INSPEC BY CHEF

Stop treating information security as an afterthought. Build security directly into the software delivery lifecycle by turning compliance, security, and other policy requirements into code.

InSpec is an open-source framework for describing security & compliance rules that can be shared between software engineers, operations, and security engineers. It is designed to be used at all stages of the software delivery process, from a developer's workstation all the way to production, with no performance impact or side-effects.

Using InSpec, you can:

- **Make compliance part of the development process.** Relying only on pre-production security scans slows down your development process and creates rework for engineers. Clear intent via executable code enables collaboration, replacing ambiguous rules written in imprecise formats like PDF or Excel.
- **Continuously detect compliance shortcomings and prioritize remediation.** InSpec's easy-to-use, agentless nature helps you quickly assess your compliance exposure. Built-in metadata for impact scoring allows you to focus on areas for subsequent remediation. Severity levels per control can also be customized to increase or decrease the criticality of findings, or even disable them in the face of compensating controls.
- **Make audits painless.** Answer audit questions at any time, not just quarterly or yearly. Enter an audit cycle knowing exactly your compliance posture, rather than being surprised by auditors finding weak points in your environment. Easily demonstrate how compliance has evolved and improved over time.

InSpec is easy to read and write by all parties involved in security. For example, here's how to translate a common compliance requirement into code using just a few lines:

```
control 'mac-01' do
  title 'Ensure SELinux is installed and enabled'
  desc  'SELinux provides Mandatory Access Control on Linux'
  impact 1.0
  describe package('libselinux') do
    it { should be_installed }
  end
  describe command('/sbin/getenforce') do
    its('stdout') { should match /Enforcing/ }
  end
  describe file('/etc/selinux/config') do
    its('content') { should match /SELINUX=enforcing/ }
  end
end
```

- A control allows for grouping of related tests
- Descriptive metadata helps relate code to the requirement
- Impact scoring allows you to prioritize remediation when controls go out of compliance
- High-level abstractions, known as resources, allow you to focus on the parameters to be tested, rather than needing to know how the data is being collected
- Matchers allow easy parsing of results without complicated regular expressions

InSpec comes with nearly 150 built-in resources to help you write compliance rules against common system and application configurations.

CHEF

619 Western Avenue Suite 400 | Seattle, WA 98104 PH: 206.508.4799 | sales@chef.io | www.chef.io

Cloud Compliance with InSpec

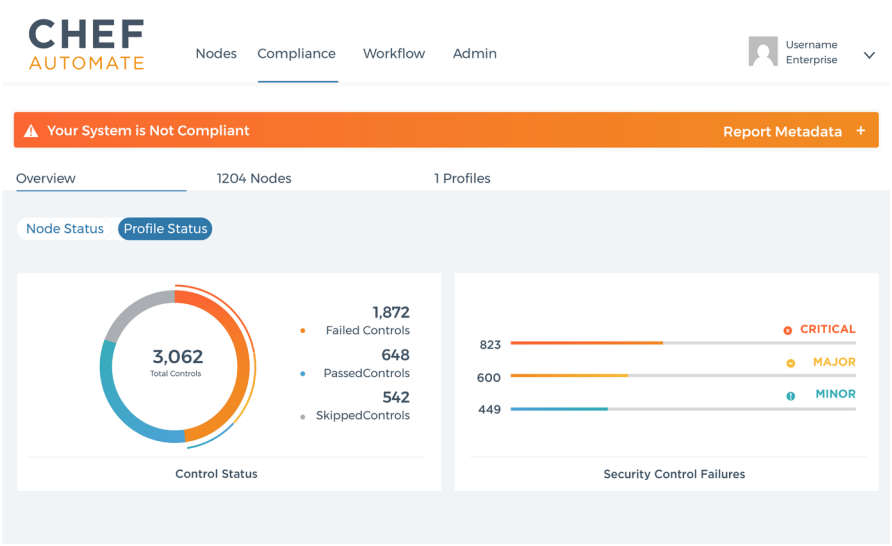
InSpec can check cloud resources for compliance using the cloud provider's API. For example, here is a rule to check that a webserver in Amazon Web Services (AWS) has the right configuration:

```
describe aws_ec2_instance(name: 'webserver') do
  it { should exist }
  it { should have_roles }
  its('instance_type') { should cmp 't2.medium' }
  its('image_id') { should cmp 'ami-fadc03fa' }
  its('subnet_id') { should cmp 'subnet-285c0900' }
end
```

Many other cloud resources such as security groups, storage buckets, and networking configurations can be checked in this way.

InSpec and Chef Automate

Chef Automate provides a real-time dashboard of all compliance data gathered by InSpec and displays it alongside infrastructure automation data from Chef if you are using it for configuration management. You can also initiate one-time or scheduled InSpec scans from within Chef Automate. Finally, Chef Automate supplies over 90 built-in InSpec profiles for standards like the Center for Internet Security (CIS) benchmarks, Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) and more, to get you started quickly with applying continuous compliance to your infrastructure.



Make compliance a priority in your software delivery process today by introducing continuous compliance using InSpec. Download or try **InSpec** at **www.inspec.io.**

> "InSpec has helped us unify our compliance, security and DevOps teams and streamlined audits, reducing the thousands of staff hours usually required by as much as 95 percent."
>
> ***— Jon Williams, CTO, Niu Solutions***