
# Continuous Patch and Security Assessment with


Christoph Hartmann

@chri_hartmann | chartmann@chef.io

# $> whoami

Christoph Hartmann

@chri_hartmann

- 8 years in industry
  - Deutsche Telekom and SAP
- Co-Founded startup VulcanoSec
  - need for missing compliance solutions
  - close collaboration with auditors
  - InSpec Creator
- Acquired by Chef Software
  - heading engineering for compliance


Source: http://content.time.com/time/covers/europe/0,16641,20020708,00.html

BUSINESS DAY

# $10 Million Settlement in Target Data Breach Gets Preliminary Approval

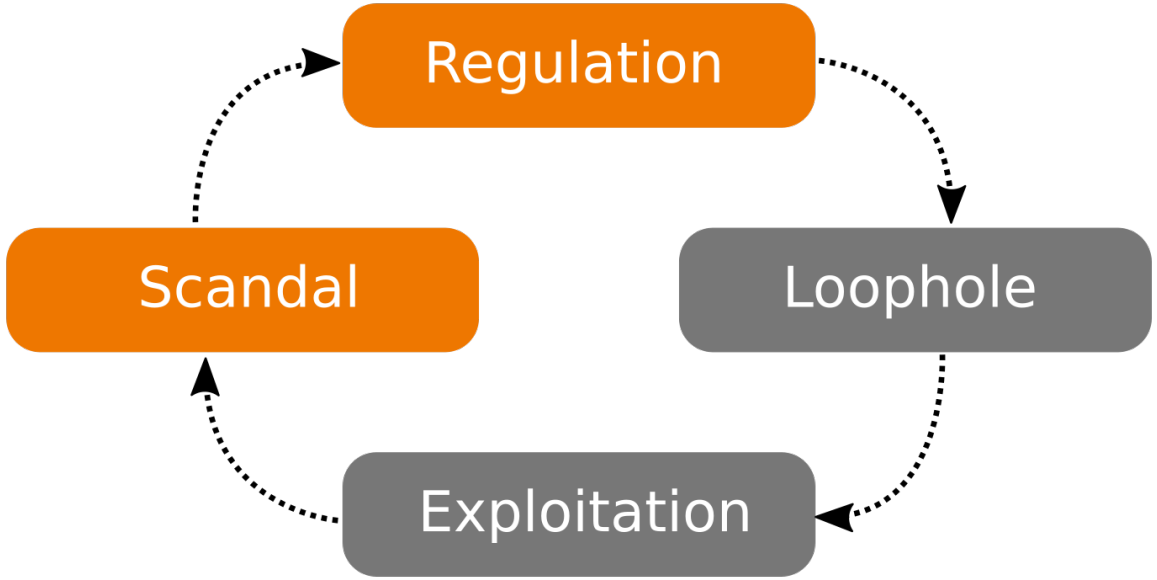
By HIROKO TABUCHI MARCH 19, 2015


A Target store in Maine. Shoppers affected by a data breach could receive up to $10,000 each.
Robert F. Bukaty/Associated Press

RELATED COVERAGE

For Target, the Breach Numbers Grow
JAN. 10, 2014

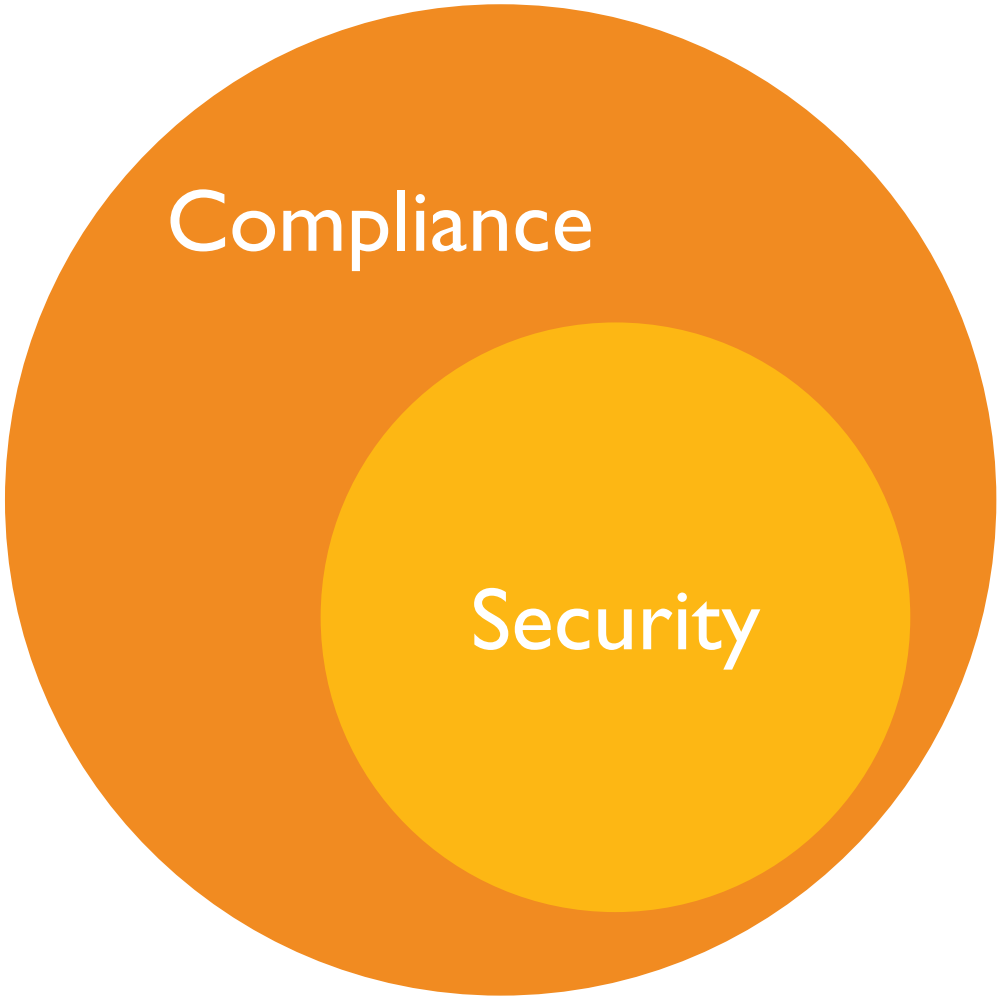
Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop AUG. 5, 2014


Regulation
Loophole
Exploitation
Scandal


# Regulatory Compliance

| | | |
|---|---|---|
| PCI-DSS | Gramm-Leach-Bliley Act | HIPAA |
| Dodd-Frank | ISO | Sarbanes-Oxley |
| HITECH | Grundschutz | European Central Bank Regulations |

# COMPLIANCE AND SECURITY




# State of Security in 2014

- In 60% of cases, attackers can compromise organizations within minutes.
- 99.9% of the exploited vulnerabilities were compromised more than a year after the vulnerability was published.
- Ten vulnerabilities account for 97% of the exploits observed.

Verizon Data Breach Report


# OWASP Top 10

| OWASP Top 10 – 2013 (Previous) | OWASP Top 10 – 2017 (New) |
|---|---|
| A1 – Injection | A1 – Injection |
| A2 – Broken Authentication and Session Management | A2 – Broken Authentication and Session Management |
| A3 – Cross-Site Scripting (XSS) | A3 – Cross-Site Scripting (XSS) |
| A4 – Insecure Direct Object References - Merged with A7 | A4 – Broken Access Control (Original category in 2003/2004) |
| A5 – Security Misconfiguration | A5 – Security Misconfiguration |
| A6 – Sensitive Data Exposure | A6 – Sensitive Data Exposure |
| A7 – Missing Function Level Access Control - Merged with A4 | A7 – Insufficient Attack Protection (NEW) |
| A8 – Cross-Site Request Forgery (CSRF) | A8 – Cross-Site Request Forgery (CSRF) |
| A9 – Using Components with Known Vulnerabilities | A9 – Using Components with Known Vulnerabilities |
| A10 – Unvalidated Redirects and Forwards - Dropped | A10 – Underprotected APIs (NEW) |

# OWASP Top 10


## A5 – Security Misconfiguration

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, platform, etc. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.

## A9 – Using Components with Known Vulnerabilities

Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.

# Why is it so difficult?

**References:**

1. AJ Lewis, "LVM HOWTO", http://tldp.org/HOWTO/LVM-HOWTO/

### 1.1.10 Add nodev Option to /home (Scored)

**Profile Applicability:**

- Level 1

**Description:**

When set on a file system, this option prevents character and block special devices from being defined, or if they exist, from being used as character and block special devices.

**Rationale:**

Since the user partitions are not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices.

**Note:** The actions in the item refer to the `/home` partition, which is the default user partition that is defined in CentOS 6. If you have created other user partitions, it is recommended that the Remediation and Audit steps be applied to these partitions as well.

**Audit:**

Run the following commands to determine if the system is configured as recommended.

```
# grep /tmp /etc/fstab | grep noexec
# mount | grep /tmp | grep noexec
```

If either command emits no output then the system is not configured as recommended.

**Remediation:**

Edit the `/etc/fstab` file and add `nodev` to the fourth field (mounting options). See the `fstab(5)` manual page for more information.

```
# mount -o remount,nodev /home
```

### 1.1.11 Add nodev Option to Removable Media Partitions (Not Scored)

**Profile Applicability:**

- Level 1

**Description:**

Set `nodev` on removable media to prevent character and block special devices that are present on the removable be treated as these device files.

**Rationale:**

Removable media containing character and block special devices could be used to circumvent security controls by allowing non-root users to access sensitive device files such as `/dev/kmem` or the raw disk partitions.

**Audit:**

```
# grep <each removable media mountpoint> /etc/fstab
Verify that nodev is an option
```

**Remediation:**

Edit the `/etc/fstab` file and add "`nodev`" to the fourth field (mounting options). Look for entries that have mount points that contain words such as floppy or cdrom. See the `fstab(5)` manual page for more information.

### 1.1.12 Add noexec Option to Removable Media Partitions (Not Scored)

**Profile Applicability:**

- Level 1

**Description:**

Set `noexec` on removable media to prevent programs from executing from the removable media.

**Rationale:**

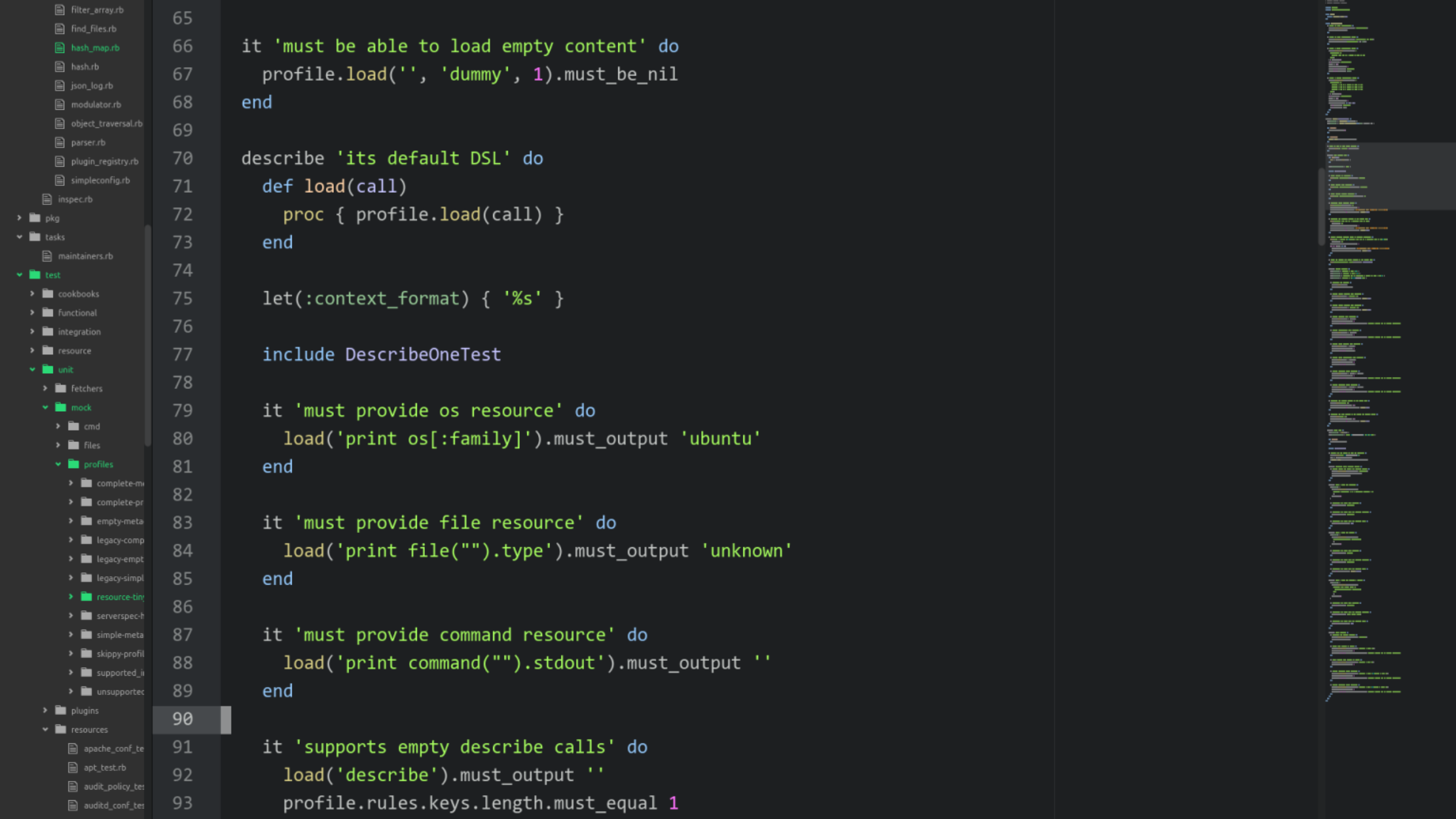
Setting this option on a file system prevents users from executing programs from the removable. This deters users from being to introduce potentially malicious software on the system.

**Audit:**

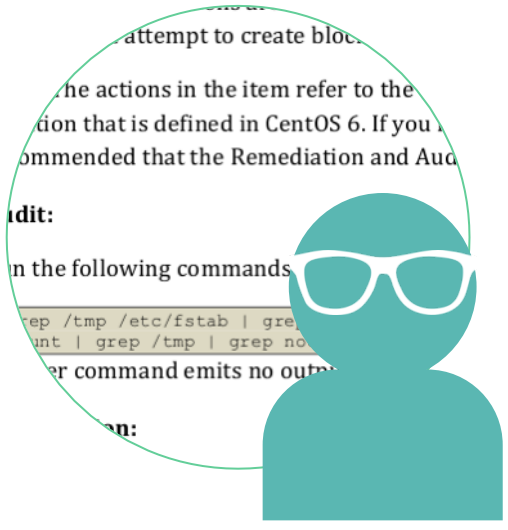
```
# grep <each removable media mountpoint> /etc/fstab
```

**Note:** Verify that `noexec` is an option

**Remediation:**


filter_array.rb
find_files.rb
hash_map.rb
hash.rb
json_log.rb
modulator.rb
object_traversal.rb
parser.rb
plugin_registry.rb
simpleconfig.rb
inspec.rb
pkg
tasks
maintainers.rb
test
cookbooks
functional
integration
resource
unit
fetchers
mock
cmd
files
profiles
plugins
resources
apache_conf_te
apt_test.rb
audit_policy_tes
auditd_conf_tes
65
66 it 'must be able to load empty content' do
67 profile.load('', 'dummy', 1).must_be_nil
68 end
69
70 describe 'its default DSL' do
71 def load(call)
72 proc { profile.load(call) }
73 end
74
75 let(:context_format) { '%s' }
76
77 include DescribeOneTest
78
79 it 'must provide os resource' do
80 load('print os[:family]').must_output 'ubuntu'
81 end
82
83 it 'must provide file resource' do
84 load('print file("").type').must_output 'unknown'
85 end
86
87 it 'must provide command resource' do
88 load('print command("").stdout').must_output ''
89 end
90
91 it 'supports empty describe calls' do
92 load('describe').must_output ''
93 profile.rules.keys.length.must_equal 1

# Language

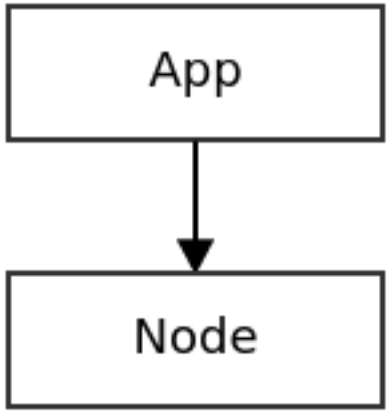



Compliance

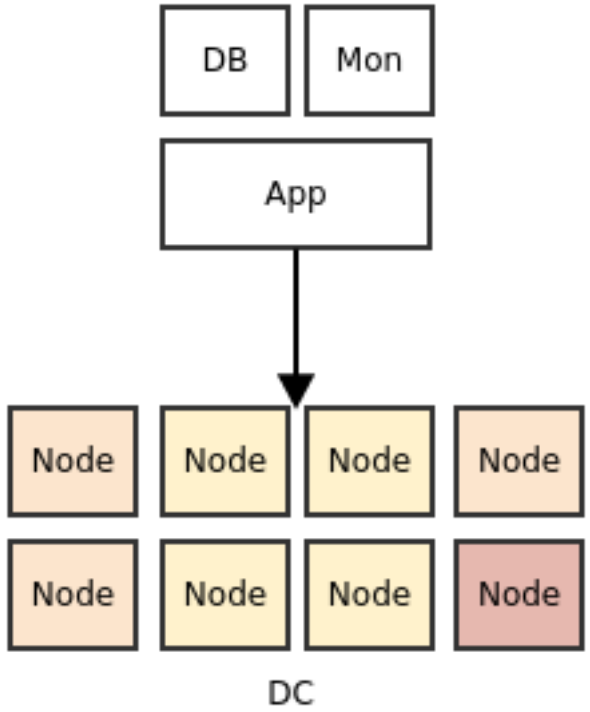

Security


DevOps

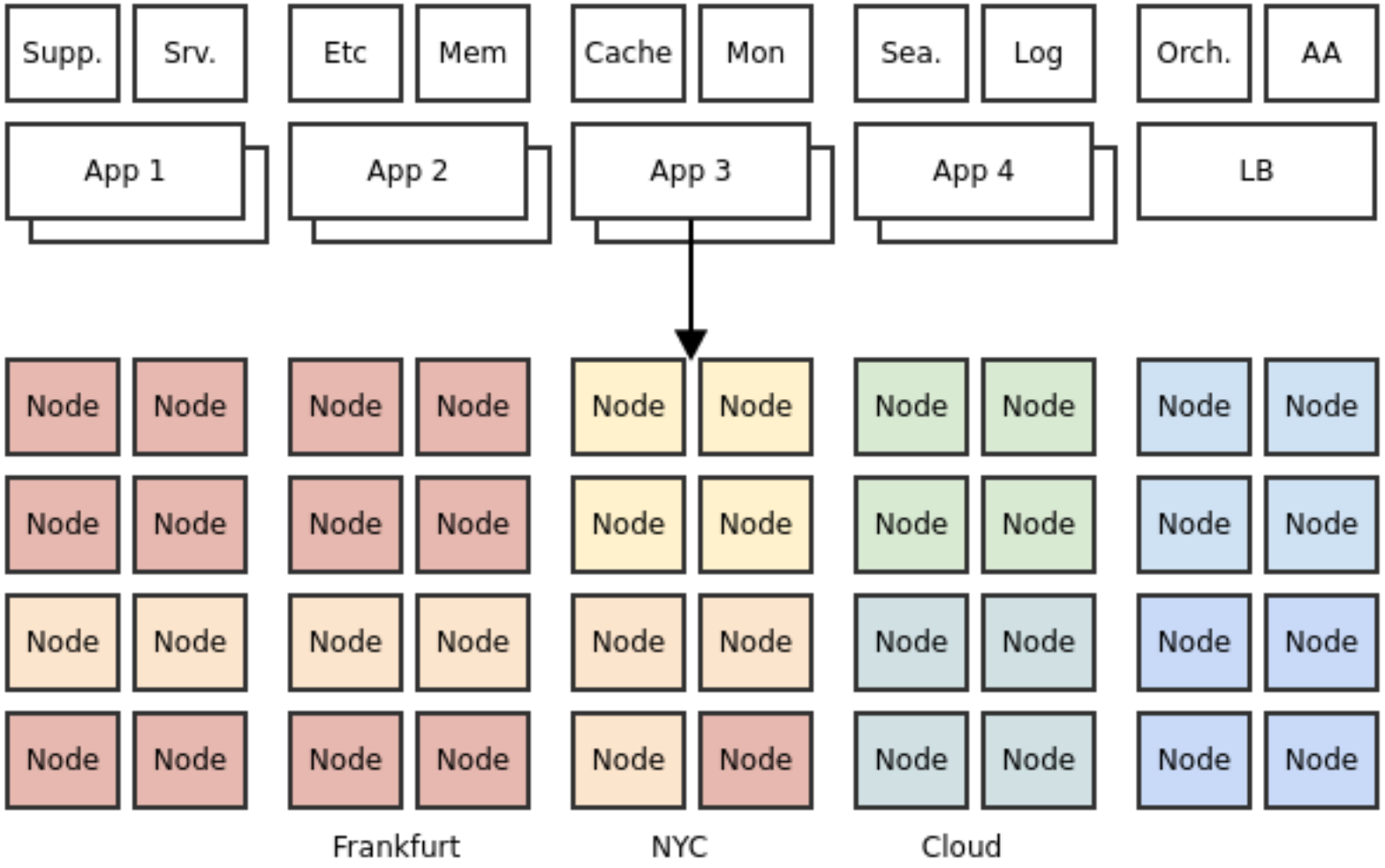
# Scale

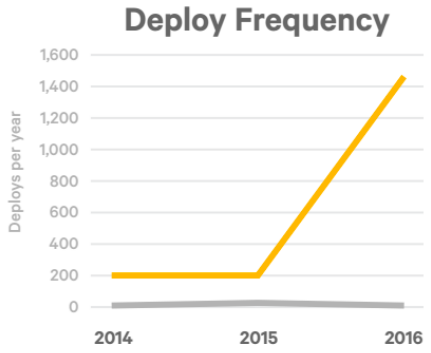


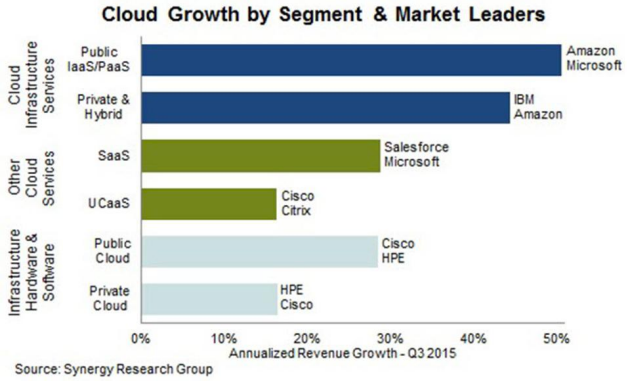
# Scale

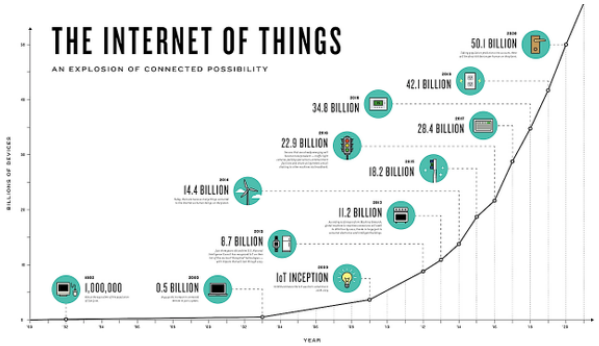


# Scale


Supp.
Srv.
Etc
Mem
Cache
Mon
Sea.
Log
Orch.
AA
App 1
App 2
App 3
App 4
LB
Node
Frankfurt
NYC
Cloud




**DevOps**

**Cloud**

**IoT**

# Compliance-Driven Infrastructure


# Let's talk about solutions

INSPEC

github.com/dev-sec


InSpec turns infrastructure testing, compliance
and security requirements into code

# Documentation


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.

# Scripting tools


```
> grep "^Protocol" /etc/ssh/sshd_config | sed 's/Protocol //'
2
```

# The better way
# TESTING A REQUIREMENT


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

# Compliance Language


```
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
```


# Standalone Usage

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

```
$ inspec exec test.rb
$ inspec exec test.rb -i vagrant.key -t ssh://root@172.17.0.1:11022
$ inspec exec test.rb -t winrm://Admin@192.168.1.2 --password super
$ inspec exec test.rb -t docker://3cc8837bb6a8
```

OWASP
AppSec EU
Belfast
May 2017

# Supported Operating Systems


Amazon Linux
2014.09 / 2015.03

CentOS
6 / 7


HP UX
11i


IBM AIX
5.3 / 6.1 / 7.1

RHEL
6 / 7


SLES
11 / 12

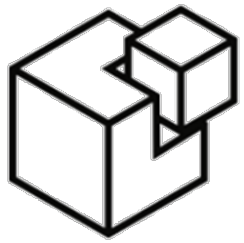
Ubuntu Server
12.04 / 14.04

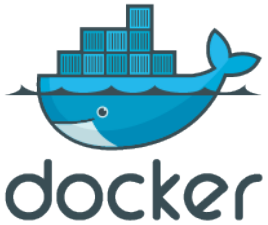
Windows
2012 R2

# Built-in resources


**apache** apache_conf **apt audit_policy** auditd_conf auditd_rules bash bond bridge bsd_service **command** crontab csv dh_params directory **docker** docker_container docker_image etc_group **file** gem group **groups** grub_conf host http **iis_site** iis_website inetd_conf ini interface iptables json kernel_module **kernel_parameter key_rsa** launchd_service limits_conf login_defs mount **mssql_session** mysql mysql_conf **mysql_session** npm ntp_conf oneget **oracledb_session** os os_env package packages parse_config parse_config_file passwd pip port **postgres** postgres_conf postgres_session **powershell** ppa processes rabbitmq_config **registry_key** runit_service script security_policy **service** shadow **ssh_config** sshd_config **ssl** sys_info systemd_service sysv_service upstart_service user **users** vbscript windows_feature windows_registry_key windows_task wmi **x509_certificate** xinetd_conf yaml yum yumrepo zfs_dataset zfs_pool

# Works with all DevOps tools e.g.





# 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
```

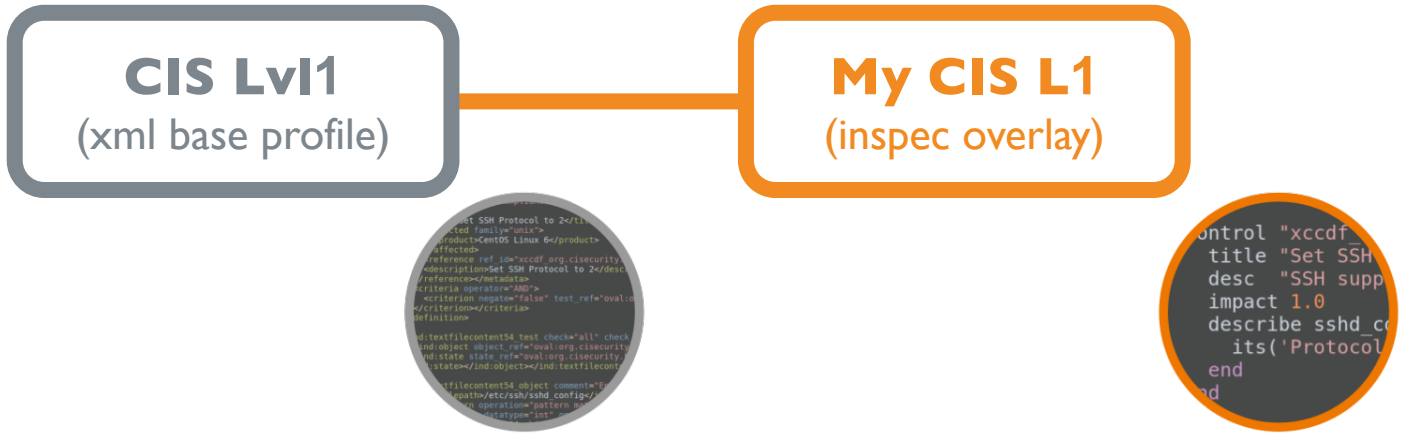
**Remediation:**

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

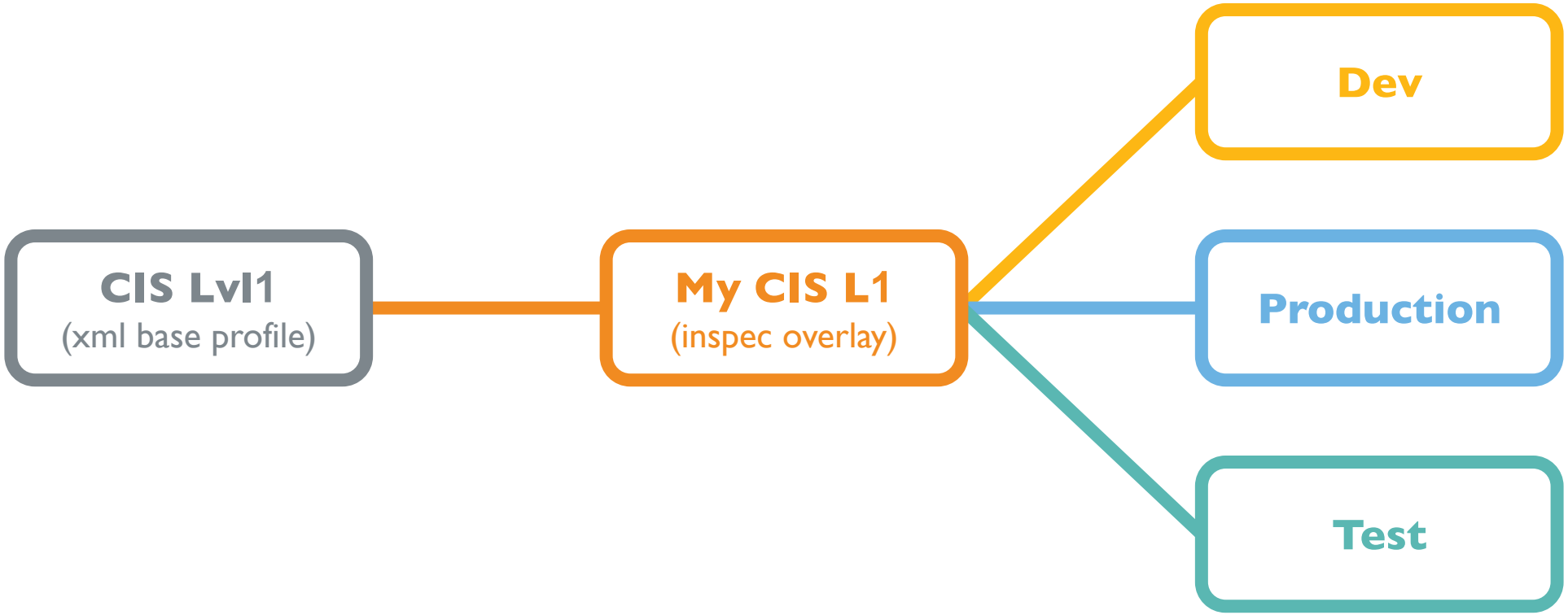
```
Protocol 2
```

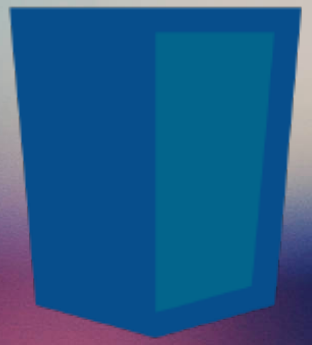
```
control 'ssh-1234' do
  impact 1.0
  title 'Server: Set protocol version to SSHv2'
  desc "
    Set the SSH protocol version to 2. Don't use legacy
    insecure SSHv1 connections anymore...
  "

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

# Manage Baselines



# Manage Baseline Overlays





github.com/dev-sec


# InSpec Profiles

DevSec Linux Baseline

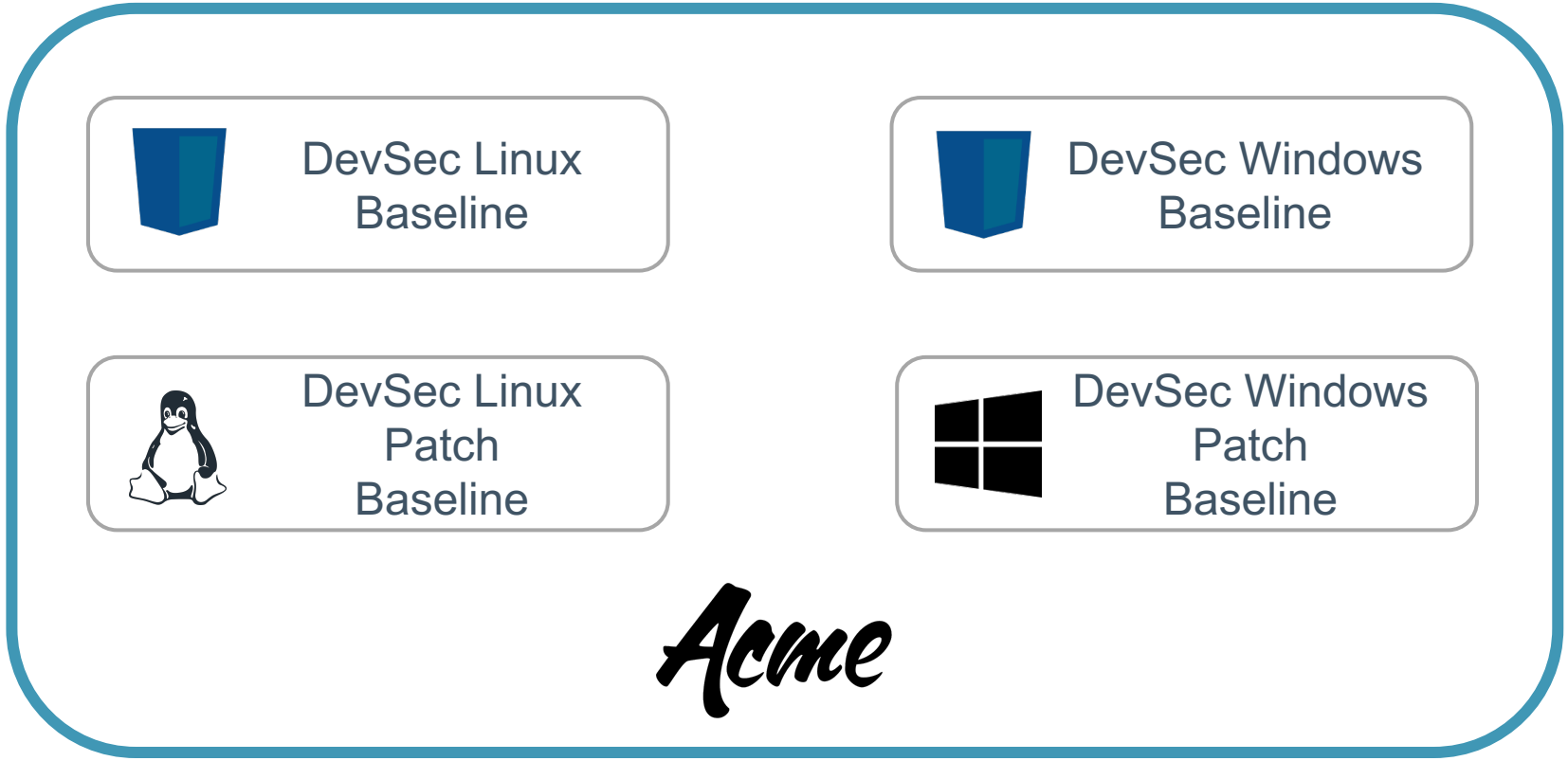
DevSec Windows Baseline

DevSec Linux Patch Baseline

DevSec Windows Patch Baseline

github.com/dev-sec
github.com/chris-rock/acme-inspec-profile


# InSpec Profiles

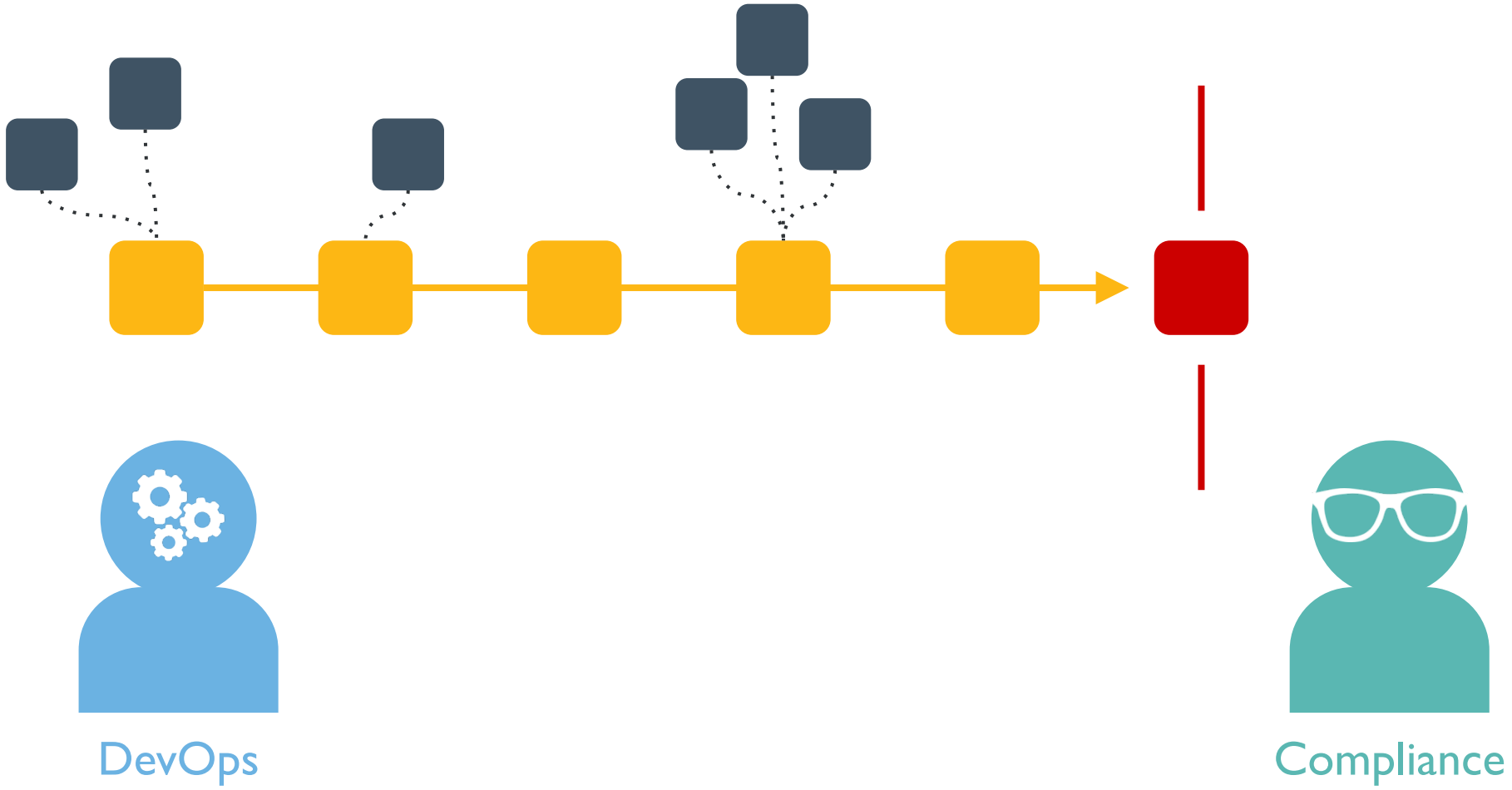



github.com/dev-sec
github.com/chris-rock/acme-inspec-profile

# InSpec Profiles


```
include_controls 'os-hardening' do
  skip_control 'os-06'

  control 'os-02' do
    impact 0.7
  end
end

include_controls 'ssh-hardening'
```

# Continuous Compliance



# Continuous Compliance

Scan for Compliance

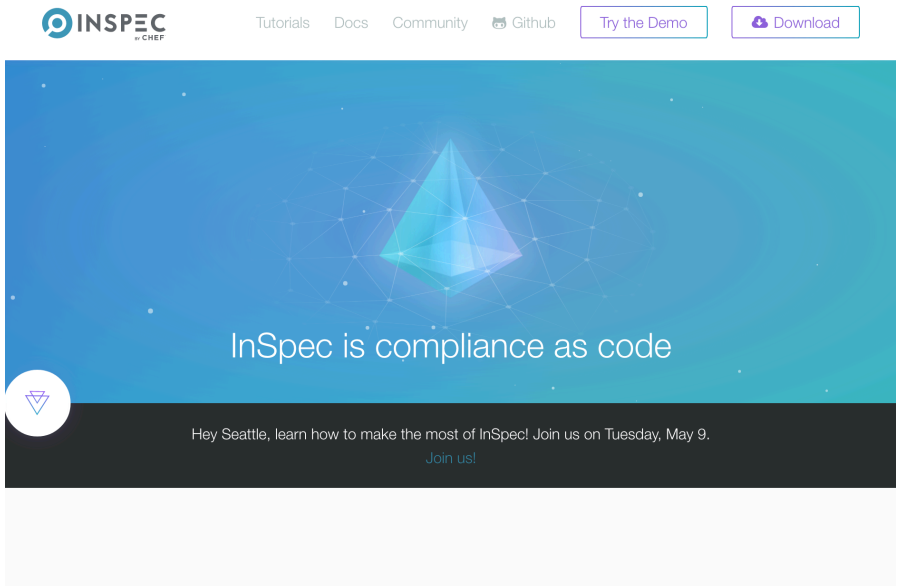
Build & Test Locally

Build & Test CI/CD

Remediate

Verify

# Further Resources




## inspec.io

- Hands on tutorials
- Extensive documentation
- Code examples


## dev-sec.io

- github.com/dev-sec/linux-baseline
- github.com/dev-sec/windows-baseline
- github.com/dev-sec/ssh-baseline
- github.com/dev-sec/windows-patch-baseline
- github.com/dev-sec/linux-patch-baseline


Join


Christoph Hartmann


chartmann@chef.io


@chri_hartmann


# Chef vs InSpec

| | chef-client | inspec |
|---|---|---|
| Project | github.com/chef/chef | github.com/chef/inspec |
| First Commit | March 2008 | April 2015 |
| Language | Ruby DSL | Ruby DSL |
| Code | `service 'iptables' do`<br>`  action [ :enable, :start ]`<br>`end` | `describe service('iptables') d`<br>`  it { should be_enabled }`<br>`  it { should be_running }`<br>`end` |
| Execution | Local | Local / Remote (SSH, WinRM, Docker) |
| Artifacts | Recipes, Resources, Cookbooks | Controls, Resources, Profiles |
| Share | Chef Supermarket, Github, Bitbucket, etc | Chef Supermarket, Github, Bitbucket, etc |