- Differences in language - The way that security, compliance, developers and ops talk about the same problem need to be bridged

Takeaways

- Build a mutual understanding of the trust model that's underlying the system(s)
- Transparency of the processes and mutual understanding of how things work is key
- The end resulting processes should be:
  - Intuitive
  - Reportable
  - Audited
  - Independent of the specific tools in the continuous delivery toolchain, because architectures can and will change

Apply: The Complete Equation

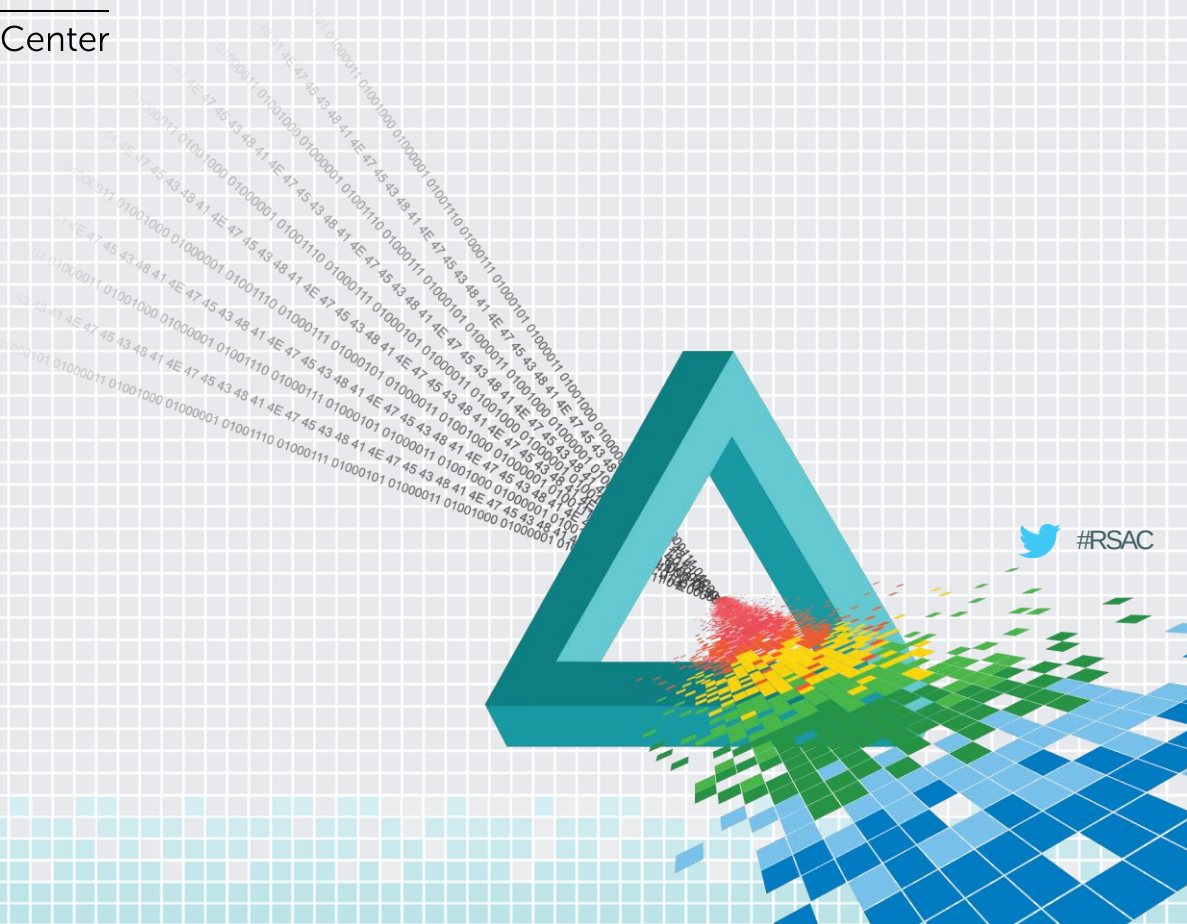
Educate + Learn = Apply

SecDevOps 1.0 makes use of existing SCM, CI and CM tools

Though well intentioned, approach results in a number of challenges for both Security and DevOps. SecDevOps 2.0 provides a path forward that can tackle the technical and organizational challenges of DevOps.

Pull together a conversation between Security and DevOps to discuss the “Access Control Automation Gap”

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

RSAConference2015

San Francisco | April 20-24 | Moscone Center

CHANGE

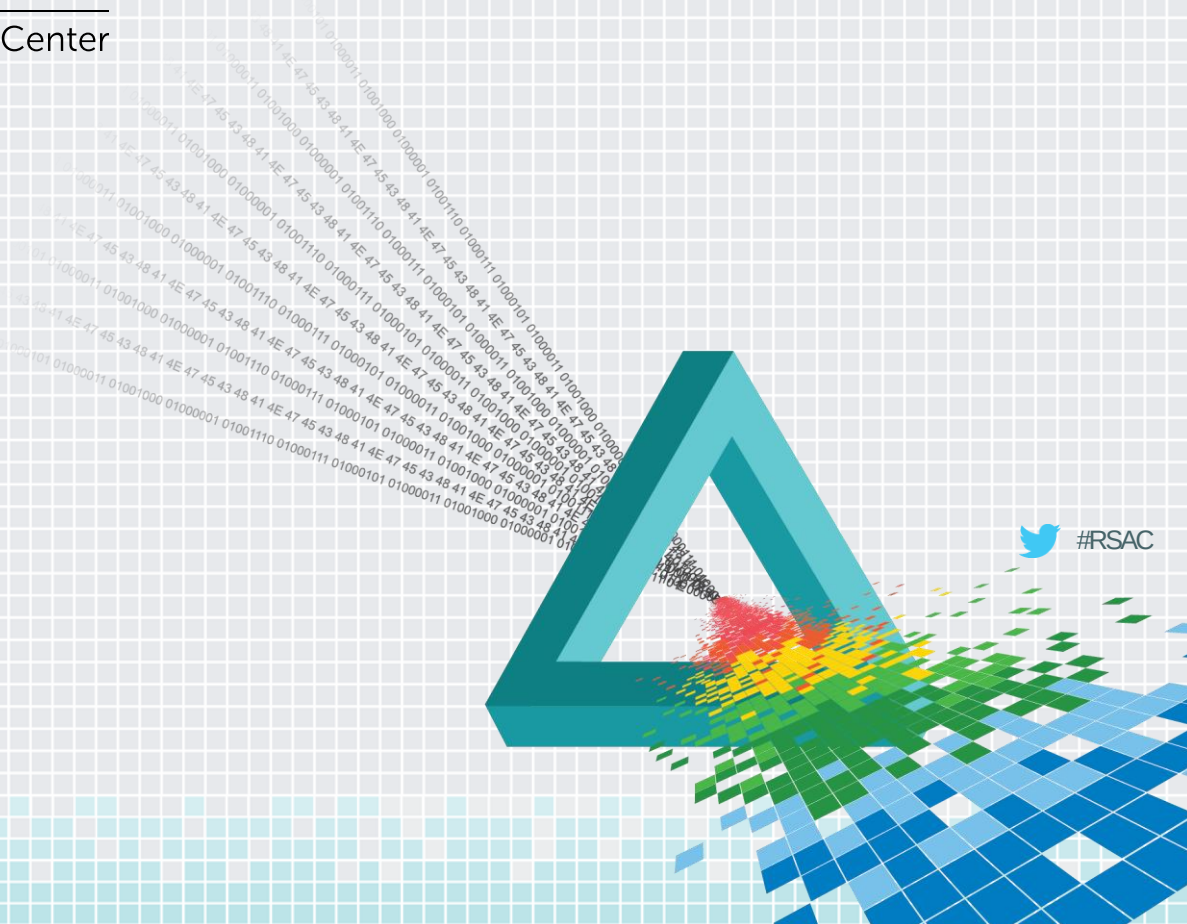
Challenge today's security thinking

SESSION ID:

#RSAC

RSAConference2015

San Francisco | April 20-24 | Moscone Center



Apply Slide

- Bullet point here (see slides 5 - 8 for instructions)
- Bullet point here
- Bullet point here