INSPEC

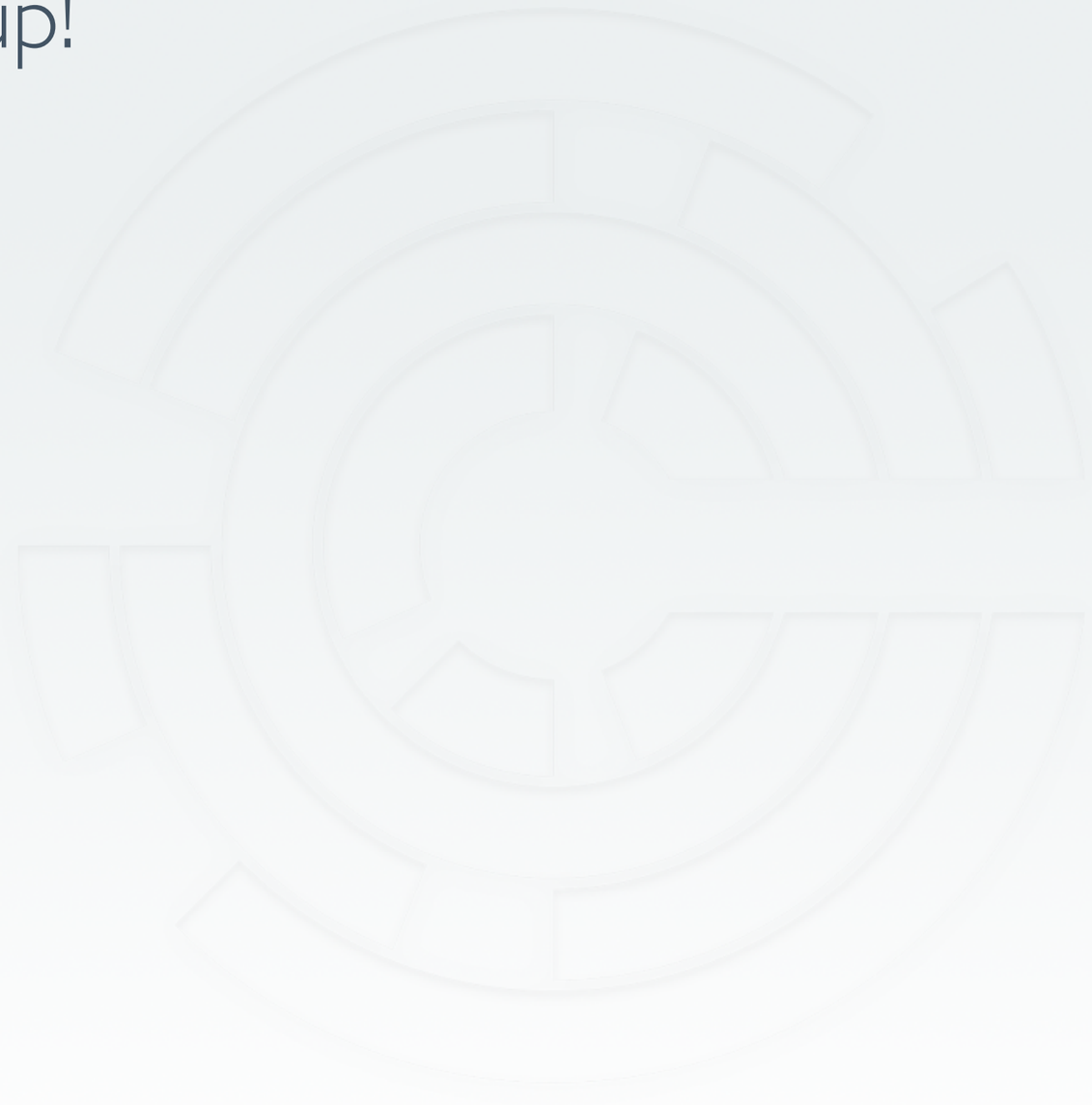
Making Compliance Fun

Nathen Harvey

CHEF

Hey, Nathen! Stream this meetup!

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



CHEF

Nathen Harvey

VP, Community Development at Chef

Co-host of the Food Fight Show Podcast

Occasional farmer – http://ei.chef.io

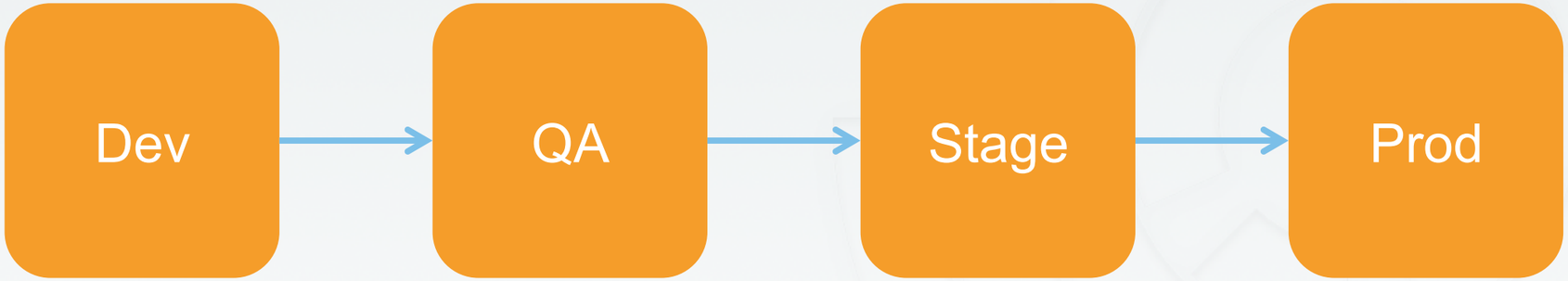
Love eggs – http://eggs.chef.io

#hugops – http://hugops.chef.io

@nathenharvey

nharvey@chef.io

CHEF



CHEF

CHEF™

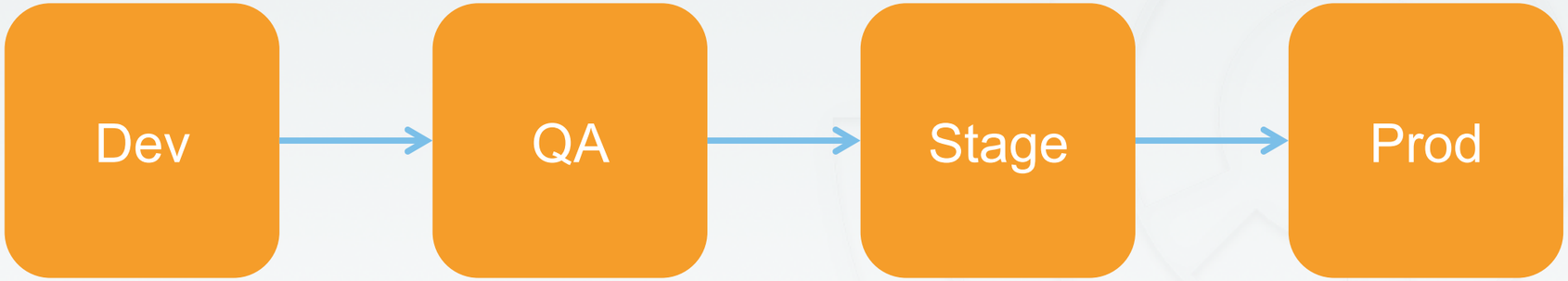
Demo

- 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

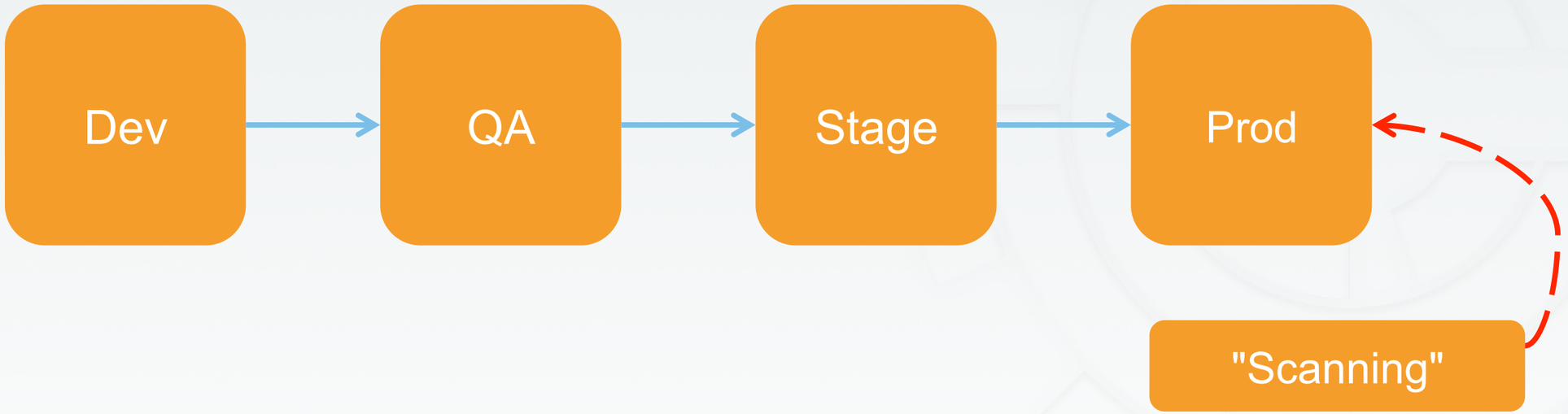
SSH supports two different protocol versions. The original version, SSHv1, was subject to a number of security issues. Please use SSHv2 instead to avoid these.



CHEF

CHEF

CHEF



CHEF

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

CHEF

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'

end
```

CHEF

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 [illegible] 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 ...
  "

end
```

CHEF

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 [illegible] 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
```

CHEF

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 [illegible] 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
```

CHEF

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
```

CHEF

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
```

CHEF

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
```

CHEF

Test a Docker Container

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

```
Target:  docker://
8eb7760bd9db046cfc826f36a6997b02a1cd884684870b78cede0ab03b62571a
 ✔  ssh-6.2.1: Set SSH Protocol to 2
     ✔  SSH Configuration Protocol should eq "2"



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

CHEF

Stand Alone Usage

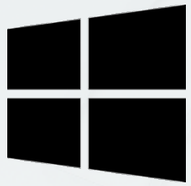
```
describe sshd_config do
  its('Protocol') { should cmp 2 }
end
```

```
$ 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



Windows Support

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

Native Packages

- Windows
- macOS
- Redhat & Ubuntu

Remote and agent-based execution

- Custom sudo commands
- more ssh options

Patch Management

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

Chef Ecosystem

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

CHEF™

InSpec Profiles

OS Hardening Profile

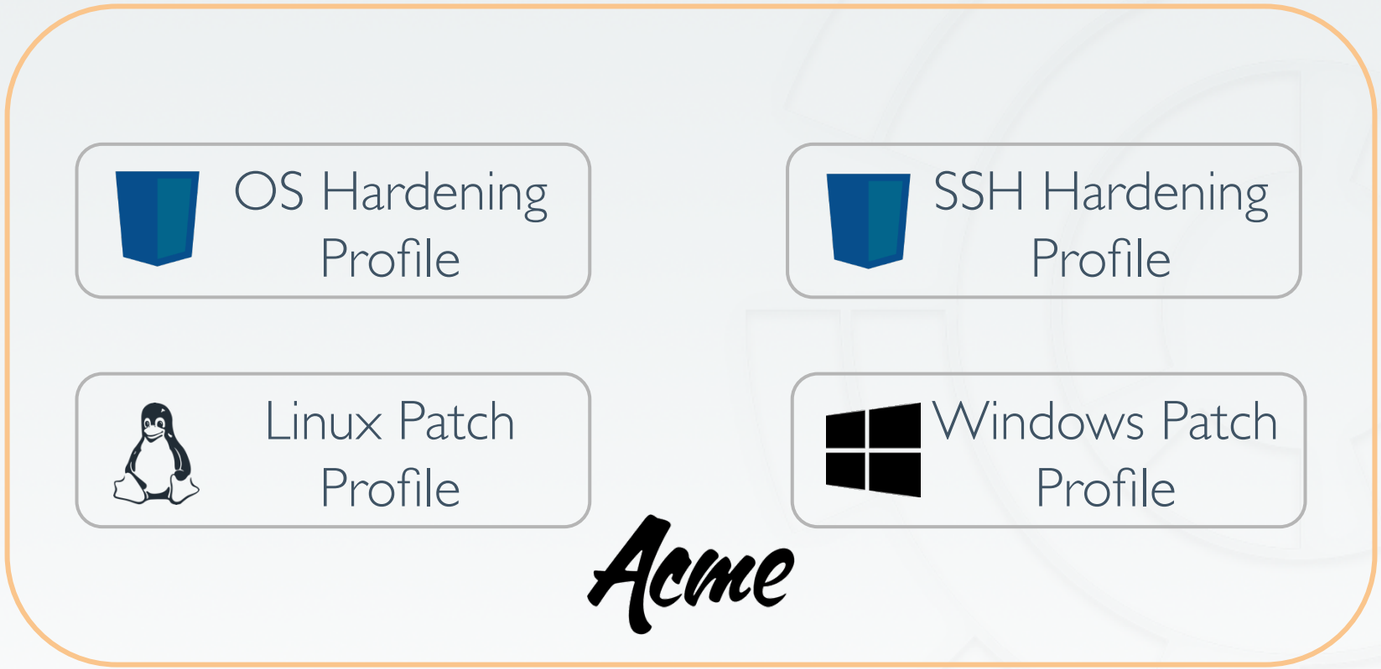
SSH Hardening Profile

Linux Patch Profile

Windows Patch Profile

CHEF

InSpec Profiles



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.

CHEF

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
```

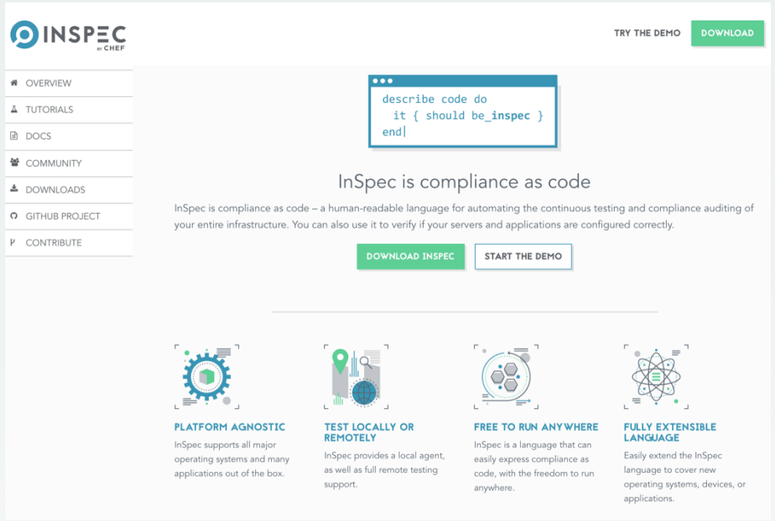
INSPEC

Available Resources

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

CHEF

Further Resources



inspec.io

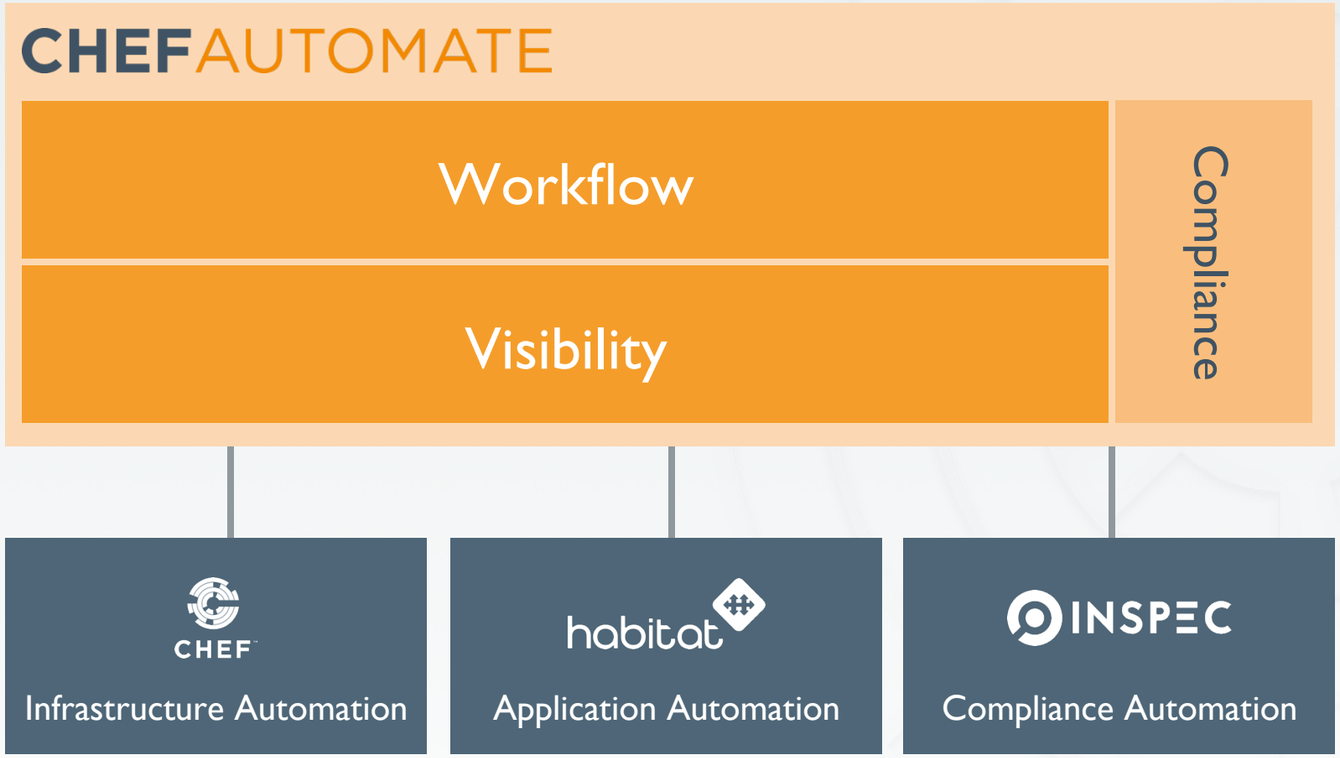
- Hands on tutorials
- Extensive documentation
- Code examples

learn.chef.io

- More tutorials about Compliance and Inspec

CHEF

Chef Automate



Chef Automate

Center for Internet Security®

Chef Compliance ships with profiles for:

Amazon Linux
2014.09 / 2015.03

CentOS
6 / 7

HP UX
11i

IBM AIX
5.3 / 6.1 / 7.1

RHEL
6 / 7

SLES
11 / 12

Ubuntu Server
12.04 / 14.04

Windows
2012 R2

CHEF


SHARE
YOUR
VOICE
CHEF
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

nharvey@chef.io

CHEF

CHEF™