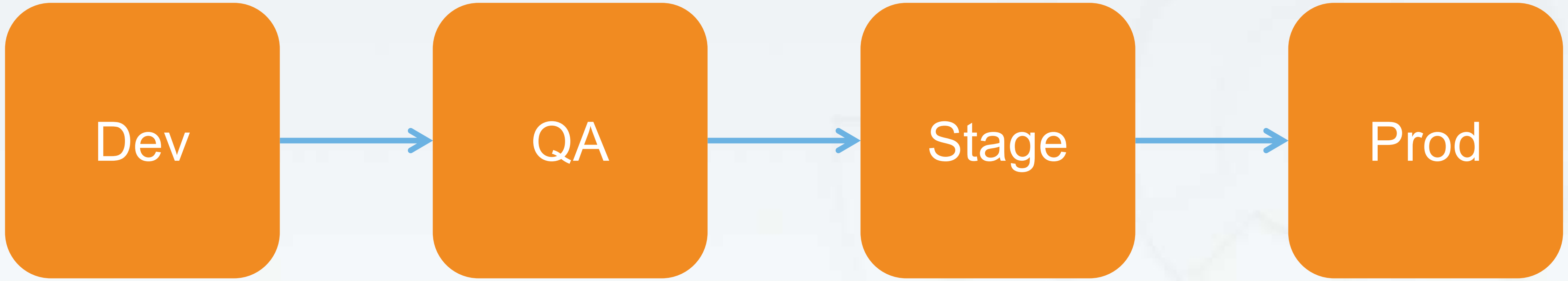
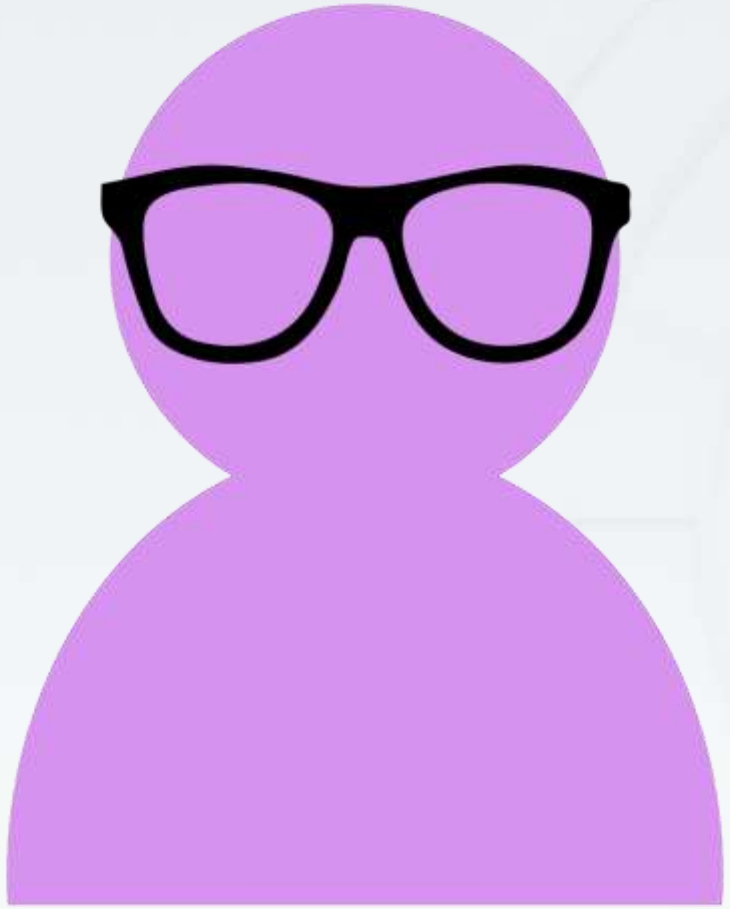
CHEF™

Getting Started with Compliance Automation

CHEF


Dev
QA
Stage
Prod



Compliance

SSH Control

SSH supports two different protocol versions. The original version, SSHv1, was subject to a number of security issues. Please use SSHv2 instead to avoid these.

How will I verify this?

Whip up a one-liner!

```
grep "^Protocol" /etc/ssh/sshd_config | sed 's/Protocol //'
```

Apache Server Information Leakage – Server Token Directive

- Description

  This Directive Controls weather Server response field is sent back to clients includes a description of Generic OS Type of the Server.

  This allows attackers to identify web servers details greatly and increases the efficiency of any attack,as security vulnerabilities are dependent upon specific software versions.

- How to Test

  In order to test for ServerToken configuration, one should check the Apache configuration file.

- Misconfiguration

  ```
  ServerTokens Full
  ```

- Remediation

  Configure the ServerTokens directive in the Apache configuration to value of Prod or ProductOnly. This tells Apache to only return "Apache" in the Server header, returned on every page request.

  ```
  ServerTokens Prod
  ```

  or

  ```
  ServerTokens ProductOnly
  ```

https://www.owasp.org/index.php/SCG_WS_Apache

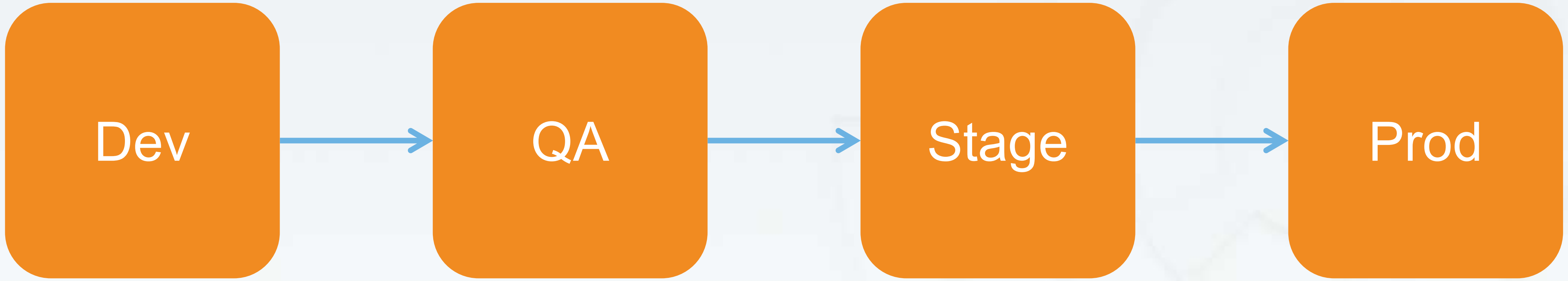
Whip up a one-liner!

```
grep "^ServerTokens" /etc/httpd/conf/httpd.conf | sed 's/ServerTokens //'
```

Security

Whip up a two-liner!

```
TARGET=2
grep "^Protocol" /etc/ssh/sshd_config | sed 's/Protocol //'
> /dev/null && echo $TARGET
```

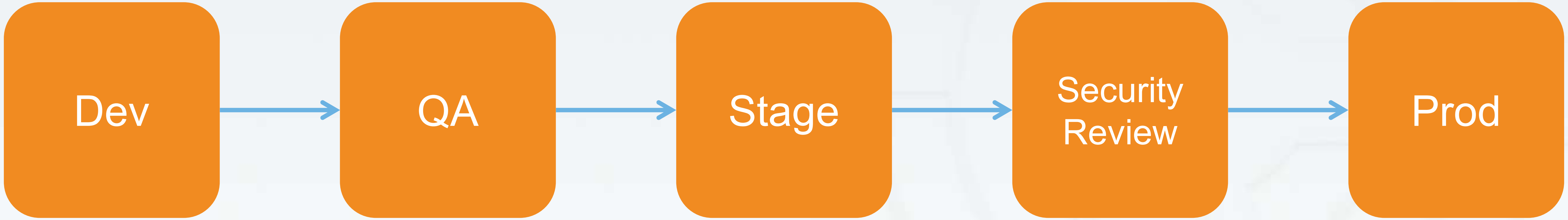


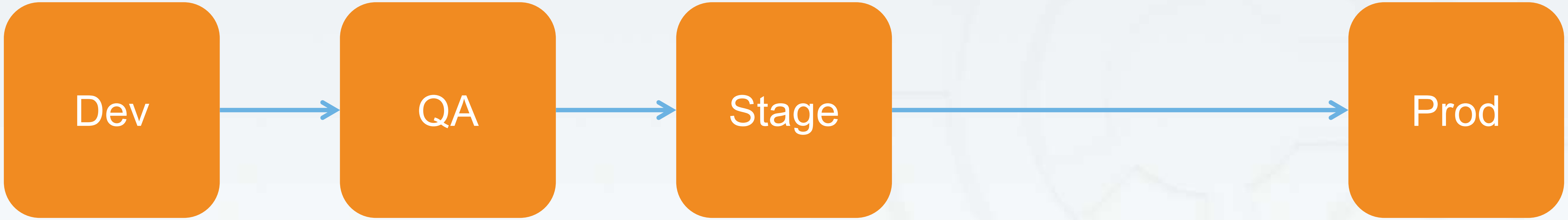
Dev

QA

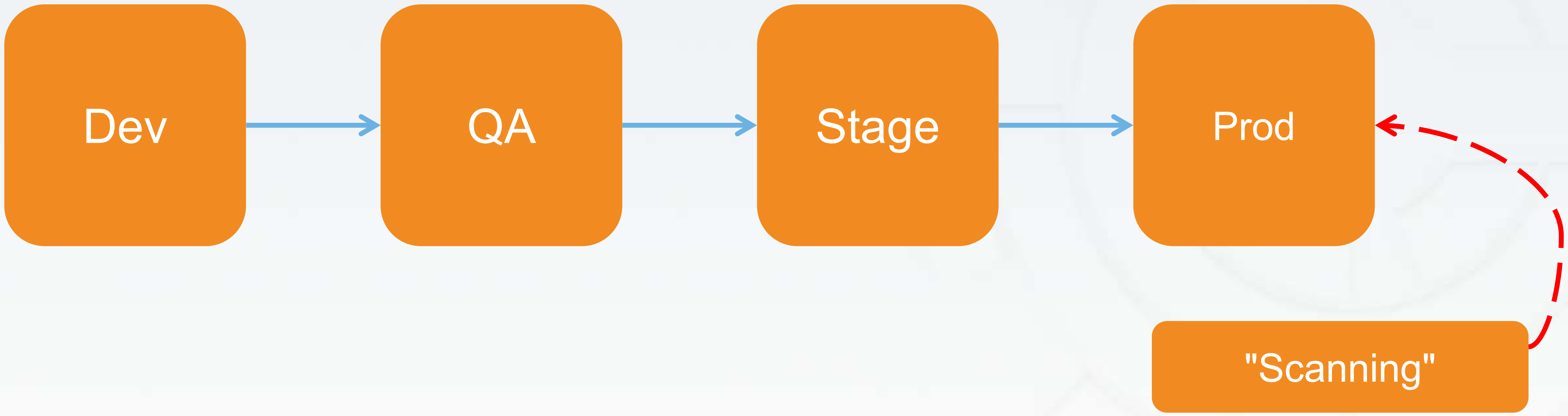
Stage

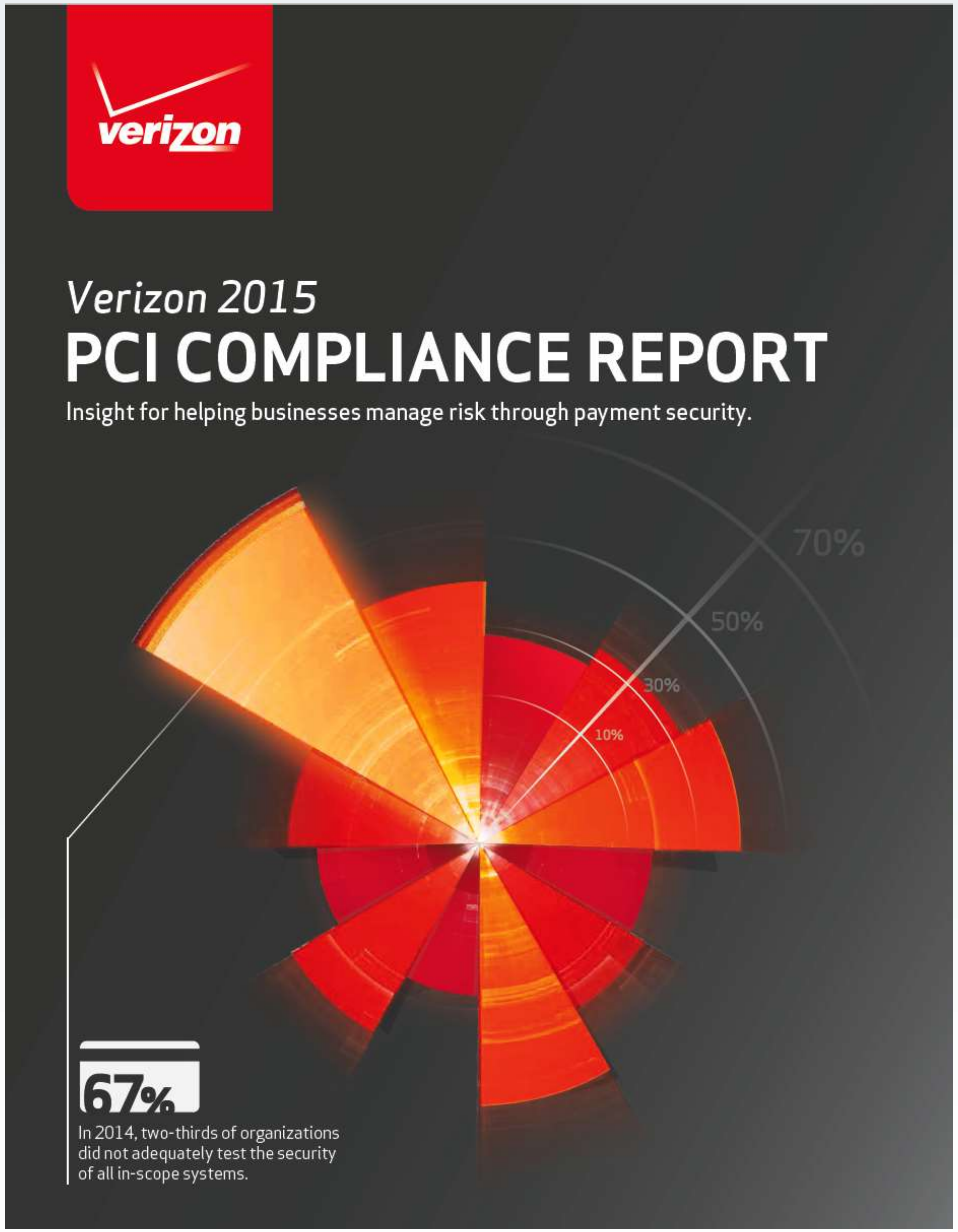
Prod


Dev
QA
Stage
Security Review
Prod



Dev → QA → Stage → Prod


Dev
QA
Stage
Prod
"Scanning"



verizon

Verizon 2015

PCI COMPLIANCE REPORT

Insight for helping businesses manage risk through payment security.

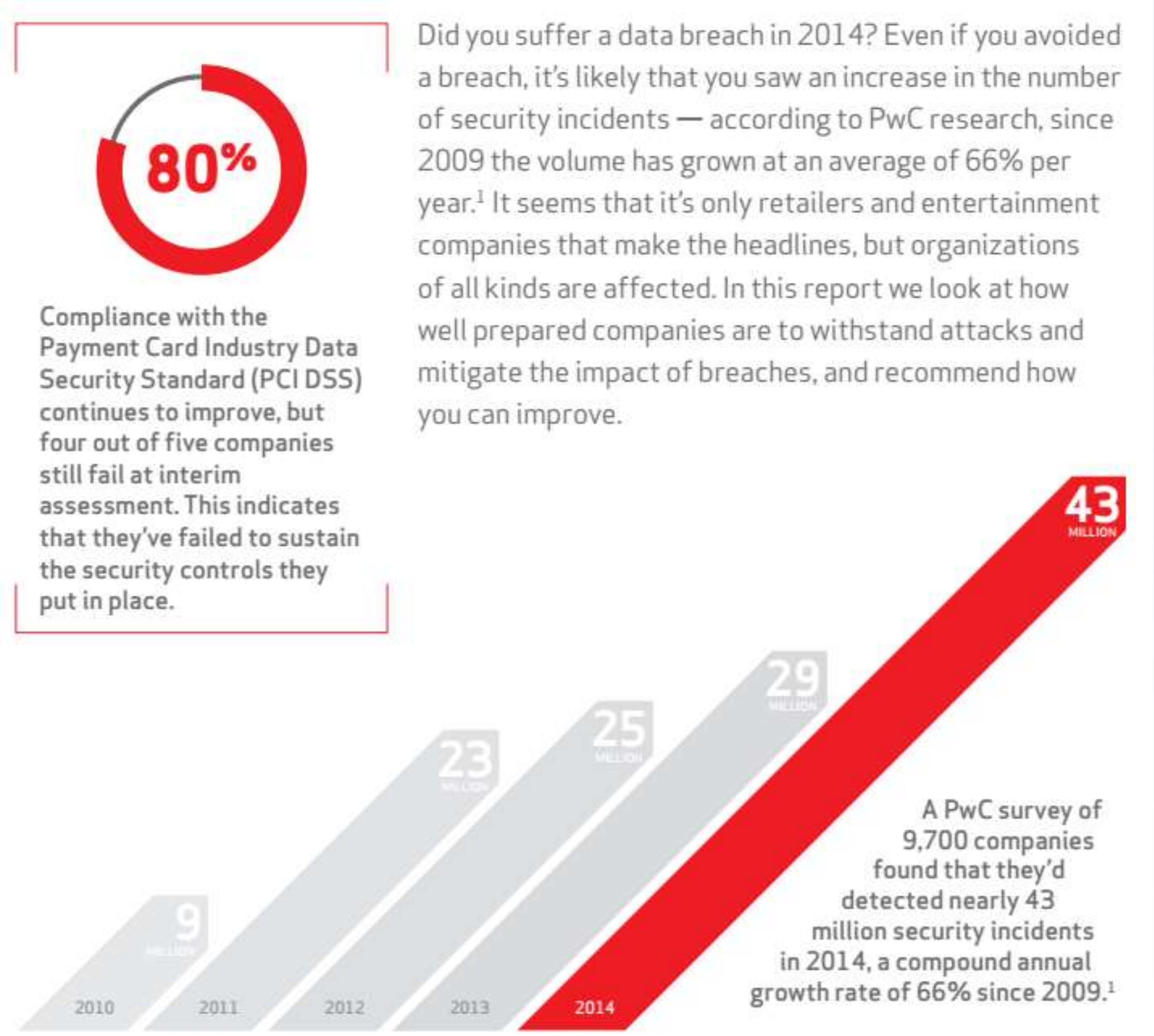
67%

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

Two-thirds of organizations did not adequately test the security of all in-scope systems

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.



Compliance with the Payment Card Industry Data Security Standard (PCI DSS) continues to improve, but four out of five companies still fail at interim assessment. This indicates that they've failed to sustain the security controls they put in place.

Did you suffer a data breach in 2014? Even if you avoided a breach, it's likely that you saw an increase in the number of security incidents — according to PwC research, since 2009 the volume has grown at an average of 66% per year.[1] It seems that it's only retailers and entertainment companies that make the headlines, but organizations of all kinds are affected. In this report we look at how well prepared companies are to withstand attacks and mitigate the impact of breaches, and recommend how you can improve.

A PwC survey of 9,700 companies found that they'd detected nearly 43 million security incidents in 2014, a compound annual growth rate of 66% since 2009.[1]

Compliance

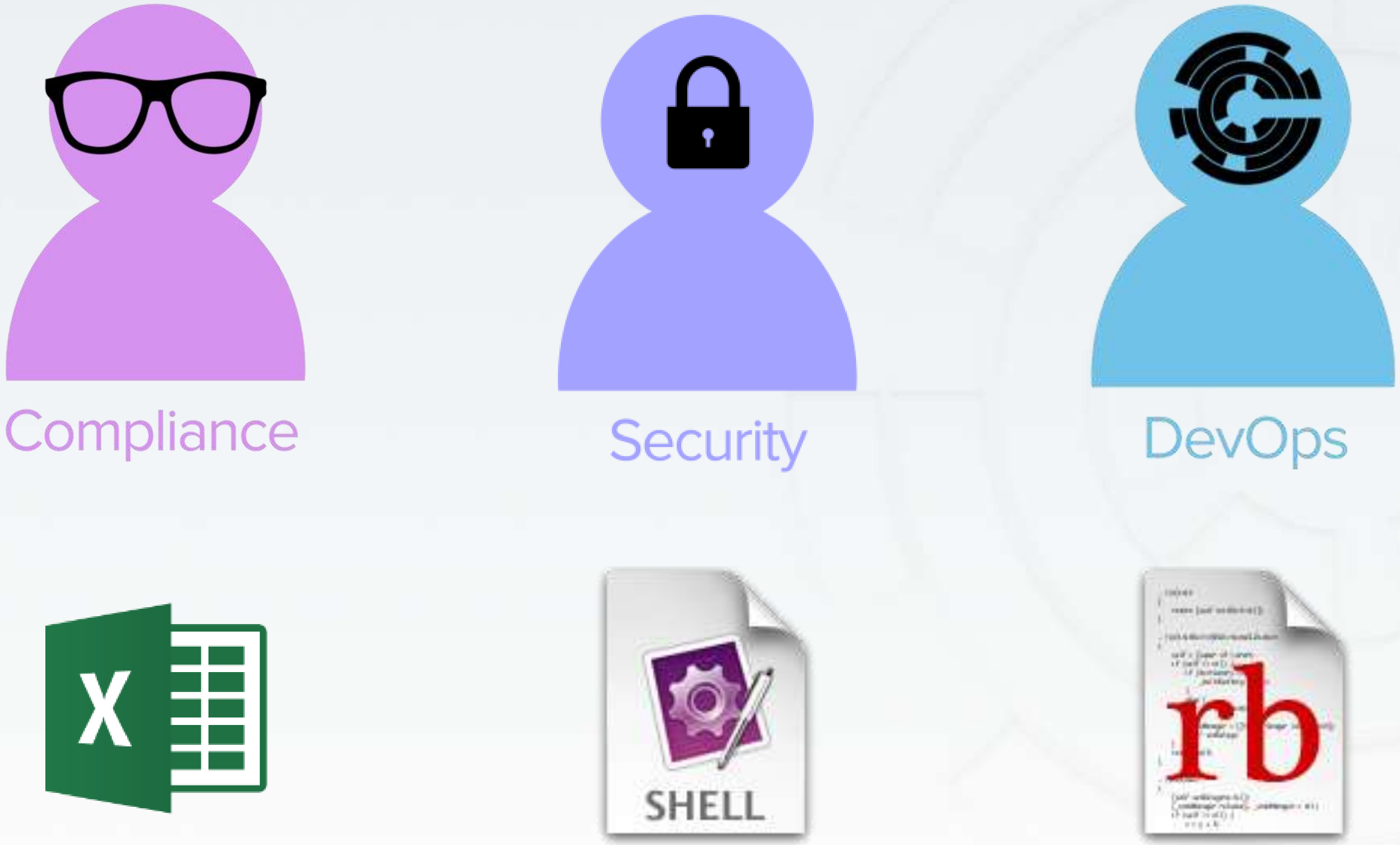
Shell Scripts

```
grep "^Protocol" /etc/ssh/sshd_config | sed 's/Protocol //'
grep "^ServerTokens" /etc/httpd/conf/httpd.conf | sed 's/ServerTokens //'
```

Infrastructure Code

```
package 'httpd' do
  action :install
end

service 'httpd' do
  action [ :start, :enable ]
end
```

What We Have Here Is A Communications Problem



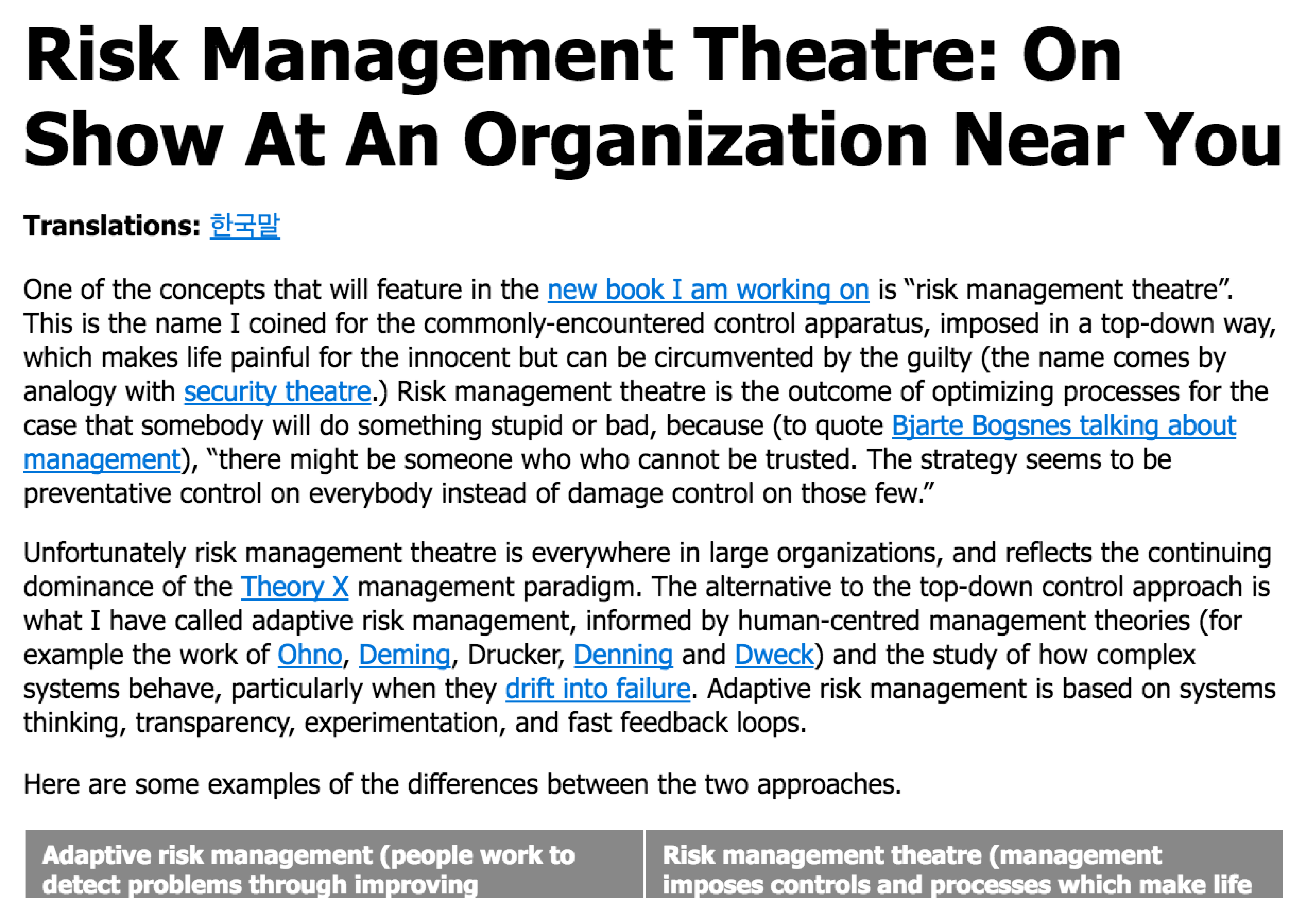
Compliance

Security

DevOps

STOP

Security != Compliance



Risk Management Theatre: On Show At An Organization Near You

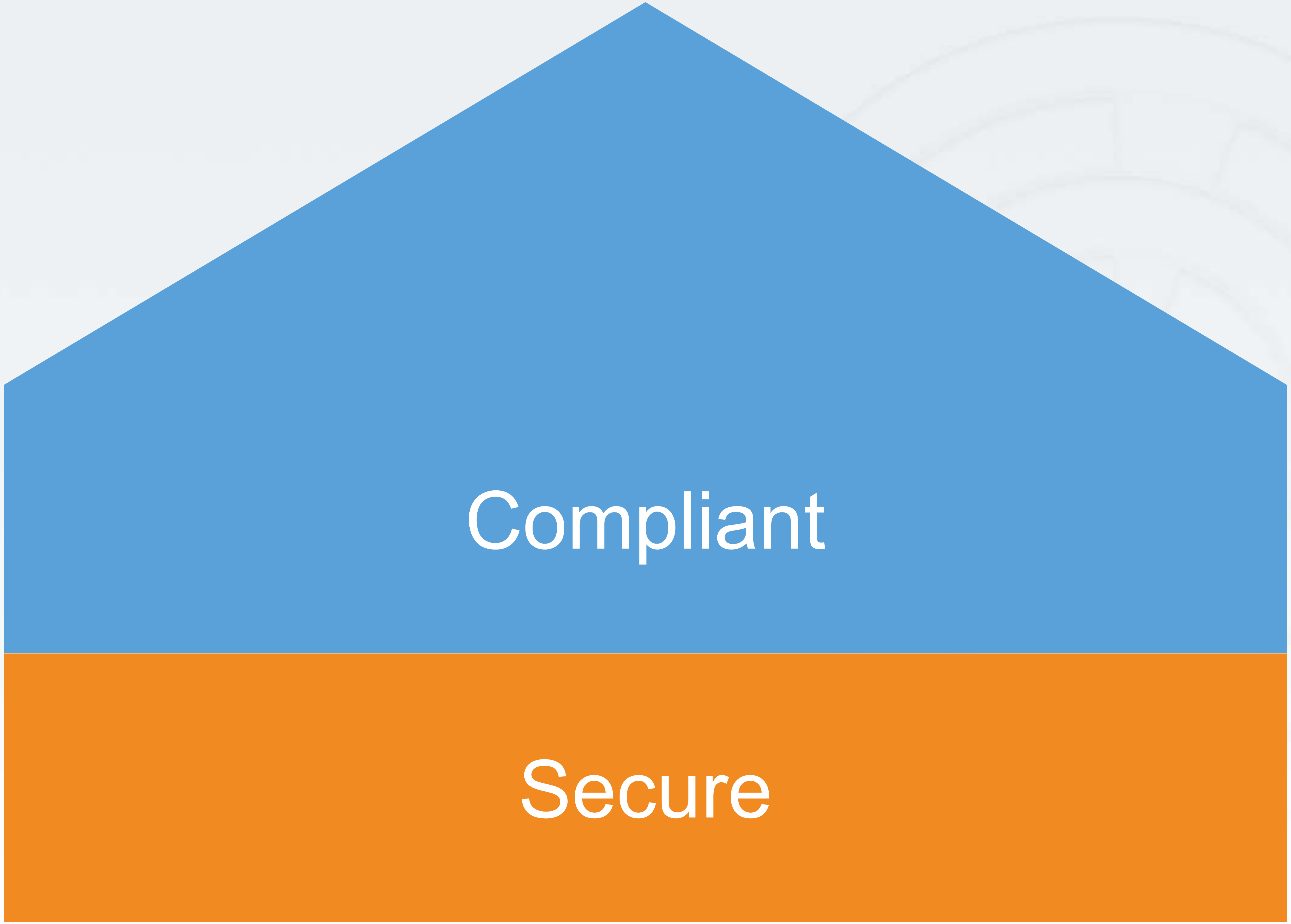
Translations: 한국말

One of the concepts that will feature in the new book I am working on is “risk management theatre”. This is the name I coined for the commonly-encountered control apparatus, imposed in a top-down way, which makes life painful for the innocent but can be circumvented by the guilty (the name comes by analogy with security theatre.) Risk management theatre is the outcome of optimizing processes for the case that somebody will do something stupid or bad, because (to quote Bjarte Bogsnes talking about management), “there might be someone who who cannot be trusted. The strategy seems to be preventative control on everybody instead of damage control on those few.”

Unfortunately risk management theatre is everywhere in large organizations, and reflects the continuing dominance of the Theory X management paradigm. The alternative to the top-down control approach is what I have called adaptive risk management, informed by human-centred management theories (for example the work of Ohno, Deming, Drucker, Denning and Dweck) and the study of how complex systems behave, particularly when they drift into failure. Adaptive risk management is based on systems thinking, transparency, experimentation, and fast feedback loops.

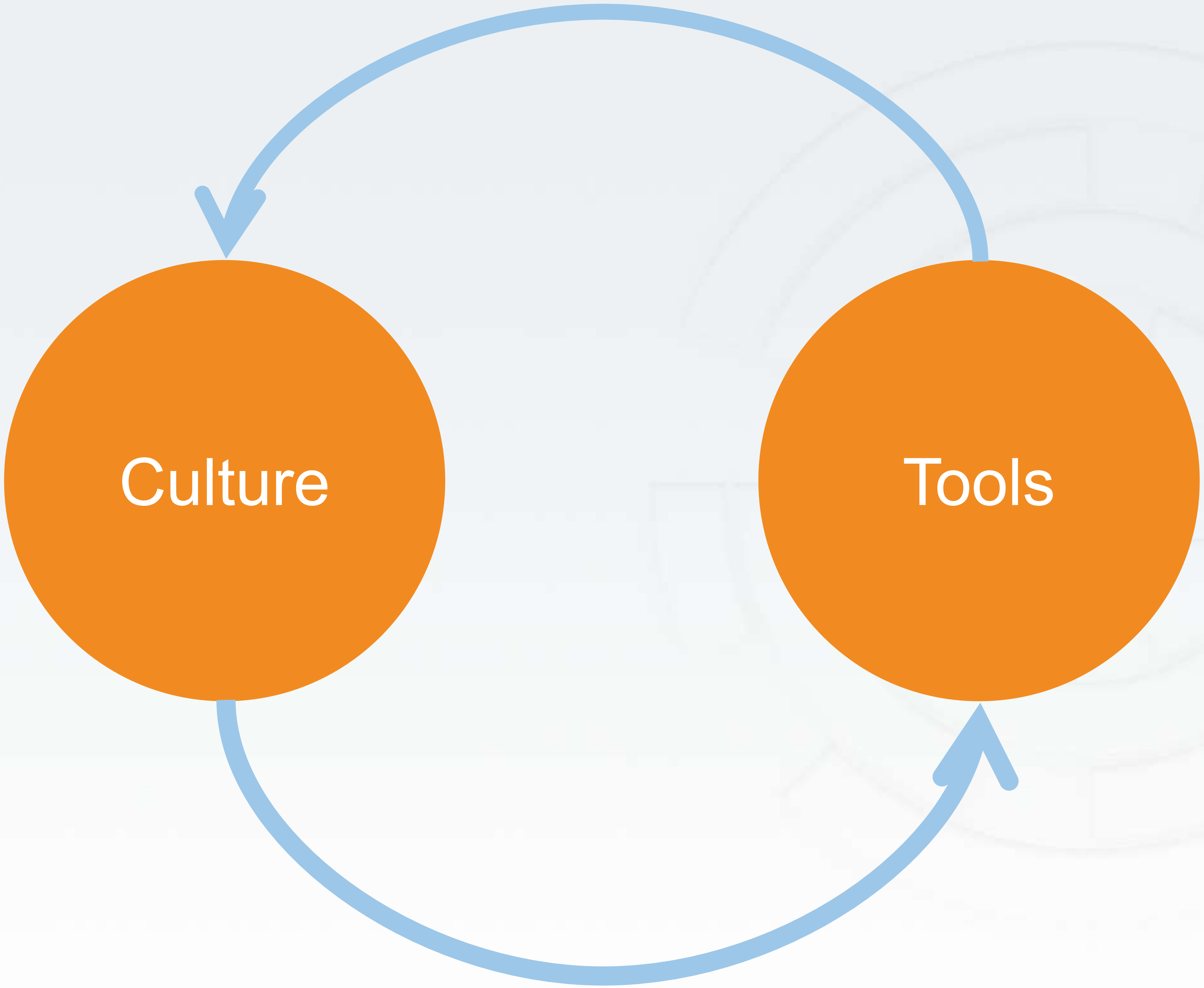
Here are some examples of the differences between the two approaches.

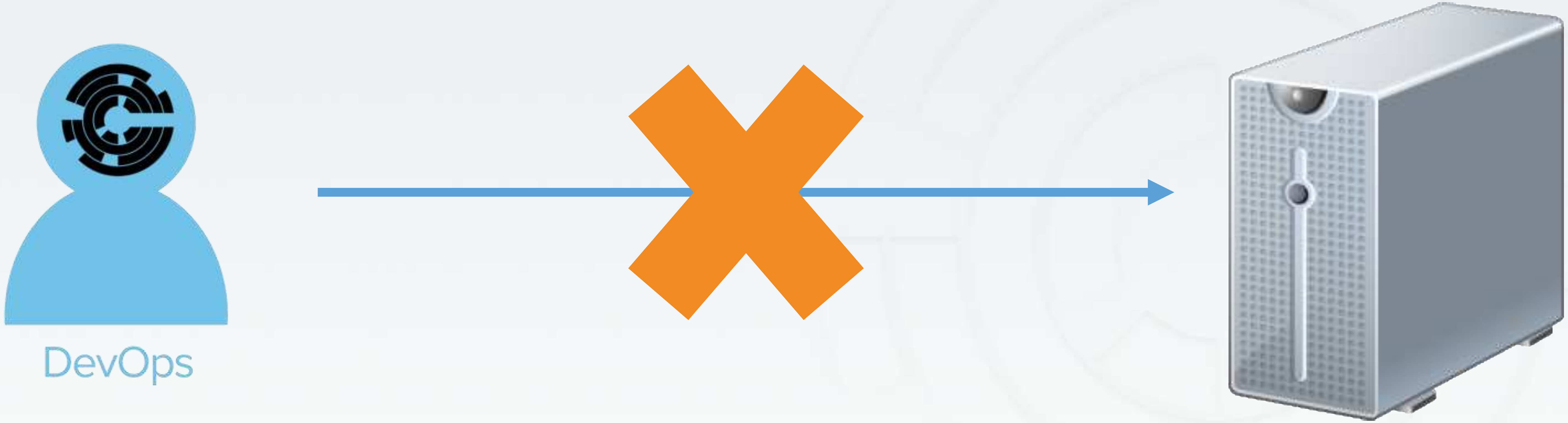
Adaptive risk management (people work to detect problems through improving	Risk management theatre (management imposes controls and processes which make life

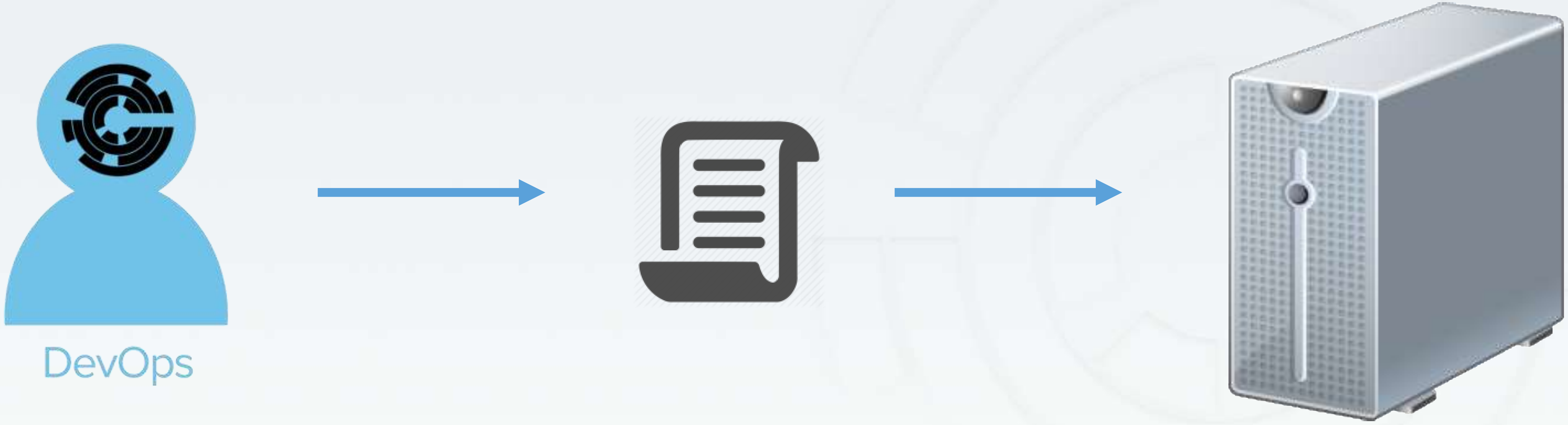


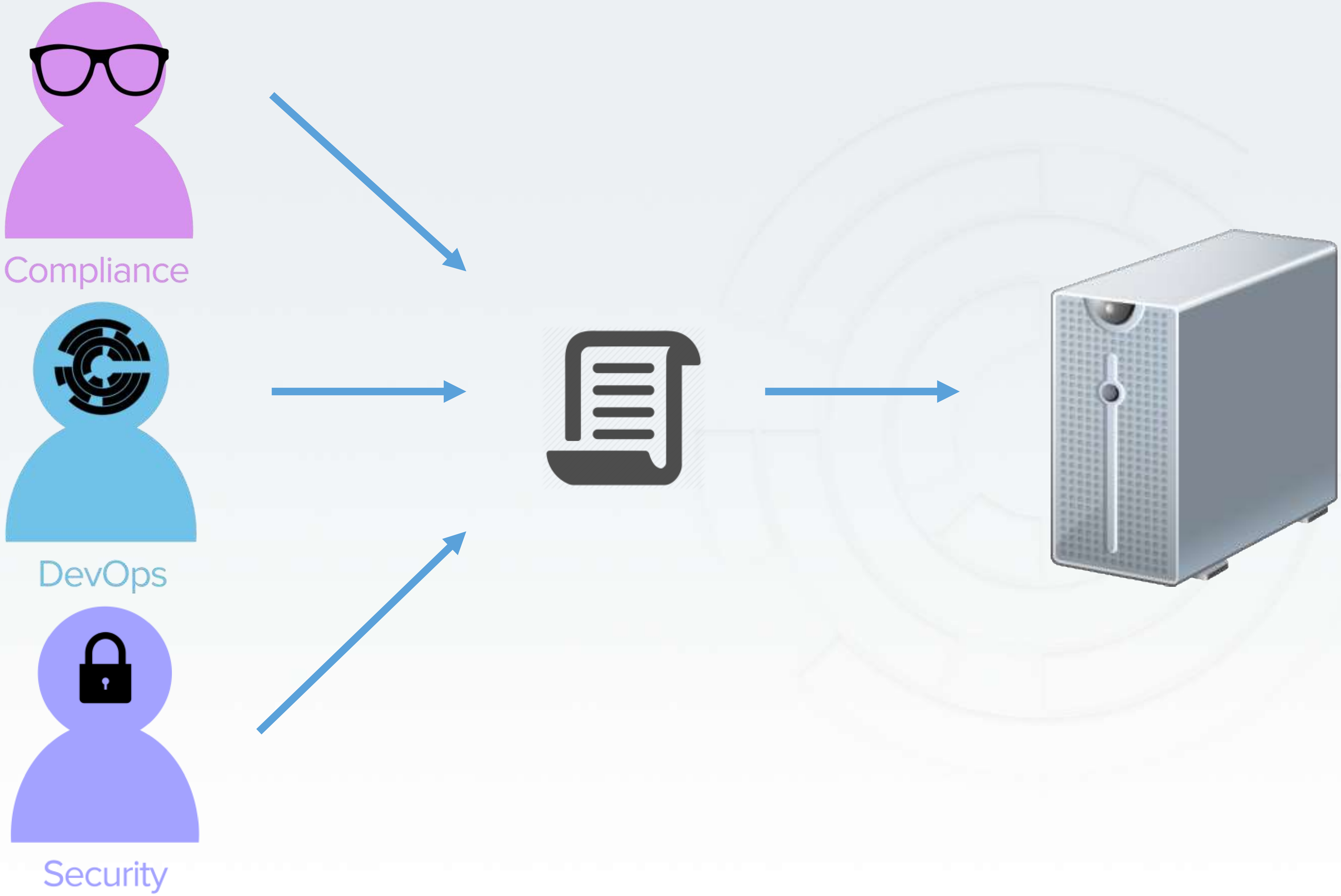
Compliant

Secure


Culture
Tools


DevOps


DevOps



Compliance

DevOps

Security

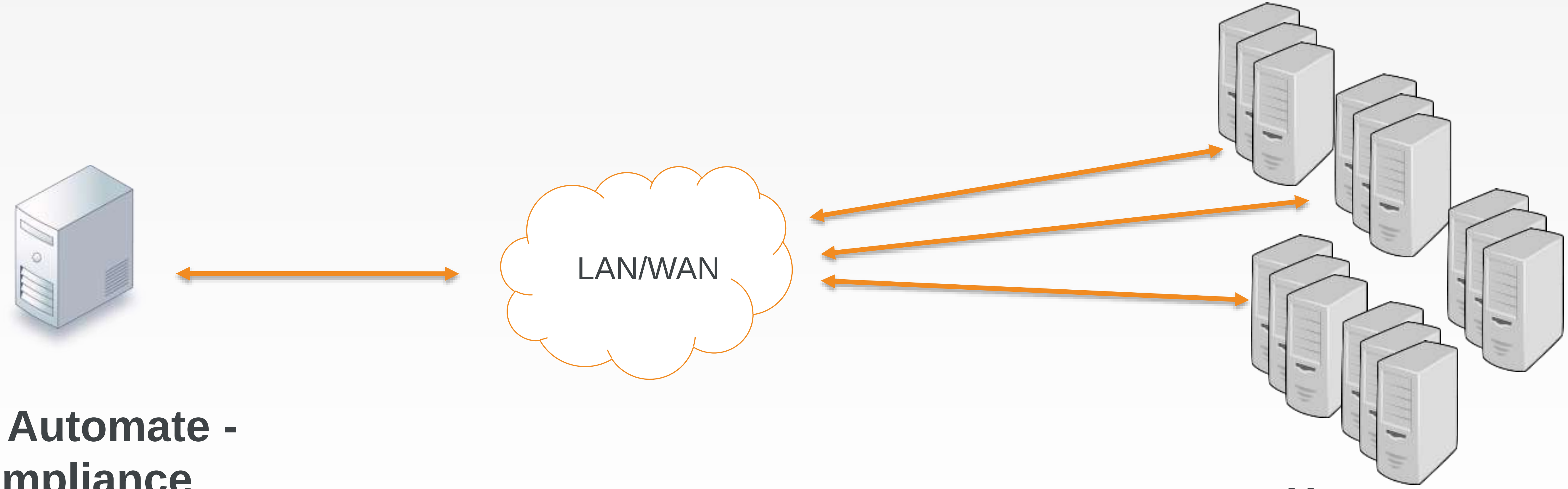
CONCEPT

Chef Compliance

Identify compliance issues, security risks, and outdated software with customizable reports. Write your own compliance rules in InSpec or get started quickly by using built-in profiles – predefined rule sets for a variety of security frameworks.

CONCEPT

Chef Compliance



Chef Automate - Compliance

Your Infrastructure

CONCEPT

Chef Compliance

Chef Compliance can run without any other Chef software installed.

The nodes you scan don't even need Chef software on them if you are scanning them for compliance.

However, you would need Chef software to create and implement remediation recipes.

CONCEPT

Chef Compliance

Reports: Chef Compliance can produce reports that indicate risks and issues classified by severity and impact levels.

Compliance Profiles: You can get started quickly with pre-built Compliance profiles for scanning Linux and Windows nodes.

Turn Compliance into Code

Chef Compliance leverages InSpec.

InSpec is an open-source run-time framework and rule language used to specify compliance, security, and policy requirements for testing any node in your infrastructure.

```
control 'cis-3.1' do
  impact 0.7
  title 'Set Daemon umask'
  desc '
    Set the default umask for all processes
    started at boot time.
  '
  describe file('/etc/sysconfig/init') do
    its('content') {should match 'umask 027'}
  end
end
```

Clearly Express Statements of Policy

InSpec includes a collection of resources to help you write auditing rules quickly and easily using the Compliance DSL.

Use InSpec to examine any node in your infrastructure; run the tests locally or remotely.

Any detected security, compliance, or policy issues are flagged in a log and in Chef Compliance, displayed in a GUI.

```
describe port(80) do
  it { should_not be_listening }
end

describe port(443) do
  it { should be_listening }
  its('protocols') {should include 'tcp'}
end
```

Find Issues Early

Execute the compliance tests as part of your local development.

Use InSpec as part of the Test Kitchen verification.

Check running systems against your Compliance Profiles.

Write code quickly

InSpec includes a collection of resources that help you write audit controls quickly and easily.

Write code quickly

```
describe file('/etc/ssh/sshd_config') do
  its(:content) { should match /Protocol 2/ }
end
```

Write code quickly

```
describe sshd_config do
  its(:content) { should match /Protocol 2/ }
end
```

Write code quickly

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

Available Resources

apache
apache_conf
apt
audit_policy
auditd_conf
auditd_rules
bash
bond
bridge
command
csv
directory
etc_group
file
gem
group

grub_conf
host
iis_site
inetd_conf
ini
interface
iptables
json
kernel_module
kernel_parameter
limits_conf
login_def
mount
mssql_session
mysql

mysql_conf
mysql_session
npm
ntp_conf
oneget
os
os_env
package
parse_config
passwd
pip
port
postgres
postgres_conf
postgres_session

powershell
processes
registry_key
security_policy
service
shadow
ssh_conf
ssl
user
vbscript
windows_feature
wmi
xinetd
yaml
yum

Run Code Anywhere

Test Locally:

```
$ inspec exec test.rb
```

Run Code Anywhere

Remote via SSH:

```
$ inspec exec test.rb -t ssh://54.163.150.246 --user=chef --password=chef.io
```

Run Code Anywhere

Remote via WinRM:

```
$ inspec exec test.rb -t winrm://Admin@192.168.1.2 --password super
```

Run Code Anywhere

Docker Container

```
$ inspec exec test.rb -t docker://3dda08e75838
```

Run Code Anywhere

```
$ inspec exec test.rb

$ inspec exec test.rb -i ~/.aws/nathen.pem -t ssh://ec2-user@54.152.7.203

$ inspec exec test.rb -t winrm://Admin@192.168.1.2 --password super

$ inspec exec test.rb -t docker://3dda08e75838
```

Inspect machines, data, & APIs

```
describe host('example.com', port: 80, proto: 'tcp') do
  it { should be_reachable }
end
```

Inspect machines, data, & APIs

```
describe mysql_conf do
  its('slow_query_log_file') { should eq 'hostname_slow.log' }
  its('slow_query_log') { should eq '0' }
  its('log_queries_not_using_indexes') { should eq '1' }
  its('long_query_time') { should eq '0.5' }
  its('min_examined_row_limit') { should eq '100' }
end
```

Inspect machines, data, & APIs

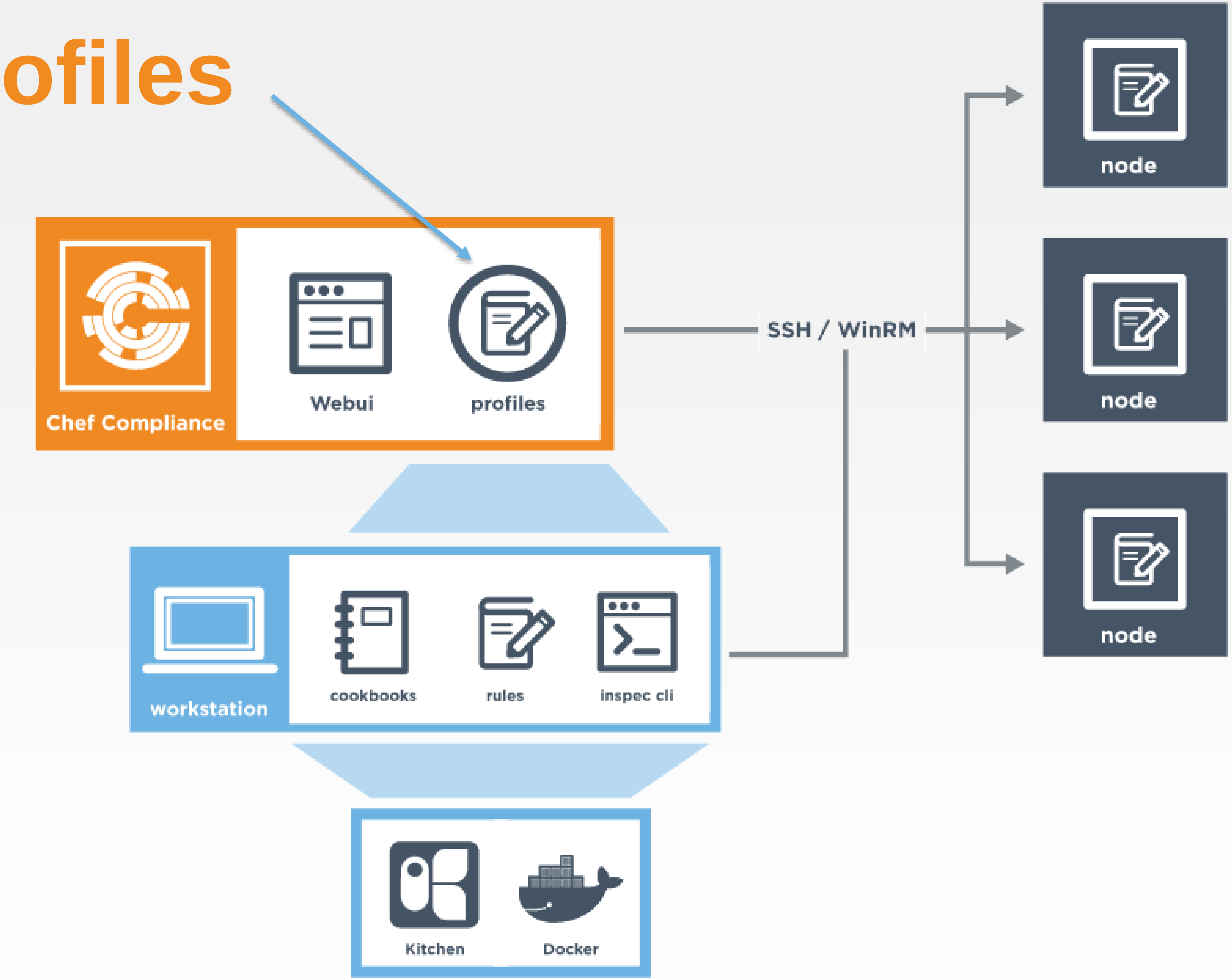
```
control 'sg-1' do
  impact 1.0
  title 'Security Group: No ingress access to CIDR block 0.0.0.0/0'
  desc 'Security Groups must not allow inbound access from anywhere'

  Vpc.new(id: ENV['vpc_id']).security_groups.each do |security_group|
    describe security_group do
      it { should_not have_ingress_rule().with_source('0.0.0.0/0') }
    end
  end
end
```

Compliance Profiles

Compliance profiles exist for many scenarios, such as those created by the Center for Internet Security (CIS)

Chef Compliance maintains profiles as a collection of individual controls that comprise a complete audit.

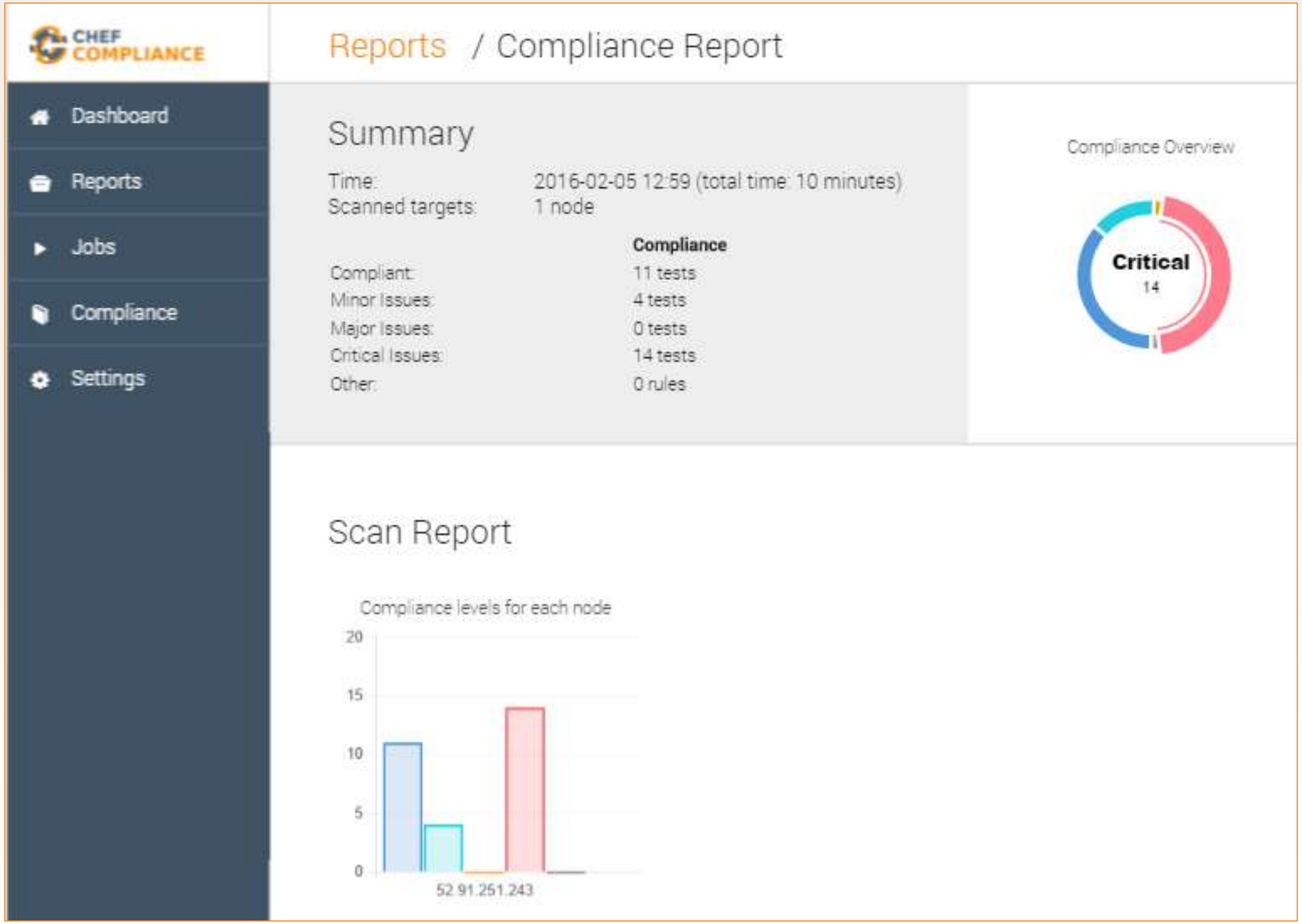
You can also create your own custom Compliance profiles.



Compliance Web UI

The Chef Compliance web UI provides views into compliance scan results as well as views of Chef Compliance profiles.

You execute scans via the Compliance web UI as well.



Reports / Compliance Report

Summary

Time: 2016-02-05 12:59 (total time: 10 minutes)
Scanned targets: 1 node

	Compliance
Compliant:	11 tests
Minor Issues:	4 tests
Major Issues:	0 tests
Critical Issues:	14 tests
Other:	0 rules

Scan Report

CHEF™