Accrediting OpenShift

SHAWN WELLS
Director, Innovation Programs
U.S. Public Sector

unclass: shawn@redhat.com
JWICS: sdwell2@nsa.ic.gov
(+1) 443-534-0130

30 MINUTES, 3 GOALS

1. Review OpenShift Multi-Tenancy
    - sVirt
    - MCS & Type Enforcement
2. Current compliance tech + initiatives
    - U.S. Army Configuration, SCAP Security Guide (SSG)
    - Host/Tenant Security Boundary Model
3. Future Plans (discussion)
    - OpenShift NIST Baseline
    - OpenShift STIG, hardened cartridges

OpenShift Multi-tenancy

- Think of the gears as boxes, nodes as the truck
- We don't care what's inside the box, it's just cargo

OpenShift Multi-tenancy

RHEL

HYPERVISOR (RHEV, OpenStack, KVM...)

OpenShift Multi-tenancy

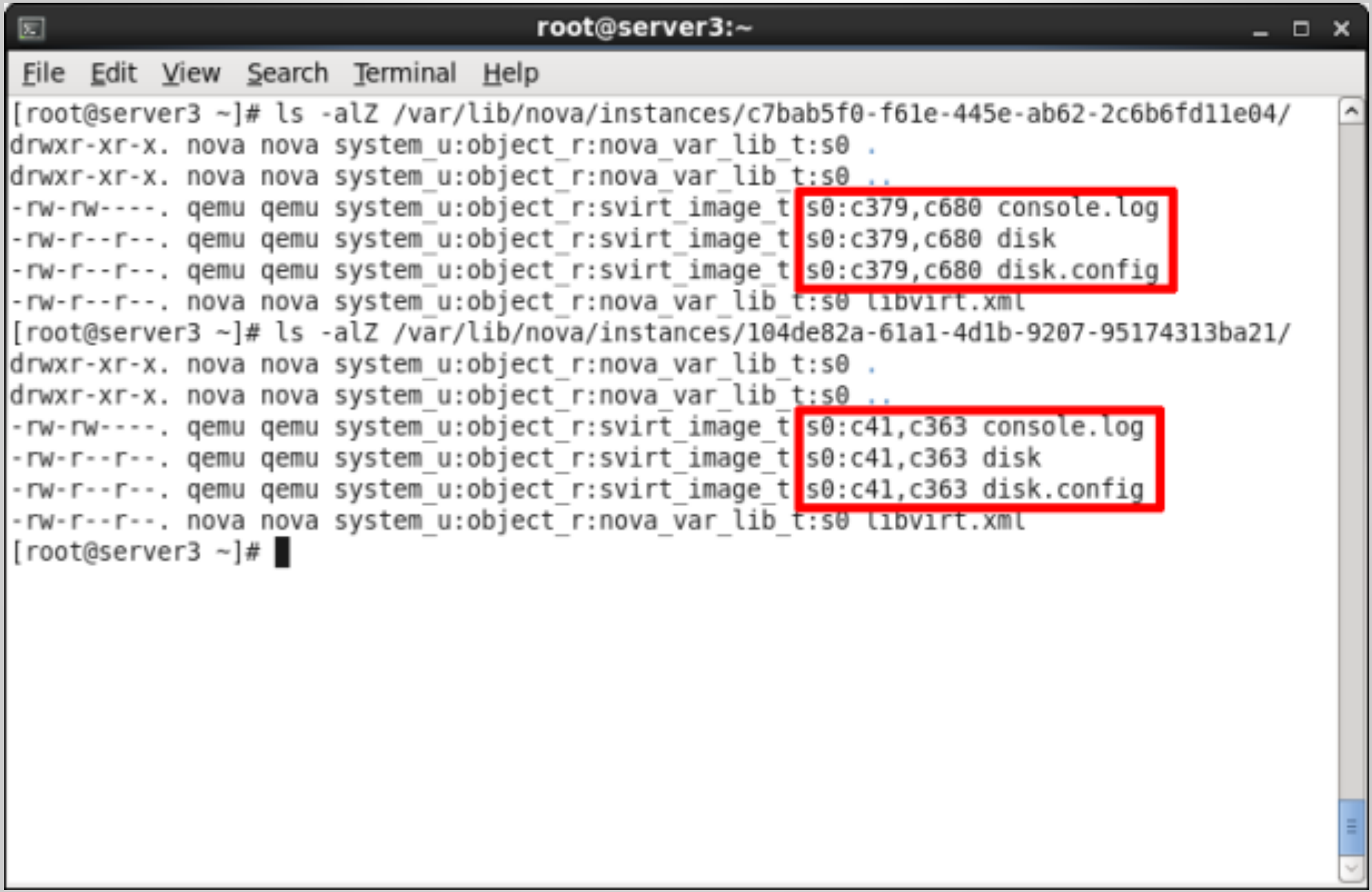
system_u:system_r:svirt_t:s0:c379,c680

system_u:system_r:svirt_t:s0:c41,c368

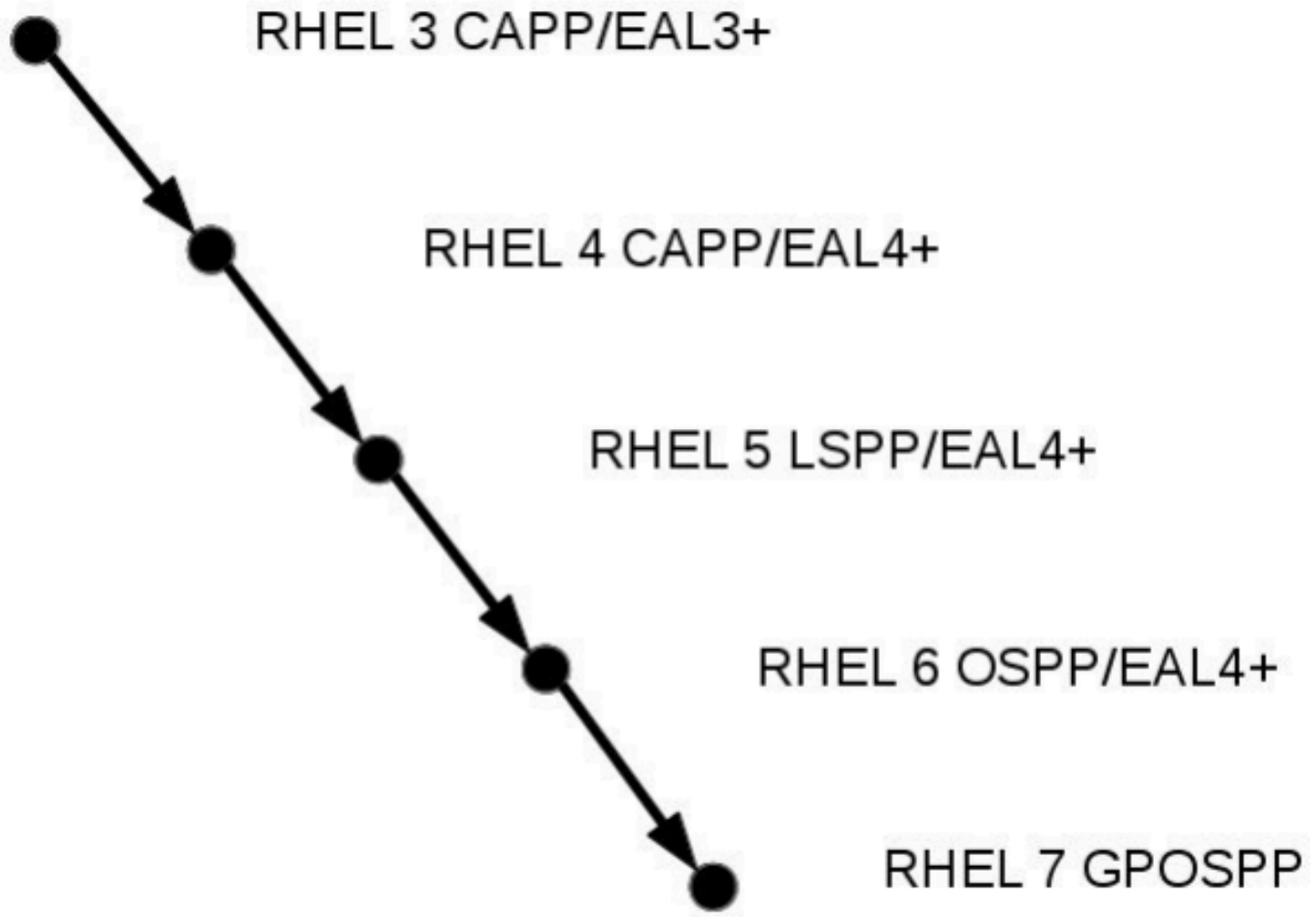
RHEL

HYPERVISOR (RHEV, OpenStack, KVM...)

OpenShift Multi-tenancy



Collaboration with NSA C63 (aka NIAP): where we've been… and next stop



	Red Hat Enterprise Linux 6 with KVM	Red Hat Enterprise Linux 5.6 with KVM	IBM z/VM Version 5 Release 3 (for IBM System z Mainframes)	VMWare vSphere 5.0	VMWare ESXi 4.1	Microsoft Windows Server 2008 Hyper-V Role with HotFix KB950050
Certification Date	2012-10-08	2012-04-20	2008-08-06	2012-05-18	2010-12-15	2009-07-24
EAL Level	EAP4+	EAP4+	EAP4+	EAP4+	EAP4+	EAP4+
CAPP	YES	YES	YES	NO	NO	NO
RBAC	YES	YES	NO	NO	NO	NO
LSPP	YES	YES	YES	NO	NO	NO

CAPP: Users control data access'
RBAC: Users classified into roles ("BackupAdm," "AuditAdm"...)
LSPP: Compartmentalizes users and applications from each other. Enables MLS.

Source: http://www.commoncriteriaportal.org/

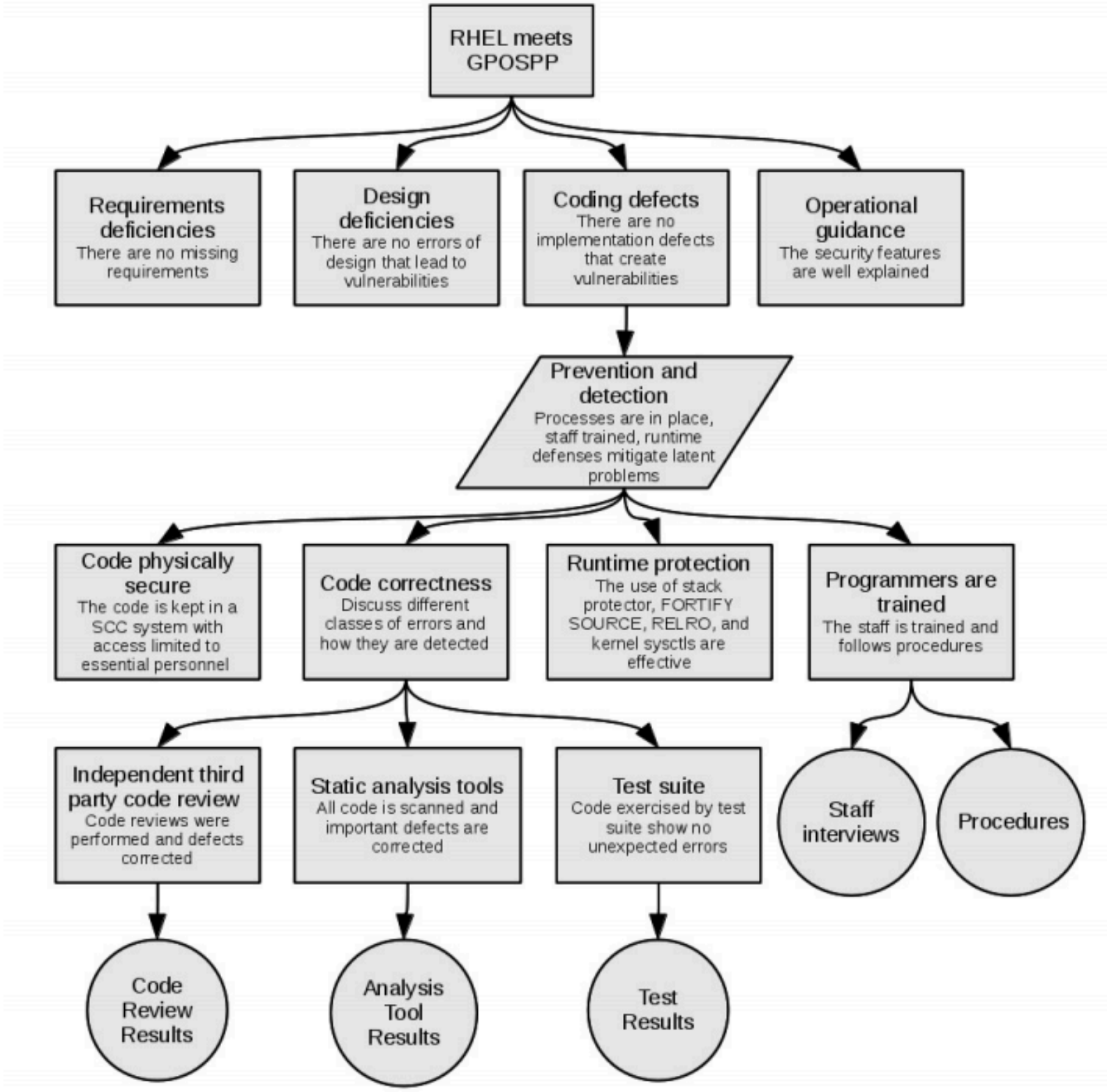
Red Hat® OpenShift Configuration Guide

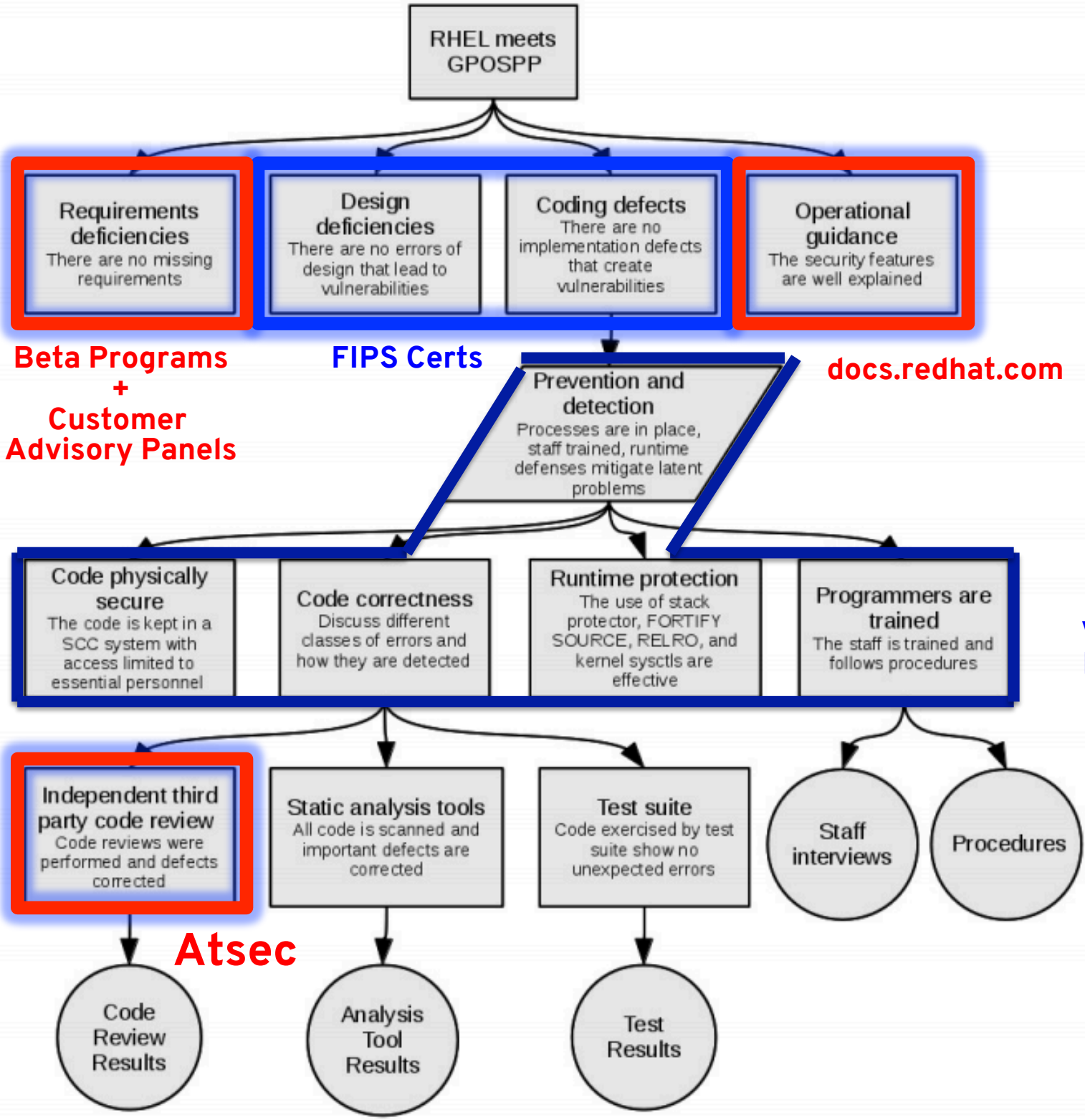
March 2014

ASA (ALT)
1400 Defense Pentagon
Washington DC 20301-1400

http://www.army.mil/asalt/

TABLE OF CONTENTS


RHEL meets GPOSPP
Requirements deficiencies
There are no missing requirements
Design deficiencies
There are no errors of design that lead to vulnerabilities
Coding defects
There are no implementation defects that create vulnerabilities
Operational guidance
The security features are well explained
Prevention and detection
Processes are in place, staff trained, runtime defenses mitigate latent problems
Code physically secure
The code is kept in a SCC system with access limited to essential personnel
Code correctness
Discuss different classes of errors and how they are detected
Runtime protection
The use of stack protector, FORTIFY SOURCE, RELRO, and kernel sysctls are effective
Programmers are trained
The staff is trained and follows procedures
Independent third party code review
Code reviews were performed and defects corrected
Static analysis tools
All code is scanned and important defects are corrected
Test suite
Code exercised by test suite show no unexpected errors
Staff interviews
Procedures
Code Review Results
Analysis Tool Results
Test Results


RHEL meets GPOSPP
Requirements deficiencies
There are no missing requirements
Design deficiencies
There are no errors of design that lead to vulnerabilities
Coding defects
There are no implementation defects that create vulnerabilities
Operational guidance
The security features are well explained
Beta Programs + Customer Advisory Panels
FIPS Certs
docs.redhat.com
Prevention and detection
Processes are in place, staff trained, runtime defenses mitigate latent problems
Code physically secure
The code is kept in a SCC system with access limited to essential personnel
Code correctness
Discuss different classes of errors and how they are detected
Runtime protection
The use of stack protector, FORTIFY SOURCE, RELRO, and kernel sysctls are effective
Programmers are trained
The staff is trained and follows procedures
Value of Red Hat
Independent third party code review
Code reviews were performed and defects corrected
Static analysis tools
All code is scanned and important defects are corrected
Test suite
Code exercised by test suite show no unexpected errors
Staff interviews
Procedures
Atsec
Code Review Results
Analysis Tool Results
Test Results

Common Criteria

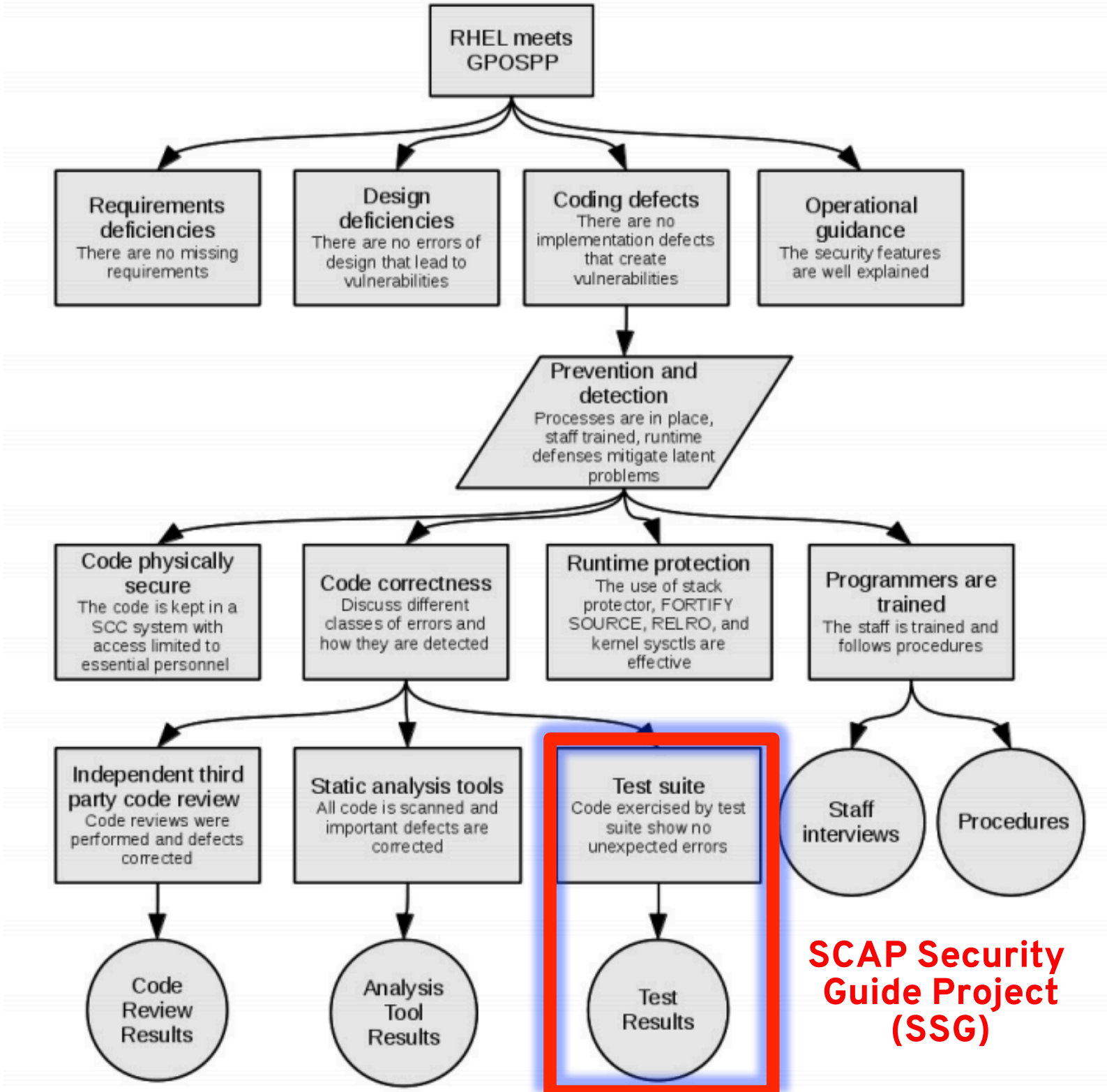
!=

Compliance Policy

STIG

==

Compliance Policy


RHEL meets GPOSPP
Requirements deficiencies
There are no missing requirements
Design deficiencies
There are no errors of design that lead to vulnerabilities
Coding defects
There are no implementation defects that create vulnerabilities
Operational guidance
The security features are well explained
Prevention and detection
Processes are in place, staff trained, runtime defenses mitigate latent problems
Code physically secure
The code is kept in a SCC system with access limited to essential personnel
Code correctness
Discuss different classes of errors and how they are detected
Runtime protection
The use of stack protector, FORTIFY SOURCE, RELRO, and kernel sysctls are effective
Programmers are trained
The staff is trained and follows procedures
Independent third party code review
Code reviews were performed and defects corrected
Static analysis tools
All code is scanned and important defects are corrected
Test suite
Code exercised by test suite show no unexpected errors
Staff interviews
Procedures
Code Review Results
Analysis Tool Results
Test Results
SCAP Security Guide Project (SSG)

SCAP Security Guide

Community In a Nutshell:

… has had 7,149 commits from 104 contributors,
representing 1,641,075 lines of source

… has become upstream for
all Red Hat DISA FSO (aka, STIG) content,
all Red Hat NIST baselines,
all Red Hat USGCB content,
NSA and CIA RHEL baselines,
OpenShift work just beginning

… As of October 2014, ships natively
in RHEL 6.6 and 7.1

AC-19(e)	Disable GNOME Automounting	The system's default desktop environment, GNOME, will mount devices and rem inserted into the system. Disable automount and autorun within GNOME by run
		
		`# gconftool-2 --direct \`
		`--config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory`
		`--type bool \`
		`--set /apps/nautilus/preferences/media_automount false`
		`# gconftool-2 --direct \`
		`--config-source xml:readwrite:/etc/gconf/gconf.xml.mandatory`
		`--type bool \`
		`--set /apps/nautilus/preferences/media_autorun_never true`
		
		These settings can be verified by running the following:
		
		`$ gconftool-2 --direct \`
		`--config-source xml:read:/etc/gconf/gconf.xml.mandatory \`
		`--get /apps/nautilus/preferences/media_automount`
		`$ gconftool-2 --direct \`
		`--config-source xml:read:/etc/gconf/gconf.xml.mandatory \`
		`--get /apps/nautilus/preferences/media_autorun_never`

CM-7	Disable Mounting of cramfs	To configure the system to prevent the `cramfs` kernel module from being loaded `install cramfs /bin/false` This effectively prevents usage of this uncommon filesystem.
CM-7	Disable Mounting of freevxfs	To configure the system to prevent the `freevxfs` kernel module from being load `install freevxfs /bin/false` This effectively prevents usage of this uncommon filesystem.
CM-7	Disable Mounting of jffs2	To configure the system to prevent the `jffs2` kernel module from being loaded, `install jffs2 /bin/false` This effectively prevents usage of this uncommon filesystem.

oval:com.redhat.rhsa:def:20130744	true	patch	RHSA-2013:0744-01 CVE-2012-6537 CVE-2012-6538 CVE-2012-6546 CVE-2012-6547 CVE-2013-0349 CVE-2013-0913 CVE-2013-1767 CVE-2013-1773 CVE-2013-1774 CVE-2013-1792 CVE-2013-1796 CVE-2013-1797 CVE-2013-1798 CVE-2013-1826 CVE-2013-1827	RHSA-2013:0744: kernel security and bug fix update (Important)
oval:com.redhat.rhsa:def:20130898	false	patch	RHSA-2013:0898-00 CVE-2013-1993	RHSA-2013:0898: mesa security update (Moderate)
oval:com.redhat.rhsa:def:20130896	false	patch	RHSA-2013:0896-00 CVE-2013-2007	RHSA-2013:0896: qemu-kvm security and bug fix update (Moderate)

Shawn Wells
shawn@redhat.com || sdwell2@nsa.ic.gov
443-534-0130