



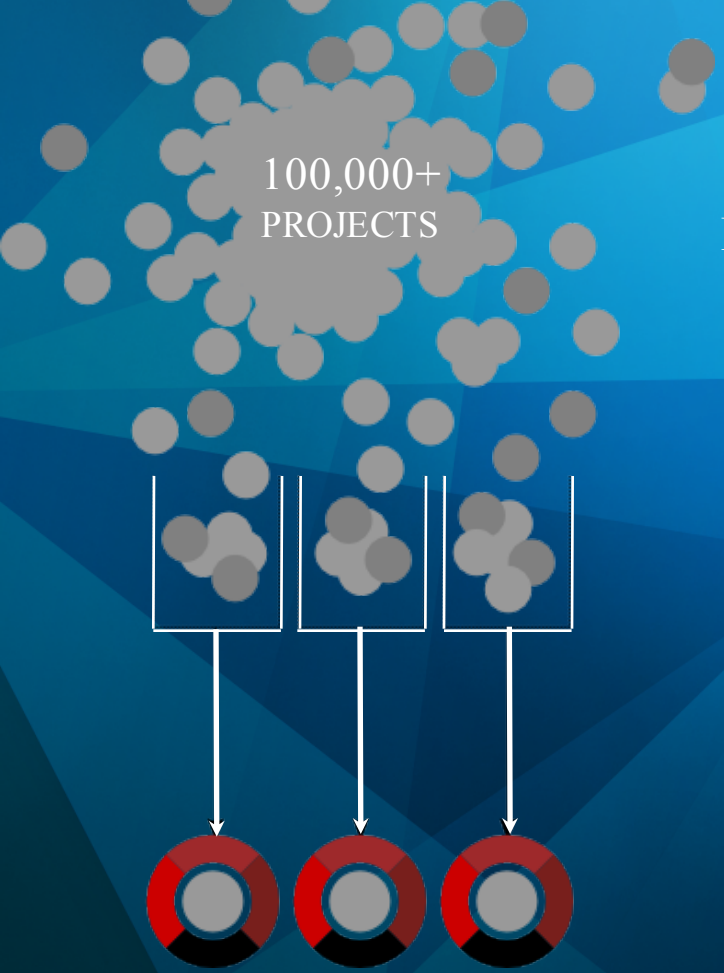


Applied Cross Domain: Red Hat Foundations

Shawn Wells
Office of the Chief Technologist, Red Hat Public Sector
shawn@redhat.com || 443-534-0130







PARTICIPATE

CSCF participates in community-powered upstream projects, such as SELinux, OpenSCAP and the SCAP Security Guide

INTEGRATE

CSCF collaborates with Red Hat to integrate upstream projects into Enterprise Linux, fostering open community platforms.

STABILIZE

We commercialize these platforms together with a rich ecosystem of services and certifications, such as ICD 503 and CNSSI 12-53 accreditations.

SELinux

- Type Separation: How users, processes, and data are isolated
- Role Based Access Control (RBAC)
- MLS Policy

SELinux

- Type Separation: How users, processes, and data are isolated
- Role Based Access Control (RBAC)
- MLS Policy

Security Automation

- Configuration Monitoring
- Compliance Reports
- Secure Provisioning
- Remediation

SELinux Refresher

- Type Separation: How users, processes, and data are isolated
- Role Based Access Control (RBAC)
- MLS Policy

Certifications & Standards

- Common Criteria & NIAP
- Intelligence Community Directive 503 (ICD 503)
- US Government Configuration Baseline (USGCB)

Security Automation

- Configuration Monitoring
- Compliance Reports
- Secure Provisioning
- Remediation

SELinux Refresher

Multi-Level Security (MLS) Policy

- Focuses on confidentiality (i.e. separation of multiple classifications of data)

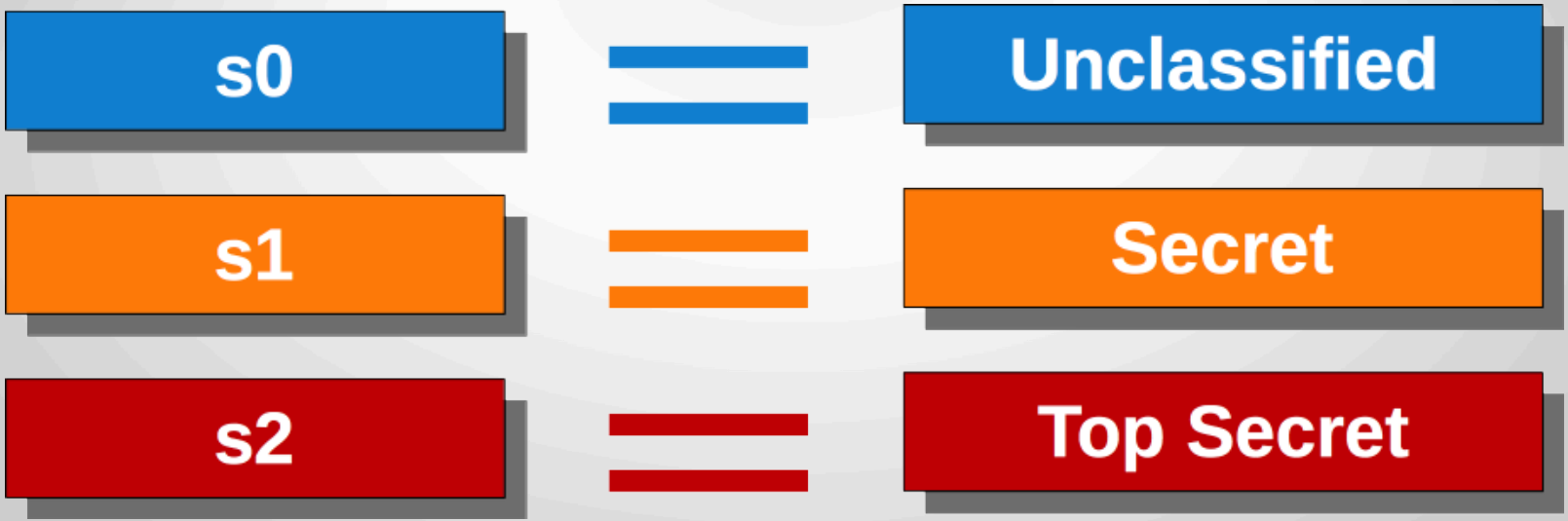
Multi-Level Security (MLS) Policy

- Focuses on confidentiality (i.e. separation of multiple classifications of data)
- Ability to manage {processes, users} with varying levels of access. (i.e. "*the need to know*")

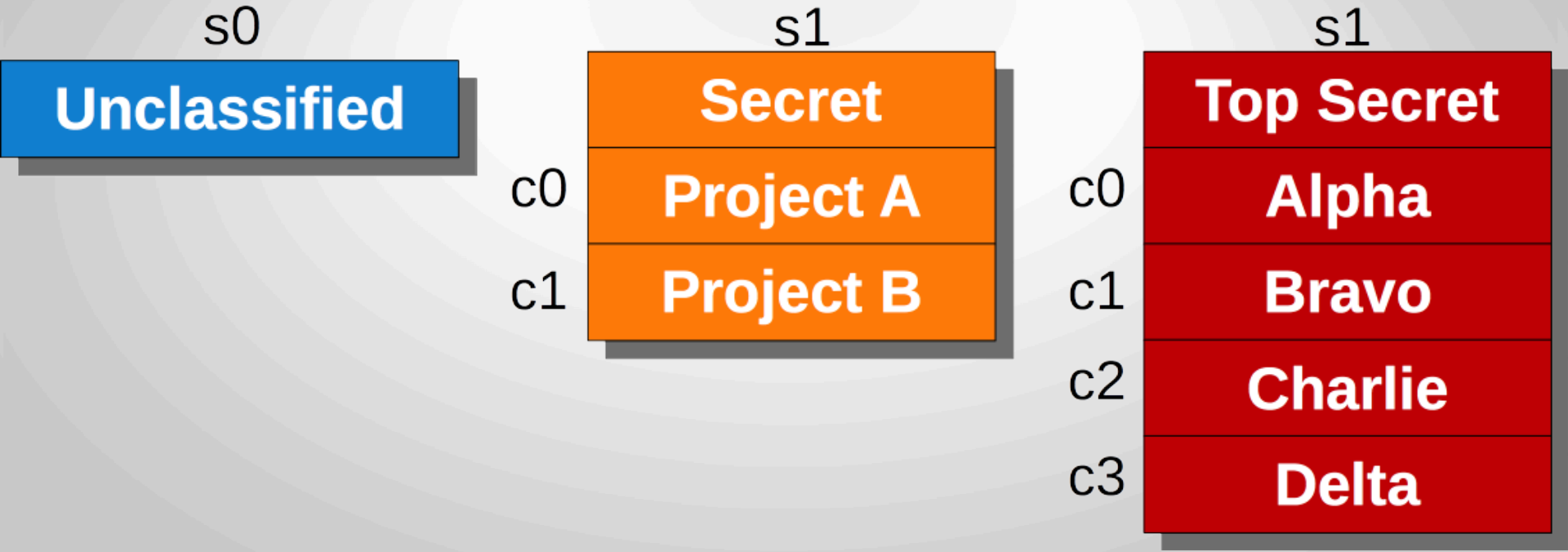
Multi-Level Security (MLS) Policy

- Focuses on confidentiality (i.e. separation of multiple classifications of data)
- Ability to manage {processes, users} with varying levels of access. (i.e. "*the need to know*")
- Uses category & sensitivity levels

Sensitivity Labels



Category Labels



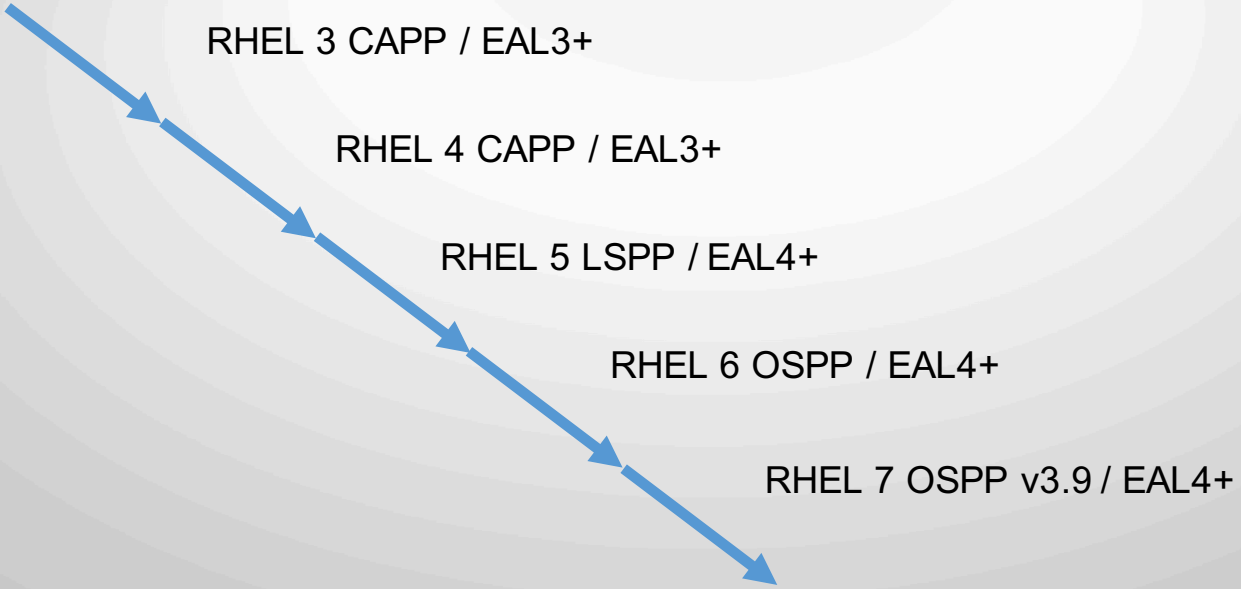
Polyinstantiation

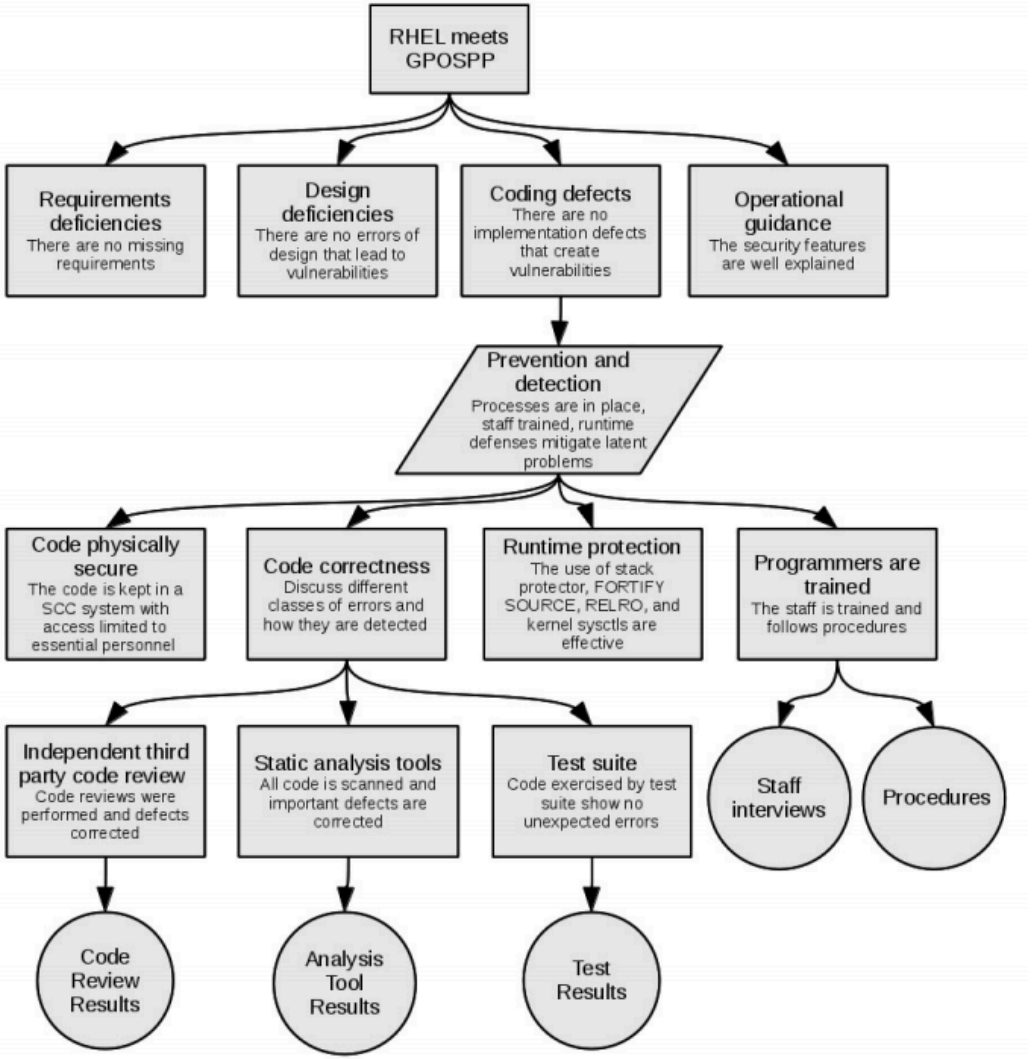
id –Z
staff_u:WebServer_Admin_r:WebServer_Admin_t:**s0:c0**
ls -l /data
secret-file-1
secret-file 2

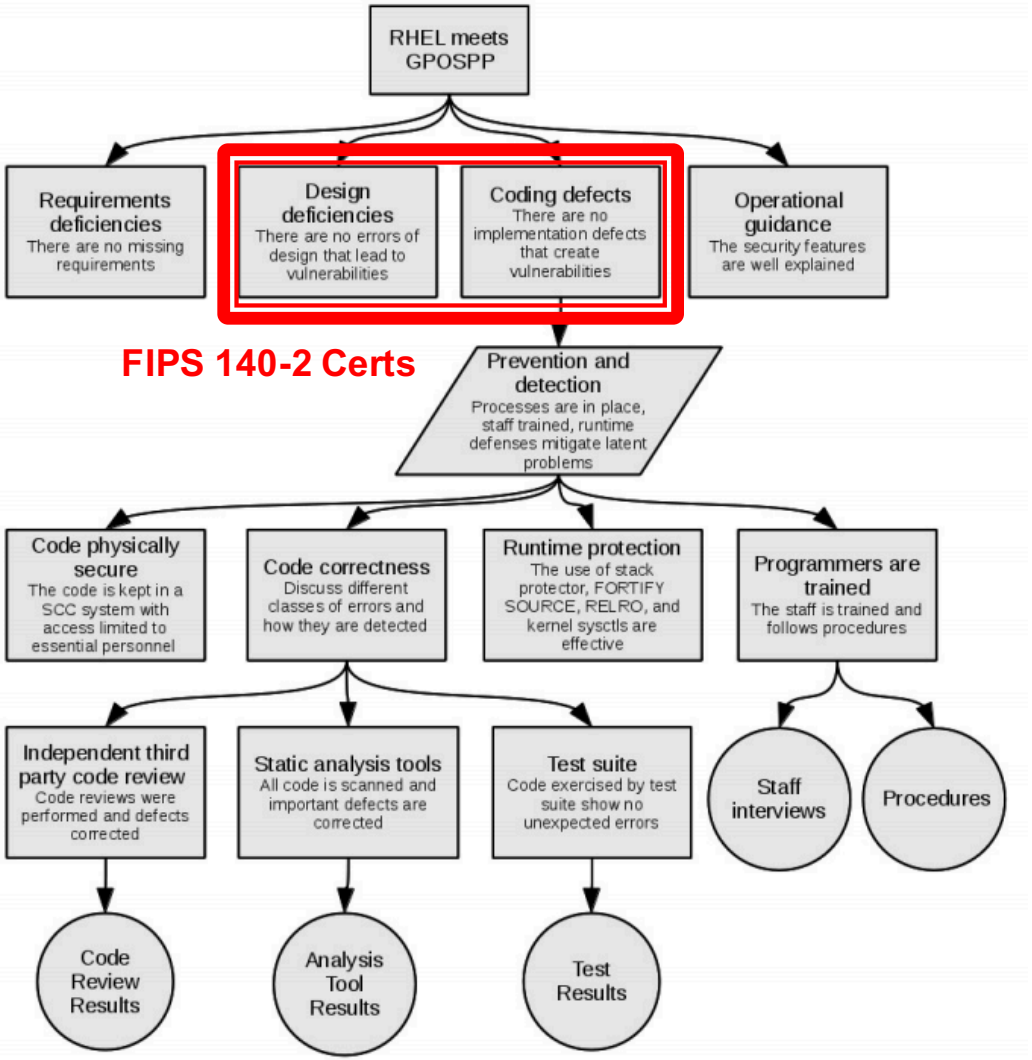
id –Z
staff_u:WebServer_Admin_r:WebServer_Admin_t:**s1:c0**
ls -l /data
secret-file-1
secret-file 2
top-secret-file-1

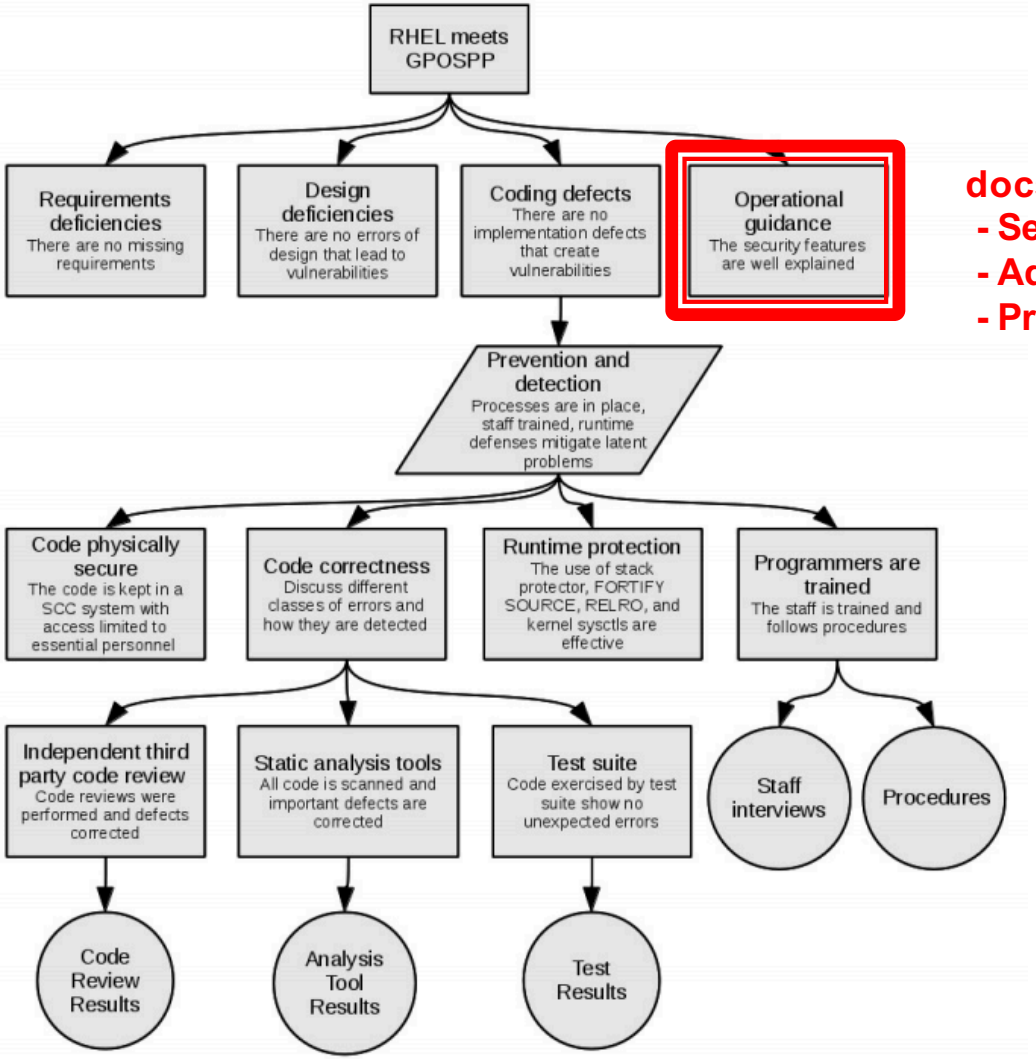
Certifications & Standards

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

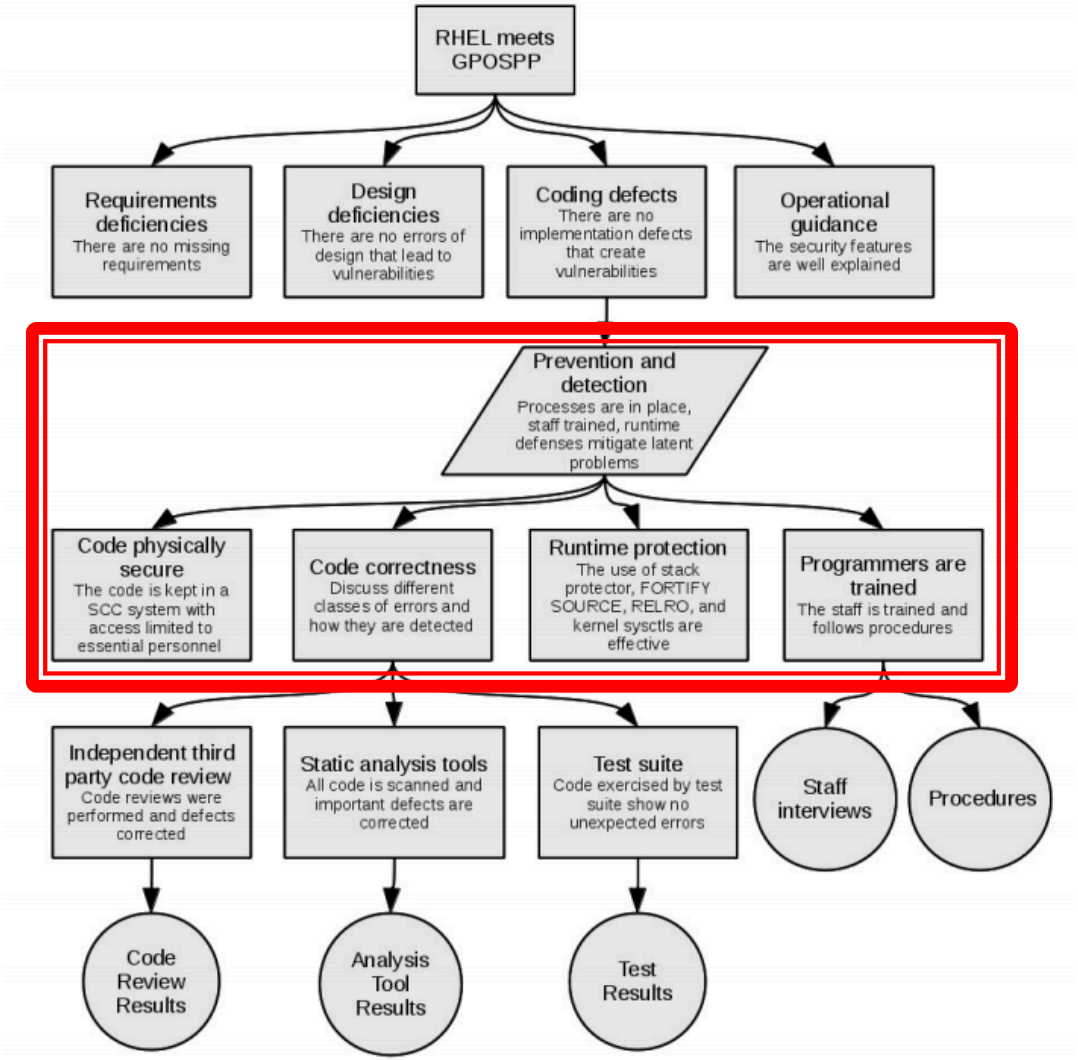



RHEL meets GPOSPP
Requirements deficiencies
There are no missing requirements
Design deficiencies
There are no errors of design that lead to vulnerabilities
Coding defects
There are no implementation defects that create vulnerabilities
Operational guidance
The security features are well explained
Prevention 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

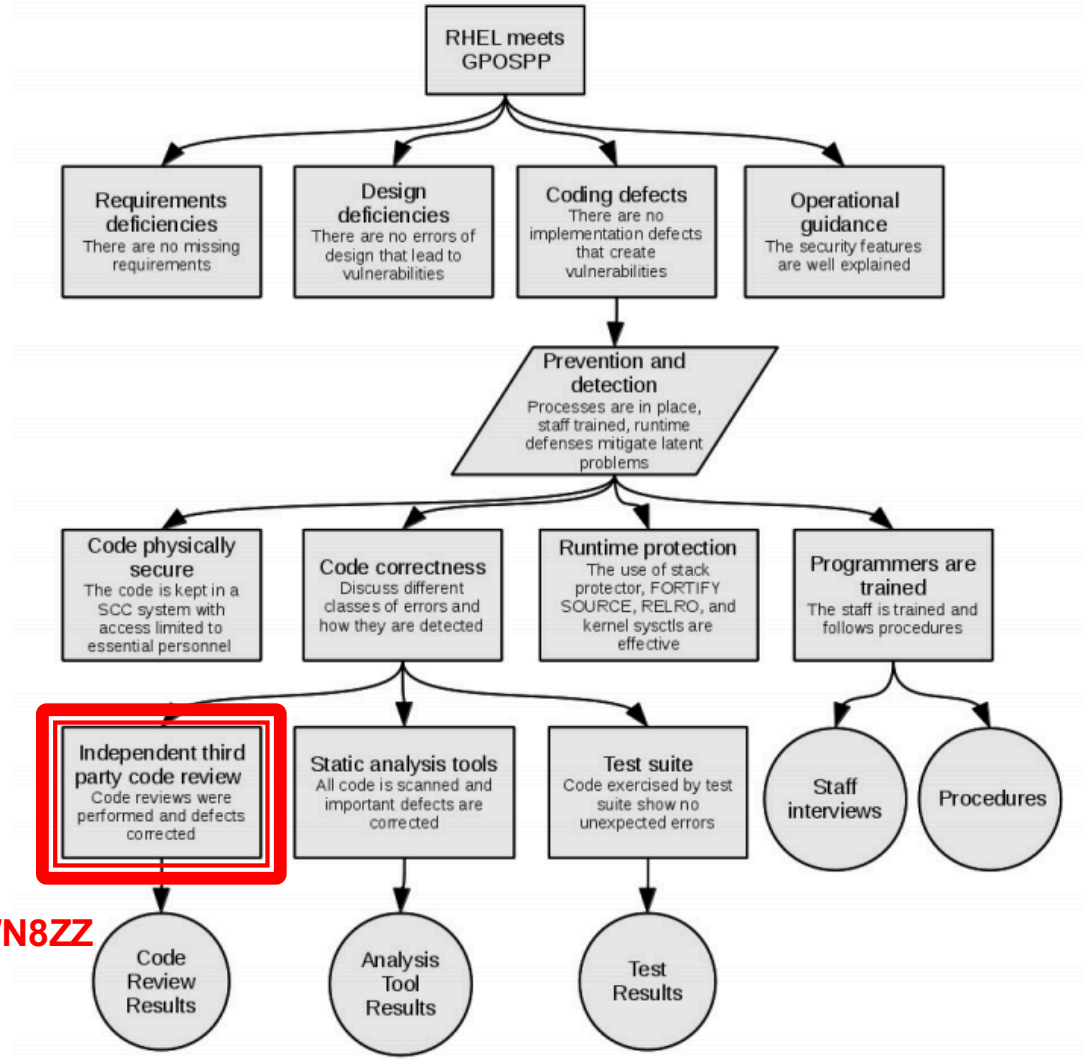

RHEL meets GPOSPP
Requirements deficiencies
There are no missing requirements
Design deficiencies
There are no errors of design that lead to vulnerabilities
Coding defects
There are no implementation defects that create vulnerabilities
Operational guidance
The security features are well explained
FIPS 140-2 Certs
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



docs.redhat.com
- Security Guide
- Admin. Guide
- Priv User Guide



Red Hat corporate development & responsibilities



We use Atsec
http://red.ht/1kWN8ZZ

Common Criteria

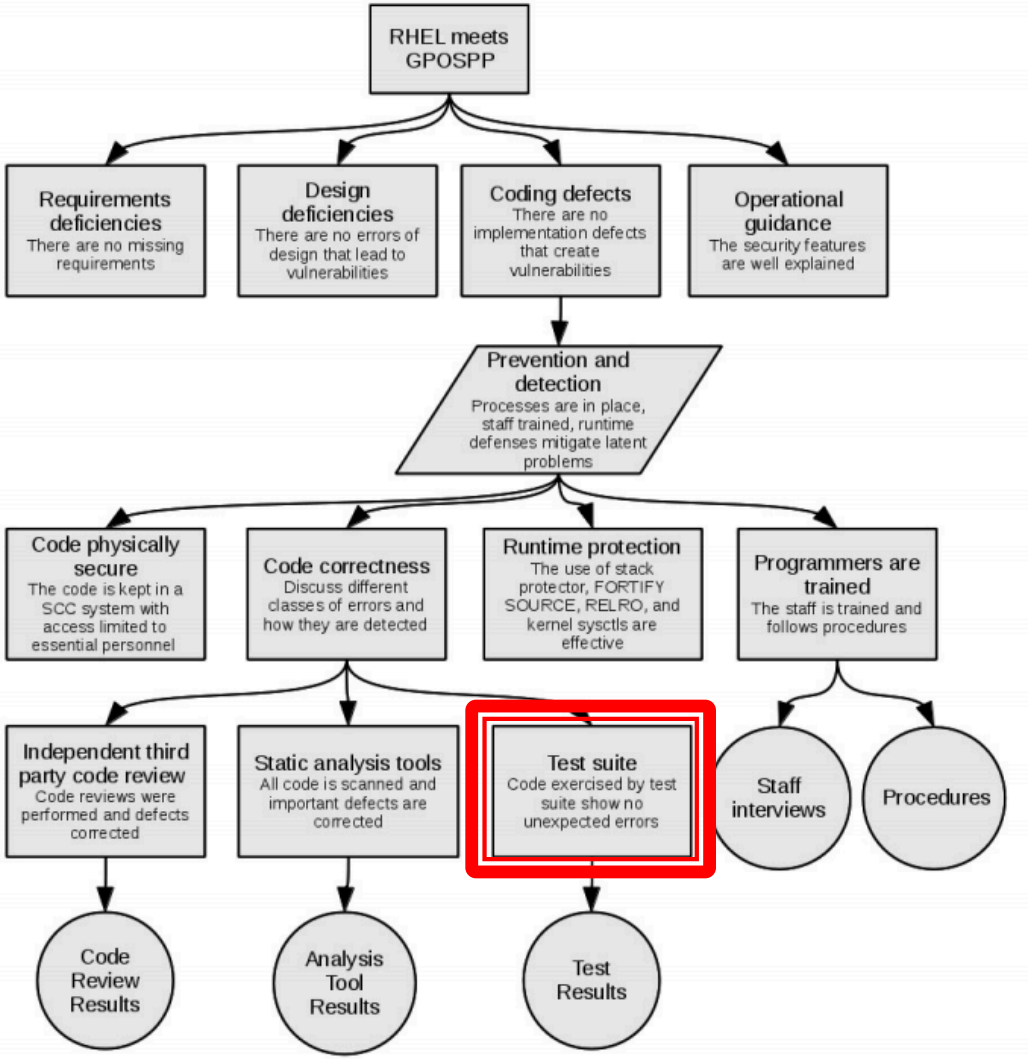
!=

Compliance Policy

ICD 503, STIG, FISMA

==

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

http://open-scap.org,
http://github.com/OpenSCAP

Guide to the Secure Configuration of Red Hat Enterprise Linux 7

Description

This guide presents a catalog of security-relevant configuration settings for Red Hat Enterprise Linux 7 formatted in the eXtensible Configuration Checklist Description Format (XCCDF). 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 many operational scenarios. 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 7 is one example of a baseline created from this guidance.

Set Password Minimum Length

rule

The pam_pwquality module's minlen parameter controls requirements for minimum characters required in a password. Add minlen=15 after pam_pwquality to set minimum password length requirements.

identifiers: CCE-27293-0

references: IA-5(1)(a), 205, 78, Req-8, Test attestation on 20140928 by swells

Remediation script:

```
var_password_pam_minlen="15"
if egrep -q ^minlen[[:space:]]*=[[:space:]]*[[:digit:]]+ /etc/security/pwquality.conf; then
        sed -i "s/^\(minlen *= *\).*/\1$var_password_pam_minlen/" /etc/security/pwquality.conf
else
        sed -i "/\(minlen *= *\).*/a minlen = $var_password_pam_minlen" /etc/security/pwquality.conf
fi
```

Limit the ciphers to those algorithms which are FIPS-approved. Counter (CTR) mode is also preferred over cipher-block chaining (CBC) mode. The following line in `/etc/ssh/sshd_config` demonstrates use of FIPS-approved ciphers: `Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-cbc,aes256-cbc` The man page `sshd_config(5)` contains a list of supported ciphers.	Approved algorithms should impart some level of confidence in their implementation. These are also required for compliance.	AC-3 AC-17(2 AU-10(5 IA-5(1)(c) IA-7
Limit the MACs to those hash algorithms which are FIPS-approved. The following line in `/etc/ssh/sshd_config` demonstrates use of FIPS-approved MACs: `MACs hmac-sha2-512,hmac-sha2-256,hmac-sha1` The man page `sshd_config(5)` contains a list of supported MACs.	Approved algorithms should impart some level of confidence in their implementation. These are also required for compliance.	AC-17(2 IA-7 SC-13

Compliance and Scoring

The target system did not satisfy conditions of 47 rules! Please review rule results and consider applying remediation.

Rule result breakdown

Failed rules by severity breakdown

Install AIDE

Rule ID	package_aide_installed
Result	fail
Time	2015-08-27T00:31:48
Severity	medium
Identifiers and References	identifiers: CCE-26741-9 references: CM-3(d), CM-3(e), CM-6(d), CM-6(3), SC-28, SI-7, http://iase.disa.mil/stigs/cci/Pages/index.aspx, Test attestation on 20121024 by DS

Install the AIDE package with the command: $ sudo yum install aide

Remediation script:

```
yum -y install aide
```

```
this is a simple kickstart file for testing OSCAP addon's features

# values saving a lot of clicks in the GUI
lang en US.UTF-8
keyboard --xlayour=us --vckeymap=us
timezone Europe/Prague
rootpw aaaaa
bootloader --location=mbr
clearpart --initlabel --all
autopart --type=plain

%packages
vim
%end

%addon org_fedora_oscap
        content-type = archive
        content-url = http://192.168.122.1/xccdf_content.zip
        profile = xccdf_com.stig-rhel6-server
        xccdf-path = xccdf.xml
%end
```

Shawn Wells
Director, Innovation Programs
Office of the Chief Technologist, Red Hat Public Sector
shawn@redhat.com || 443-534-0130