



COMPLIANCE MADE EASY

SHAWN WELLS

unclass: shawn@redhat.com

JWICS: wellsha@nro.ic.gov

NSA: sdwell2@nsa.ic.gov

(+1) 443-534-0130

60 MINUTES, 2 GOALS

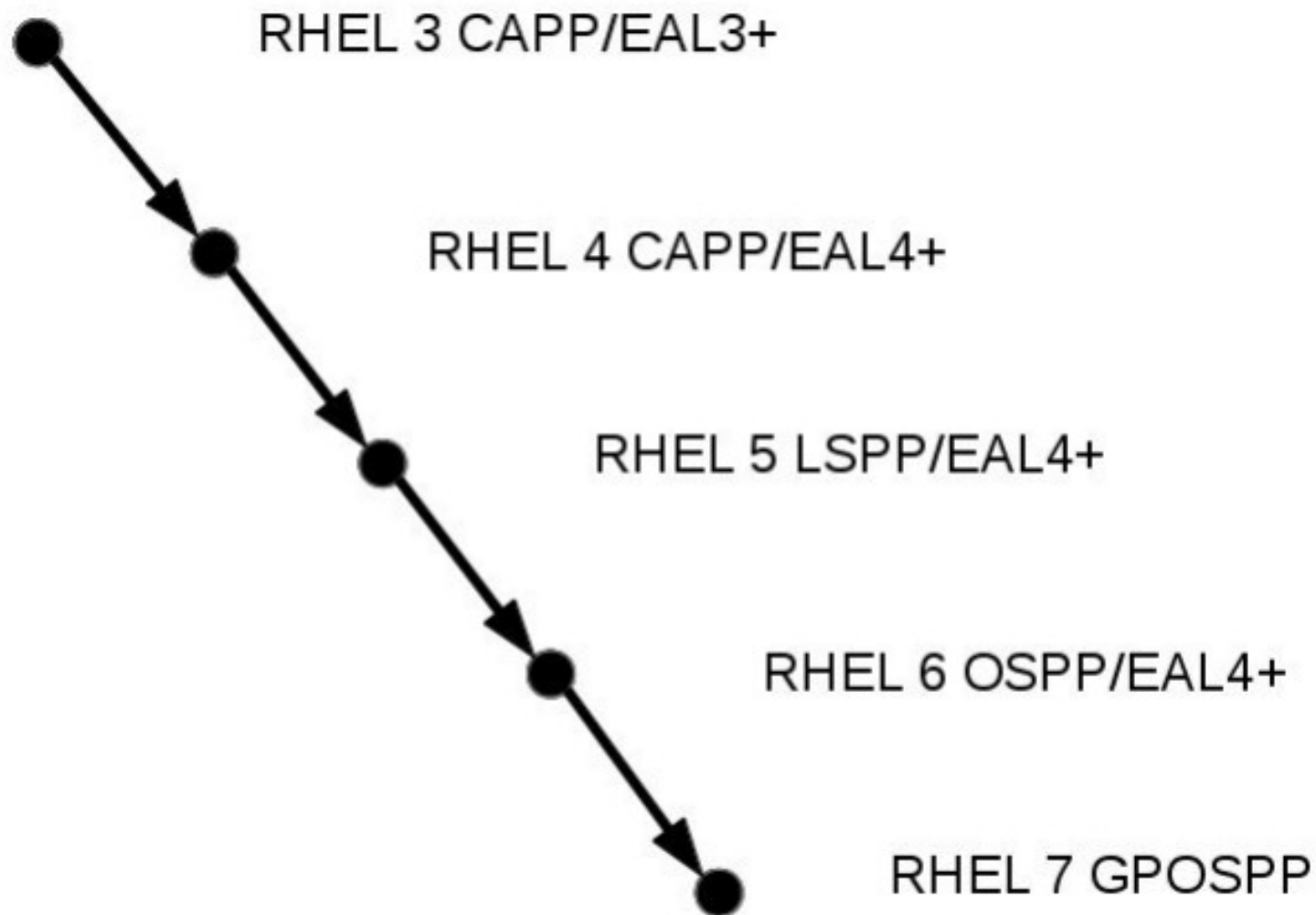
1. Review compliance tech + initiatives

- Upstream: SCAP Security Guide (SSG)
- Downstream: NSA SNAC Guides & STIGs

2. SCAP Demo

- OpenSCAP + SSG
- C&A Document Generation

NSA C63 (aka NIAP) & Red Hat: where we've been... and next stop

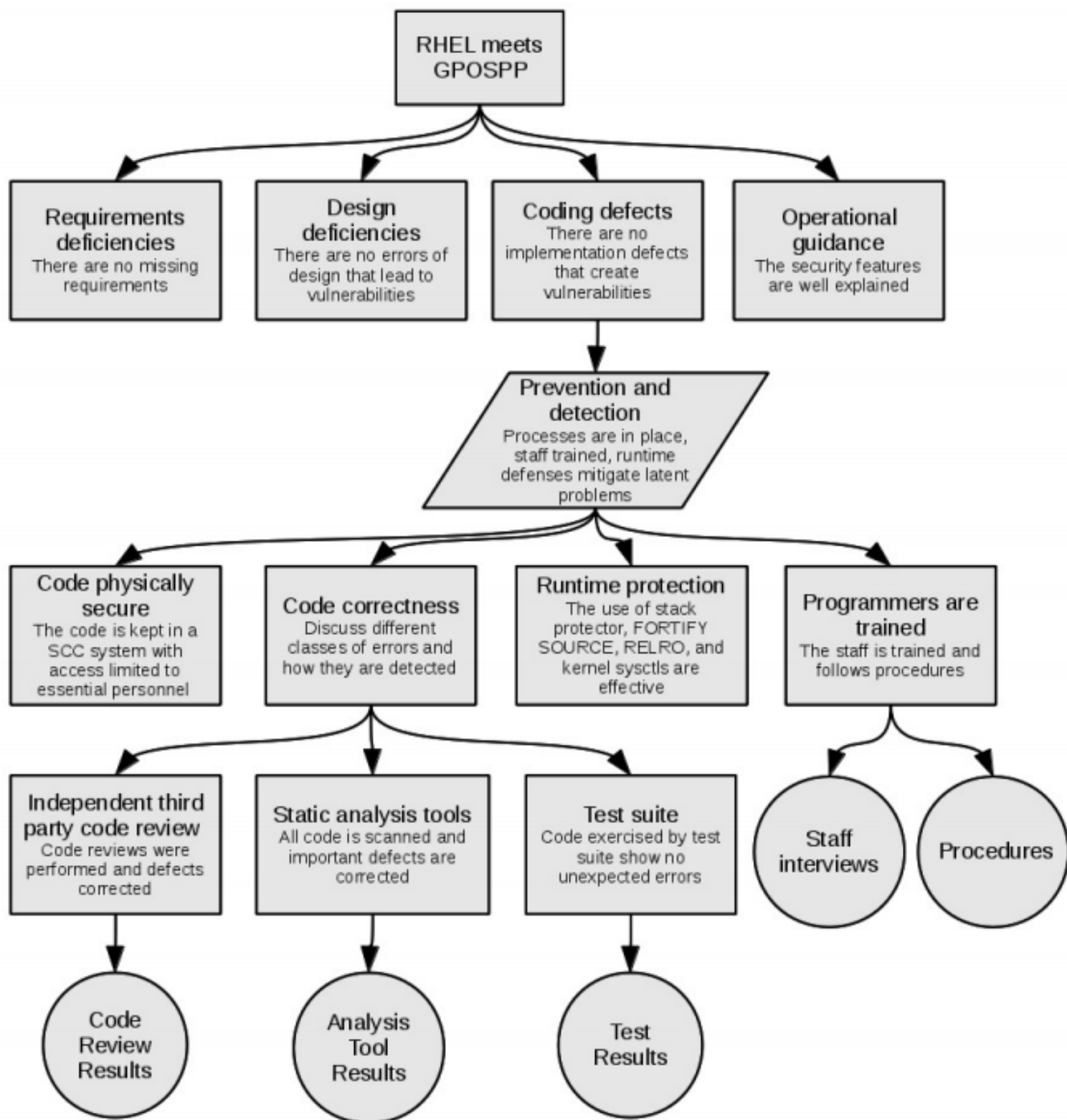


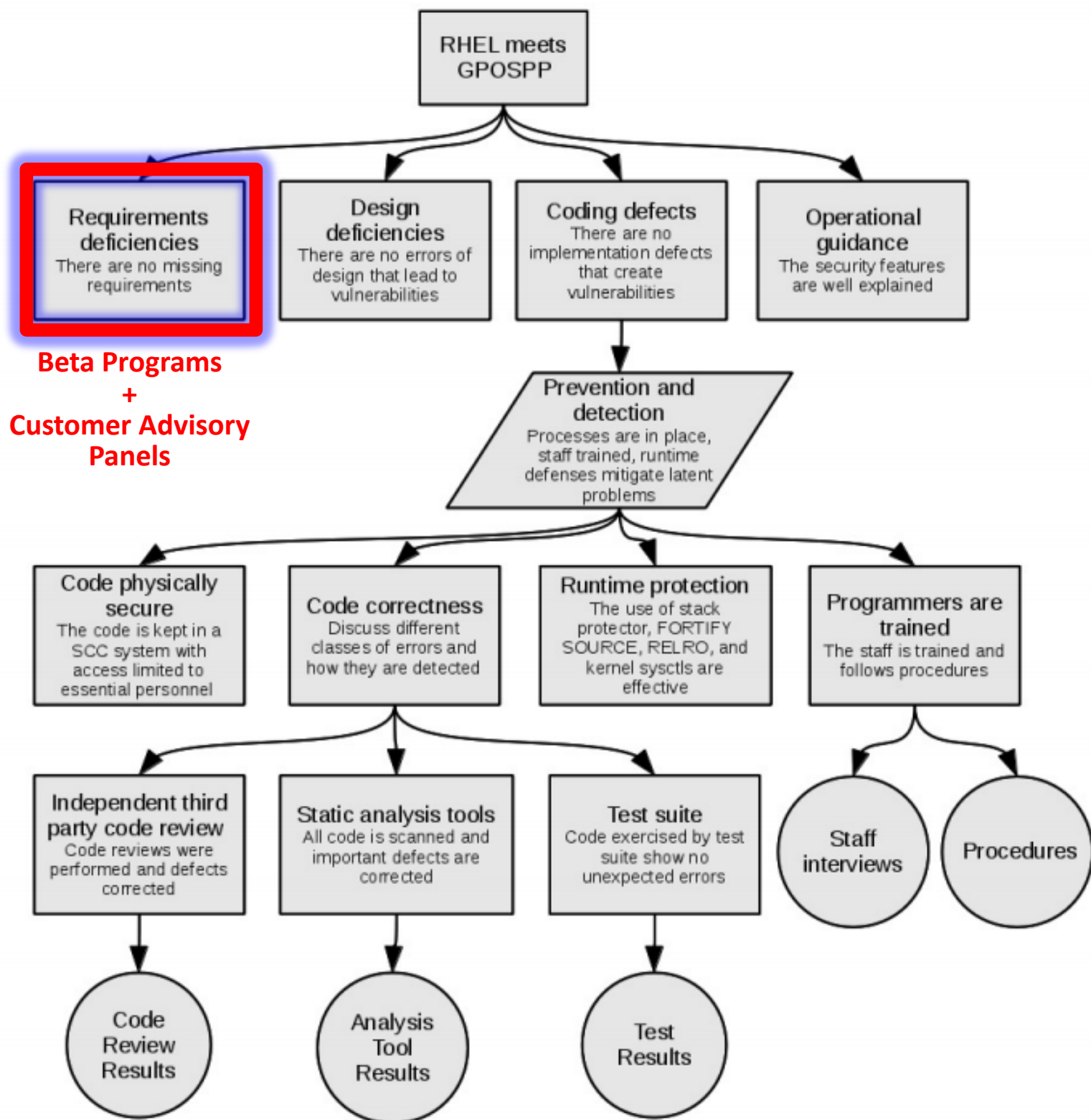
	Red Hat Enterprise Linux 6 with KVM	Red Hat Enterprise Linux 5.6 with KVM	IBM z/VM Version 5 Release 3 (for IBM System z Mainframes)	VMWare vSphere 5.0	VMWare ESXi 4.1	Microsoft Windows Server 2008 Hyper-V Role with HotFix KB950050
Certification Date	2012-10-08	2012-04-20	2008-08-06	2012-05-18	2010-12-15	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

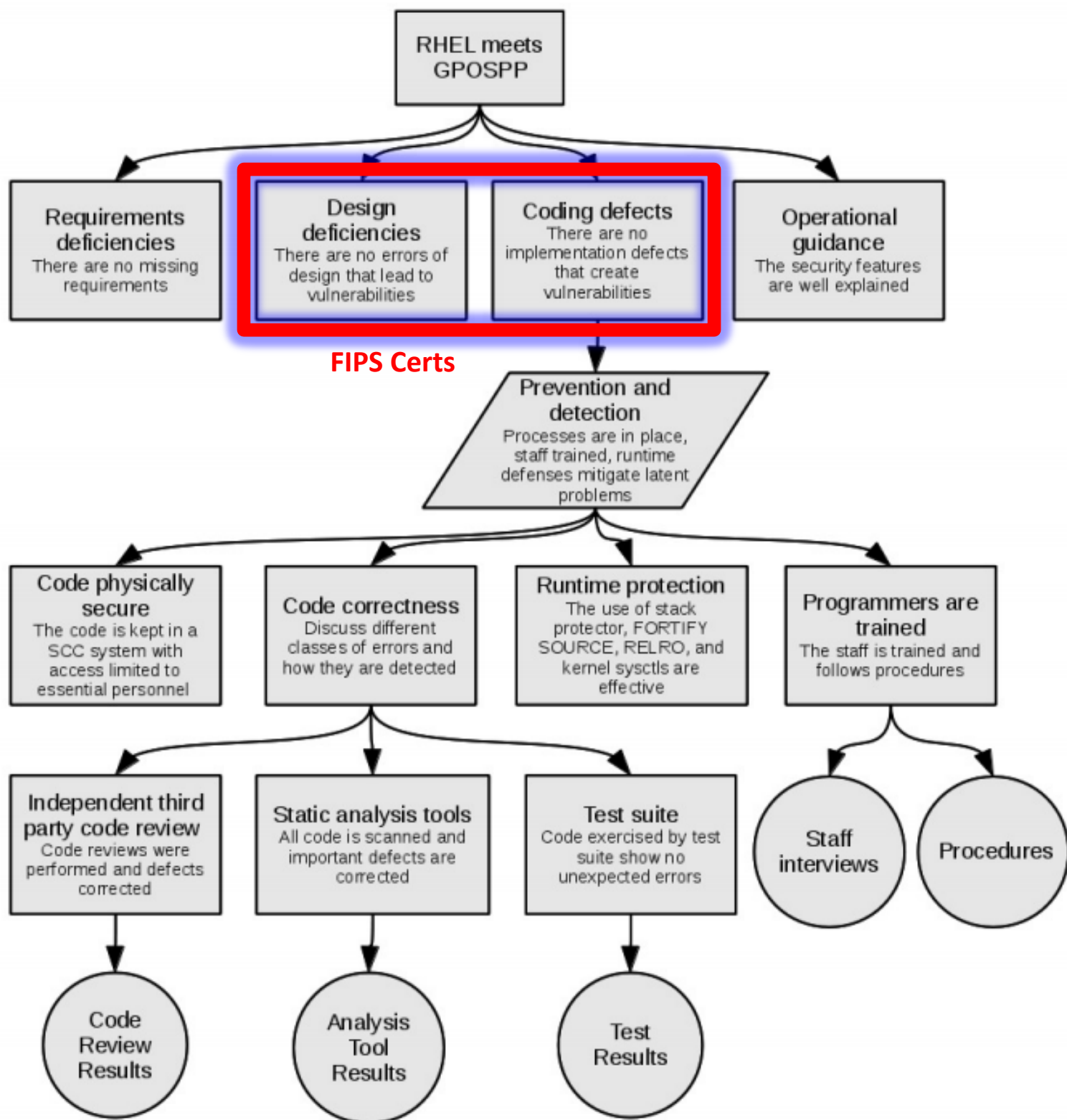
CAPP: Users control data access'

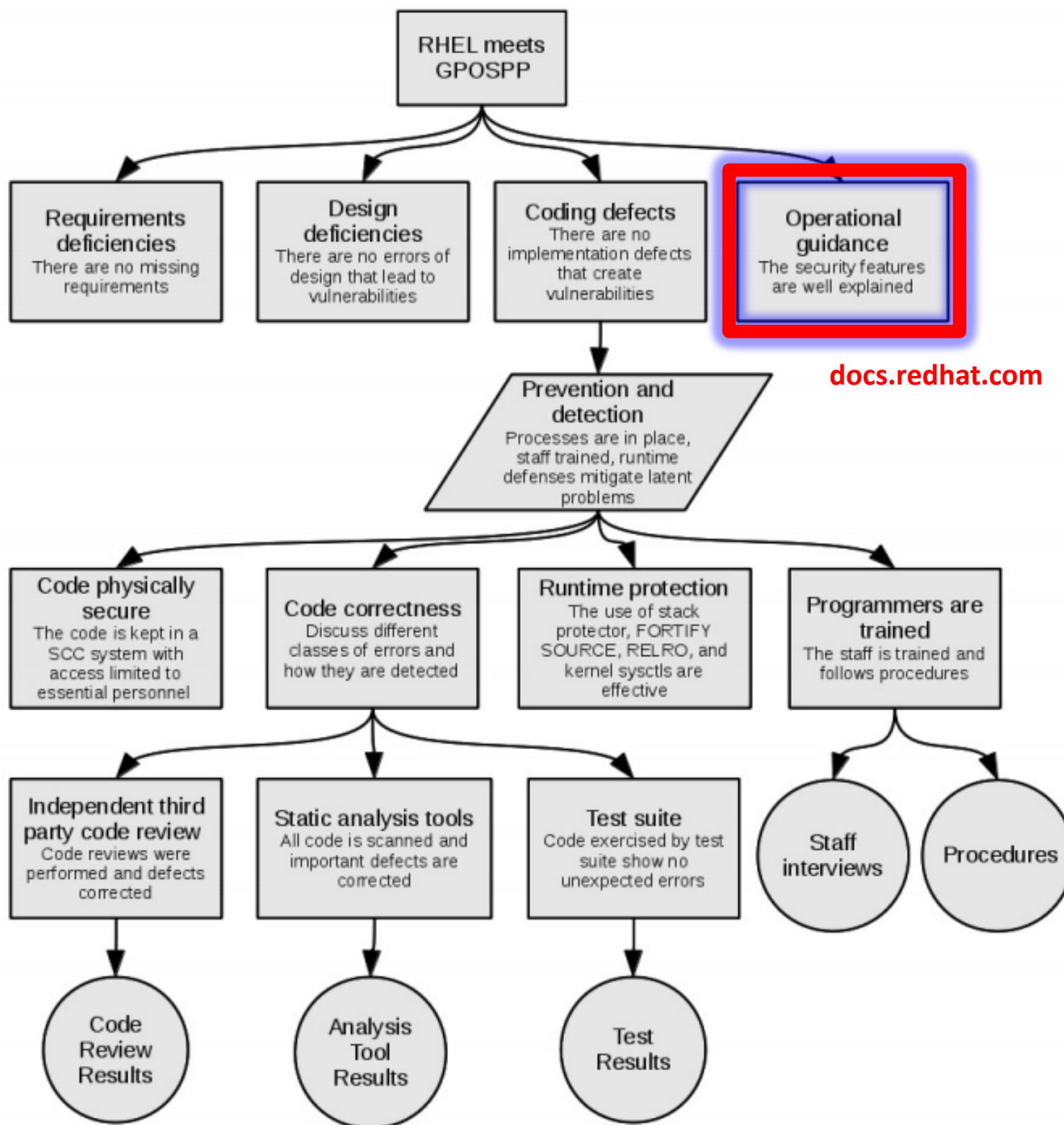
RBAC: Users classified into roles ("BackupAdm," "AuditAdm"...)

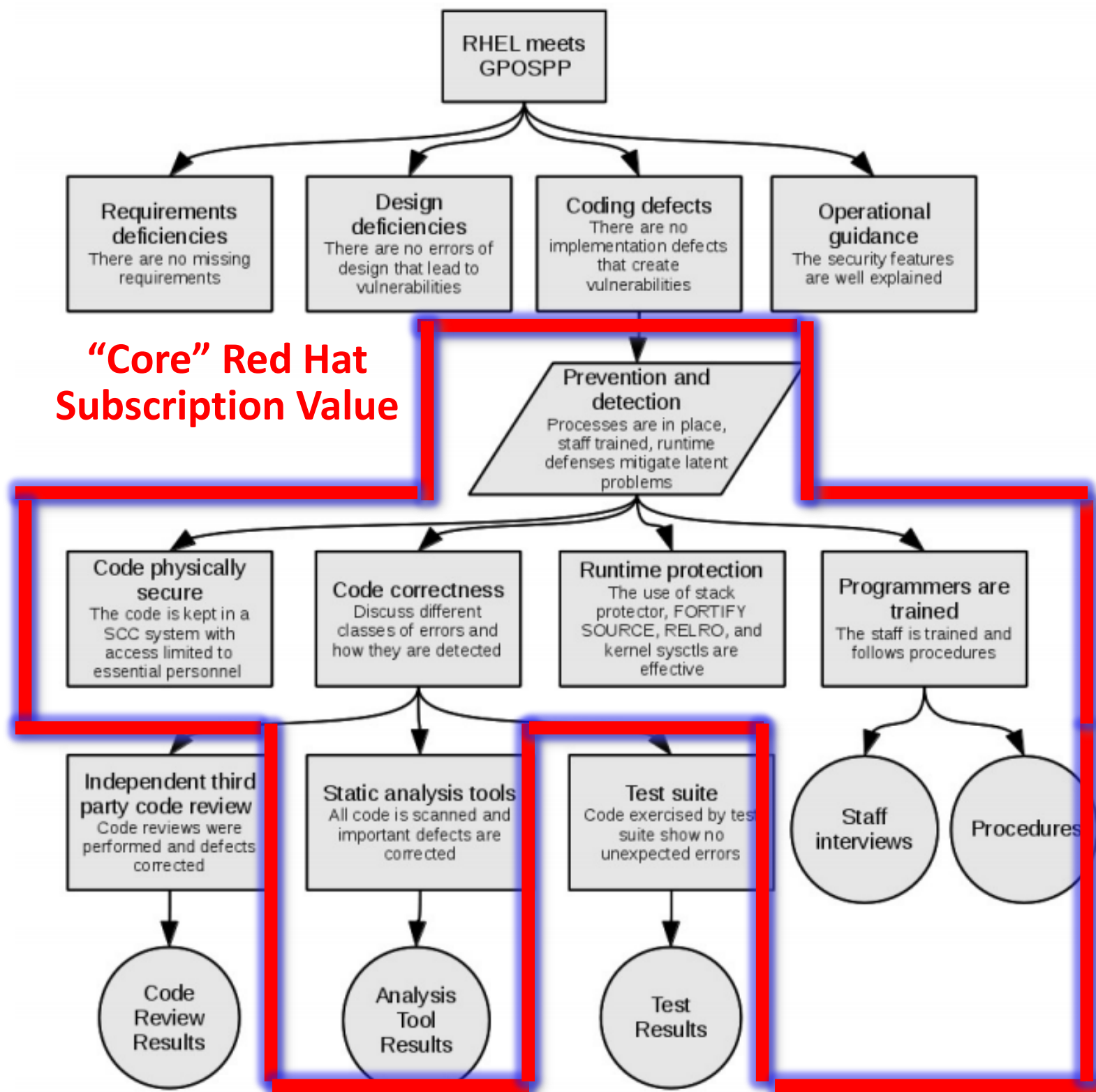
LSPP: Compartmentalizes users and applications from each other. Enables MLS.

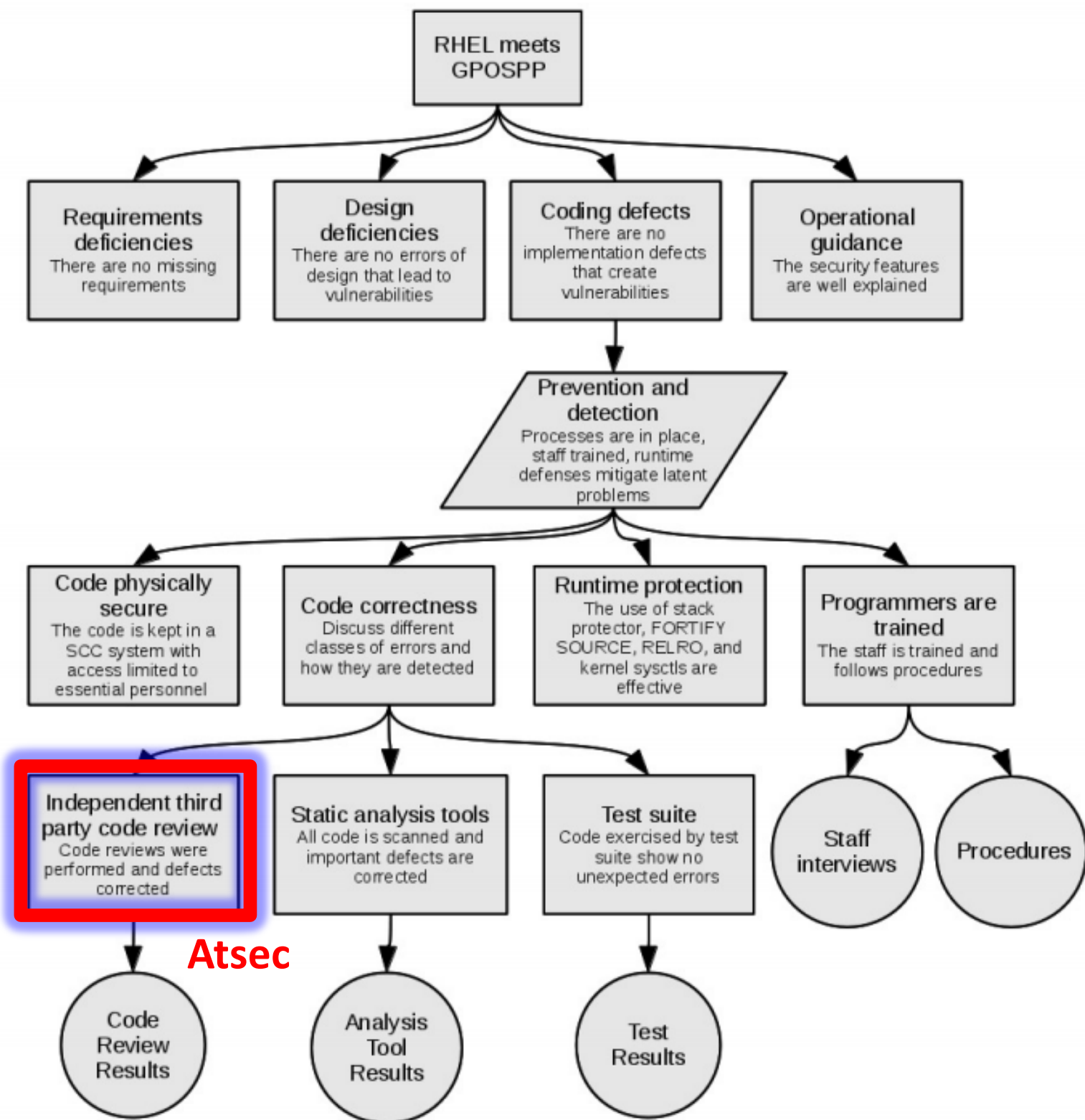












Common Criteria

!=

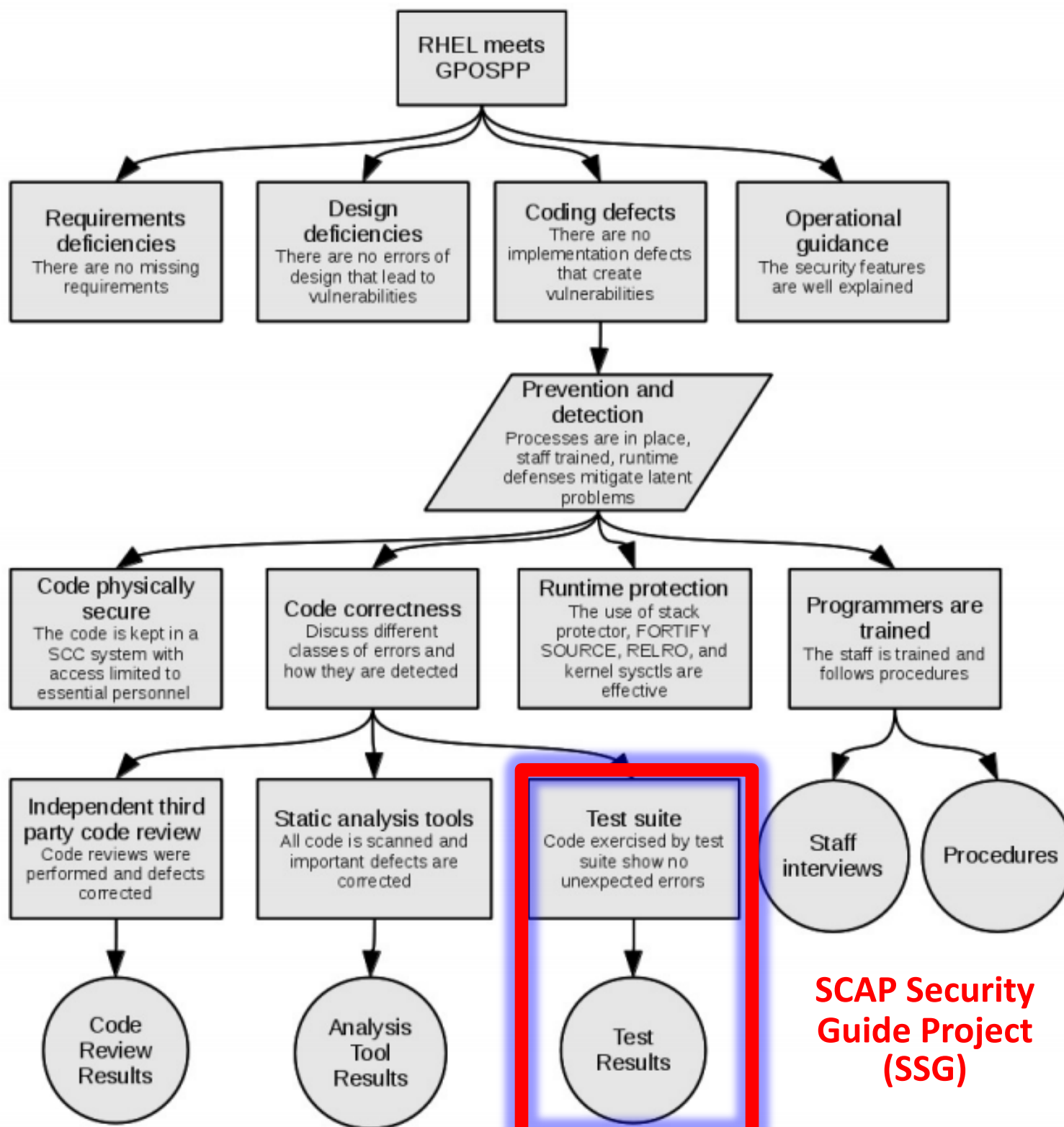
Compliance Policy



STIG

==

Compliance Policy



**SCAP Security
Guide Project
(SSG)**

SCAP Security Guide



LOCKHEED MARTIN



In a Nutshell, SCAP Security Guide:

... has had 1,943 commits from 24 contributors,
representing 164,355 lines of source

... took an estimated 43 years of effort (COCOMO
model)

... has become upstream for DISA RHEL6 STIG, NIST
NVD for JBoss EAP,
NSA SNAC guide in progress

RHEL5 STIG Delay:
1,988 days

RHEL5 STIG Delay:

1,988 days

RHEL6 STIG Delay:


932 days

STIG Version 1, Release 2, Section 1.1:

“The consensus content was developed using an open source project called SCAP Security Guide. The project’s website is <https://fedorahosted.org/scap-security-guide/>. Except for differences in formatting to accommodate the DISA STIG publishing process, the content of the RHEL6 STIG should mirror the SCAP Security Guide content with only minor divergences as updates from multiple sources work through the consensus process”

AC-19(e)	Disable GNOME Automounting	<p>The system's default desktop environment, GNOME, will mount devices and rem inserted into the system. Disable automount and autorun within GNOME by run</p> <pre># 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</pre> <p>These settings can be verified by running the following:</p> <pre>\$ 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</pre>
CM-7	Disable Mounting of cramfs	<p>To configure the system to prevent the <code>cramfs</code> kernel module from being loaded</p> <pre>install cramfs /bin/false</pre> <p>This effectively prevents usage of this uncommon filesystem.</p>
CM-7	Disable Mounting of freevxfs	<p>To configure the system to prevent the <code>freevxfs</code> kernel module from being load</p> <pre>install freevxfs /bin/false</pre> <p>This effectively prevents usage of this uncommon filesystem.</p>
CM-7	Disable Mounting of jffs2	<p>To configure the system to prevent the <code>jffs2</code> kernel module from being loaded,</p> <pre>install jffs2 /bin/false</pre> <p>This effectively prevents usage of this uncommon filesystem.</p>

SCAP Security Guide

- Guidance broken into profiles:
 - RHEL6 STIG
 - CS2 
 - NIST NVD (JBoss only)

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)

I DON'T ALWAYS TEST MY CODE



**BUT WHEN I DO,
IT'S DURING LIVE DEMOS**



LOCALIZATION



DATE & TIME

Europe/Prague timezone



KEYBOARD

English (English (US))



LANGUAGE SUPPORT

English (United States)

SECURITY



SECURITY PROFILE

Misconfiguration detected

SOFTWARE



INSTALLATION SOURCE

Closest mirror



NETWORK CONFIGURATION

Wired (eth0) connected




SOFTWARE SELECTION

Custom software selected

STORAGE



Done us

Data stream: scap_org.open-scap_datastream_tst ▾

Checklist: scap_org.open-scap_cref_first-xccdf.xml ▾

Choose profile below:

My testing profile





A profile for testing purposes.

My testing profile2

Another profile for testing purposes.

Select profile

Changes that were done or need to be done:

-  /tmp must be on a separate partition or logical volume
-  root password was too short, a longer one with at least 10 characters will be required
-  package 'iptables' has been added to the list of to be installed packages
-  package 'telnet' has been added to the list of excluded packages

```
1 this is a simple kickstart file for testing OSCP addon's features
2
3 # values saving a lot of clicks in the GUI
4 lang en US.UTF-8
5 keyboard --xlayout=us --vckeymap=us
6 timezone Europe/Prague
7 rootpw aaaaa
8 bootloader --location=mbr
9 clearpart --initlabel --all
10 autopart --type=plain
11
12 %packages
13 vim
14 %end
15
16 %addon org_fedora_oscap
17     content-type = archive
18     content-url = http://192.168.122.1/xccdf_content.zip
19     profile = xccdf_com.stig-rhel6-server
20     xccdf-path = xccdf.xml
21 %end
```