September 25 - 27, 2018
Amsterdam, The Netherlands

ons

EUROPE

OPEN NETWORKING //
Integrate, Automate, Accelerate

ons

EUROPE

OPEN NETWORKING //
Integrate, Automate, Accelerate

September 25 - 27, 2018
Amsterdam, The Netherlands

InSpec for Network Devices:

Extending Compliance-as-Code to the Network Administrator

Julian C. Dunn
Director of Product Marketing, Chef Software Inc.
jdunn@chef.io | @julian_dunn

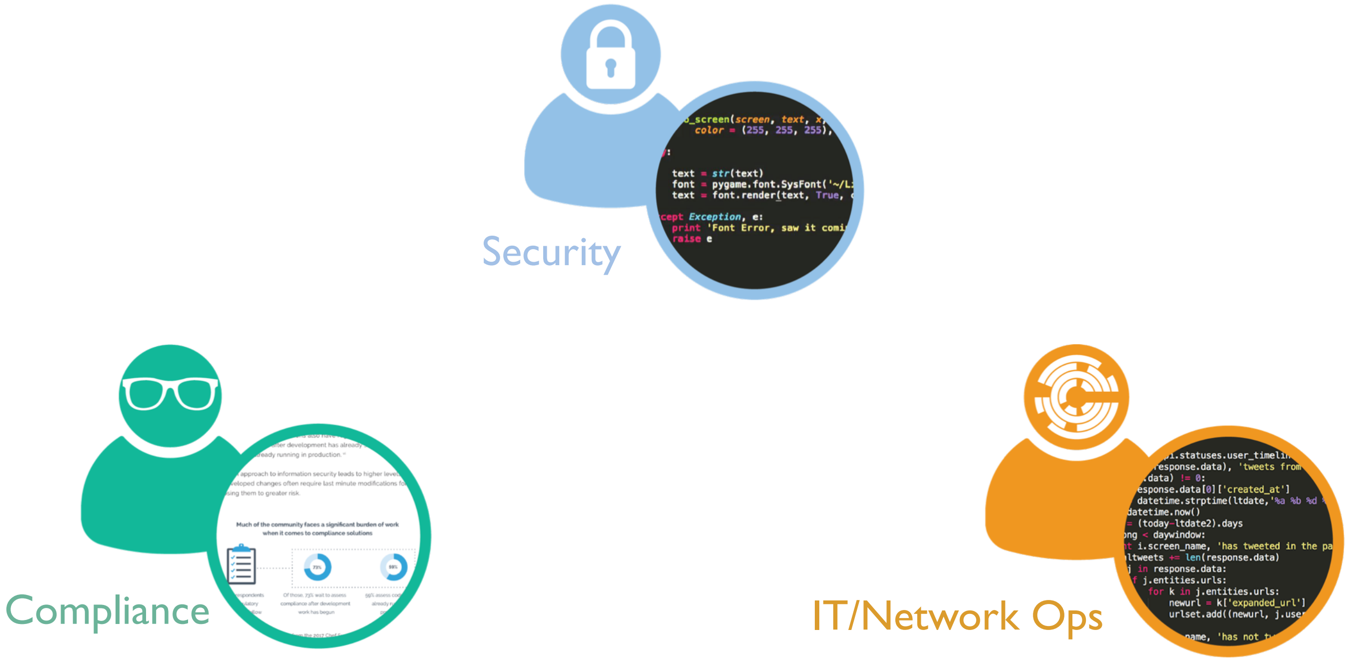
Agenda

- What is InSpec and Compliance as Code?
- InSpec Basics
- InSpec for Cloud Networking Compliance
- InSpec for Network Device Compliance
- How to get started

You have a lot of things in your network: servers, containers, network devices, clouds, Kubernetes, etc.

How do you know they’re installed and configured correctly?

Compliance is Often A Communication Problem



```
o_screen(screen, text, x,
    color = (255, 255, 255),

y:

    text = str(text)
    font = pygame.font.SysFont('~/Li
    text = font.render(text, True, c

cept Exception, e:
    print 'Font Error, saw it comi
    raise e
```

after development has already
already running in production.

approach to information security leads to higher level
veloped changes often require last minute modifications fo
sing them to greater risk.

Much of the community faces a significant burden of work when it comes to compliance solutions

73%

59%

respondents
ulatory
llow

Of those, 73% wait to assess compliance after development work has begun

59% assess cod
already ru
pr

from the 2017 Chef S

```
pi.statuses.user_timelin
response.data), 'tweets from
.data) != 0:
esponse.data[0]['created_at']
 datetime.strptime(ltdate,'%a %b %d %
datetime.now()
= (today-ltdate2).days
ong < daywindow:
nt i.screen_name, 'has tweeted in the pa
ltweets += len(response.data)
j in response.data:
f j.entities.urls:
   for k in j.entities.urls:
       newurl = k['expanded_url']
       urlset.add((newurl, j.user

   name, 'has not tw
```

Introducing InSpec

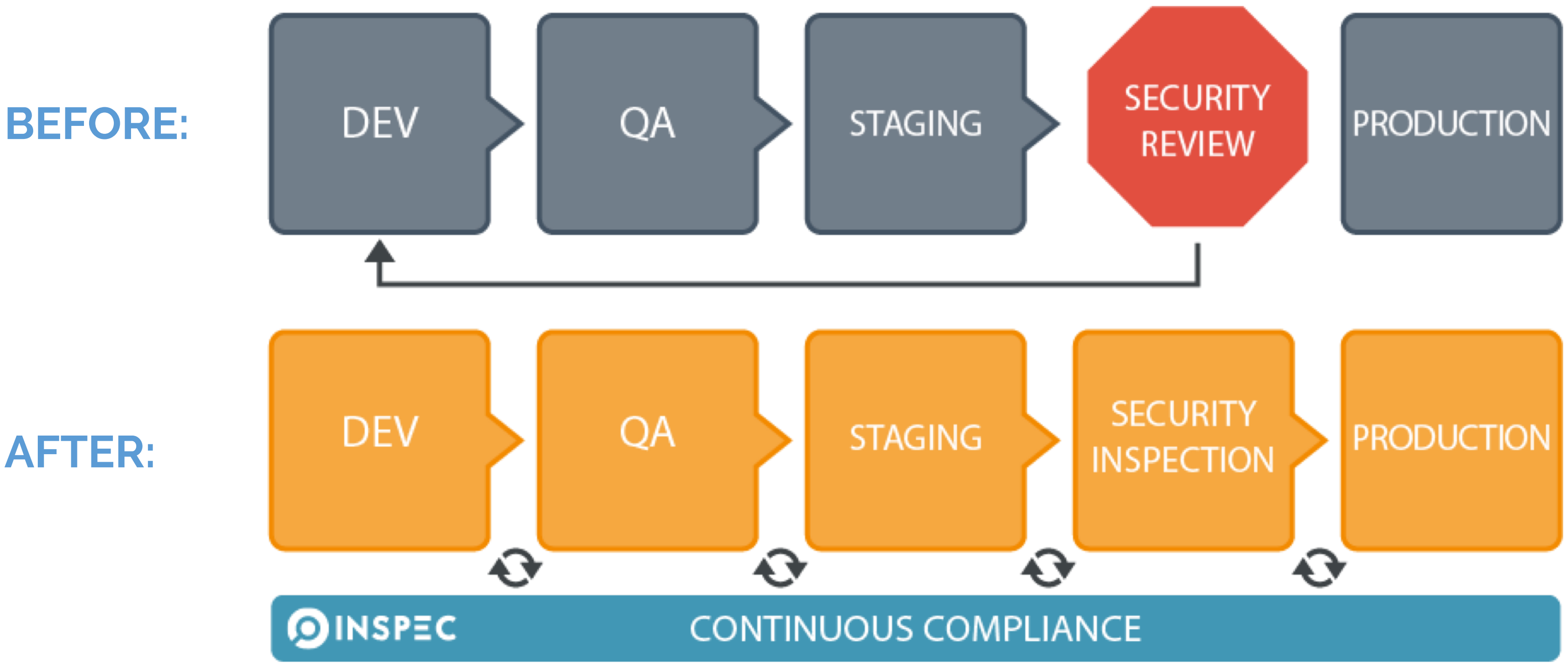
InSpec helps express security & compliance requirements as code and incorporate it directly into the delivery process.

Systems shall have a Mandatory Access Control system installed and enabled.

→

```
control 'ensure_selinux_installed' do
  impact 1.0
  title 'Ensure SELinux is installed'
  desc <<-EOD
   SELinux provides Mandatory Access Control
  EOD
  describe package('libselinux') do
    it { should be_installed }
  end
end
```

Traditional Compliance Versus InSpec



Compliance and policy configuration throughout the SDLC

InSpec 1.0: Servers & Containers

```
control
"cisecurity.benchmarks_rule_5.2.9_Ensure_SSH_PermitEmptyPasswords_is_disabled" do

  title "Ensure SSH PermitEmptyPasswords is disabled"

  desc  "The PermitEmptyPasswords parameter specifies if the SSH server allows login
to accounts with empty password strings. Rationale: Disallowing remote shell access
to accounts that have an empty password reduces the probability of unauthorized
access to the system"

  impact 1.0

  tag "cis-rhel7-2.1.1": "5.2.9"

  tag "level": "1"

  tag "type": ["Server", "Workstation"]

  describe sshd_config do

    its('PermitEmptyPasswords') { should eq 'no' }

  end

end
```

A Quick Primer on InSpec Terminology

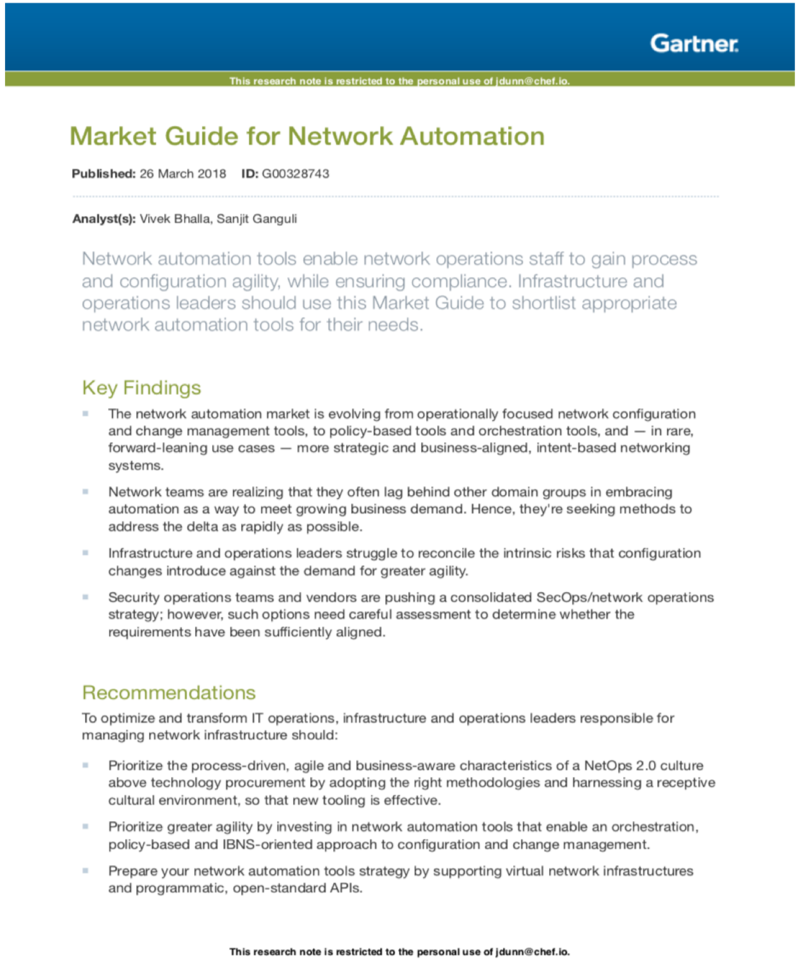
- Resources
- Controls
- Profiles
- Nodes
- Scan Jobs

Network Automation is Necessary for Business Agility

"Network teams are realizing that they often lag behind other domain groups in embracing automation as a way to meet growing business demand. Hence, they're seeking methods to address the delta as rapidly as possible.”

Fewer than 10% of network teams use any automation tools today.

Source: Gartner Market Guide for Network Automation (March 2018)



Gartner

Market Guide for Network Automation

Published: 26 March 2018 **ID:** G00328743

Analyst(s): Vivek Bhalla, Sanjit Ganguli

Network automation tools enable network operations staff to gain process and configuration agility, while ensuring compliance. Infrastructure and operations leaders should use this Market Guide to shortlist appropriate network automation tools for their needs.

Key Findings

- The network automation market is evolving from operationally focused network configuration and change management tools, to policy-based tools and orchestration tools, and — in rare, forward-leaning use cases — more strategic and business-aligned, intent-based networking systems.
- Network teams are realizing that they often lag behind other domain groups in embracing automation as a way to meet growing business demand. Hence, they're seeking methods to address the delta as rapidly as possible.
- Infrastructure and operations leaders struggle to reconcile the intrinsic risks that configuration changes introduce against the demand for greater agility.
- Security operations teams and vendors are pushing a consolidated SecOps/network operations strategy; however, such options need careful assessment to determine whether the requirements have been sufficiently aligned.

Recommendations

To optimize and transform IT operations, infrastructure and operations leaders responsible for managing network infrastructure should:

- Prioritize the process-driven, agile and business-aware characteristics of a NetOps 2.0 culture above technology procurement by adopting the right methodologies and harnessing a receptive cultural environment, so that new tooling is effective.
- Prioritize greater agility by investing in network automation tools that enable an orchestration, policy-based and IBNS-oriented approach to configuration and change management.
- Prepare your network automation tools strategy by supporting virtual network infrastructures and programmatic, open-standard APIs.

InSpec 2.0: Networks and Clouds

Write compliance policies for all aspects of cloud configuration:

- Virtual machines
- Security groups
- Block storage security policies
- Networking
- Identity and access management
- Log management

AWS and Microsoft Azure are supported; Google Cloud Platform support in beta.

Example: Microsoft Azure Server Policy

```
control 'azure-virtual-machine-policy-1.0' do
  impact 1.0
  title 'Ensure that the webserver has been set up as expected'

  describe azure_virtual_machine(group_name: 'Inspec-Azure', name: 'webserver') do
    its('location') { should cmp 'westeurope' }
    its('tags') { should include 'Description' }
    its('disk_size_gb') { should be >= 25 }
    its('vm_size') { should cmp 'Standard_DS2_v2'}
  end
end
```

Example: Avoid AWS S3 Mistakes

```
describe aws_s3_bucket(bucket_name: 'secret_files') do
  it { should exist }
  it { should_not be_public }
  it { should have_access_logging_enabled }
end
```

Example: Microsoft Azure Network Policy

```
control 'azure-generic-virtual-network-2.0' do
  impact 1.0
  title 'Ensure that the virtual network has been created with the correct address space and subnet'
  describe azure_generic_resource(group_name: 'Inspec-Azure’, name: 'Inspec-VNet') do
    its('type') { should cmp 'Microsoft.Network/virtualNetworks' }
    its('location') { should cmp 'westeurope’ }
    its('properties.addressSpace.addressPrefixes') { should include ‘192.168.14.0/24’ }
    its('properties.subnets.count') { should eq 1 }
  end
end
```

Extending InSpec to Traditional Network Devices

- Recently extended InSpec to certain Cisco network devices (IOS 12.x and 15.x) with support for others soon.
- Commercial product (Chef Automate) includes agentless scanner & premium content (e.g. CIS Benchmarks for Cisco IOS)

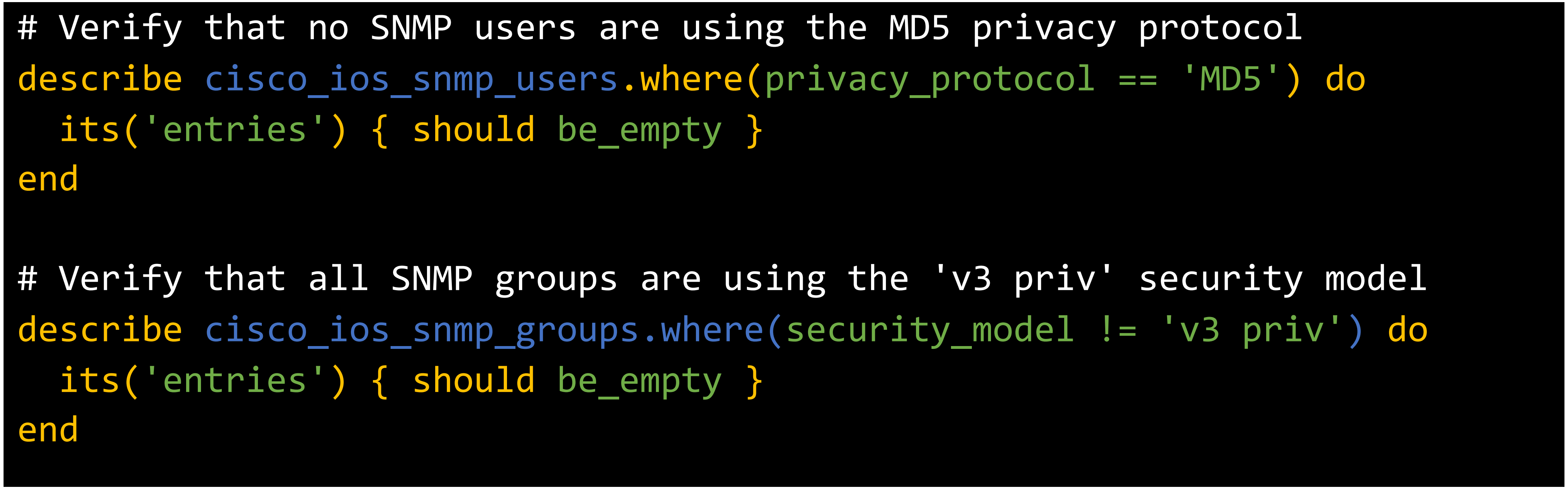
General Use on Cisco IOS

```
# Verify the contents of the running configuration
describe cisco_ios_running_config do
  it { should have_line 'no ip http server' }
end

# Validate the output of arbitrary commands
describe cisco_ios_command('show cdp') do
  its('output') { should match /CDP is not enabled/ }
end
```

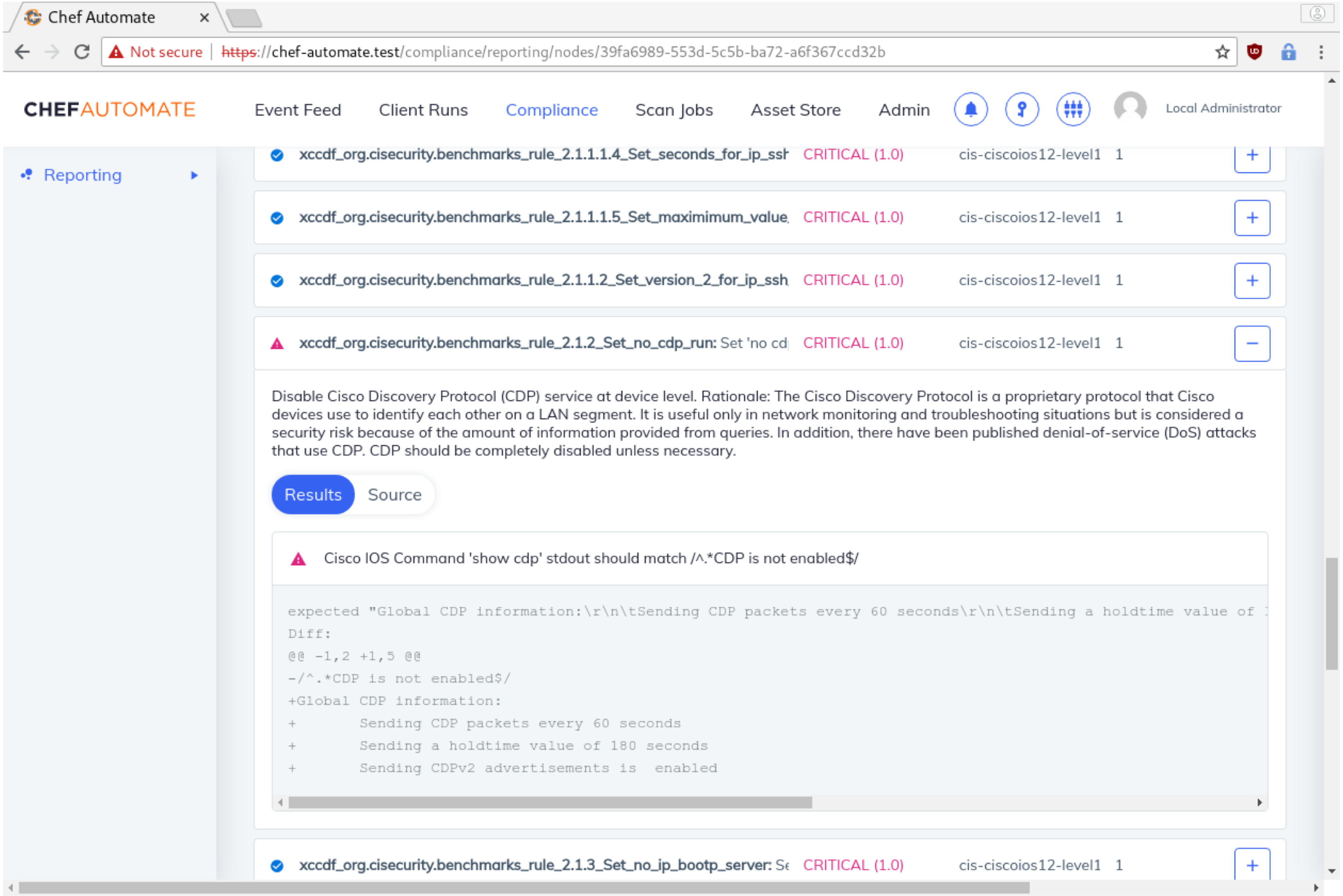
Example: Auditing Interfaces

```
# Verify that at least one Loopback interface exists
describe cisco_ios_interfaces.where(name: /Loopback/) do
  its('entries') { should_not be_empty }
end

# Verify that the FastEthernet0/0 interface has the correct IP
describe cisco_ios_interface('FastEthernet0/0') do
  its('ip_address') { should eq '10.2.3.1' }
end
```

Verify SNMP User and Group Configuration



```
# Verify that no SNMP users are using the MD5 privacy protocol
describe cisco_ios_snmp_users.where(privacy_protocol == 'MD5') do
  its('entries') { should be_empty }
end

# Verify that all SNMP groups are using the 'v3 priv' security model
describe cisco_ios_snmp_groups.where(security_model != 'v3 priv') do
  its('entries') { should be_empty }
end
```



✓	xccdf_org.cisecurity.benchmarks_rule_2.1.1.1.4_Set_seconds_for_ip_ssh	CRITICAL (1.0)	cis-ciscoios12-level1	1
✓	xccdf_org.cisecurity.benchmarks_rule_2.1.1.1.5_Set_maximimum_value,	CRITICAL (1.0)	cis-ciscoios12-level1	1
✓	xccdf_org.cisecurity.benchmarks_rule_2.1.1.2_Set_version_2_for_ip_ssh	CRITICAL (1.0)	cis-ciscoios12-level1	1
▲	xccdf_org.cisecurity.benchmarks_rule_2.1.2_Set_no_cdp_run: Set 'no cd	CRITICAL (1.0)	cis-ciscoios12-level1	1

Disable Cisco Discovery Protocol (CDP) service at device level. Rationale: The Cisco Discovery Protocol is a proprietary protocol that Cisco devices use to identify each other on a LAN segment. It is useful only in network monitoring and troubleshooting situations but is considered a security risk because of the amount of information provided from queries. In addition, there have been published denial-of-service (DoS) attacks that use CDP. CDP should be completely disabled unless necessary.

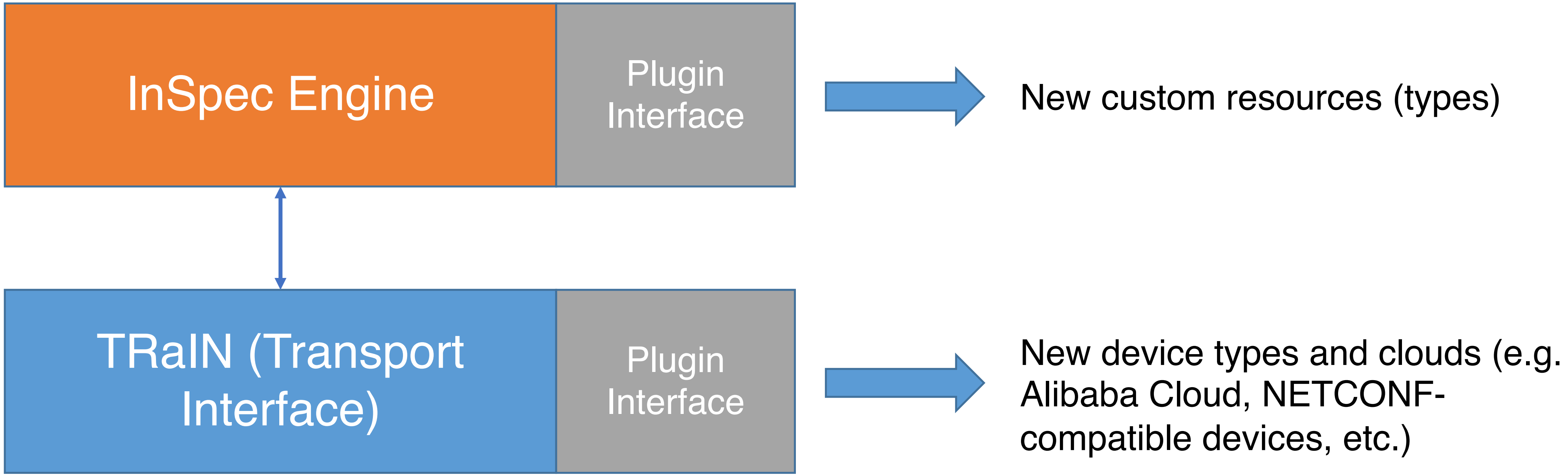
▲ Cisco IOS Command 'show cdp' stdout should match /^.*CDP is not enabled$/

```
expected "Global CDP information:\r\n\tSending CDP packets every 60 seconds\r\n\tSending a holdtime value of 
Diff:
@@ -1,2 +1,5 @@
-/^.*CDP is not enabled$/
+Global CDP information:
+       Sending CDP packets every 60 seconds
+       Sending a holdtime value of 180 seconds
+       Sending CDPv2 advertisements is  enabled
```

✓	xccdf_org.cisecurity.benchmarks_rule_2.1.3_Set_no_ip_bootp_server: Se	CRITICAL (1.0)	cis-ciscoios12-level1	1

Demo

Coming Soon: InSpec 3.0



InSpec Engine

Plugin Interface

New custom resources (types)

TRaIN (Transport Interface)

Plugin Interface

New device types and clouds (e.g. Alibaba Cloud, NETCONF-compatible devices, etc.)

Summary

- InSpec is an open-source language for compliance-as-code
- Compliance-as-code approaches can be used for security/audit verification as well as validation of configuration correctness
- InSpec >=2.0 can validate configurations of servers, clouds, network devices
- Get started today at **www.inspec.io**

ons

EUROPE

OPEN NETWORKING //
Integrate, Automate, Accelerate

September 25 - 27, 2018
Amsterdam, The Netherlands

Thank You

jdunn@chef.io | *@julian_dunn*
https://www.inspec.io/