

CHEF™

Enough "Security Scanning" Already!

New Approaches To Compliance In An Era Of Constant Change

CHEF™



Julian Dunn
Product Manager
jdunn@chef.io

CHEF

PERSONAL TECH

How Many Times Has Your Personal Information Been Exposed to Hackers?

By JOSH KELLER, K.K. REBECCA LAI and NICOLE PERLROTH JULY 29, 2015

Half of American adults had their personal information exposed to hackers last year alone. In a recent attack at the federal Office of Personnel Management, hackers stole the most sensitive personal data for 21.5 million people.

Answer the questions below to learn which parts of your identity may have been stolen in some of the major hacking attacks over the last two years and what you can do about it. Not all attacks are included here, and many attacks go undetected, so think of your results as a minimum level of exposure.

How many times your information has been exposed to hackers

Have you applied for a job with or worked for the federal government since 2000?

CHEF

verizon

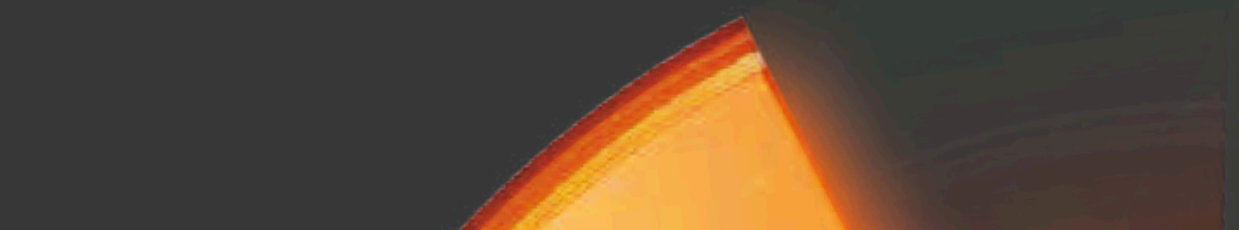
67%

In 2014, two-thirds of organizations did not adequately test the security of all in-scope systems.

Verizon 2015

PCI COMPLIANCE REPORT

Insight for helping businesses manage risk through payment security.



70%

CHEF



Key Findings

- 10,000 companies surveyed
- 4 in 5 fail at interim assessment

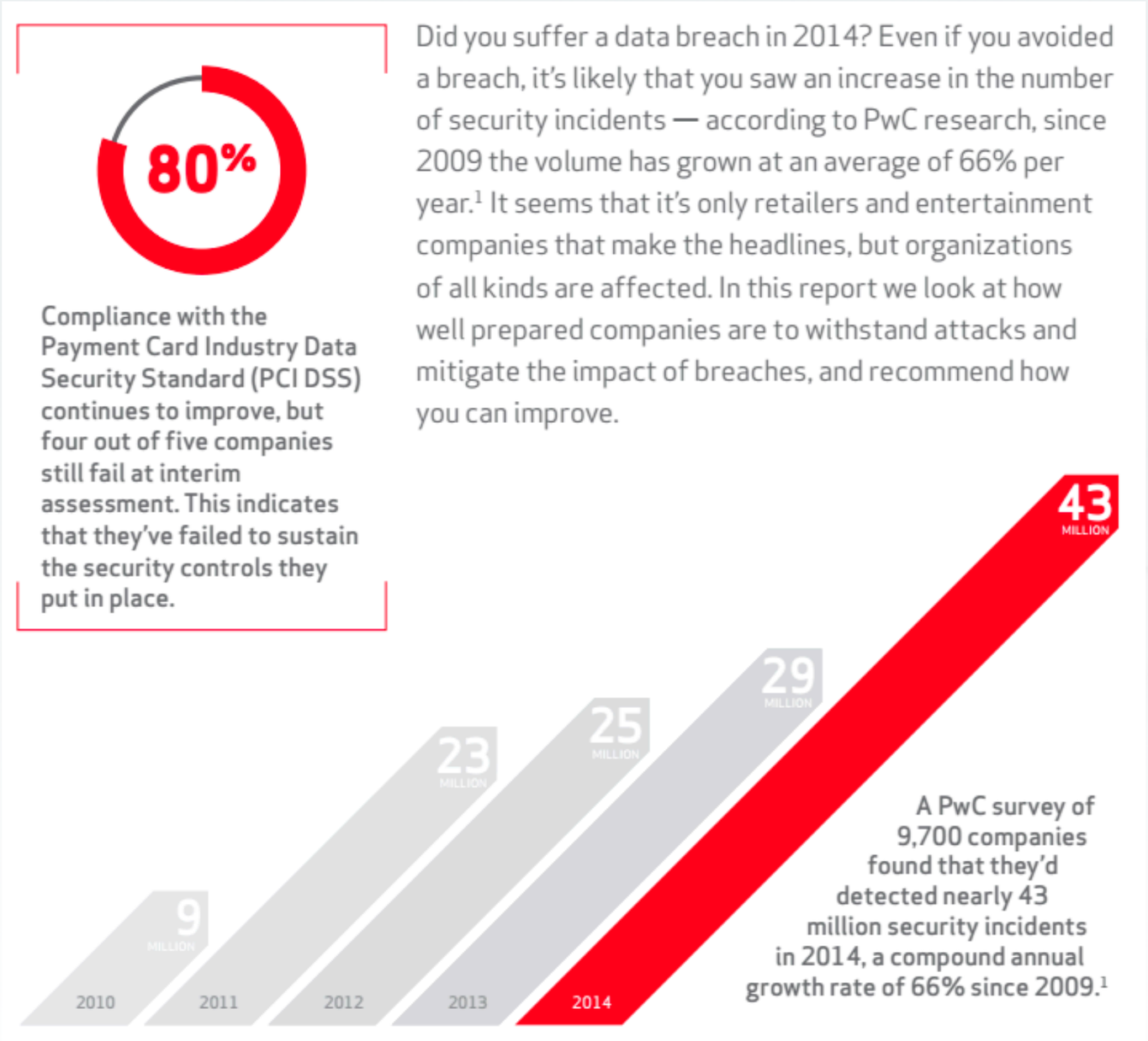
Non-compliant breached companies:

- 45% due to patch management and dev security
- 72% due to log management and configuration
- 73% due to firewall configuration

CHEF

Key Trends

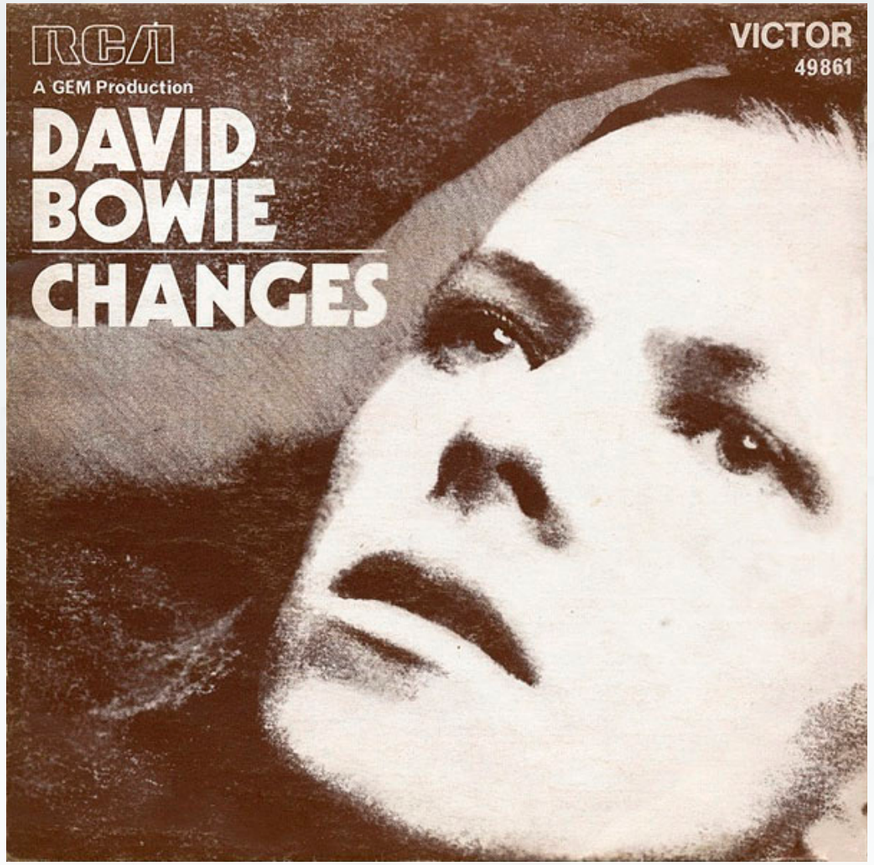
- While individual rule compliance is up, **testing of security systems is down**
- **Sustainability is low.** Fewer than a third of companies were found to be still fully compliant less than a year after successful validation.



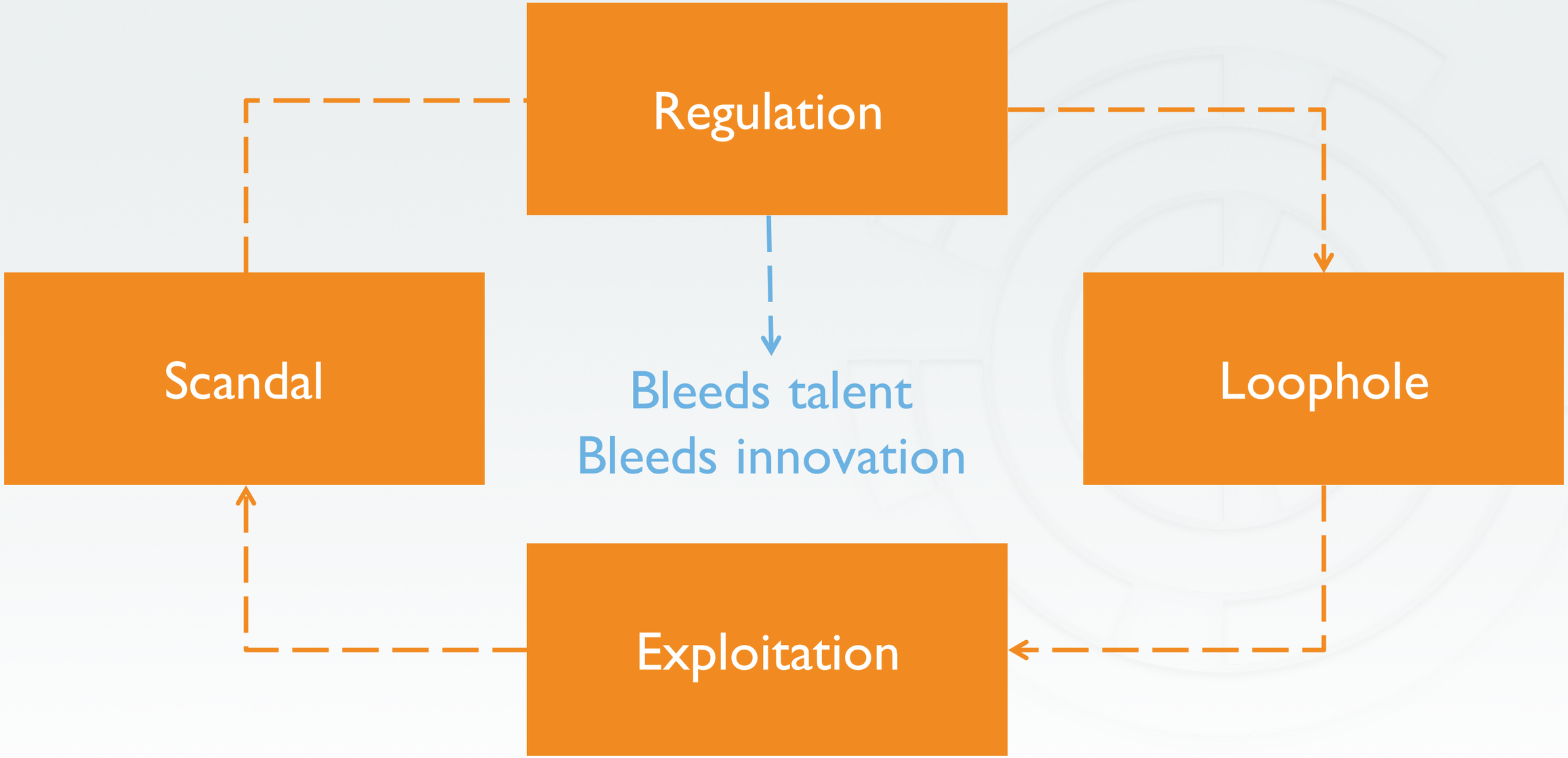
CHEF

Ecosystem Drivers

- Inability to keep up with a moving target
  - Compliance requirements change by an average of 18% over a year
  - Line-of-business initiated changes
- Inability to continuously monitor environments for changes



CHEF

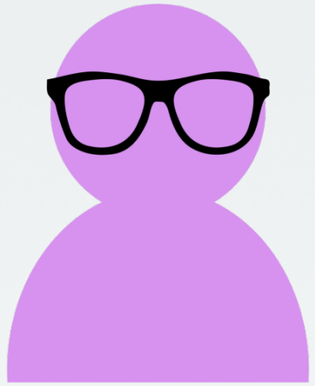

Regulation
Scandal
Bleeds talent
Bleeds innovation
Loophole
Exploitation

CHEF



CHEF

The Compliance Tower of Babel



Compliance



Security



DevOps







CHEF



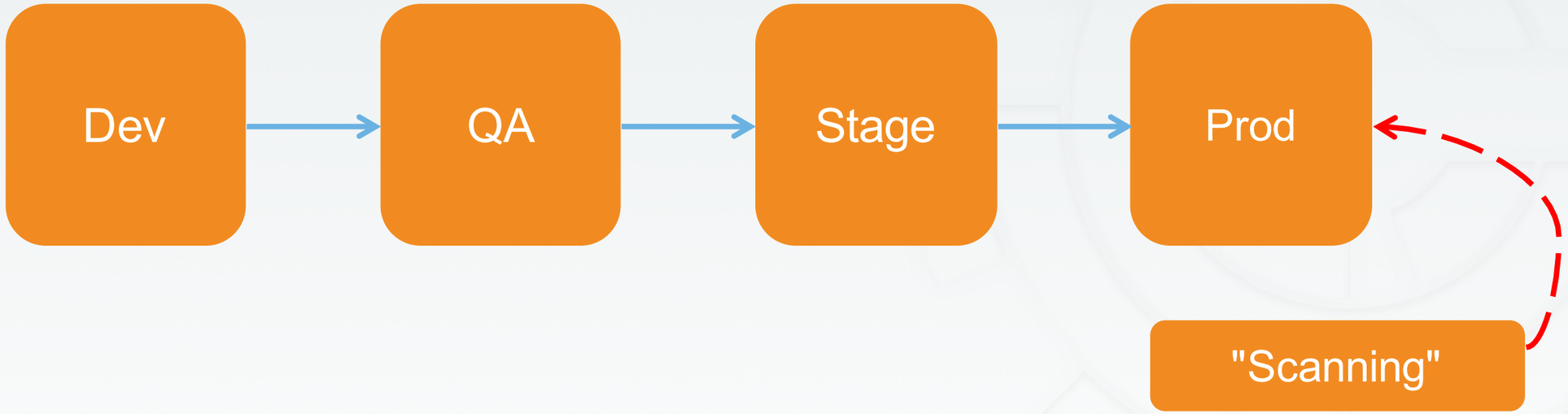


CHEF





CHEF



CHEF

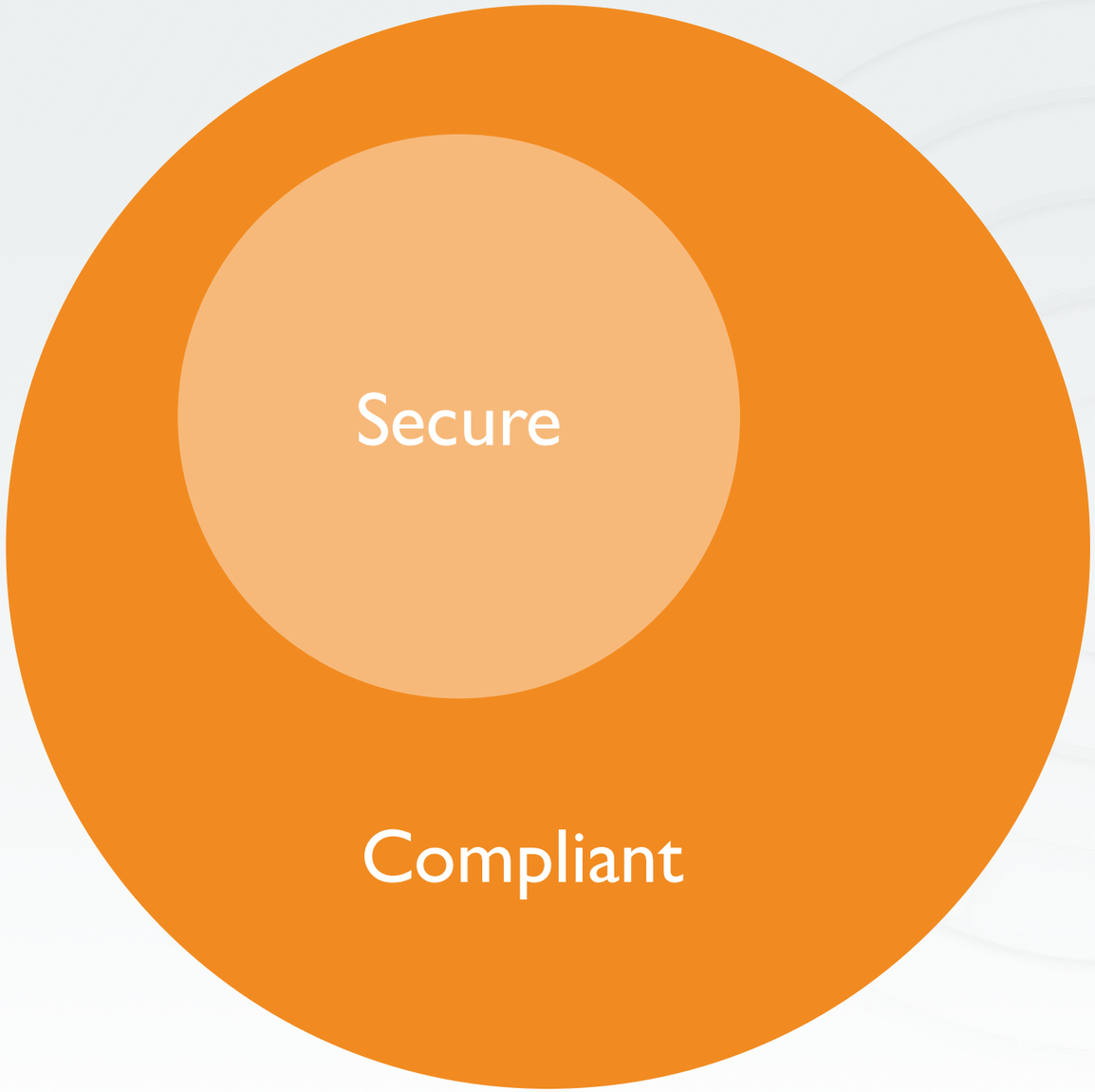


CHEF

Security != Compliance



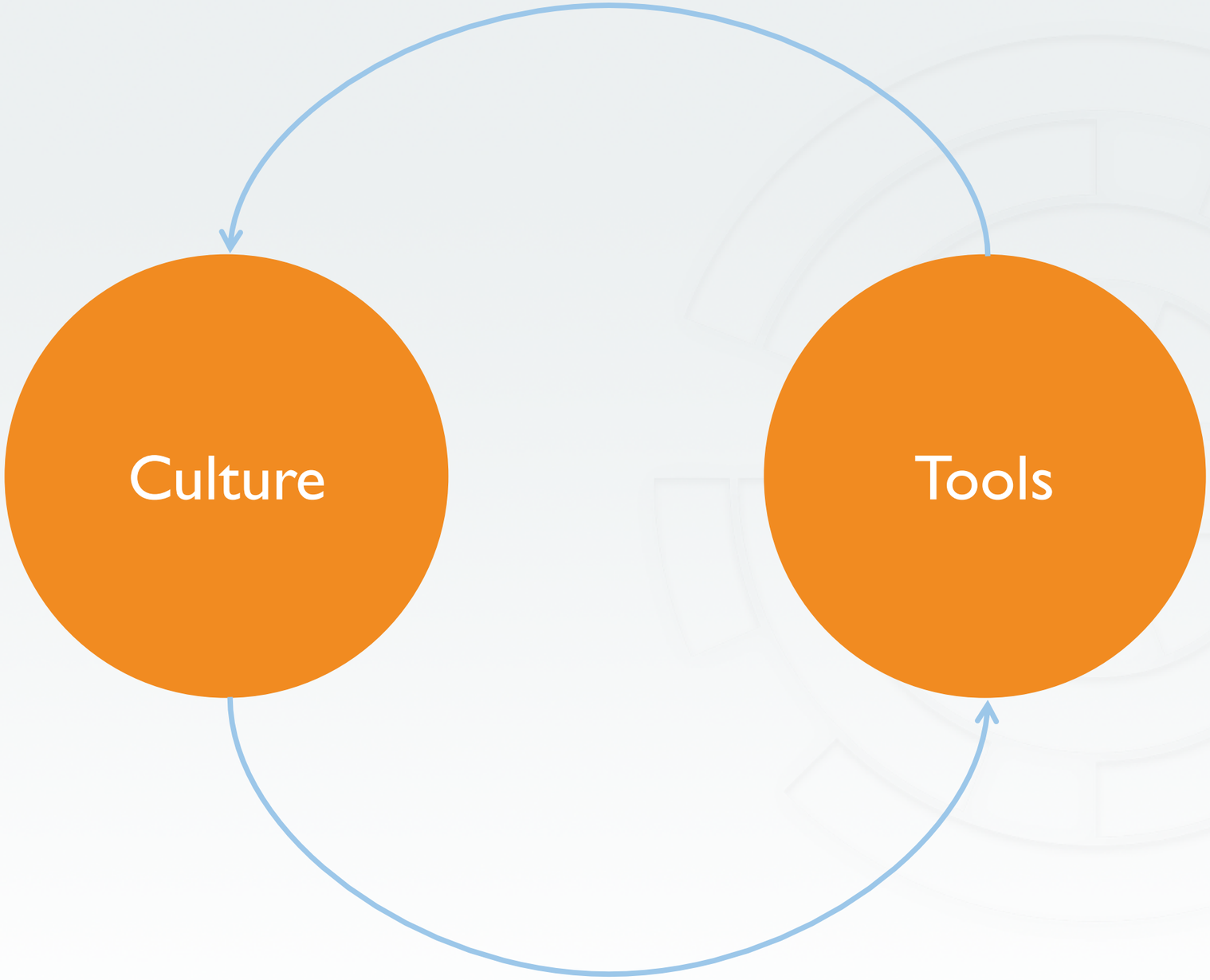
CHEF



CHEF



CHEF



CHEF

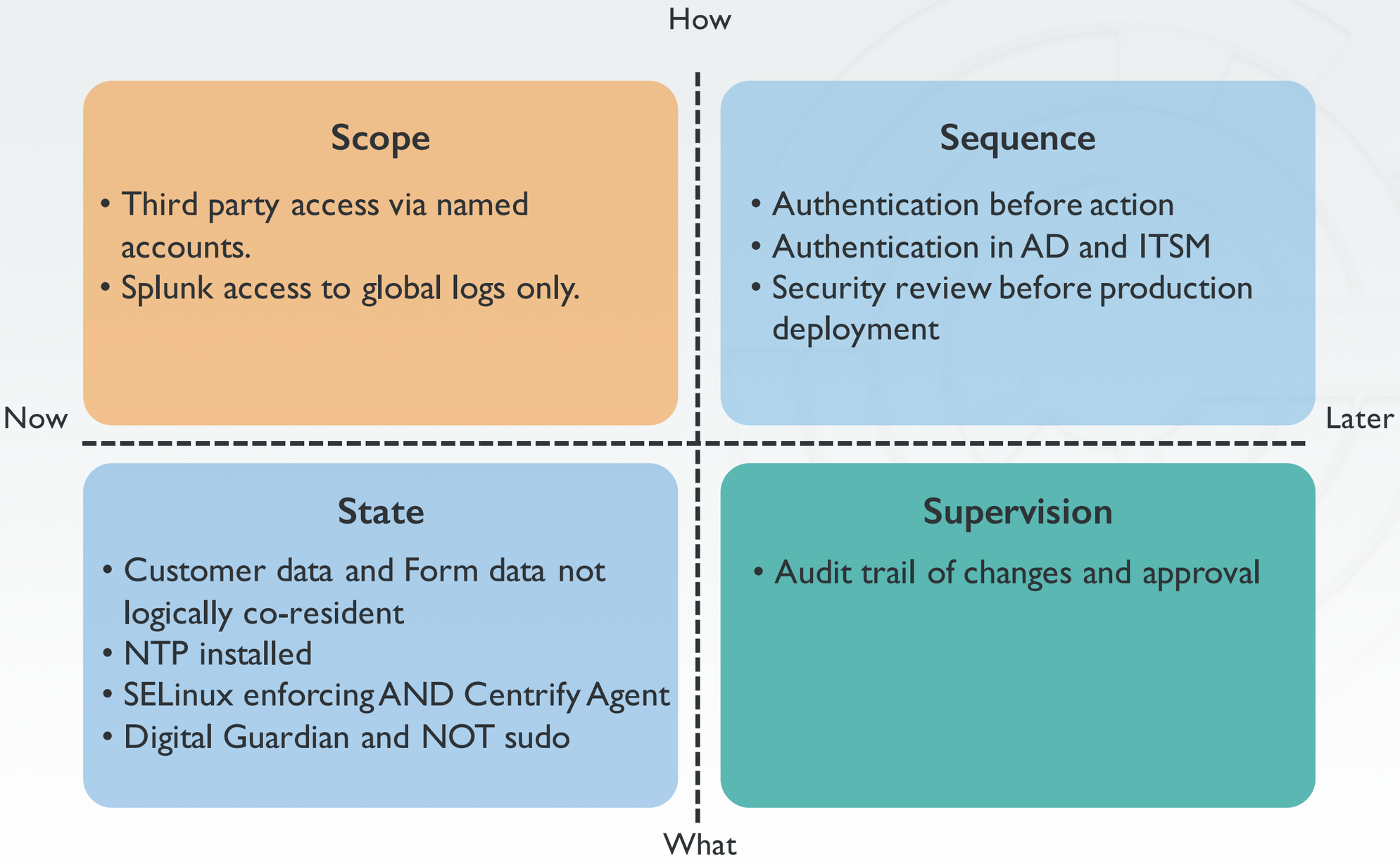
Regulatory Compliance Frameworks

OFAC	USA PATRIOT Act	Gramm-Leach-Bliley Act	Red Flags Rule
Bank Secrecy Act	Sarbanes-Oxley	Regulation E	Dodd-Frank
False Claims Act	HIPAA	European Central Bank Regulations	Prudential Regulation Authority
Financial Conduct Authority	HITECH	PCI DSS	

What are the commonalities?

CHEF

Compliance Rule Types



CHEF

Introducing InSpec

- Flexible, cross-platform, domain-specific-language for compliance
- Run locally or remotely
- Easily usable by operations, infosec, and compliance officers
- Fully **open source and available today**

https://www.chef.io/inspec/

CHEF

A Simple Example

```
control 'cis-secureboot-3.1' do
  impact 0.7
  title '3.1 Set User/Group owner on bootloader config'
  describe file('/boot/grub/grub.cfg') do
    it { should be_owned_by('root') }
    it { be_grouped_into('root') }
  end
end
```

- Set impact per-control
- Set descriptive metadata for use in reports
- Easy-to-use helpers for non-sysadmins
- Easy to extend by developers

CHEF

Example – PCI Compliance

- PCI 2.3 - Encrypt all non-console administrative access such as browser/Web-based management tools.

Control

```
controls 'port compliance' do
  control port(23) do
    it "has nothing listening"
      expect(port(23)).to_not
be_listening
    end
  end
end
```

Rule

```
rules 'PCI 2.3 – Confirm telnet port not available'
  rule on run_control
  when
    name = 'should be listening'
    resource_type = 'port'
    resource_name = '23'
    status != 'success'
  then
    audit:error("PCI 2.3 - Encrypt all non-console
administrative access such as browser/Web-based
management tools.")
    notify("security-team@financialcorp.com", "A
machine is listening for connections on port
23/telnet!")
  end
end
```

CHEF

Example - SOX Compliance

- SOX Section 302.4.B – Establish verifiable controls to track data access.

Control

```
controls 'password authentication' do
  control file('/etc/ssh/sshd_config') do
    it "is disabled"
      expect(file('/etc/ssh/sshd_config'))
    .to_not
     match(/^\s*PasswordAuthentication\s+yes/i)
    end
  end
end
```

Rule

```
rules 'force key based auth'
  rule on run_control
  when
    name = ‘should be “yes”'
    resource_type = ‘sshd_config.param'
    resource_name = 'PasswordAuthentication'
    status = 'failed'
  then
    audit:error("SOX Section 302.4.B – Establish
verifiable controls to track data access.")
    notify(‘security-team@financialcorp.com’, "A machine
has password login enabled!")
  end
end
```

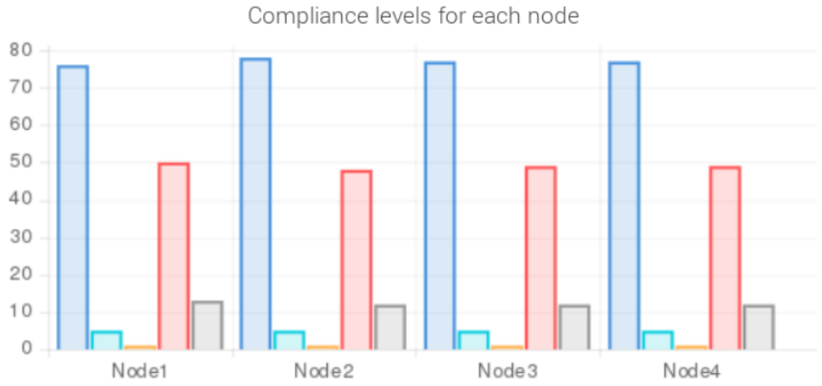
CHEF

CHEF COMPLIANCE

- Dashboard
- Reports
- Jobs
- Patch Logs
- Compliance
- Patch Profiles
- Settings

admin

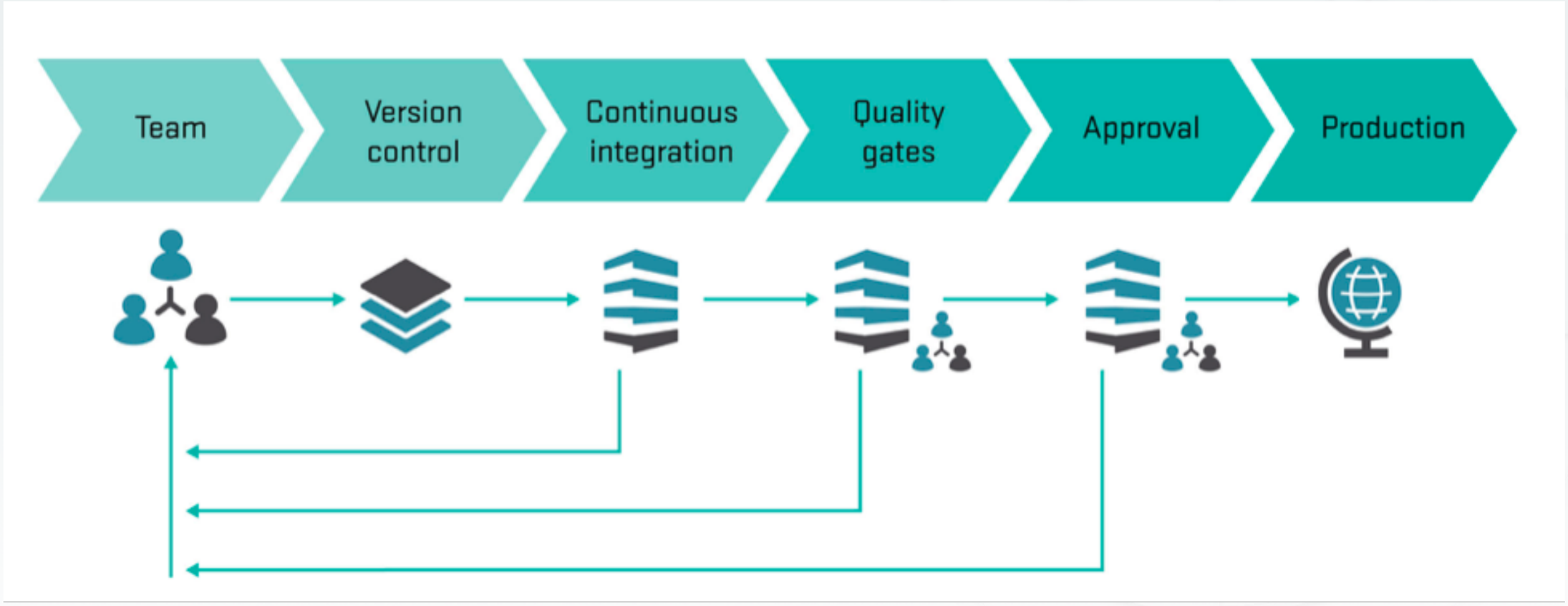
Nodes Report



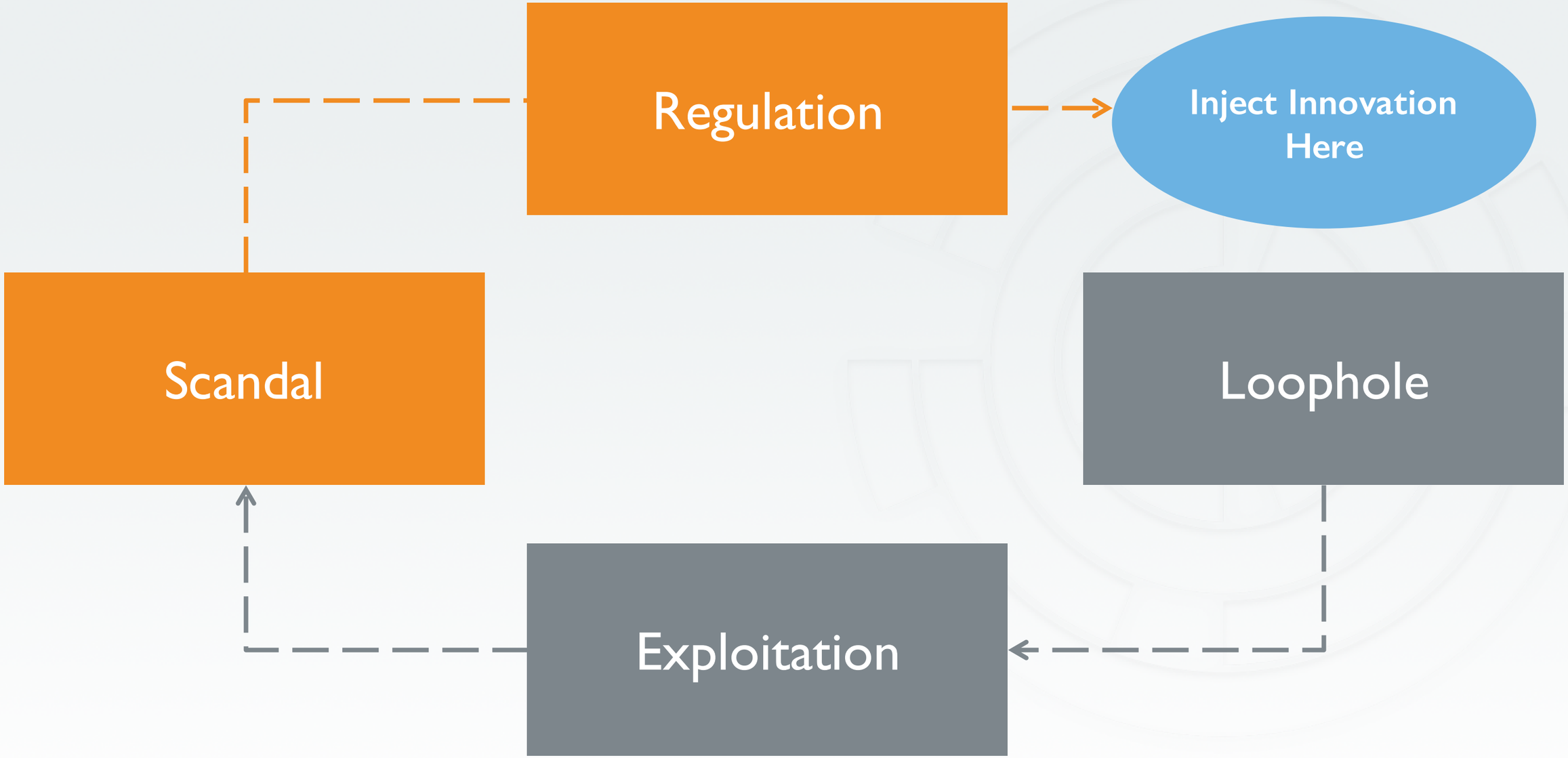
The table below summarize the scan results for each node.
By selecting each node, you get a list of all rules and their status during this compliance scan.

Hostname	Compliant	Minor Issues	Major Issues	Critical Issues	Skipped
Node1	76	5	1	50	13
cis/cis-ubuntu-level1: 9.1.1 Enable cron Daemon			Critical Issues		
cis/cis-ubuntu-level1: 9.1.2 Set User/Group Owner and Permission on /etc/crontab			Critical Issues		
cis/cis-ubuntu-level1: 9.1.3 Set User/Group Owner and Permission on /etc/cron.hourly			Critical Issues		
cis/cis-ubuntu-level1: 9.1.4 Set User/Group Owner and Permission on /etc/cron.daily			Critical Issues		
cis/cis-ubuntu-level1: 9.1.5 Set User/Group Owner and Permission on /etc/cron.weekly			Critical Issues		
cis/cis-ubuntu-level1: 9.1.6 Set User/Group Owner and Permission on /etc/cron.monthly			Critical Issues		
cis/cis-ubuntu-level1: 9.1.7 Set User/Group Owner and Permission on /etc/cron.d			Critical Issues		
cis/cis-ubuntu-level1: 9.1.8 Restrict at/cron to Authorized Users			Critical Issues		
cis/cis-ubuntu-level1: 9.3.12 Set Idle Timeout Interval for User Login			Critical Issues		
cis/cis-ubuntu-level1: 9.3.13 Limit Access via SSH			Critical Issues		
cis/cis-ubuntu-level1: 9.3.3 Set Permissions on /etc/ssh/sshd_config			Critical Issues		
cis/cis-ubuntu-level1: 9.3.6 Set SSH IgnoreRhosts to Yes			Critical Issues		

CHEF

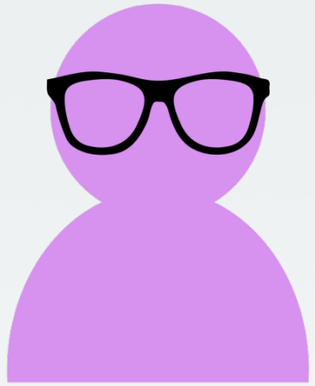

Team
Version control
Continuous integration
Quality gates
Approval
Production

CHEF


Regulation
Inject Innovation Here
Loophole
Exploitation
Scandal

CHEF

The Compliance Tower of Babel



Compliance



Security



DevOps

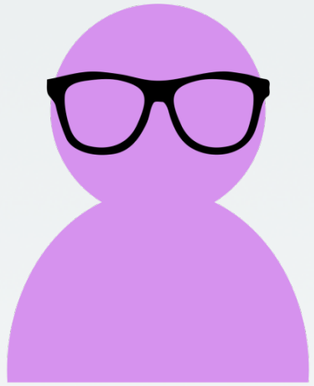






CHEF

InSpec: A Common Denominator



Compliance



Security



DevOps

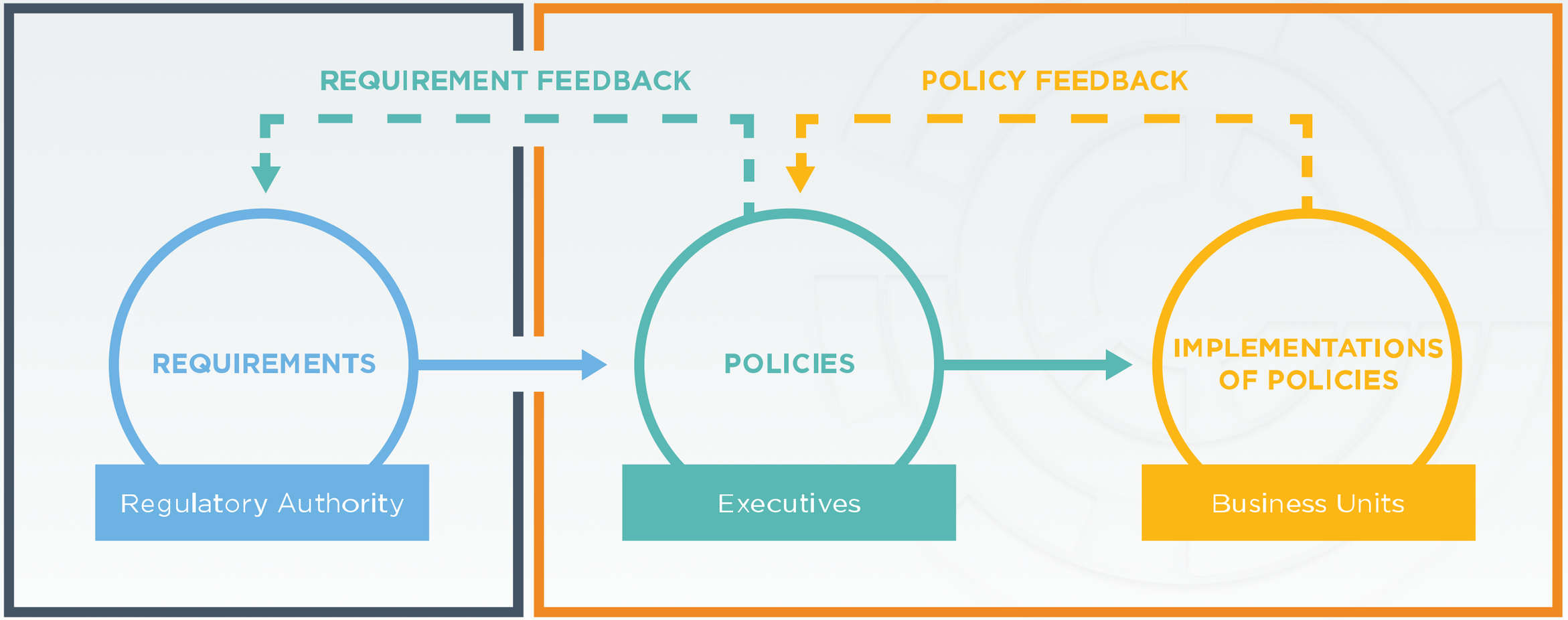






CHEF

Fixing The Compliance Cycle



CHEF



InfoSec Taylor
@SwiftOnSecurity

Following

We can head into this audit together,
You don't have to live in fear,
Because for the first time in forever,
We are in full compliance here.

RETWEETS	FAVORITES
82	136



2:45 PM - 14 Jun 2015

CHEF



CHEF™