RED HAT SUMMIT

BOSTON, MA
JUNE 23-26, 2015

Security compliance automation with Red Hat Satellite

Matt Micene
Solution Architect, DLT Solutions

@cleverbeard

@nzwulfin

Created with http://wordle.net

Compliance is a major problem

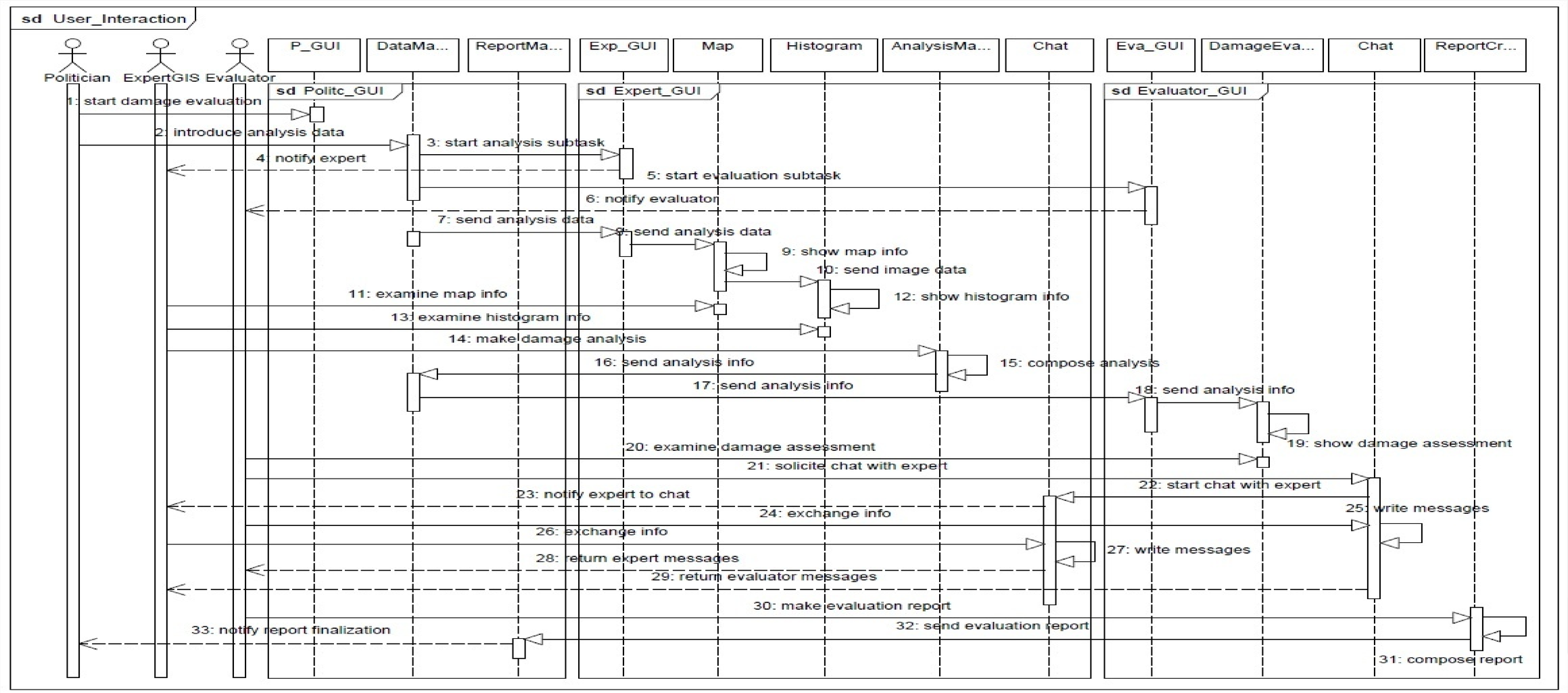
- About half of the CVEs exploited in 2014 went from **publish to pwn in less than a month**." - Verizon Breach Investigations Report, 2015
- "We found that **99.9%** of the exploited vulnerabilities had been compromised **more than a year after** the associated CVE was published." - Verizon Breach Investigations Report, 2015
- "Patch management and **associated vulnerability management processes** represent the biggest problem areas, because they're **rarely well documented and automated**." – Anton Chuvakin [http://blogs.gartner.com/anton-chuvakin/2014/02/13/highlights-from-verizon-pci-report-2014/]

“YourApp™ from MyCO poised to revolutionize the industry”

– MyCo CEO

Meet Simon, MyCo Lead System Engineer

YourApp


sd User_Interaction
Politician
ExpertGIS
Evaluator
P_GUI
DataMa...
ReportMa...
Exp_GUI
Map
Histogram
AnalysisMa...
Chat
Eva_GUI
DamageEva...
Chat
ReportCr...
sd Politc_GUI
sd Expert_GUI
sd Evaluator_GUI
1: start damage evaluation
2: introduce analysis data
3: start analysis subtask
4: notify expert
5: start evaluation subtask
6: notify evaluator
7: send analysis data
8: send analysis data
9: show map info
10: send image data
11: examine map info
12: show histogram info
13: examine histogram info
14: make damage analysis
15: compose analysis
16: send analysis info
17: send analysis info
18: send analysis info
19: show damage assessment
20: examine damage assessment
21: solicite chat with expert
22: start chat with expert
23: notify expert to chat
24: exchange info
25: write messages
26: exchange info
27: write messages
28: return expert messages
29: return evaluator messages
30: make evaluation report
31: compose report
32: send evaluation report
33: notify report finalization

Regulations, Catalogs, Guidelines

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

ISO

IEC

IETF®

ETSI
World Class Standards

SANS

PCI Security Standards Council™

DEPARTMENT OF DEFENSE
UNITED STATES OF AMERICA

HIPAA
Health Insurance Portability & Accountability Act

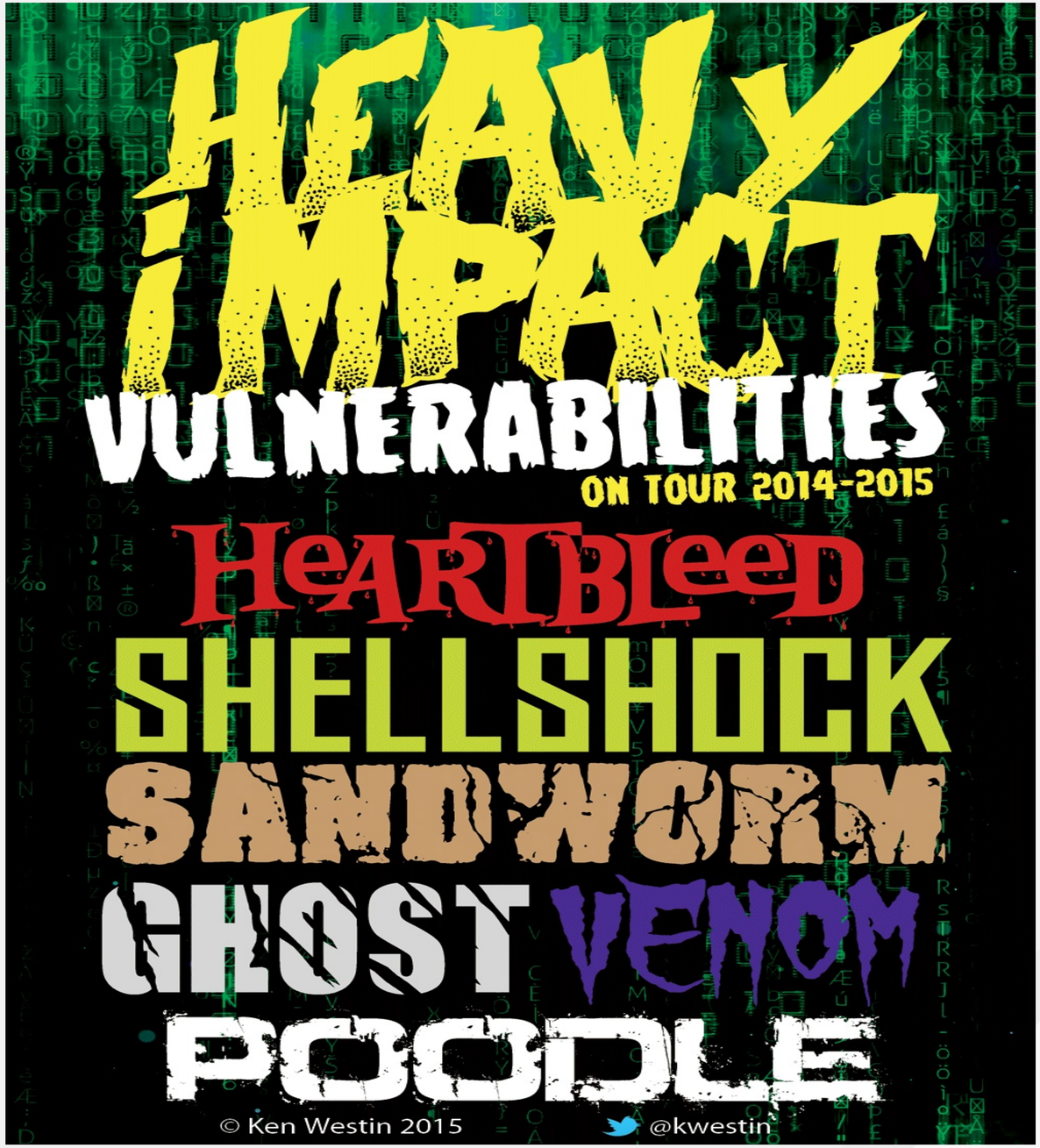
U.S. SECURITIES AND EXCHANGE COMMISSION
MCMXXXIV

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
UNITED STATES OF AMERICA

HIMSS®

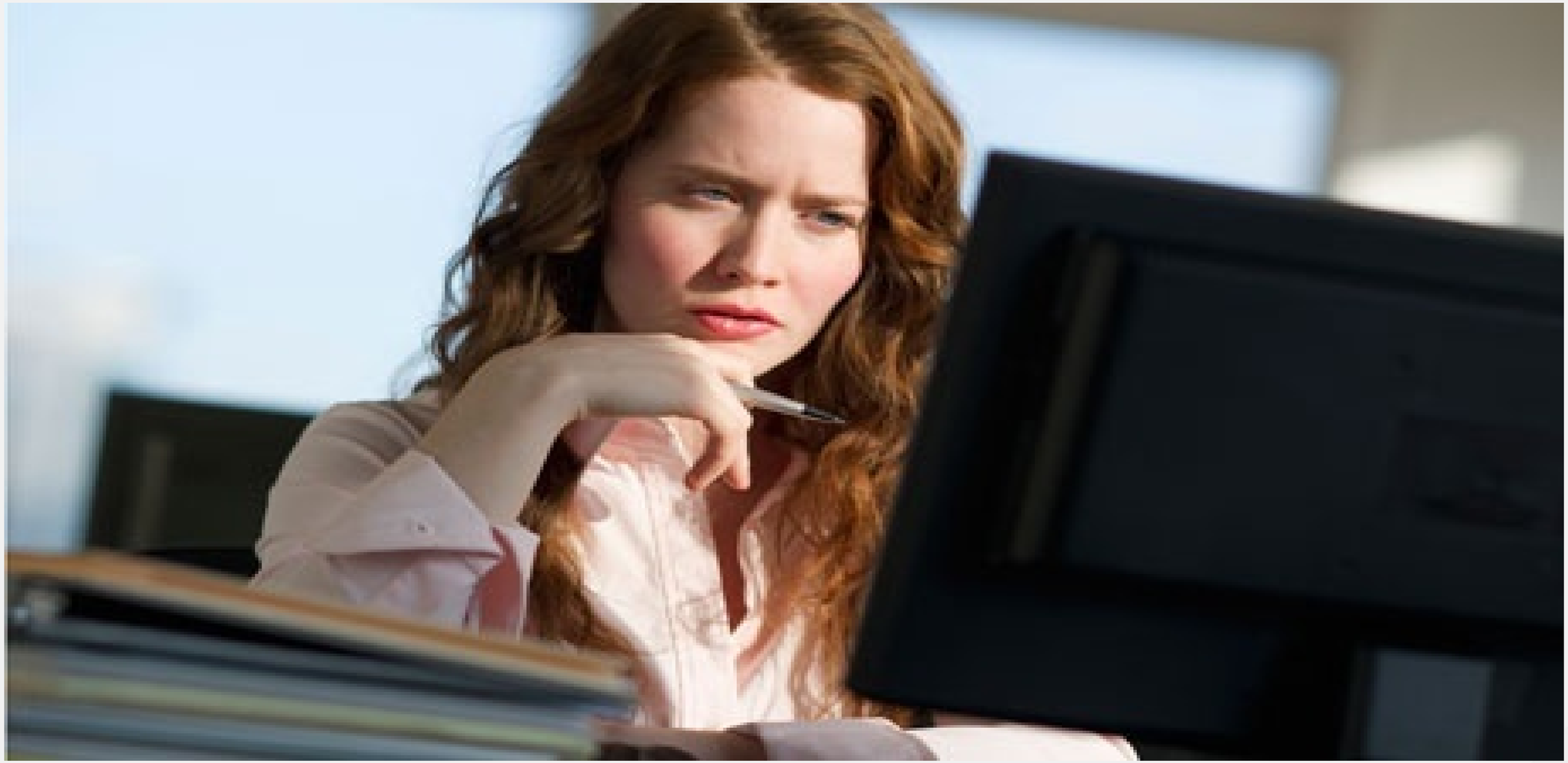

ZDNET TOLD ME OUR
SERVERS HAVE POODLES
I'LL NEED YOU TO
PATCH ALL THE BASHES
imgflip.com

Advanced Persistent Marketing



Poster created by Ken Westin, 2015, used with permission of author. Hi Ken!

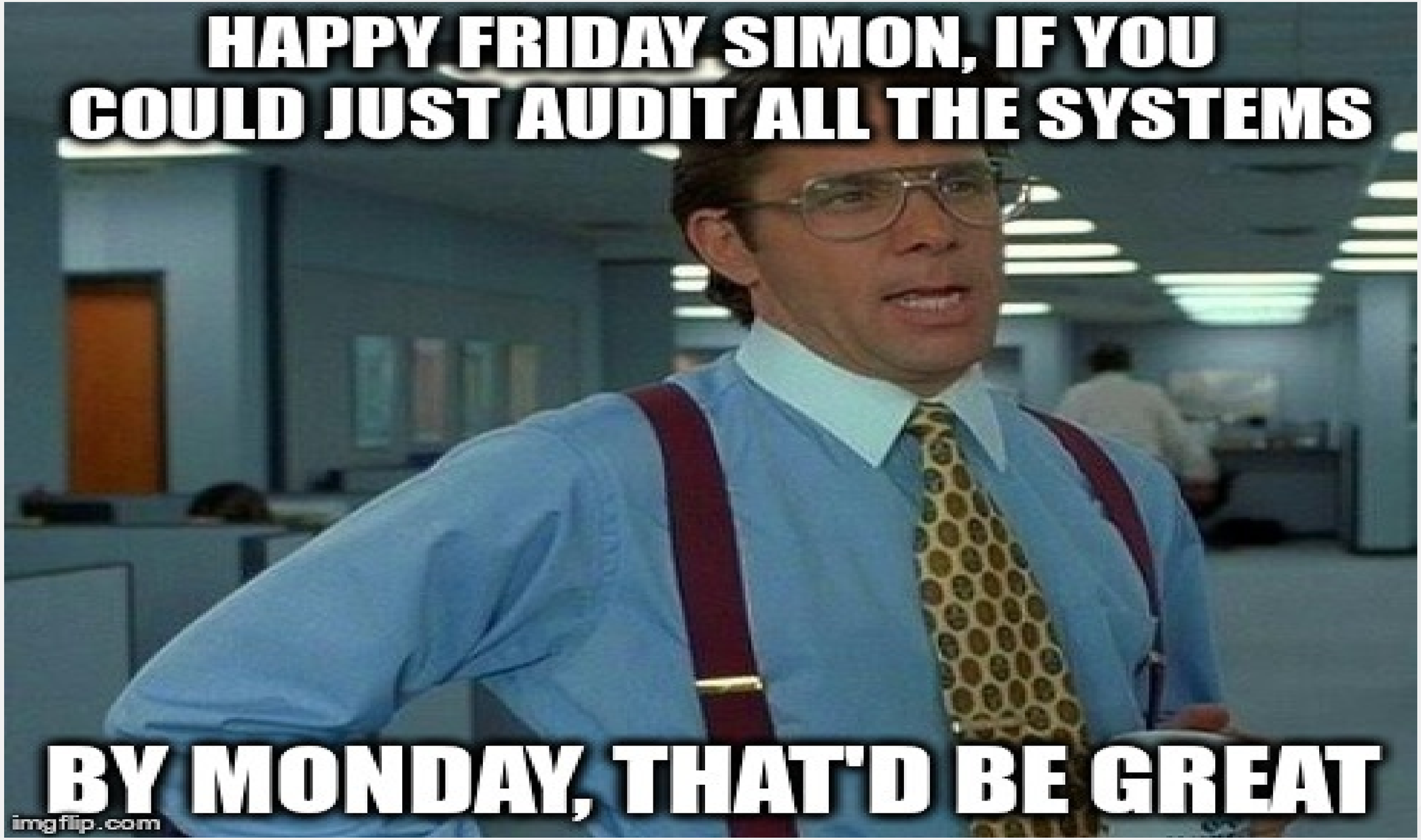
Meet Sarah, MyCo CISO



Sarah's initial SWAG

- Need local values for 50 controls (password lengths, login timeouts, etc)
- Only YourApp new systems in scope
- Project team bringing Security in late

C2S Profile = **250** controls
YourApp Env = **35** systems


HAPPY FRIDAY SIMON, IF YOU
COULD JUST AUDIT ALL THE SYSTEMS
BY MONDAY, THAT'D BE GREAT
imgflip.com

Simon's back of the napkin

$$\frac{Number\ of\ Controls * Time\ per\ Control * Number\ of\ Hosts}{Minutes\ per\ Hour}$$

$$\frac{250 * 1\,min * 35}{60\,min}$$

145 hours or **~18 Days**

KEEP CALM AND AUTOMATE ALL THE THINGS

```
# 'dev' option (not prefixed with 'no') present in the list?
echo $DEV_SHM_OPTS | grep -q -P '(?<!no)dev'
if [ $? -eq 0 ]
then
        # 'dev' option found, replace with 'nodev'
        DEV_SHM_OPTS=${DEV_SHM_OPTS//dev/nodev}
fi

# at least one 'nodev' present in the options list?
echo $DEV_SHM_OPTS | grep -q -v 'nodev'
if [ $? -eq 0 ]
then
        # 'nodev' not found yet, append it
        DEV_SHM_OPTS="$DEV_SHM_OPTS,nodev"
fi

# DEV_SHM_OPTS now contains final list of mount options. Replace original form of /dev/shm row
# in /etc/fstab with the corrected version
sed -i "s#${DEV_SHM_HEAD}\(.*\)${DEV_SHM_TAIL}#${DEV_SHM_HEAD}${DEV_SHM_OPTS}${DEV_SHM_TAIL}#" /etc/fsta

# Load /etc/fstab's /dev/shm row into DEV_SHM_FSTAB variable separating start &
# end of the filesystem mount options (4-th field) with the '#' character
DEV_SHM_FSTAB=$(sed -n "s/\(.*[[:space:]]\+\/dev\/shm[[:space:]]\+tmpfs[[:space:]]\+\)\([^[:space:]]\+\)

# Save the:
# * 1-th, 2-nd, 3-rd fields into DEV_SHM_HEAD variable
# * 4-th field into DEV_SHM_OPTS variable, and
# * 5-th, and 6-th fields into DEV_SHM_TAIL variable
# splitting DEV_SHM_FSTAB variable value based on the '#' separator
IFS='#' read DEV_SHM_HEAD DEV_SHM_OPTS DEV_SHM_TAIL <<< "$DEV_SHM_FSTAB"
```

SCAP

Brought to you by the letters NVD and CVE!

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

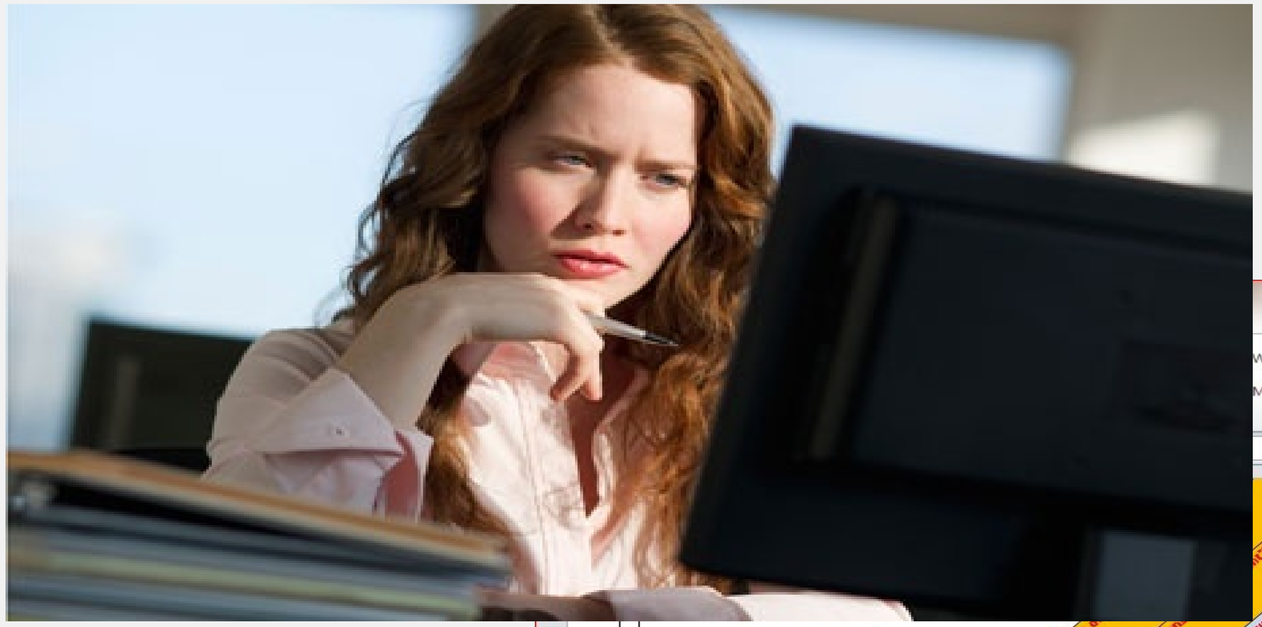
What does Simon need?

SCAP Content

SCAP Scanner

Centralization

The final controls!



DROPS Hazard Registry.xlsx - Microsoft Excel

					Primary Means of	Secondary Means	Personnel Frequently Beneath? (H-3, M-2, L-1)**	Weather Effects (H-3, M-2, L-1)**	Vibration Effects (H-3, M-2, L-1)**	Contact with moving parts? (H-3, M-2, L-1)**	Probability (1-3)**	Severity (1-4)**	Jonas Risk Score**	Cumulative Risk Score (Sum of blue * Jonas Risk S	Indexed Risk Score (Cumulative Scores/144)**
		Total Score (all items)**					141	75	95	108	88	196	343		
		Total Possible Score (all items)**					153	153	153	153	153	204	612		
		% of Total Possible Score**					92.2%	49.0%	62.1%	70.6%	57.5%	96.1%	56.0%		
5	1	NO LOOSE OBJECTS IN MONKEY BOARD AREA	None	None			3	3	3	3	3	4	12	144	100
6	2	1ST TURNBUCKLE HOOK UP POINT	Lock nut	None			3	2	3	3	3	4	12	132	92
7	3	2ND SET OF TURNBUCKLES & CLAMPS	Lock nut	None			3	2	3	3	3	4	12	132	92
8	4	3RD SET OF TURNBUCKLES & CLAMPS	Lock nut	None			3	2	3	3	3	4	12	132	92
9	5	4TH SET OF TURNBUCKLES & CLAMPS	Lock nut	None			3	2	3	3	3	4	12	132	92
10	6	DERRICK IS FREE OF LOOSE PARTS AND ALL TOOLS HAVE BEEN REMOVED	Tethered tools	Compliance			3	2	3	2	3	4	12	120	83
11	7	SRL'S & ANCHOR POINTS IN GOOD CONDITION (X3	Bolt & nut	None??			3	3	3	3	2	4	8	96	67
12	8	FLAG POST X2 W/SAFETY CABLES IN PLACE	Bracket,	Safety cable			3	3	3	3	2	4	8	96	67
13	9	KELLY HOSE HAS PROPERLY SIZED SNUB LIES ATTACHED AT BOTH ENDS WITH SECONDARY SECUREMENT/ 4 PART OVERHEAD SHACKLES USED/	Snub lines, Chain, Shackle	Cotter pins			3	2	3	3	2	4	8	88	61
14	10	TORQUE TUBE HOOK UP POINT WITH COTTER PINS IN	Shackles	Cotter pins			3	2	3	3	2	4	8	88	61
15	11	DERRICK IS FREE OF LOOSE LINES AND ROPES THAT CAN SNAG ON TOP DRIVE OR TRAVELING BLOCKS (TIRAK MANRIDER, CATLINE, TUGGER, SRL ROPE)	Compliance, Monitoring	Compliance, Monitoring			3	2	3	3	2	4	8	88	61
16	12	DERRICK HAS NO BENT STRUCTURAL MEMBERS AND NO VISUAL CRACKS ARE EVIDENT	Welds	None			3	1	1	2	3	4	12	84	58
17	13	TONG LINE CABLES IN GOOD SHAPE (ESPECIALLY AT	Shackles	Cotter pins			3	2	2	3	2	4	8	80	56
18	14	TONG LINE SHEAVES ARE SECURELY ATTACHED AND HAVE SAFETY LINES PROPERLY INSTALLED					3	2	2	3	2	4	8	80	56

DROPS List | Definitions | Risk Matrix | ANALYSIS

Final policy

- **Annual** audits
  - Requires **2 additional** regular reviews
- Need local values for **100 controls** (password lengths, login timeouts, etc)
- **15 current production systems** added to scope
- **DR site** also required

C2S Profile = **400** controls
YourApp Env = **100** systems

Simon's new napkin

$$\frac{Number\ of\ Controls * Time\ per\ Control * Number\ of\ Hosts}{Minutes\ per\ Hour}$$

$$\frac{400 * 1\,min * 100}{60\,min}$$

~666 hours or **~83 Days**

SPOILER ALERT!

What Simon's compliance system can do

C2S Run time = **73** seconds

$$\frac{400 * 5.5\ s * 100}{60\ min}$$

~61 hours or **~8 Days**

~8 Days *

- Mostly **computer** time, highly parallel
- **Little** administrator interaction required
- Still …
- Oh, and **150** more checks (**62.5%** more work)

~75 Days saved
Or 90.36 %

The Tool Chain that Simon Built

What does Simon need?

SCAP Content

SCAP Scanner

Centralization

The Content

SCAP Scanner

Centralization

SCAP (Security Content Automation Protocol) 1.2

NIST SP 800-126 Rev. 2

- **CCE™:** Common Configuration Enumeration
- **CPE™:** Common Platform Enumeration
- **CVE®:** Common Vulnerabilities and Exposures
- **CVSS:** Common Vulnerability Scoring System
- **CCSS:** Common Configuration Scoring System
- **XCCDF:** The Extensible Configuration Checklist Description Format
- **OVAL®:** Open Vulnerability and Assessment Language
- **OCIL:** Open Checklist Interactive Language
- **AI:** Asset Identification
- **ARF:** Asset Reporting Format

SCAP (Security Content Automation Protocol) 1.2

NIST SP 800-126 Rev. 2

- CCE™: Common Configuration Enumeration
- CPE™: Common Platform Enumeration
- CVE®: Common Vulnerabilities and Exposures
- CVSS: Common Vulnerability Scoring System
- CCSS: Common Configuration Scoring System
- **XCCDF: The Extensible Configuration Checklist Description Format**
- **OVAL®: Open Vulnerability and Assessment Language**
- OCIL: Open Checklist Interactive Language
- AI: Asset Identification
- ARF: Asset Reporting Format

Great who makes it?

SCAP
SECURITY GUIDE

DISA
DEFENSE INFORMATION SYSTEMS AGENCY
DEPARTMENT OF DEFENSE

redhat

Red Hat provided feeds

Filter by Package Name: Go Display 25 items per page 1 - 21 of 21

Package Name	Summary
openscap-scanner	OpenSCAP Scanner Tool (oscap)
openscap-perl	Perl bindings for openscap
inkscape-docs	Documentation for Inkscape
openscap-content	SCAP content
openscap	Set of open source libraries enabling integration of the SCAP line of standards
openscap-engine-sce	Script Check Engine plug-in for OpenSCAP
spacewalk-oscap	OpenSCAP plug-in for rhn-check
openscap-extra-probes	SCAP probes
openscap-utils	OpenSCAP Utilities
openscap-selinux	SELinux policy module for openscap
openscap-devel	Development files for openscap
openscap-python	Python bindings for openscap
perl-Pod-Escapes	Perl module for resolving POD escape sequences
scap-security-guide	Security guidance and baselines in SCAP formats
scap-workbench	Scanning, tailoring, editing and validation tool for SCAP content
oscap-anaconda-addon	Anaconda addon integrating OpenSCAP to the installation process
openscap-engine-sce-devel	Development files for openscap-engine-sce
firstaidkit-plugin-openscap	OpenSCAP plugin for FirstAidKit
rhsa-scap	Complete XCCDF and OVAL for all RHSA to date
inkscape	Vector-based drawing program using SVG
inkscape-view	Viewing program for SVG files

1 - 21 of 21

redhat. CUSTOMER PORTAL Products & Services Tools Security Community

Security Data

Red Hat Product Security are committed to providing tools and security data to help security measurement. Part of this commitment is our participation at board level in various projects such as MITRE CVE and OVAL. We also provide reports and metrics, but more importantly, we also provide the raw data below so customers and researchers can produce their own metrics, for their own unique situations, and hold us accountable.

CVRF Documents

The Common Vulnerability Reporting Framework (CVRF) standard enables organisations to share information about security issues with a consistent and common format. We provide Red Hat security advisories in CVRF format.

- CVRF compatibility FAQ
- Link to CVRF documents
- CVRF 1.1 samples (zip) (updated 2012-05-15)

OVAL Definitions

OVAL definitions are available for all vulnerabilities that affect Red Hat Enterprise Linux 3, 4, 5, 6, 7:

- OVAL compatibility FAQ
- OVAL definitions (consolidated XML file, .bz2) (constantly updated)
- OVAL repository (separate files)

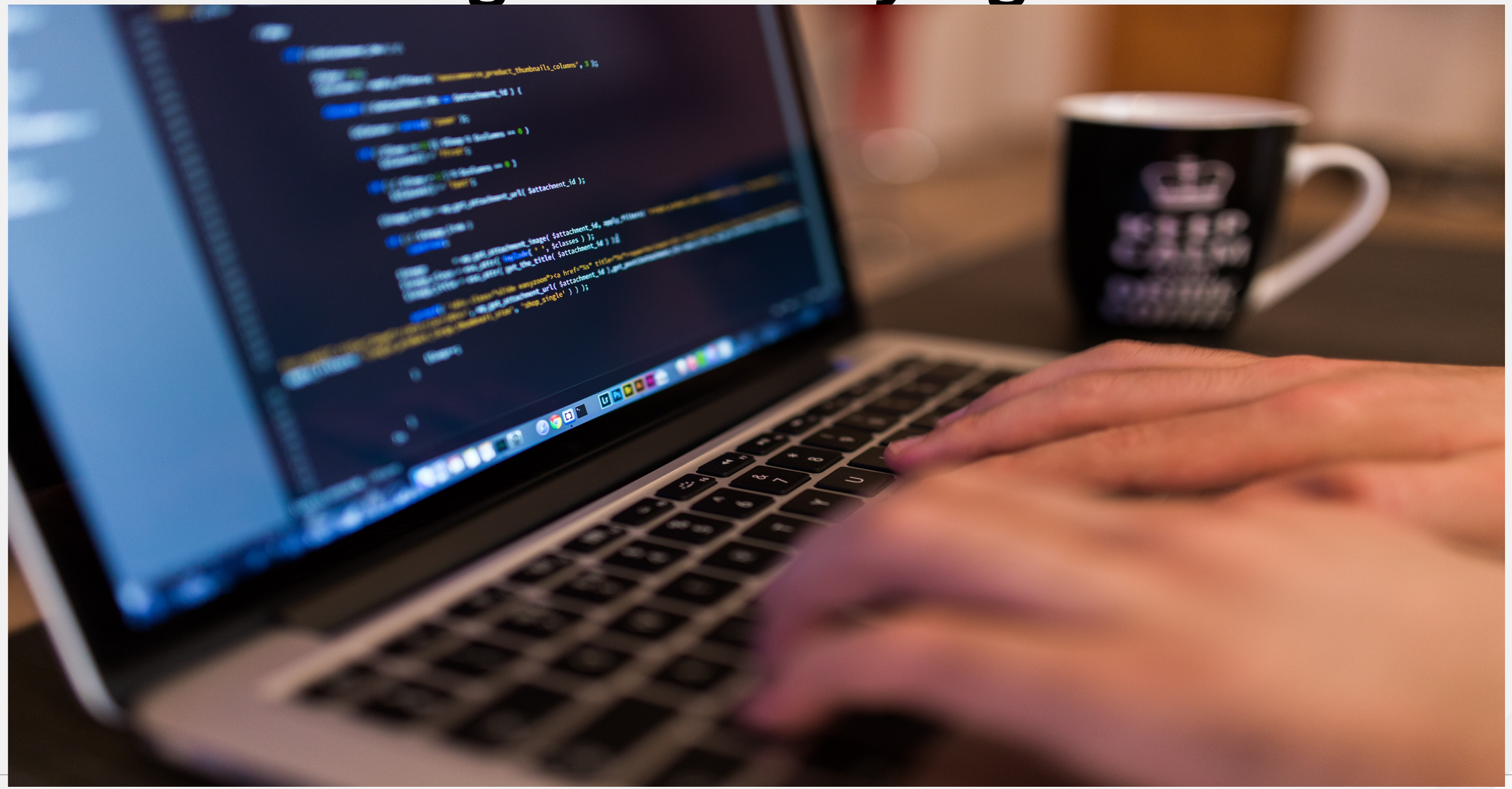
Vulnerability Statements and Acknowledgements

We publish acknowledgments and official statements for vulnerabilities currently under investigation and for vulnerabilities that do not affect our products and services. These statements appear on our in CVE pages

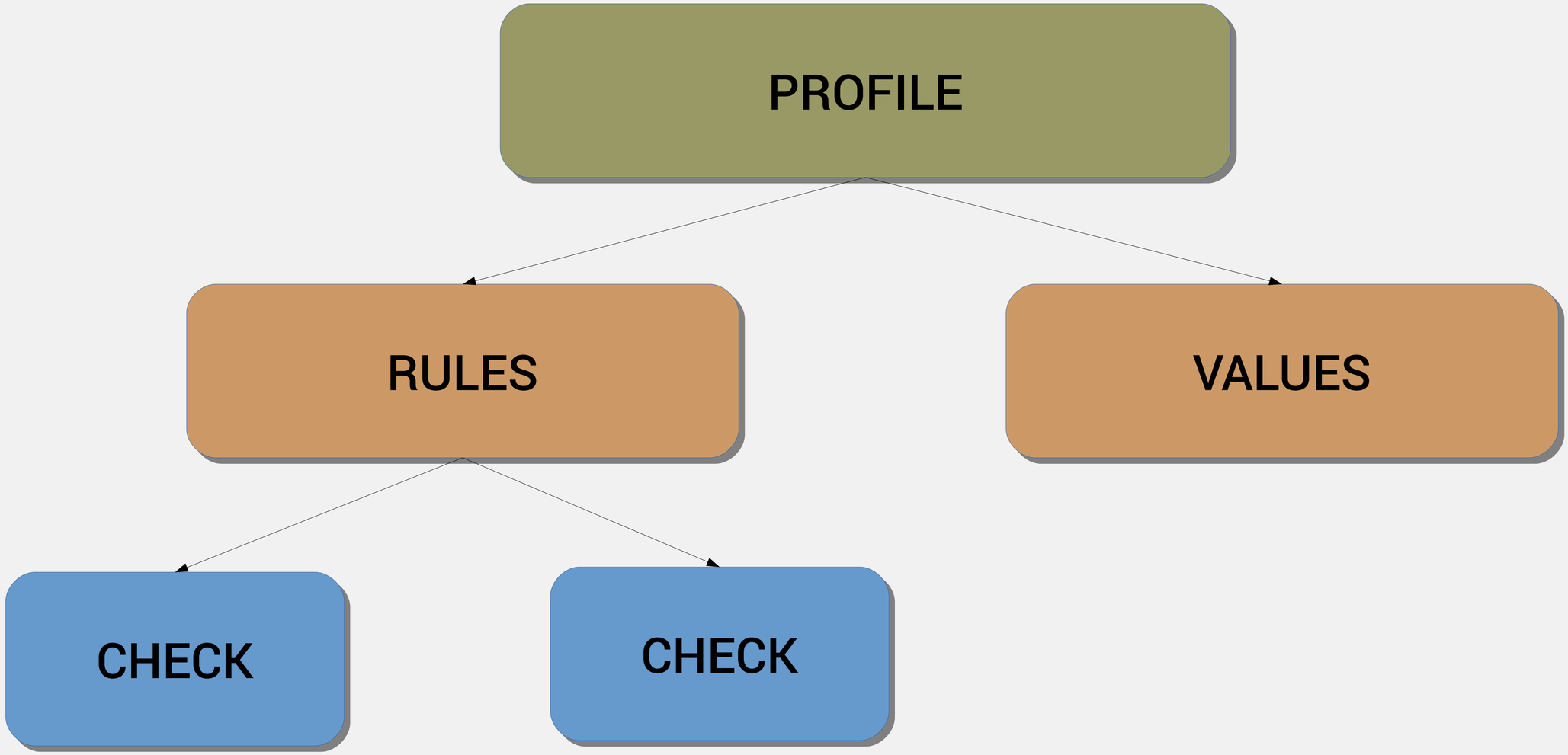
- cve-metadata-from-bugzilla.xml (XML feed, updated twice a day)

http://www.redhat.com/security/data/metrics/
http://www.redhat.com/security/data/metrics/com.redhat.rhsa-all.xccdf.xml

Building and modifying content



XCCDF



XCCDF Profile

```
<Profile id="common">
  <title xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">Common Profile for
  General-Purpose Fedora Systems</title>
  <description xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">This profile
  contains items common to general-purpose Fedora installations.</description>
  <select idref="disable_prelink" selected="true"/>
  <select idref="ensure_gpgcheck_globally_activated" selected="true"/>
  <select idref="ensure_gpgcheck_never_disabled" selected="true"/>
  <select idref="file_permissions_library_dirs" selected="true"/>
  <select idref="file_ownership_library_dirs" selected="true"/>
  <select idref="file_permissions_binary_dirs" selected="true"/>
  <select idref="file_ownership_binary_dirs" selected="true"/>
  <select idref="no_direct_root_logins" selected="true"/>
  <select idref="securetty_root_login_console_only" selected="true"/>
  <select idref="restrict_serial_port_logins" selected="true"/>
  <select idref="no_uidzero_except_root" selected="true"/>
  <select idref="no_empty_passwords" selected="true"/>
  <select idref="no_hashes_outside_shadow" selected="true"/>
  <select idref="no_netrc_files" selected="true"/>
  <select idref="accounts_password_minlen_login_defs" selected="true"/>
  <select idref="accounts_minimum_age_login_defs" selected="true"/>
  <select idref="accounts_maximum_age_login_defs" selected="true"/>
  <select idref="accounts_password_warn_age_login_defs" selected="true"/>
  <select idref="root_path_no_groupother_writable" selected="true"/>
  <select idref="service_ntpd_enabled" selected="true"/>
  <select idref="ntpd_specify_remote_server" selected="true"/>
  <select idref="sshd_disable_root_login" selected="true"/>
  <select idref="sshd_disable_empty_passwords" selected="true"/>
  <select idref="sshd_set_idle_timeout" selected="true"/>
  <select idref="sshd_set_keepalive" selected="true"/>
  <refine-value idref="var_accounts_password_minlen_login_defs" selector="12"/>
  <refine-value idref="var_accounts_minimum_age_login_defs" selector="7"/>
  <refine-value idref="var_accounts_maximum_age_login_defs" selector="90"/>
  <refine-value idref="var_accounts_password_warn_age_login_defs" selector="7"/>
  <refine-value idref="sshd_idle_timeout_value" selector="5_minutes"/>
</Profile>
```

XCCDF Profile

```
<Profile id="common">
  <title xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">Common Profile for
  General-Purpose Fedora Systems</title>
  <description xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">This profile
  contains items common to general-purpose Fedora installations.</description>
  <select idref="disable_prelink" selected="true"/>
  <select idref="ensure_gpgcheck_globally_activated" selected="true"/>
  <select idref="ensure_gpgcheck_never_disabled" selected="true"/>
  <select idref="file_permissions_library_dirs" selected="true"/>
  <select idref="file_ownership_library_dirs" selected="true"/>
  <select idref="file_permissions_binary_dirs" selected="true"/>
  <select idref="file_ownership_binary_dirs" selected="true"/>
  <select idref="no_direct_root_logins" selected="true"/>
  <select idref="securetty_root_login_console_only" selected="true"/>
  <select idref="restrict_serial_port_logins" selected="true"/>
  <select idref="no_uidzero_except_root" selected="true"/>
  <select idref="no_empty_passwords" selected="true"/>
  <select idref="no_hashes_outside_shadow" selected="true"/>
  <select idref="no_netrc_files" selected="true"/>
  <select idref="accounts_password_minlen_login_defs" selected="true"/>
  <select idref="accounts_minimum_age_login_defs" selected="true"/>
  <select idref="accounts_maximum_age_login_defs" selected="true"/>
  <select idref="accounts_password_warn_age_login_defs" selected="true"/>
  <select idref="root_path_no_groupother_writable" selected="true"/>
  <select idref="service_ntpd_enabled" selected="true"/>
  <select idref="ntpd_specify_remote_server" selected="true"/>
  <select idref="sshd_disable_root_login" selected="true"/>
  <select idref="sshd_disable_empty_passwords" selected="true"/>
  <select idref="sshd_set_idle_timeout" selected="true"/>
  <select idref="sshd_set_keepalive" selected="true"/>
  <refine-value idref="var_accounts_password_minlen_login_defs" selector="12"/>
  <refine-value idref="var_accounts_minimum_age_login_defs" selector="7"/>
  <refine-value idref="var_accounts_maximum_age_login_defs" selector="90"/>
  <refine-value idref="var_accounts_password_warn_age_login_defs" selector="7"/>
  <refine-value idref="sshd_idle_timeout_value" selector="5_minutes"/>
</Profile>
```

XCCDF Profile

```
<Profile id="common">
  <title xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">Common Profile for
  General-Purpose Fedora Systems</title>
  <description xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">This profile
  contains items common to general-purpose Fedora installations.</description>
  <select idref="disable_prelink" selected="true"/>
  <select idref="ensure_gpgcheck_globally_activated" selected="true"/>
  <select idref="ensure_gpgcheck_never_disabled" selected="true"/>
  <select idref="file_permissions_library_dirs" selected="true"/>
  <select idref="file_ownership_library_dirs" selected="true"/>
  <select idref="file_permissions_binary_dirs" selected="true"/>
  <select idref="file_ownership_binary_dirs" selected="true"/>
  <select idref="no_direct_root_logins" selected="true"/>
  <select idref="securetty_root_login_console_only" selected="true"/>
  <select idref="restrict_serial_port_logins" selected="true"/>
  <select idref="no_uidzero_except_root" selected="true"/>
  <select idref="no_empty_passwords" selected="true"/>
  <select idref="no_hashes_outside_shadow" selected="true"/>
  <select idref="no_netrc_files" selected="true"/>
  <select idref="accounts_password_minlen_login_defs" selected="true"/>
  <select idref="accounts_minimum_age_login_defs" selected="true"/>
  <select idref="accounts_maximum_age_login_defs" selected="true"/>
  <select idref="accounts_password_warn_age_login_defs" selected="true"/>
  <select idref="root_path_no_groupother_writable" selected="true"/>
  <select idref="service_ntpd_enabled" selected="true"/>
  <select idref="ntpd_specify_remote_server" selected="true"/>
  <select idref="sshd_disable_root_login" selected="true"/>
  <select idref="sshd_disable_empty_passwords" selected="true"/>
  <select idref="sshd_set_idle_timeout" selected="true"/>
  <select idref="sshd_set_keepalive" selected="true"/>
  <refine-value idref="var_accounts_password_minlen_login_defs" selector="12"/>
  <refine-value idref="var_accounts_minimum_age_login_defs" selector="7"/>
  <refine-value idref="var_accounts_maximum_age_login_defs" selector="90"/>
  <refine-value idref="var_accounts_password_warn_age_login_defs" selector="7"/>
  <refine-value idref="sshd_idle_timeout_value" selector="5_minutes"/>
</Profile>
```

XCCDF Rule

```
<Rule id="set_password_hashing_algorithm_logindefs" selected="false" severity="medium"
>
  <title xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">Set Password
  Hashing Algorithm in /etc/login.defs</title>
  <description xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">
In <xhtml:code>/etc/login.defs</xhtml:code>, add or correct the following line to ensure
the system will use SHA-512 as the hashing algorithm:
<pre xmlns="http://www.w3.org/1999/xhtml">ENCRYPT_METHOD SHA512</pre>
</description>
  <reference href="http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-
  rev3-final.pdf">IA-5(b)</reference>
  <reference href="http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-
  rev3-final.pdf">IA-5(c)</reference>
  <reference href="http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-
  rev3-final.pdf">IA-5(1)(c)</reference>
  <reference href="http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-
  rev3-final.pdf">IA-7</reference>
  <reference href="http://iase.disa.mil/stigs/cci/Pages/index.aspx"/>
  <rationale xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">
Using a stronger hashing algorithm makes password cracking attacks more difficult.
</rationale>
  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <check-content-ref name="oval:ssg:def:208" href="ssg-fedora-oval.xml"/>
  </check>
  <check system="ocil-transitional">
    <check-export export-name="it does not" value-id="conditional_clause"/>
    <check-content xmlns:xhtml="http://www.w3.org/1999/xhtml">
Inspect <xhtml:code>/etc/login.defs</xhtml:code> and ensure the following line appears:
<pre xmlns="http://www.w3.org/1999/xhtml">ENCRYPT_METHOD SHA512</pre>
</check-content>
  </check>
</Rule>
```

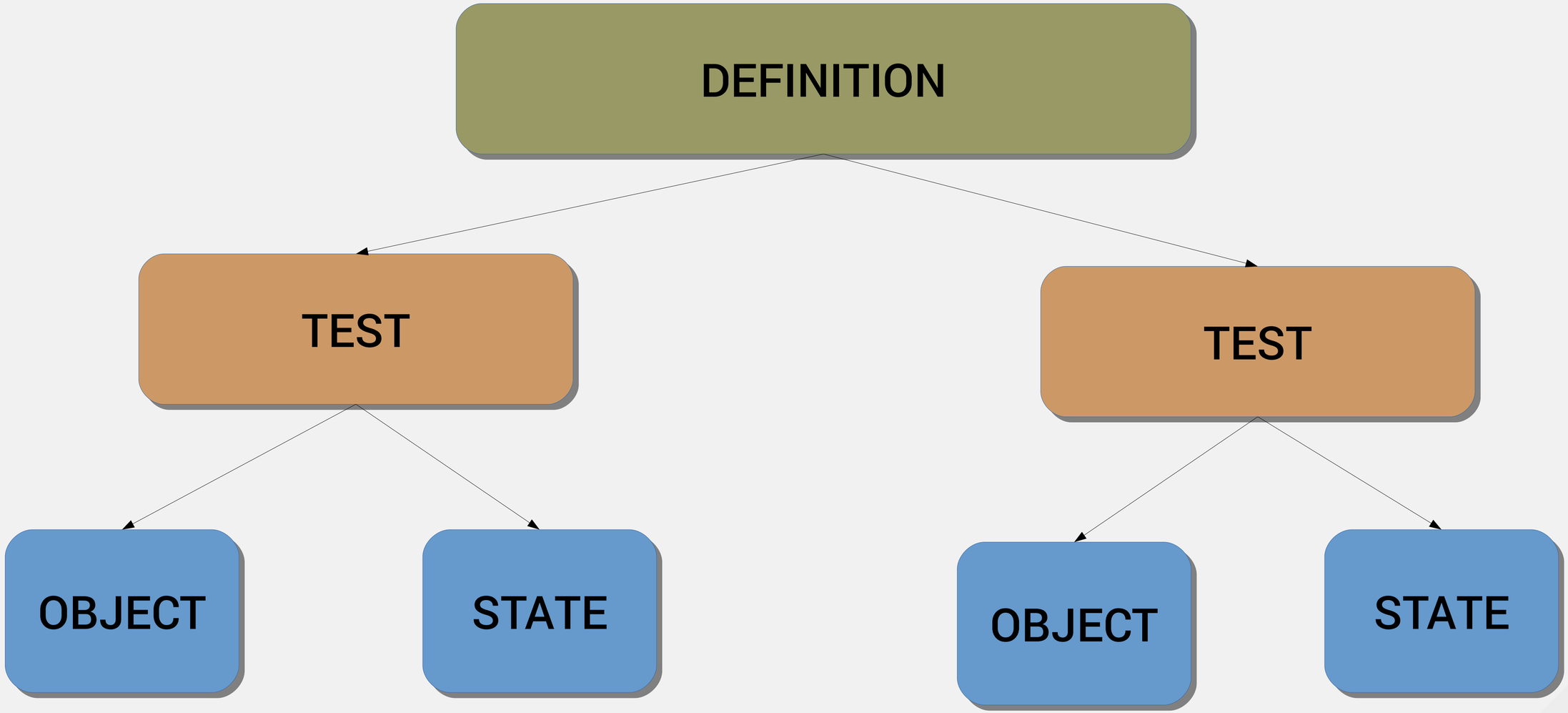
XCCDF Rule

```
<Rule id="set_password_hashing_algorithm_logindefs" selected="false" severity="medium"
>
  <title xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">Set Password
  Hashing Algorithm in /etc/login.defs</title>
  <description xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">
In <xhtml:code>/etc/login.defs</xhtml:code>, add or correct the following line to ensure
the system will use SHA-512 as the hashing algorithm:
<pre xmlns="http://www.w3.org/1999/xhtml">ENCRYPT_METHOD SHA512</pre>
</description>
  <reference href="http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-
  rev3-final.pdf">IA-5(b)</reference>
  <reference href="http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-
  rev3-final.pdf">IA-5(c)</reference>
  <reference href="http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-
  rev3-final.pdf">IA-5(1)(c)</reference>
  <reference href="http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-
  rev3-final.pdf">IA-7</reference>
  <reference href="http://iase.disa.mil/stigs/cci/Pages/index.aspx"/>
  <rationale xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">
Using a stronger hashing algorithm makes password cracking attacks more difficult.
</rationale>
  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <check-content-ref name="oval:ssg:def:208" href="ssg-fedora-oval.xml"/>
  </check>
  <check system="ocil-transitional">
    <check-export export-name="it does not" value-id="conditional_clause"/>
    <check-content xmlns:xhtml="http://www.w3.org/1999/xhtml">
Inspect <xhtml:code>/etc/login.defs</xhtml:code> and ensure the following line appears:
<pre xmlns="http://www.w3.org/1999/xhtml">ENCRYPT_METHOD SHA512</pre>
</check-content>
  </check>
</Rule>
```

XCCDF Rule

```
<Rule id="set_password_hashing_algorithm_logindefs" selected="false" severity="medium"
>
  <title xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">Set Password
  Hashing Algorithm in /etc/login.defs</title>
  <description xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">
In <xhtml:code>/etc/login.defs</xhtml:code>, add or correct the following line to ensure
the system will use SHA-512 as the hashing algorithm:
<pre xmlns="http://www.w3.org/1999/xhtml">ENCRYPT_METHOD SHA512</pre>
</description>
  <reference href="http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-
  rev3-final.pdf">IA-5(b)</reference>
  <reference href="http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-
  rev3-final.pdf">IA-5(c)</reference>
  <reference href="http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-
  rev3-final.pdf">IA-5(1)(c)</reference>
  <reference href="http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-
  rev3-final.pdf">IA-7</reference>
  <reference href="http://iase.disa.mil/stigs/cci/Pages/index.aspx"/>
  <rationale xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">
Using a stronger hashing algorithm makes password cracking attacks more difficult.
</rationale>
  <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
    <check-content-ref name="oval:ssg:def:208" href="ssg-fedora-oval.xml"/>
  </check>
  <check system="ocil-transitional">
    <check-export export-name="it does not" value-id="conditional_clause"/>
    <check-content xmlns:xhtml="http://www.w3.org/1999/xhtml">
Inspect <xhtml:code>/etc/login.defs</xhtml:code> and ensure the following line appears:
<pre xmlns="http://www.w3.org/1999/xhtml">ENCRYPT_METHOD SHA512</pre>
</check-content>
  </check>
</Rule>
```

OVAL Entities



OVAL Definition

```
<definition class="compliance" id="oval:ssg:def:208" version="2">
  <metadata>
    <title>Set SHA512 Password Hashing Algorithm in /etc/login.defs</title>
    <affected family="unix">
      <platform>Red Hat Enterprise Linux 6</platform>
      <platform>Red Hat Enterprise Linux 7</platform>
    </affected>
    <description>The password hashing algorithm should be set correctly in /etc/login.defs.
    </description>
    <reference source="JL" ref_id="RHEL6_20150201" ref_url="test_attestation"/>
    <reference source="JL" ref_id="RHEL7_20150201" ref_url="test_attestation"/>
    <reference source="JL" ref_id="FEDORA20_20150201" ref_url="test_attestation"/>
  <reference ref_id="set_password_hashing_algorithm_logindefs" source="ssg"/></metadata>
  <criteria operator="AND">
    <criterion test_ref="oval:ssg:tst:209"/>
  </criteria>
</definition>
```

OVAL Walking back the cat

```
<ind:variable_test id="oval:ssg:tst:209" check="all" comment="The value of ENCRYPT_METHOD
should be set appropriately in /etc/login.defs" version="1">
  <ind:object object_ref="oval:ssg:obj:367"/>
  <ind:state state_ref="oval:ssg:ste:368"/>
</ind:variable_test>
```

```
<ind:variable_object id="oval:ssg:obj:367" version="1">
  <ind:var_ref>oval:ssg:var:451</ind:var_ref>
</ind:variable_object>
```

```
<local_variable id="oval:ssg:var:451" datatype="string" comment="The value of last
ENCRYPT_METHOD directive in /etc/login.defs" version="1">
  <regex_capture pattern="ENCRYPT_METHOD\s+(\w+)">
    <object_component item_field="subexpression" object_ref="oval:ssg:obj:450"/>
  </regex_capture>
</local_variable>
```

```
<ind:textfilecontent54_object id="oval:ssg:obj:450" version="1">
  <!-- Read whole /etc/login.defs as single line so we can retrieve last ENCRYPT_METHOD
  directive occurrence -->
  <ind:behaviors singleline="true"/>
  <ind:filepath>/etc/login.defs</ind:filepath>
  <!-- Retrieve last (uncommented) occurrence of ENCRYPT_METHOD directive -->
  <ind:pattern operation="pattern match">.*\n[^#]*(ENCRYPT_METHOD\s+\w+)\s*\n</ind:pattern>
  <ind:instance datatype="int" operation="greater than or equal">1</ind:instance>
</ind:textfilecontent54_object>
```

```
<ind:variable_state id="oval:ssg:ste:368" version="1">
  <ind:value operation="equals" datatype="string">SHA512</ind:value>
</ind:variable_state>
```

A plug for upstream

- Sane **separation of files** with XSLT to create valid content
- OVAL in **single check file** with human readable IDs
- XCCDF in **descriptive structure**
- Modify **make file** to include and build content or **RPM**

```
<def-group>
  <definition class="compliance" id="set_password_hashing_algorithm_logindefs" version="2">
    <metadata>
      <title>Set SHA512 Password Hashing Algorithm in /etc/login.defs</title>
      <affected family="unix">
        <platform>multi_platform_rhel</platform>
      </affected>
      <description>The password hashing algorithm should be set correctly in /etc/login.defs.</
      description>
      <reference source="JL" ref_id="RHEL6_20150201" ref_url="test_attestation" />
      <reference source="JL" ref_id="RHEL7_20150201" ref_url="test_attestation" />
      <reference source="JL" ref_id="FEDORA20_20150201" ref_url="test_attestation" />
    </metadata>
    <criteria operator="AND">
      <criterion test_ref="test_etc_login_defs_encrypt_method" />
    </criteria>
  </definition>

  <ind:variable_test id="test_etc_login_defs_encrypt_method" check="all" comment="The value of
  ENCRYPT_METHOD should be set appropriately in /etc/login.defs" version="1">
    <ind:object object_ref="object_last_encrypt_method_instance_value" />
    <ind:state state_ref="state_last_encrypt_method_instance_value" />
  </ind:variable_test>

  <ind:textfilecontent54_object id="object_last_encrypt_method_from_etc_login_defs" version="1">
    <!-- Read whole /etc/login.defs as single line so we can retrieve last ENCRYPT_METHOD directive
    occurrence -->
    <ind:behaviors singleline="true" />
    <ind:filepath>/etc/login.defs</ind:filepath>
    <!-- Retrieve last (uncommented) occurrence of ENCRYPT_METHOD directive -->
    <ind:pattern operation="pattern match">.*\n[^#]*(ENCRYPT_METHOD\s+\w+)\s*\n</ind:pattern>
    <ind:instance datatype="int" operation="greater than or equal">1</ind:instance>
  </ind:textfilecontent54_object>

  <!-- Capture the actual ENCRYPT_METHOD string value from the previously retrieved last instance -->
  <local_variable id="variable_last_encrypt_method_instance_value" datatype="string" comment="The
  value of last ENCRYPT_METHOD directive in /etc/login.defs" version="1">
    <regex_capture pattern="ENCRYPT_METHOD\s+(\w+)">
      <object_component item_field="subexpression" object_ref="
      object_last_encrypt_method_from_etc_login_defs" />
    </regex_capture>
  </local_variable>

  <!-- Construct OVAL object from this local variable so we can use it in variable test above -->
  <ind:variable_object id="object_last_encrypt_method_instance_value" version="1">
    <ind:var_ref>variable_last_encrypt_method_instance_value</ind:var_ref>
  </ind:variable_object>

  <!-- Define corresponding variable state (the requirement) for the variable object -->
  <!-- The check should PASS if retrieved last ENCRYPT_METHOD value is equal to the requirement -->
  <ind:variable_state id="state_last_encrypt_method_instance_value" version="1">
    <ind:value operation="equals" datatype="string">SHA512</ind:value>
  </ind:variable_state>

</def-group>
```

SCAP
SECURITY GUIDE

What about the analyst?

ssg-rhel6-ds.xml - SCAP Workbench

File Help

Title: Guide to the Secure Configuration of Red Hat Enterprise Linux 6

Customization: (no customization)

Profile: C2S for Red Hat Enterprise Linux 6 — Customize

Target: Local Machine / Remote Machine (over SSH)

- Ensure /tmp Located On Separate Partition
- Ensure /var Located On Separate Partition
- Ensure /var/log Located On Separate Partition
- Ensure /var/log/audit Located On Separate Partition

  Audit logs are stored in the /var/log/audit directory. Ensure that it has its own partition or logical volume at installation time, or migrate it later using LVM. Make absolutely certain that it is large enough to store all audit logs that will be created by the auditing daemon.
- Ensure /home Located On Separate Partition
- Ensure Red Hat GPG Key Installed

  To ensure the system can cryptographically verify base software packages come from Red Hat (and to connect to the Red Hat Network to receive them), the Red Hat GPG key must properly be installed. To install the Red Hat GPG key, run:

  ```
  $ sudo rhn_register
  ```

  If the system is not connected to the Internet or an RHN Satellite, then install the Red Hat GPG key from trusted media such as the Red Hat installation CD-ROM or DVD. Assuming the disc is mounted in /media/cdrom, use the following command as the root user to import it into the keyring:

  ```
  $ sudo rpm --import /media/cdrom/RPM-GPG-KEY
  ```

0% (0 results, 177 rules selected)

Remediate — Scan

Customizing "C2S for Red Hat Enterprise Linux 6 [CUSTOMIZED]"

Undo History | Deselect All | hashing | Search | Showing match 1 out of 4 total found.

- Ensure that System Accounts Do Not Run a Shell Upon Login
- Verify Only Root Has UID 0
- Root Path Must Be Vendor Default
- Verify Proper Storage and Existence of PasswordHashes
  - Prevent Log In to Accounts With Empty Password
  - Verify All Account Password Hashes are Shadowed
  - All GIDs referenced in /etc/passwd must be defined in /etc/group
  - Verify No netrc Files Exist
- Set Password Expiration Parameters
  - minimum password length
  - maximum password age
  - minimum password age
  - warning days before password expires
  - Set Password Minimum Length in login.defs
  - Set Password Minimum Age
  - Set Password Maximum Age
  - Set Password Warning Age
- Set Account Expiration Parameters
  - number of days after a password expires until the account is permanently disabled
  - Set Account Expiration Following Inactivity
  - Ensure All Accounts on the System Have Unique Names
  - Assign Expiration Date to Temporary Accounts
- Protect Accounts by Configuring PAM
  - remember
  - Set Last Login/Access Notification
  - Set Password Quality Requirem
    - Set Password Quality Re ements if cracklib
      - retry
      - maxrepeat

Selected Item Properties

Title: maximum password age

ID: value_var_accounts_maximum_age_login_defs

Type: xccdf:Value

Modify Value
Only takes effect when this profile is used for evaluation.

60 (number)

Description

Maximum age of password in days

Affects Rule

- Set Password Maximum Age

Delete profile

SCAP WORKBENCH

SCAP Tailoring file

```
<xccdf:Tailoring xmlns:xccdf="http://checklists.nist.gov/xccdf/1.2" id="xccdf_scap-
workbench_tailoring_default">
  <xccdf:benchmark href="/usr/share/xml/scap/ssg/content/ssg-rhel6-ds.xml"/>
  <xccdf:version time="2015-04-20T09:51:07">1</xccdf:version>
  <xccdf:Profile id="xccdf_com.dlt.content_profile_C2S_baseline" extends="xccdf_org.ssgproject.
  content_profile_C2S">
```

```
    <xccdf:select idref="xccdf_org.ssgproject.
    content_rule_set_password_hashing_algorithm_libuserconf" selected="true"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_rule_root_path_no_groupother_writable"
    selected="true"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_rule_root_path_no_dot" selected="true"/>
    <xccdf:select idref="xccdf_org.ssgproject.content_rule_network_disable_zeroconf" selected="
    true"/>
    <xccdf:set-value idref="xccdf_org.ssgproject.content_value_var_umask_for_daemons">022</xccdf:
    set-value>
    <xccdf:set-value idref="xccdf_org.ssgproject.
    content_value_var_accounts_password_minlen_login_defs">8</xccdf:set-value>
    <xccdf:set-value idref="xccdf_org.ssgproject.content_value_var_accounts_minimum_age_login_defs
    ">0</xccdf:set-value>
    <xccdf:set-value idref="xccdf_org.ssgproject.
    content_value_var_accounts_password_warn_age_login_defs">14</xccdf:set-value>
    <xccdf:set-value idref="xccdf_org.ssgproject.
    content_value_var_accounts_passwords_pam_faillock_unlock_time">900</xccdf:set-value>
  </xccdf:Profile>
</xccdf:Tailoring>
```

The Scanner

Centralization

OpenSCAP

NIST **validated** SCAP scanner by Red Hat

redhat	OpenSCAP 1.0	- Authenticated Configuration Scanner - Common Vulnerabilities and Exposures (CVE)	- Red Hat Enterprise Linux 5.9 Desktop, (x86_64) - Red Hat Enterprise Linux 5.9 Desktop, (x86)	April 17, 2014

https://nvd.nist.gov/scapproducts.cfm

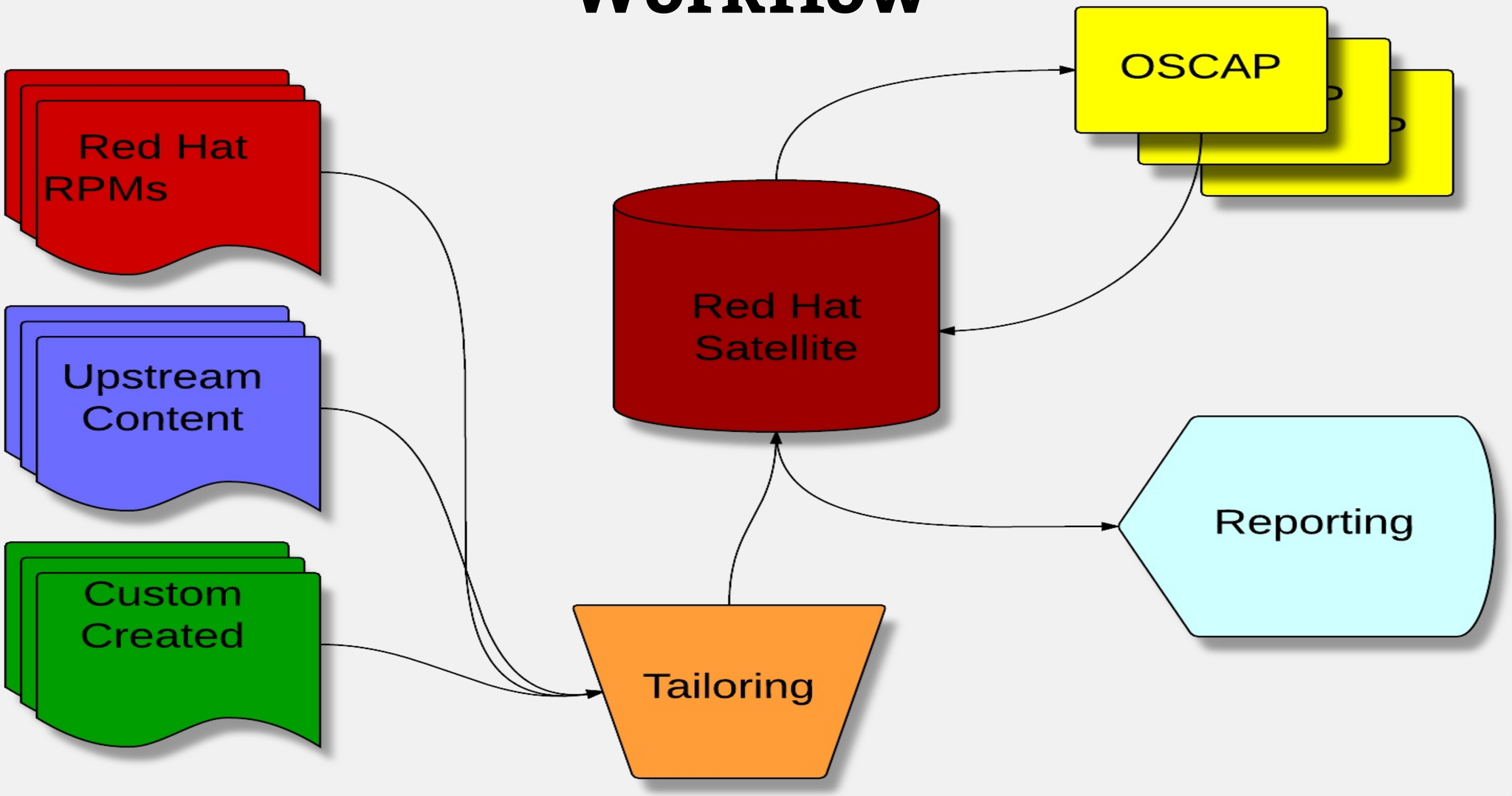
The Centralization

SCAP SECURITY GUIDE

OpenSCAP

redhat | RED HAT SATELLITE

Workflow


Red Hat
RPMs
Upstream
Content
Custom
Created
Tailoring
Red Hat
Satellite
OSCAP
Reporting

SATELLITE 5 WORK FLOW

Use RPMs

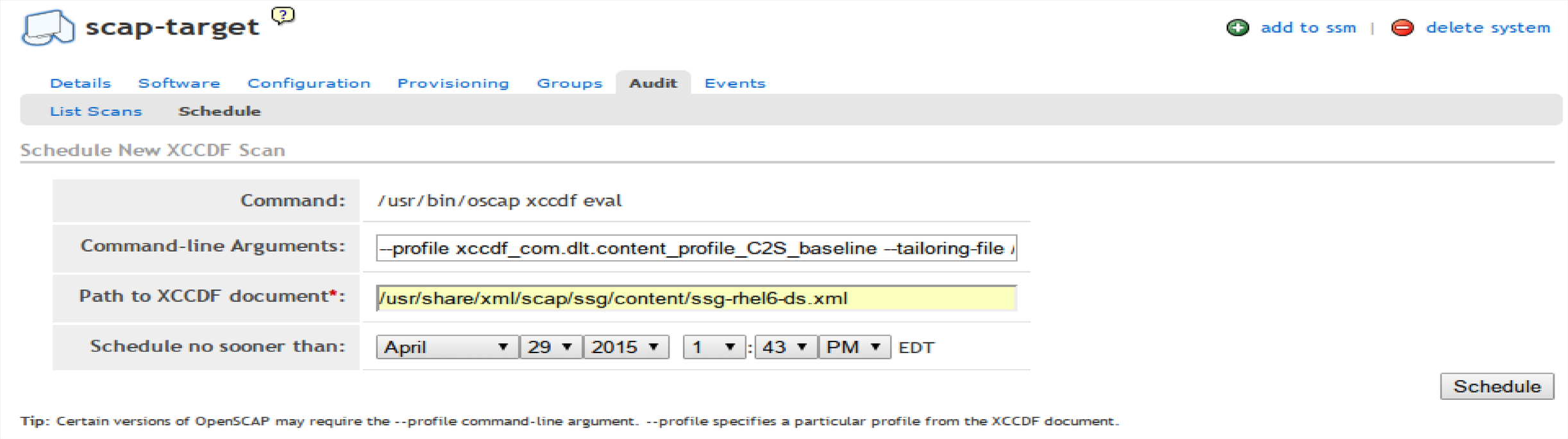
```
[root@ep-mgmt01 ~]# gpg --list-keys
/root/.gnupg/pubring.gpg
------------------------
pub   2048R/96D46A3F 2015-04-09
uid                  Package Builder (This is for signing local RPMs) <pkgs@dlt
.com>
sub   2048R/4558B67D 2015-04-09

[root@ep-mgmt01 noarch]# rpm --resign rhsa-scap-1.0-2.el6.noarch.rpm
Enter pass phrase:
Pass phrase is good.
rhsa-scap-1.0-2.el6.noarch.rpm:

[root@ep-sat01 pub]# rhnpush -c rhsa-scap-el6 /tmp/rhsa-scap-1.0-2.el6.noarch.
rpm -o 2
Username: de
Password:
```

```
[root@localhost ~]# ls -l /usr/share/xml/scap/ssg/content
total 4780
-rw-r--r--. 1 root root     600 Aug 28  2014 ssg-rhel6-cpe-dictionary.xml
-rw-r--r--. 1 root root    3712 Aug 28  2014 ssg-rhel6-cpe-oval.xml
-rw-r--r--. 1 root root 2875837 Aug 28  2014 ssg-rhel6-ds.xml
-rw-r--r--. 1 root root  760158 Aug 28  2014 ssg-rhel6-oval.xml
-rw-r--r--. 1 root root 1242376 Aug 28  2014 ssg-rhel6-xccdf.xml
[root@localhost ~]# ls -l /usr/share/xml/scap/rhsa/
total 27976
-rw-r--r--. 1 root root  1776419 Apr  9 12:41 com.redhat.rhsa-all.xccdf.xml
-rw-r--r--. 1 root root 26869032 Apr  9 12:46 com.redhat.rhsa-all.xml
```

Scanning hosts



Scan list

Xccdf Test Result	Completed	Compliance	P	F	E	U	N	K	S	I	X	Total
xccdf_org.open-scap_testresult_default-profile	Thu Apr 23 13:31:51 EDT 2015	99 %	2544	21	0	0	0	0	0	0	0	2565
xccdf_org.open-scap_testresult_default-profile	Mon Apr 20 13:41:09 EDT 2015	99 %	2544	21	0	0	0	0	0	0	0	2565
xccdf_org.open-scap_testresult_xccdf_com.dlt.content_profile_C2S_baseline	Mon Apr 20 13:38:37 EDT 2015	46 %	88	91	0	1	0	10	210	0	0	400
xccdf_org.open-scap_testresult_xccdf_com.dlt.content_profile_C2S_baseline	Mon Apr 20 13:34:46 EDT 2015	46 %	88	91	0	1	0	10	210	0	0	400

Scan detail

XCCDF Rule Results

Filter by Result: Go Display 25 items per page 1 - 25 of 400

XCCDF Rule Identifier	XCCDF Ident Tags	Result
xccdf_org.ssgproject.content_rule_ensure_gpgcheck_never_disabled	CCE-26647-8	pass
xccdf_org.ssgproject.content_rule_aide_periodic_cron_checking	CCE-27222-9	pass
xccdf_org.ssgproject.content_rule_rpm_verify_hashes	CCE-27223-7	pass
xccdf_org.ssgproject.content_rule_mount_option_nodev_removable_partitions	CCE-26860-7	pass
xccdf_org.ssgproject.content_rule_mount_option_noexec_removable_partitions	CCE-27196-5	pass
xccdf_org.ssgproject.content_rule_mount_option_nosuid_removable_partitions	CCE-27056-1	pass
xccdf_org.ssgproject.content_rule_userowner_shadow_file	CCE-26947-2	pass
xccdf_org.ssgproject.content_rule_groupowner_shadow_file	CCE-26967-0	pass
xccdf_org.ssgproject.content_rule_file_permissions_etc_shadow	CCE-26992-8	pass
xccdf_org.ssgproject.content_rule_file_owner_etc_group	CCE-26822-7	pass
xccdf_org.ssgproject.content_rule_file_groupowner_etc_group	CCE-26930-8	pass
xccdf_org.ssgproject.content_rule_file_permissions_etc_group	CCE-26954-8	pass
xccdf_org.ssgproject.content_rule_file_owner_etc_gshadow	CCE-27026-4	pass
xccdf_org.ssgproject.content_rule_file_groupowner_etc_gshadow	CCE-26975-3	pass
xccdf_org.ssgproject.content_rule_file_permissions_etc_gshadow	CCE-26951-4	pass
xccdf_org.ssgproject.content_rule_file_owner_etc_passwd	CCE-26953-0	pass
xccdf_org.ssgproject.content_rule_file_groupowner_etc_passwd	CCE-26856-5	pass
xccdf_org.ssgproject.content_rule_file_permissions_etc_passwd	CCE-26868-0	pass
xccdf_org.ssgproject.content_rule_file_permissions_binary_dirs	CCE-27289-8	pass

Diff results

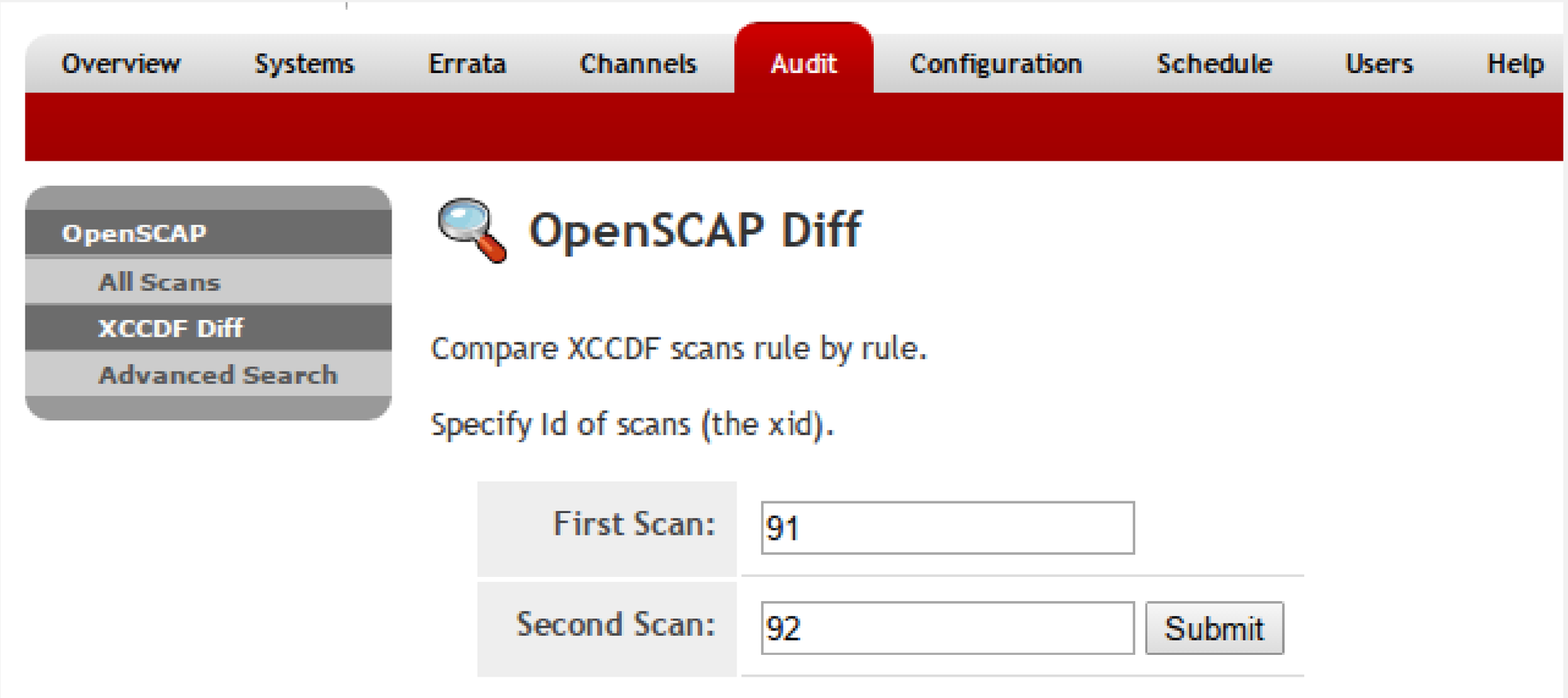
XCCDF Rule Results

Display 25 items per page

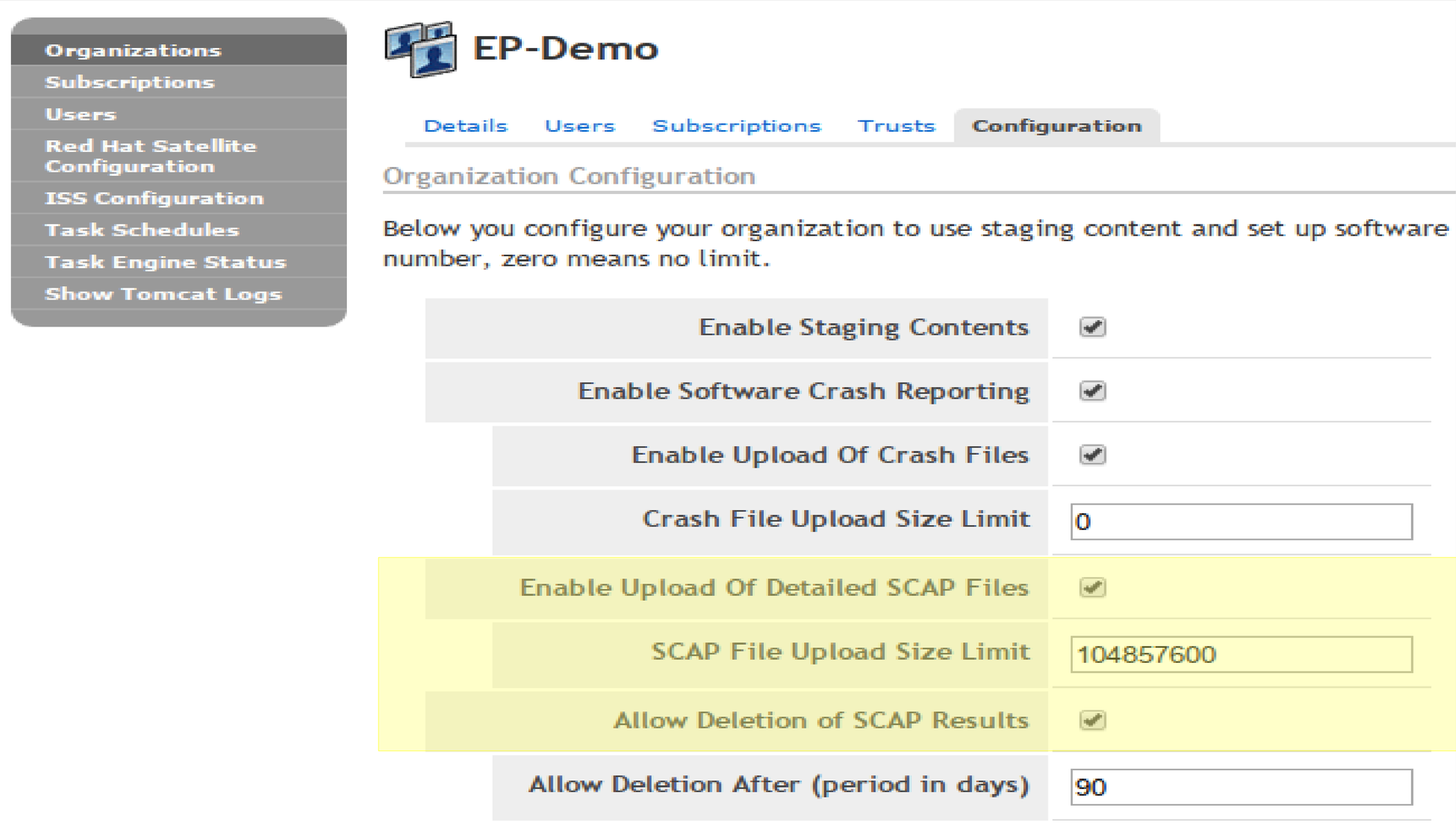
1 - 25 of 400

XCCDF Rule Identifier	First Scan	Second Scan
xccdf_org.ssgproject.content_rule_rpm_verify_hashes	pass	pass
xccdf_org.ssgproject.content_rule_file_permissions_etc_group	pass	pass
xccdf_org.ssgproject.content_rule_service_cgred_disabled	pass	notselected
xccdf_org.ssgproject.content_rule_set_password_hashing_algorithm_systemauth	fail	fail
xccdf_org.ssgproject.content_rule_dns_server_authenticate_zone_transfers	notselected	notselected
xccdf_org.ssgproject.content_rule_file_permissions_etc_gshadow	pass	pass
xccdf_org.ssgproject.content_rule_kernel_module_ipv6_option_disabled	fail	notselected
xccdf_org.ssgproject.content_rule_audit_rules_dac_modification_chmod	fail	notselected
xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_default_secure_redirects	fail	fail
xccdf_org.ssgproject.content_rule_sysctl_net_ipv4_conf_default_rp_filter	pass	pass
xccdf_org.ssgproject.content_rule_network_ipv6_disable_rpc	pass	notselected
xccdf_org.ssgproject.content_rule_ftp_present_banner	pass	notselected
xccdf_org.ssgproject.content_rule_ftp_log_transactions	pass	notselected
xccdf_org.ssgproject.content_rule_package_openswan_installed	fail	notselected
xccdf_org.ssgproject.content_rule_file_ownership_binary_dirs	pass	notselected
xccdf_org.ssgproject.content_rule_sysctl_kernel_randomize_va_space	fail	fail
xccdf_org.ssgproject.content_rule_sshd_limit_user_access	notchecked	notchecked
xccdf_org.ssgproject.content_rule_file_groupowner_etc_gshadow	pass	pass
xccdf_org.ssgproject.content_rule_service_auditd_enabled	notselected	pass

Diff to any!


Overview
Systems
Errata
Channels
Audit
Configuration
Schedule
Users
Help
OpenSCAP
All Scans
XCCDF Diff
Advanced Search
OpenSCAP Diff
Compare XCCDF scans rule by rule.
Specify Id of scans (the xid).
First Scan:
91
Second Scan:
92
Submit

Change some defaults



Detailed Report

Score

system	score	max	%	bar
urn:xccdf:scoring:default	67.51	100.00	67.51%	

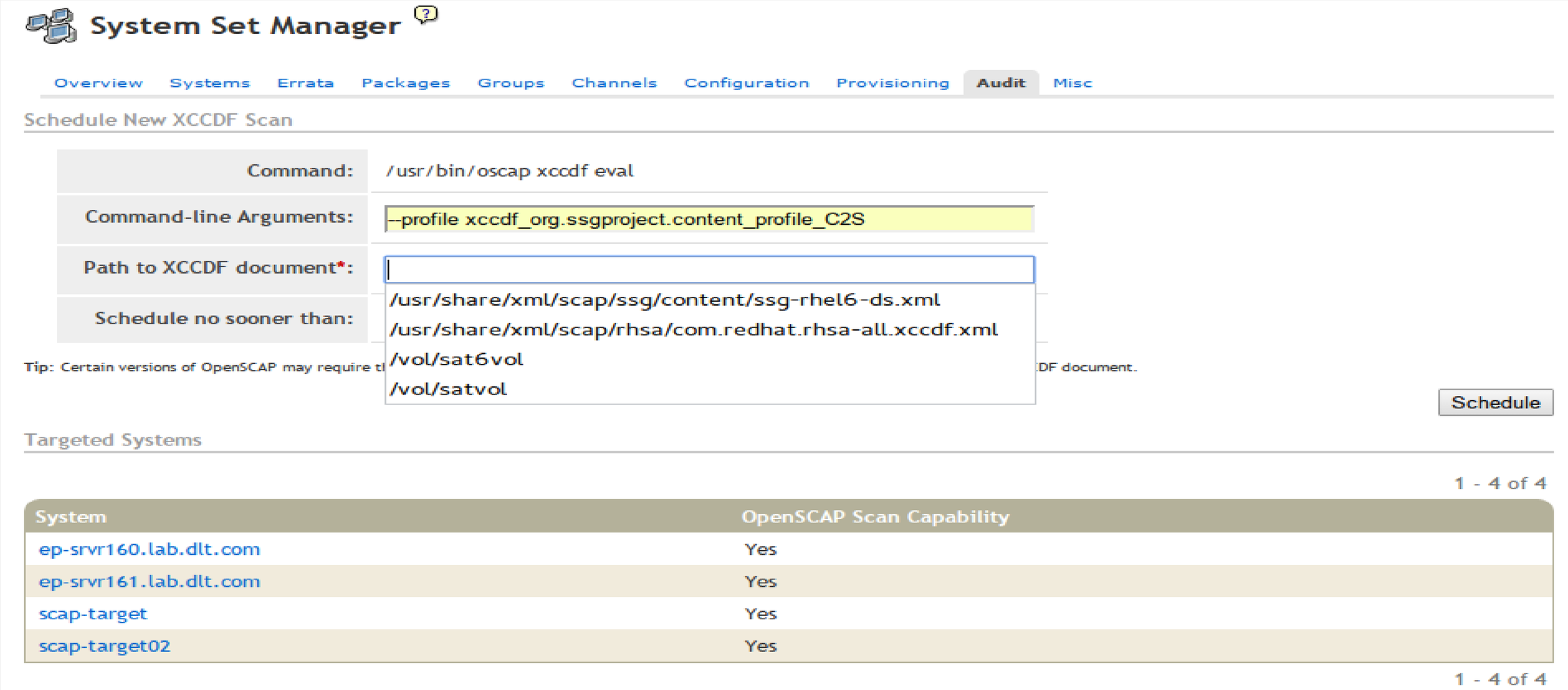
Results overview

Rule Results Summary

pass	fixed	fail	error	not selected	not checked	not applicable	informational	unknown	total
88	0	91	0	210	10	0	0	1	400

Title	Result
Ensure /tmp Located On Separate Partition	fail
Ensure /home Located On Separate Partition	fail
Ensure Red Hat GPG Key Installed	pass
Ensure gpgcheck Enabled In Main Yum Configuration	pass
Ensure gpgcheck Enabled For All Yum Package Repositories	pass
Install AIDE	fail
Disable Prelinking	fail
Build and Test AIDE Database	notchecked
Configure Periodic Execution of AIDE	pass
Verify and Correct File Permissions with RPM	fail
Verify File Hashes with RPM	pass
Add nodev Option to Non-Root Local Partitions	fail

Scanning groups with SSM



Scanning groups with SSM

Targeted Systems

1 - 6 of 6

System	OpenSCAP Scan Capability
ep-builder02.lab.dlt.com	No
ep-srvr160.lab.dlt.com	Yes
ep-srvr161.lab.dlt.com	Yes
ep-web01.lab.dlt.com	No
scap-target	Yes
scap-target02	Yes

1 - 6 of 6

OpenSCAP xccdf scanning

Details | Completed Systems | **In Progress Systems** | Failed Systems

In Progress Systems

1 - 4 of 4 (0 selected)

	System	Earliest execution	Base Channel
☐	ep-srvr160.lab.dlt.com	5/1/15 9:23:00 AM EDT	Red Hat Enterprise Linux Server (v. 6 for 64-bit x86_64)
☐	ep-srvr161.lab.dlt.com	5/1/15 9:23:00 AM EDT	Red Hat Enterprise Linux Server (v. 6 for 64-bit x86_64)
☐	scap-target	5/1/15 9:23:00 AM EDT	Red Hat Enterprise Linux Server (v. 6 for 64-bit x86_64)
☐	scap-target02	5/1/15 9:23:00 AM EDT	Red Hat Enterprise Linux Server (v. 6 for 64-bit x86_64)

Select All

1 - 4 of 4 (0 selected)

Unschedule Action

Advanced searches

CVE-2014-6271

OpenSCAP Search

OpenSCAP Search will return finished OpenSCAP scans from all scans you have access.

Specify your search criteria below.

Search XCCDF Rules For:	CVE-2014-6271 [Search] Examples: 'no_hashes_outside_shadow', 'CCE-14300-8'
With Result:	fail
Where to Search:	(•) Search all systems ( ) Search system set manager
Scan Dates to Search:	[x] Search Scans Performed Between Dates Start Date: April 26 2015 12 : 00 AM EDT End Date: April 30 2015 11 : 21 AM EDT
Show Search Result As:	( ) List of XCCDF Rule Results (•) List of XCCDF Scans

System built after scans

Filter by Xccdf Profile: Go Display 25 items per page 1 - 2 of 2

System	Xccdf Profile	Completed	Satisfied	Dissatisfied	Unknown
scap-target02	None	Wed Apr 29 13:37:15 EDT 2015	2472	93	0
scap-target02	None	Tue Apr 28 16:32:56 EDT 2015	2472	93	0

1 - 2 of 2

scap-target02

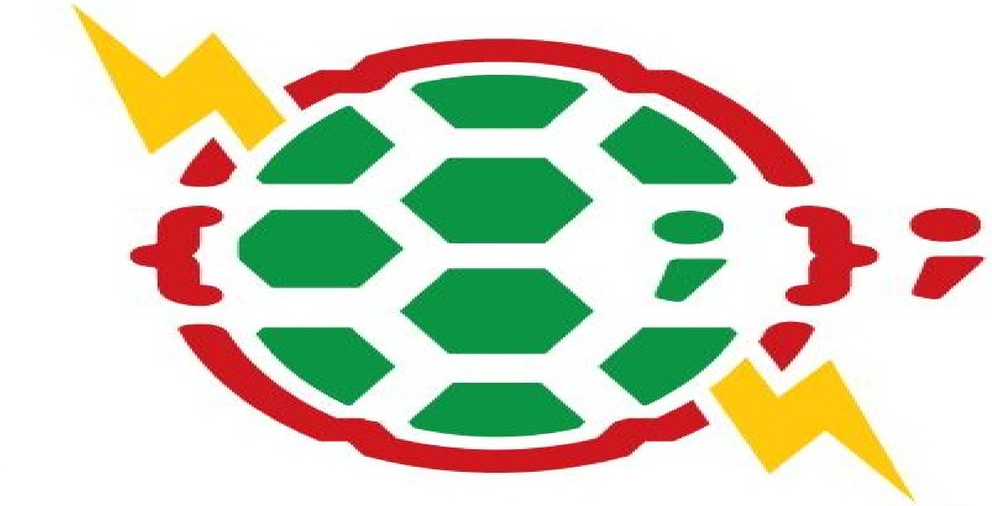
add to ssm | delete system

Details Software Configuration Provisioning Groups Audit Events

Overview Properties Remote Command Reactivation Hardware Migrate Notes Custom Info

System Events

Checked In:	4/29/15 3:11:01 PM EDT
Registered:	4/27/15 4:37:58 PM EDT
Last Booted:	4/27/15 4:40:10 PM EDT (Schedule System Reboot)
OSA Status:	offline as of 4/29/15 1:40:47 PM EDT Ping System



Automation

- Cron + Satellite **API**
- Use with a different **change manager**
- http://github.com/nzwulfin/rhsummit15

```
sysList = None
try:
  sysList = client.systemgroup.listSystemsMinimal(key, sysGroup)
  for system in sysList:
    try:
      client.system.scap.scheduleXccdfScan(key, system["id"], xccdf, oscap_opts)
    except Exception, detail:
      print 'Got API error: ', detail
      exit()
finally:
  client.auth.logout(key)
```

```
---
- name: SCAP scan host
  command: /root/bin/sat_scanGroup.py {{ sat_group_name }}
  async: 0
  poll: 0
  ignore_errors: true
```

SATELLITE 6 WORK FLOW

From Tailoring to Profile

```
<xccdf:Tailoring xmlns:xccdf="http://checklists.nist.gov/xccdf/1.2" id="xccdf_scap-
workbench_tailoring_default">
  <xccdf:benchmark href="/usr/share/xml/scap/ssg/content/ssg-rhel6-ds.xml"/>
  <xccdf:version time="2015-05-12T09:41:39">1</xccdf:version>
  <xccdf:Profile id="C2S_customized" extends="xccdf_org.ssgproject.content_profile_C2S">
```

```
17848      <refine-value idref="xccdf_org.ssgproject.content_value_var_umask_for_daemons" selector="027
           "/>
17849      <refine-value idref="xccdf_org.ssgproject.content_value_var_accounts_user_umask" selector="
           027"/>
17850      <refine-value idref="xccdf_org.ssgproject.content_value_var_accounts_maximum_age_login_defs"
            selector="90"/>
17851    </Profile>
17852    <Profile id="C2S_customized" extends="xccdf_org.ssgproject.content_profile_C2S">
17853      <title xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">C2S for Red Hat
           Enterprise Linux 6 [CUSTOMIZED]</title>
17854      <description xmlns:xhtml="http://www.w3.org/1999/xhtml" xml:lang="en-US">This profile
           demonstrates compliance against the
17855  U.S. Government Commercial Cloud Services (C2S) baseline with modifications made for OurCo.
17856
```

Upload Datastream

RED HAT SATELLITE

Default Organization@Default Location | Monitor | Content | Containers | Hosts | Configure | Infrastructure | Access Insights

SCAP Contents

Filter ... Search

Title
SSG_RHEL_7

File Upload | Locations | Organizations

Title * New_SG_Content

Scap file * Browse... No file selected.

Upload SCAP DataStream file

Notice: You need to install OpenSCAP on your hosts, and upload this content to the hosts as well.

Cancel Submit

Create scan profile

RED HAT SATELLITE

Default Organization@Default Location | Monitor | Content | Containers | Hosts | Configure | Infrastructure | Access Insights

New Compliance Policy

1 Create policy | 2 SCAP Content | 3 Schedule | 4 Locations | 5 Organizations | 6 Hostgroups

Name * SSG_For_RHEL_7_w_RHCCP_Profile

Description SCAP Security Guide for RHEL 7 with the Red Hat Certified Cloud Provider Policy

Create scan profile

RED HAT SATELLITE

Default Organization@Default Location | Monitor | Content | Containers | Hosts | Configure | Infrastructure | Access Insights

New Compliance Policy

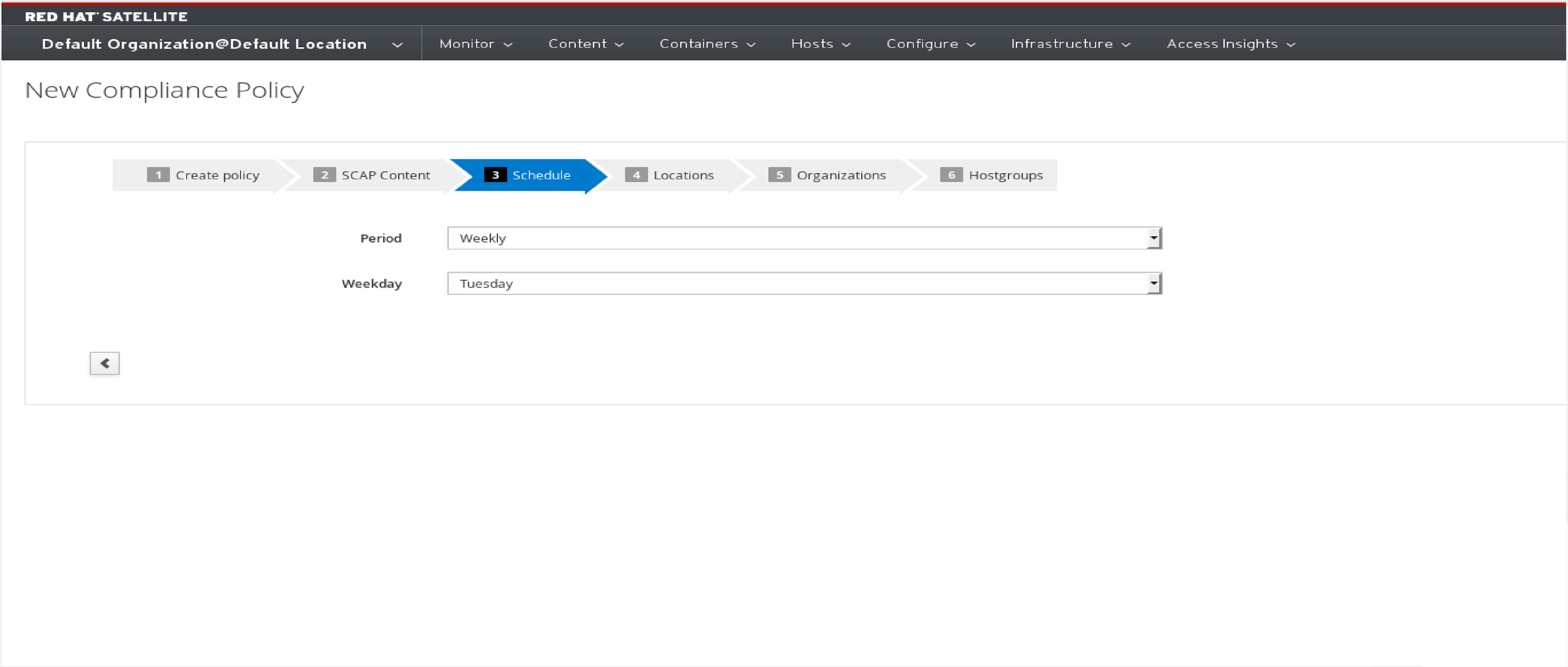
1 Create policy | 2 SCAP Content | 3 Schedule | 4 Locations | 5 Organizations | 6 Hostgroups

Scap content SSG_RHEL_7

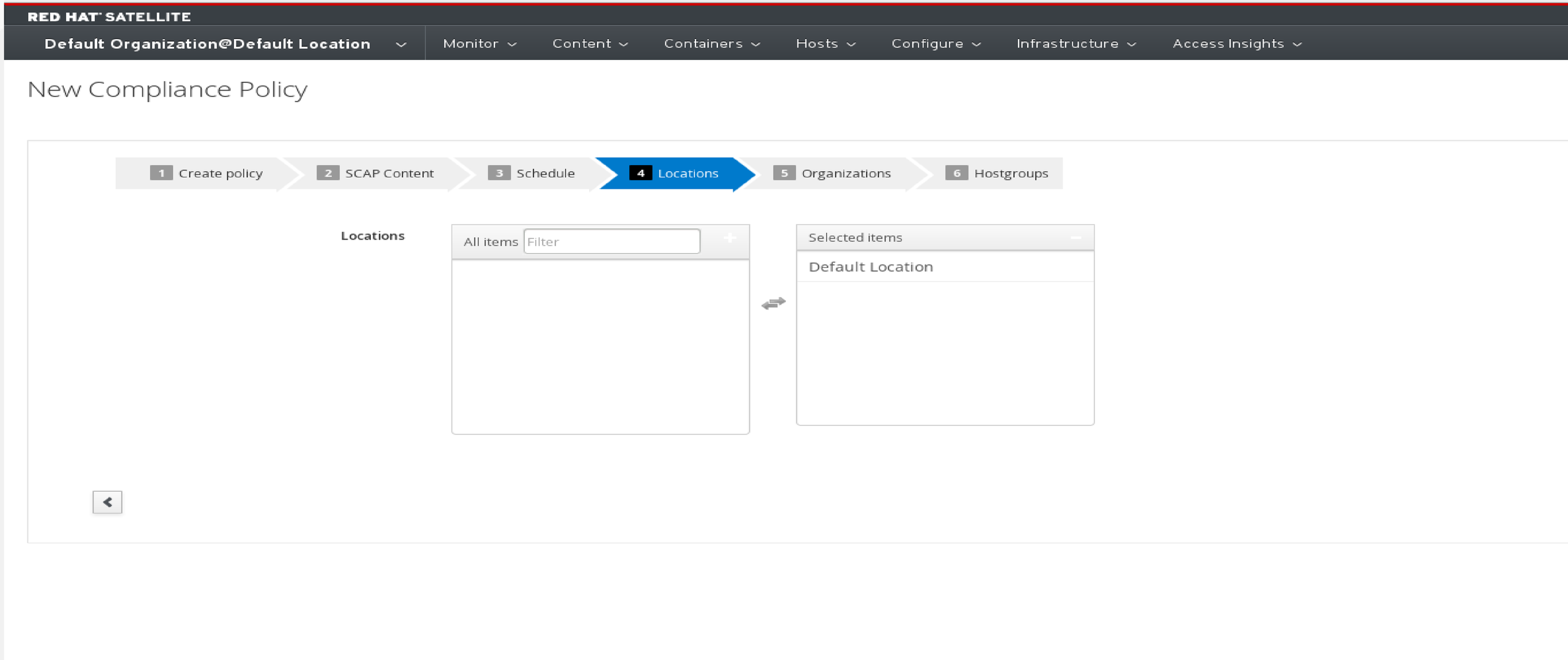
XCCDF Profile Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)

Notice: Ensure the selected SCAP content exists on your hosts.

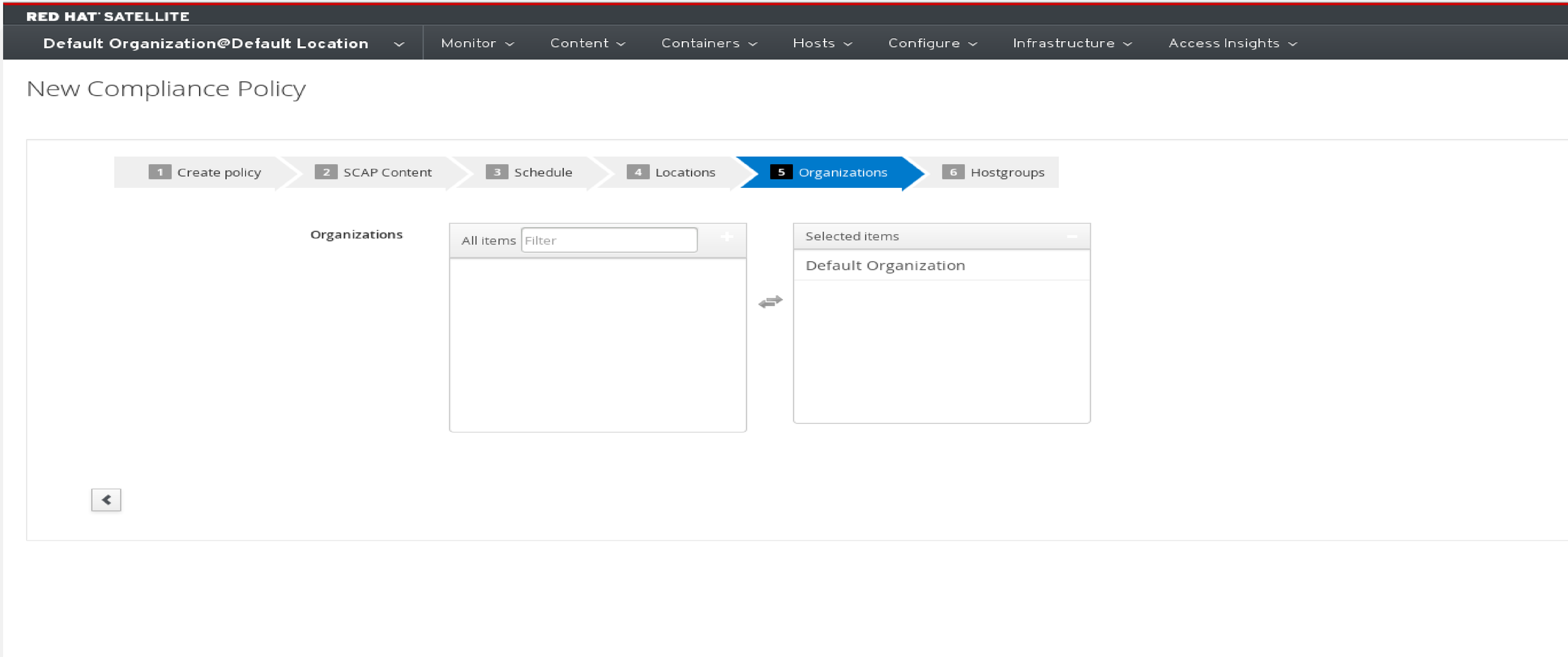
Create scan profile



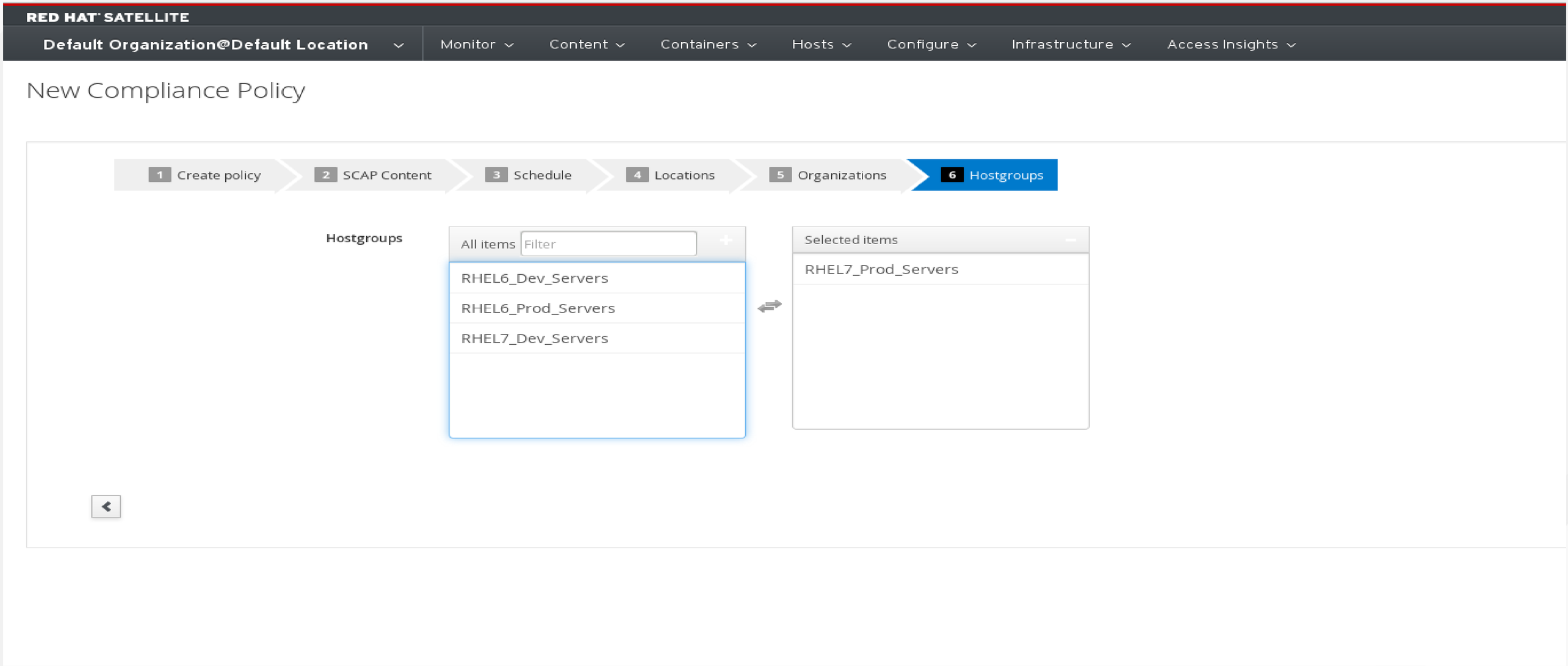
Create scan profile



Create scan profile



Create scan profile



Reporting

Compliance Policies – Mozilla Firefox (Build 20150416103922)

File Edit View History Bookmarks Tools Help

Compliance Policies

https://bldr15ca01.core.cmbu.redhat.com/compliance/policies

RED HAT SATELLITE

Red Hat Access | Admin User

Default Organization@Default Location | Monitor | Content | Containers | Hosts | Configure | Infrastructure | Access Insights | Administer

Compliance Policies

Filter ... | Search | New Compliance Policy | Help

Name	Content	Profile	
SCAP_Security_Guide_for_RHEL_6	SSG_RHEL_6	Default	Show Guide
SCAP_Security_Guide_for_RHEL_7	SSG_RHEL_7	Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)	Show Guide
SSG_For_RHEL_7_w_RHCCP_Profile	SSG_RHEL_7	Red Hat Corporate Profile for Certified Cloud Providers (RH CCP)	Show Guide

Reporting

Compliance policy: SCAP_Security_Guide_for_RHEL_7 – Mozilla Firefox (Build 20150416103922)

File Edit View History Bookmarks Tools Help

Compliance policy: SCAP_S...

https://bldr15ca01.core.cmbu.redhat.com/compliance/policies/2/dashboard

RED HAT SATELLITE

Red Hat Access | Admin User

Default Organization@Default Location | Monitor | Content | Containers | Hosts | Configure | Infrastructure | Access Insights | Administer

Compliance policy: SCAP_Security_Guide_for_RHEL_7

Hosts Breakdown

Compliant with the policy	0
Not compliant with the policy	2
Inconclusive results	0
Never audited	0

Total hosts: 2

Host Breakdown Chart

Latest reports for policy: SCAP_Security_Guide_for_RHEL_7

Host	Date	Passed	Failed	Other	
devnode-0003.example.com	8 days ago	34	33	1	View Report
devnode-0004.example.com	8 days ago	34	33	1	View Report
devnode-0003.example.com	8 days ago	34	33	1	View Report
devnode-0003.example.com	8 days ago	34	33	1	View Report

Reporting

Mozilla Firefox (Build 20150416103922)

File Edit View History Bookmarks Tools Help

https://bldr15...rf_reports/22

https://bldr15ca01.core.cmbu.redhat.com/compliance/arf_reports/22

RED HAT SATELLITE — Red Hat Access — Admin User

Default Organization@Default Location — Monitor — Content — Containers — Hosts — Configure — Infrastructure — Access Insights — Administer

OpenSCAP Evaluation Report

Evaluation Characteristics

Target machine	devnode-0003.example.com
Benchmark URL	/var/lib/openscap/content /1fbdc87d24db51ca184419a2b6f7018f1361c27cd818755d5bc4f5b08fed0a7c.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_RHEL-7
Profile ID	xccdf_org.ssgproject.content_profile_rht-ccp
Started at	2015-04-29T01:00:02
Finished at	2015-04-29T01:00:05
Performed by	root

CPE Platforms

- cpe:/o:redhat:enterprise_linux:7
- cpe:/o:redhat:enterprise_linux:7::client

Addresses

- IPv4 127.0.0.1
- IPv4 192.168.124.111
- IPv6 0:0:0:0:0:0:0:1
- IPv6 fe80:0:0:0:5054:ff:fedf:d6e9
- MAC 00:00:00:00:00:00
- MAC 52:54:00:DF:D6:E9

Compliance and Scoring

The target system did not satisfy the conditions of 33 rules! Please review rule results and consider applying remediation.

Rule results

34 passed | 33 failed | 1

Severity of failed rules

12 low | 17 medium | 4 high

Reporting

Mozilla Firefox (Build 20150416103922)

File Edit View History Bookmarks Tools Help

https://bldr15...rf_reports/22

https://bldr15ca01.core.cmbu.redhat.com/compliance/arf_reports/22

RED HAT SATELLITE — Red Hat Access — Admin User

Default Organization@Default Location — Monitor — Content — Containers — Hosts — Configure — Infrastructure — Access Insights — Administer

Rule results

34 passed | 33 failed | 1

Severity of failed rules

12 low | 17 medium | 4 high

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	66.064819	100.000000	66.06%

Rule Overview

- [x] pass
- [x] fail
- [x] notchecked
- [x] fixed
- [x] error
- [ ] notselected
- [x] informational
- [x] unknown
- [x] notapplicable

Search through XCCDF rules — Search

Title	Severity	Result
Guide to the Secure Configuration of Red Hat Enterprise Linux 7 (33x fail) (1x notchecked)		
Introduction		
System Settings (25x fail) (1x notchecked)		
Installing and Maintaining Software (6x fail) (1x notchecked)		
Disk Partitioning (4x fail)		
Ensure /tmp Located On Separate Partition	low	fail
Ensure /var Located On Separate Partition	low	fail
Ensure /var/log Located On Separate Partition	low	fail

Install tools on client

RED HAT SATELLITE

Red Hat Access | Richard Jerrido

Default Organization@Default Location | Monitor | Content | Containers | Hosts | Configure | Infrastructure | Access Insights | Administer

Edit RHEL7_Dev_Servers

Host Group | Puppet Classes | Network | Operating System | Parameters | Locations | Organizations | Activation Keys

Included Classes

motd
foreman_scap_client

Available Classes

Filter classes

+ access_insights_client
+ foreman_scap_client
motd
+ stdlib

Cancel | Submit

RED HAT SUMMIT

LEARN. NETWORK.
EXPERIENCE OPEN SOURCE.

Matt Micene
Solution Architect, DLT Solutions

@cleverbeard

@nzwulfin

Resources

- John Boyd and the OODA Loop
- Satellite API scripts and RPM spec file
- OpenSCAP Github Organization
- Red Hat Security Data site
- Red Hat Security RHSA Checklist
- Anton Chuvakin: Highlights from '14 Verizon PCI Report
- NIST Validated SCAP tools