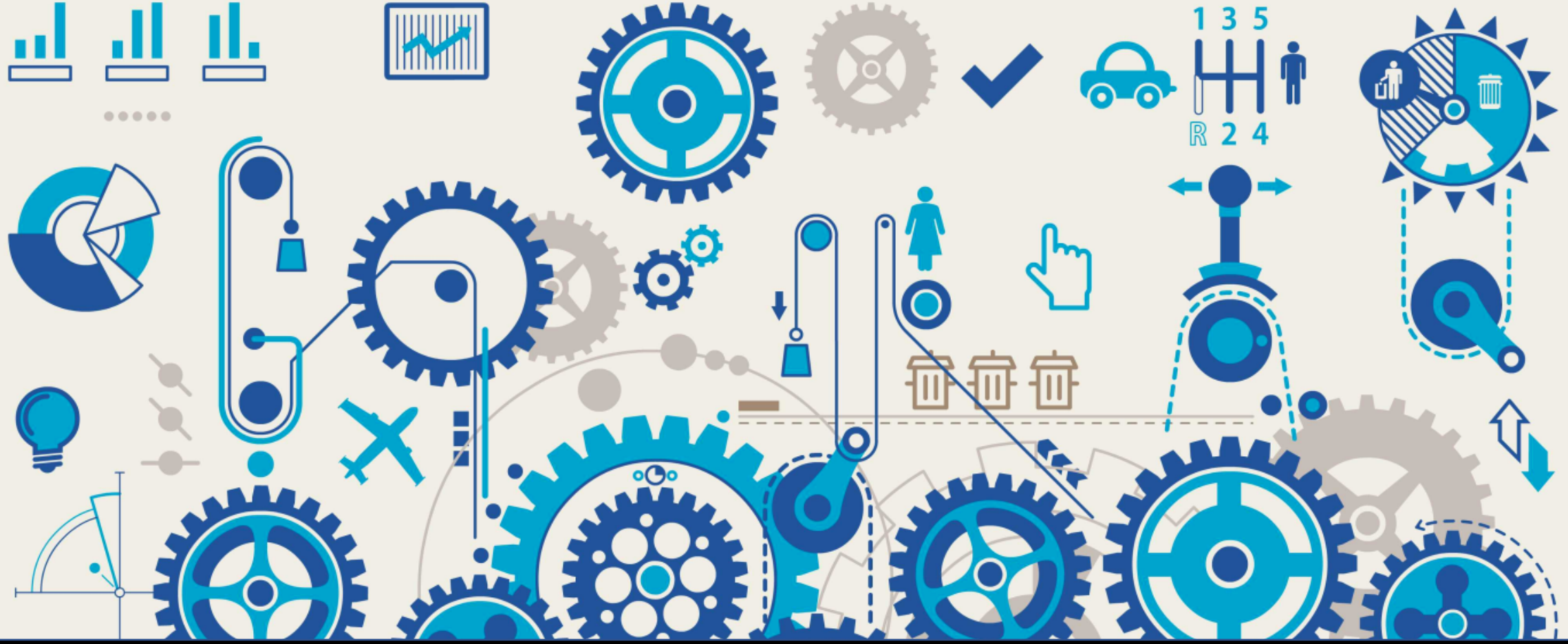


Continuous Automation / Continuous Compliance

Scott Ford
November 1st, 2017

$> whoami

scott ford
ww technical enablement lead, chef software
sford@chef.io
sford422 smford22

A true story…

Auditor: "Communication from your network devices to your authentication server must be encrypted."

A true story…

Auditor: "Communication from your network devices to your authentication server must be encrypted.”

Me: "We use *BlahBlah* TACACS+ server. You can't disable encryption."

A true story…

Auditor: "Okay. Please show me that encryption is enabled in your configuration."

A true story…

Auditor: "Okay. Please show me that encryption is enabled in your configuration.”

Me: "Um… I can't. I can't disable it, so I can't show you where it's enabled. But I can show you that I'm using *BlahBlah* TACACS+ server."

A true story…

Auditor: "Can you show me how you can't disable it?"

A true story…

Auditor: "Can you show me how you can't disable it?”

Me:

A true story…

Auditor: "Can you show me how you can't disable it?”

Me:

A true story…

Me: "How about I show you where I configured the encryption key? Is that good enough?”

A true story…

Me: "How about I show you where I configured the encryption key? Is that good enough?”

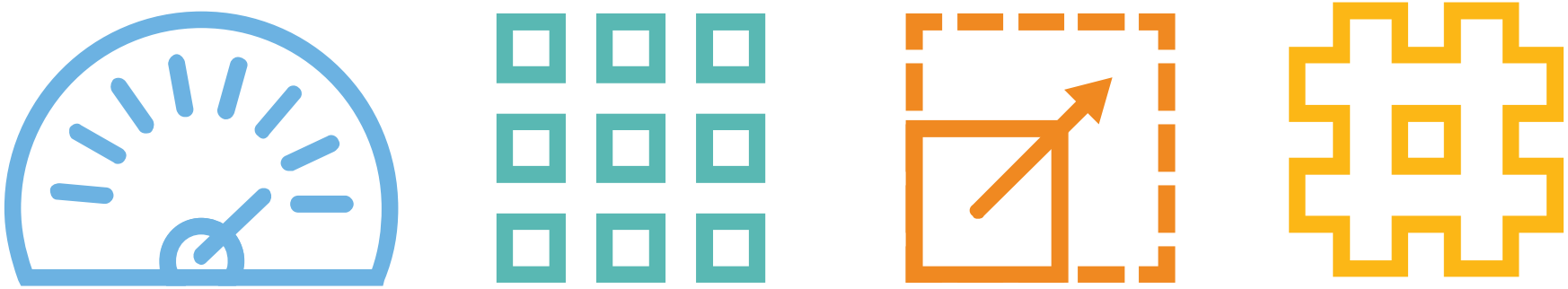
Auditor: "Ummmm… sure."

Why did I tell you this?

- How to prove "compliance" might not be obvious
- What the auditor was looking for can be automated
- This happened multiple times a year
- We **really** need to automate


A always
B be
automating

ABA: ALWAYS BE AUTOMATING

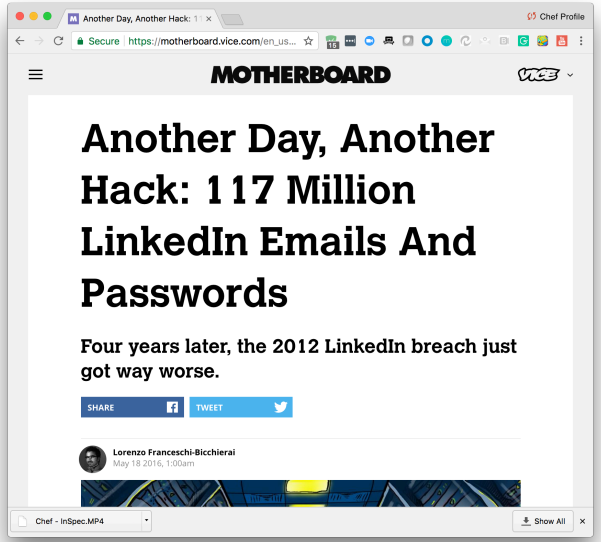


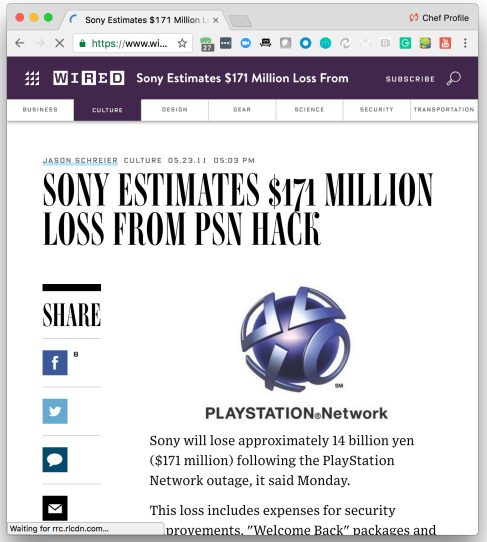
VELOCITY CONSISTENCY SCALE FEEDBACK

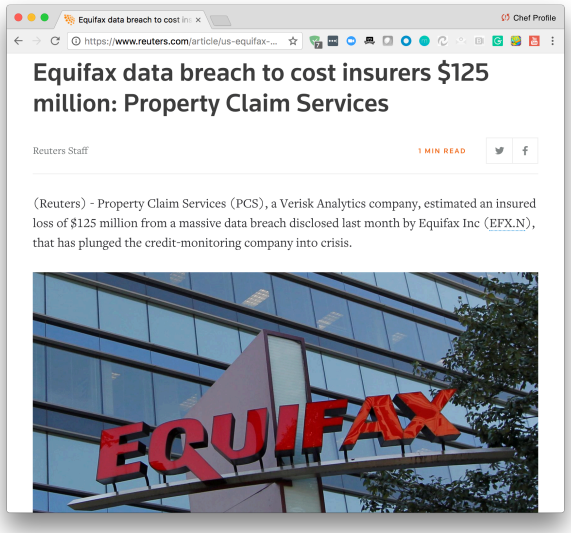
The path to production

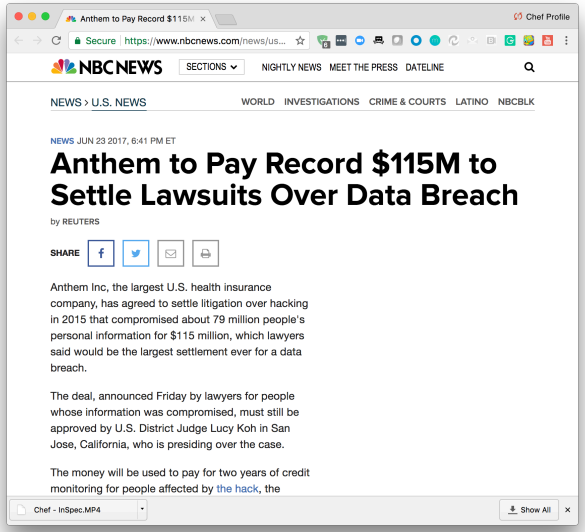

Product Ideas and Features
Security Review
Production

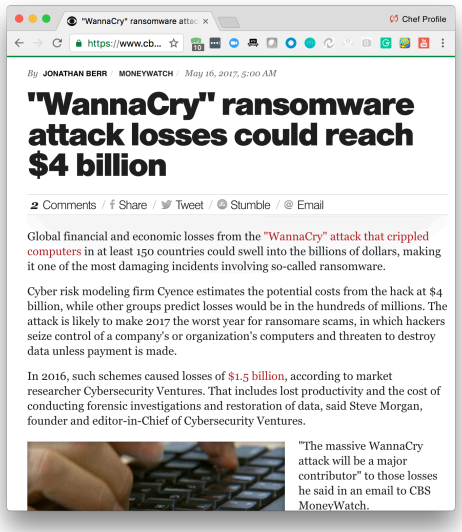

Every single Yahoo account
money.cnn...
Chef Profile
tech
BUSINESS
CULTURE
GADGETS
FUTURE
STARTUPS
Cyber-Safe
Every single Yahoo account was hacked - 3 billion in all
by Selena Larson @selenalarson
October 4, 2017: 6:36 AM ET
YAHOO!
Hilton, Brady beware
Timeline: The rise and fall of Yahoo
Sitting down? An epic and historic data breach at Yahoo in August 2013 affected every single customer account that existed at the time, Yahoo parent company Verizon said on Tuesday.
That's three billion accounts -- including email, Tumblr, Fantasy and Flickr -- or three times as many as the company initially reported in 2016.
Names, email addresses and passwords, but not financial information, were breached, Yahoo said last year.
Related: Who the Russian hackers targeted when they stole Yahoo emails
The new disclosure comes four months after Verizon (VZ, Tech30) acquired Yahoo's core internet assets for $4.48 billion. Yahoo is part of Verizon's digital media company, which is called
money.cnn.com/2017/03/16/technology/yahoo-hackers-targeted-erectile-dysfunction/index.html?iid=EL


Another Day, Another Hack: 1
Secure
https://motherboard.vice.com/en_us...
Chef Profile
MOTHERBOARD
VICE
Another Day, Another Hack: 117 Million LinkedIn Emails And Passwords
Four years later, the 2012 LinkedIn breach just got way worse.
SHARE
TWEET
Lorenzo Franceschi-Bicchierai
May 18 2016, 1:00am
Chef - InSpec.MP4
Show All

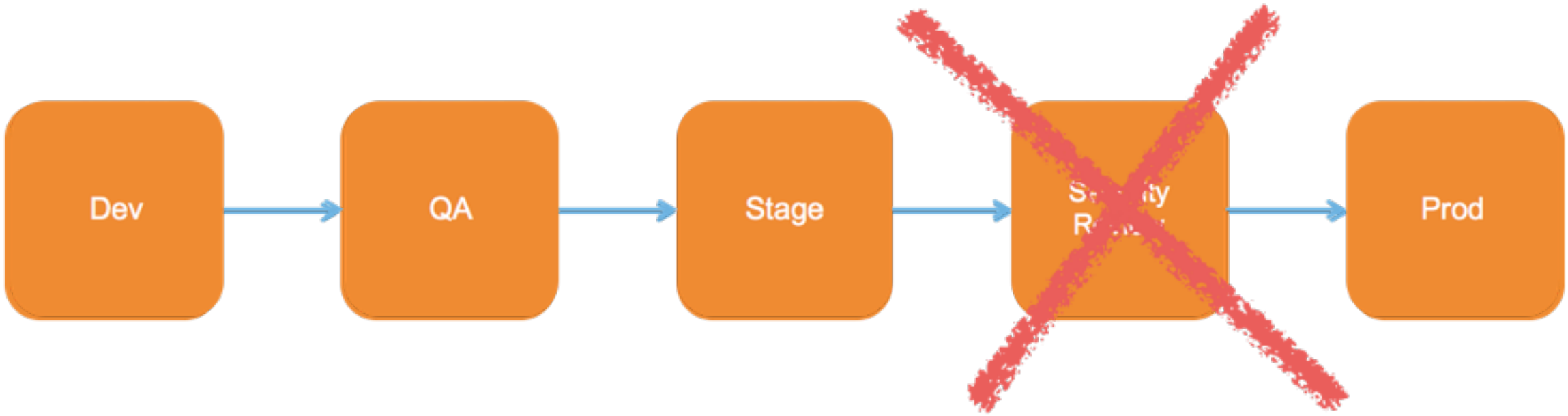

Sony Estimates $171 Million L
https://www.wi...
Chef Profile
WIRED
Sony Estimates $171 Million Loss From
SUBSCRIBE
BUSINESS
CULTURE
DESIGN
GEAR
SCIENCE
SECURITY
TRANSPORTATION
JASON SCHREIER CULTURE 05.23.11 05:03 PM
SONY ESTIMATES $171 MILLION LOSS FROM PSN HACK
SHARE
PLAYSTATION Network
Sony will lose approximately 14 billion yen ($171 million) following the PlayStation Network outage, it said Monday.
This loss includes expenses for security
Waiting for rrc.rlcdn.com...


Equifax data breach to cost in
https://www.reuters.com/article/us-equifax-...
Chef Profile
Equifax data breach to cost insurers $125 million: Property Claim Services
Reuters Staff
1 MIN READ
(Reuters) - Property Claim Services (PCS), a Verisk Analytics company, estimated an insured loss of $125 million from a massive data breach disclosed last month by Equifax Inc (EFX.N), that has plunged the credit-monitoring company into crisis.
EQUIFAX


Anthem to Pay Record $115M
Secure
https://www.nbcnews.com/news/us...
Chef Profile
NBC NEWS
SECTIONS
NIGHTLY NEWS
MEET THE PRESS
DATELINE
NEWS > U.S. NEWS
WORLD
INVESTIGATIONS
CRIME & COURTS
LATINO
NBCBLK
NEWS JUN 23 2017, 6:41 PM ET
Anthem to Pay Record $115M to Settle Lawsuits Over Data Breach
by REUTERS
SHARE
Anthem Inc, the largest U.S. health insurance company, has agreed to settle litigation over hacking in 2015 that compromised about 79 million people's personal information for $115 million, which lawyers said would be the largest settlement ever for a data breach.
The deal, announced Friday by lawyers for people whose information was compromised, must still be approved by U.S. District Judge Lucy Koh in San Jose, California, who is presiding over the case.
The money will be used to pay for two years of credit monitoring for people affected by the hack, the
Chef - InSpec.MP4
Show All


"WannaCry" ransomware attac
https://www.cb...
Chef Profile
By JONATHAN BERR / MONEYWATCH / May 16, 2017, 5:00 AM
"WannaCry" ransomware attack losses could reach $4 billion
2 Comments / Share / Tweet / Stumble / Email
Global financial and economic losses from the "WannaCry" attack that crippled computers in at least 150 countries could swell into the billions of dollars, making it one of the most damaging incidents involving so-called ransomware.
Cyber risk modeling firm Cyence estimates the potential costs from the hack at $4 billion, while other groups predict losses would be in the hundreds of millions. The attack is likely to make 2017 the worst year for ransomare scams, in which hackers seize control of a company's or organization's computers and threaten to destroy data unless payment is made.
In 2016, such schemes caused losses of $1.5 billion, according to market researcher Cybersecurity Ventures. That includes lost productivity and the cost of conducting forensic investigations and restoration of data, said Steve Morgan, founder and editor-in-Chief of Cybersecurity Ventures.
"The massive WannaCry attack will be a major contributor" to those losses he said in an email to CBS MoneyWatch.

The security/compliance roadblock



Compliance begins with policy

REGULATORY COMPLIANCE

OFAC	USA PATRIOT Act	Gramm-Leach-Bliley Act	Red Flags Rule
Bank Secrecy Act	Sarbanes-Oxley	Regulation E	Dodd-Frank
False Claims Act	HIPAA	European Central Bank regulations	Prudential Regulation Authority
Financial Conduct Authority	HITECH	PCI DSS	GDPR

References:

1. AJ Lewis, "LVM HOWTO", http://tldp.org/HOWTO/LVM-HOWTO/

1.1.10 Add nodev Option to /home (Scored)

Profile Applicability:

- Level 1

Description:

When set on a file system, this option prevents character and block special devices from being defined, or if they exist, from being used as character and block special devices.

Rationale:

Since the user partitions are not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices.

Note: The actions in the item refer to the `/home` partition, which is the default user partition that is defined in CentOS 6. If you have created other user partitions, it is recommended that the Remediation and Audit steps be applied to these partitions as well.

Audit:

Run the following commands to determine if the system is configured as recommended.

```
# grep /tmp /etc/fstab | grep noexec
# mount | grep /tmp | grep noexec
```

If either command emits no output then the system is not configured as recommended.

Remediation:

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options). See the `fstab(5)` manual page for more information.

```
# mount -o remount,nodev /home
```

1.1.11 Add nodev Option to Removable Media Partitions (Not Scored)

Profile Applicability:

Set `nodev` on removable media to prevent character and block special devices that are present on the removable be treated as these device files.

Rationale:

Removable media containing character and block special devices could be used to circumvent security controls by allowing non-root users to access sensitive device files such as `/dev/kmem` or the raw disk partitions.

Audit:

```
# grep <each removable media mountpoint> /etc/fstab
Verify that nodev is an option
```

Remediation:

Edit the `/etc/fstab` file and add "`nodev`" to the fourth field (mounting options). Look for entries that have mount points that contain words such as floppy or cdrom. See the `fstab(5)` manual page for more information.

1.1.12 Add noexec Option to Removable Media Partitions (Not Scored)

Profile Applicability:

- Level 1

Description:

Set `noexec` on removable media to prevent programs from executing from the removable media.

Rationale:

Setting this option on a file system prevents users from executing programs from the removable. This deters users from being to introduce potentially malicious software on the system.

Audit:

```
# grep <each removable media mountpoint> /etc/fstab
```

Note: Verify that `noexec` is an option

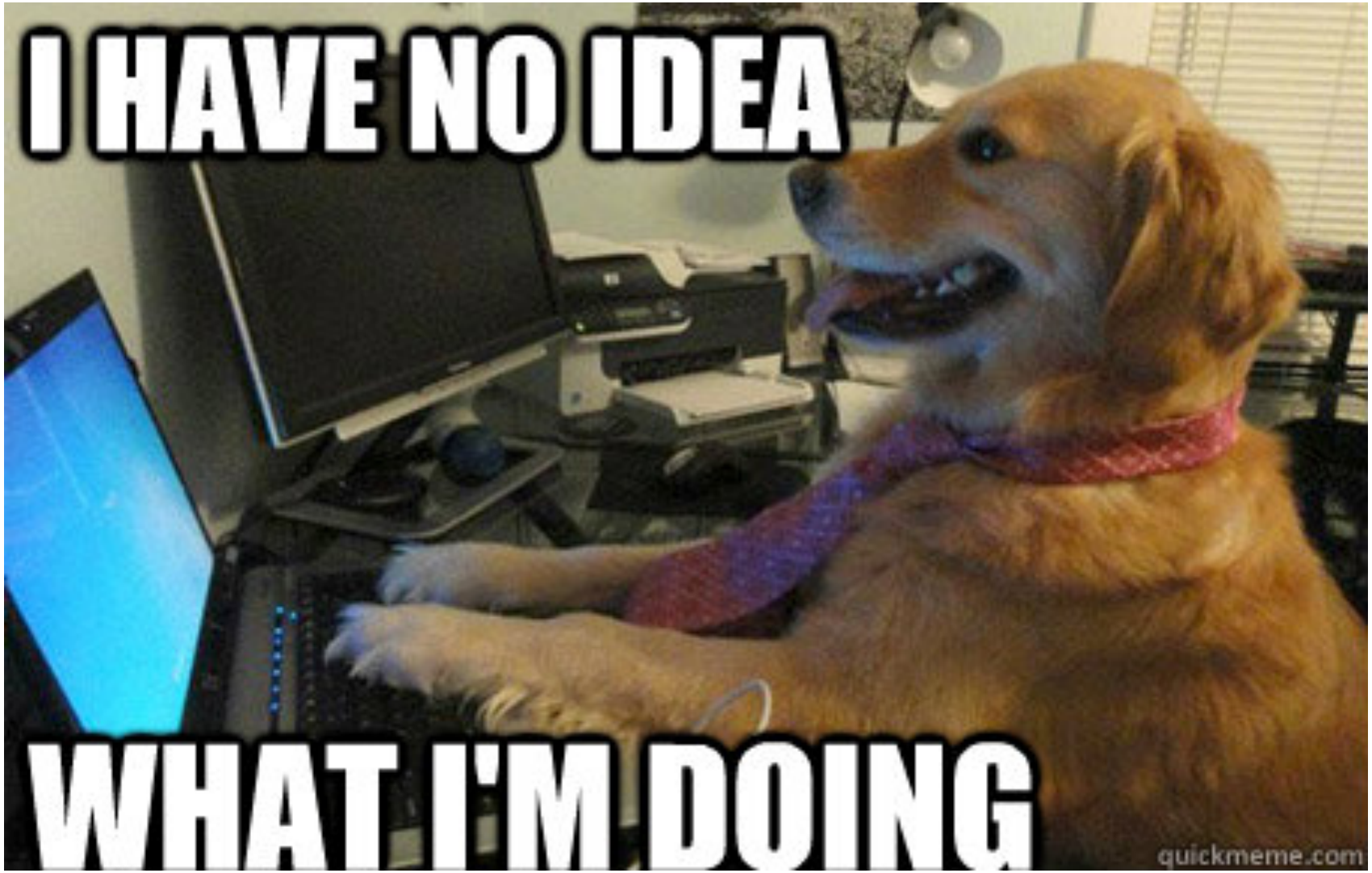
An Example from Documentation

404.3.5: *Communication between network devices and central authentication systems must be encrypted at all times.*

I can totally script that...

```
$ grep "key" /etc/tac_plus.conf | sed 's/key = //'
s00persecretkey
```

...but there's no context.



A tale of three personas…

…what's the common language???

Security

Compliance

Language
???

DevOps


INSPEC
BY CHEF™

InSpec

- Human-readable specification language used for testing systems for functional, security, or compliance

InSpec

- Human-readable specification language used for testing systems for functional, security, or compliance
- Includes facilities for creating, sharing, reusing profiles

InSpec

- Human-readable specification language used for testing systems for functional, security, or compliance
- Includes facilities for creating, sharing, reusing profiles
- Extensible so you can build your own rules for your applications and systems

InSpec

- Human-readable specification language used for testing systems for functional, security, or compliance
- Includes facilities for creating, sharing, reusing profiles
- Extensible so you can build your own rules for your applications and systems
- Command-line tool for plugging into your existing workflows / build systems

InSpec

- Human-readable specification language used for testing systems for functional, security, or compliance
- Includes facilities for creating, sharing, reusing profiles
- Extensible so you can build your own rules for your applications and systems
- Command-line tool for plugging into your existing workflows / build systems
- Integrates with Test Kitchen for fast-feedback local testing by developers

From lemons...

```
$ grep "key" /etc/tac_plus.conf | sed 's/key = //'
s00persecretkey
$
```

… create lemonade!

```
describe ini('/etc/tac_plus/tac_plus.conf') do
  its('key') { should_not be_nil }
end
```

… create lemonade!

```
control 'sox-404.3.5' do
  title 'Network Device to Central Auth Encryption'
  impact 1.0
  desc "
    All communication between network devices and central auth
    must be encrypted. Our TACACS+ servers encrypt all the time
    and the presence of a pre-shared key proves it."

  describe ini('/etc/tac_plus/tac_plus.conf') do
    its('key') { should_not be_nil }
  end
end
```

Map Documentation to Controls

404.3.5: *Communication between network devices and central authentication systems must be encrypted at all times.*

```
control 'sox-404.3.5' do
  title 'Network Device to Central Auth Encryption'
  impact 1.0
  desc "
    All communication between network devices and
    central auth must be encrypted. Our TACACS+ servers
    encrypt all the time and the presence of a
    pre-shared key proves it."

  describe ini('/etc/tac_plus/tac_plus.conf') do
    its('key') { should_not be_nil }
  end
end
```

Share Context

404.3.5: *Communication between network devices and central authentication systems must be encrypted at all times.*

```
control 'sox-404.3.5' do
  title 'Network Device to Central Auth Encryption'
  impact 1.0
  desc "
    All communication between network devices and
    central auth must be encrypted. Our TACACS+ servers
    encrypt all the time and the presence of a
    pre-shared key proves it."

  describe ini('/etc/tac_plus/tac_plus.conf') do
    its('key') { should_not be_nil }
  end
end
```

Automate Test Execution

404.3.5: *Communication between network devices and central authentication systems must be encrypted at all times.*

```
control 'sox-404.3.5' do
  title 'Network Device to Central Auth Encryption'
  impact 1.0
  desc "
    All communication between network devices and
    central auth must be encrypted. Our TACACS+ servers
    encrypt all the time and the presence of a
    pre-shared key proves it."

  describe ini('/etc/tac_plus/tac_plus.conf') do
    its('key') { should_not be_nil }
  end
end
```

Assessing Impact and Priority

404.3.5: *Communication between network devices and central authentication systems must be encrypted at all times.*

```
control 'sox-404.3.5' do
  title 'Network Device to Central Auth Encryption'
  impact 1.0
  desc "
    All communication between network devices and
    central auth must be encrypted. Our TACACS+ servers
    encrypt all the time and the presence of a
    pre-shared key proves it."

  describe ini('/etc/tac_plus/tac_plus.conf') do
    its('key') { should_not be_nil }
  end
end
```

Assessing Impact and Priority

```
control 'no-telnet' do
  title 'telnet not installed'
  impact 0.5
  tag 'pci'
  ref 'pci stage 1', url: 'https://wiki.mycompany.biz/…'
  desc "
    PCI-DSS requires all admin traffic to be encrypted. Telnet
    is not encrypted and is therefore not permitted."

  describe package('telnetd') do
    it { should_not be_installed }
  end
end
```

InSpec Everywhere

Any OS
- Linux, Windows, OS X, Solaris, AIX, HP UX

Any Platform
- Bare metal, VMs, Containers, APIs

Any Target
- Local (via inspec cli, chef audit cookbook)
- Remote (ssh, winrm, docker, HTTP for APIs)
- Test Kitchen

InSpec Everywhere

Any OS
- Linux, Windows, OS X, Solaris, AIX, HP UX

Any Platform
- Bare metal, VMs, Containers APIs

Any Target
- Local (via inspec cli, chef audit cookbook)
- Remote (ssh, winrm, docker, HTTP fo APIs
- Test Kitchen

InSpec for Cloud APIs

inspec-aws

```
control 'aws-1' do
  impact 1.0
  title 'Checks root account has an mfa enabled'

  describe aws_iam_root_user do
    it { should have_mfa_enabled }
  end
end
```

inspec-azure

```
control 'azure-1' do
  impact 1.0
  title 'Checks base image of machine'

  describe azure_virtual_machine('example-01) do
    its('sku') { should eq '16.04.0-LTS' }
  end
end
```

inspec-vmware

```
control "vmware-1" do
  impact 0.7
  title 'Checks that soft power off is diabled'

  describe vmware_vm_advancedsetting({datacenter: 'ha-datacenter', vm: 'testvm'}) do
    its('softPowerOff') { should cmp 'false' }
  end
end
```

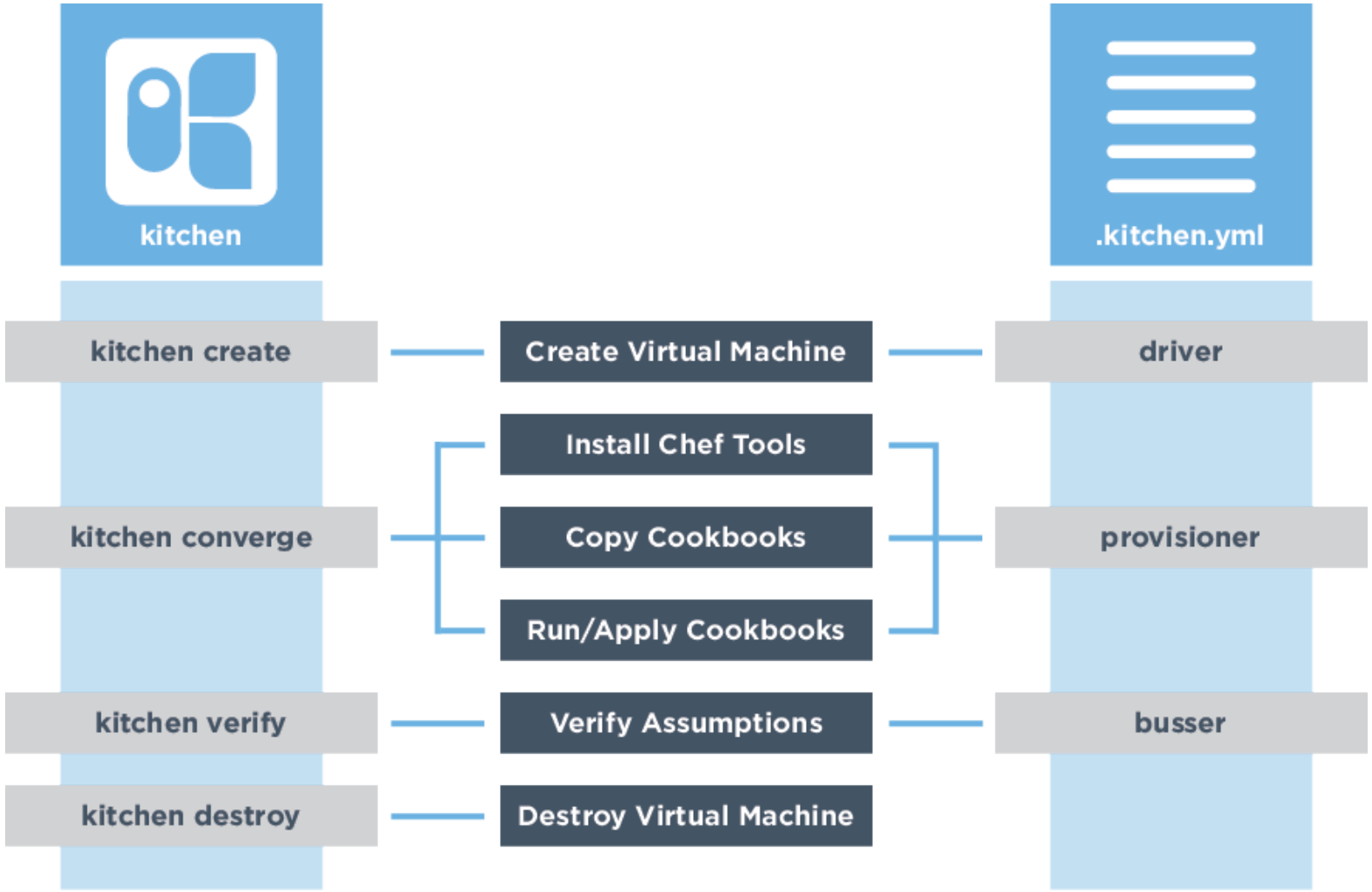
InSpec Everywhere

Any OS
- Linux, Windows, OS X, Solaris, AIX, HP UX

Any Platform
- Bare metal, VMs, Containers, APIs

Any Target
- Local (via inspec cli, chef audit cookbook)
- Remote (ssh, winrm, docker, HTTP for APIs)
- Test Kitchen

Tesk Kitchen



amazon web services

Microsoft Azure

vmware

openstack

VAGRANT

docker

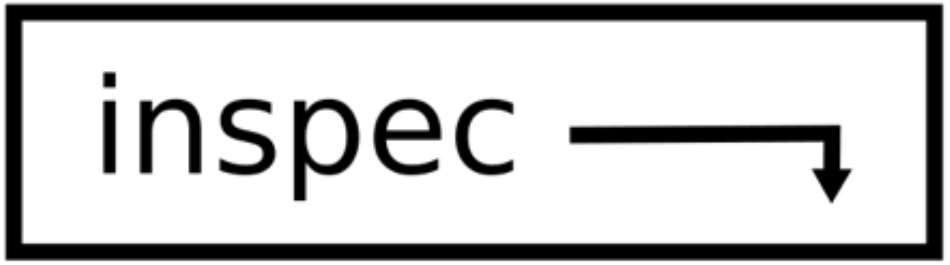
Test via Test Kitchen

```
verifier:
  name: inspec
  inspec_tests:
    - name: company-base
      git: https://github.com/myorg/base-profile.git
    - name: app1
      url: https://myco.artifactory.com/app1.tar.gz
```

DEMO

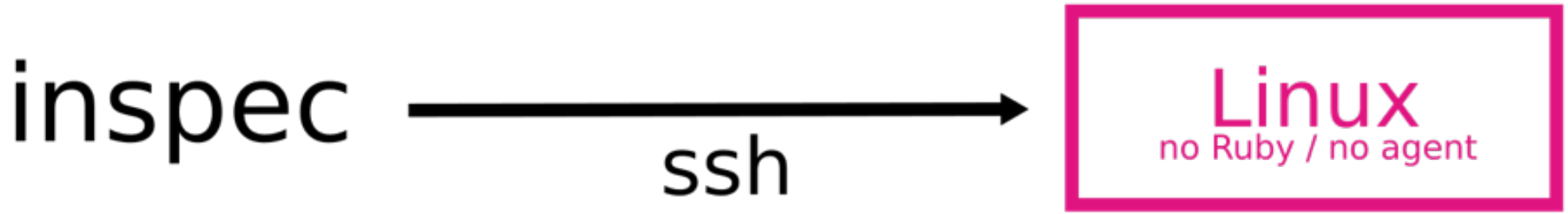
TACACS Encryption with Inspec

Test Locally




```
$ inspec exec /path/to/profile
```

Test Remotely

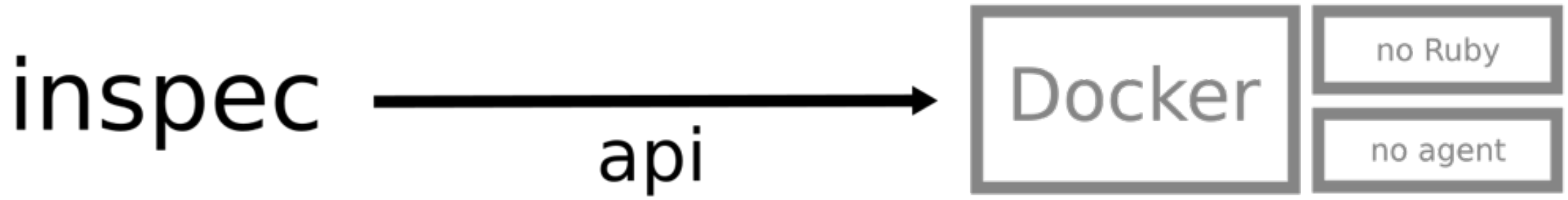



```
$ inspec exec /path/to/profile -i ssh.key -t ssh://me@myhost
```

Test Remotely

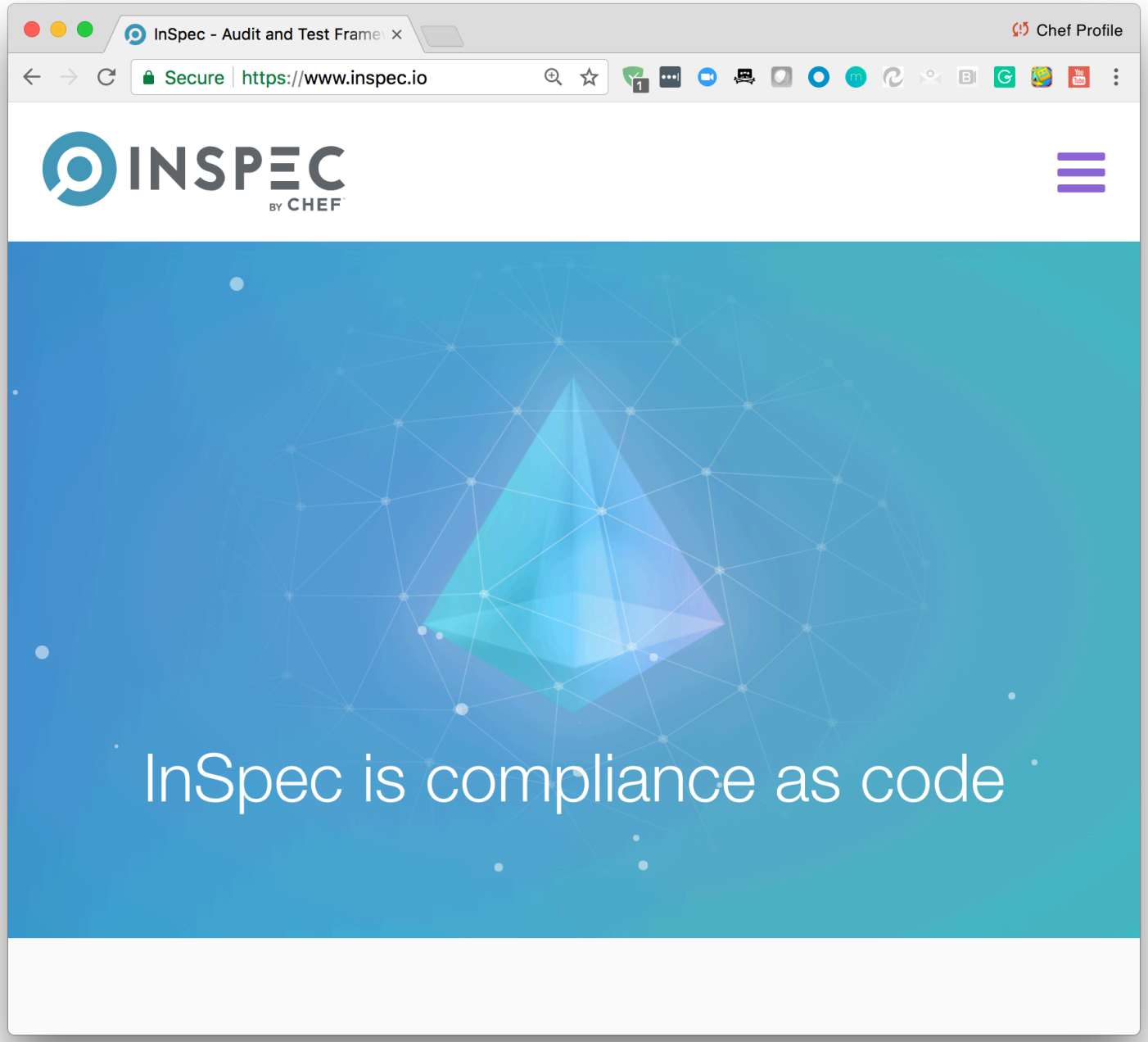

```
$ inspec exec /path/to/profile -t winrm://me@myhost --password secret
```

Test Remotely

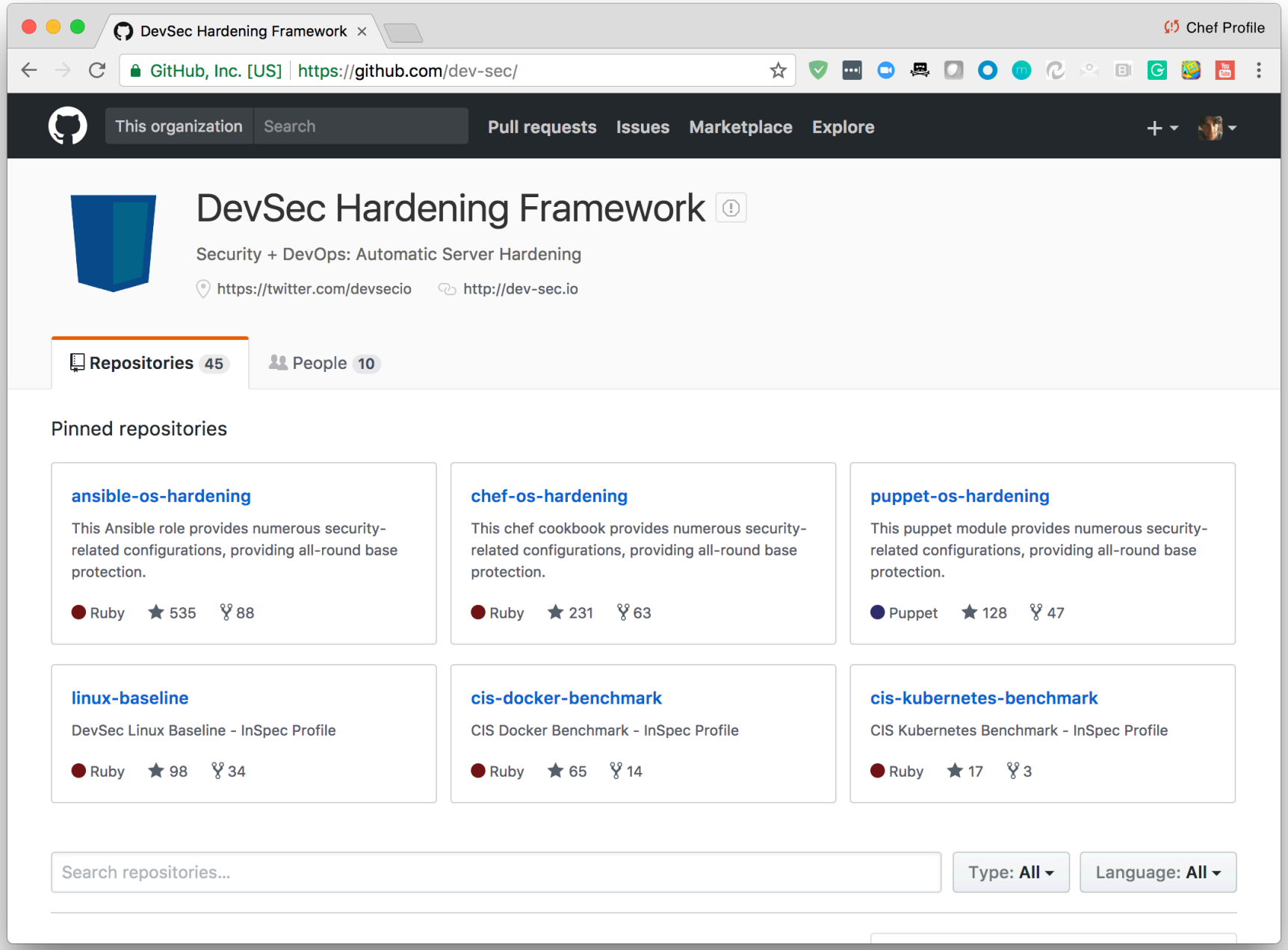



```
$ inspec exec /path/to/profile -t docker://3cc8837bb6a8
```

Test via Chef Client Runs



https://inspec.io

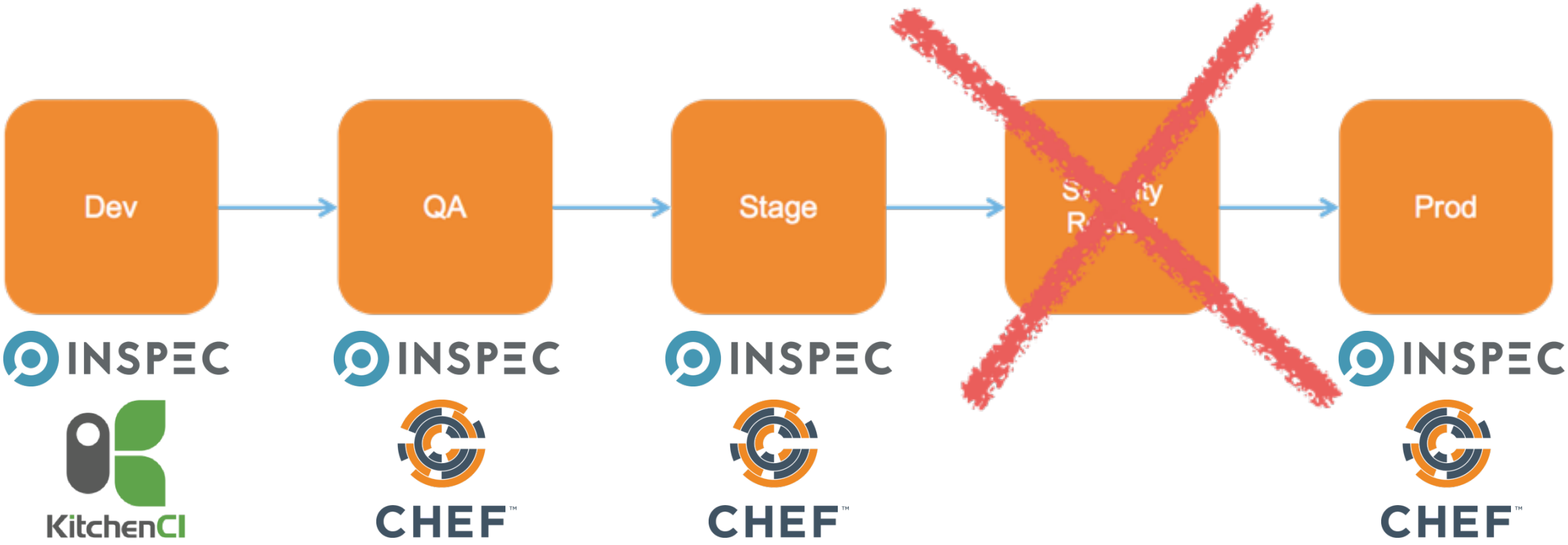


https://github.com/dev-sec

DEMO

DevSec Hardening

Compliance at every step



Why InSpec?

- Break down silos between organizations
- Codify your compliance policies and requirements
- Share context about your compliance requirements
- Achieve safety at velocity with compliance at every step
- Completely **free**! and **open source**!

InSpec by the numbers…

Since January 1st, 2017

- 408 Pull requests – **116 from non-Chef employees!**
- 89 PR Contributions – **61 non-Chef employees!**
- 23 core resources added – **12 from non-Chef employees!**

THANK YOU!

sford@chef.io

source code…

https://goo.gl/TUssQi