puppet

Is it safe?
How compliance and auditing fit with Config Management

Peter Souter

Senior Professional Services Engineer | Puppet
@petersouter

Who am I?

@petersouter

petems
IRC/Slack/GitHub

Senior Professional Services Engineer

5 years using Puppet

2 years @ Puppet Inc

Help customers deploy Puppet

Teach Puppet classes

Contribute to the community and open-source

Warning: I speak quickly

And I have a different accent...

Warning: I am not a lawyer or auditor

Always go speak to one of them before implementing some of the stuff I’m talking about!

So, why are we here?

(This room specifically, listening to this talk...)

Show of hands in the room

Who has to deal with IT compliance or auditing in their current role?

So what is compliance?

What does it mean?

“Many organisations in the public sector and the regulated industries, such as utilities and legal or financial services, have to demonstrate an information security policy that proves they have a range of steps and measures in place...**If these policies are not adhered to, the regulators reserve the right to prosecute**”

- http://www.computerweekly.com/feature/Information-security-The-route-to-compliance

Sidebar: Important distinction

Compliance is not security!

“Compliance is the discipline of verification at scale”

It’s the ops equivalent of planning permission, zoning laws, building guidelines etc.

Think about how many files, scripts, artifacts and services make up your estate

How could you ever check every single one of them, and what should you be prioritising?

This means compliance straddles an awkward organisational line

- Who’s responsible?
- Who runs the scans?
- Who fixes things when they go wrong?

Regardless: Someone has told you you need to follow the rules

Either for best practise or legal reasons...

Alphabet Soup

Control Objectives for Information and related Technology **(COBIT)**
Defense Information Systems Agency **(DISA) STIGs**
Federal Information Security Management Act **(FISMA)**
Federal Desktop Core Configuration **(FDCC)**
Gramm-Leach-Bliley Act **(GLBA)**
Health Insurance Portability and Accountability Act **(HIPAA)**
ISO 27002/17799 Security Standards
Information Technology Information Library **(ITIL)**
National Institute of Standards **(NIST)** configuration guidelines
National Security Agency **(NSA)** configuration guidelines
Payment Card Industry Data Security Standards **(PCI DSS)**
Sarbanes-Oxley **(SOX)**
Site Data Protection **(SDP)**
United States Government Configuration Baseline **(USGCB)**
California's Security Breach Notification Act - **SB 1386**

You might have your own **hardening** policies

Removing non-essential users etc.

Center for Internet Security (CIS)

“Enhance the cyber security readiness and response of public and private sector entities, with a commitment to excellence through collaboration”

- Founded in October, 2000
- It is composed of roughly 180 members from 17 different countries.
- Wide range of entities, including academia and the government
- Kind of a non-government fork of the STIG standards

CIS standard exist for a lot of applications and tools:

Amazon Linux, Amazon Web Services
Apache Tomcat, Apache HTTP Server Assessment Tool
Apple iOS, Apple OSX, Apple Safari, Benchmark Mappings: Medical Device Security Standards
CentOS Linux, CheckPoint Firewall, Cisco Device
Debian Linux, Distribution Independent Linux, Docker, FreeBSD, FreeRadius, Google Android, Google Chrome, HP-UX, IBM AIX, IBM DB2, IBM DB2 Benchmark Archive
ISC BIND, Juniper Device, Kerberos, LDAP, Microsoft Exchange Server, Microsoft IIS, Microsoft Internet Explorer, Microsoft MS SQL Server, Microsoft Office, Microsoft SharePoint Server, Microsoft Windows 10, Microsoft Windows 7, Microsoft Windows 8, Microsoft Windows NT, Microsoft Windows Server 2000, Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2012, Microsoft Windows XP, Mozilla Firefox, MySQL
Novell Netware, Opera, Oracle Database Server, Oracle Database Server Assessment Tool
Oracle Linux, Oracle Solaris, Red Hat Linux, Slackware Linux, SuSE Linux, Sybase ASE, Ubuntu
VMware, Wireless Network Devices, Xen

A lot of the time, you have to dig through a lot of legalese to get to an engineerable problem

And whether your engineering solution actually succeeds in it’s goal is entirely up to the discretion of your auditor

An example: HIPAA

Health Insurance Portability and Accountability Act of 1996

The HIPAA Security Rule establishes national standards to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164.

- https://www.hhs.gov/hipaa/for-professionals/security/index.html

Ok, let's go digging

Let's look for 45 CFR Part 160 and Subparts A and C of 164

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS
Contents
Subpart A—General Provisions

§160.101 Statutory basis and purpose.
§160.102 Applicability.
§160.103 Definitions.
§160.104 Modifications.
§160.105 Compliance dates for implementation of new or modified standards and implementation specifications.
Subpart B—Preemption of State Law

§160.201 Statutory basis.
§160.202 Definitions.
§160.203 General rule and exceptions.
§160.204 Process for requesting exception determinations.
§160.205 Duration of effectiveness of exception determinations.
Subpart C—Compliance and Investigations

§160.300 Applicability.
§160.302 [Reserved]
§160.304 Principles for achieving compliance.
§160.306 Complaints to the Secretary.
§160.308 Compliance reviews.
§160.310 Responsibilities of covered entities and business associates.
§160.312 Secretarial action regarding complaints and compliance reviews.
§160.314 Investigational subpoenas and inquiries.
§160.316 Refraining from intimidation or retaliation.
Subpart D—Imposition of Civil Money Penalties

§160.400 Applicability.
§160.401 Definitions.
§160.402 Basis for a civil money penalty.
§160.404 Amount of a civil money penalty.
§160.406 Violations of an identical requirement or prohibition.
§160.408 Factors considered in determining the amount of a civil money penalty.
§160.410 Affirmative defenses.
§160.412 Waiver.
§160.414 Limitations.
§160.416 Authority to settle.
§160.418 Penalty not exclusive.
§160.420 Notice of proposed determination.
§160.422 Failure to request a hearing.
§160.424 Collection of penalty.
§160.426 Notification of the public and other agencies.
Subpart E—Procedures for Hearings

45 CFR Part 164, Subpart C - Security Standards for the Protection of Electronic Protected Health Information

§ 164.302 — Applicability.
§ 164.304 — Definitions.
§ 164.306 — Security standards: General rules.
§ 164.308 — Administrative safeguards.
§ 164.310 — Physical safeguards.
§ 164.312 — Technical safeguards.
§ 164.314 — Organizational requirements.
§ 164.316 — Policies and procedures and documentation requirements.
§ 164.318 — Compliance dates for the initial implementation of the security standards.

PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS
Contents
Subpart A—General Provisions

§160.101 Statutory basis and purpose.
§160.102 Applicability.
§160.103 Definitions.
§160.104 Modifications.
§160.105 Compliance dates for implementation of new or modified standards and implementation specifications.
Subpart B—Preemption of State Law

§160.201 Statutory basis.
§160.202 Definitions.
§160.203 General rule and exceptions.
§160.204 Process for requesting exception determinations.
§160.205 Duration of effectiveness of exception determinations.
Subpart C—Compliance and Investigations

§160.300 Applicability.
§160.302 [Reserved]
§160.304 Principles for achieving compliance.
§160.306 Complaints to the Secretary.
§160.308 Compliance reviews.
§160.310 Responsibilities of covered entities and business associates.
§160.312 Secretarial action regarding complaints and compliance reviews.
§160.314 Investigational subpoenas and inquiries.
§160.316 Refraining from intimidation or retaliation.
Subpart D—Imposition of Civil Money Penalties

§160.400 Applicability.
§160.401 Definitions.
§160.402 Basis for a civil money penalty.
§160.404 Amount of a civil money penalty.
§160.406 Violations of an identical requirement or prohibition.
§160.408 Factors considered in determining the amount of a civil money penalty.
§160.410 Affirmative defenses.
§160.412 Waiver.
§160.414 Limitations.
§160.416 Authority to settle.
§160.418 Penalty not exclusive.
§160.420 Notice of proposed determination.
§160.422 Failure to request a hearing.
§160.424 Collection of penalty.
§160.426 Notification of the public and other agencies.
Subpart E—Procedures for Hearings

45 CFR Part 164, Subpart C - Security Standards for the Protection of Electronic Protected Health Information

§ 164.302 — Applicability.
§ 164.304 — Definitions.
§ 164.306 — Security standards: General rules.
§ 164.308 — Administrative safeguards.
§ 164.310 — Physical safeguards.
§ 164.312 — Technical safeguards.
§ 164.314 — Organizational requirements.
§ 164.316 — Policies and procedures and documentation requirements.
§ 164.318 — Compliance dates for the initial implementation of the security standards.

Technical Safeguards!

Finally we’re getting somewhere...

§ 164.312 Technical safeguards.

A covered entity or business associate must, in accordance with § 164.306:

(a)

(1) Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in § 164.308(a)(4).

(2) Implementation specifications:

(i) Unique user identification (Required). Assign a unique name and/or number for identifying and tracking user identity.

(ii) Emergency access procedure (Required). Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.

(iii) Automatic logoff (Addressable). Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.

(iv) Encryption and decryption (Addressable). Implement a mechanism to encrypt and decrypt electronic protected health information.

(b) Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

The pain of compliance will be directly correlated to the relationship with your auditors

Ultimately, they are the ones that you need to prove that you are in compliance too

Unfortunately, this is often a manual process

- Emails
- PDFs
- Dead trees
- Humans

There’s got to be a better way!

If only there was something better...

What is IT compliance?

A series of rules for systems that need to be enforced and reported on

What is configuration management?

A series of rules for systems that need to be enforced and reported on

Great, let's use config management tools!

But...what’s so great about using config management tools to enforce these standards?

Reduce cost and time per release

Pre-existing code for known standards often available

Potential for sharing and reuse

Share within your company or with the public

Single Source of Truth

Your infrastructure as code repository becomes your one place to look for compliance code

Less arguments about semantics

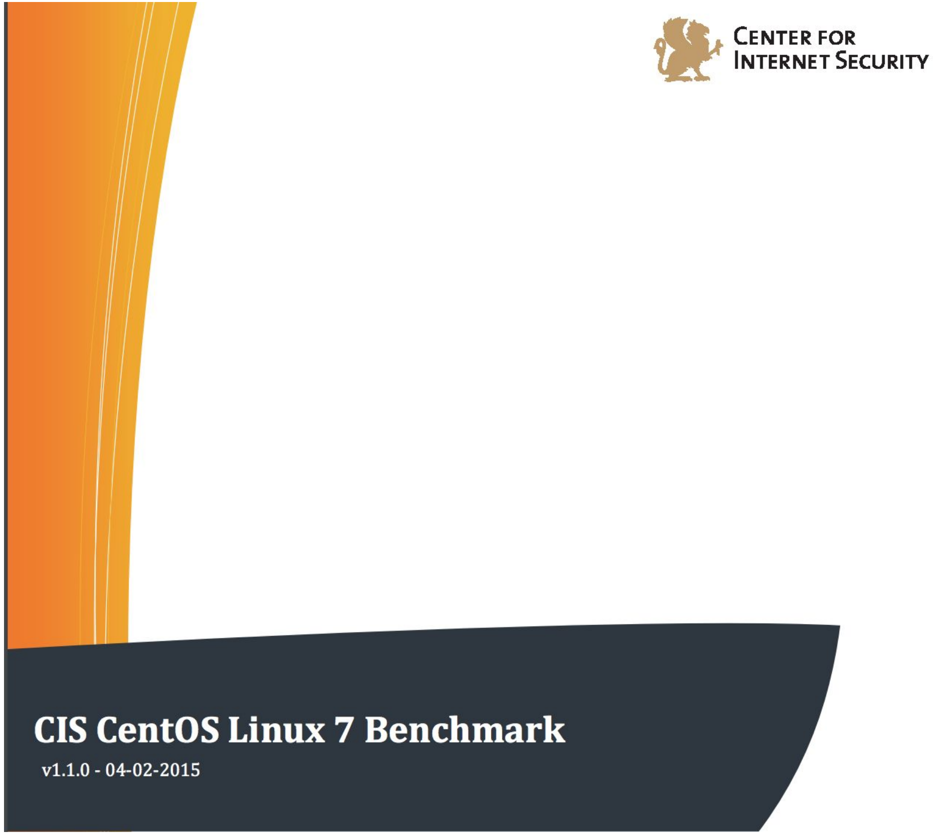
Agreed upon DSL means closer collaboration between policymakers and practitioners

Make time for the things that can’t be automated

Not everything can be automated, like physical safeguards

How does this look like in action?

Let’s pick a really basic example



CENTER FOR INTERNET SECURITY

CIS CentOS Linux 7 Benchmark

v1.1.0 - 04-02-2015

- https://benchmarks.cisecurity.org/tools2/linux/CIS_CentOS_Linux_7_Benchmark_v1.1.0.pdf

An example from CIS CentOS 7 Standards

1.2.3 Verify that gpgcheck is Globally Activated

- Profile Applicability: Level 1
- Description: The gpgcheck option, found in the main section of the /etc/yum.conf file determines if an RPM package's signature is always checked prior to its installation.
- Rationale: It is important to ensure that an RPM's package signature is always checked prior to installation to ensure that the software is obtained from a trusted source.
- Audit: Run the following command to verify that gpgcheck is set to 1 in all occurrences of the /etc/yum.conf file:

  ```
  $ grep gpgcheck /etc/yum.conf gpgcheck=1
  ```

- Remediation: Edit the /etc/yum.conf file and set the gpgcheck to 1 as follows: gpgcheck=1

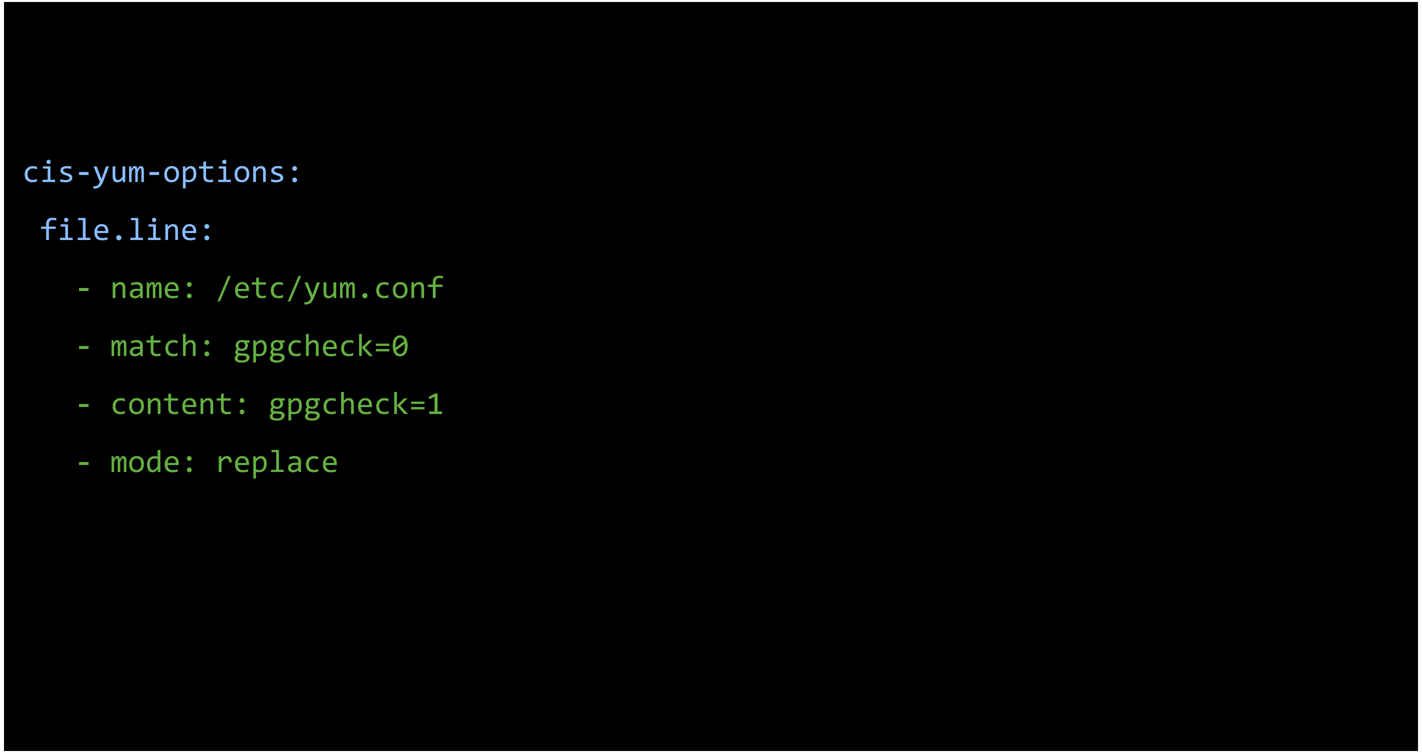
Reflected in Puppet

```
# 1.2.3 - Verify that gpgcheck is globaly Activated (Scored)

file { '/etc/yum.conf':
  ensure => file,
  owner  => 'root',
  group  => 'root',
  mode   => '0644',
}

file_line { '(1.2.3) /etc/yum.conf contains gpgcheck=1':
  ensure => present,
  path   => '/etc/yum.conf',
  line   => 'gpgcheck=1',
}
```

Reflected in Chef

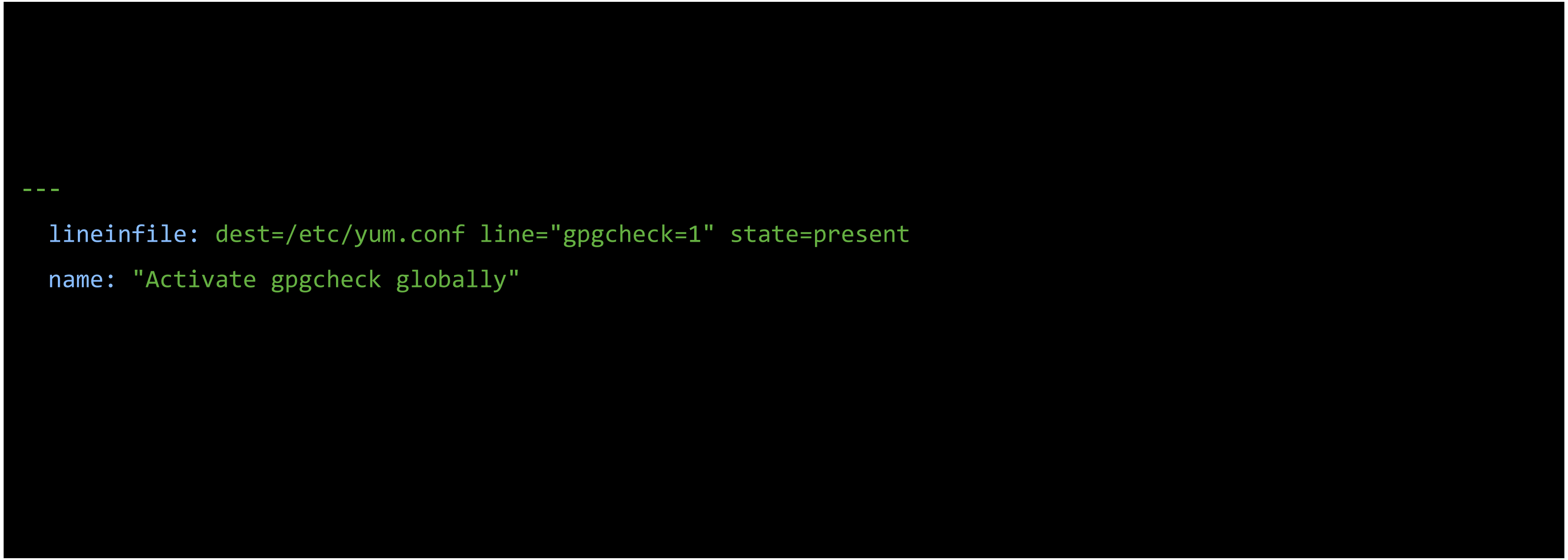
```
# CIS RHEL 1.2.3
replace_or_add 'Ensure GPG Check is enabled globally' do
 path '/etc/yum.conf'
 pattern 'gpgcheck.*'
 line 'gpgcheck=1'
end
```

Reflected in Salt



```
cis-yum-options:
 file.line:
   - name: /etc/yum.conf
   - match: gpgcheck=0
   - content: gpgcheck=1
   - mode: replace
```

Reflected in Ansible



```
---
  lineinfile: dest=/etc/yum.conf line="gpgcheck=1" state=present
  name: "Activate gpgcheck globally"
```

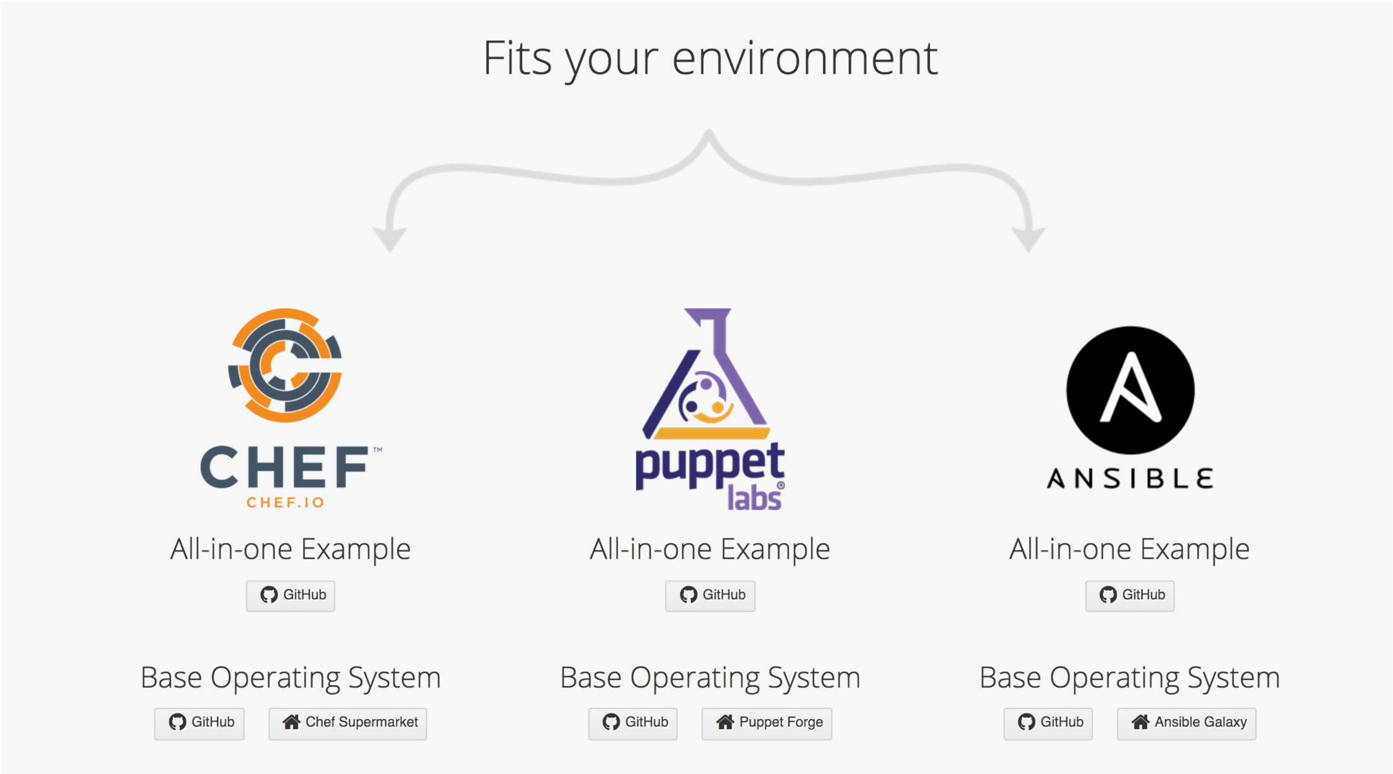
A few different design approaches available here...

Dedicated modules for compliance?
Use existing code and enforce standards?
Dry run modes when silo'd or change frozen?

Remember when we talked about sharing and reuse?

There’s a lot of prior art for this work

DEV-SEC.IO



Fits your environment

CHEF
CHEF.IO

All-in-one Example

GitHub

Base Operating System

GitHub | Chef Supermarket

puppet labs

All-in-one Example

GitHub

Base Operating System

GitHub | Puppet Forge

ANSIBLE

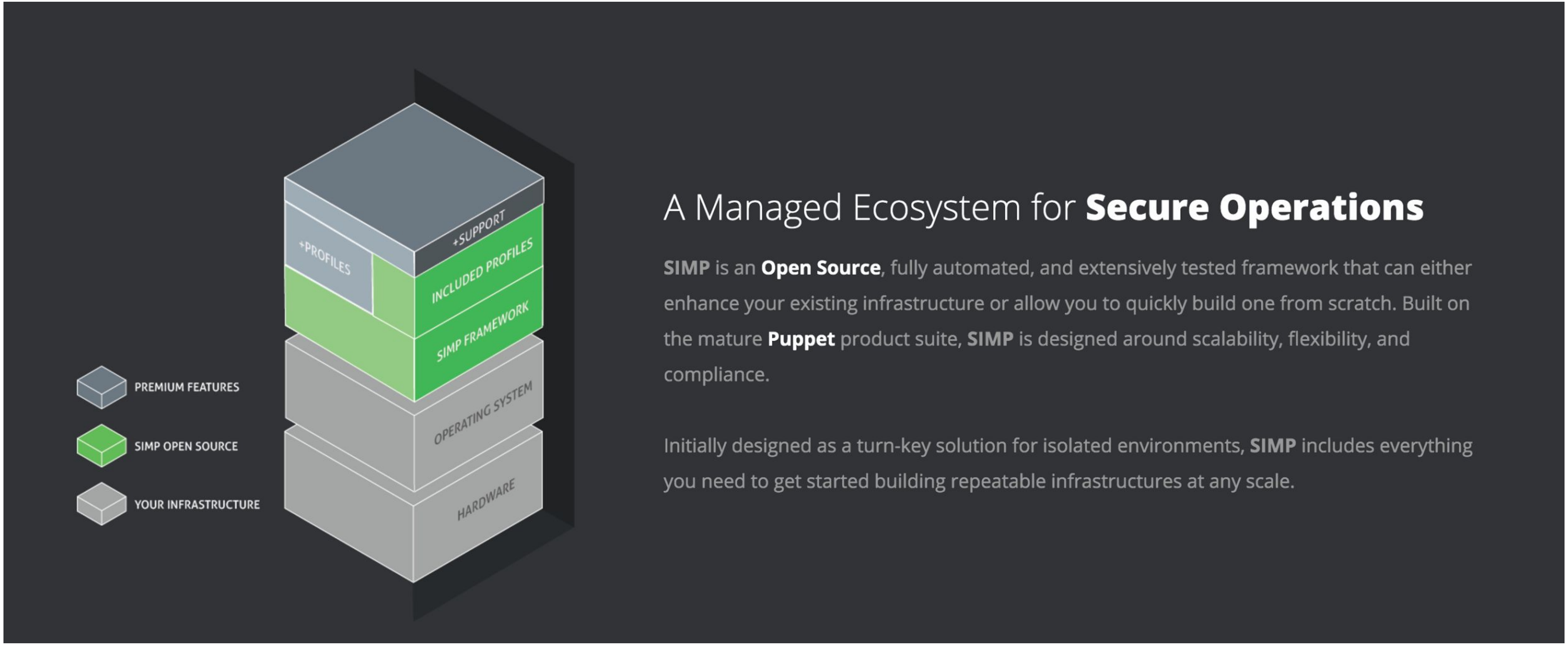
All-in-one Example

GitHub

Base Operating System

GitHub | Ansible Galaxy

SIMP - System Integrity Management Platform



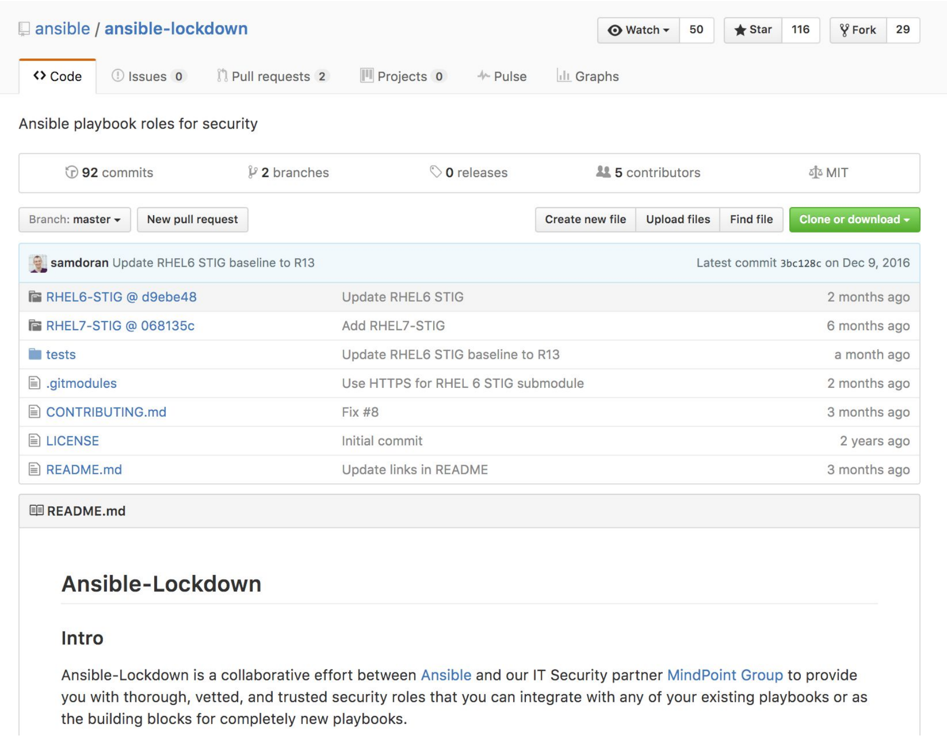
A Managed Ecosystem for **Secure Operations**

SIMP is an **Open Source**, fully automated, and extensively tested framework that can either enhance your existing infrastructure or allow you to quickly build one from scratch. Built on the mature **Puppet** product suite, **SIMP** is designed around scalability, flexibility, and compliance.

Initially designed as a turn-key solution for isolated environments, **SIMP** includes everything you need to get started building repeatable infrastructures at any scale.

- https://simp-project.com/

Ansible Lockdown



Ansible playbook roles for security

92 commits | 2 branches | 0 releases | 5 contributors | MIT

samdoran Update RHEL6 STIG baseline to R13 — Latest commit 3bc128c on Dec 9, 2016

RHEL6-STIG @ d9ebe48	Update RHEL6 STIG	2 months ago
RHEL7-STIG @ 068135c	Add RHEL7-STIG	6 months ago
tests	Update RHEL6 STIG baseline to R13	a month ago
.gitmodules	Use HTTPS for RHEL 6 STIG submodule	2 months ago
CONTRIBUTING.md	Fix #8	3 months ago
LICENSE	Initial commit	2 years ago
README.md	Update links in README	3 months ago

README.md

Ansible-Lockdown

Intro

Ansible-Lockdown is a collaborative effort between Ansible and our IT Security partner MindPoint Group to provide you with thorough, vetted, and trusted security roles that you can integrate with any of your existing playbooks or as the building blocks for completely new playbooks.

- https://github.com/ansible/ansible-lockdown

Check the community hubs

Puppet Forge, Chef Supermarket, Ansible Galaxy, Github

However there are two parts to IT compliance

1. Enforcement
2. Reporting

Config management tools can be used for both

They’re generally better at the enforcing bit

So let's talk about scanning and reporting

And here is some bad news...

Bad news: Not a lot of the tools out there for scanning are open-source

eg. Nessus, QualysGuard, Nexpose

That is not to say they’re not good...

But we are at FOSDEM, so let's talk about the OSS options!

Also bad news: there’s normally an approval process or tool to get something signed off as a scanner for a particular standard

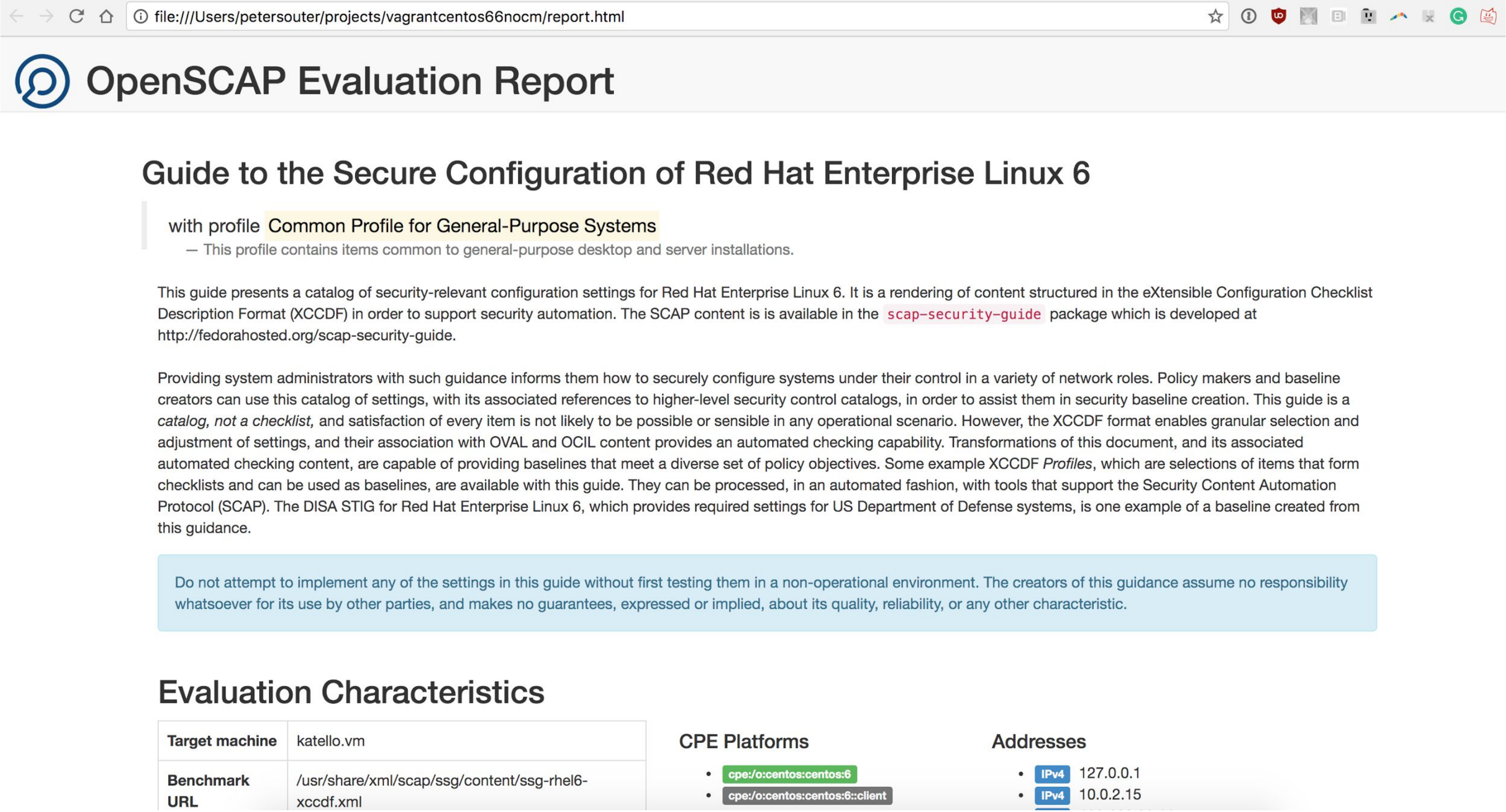
eg. PCI, there are ASV (Approved Scanning Vendors)

OpenSCAP

- SCAP is U.S. standard maintained by National Institute of Standards and Technology (NIST)
- The OpenSCAP project is a collection of open source tools for implementing and enforcing the standard
- Lots of existing profiles for various OS’s and compliance standards (PCI DSS, FISMA)
- Existing integrations with various tools and projects

oscap

```
$ yum install openscap-utils scap-security-guide -y
$ oscap xccdf eval --profile common --report \
/vagrant/report.html --results /vagrant/results.xml \
--cpe/usr/share/xml/scap/ssg/content/ssg-rhel6-cpe-dictionary.xml \
/usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml
```



file:///Users/petersouter/projects/vagrantcentos66nocm/report.html

OpenSCAP Evaluation Report

Guide to the Secure Configuration of Red Hat Enterprise Linux 6

> with profile Common Profile for General-Purpose Systems
> — This profile contains items common to general-purpose desktop and server installations.

This guide presents a catalog of security-relevant configuration settings for Red Hat Enterprise Linux 6. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is is available in the `scap-security-guide` package which is developed at http://fedorahosted.org/scap-security-guide.

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog, not a checklist,* and satisfaction of every item is not likely to be possible or sensible in any operational scenario. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG for Red Hat Enterprise Linux 6, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

Evaluation Characteristics

Target machine	katello.vm
Benchmark URL	/usr/share/xml/scap/ssg/content/ssg-rhel6-xccdf.xml

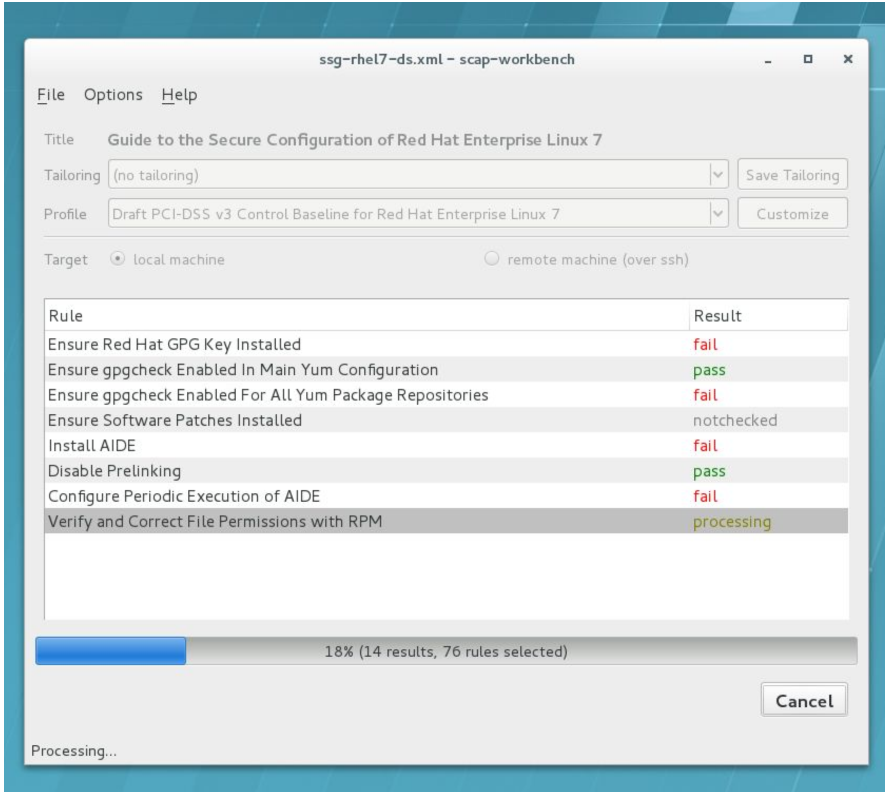
CPE Platforms

- cpe:/o:centos:centos:6
- cpe:/o:centos:centos:6::client

Addresses

- IPv4 127.0.0.1
- IPv4 10.0.2.15

SCAP Workbench



ssg-rhel7-ds.xml – scap-workbench

Title Guide to the Secure Configuration of Red Hat Enterprise Linux 7

Tailoring (no tailoring)

Profile Draft PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7

Target ● local machine ○ remote machine (over ssh)

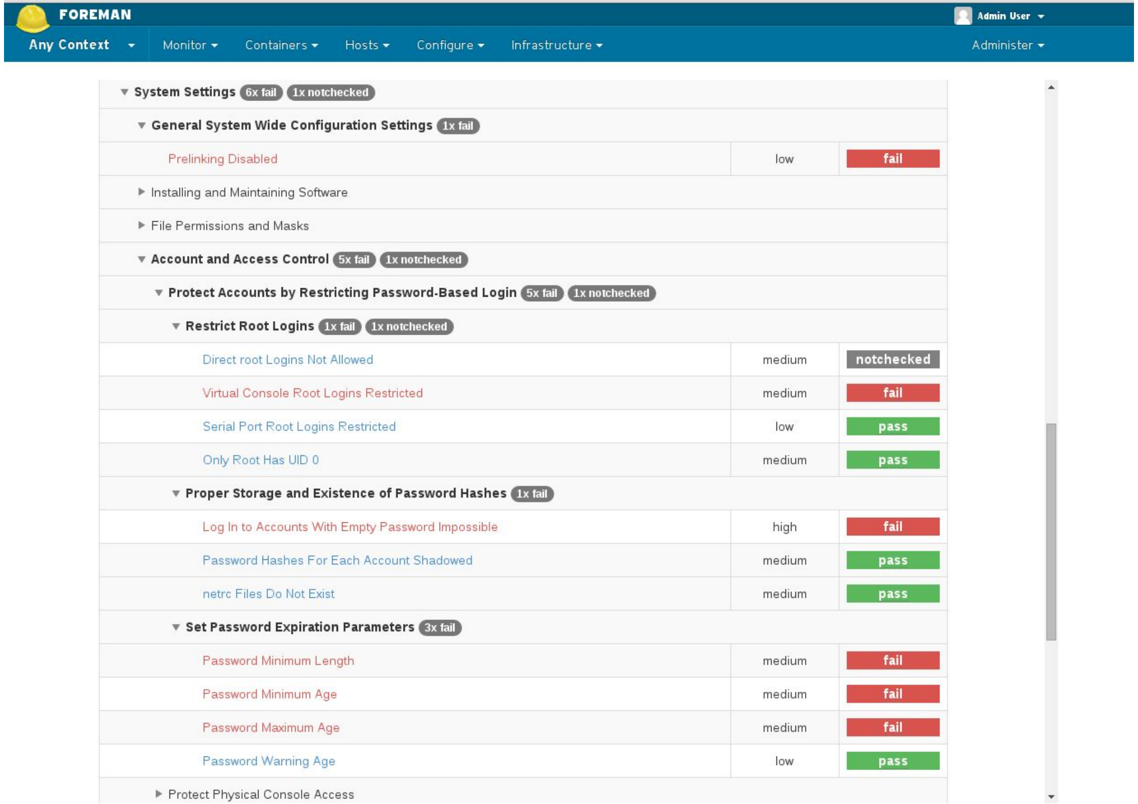
Rule	Result
Ensure Red Hat GPG Key Installed	fail
Ensure gpgcheck Enabled In Main Yum Configuration	pass
Ensure gpgcheck Enabled For All Yum Package Repositories	fail
Ensure Software Patches Installed	notchecked
Install AIDE	fail
Disable Prelinking	pass
Configure Periodic Execution of AIDE	fail
Verify and Correct File Permissions with RPM	processing

18% (14 results, 76 rules selected)

Processing...

- https://www.open-scap.org/resources/documentation/make-a-rhel7-server-compliant-with-pci-dss/

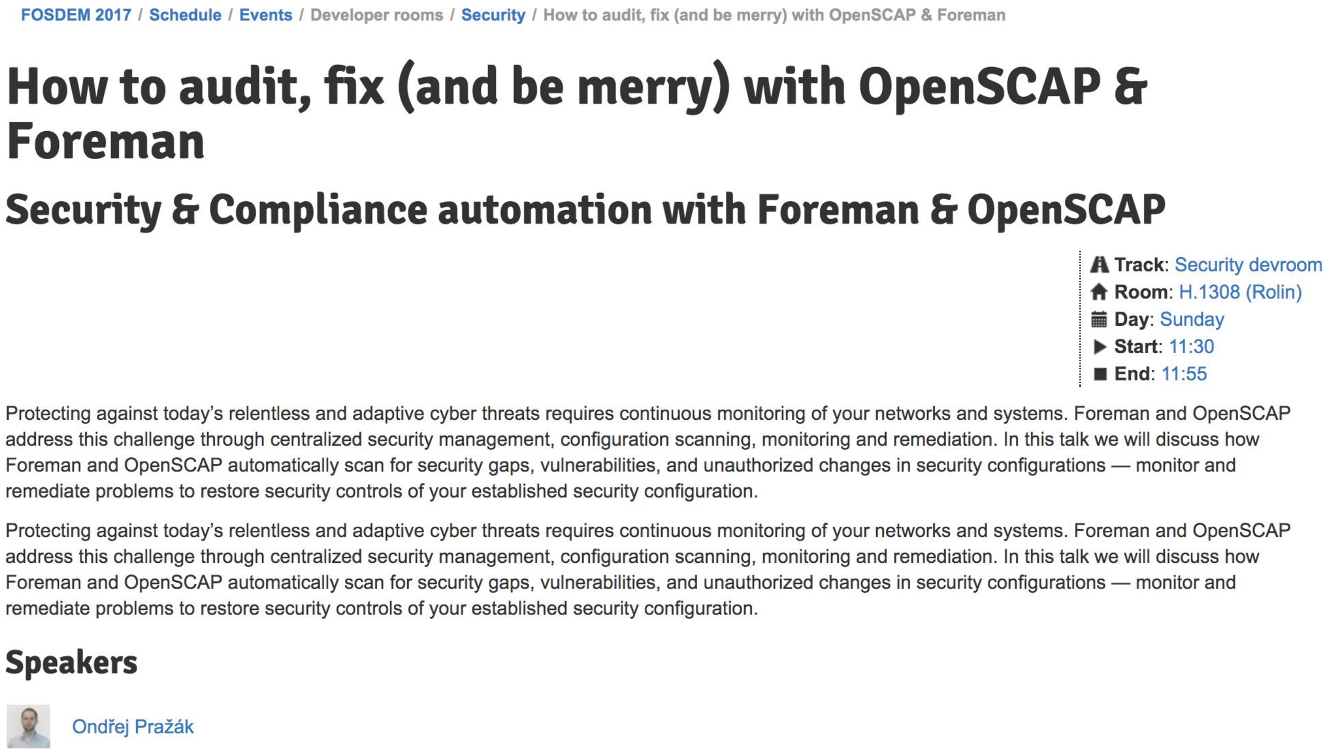
Foreman/Satellite Integration



▼ System Settings 6x fail 1x notchecked		
▼ General System Wide Configuration Settings 1x fail		
Prelinking Disabled	low	fail
▶ Installing and Maintaining Software		
▶ File Permissions and Masks		
▼ Account and Access Control 5x fail 1x notchecked		
▼ Protect Accounts by Restricting Password-Based Login 5x fail 1x notchecked		
▼ Restrict Root Logins 1x fail 1x notchecked		
Direct root Logins Not Allowed	medium	notchecked
Virtual Console Root Logins Restricted	medium	fail
Serial Port Root Logins Restricted	low	pass
Only Root Has UID 0	medium	pass
▼ Proper Storage and Existence of Password Hashes 1x fail		
Log In to Accounts With Empty Password Impossible	high	fail
Password Hashes For Each Account Shadowed	medium	pass
netrc Files Do Not Exist	medium	pass
▼ Set Password Expiration Parameters 3x fail		
Password Minimum Length	medium	fail
Password Minimum Age	medium	fail
Password Maximum Age	medium	fail
Password Warning Age	low	pass
▶ Protect Physical Console Access		

- https://www.theforeman.org/plugins/foreman_openscap/0.6/

There’s a talk on this tomorrow



FOSDEM 2017 / Schedule / Events / Developer rooms / Security / How to audit, fix (and be merry) with OpenSCAP & Foreman

How to audit, fix (and be merry) with OpenSCAP & Foreman

Security & Compliance automation with Foreman & OpenSCAP

- **Track**: Security devroom
- **Room**: H.1308 (Rolin)
- **Day**: Sunday
- ▶ **Start**: 11:30
- ■ **End**: 11:55

Protecting against today’s relentless and adaptive cyber threats requires continuous monitoring of your networks and systems. Foreman and OpenSCAP address this challenge through centralized security management, configuration scanning, monitoring and remediation. In this talk we will discuss how Foreman and OpenSCAP automatically scan for security gaps, vulnerabilities, and unauthorized changes in security configurations — monitor and remediate problems to restore security controls of your established security configuration.

Protecting against today’s relentless and adaptive cyber threats requires continuous monitoring of your networks and systems. Foreman and OpenSCAP address this challenge through centralized security management, configuration scanning, monitoring and remediation. In this talk we will discuss how Foreman and OpenSCAP automatically scan for security gaps, vulnerabilities, and unauthorized changes in security configurations — monitor and remediate problems to restore security controls of your established security configuration.

Speakers

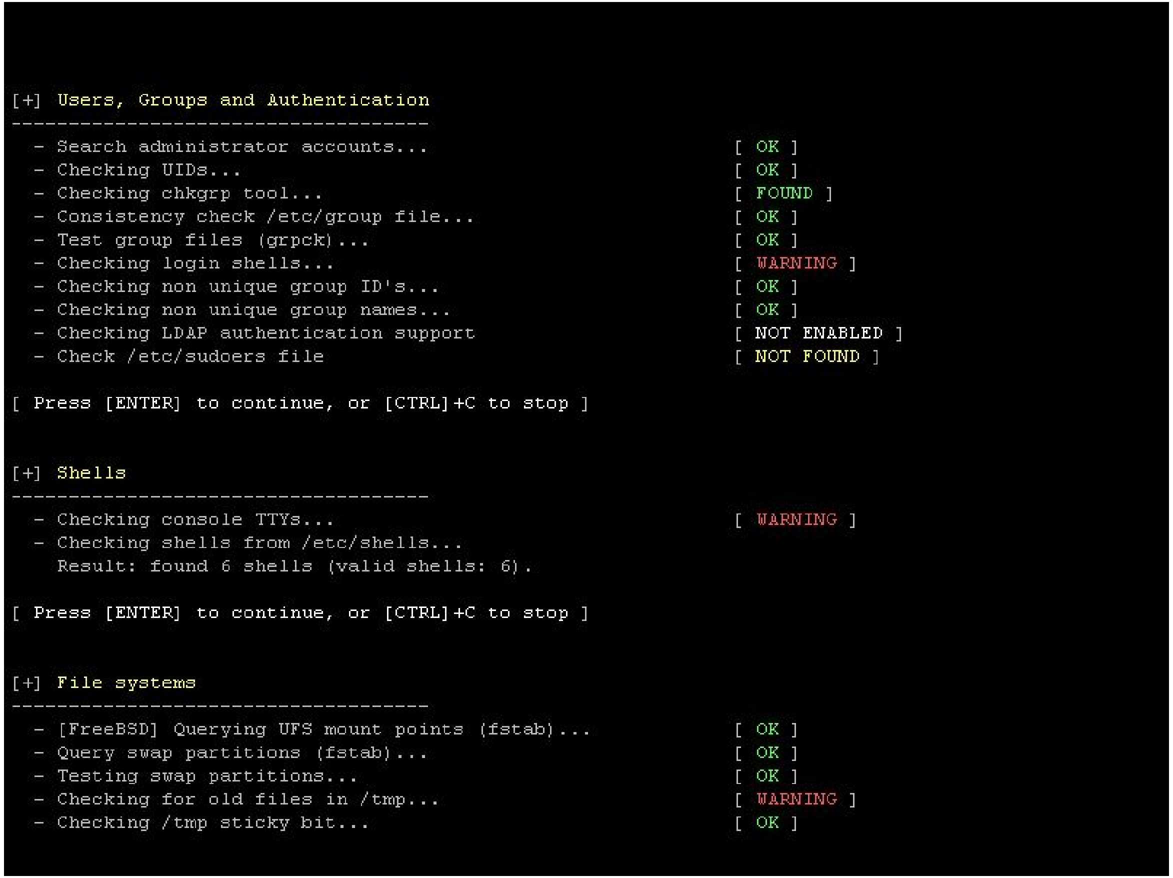
Ondřej Pražák

- https://fosdem.org/2017/schedule/event/openscap_foreman/

Lynis

CISOFY
AUDITING-HARDENING-COMPLIANCE

- Basic hardening standards scanner
- Easy to install
- Bad news: PCI and other standards are plugins and are commercial only



```
[+] Users, Groups and Authentication
------------------------------------
  - Search administrator accounts...                            [ OK ]
  - Checking UIDs...                                            [ OK ]
  - Checking chkgrp tool...                                     [ FOUND ]
  - Consistency check /etc/group file...                        [ OK ]
  - Test group files (grpck)...                                 [ OK ]
  - Checking login shells...                                    [ WARNING ]
  - Checking non unique group ID's...                           [ OK ]
  - Checking non unique group names...                          [ OK ]
  - Checking LDAP authentication support                        [ NOT ENABLED ]
  - Check /etc/sudoers file                                     [ NOT FOUND ]

[ Press [ENTER] to continue, or [CTRL]+C to stop ]


[+] Shells
------------------------------------
  - Checking console TTYs...                                    [ WARNING ]
  - Checking shells from /etc/shells...
    Result: found 6 shells (valid shells: 6).

[ Press [ENTER] to continue, or [CTRL]+C to stop ]


[+] File systems
------------------------------------
  - [FreeBSD] Querying UFS mount points (fstab)...              [ OK ]
  - Query swap partitions (fstab)...                            [ OK ]
  - Testing swap partitions...                                  [ OK ]
  - Checking for old files in /tmp...                           [ WARNING ]
  - Checking /tmp sticky bit...                                 [ OK ]
```

Packer

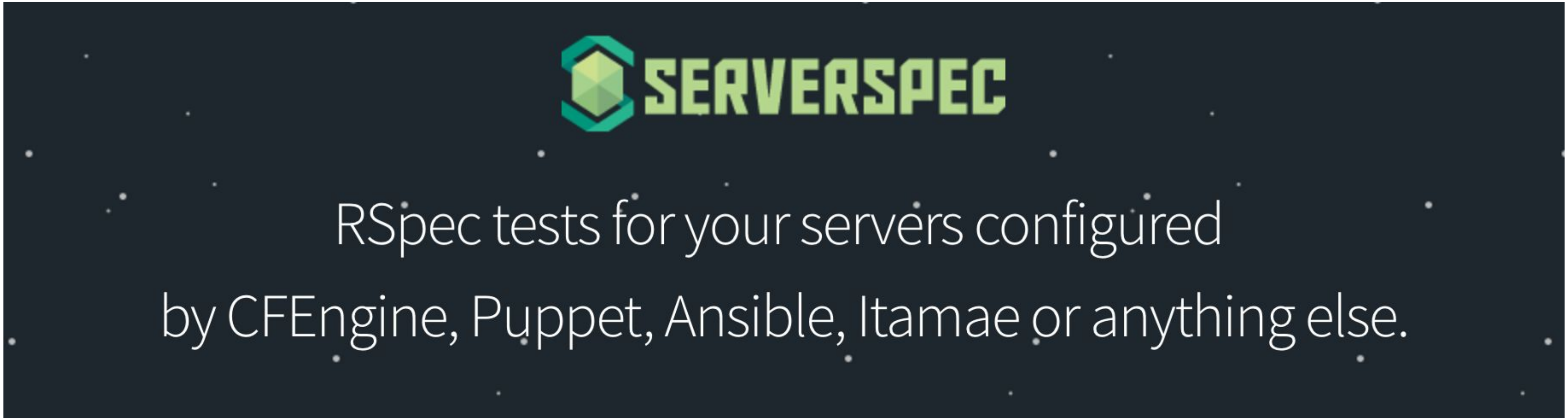
Bake your compliance steps into your base images

- Hashicorp tool
- Image management
- Provisioners for config management tools and shell scripts
- Some compliance steps can be hard to change on a running system
- Werner Buck had a great talk about compliance standards with Packer: http://wernerb.github.io/hashiconf-hardening/

System Testing DSL’s

Domain Specific Languages to test system correctness

Serverspec

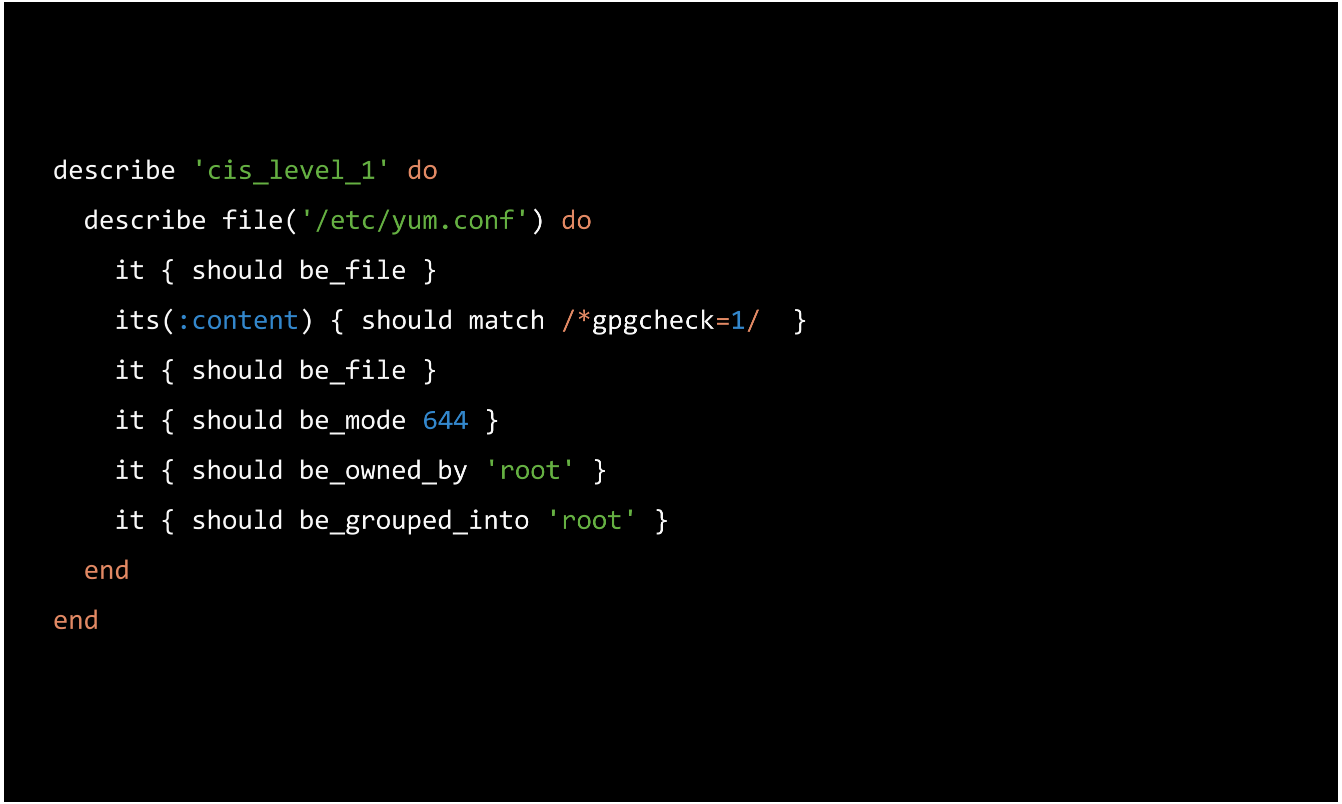


SERVERSPEC

RSpec tests for your servers configured

by CFEngine, Puppet, Ansible, Itamae or anything else.

Serverspec



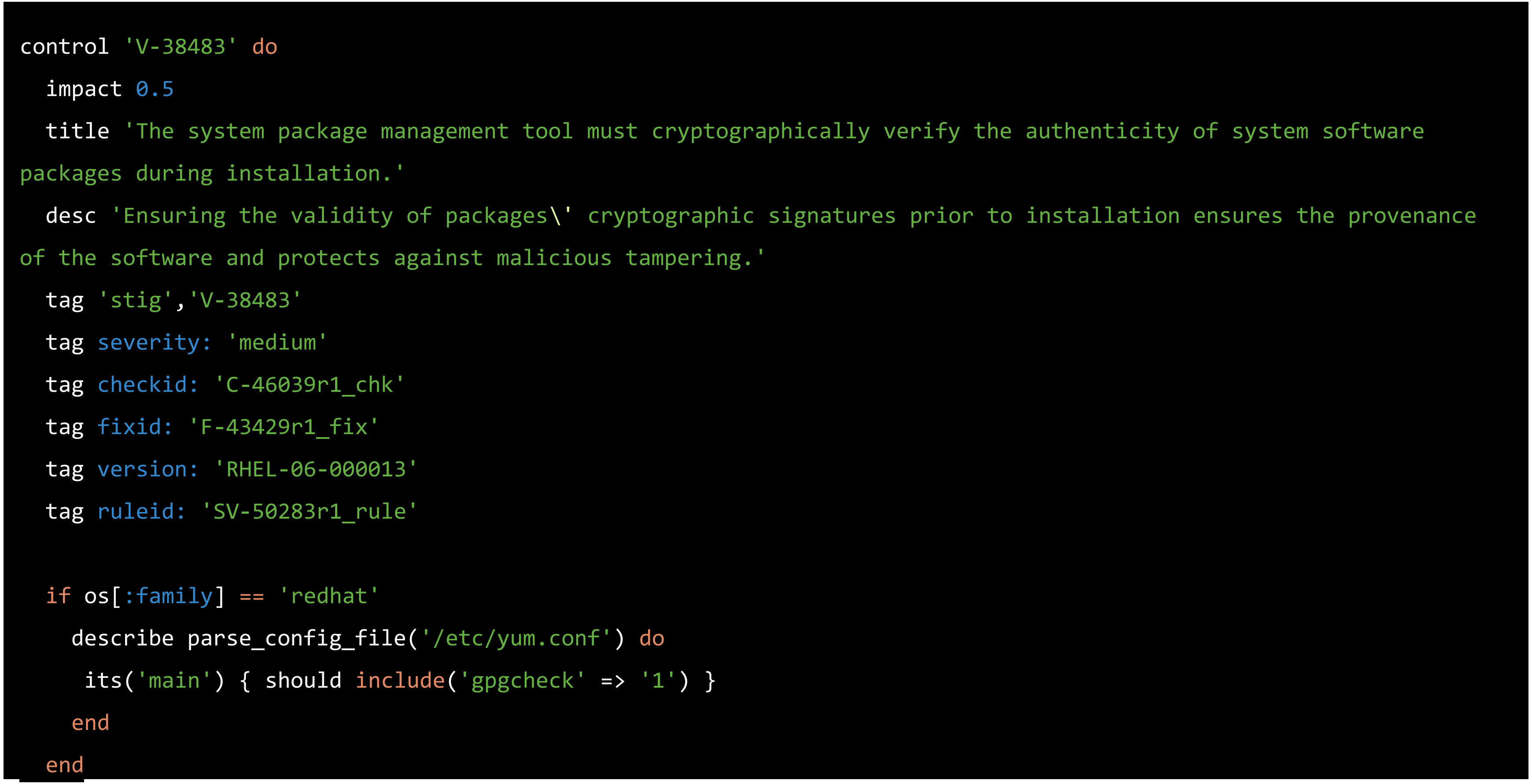
```
describe 'cis_level_1' do
  describe file('/etc/yum.conf') do
    it { should be_file }
    its(:content) { should match /*gpgcheck=1/  }
    it { should be_file }
    it { should be_mode 644 }
    it { should be_owned_by 'root' }
    it { should be_grouped_into 'root' }
  end
end
```

A number of similar and inspired projects

- goss - https://github.com/aelsabbahy/goss - Inspired by serverspec, but written in golang
- infrataster - http://infrataster.net/ - Has specific methods and keywords for http, mysql etc
- testinfra - https://github.com/philpep/testinfra - Python version of serverspec
- gauntlt - http://gauntlt.org/ - BDD wrappers around common security tools (nmap, sslyze etc)
- bddsecurity - http://bbdsecurity.com - Similar BDD focussed security tool

InSpec

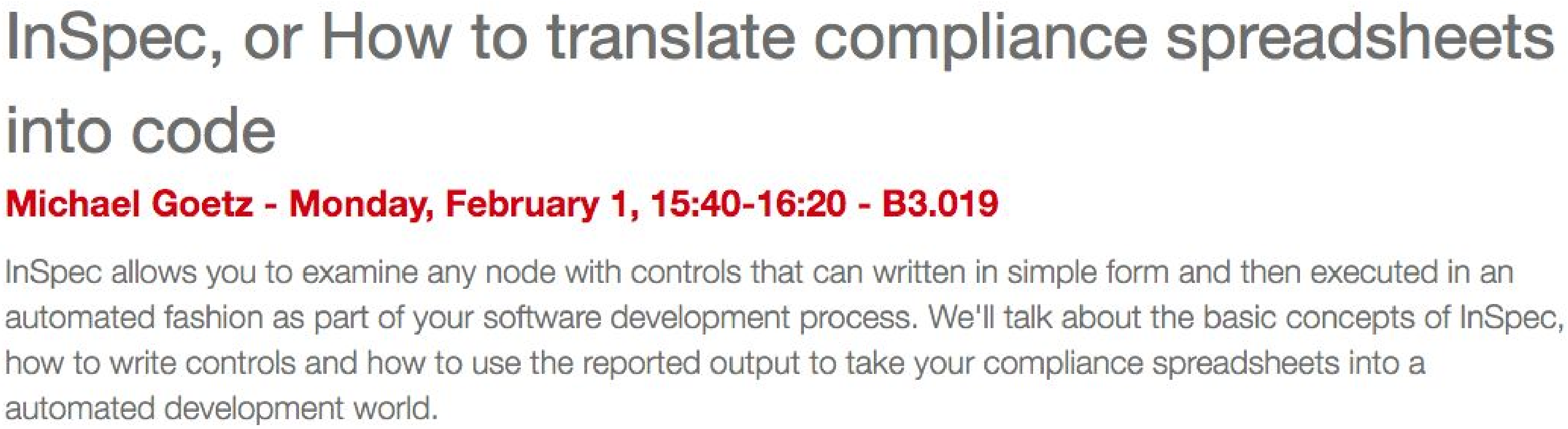
- "InSpec is an open-source testing framework for infrastructure with a human-readable language for specifying compliance, security and other policy requirements"
- Chef's compliance product
- Started as a fork of serverspec



```
control 'V-38483' do
  impact 0.5
  title 'The system package management tool must cryptographically verify the authenticity of system software
packages during installation.'
  desc 'Ensuring the validity of packages\' cryptographic signatures prior to installation ensures the provenance
of the software and protects against malicious tampering.'
  tag 'stig','V-38483'
  tag severity: 'medium'
  tag checkid: 'C-46039r1_chk'
  tag fixid: 'F-43429r1_fix'
  tag version: 'RHEL-06-000013'
  tag ruleid: 'SV-50283r1_rule'

  if os[:family] == 'redhat'
    describe parse_config_file('/etc/yum.conf') do
     its('main') { should include('gpgcheck' => '1') }
    end
  end
```

- https://supermarket.chef.io/tools?type=compliance_profile
- https://github.com/inspec-stigs/inspec-stigs/

Talk from Config Management Camp 2016



InSpec, or How to translate compliance spreadsheets into code

Michael Goetz - Monday, February 1, 15:40-16:20 - B3.019

InSpec allows you to examine any node with controls that can written in simple form and then executed in an automated fashion as part of your software development process. We'll talk about the basic concepts of InSpec, how to write controls and how to use the reported output to take your compliance spreadsheets into a automated development world.

- http://cfgmgmtcamp.eu/gent-2016/schedule/chef/goetz.html

Summary

What have we learnt?

Compliance is enforcement of standards

It’s not security, it’s standards for scaling security

Compliance responsibility can be tricky

Try to bring into teams if possible, move security left!

Config management tools are a great fit for compliance

They fit the model of enforcing rules in a defined way

Regardless of the config management tool you use, there’s pre-existing work

“Stand on the shoulders of giants”

Enforcement is just one part of the puzzle

Reporting is the other half

Unfortunately, not much OSS for compliance scanning

OpenSCAP, System DSL’s, InSpec and Lynis

Want to know more?

- **A Year in Open Source Automated Compliance With Puppet – Trevor Vaughan at PuppetConf 2016**
  https://www.youtube.com/watch?v=a270uDh8muE
- **Compliance Is Not Security. Compliance Scales Security.**
  https://medium.com/compliance-at-velocity/compliance-is-not-security-compliance-scales-security-50846e7a47c2#.k63bpravl
- **Prove it! The Last Mile for DevOps in Regulated Organizations - DOES15 - Bill Shinn**
  https://www.youtube.com/watch?v=gg8gGisl4zM
- **The Technical Practises of Integrating Information Security, Change Management and Compliance**
  Kim, Gene. 2016. The Devops Handbook: How to Create World-Class Agility, Reliability, and Security in Technology Organizations. Portland: IT Revolution Press

Q&A