Compliance… and You!

Using Red Hat Satellite to monitor and deliver compliance solutions.

Presented By: Alan Patrick & Shane Strong

Who Are We?

Alan Patrick
RHCSA, RHCE

- AF Group Infrastructure Engineer
- Former training manager for Liquid Web
- Designed and oversaw Red Hat-approved in-house training program for formal certification

Huge D&D nerd.

Shane Strone
RHCSA

- AF Group Lead Infrastructure Engineer
- Drove Linux expansion from 12 servers to 450+
- Oversaw transition of physical servers to virtual instances

Recovering web developer.

AF Group
Individual focus. Collective strength.

Overview

- What Compliance Is
- What Compliance Isn’t
- Using Red Hat Satellite’s Compliance Tools
- Using Satellite to Enable Resolutions
- Putting Minds at Ease

Compliance Defined

compliance noun

Save Word

com·pli·ance | \ kəm-ˈplī-ən(t)s \

Definition of *compliance*

1 **a** : the act or process of complying to a desire, demand, proposal, or regimen or to coercion

// Patient *compliance* in completing the treatment regimens was excellent.
— Georgia A. Chrousos

b : conformity in fulfilling official requirements

// His actions were in *compliance* with state law.

Compliance Perceived

OpenSCAP Defined

OpenSCAP = Security Content Automation Protocol

US standard maintained by National Institute of Standards and Technology (NIST). The OpenSCAP project is a collection of *open source* tools for implementing and enforcing this standard [..].

^^ this will be important in a moment

OpenSCAP Defined, additional information

DISA-STIG.

- Defense Information Systems Agency Security Technical Implementation Guide
- Standards for Department of Defense

HIPAA.

- Health Insurance Portability and Accountability
- Incredibly complex

Others.

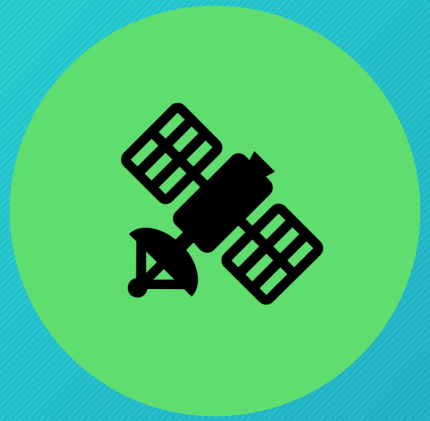
- They’re out there, but we’re focused on DISA-STIG

remember: these are catalogs, not checklists, and require ample review before implementation

What This Isn't

All The Things

Compliance + Red Hat Satellite

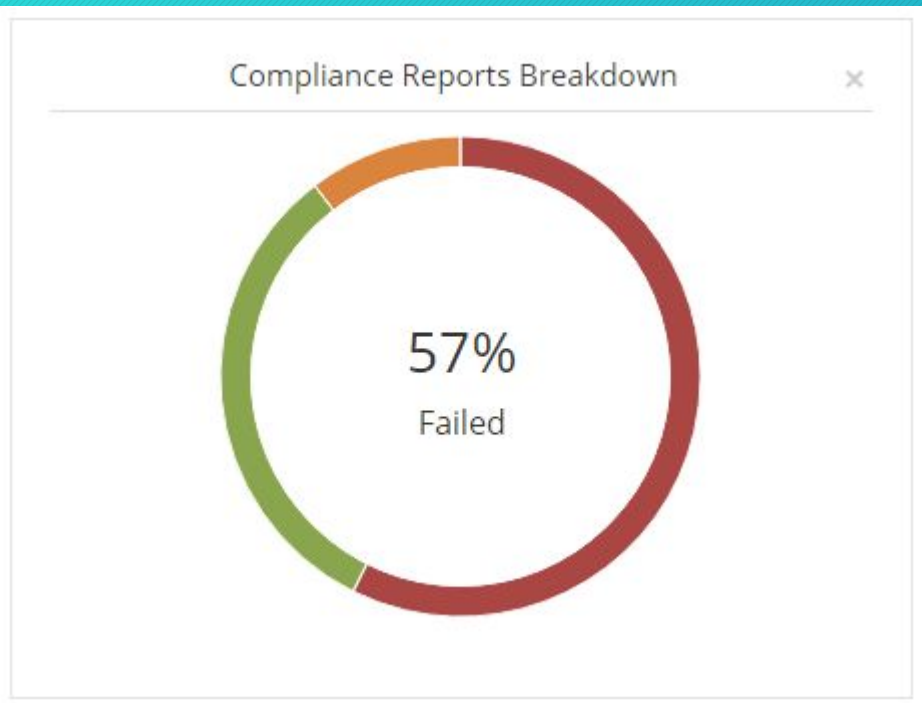


STEP 1:
CONFIGURE SATELLITE

STEP 2:
CONFIGURE OPENSCAP

STEP 3:
PROFIT!

Red Hat Satellite's OpenSCAP Report



Latest Compliance Reports

Host	Policy	P	F	O
domain.com	RHEL 7 - Standard Syste...	77	139	26
database.domain.com	CentOS 7 - Standard Sys...	14	36	1
monitor.domain.com	CentOS 7 - Standard Sys...	13	37	1
webserver-pub.domain.com	CentOS 7 - Standard Sys...	13	37	1
webserver-dev.domain.com	RHEL 7 - Standard Syste...	74	142	26
bitcoin.domain.com	CentOS 7 - Standard Sys...	16	34	1
dolen.domain.com	RHEL 6 - Standard Syste...	77	89	15
topsecret.domain.com	RHEL 7 - Standard Syste...	76	140	26
bottomsecret.domain.com	RHEL 7 - Standard Syste...	71	145	26

Braaaaaaaaaaaiiiiinnnnssss….

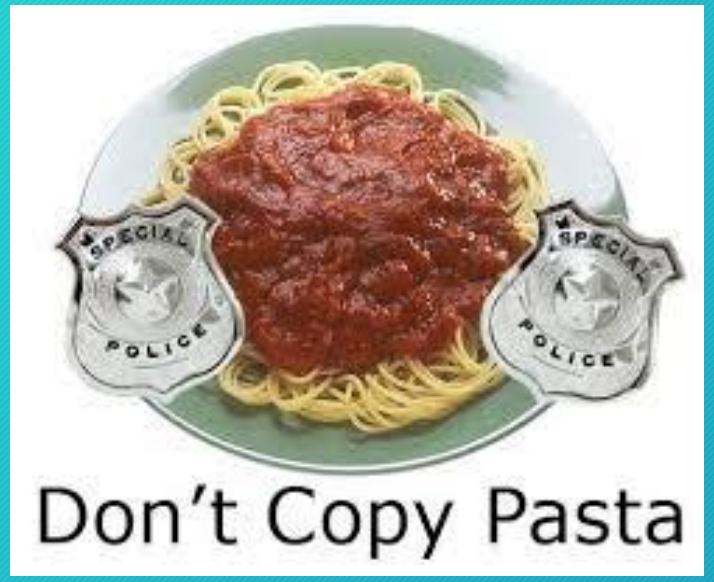
Severity	Message	Resource	Result
Medium	Disable KDump Kernel Crash Analyzer (kdump)	xccdf_org.ssgproject.content_...	fail
Medium	Verify Group Who Owns /etc/cron.allow file	xccdf_org.ssgproject.content_...	pass
Medium	Verify User Who Owns /etc/cron.allow file	xccdf_org.ssgproject.content_...	pass
High	Uninstall vsftpd Package	xccdf_org.ssgproject.content_...	pass
Medium	Prevent Unrestricted Mail Relaying	xccdf_org.ssgproject.content_...	notchecked
Medium	Mount Remote Filesystems with Kerberos Security	xccdf_org.ssgproject.content_...	pass
High	Install McAfee Virus Scanning Software	xccdf_org.ssgproject.content_...	fail

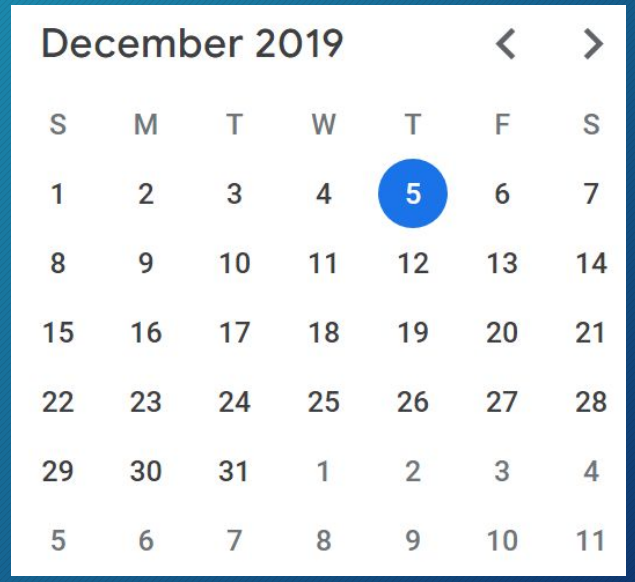
Get the Facts

- Data, breadcrumbs, and solutions

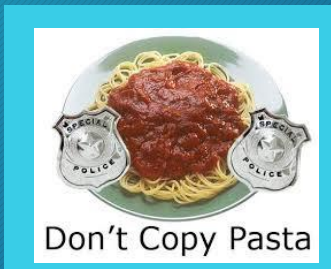
Adjustments and Ownership

Compliance, like emissions, establish only a baseline





Simple Suggestions for Resolution



Updating Software 2x fail 1x notchecked		
Ensure yum Removes Previous Package Versions	low	fail
Ensure gpgcheck Enabled In Main yum Configuration	high	pass
Ensure gpgcheck Enabled for Local Packages	high	fail
Ensure Software Patches Installed	high	notchecked

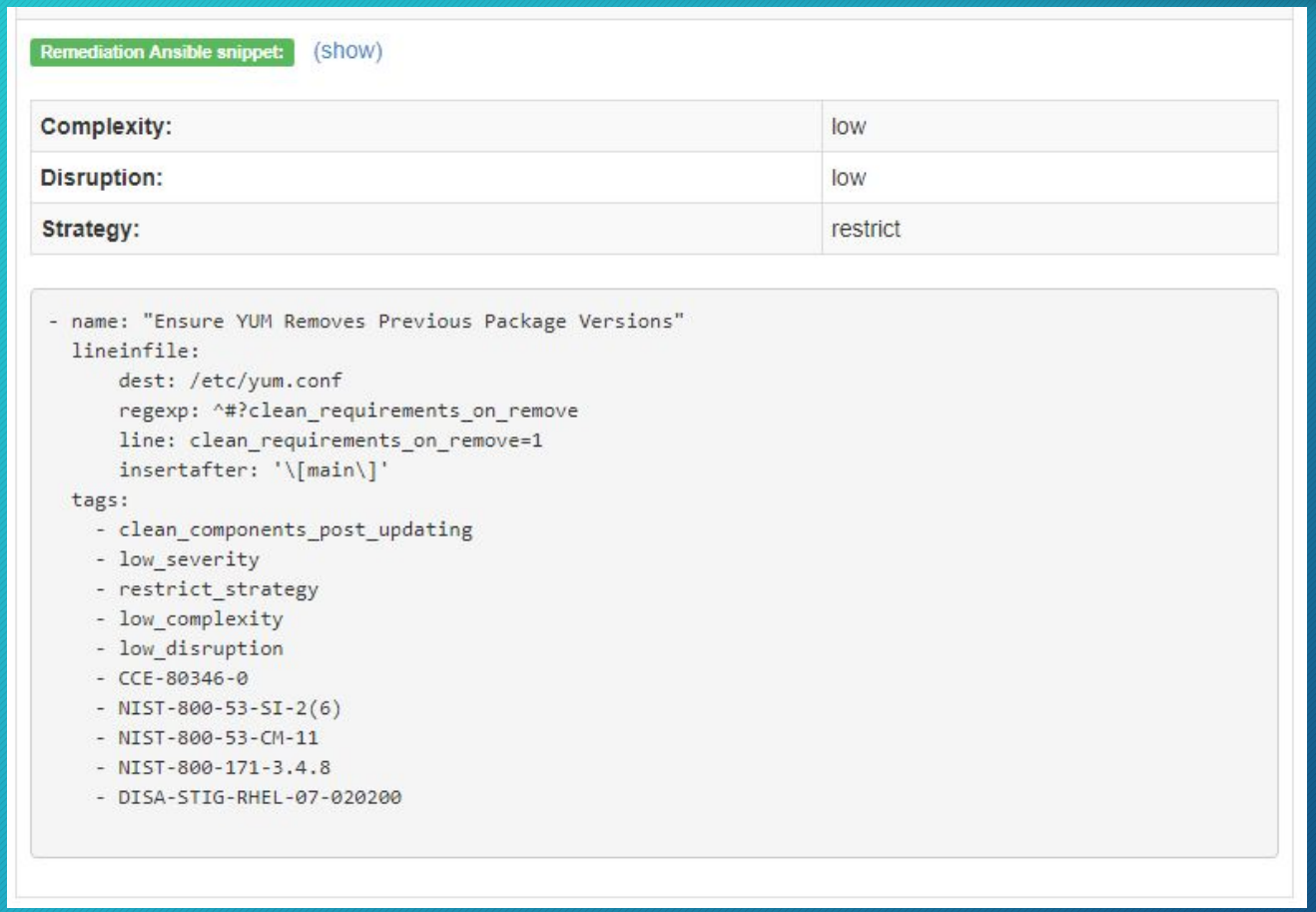
Simple Suggestions for Resolution

Ensure yum Removes Previous Package Versions

Rule ID	xccdf_org.ssgproject.content_rule_clean_components_post_updating
Result	fail
Time	2019-11-30T03:43:07
Severity	low
Identifiers and References	Identifiers: CCE-80346-0 References: RHEL-07-020200, SV-86611r2_rule, 18, 20, 4, APO12.01, APO12.02, APO12.03, APO12.04, BAI03.10, DSS05.01, DSS05.02, 3.4.8, CCI-002617, 4.2.3, 4.2.3.12, 4.2.3.7, 4.2.3.9, A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3, SI-2(6), CM-11, ID.RA-1, PR.IP-12, SRG-OS-000437-GPOS-00194
Description	`yum` should be configured to remove previous software components after new versions have been installed. To configure `yum` to remove the previous software components after updating, set the `clean_requirements_on_remove` to `1` in `/etc/yum.conf`.
Rationale	Previous versions of software components that are not removed from the information system after updates have been installed may be exploited by some adversaries.

Simple Suggestions for Resolution

Simple Suggestions for Resolution



Remediation Ansible snippet: (show)

Complexity:	low
Disruption:	low
Strategy:	restrict

```
- name: "Ensure YUM Removes Previous Package Versions"
  lineinfile:
      dest: /etc/yum.conf
      regexp: ^#?clean_requirements_on_remove
      line: clean_requirements_on_remove=1
      insertafter: '\[main\]'
  tags:
    - clean_components_post_updating
    - low_severity
    - restrict_strategy
    - low_complexity
    - low_disruption
    - CCE-80346-0
    - NIST-800-53-SI-2(6)
    - NIST-800-53-CM-11
    - NIST-800-171-3.4.8
    - DISA-STIG-RHEL-07-020200
```

Resolutions, Compared

OVAL details

check value of clean_requirements_on_remove in /etc/yum.conf **failed** because these items were missing:

Object **oval:ssg-object_yum_clean_components_post_updating:obj:1** of type **textfilecontent54_object**

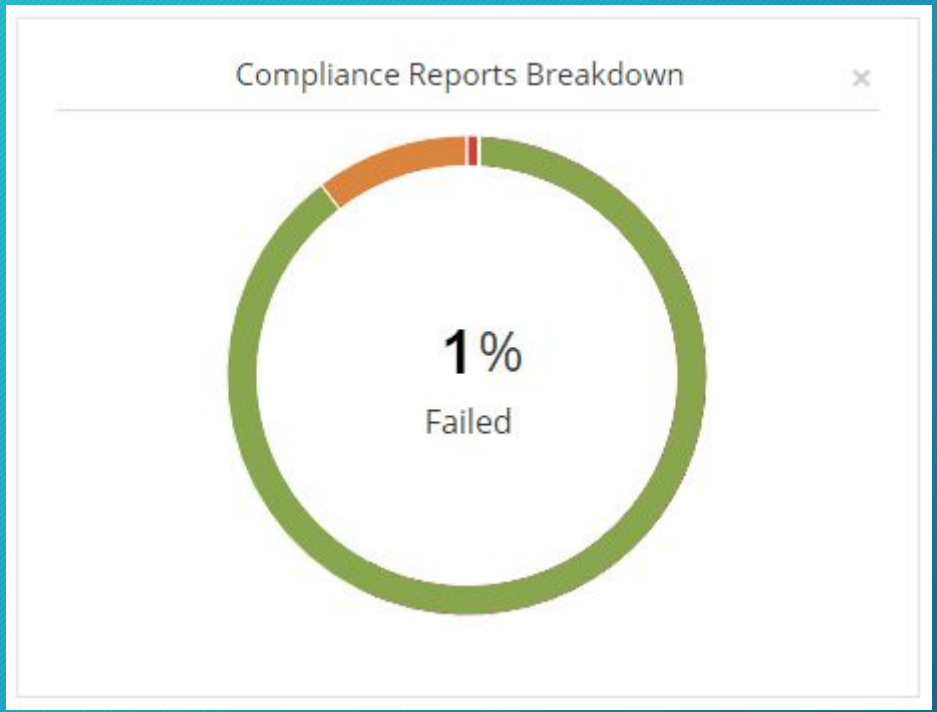
Filepath	Pattern	Instance
/etc/yum.conf	^\s*clean_requirements_on_remove\s*=\s*(1|True|yes)\s*$	1

Remediation Ansible snippet: (show)

Complexity:	low
Disruption:	low
Strategy:	restrict

```
- name: "Ensure YUM Removes Previous Package Versions"
  lineinfile:
      dest: /etc/yum.conf
      regexp: ^#?clean_requirements_on_remove
      line: clean_requirements_on_remove=1
      insertafter: '\[main\]'
  tags:
    - clean_components_post_updating
    - low_severity
    - restrict_strategy
    - low_complexity
    - low_disruption
    - CCE-80346-0
    - NIST-800-53-SI-2(6)
    - NIST-800-53-CM-11
    - NIST-800-171-3.4.8
    - DISA-STIG-RHEL-07-020200
```

End Result?



References

- https://www.open-scap.org/
- https://access.redhat.com/solutions/3641661
- https://www.open-scap.org/resources/documentation/customizing-scap-security-guide-for-your-use-case/
- https://access.redhat.com/articles/3358971
- https://icon-library.net/icon/zombie-icon-8.html