



INSPĒC

Making Compliance Fun

Nathen Harvey

Hey, Nathon! Stream this meetup!

- <https://chef.zoom.us/j/509104664>

Nathen Harvey

VP, Community Development at Chef
Co-host of the Food Fight Show Podcast



Occasional farmer – <http://ei.chef.io>

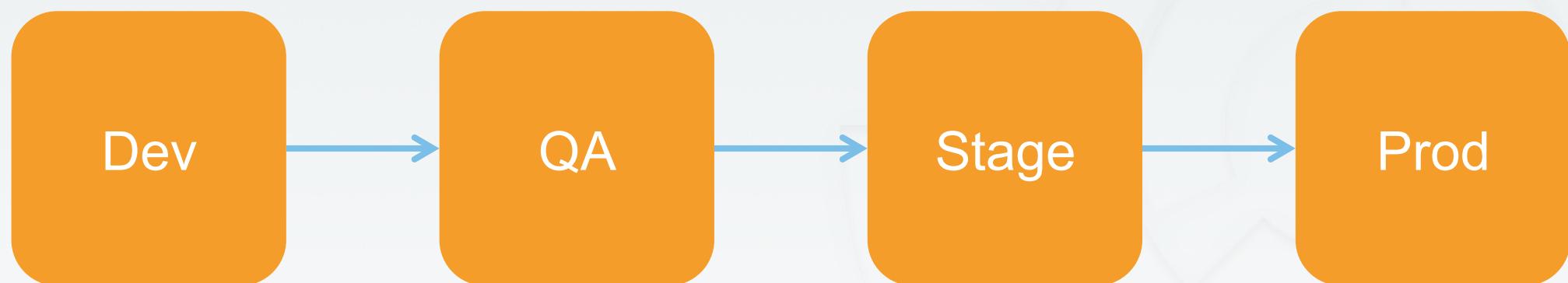
Love eggs – <http://eggs.chef.io>

#hugops – <http://hugops.chef.io>

[@nathenharvey](https://twitter.com/nathenharvey)

nharvey@chef.io







CHEFTM

Demo

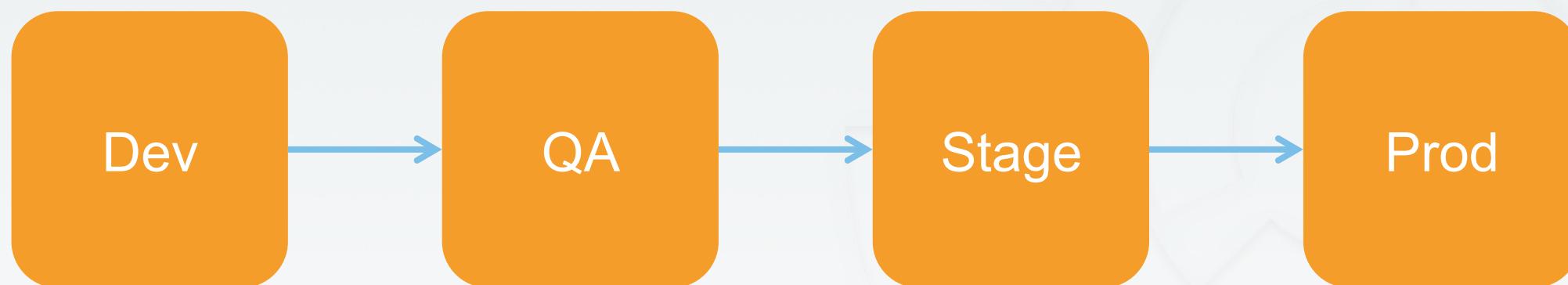
- See the running application
- Review the development environment's configuration
- Review the cookbook that creates the site
- Check out the open issues, let's resolve some of those
- https://github.com/nathenharvey/la_chef_meetup





SSH Control

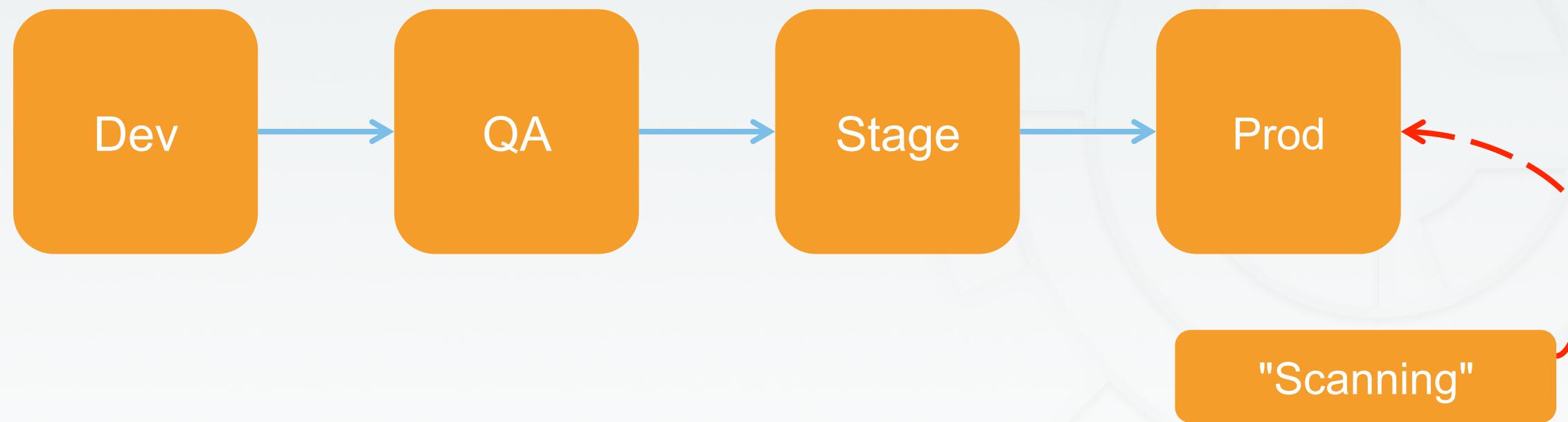
SSH supports two different protocol versions. The original version, SSHv1, was subject to a number of security issues. Please use SSHv2 instead to avoid these.













InSpec is compliance as code – a human-readable language for automating the continuous testing and compliance auditing of your entire infrastructure.

Mapping Compliance Document to InSpec

6.2.1 Set SSH Protocol to 2 (Scored)

Profile Applicability:

- Level 1

Description:

SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. SSH2 is more advanced and secure.

Rationale:

SSH v1 suffers from insecurities that do not affect SSH v2.

Audit:

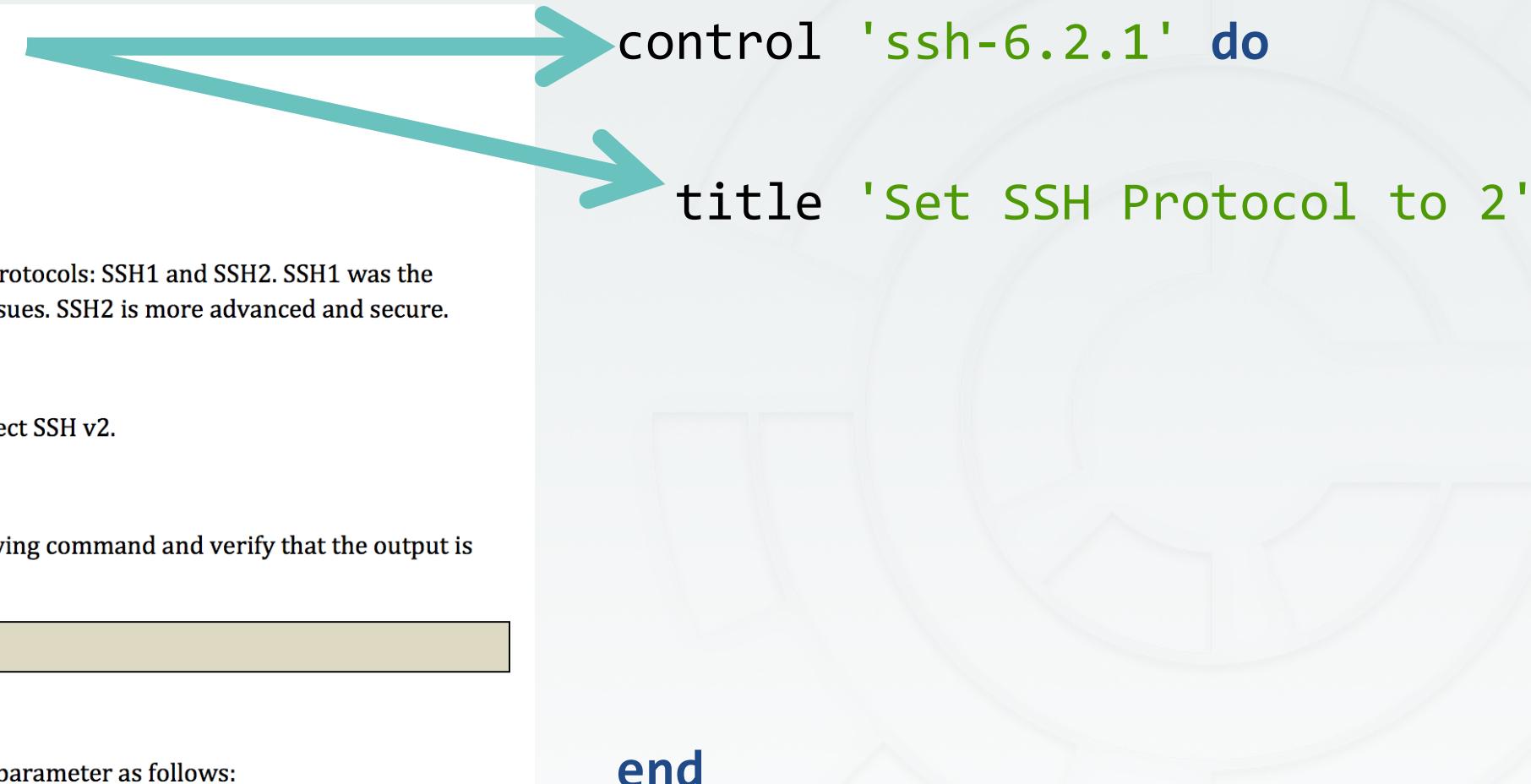
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "Protocol" /etc/ssh/sshd_config
Protocol 2
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Protocol 2
```



Mapping Compliance Document to InSpec

6.2.1 Set SSH Protocol to 2 (Scored)

Profile Applicability:

- Level 1

Description:

SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. ~~SSH2 is more advanced and secure.~~

Rationale:

SSH v1 suffers from insecurities that do not affect SSH v2.

Audit:

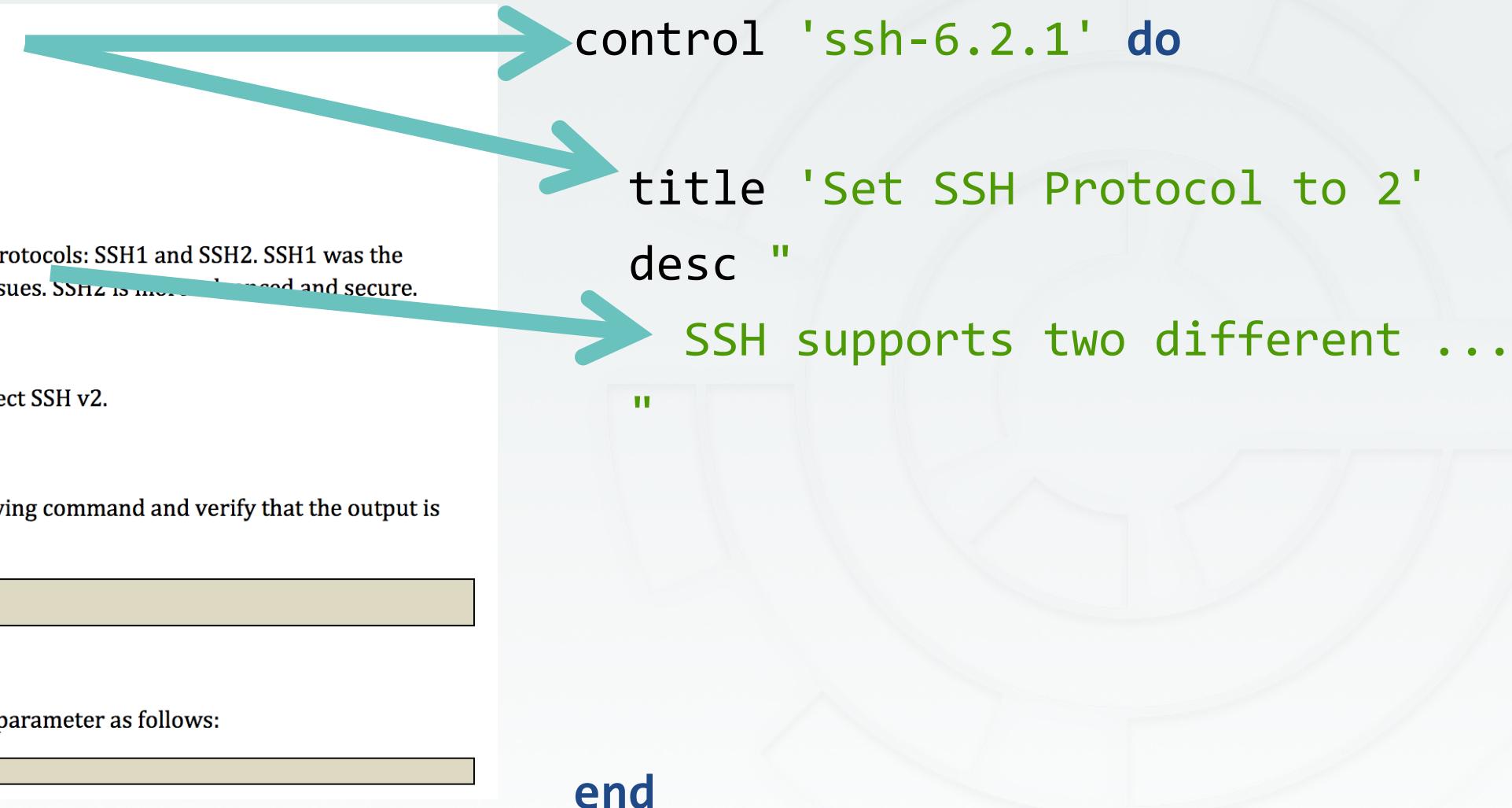
To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "Protocol" /etc/ssh/sshd_config
Protocol 2
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Protocol 2
```



Mapping Compliance Document to InSpec

6.2.1 Set SSH Protocol to 2 (Scored)

Profile Applicability:

- Level 1

Description:

SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. ~~SSH2 is more advanced and secure.~~

Rationale:

SSH v1 suffers from insecurities that do not affect SSH v2.

Audit:

To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "Protocol" /etc/ssh/sshd_config  
Protocol 2
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Protocol 2
```

```
control 'ssh-6.2.1' do
```

```
  title 'Set SSH Protocol to 2'
```

```
  desc "
```

```
    SSH supports two different ...
```

```
"
```

```
  describe sshd_config do
```

```
    its('Protocol') { should cmp('2') }
```

```
  end
```

```
end
```

Mapping Compliance Document to InSpec

6.2.1 Set SSH Protocol to 2 (Scored)

Profile Applicability:

- Level 1

Description:

SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. ~~SSH2 is more advanced and secure.~~

Rationale:

SSH v1 suffers from insecurities that do not affect SSH v2.

Audit:

To verify the correct SSH setting, run the following command and verify that the output is as shown:

```
# grep "Protocol" /etc/ssh/sshd_config  
Protocol 2
```

Remediation:

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

```
Protocol 2
```

```
control 'ssh-6.2.1' do  
  impact 1.0  
  title 'Set SSH Protocol to 2'  
  desc "  
    SSH supports two different ...  
  "  
  
  describe sshd_config do  
    its('Protocol') { should cmp('2') }  
  end  
end
```

Run Locally

```
$ inspec exec ssh-621.rb
```

- ✓ ssh-6.2.1: Set SSH Protocol to 2
 - ✓ SSH Configuration Protocol should eq "2"

Profile Summary: 1 successful, 0 failures, 0 skipped

Run Remote via ssh

```
$ inspec exec ssh-621.rb -i my.pem -t ssh://someremotehost
```

- ✓ ssh-6.2.1: Set SSH Protocol to 2
 - ✓ SSH Configuration Protocol should eq "2"

Profile Summary: 1 successful, 0 failures, 0 skipped

Run Remote via WinRM

```
$ inspec exec ssh-621.rb -t winrm://Admin@someremotehost
```

- ✓ ssh-6.2.1: Set SSH Protocol to 2
 - ✓ SSH Configuration Protocol should eq "2"

Profile Summary: 1 successful, 0 failures, 0 skipped

Test a Docker Container

```
$ inspec exec ssh-621.rb -t docker://8eb7760bd9db
```

```
Target: docker://  
8eb7760bd9db046cf826f36a6997b02a1cd884684870b78cede0ab03b62571a
```

- ✓ ssh-6.2.1: Set SSH Protocol to 2
 - ✓ SSH Configuration Protocol should eq "2"

```
Profile Summary: 1 successful, 0 failures, 0 skipped
```

Stand Alone Usage

```
describe sshd_config do
  its('Protocol') { should cmp 2 }
end
```

```
$ inspec exec test.rb
$ inspec exec test.rb -i vagrant.key -t ssh://root@172.17.0.1:11022
$ inspec exec test.rb -t winrm://Admin@192.168.1.2 --password super
$ inspec exec test.rb -t docker://3cc8837bb6a8
```

InSpec



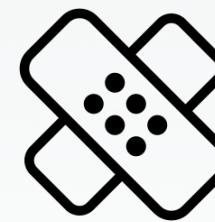
Mechanisms for Policy Definitions

- Profile Inheritance
- Attributes
- Custom Resources



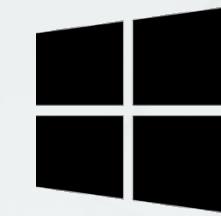
Native Packages

- Windows
- macOS
- Redhat & Ubuntu



Patch Management

- windows-patch-benchmark (dev-sec.io)
- linux-patch-benchmark (dev-sec.io)



Windows Support

- Windows 2016 / Nano Support
- Windows-specific Resources
- PowerShell remoting protocol with NTLM support



Remote and agent-based execution

- Custom sudo commands
- more ssh options



Chef Ecosystem

- Included in ChefDK package
- Kitchen support
- *audit* cookbook



InSpec Profiles



OS Hardening
Profile



Linux Patch
Profile



SSH Hardening
Profile



Windows Patch
Profile

InSpec Profiles



OS Hardening
Profile



Linux Patch
Profile



SSH Hardening
Profile



Windows Patch
Profile

Acme

InSpec Profiles

```
include_controls 'os-hardening' do
  skip_control 'os-06'

  control 'os-02' do
    impact 0.7
  end
end

include_controls 'ssh-hardening'
```

Demo

- Apply the compliance profile - <https://github.com/nathenharvey/acme-inspec-profile/>
- Remediate the issues with cookbooks from the Supermarket



InSpec is compliance as code – a human-readable language for automating the continuous testing and compliance auditing of your entire infrastructure.

InSpec: Turn security and compliance into code

- Translate compliance into Code
- Clearly express statements of policy
- Move risk to build/test from runtime
- Find issues early
- Write code quickly
- Run code anywhere
- Inspect machines, data and APIs

Part of a process of continuous compliance



A simple example of an InSpec CIS rule

```
control 'cis-1.4.1' do
  title '1.4.1 Enable SELinux in /etc/grub.conf'
  desc '
    Do not disable SELinux and enforcing in your GRUB configuration.
    These are important security features that prevent attackers from
    escalating their access to your systems. For reference see ...
  '
  impact 1.0
  expect(grub_conf.param 'selinux').to_not eq '0'
  expect(grub_conf.param 'enforcing').to_not eq '0'
end
```

Available Resources

apache	etc_group	kernel_module	os	registry_key
apache_conf	file	kernel_parameter	os_env	security_policy
apt	gem	limits_conf	package	service
audit_policy	group	login_def	parse_config	shadow
auditd_conf	grub_conf	mount	passwd	ssh_conf
auditd_rules	host	mssql_session	pip	ssl
bash	iis_site	mysql	port	user
bond	inetd_conf	mysql_conf	postgres	vbscript
bridge	ini	mysql_session	postgres_conf	windows_feature
command	interface	npm	postgres_session	wmi
csv	iptables	ntp_conf	powershell	xinetd
directory	json	oneget	processes	yaml
				yum

Further Resources

The screenshot shows the InSpec website homepage. At the top, there's a navigation bar with links for Overview, Tutorials, Docs, Community, Downloads, GitHub Project, and Contribute. Below the navigation is a code editor window displaying the following InSpec code:

```
describe code do
  it { should be_inspec }
end
```

Below the code editor, the text "InSpec is compliance as code" is followed by a brief description: "InSpec is compliance as code – a human-readable language for automating the continuous testing and compliance auditing of your entire infrastructure. You can also use it to verify if your servers and applications are configured correctly." There are two buttons: "DOWNLOAD INSPEC" and "START THE DEMO".

At the bottom, there are four circular icons with text below them:

- PLATFORM AGNOSTIC: InSpec supports all major operating systems and many applications out of the box.
- TEST LOCALLY OR REMOTELY: InSpec provides a local agent, as well as full remote testing support.
- FREE TO RUN ANYWHERE: InSpec is a language that can easily express compliance as code, with the freedom to run anywhere.
- FULLY EXTENSIBLE LANGUAGE: Easily extend the InSpec language to cover new operating systems, devices, or applications.

The screenshot shows the Learn Chef website homepage. At the top, there's a navigation bar with links for LEARN CHEF, TUTORIALS, SKILLS LIBRARY, DOCS, TRAINING, and COMMUNITY. The main heading is "WELCOME TO LEARN CHEF" with the subtext: "Welcome to Learn Chef, home to Chef tutorials, articles, technical docs and training. If you're looking to improve your understanding of Chef and DevOps, this is the place." Below the heading are five circular icons with text below them:

- TUTORIALS > (blue icon)
- SKILLS LIBRARY > (green icon)
- DOCS > (orange icon)
- TRAINING & CERTIFICATIONS > (yellow icon)
- COMMUNITY > (grey icon)

At the bottom, there's a call-to-action: "We offer a comprehensive training curriculum, as well as certification paths for different Chef skill sets – all led by a team of experienced instructors. [Get Started.](#)"

Small text at the very bottom right: "© 2016 Chef Software, Inc. All Rights Reserved."

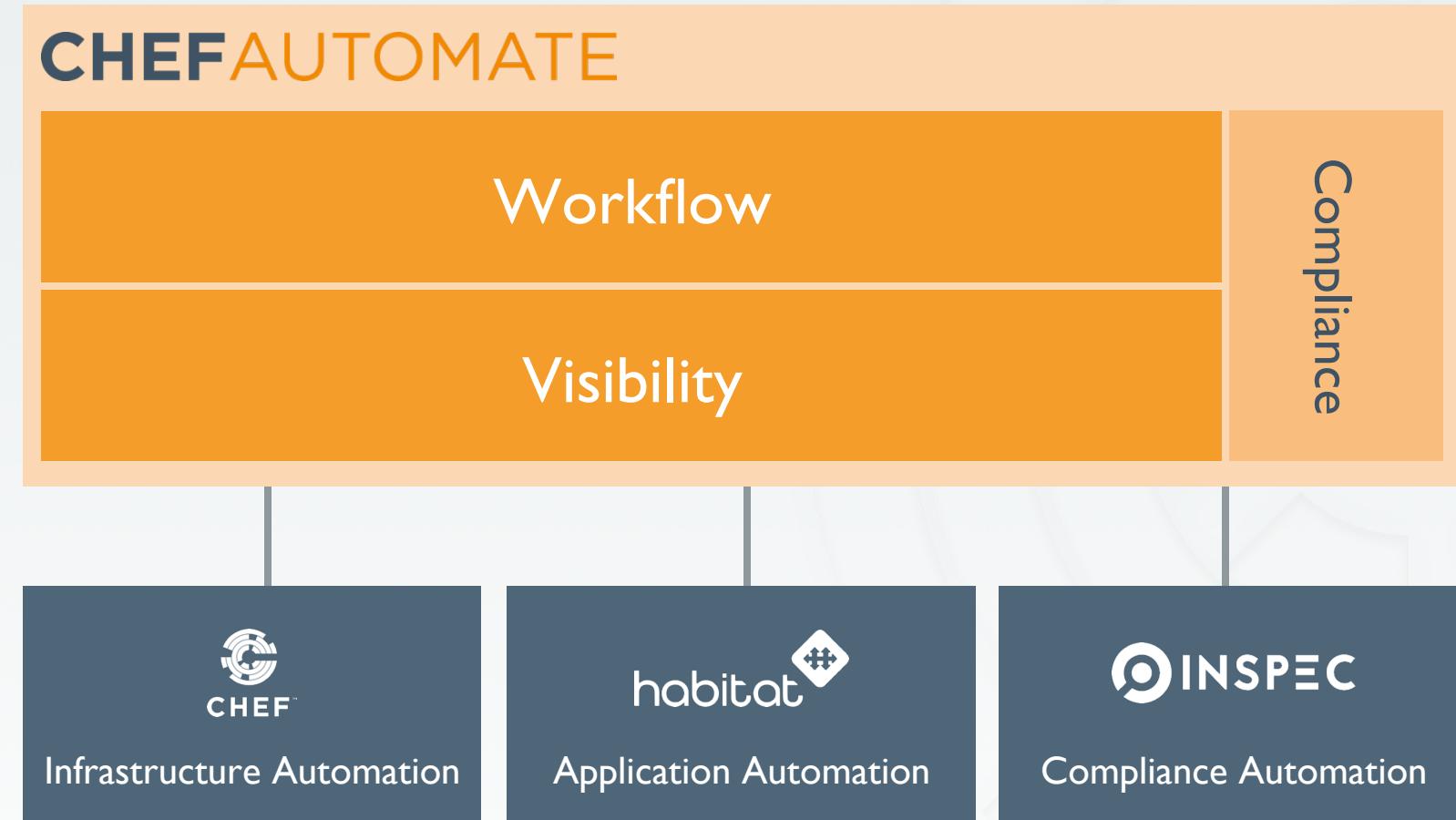
inspec.io

- Hands on tutorials
- Extensive documentation
- Code examples

learn.chef.io

- More tutorials about Compliance and Inspec

Chef Automate



Chef Automate



**Center for
Internet Security®**

Chef Compliance ships with profiles for:



Amazon Linux
2014.09 / 2015.03



CentOS
6 / 7

Hewlett Packard
Enterprise



IBM AIX
5.3 / 6.1 / 7.1



RHEL
6 / 7



SLES
11 / 12



Ubuntu Server
12.04 / 14.04



Windows
2012 R2



SHARE YOUR VOICE

CALL FOR PRESENTATIONS NOW OPEN!

CHEFCONF 2017 | AUSTIN, TX | MAY 22-24



CFP CLOSES JANUARY 18TH

Nathen Harvey

VP, Community Development at Chef
Co-host of the Food Fight Show Podcast



Occasional farmer – <http://ei.chef.io>

Love eggs – <http://eggs.chef.io>

#hugops – <http://hugops.chef.io>

[@nathenharvey](https://twitter.com/nathenharvey)

nharvey@chef.io





CHEFTM