INSPEC

OR HOW TO TRANSLATE COMPLIANCE SPREADSHEETS INTO CODE

Created by Michael Goetz / ✉ mpgoetz@chef.io / @michaelpgoetz

WHO AM I?

- Michael Goetz
- Solutions Engineering Manager @ Chef
- mpgoetz@chef.io
- @michaelpgoetz

WHAT IS INSPEC?

InSpec

“Infrastructure Specification”

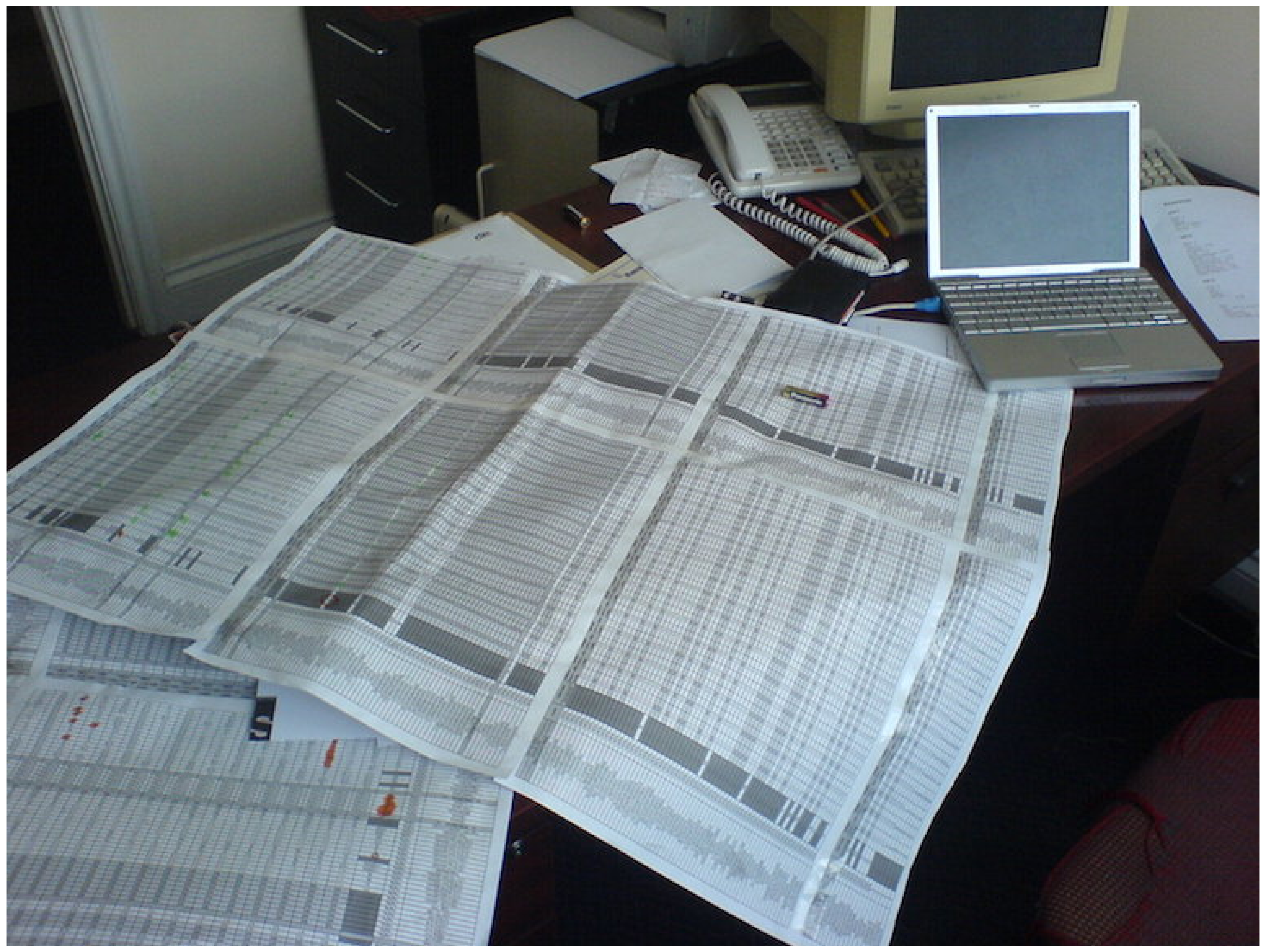
WHY NOT SERVERSPEC?

- Additional metadata (impact, title, description) make it easier to describe & share controls
- Focusing on multi-platform support (Windows, Docker, Linux)
- A command line interface (CLI) is required for faster iteration of test code.

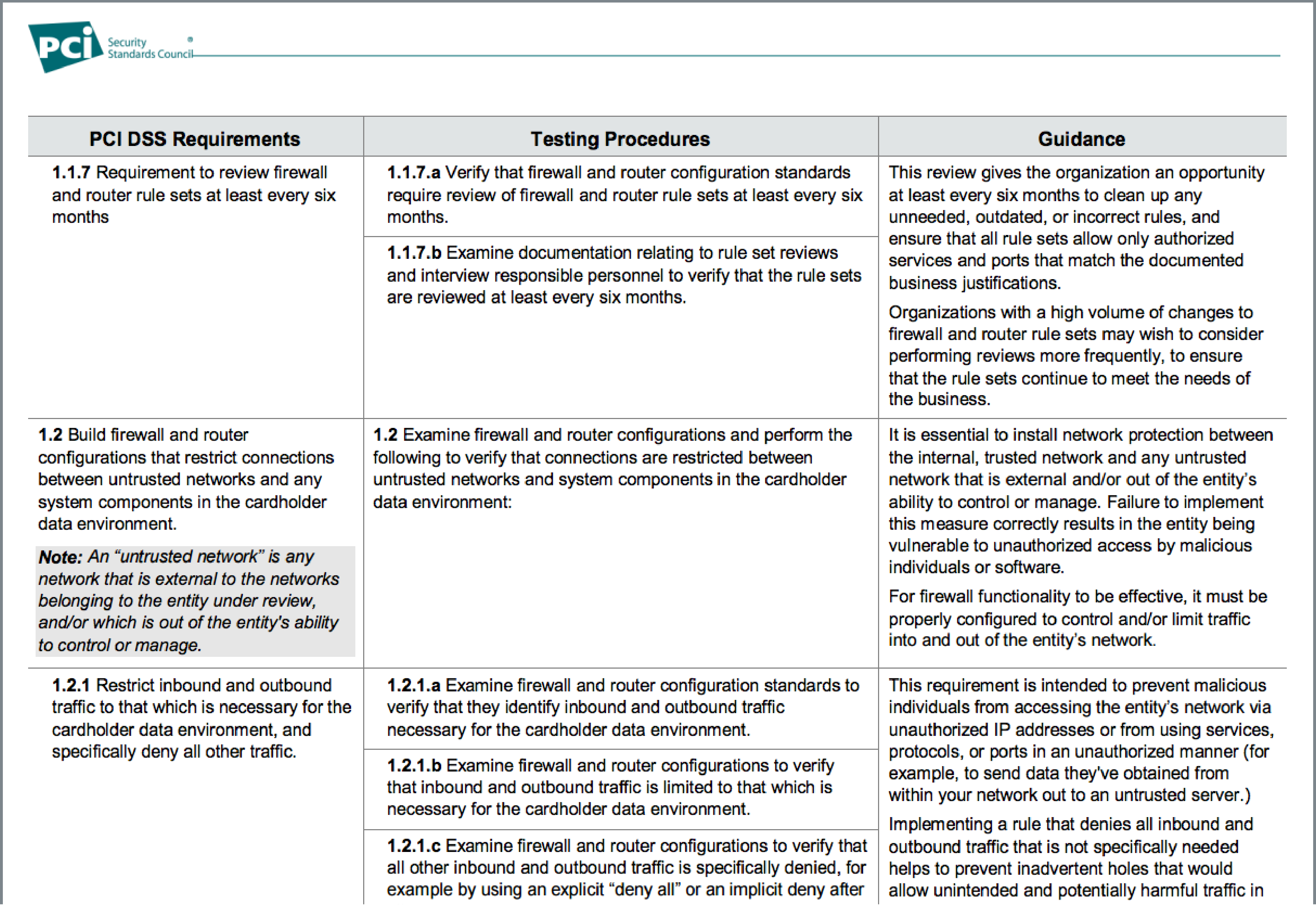
COMPLIANCE IS EVERYWHERE

DoD Security Technical Implementation Guides (STIG)	Payment Card Industry Data Security Standards (PCI)	Sarbanes-Oxley (SOX)
Health Information Technology for Economic and Clinical Health (HITECH)	Health Insurance Portability and Accountability Act of 1996 (HIPAA)	Center for Internet Security (CIS)

SPREADSHEET



PDF



PCI Security Standards Council

PCI DSS Requirements	Testing Procedures	Guidance
1.1.7 Requirement to review firewall and router rule sets at least every six months	**1.1.7.a** Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months.	This review gives the organization an opportunity at least every six months to clean up any unneeded, outdated, or incorrect rules, and ensure that all rule sets allow only authorized services and ports that match the documented business justifications. Organizations with a high volume of changes to firewall and router rule sets may wish to consider performing reviews more frequently, to ensure that the rule sets continue to meet the needs of the business.
	1.1.7.b Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months.	
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. ***Note:*** *An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	**1.2** Examine firewall and router configurations and perform the following to verify that connections are restricted between untrusted networks and system components in the cardholder data environment:	It is essential to install network protection between the internal, trusted network and any untrusted network that is external and/or out of the entity's ability to control or manage. Failure to implement this measure correctly results in the entity being vulnerable to unauthorized access by malicious individuals or software. For firewall functionality to be effective, it must be properly configured to control and/or limit traffic into and out of the entity's network.
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	**1.2.1.a** Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment.	This requirement is intended to prevent malicious individuals from accessing the entity's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within your network out to an untrusted server.) Implementing a rule that denies all inbound and outbound traffic that is not specifically needed helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic in
	1.2.1.b Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment.	
	1.2.1.c Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after	

XML

```
<Rule id="usgcb-rhel5desktop-rule-2.2.2.5.d" selected="false" weight="10
  <status date="2011-09-30">accepted</status>
  <version update="1"/>
  <title override="0">CCE-15087-0:Disable Mounting of hfs</title>
  <description override="0"> Using the install command inside /etc/modpro
      the kernel module loading system to run the command speciï¬ed (here
      /bin/true) instead of inserting the module in the kernel as normal
      effectively prevents usage of these uncommon ï¬lesystems.</descript
  <ident system="http://cce.mitre.org">CCE-15087-0</ident>
  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5" sele
    <check-content-ref href="usgcb-rhel5desktop-oval.xml" name="oval:gov
  </check>
</Rule>
```

ANATOMY OF A CONTROL

```
describe sshd_config do
  its('Port') { should eq('22') }
end
```

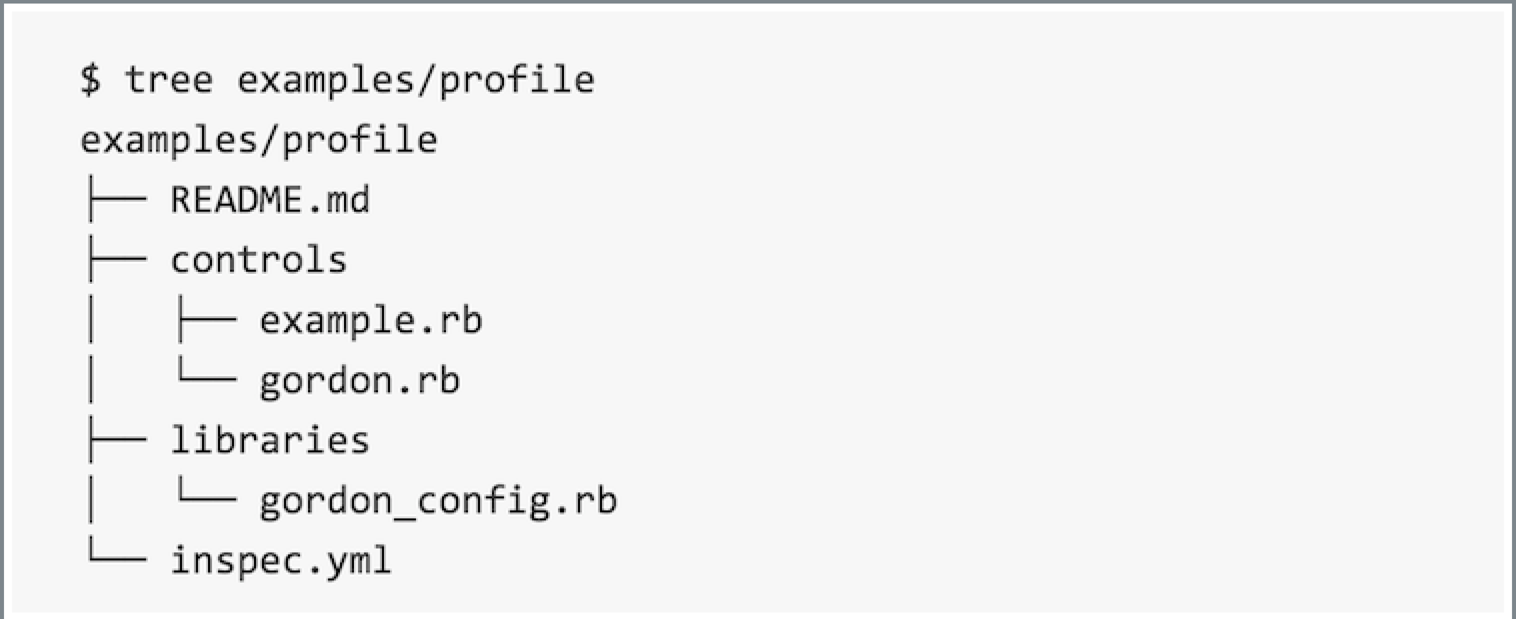
- `describe` is a block that contains at least one test
- `sshd_config` is an InSpec resource

ANATOMY OF A CONTROL

```
control 'sshd-8' do
  impact 0.6
  title 'Server: Configure the service port'
  desc '
    Always specify which port the SSH server should listen to.
    Prevent unexpected settings.
  '
  describe sshd_config do
    its('Port') { should eq('22') }
  end
end
```

- `'sshd-8'` is the name of the control
- `control` must contain at least one `describe` block
- `impact`, `title`, and `desc` define metadata to describe the control

PROFILES



```
$ tree examples/profile
examples/profile
├── README.md
├── controls
│   ├── example.rb
│   └── gordon.rb
├── libraries
│   └── gordon_config.rb
└── inspec.yml
```

- `inspec.yml` - the profile description (required)
- `controls` - contains all tests (required)
- `libraries` - contains InSpec resource extensions (optional)

PROFILE MANIFEST

```
name: profile
title: InSpec Example Profile
maintainer: Chef Software, Inc.
copyright: Chef Software, Inc.
copyright_email: support@chef.io
license: Apache 2 license
summary: Demonstrates the use of InSpec Compliance Profile
version: 1.0.0
supports:
  - os-family: linux
```

- `name` - Identifier of the profile (required)
- Profiles can also be included in other profiles by referring to the name.

PROFILE OS SUPPORT

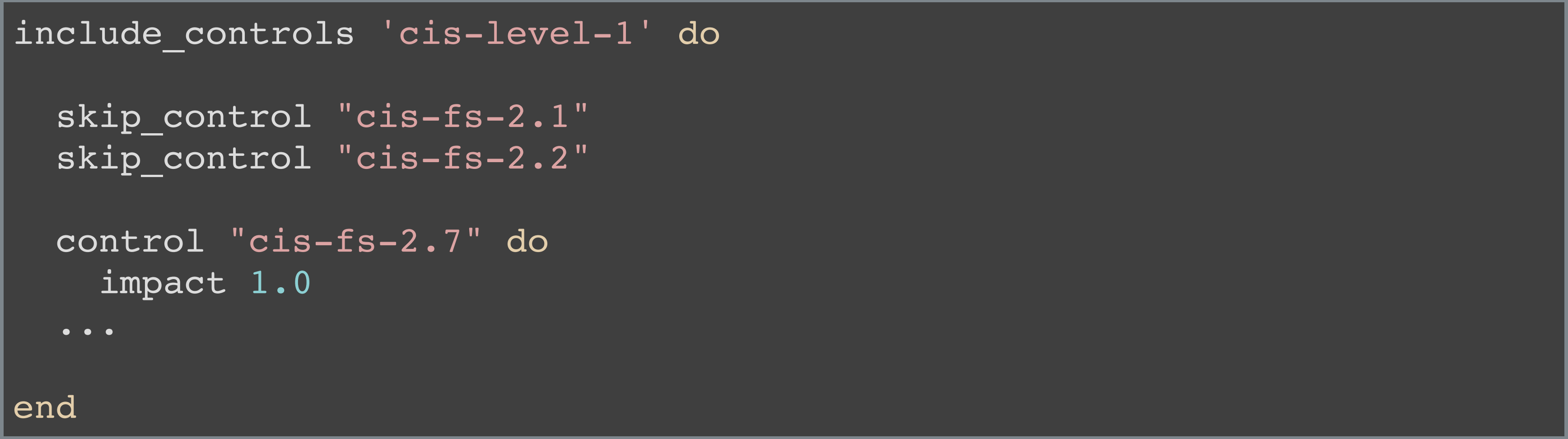
```
supports:
  // Runs on any version of Debian Linux
  - os-name: debian

  // Only runs on Ubuntu 14.04
  - os-name: ubuntu
    release: 14.04

  // Targets RedHat, CentOS, Oracle Linux ...
  - os-family: redhat
```

Restrict your profiles to only support targeted operating systems.

PROFILE INHERITANCE



```
include_controls 'cis-level-1' do

  skip_control "cis-fs-2.1"
  skip_control "cis-fs-2.2"

  control "cis-fs-2.7" do
    impact 1.0
  ...

end
```

Include all controls from external profiles and skip specific controls if necessary.

PROFILE CONTROL INCLUSION

```
require_controls 'cis-level-1' do

  control "cis-fs-2.1"
  control "cis-fs-2.2"

end
```

If you just need a few controls from a profile, you can require just specific controls.

PROFILE VALIDATION & DISTRIBUTION

```
$ inspec check examples/profile
```

Check your profile syntax with the `inspec check` command.

```
# will generate a example-profile.tar.gz
$ inspec archive examples/profile

# will generate a example-profile.zip
$ inspec archive examples/profile --zip
```

Package and redistribute using `gzip`, `bzip2`, or `xz`

CUSTOM RESOURCES

Just like Chef, you can define your own custom InSpec resources if you need them.

```
require 'yaml'

class GordonConfig < Inspec.resource(1)
  name 'gordon_config'

  def initialize
    @path = '/etc/gordon/config.yaml'
    @file = inspec.file(@path)
    return skip_resource "Can't find file \"#{@path}\"" if !@file.file?

    @params = YAML.load(@file.content)
  end

  def method_missing(name)
    @params[name.to_s]
  end
end
```

Include them in `libraries` folder in your profiles.

RUNNING INSPEC TESTS

- Local

```
inspec exec test.rb
```

- Remote via SSH

```
inspec exec test.rb -t ssh://user@hostname
```

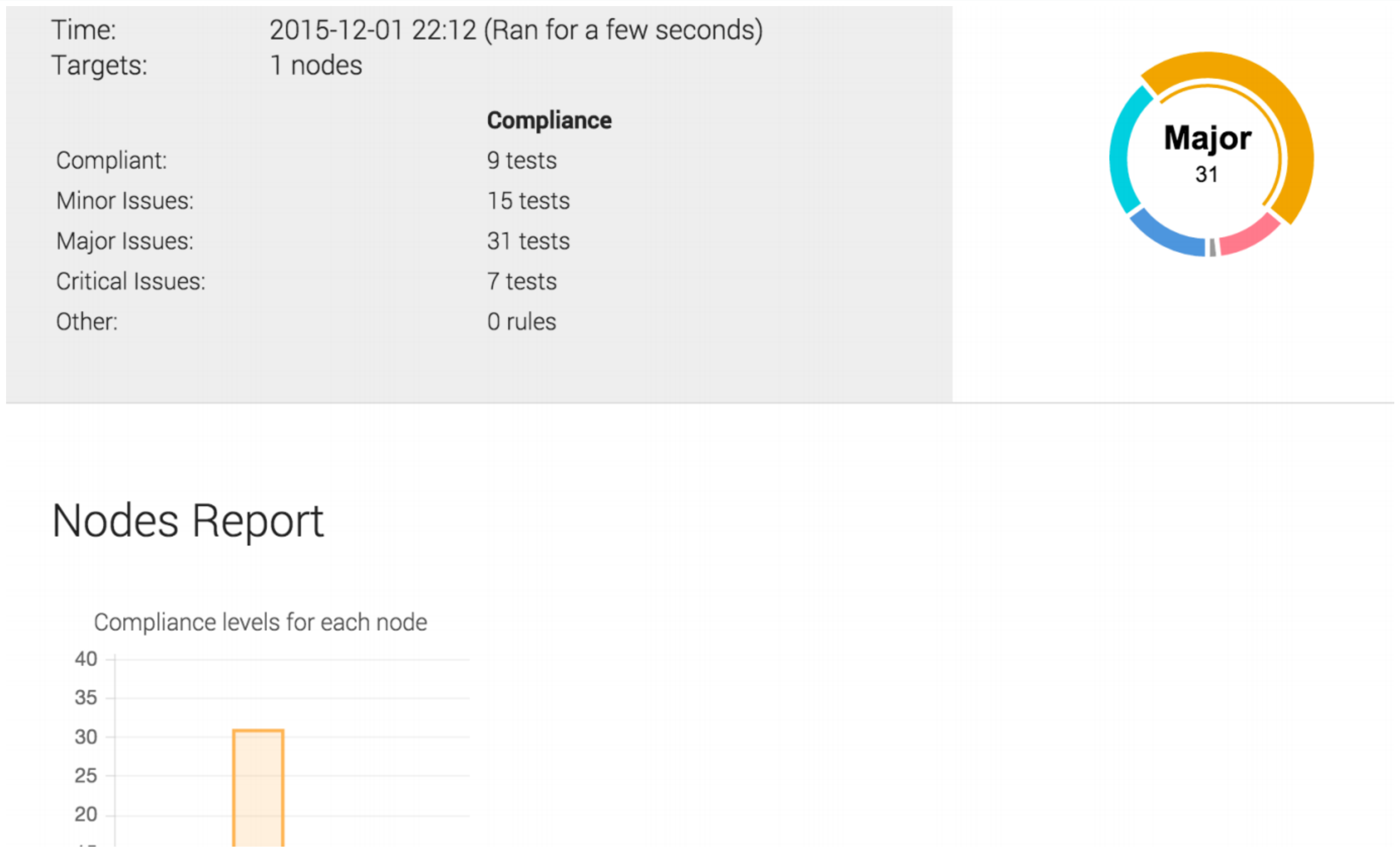
- Remote via WinRM

```
inspec exec test.rb -t winrm://Administrator@windowshost --password 'pa
```

- Docker, Docker, Docker

```
inspec exec test.rb -t docker://container_id
```

VISUALIZE RESULTS WITH CHEF COMPLIANCE



Time:	2015-12-01 22:12 (Ran for a few seconds)
Targets:	1 nodes

	Compliance
Compliant:	9 tests
Minor Issues:	15 tests
Major Issues:	31 tests
Critical Issues:	7 tests
Other:	0 rules

Nodes Report

Compliance levels for each node

MORE INFORMATION

- The Road to InSpec - https://www.chef.io/blog/2015/11/04/the-road-to-inspec/
- InSpec - https://github.com/chef/inspec
- InSpec Reference - https://docs.chef.io/inspec_reference.html

THANK YOU!

What questions do you have?