CHEF™

CHEF


InSpec

Create a check

```
describe service 'ssh-agent' do
  it { should be_running }
end
```

Test a target

```
$ inspec exec test.rb
.

Finished in 0.00901 seconds (files took 0.98501 seconds to load)
1 example, 0 failures
```

Test Locally

```
$ inspec exec test.rb
```


CHEF

Test Remote via SSH

```
$ inspec exec test.rb -i ~/.aws/nathen.pem -t ssh://ec2-user@54.152.7.203
```

CHEF

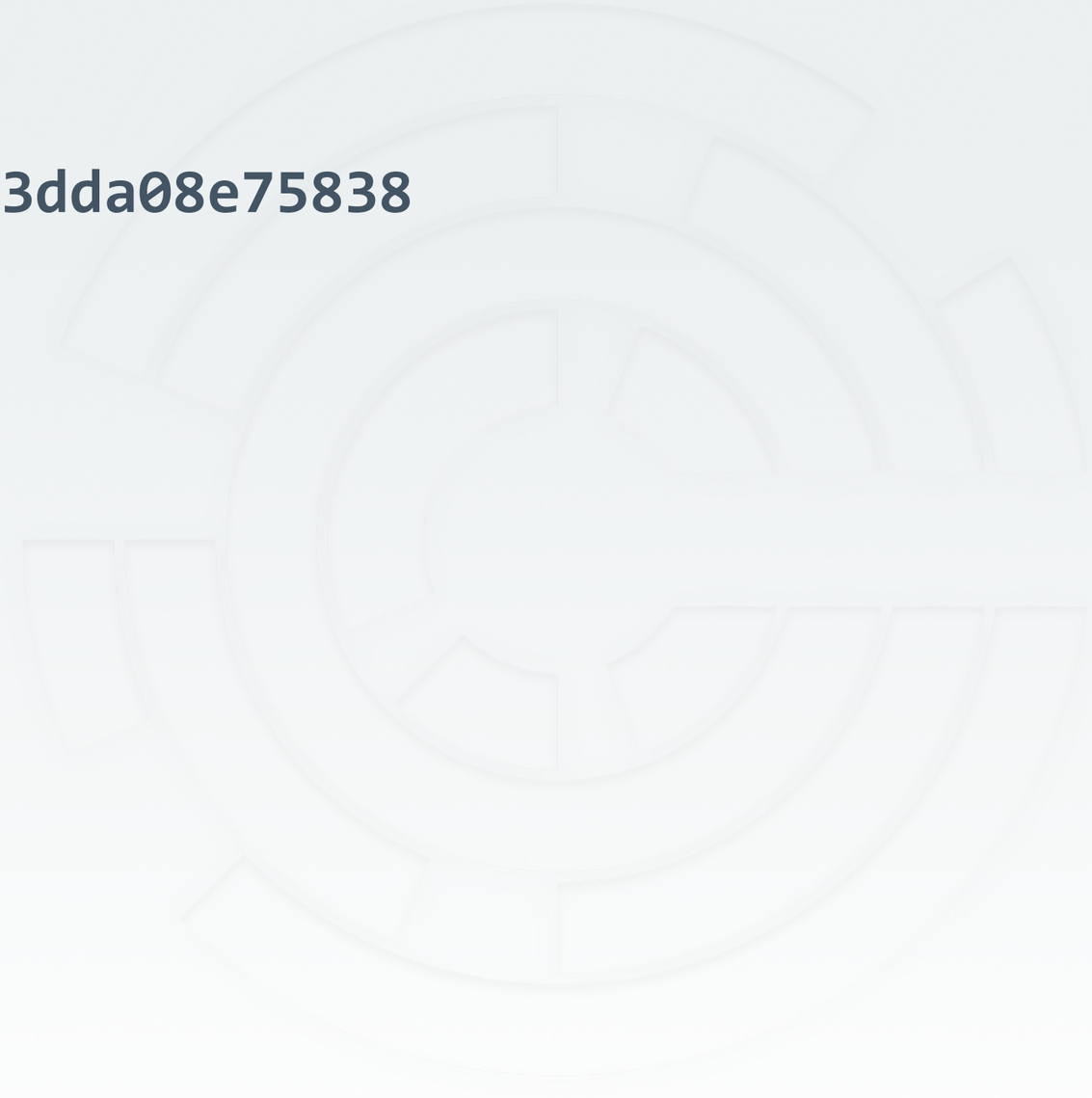
Test Remote via WinRM

```
$ inspec exec test.rb -t winrm://Admin@192.168.1.2 --password super
```

CHEF

Test Docker Container

```
$ inspec exec test.rb -t docker://3dda08e75838
```



CHEF

Test Any Target

```
$ inspec exec test.rb
```

```
$ inspec exec test.rb -i ~/.aws/nathen.pem -t ssh://ec2-user@54.152.7.203
```

```
$ inspec exec test.rb -t winrm://Admin@192.168.1.2 --password super
```

```
$ inspec exec test.rb -t docker://3dda08e75838
```

CHEF

InSpec

Test any target

CHEF

SSH Control

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.

SSH Control

SSH supports two diff… incompatible prot…H1 and SSH2. SSH1 w… original protocol and was su… security issues. SSH2 is more advanced and secure.

How would you check this?

SSH Version Check

```
describe file('/etc/ssh/sshd_config') do
  its(:content) { should match /Protocol 2/ }
end
```

SSH Version Check

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

SSH Version Check

```
describe sshd_config do

  title 'SSH Version 2'









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


CHEF

SSH Version Check

```
describe sshd_config do


  title 'SSH Version 2'

  desc <<-EOF
    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.
  EOF

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

CHEF

SSH Version Check

```
describe sshd_config do
  impact 1.0

  title 'SSH Version 2'

  desc <<-EOF
    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.
  EOF

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

CHEF

Available Resources

apache_conf
apt
audit_policy
auditd_conf
auditd_rules
bond
bridge
csv
command
directory
etc_group
file
gem
group
host
inetd_conf
interface
iptables
kernel_module
kernel_parameter
limits_conf
login_defs
mount
mysql_conf
mysql_session
npm
ntp_conf
oneget
os
os_env
package
parse_config
parse_config_file
passwd
pip
port
postgres_conf
postgres_session
powershell
processes
registry_key
security_policy
service
ssh_config
sshd_config
user
windows_feature
yaml
yum

CHEF

etc_group

```
describe etc_group.where(item: 'value', item: 'value') do
  its('gids') { should_not contain_duplicates }
  its('groups') { should include 'user_name' }
  its('users') { should include 'user_name' }
end
```

host

```
describe host('example.com', port: 80, proto: 'tcp') do
  it { should be_reachable }
end
```

CHEF

login_defs

```
describe login_defs do
  its('PASS_MAX_DAYS') { should eq '180' }
  its('PASS_MIN_DAYS') { should eq '1' }
  its('PASS_MIN_LEN') { should eq '15' }
  its('PASS_WARN_AGE') { should eq '30' }
end
```

mysql_conf

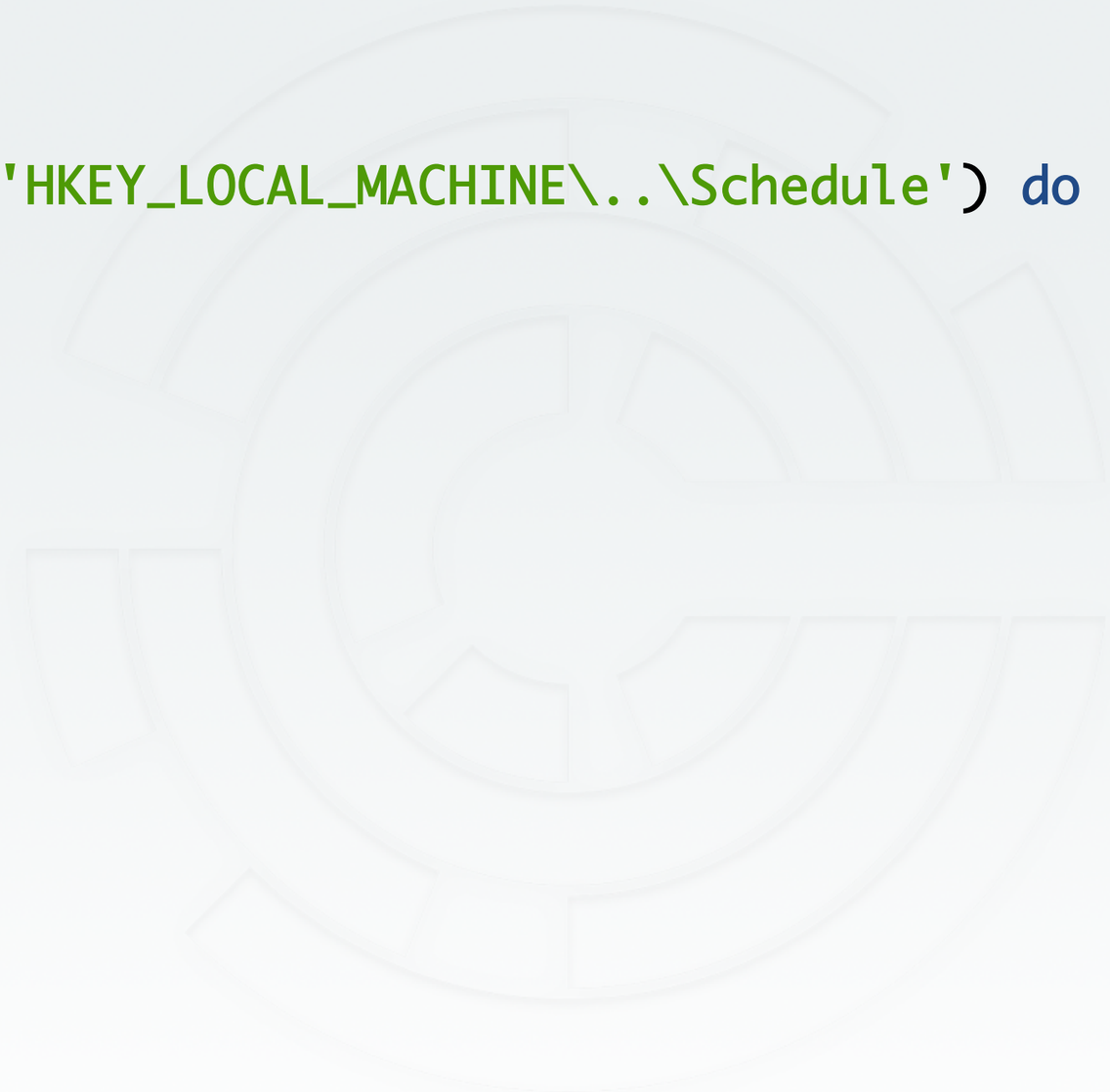
```
describe mysql_conf do
  its('slow_query_log_file') { should eq 'hostname_slow.log' }
  its('slow_query_log') { should eq '0' }
  its('log_queries_not_using_indexes') { should eq '1' }
  its('long_query_time') { should eq '0.5' }
  its('min_examined_row_limit') { should eq '100' }
end
```

mysql_session

```
sql = mysql_session('my_user','password')
describe sql.query('show databases like \'test\';') do
  its(:stdout) { should_not match(/test/) }
end
```

registry_key

```
describe registry_key('Task Scheduler','HKEY_LOCAL_MACHINE\..\Schedule') do
  its('Start') { should eq 2 }
end
```



CHEF

InSpec

Test any target

Be expressive

CHEF

InSpec

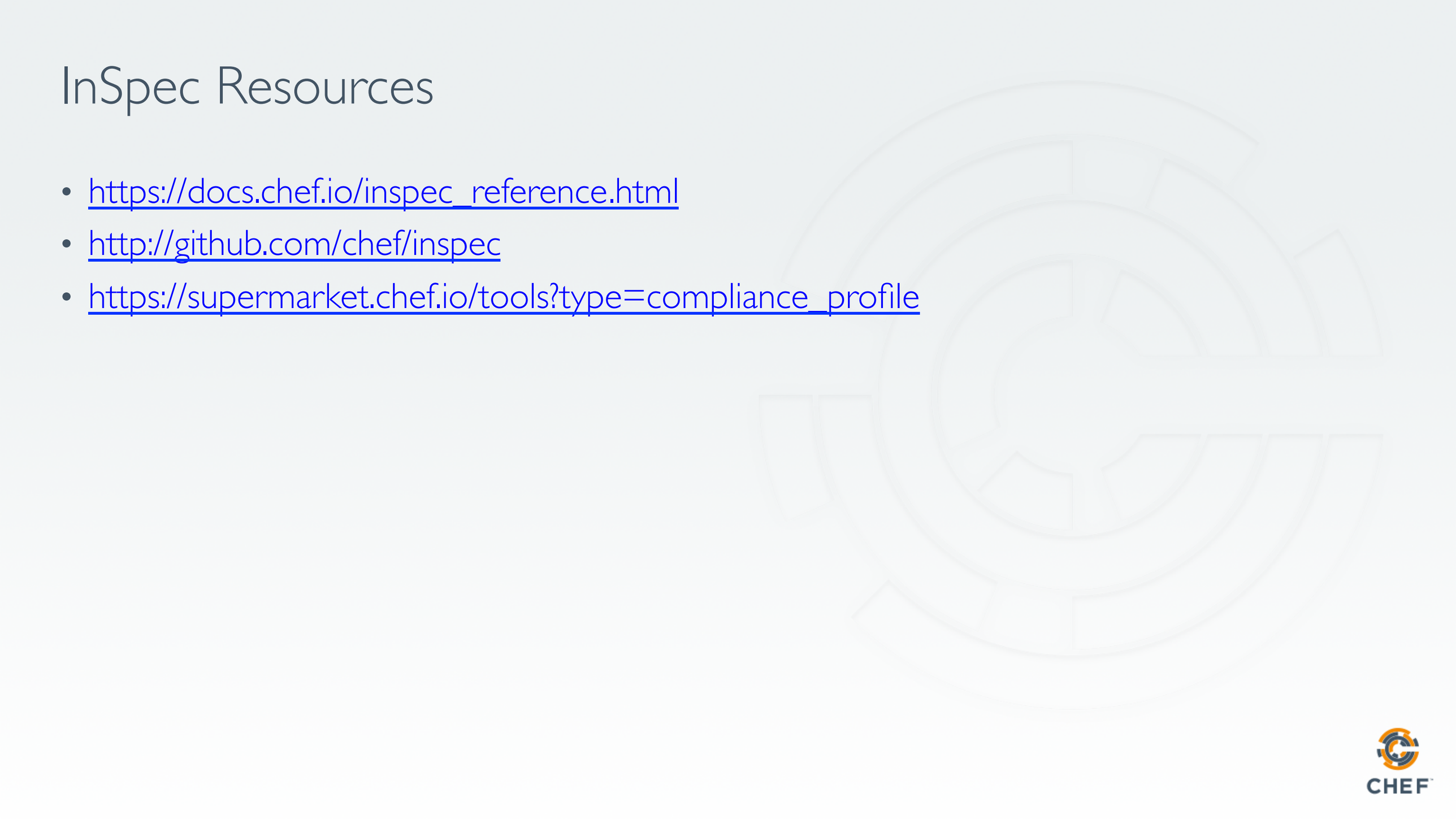
Open Source

https://github.com/chef/inspec

CHEF

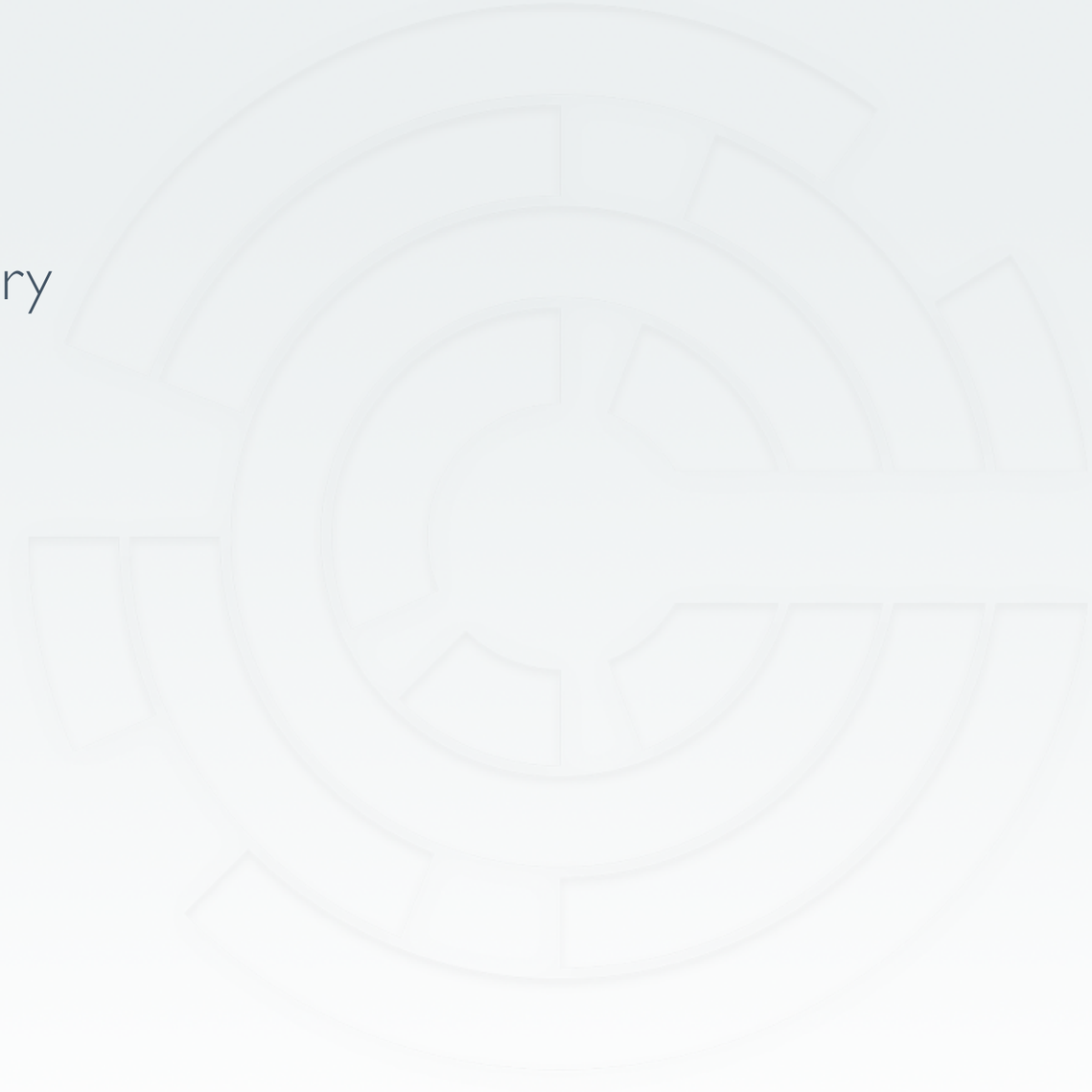
InSpec Resources

- https://docs.chef.io/inspec_reference.html
- http://github.com/chef/inspec
- https://supermarket.chef.io/tools?type=compliance_profile



Hack Day Rules

- Work in teams of 2-4 people
- Track your work in a version control repository
- Demonstrate and Share your work
- Ask for help
- Be open to learning
- Have fun



CHEF

Write & Execute Inspec for CIS Benchmarks

- https://github.com/chef-training/workshops/tree/master/InSpec
- Download the CIS CentOS Linux 6 Benchmark
- Write InSpec for some of the controls
- Execute InSpec on your target machine
- Remediate anything that is out of policy by writing Chef Cookbooks (optional)

CHEF™

CHEF