Inspec -
Compliance Automation

Powered by Chef

Compliance Testing - What and Why?

-> It is a methodology to ensure that the system meets a defined set of standards.

-> It is performed to maintain and validate the compliant state for the life of the system/software. Every industry has a regulatory and compliance board that takes care of this.

Requirements for Compliance Testing:

- Professionals, who are knowledgeable and experienced, who understand the compliance must be retained.
- Understanding the risks and impacts of being non-compliant
- Document the processes and follow them
- Perform an internal audit and follow with an action plan to fix the issues

Infrastructure Testing tools

1. InSpec
2. ChefSpec
3. Serverspec
4. Testinfra

Inspec

-> InSpec is an open-source testing framework for application and infrastructure with a human-readable language for specifying compliance, security and other policy requirements.

->InSpec works by comparing the actual state of your system with the desired state that you express in InSpec code.

->InSpec detects violations and displays findings in the form of a report, but puts you in control of remediation.

-> Easily integrate automated tests that check for adherence to policy into any stage of your deployment pipeline.

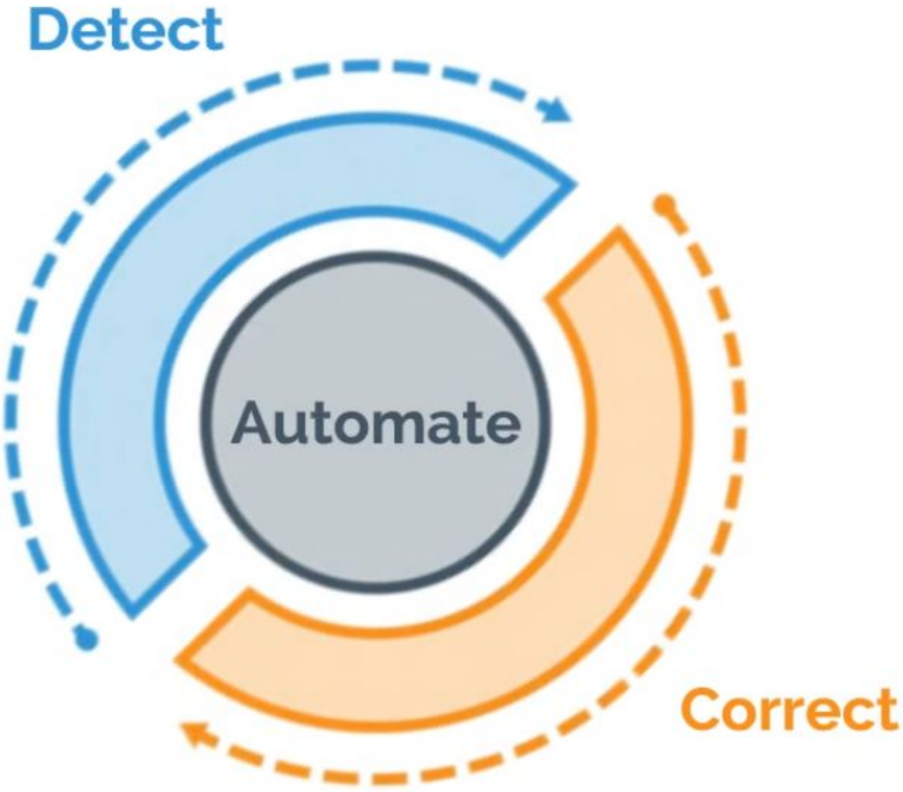
Why InSpec?

1. It's open source. It uses a a simple to understand language.
2. Its development is supported by Chef Software Inc., it probably won't disappear like some nodejs libs in the past and it won't be abandoned.
3. Awesome community. If you have any issues, you can always ask for help on Chef slack's InSpec channel, core maintainers are frequently the first responders.
4. Resource-rich. There is large library of resources available and this number is growing. If you need something unusual you can always use file/command resources or contribute to InSpec.
5. Can run anywhere. From your local workstation, you can verify machine over ssh, docker or winrm.
6. It has an interactive shell.
7. It works on most popular operating systems. On less popular too!
8. It ensures Cloud Configurations such as AWS and Azure policies are compliant.

9. InSpec doesn't require any agent to be installed on nodes. You can run InSpec tests across all of your nodes.

The journey to continuous automation

Three steps to improvement across all dimensions of software success



1. **Detect**

   Gain visibility and develop baselines

2. **Correct**

   Remediate priority issues

3. **Automate**

   Continuously detect & correct

Case Study

Compliance with InSpec at Niu Solutions

Business Challenge

Niu Solutions offers managed services to regulated industries including retail and financial services

- Customers undergoing rapid change
- Stringent regulatory reporting requirements
- Heterogeneous environments with significant legacy technology

Solution

Niu worked with Chef to automate compliance across hybrid environments and collaborate among teams

- Reduced time spent on compliance checks by 93%
- Achieved ongoing audit readiness
- Eliminated unplanned work

> **"Once something is built and it's handed over, they know it's compliant and it's continuously compliant."**
>
> - Jon Williams, CTO

Customer Journey

Detect

Applied InSpec to test against regulatory standards and best practices

Reduced time spent on compliance checks by 93%

Correct

Deployed fixes with Chef and gathered lessons learned to improve detection capabilities

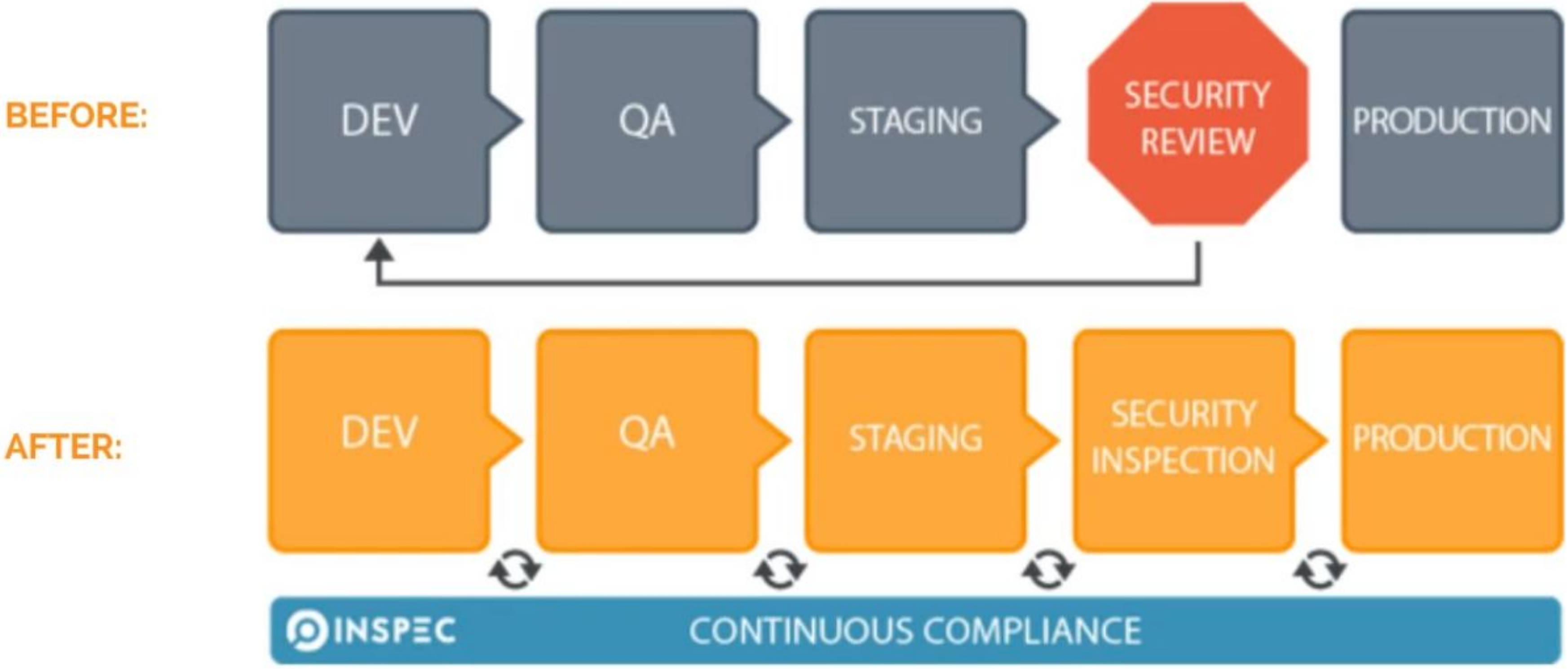
Reduced SQL setup time from one full day to 12 mins

Automate

Integrating the detect and correct cycle and collaborating across teams

Extending library of 1000 compliance controls

Traditional Compliance vs. InSpec

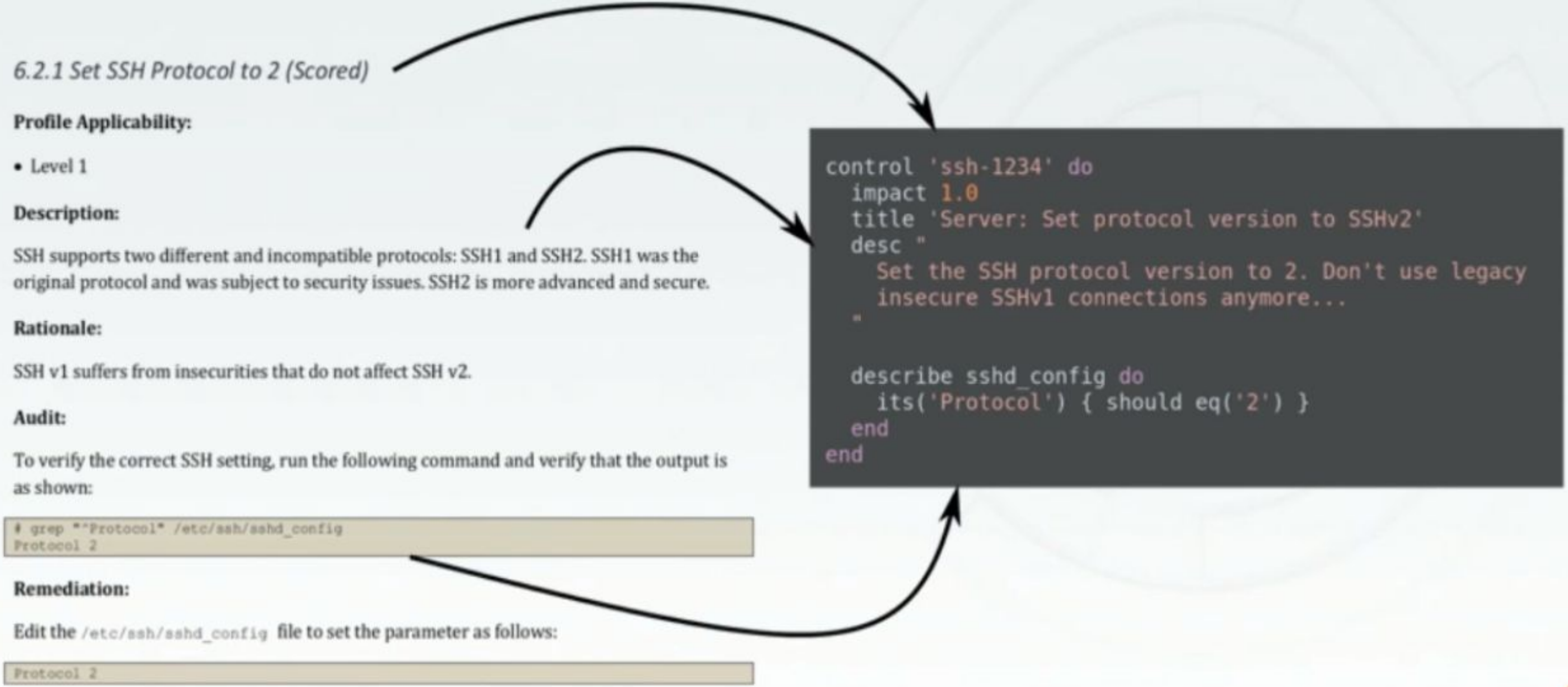


Compliance and policy configuration throughout the SDLC

InSpec

turns infrastructure testing, compliance and security requirements into code

Mapping of 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:

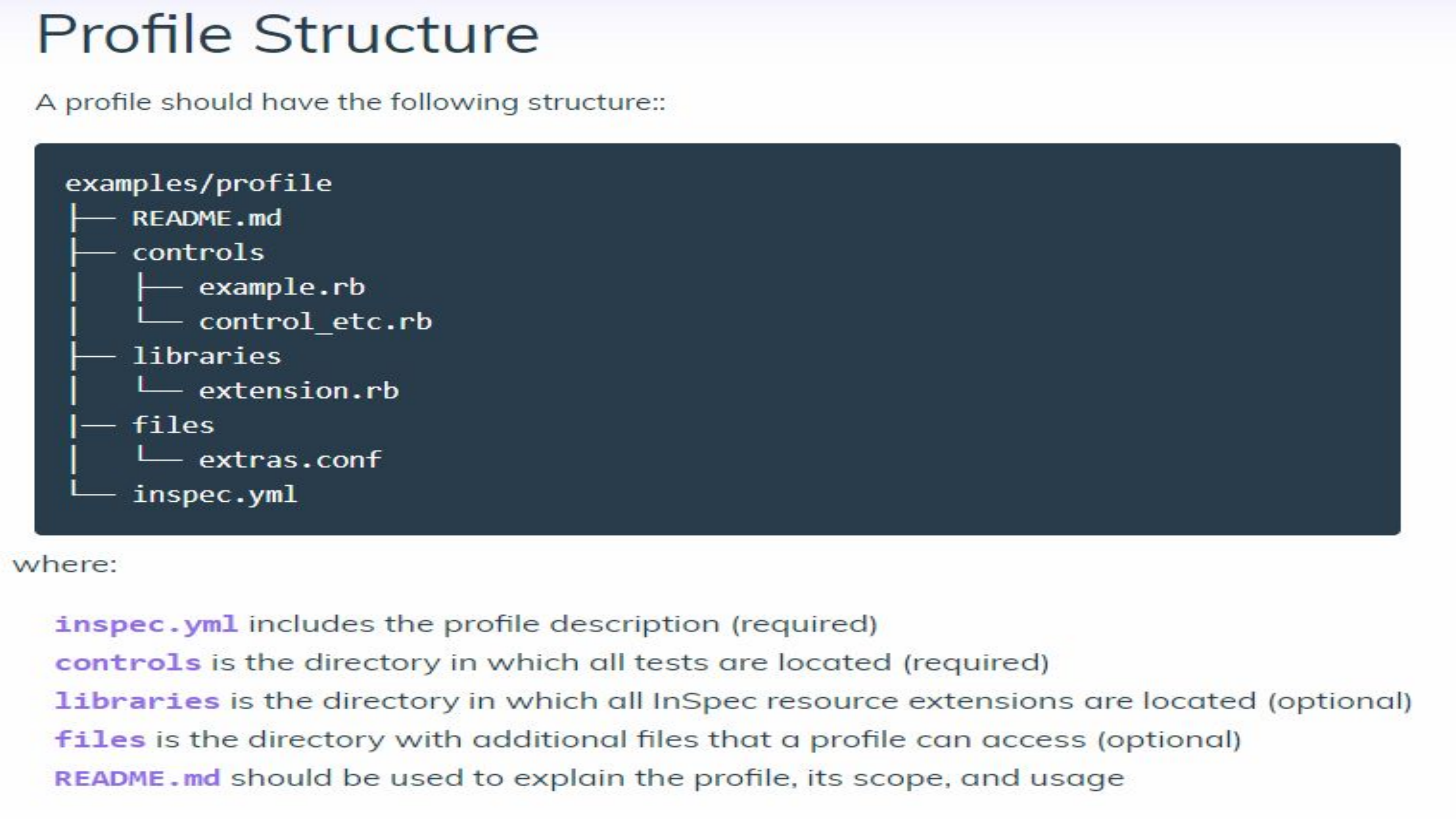
```
Protocol 2
```

```
control 'ssh-1234' do
  impact 1.0
  title 'Server: Set protocol version to SSHv2'
  desc "
    Set the SSH protocol version to 2. Don't use legacy
    insecure SSHv1 connections anymore...
  "

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

InSpec Installation

1. Chef Development Kit
2. Chef Client
3. Gem Install
4. InSpec Package



Profile Structure

A profile should have the following structure::

```
examples/profile
├── README.md
├── controls
│   ├── example.rb
│   └── control_etc.rb
├── libraries
│   └── extension.rb
|── files
│   └── extras.conf
└── inspec.yml
```

where:

- `inspec.yml` includes the profile description (required)
- `controls` is the directory in which all tests are located (required)
- `libraries` is the directory in which all InSpec resource extensions are located (optional)
- `files` is the directory with additional files that a profile can access (optional)
- `README.md` should be used to explain the profile, its scope, and usage

Demo

InSpec Tutorials

- Inspec.io
- learn.chef.io