OpenSCAP Workshop

Hands-on Labs to explore Scanning, Reporting, Remediation

Shawn Wells
shawn@redhat.com || 443-534-0130 (US EST)

redhat.

1. What's the latest in the Linux Security Automation space?
    a. Government & Commercial Initiatives
    b. Formal and Emerging SCAP Standards

2. What tools and content are available today?
    a. For enumerating (known) software vulnerabilities
    b. For assessing configuration

In the next 2 hours . . .

1. Install and review compliance profiles in RHEL 7
2. Perform and interpret compliance scans, then remediate findings
3. Create custom (derived) configuration baseline with SCAP Workbench
4. RHEL 7 “Easy Button” Installations
5. Introspectively scan Linux containers
6. _____

MOTIVATION

RHEL5 STIG

- 587 compliance items
- Many are manual

Avg Time to Configure & Verify Setting	# controls	Total Time *per RHEL instance*
1 minute	* 587	9.7 hours
3 minutes	* 587	29.4 hours
5 minutes	* 587	48.9 hours

openprivacy / ansible-scap

Watch 1 | Star 2 | F

branch: master ansible-scap / provision.yml

openprivacy 14 days ago comments cleaned up

1 contributor

15 lines (12 sloc) 0.303 kB

Raw Blame History

```
1  ---
2
3  - name: All machines get OpenSCAP scanner installed
4    hosts: all
5    sudo: true
6    roles:
7      - openscap
8  #   - harden  -- Commented out for demo purposes only
9
10 - name: Install SCAP Security Content (SSG) and GovReady on 'dashboard'
11   hosts: dashboard
12   roles:
13     - scap-security-guide
14     - govready
```

… or a single LOC in kickstart

```
$ oscap xccdf eval
--profile rhel7-stig
--remediate
--report /root/scan-report.html
/usr/share/xml/scap/content.xml
```

Compliance and Scoring

The target system did not satisfy conditions of 13 rules! Please review rule results and consider applying remediation.

Rule result breakdown

Failed rules by severity breakdown

Score

Scoring system	Score	Maximum	%
urn:xccdf:scoring:default	93.626541	100.000000	93.63%

Intro to SCAP

First, an SCAP Primer

- A family of specifications managed by NIST

- Really a bunch of XML schema
  - which are data formats
  - so not a protocol at all, it turns out
  - openly defined, community developed, and ***evolving***

First, an SCAP Primer

- Defines standardized formats

- Because you'll get:
  - Standardized inputs (e.g. a compliance baseline)
  - Standardized outputs (e.g. compliance report)

- Provides the enterprise liberty with regard to product choices
  - Avoid vendor lock-in
  - Federal procurement language starting to require SCAP

TOOLS

vs

CONTENT

U.S. Gov SCAP Validation Program

https://scap.nist.gov/validation/

- Automated test suites to verify interpreters, like OpenSCAP

- Mandated by US Gov:

  The U.S. Office of Management and Budget has required, **in the August 11, 2008, M-08-22 memorandum to Federal CIOs**, that "Both industry and government information technology providers must use SCAP validated tools with FDCC Scanner capability to certify their products operate correctly with FDCC configurations and do not alter FDCC settings. Agencies will use SCAP tools to scan for both FDCC configurations and configuration deviations approved by department or agency accrediting authority. **Agencies must also use these tools when monitoring use of these configurations as part of FISMA continuous monitoring.**"

- Required by GSA for vulnerability and configuration management products

U.S. Gov SCAP Validation Program

Also covers content (reference: NIST SP 800-70)

Tier	Machine Readable?	Automated Format?	References to Security Compliance Framework?
1	No	N/A	Optional
2	Yes	Non-standard (proprietary, product-specific, etc)	Optional
3	Yes	Complete SCAP-expressed checklist that should run in SCAP-enabled products and pass through SCAPVal with no errors	Optional
4	Yes	Tier III + Includes low-level security enumerations that map to high-level security requirements (e.g. SP 800-53 controls)	Required; must be vetted with at least one governance organization authoritative for the security compliance framework.

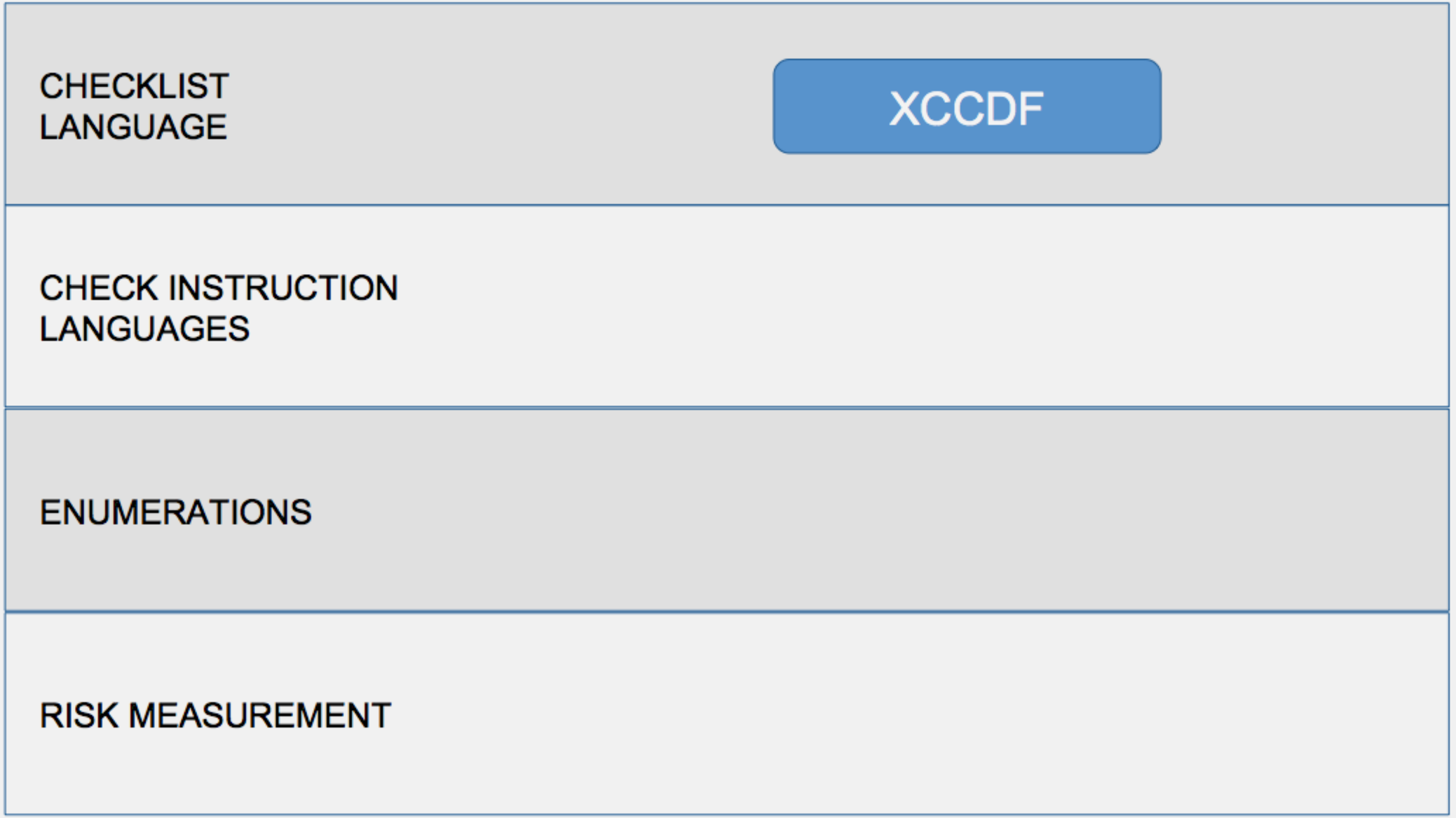
ACRONYM BREAKDOWN

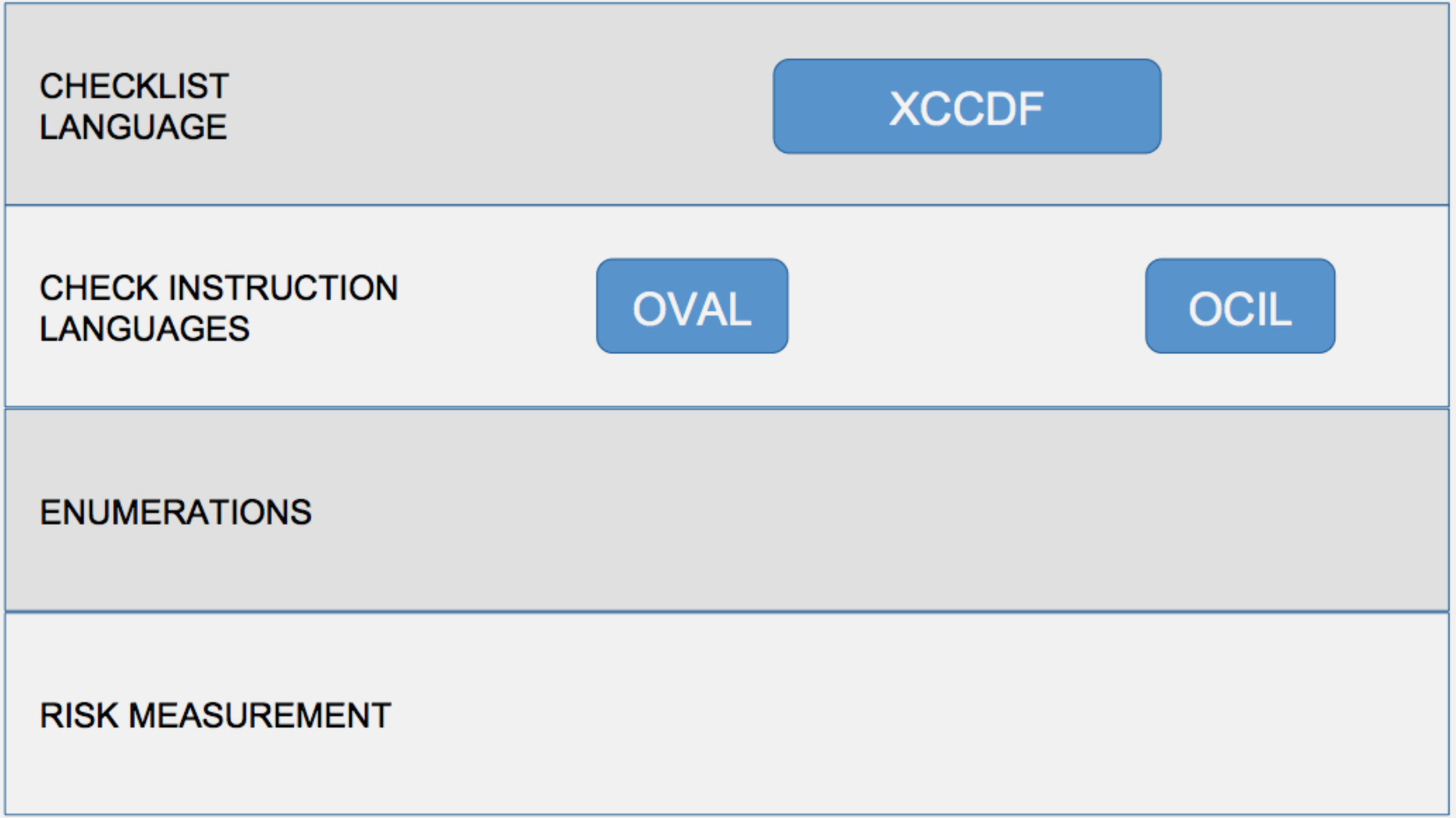
CHECKLIST
LANGUAGE

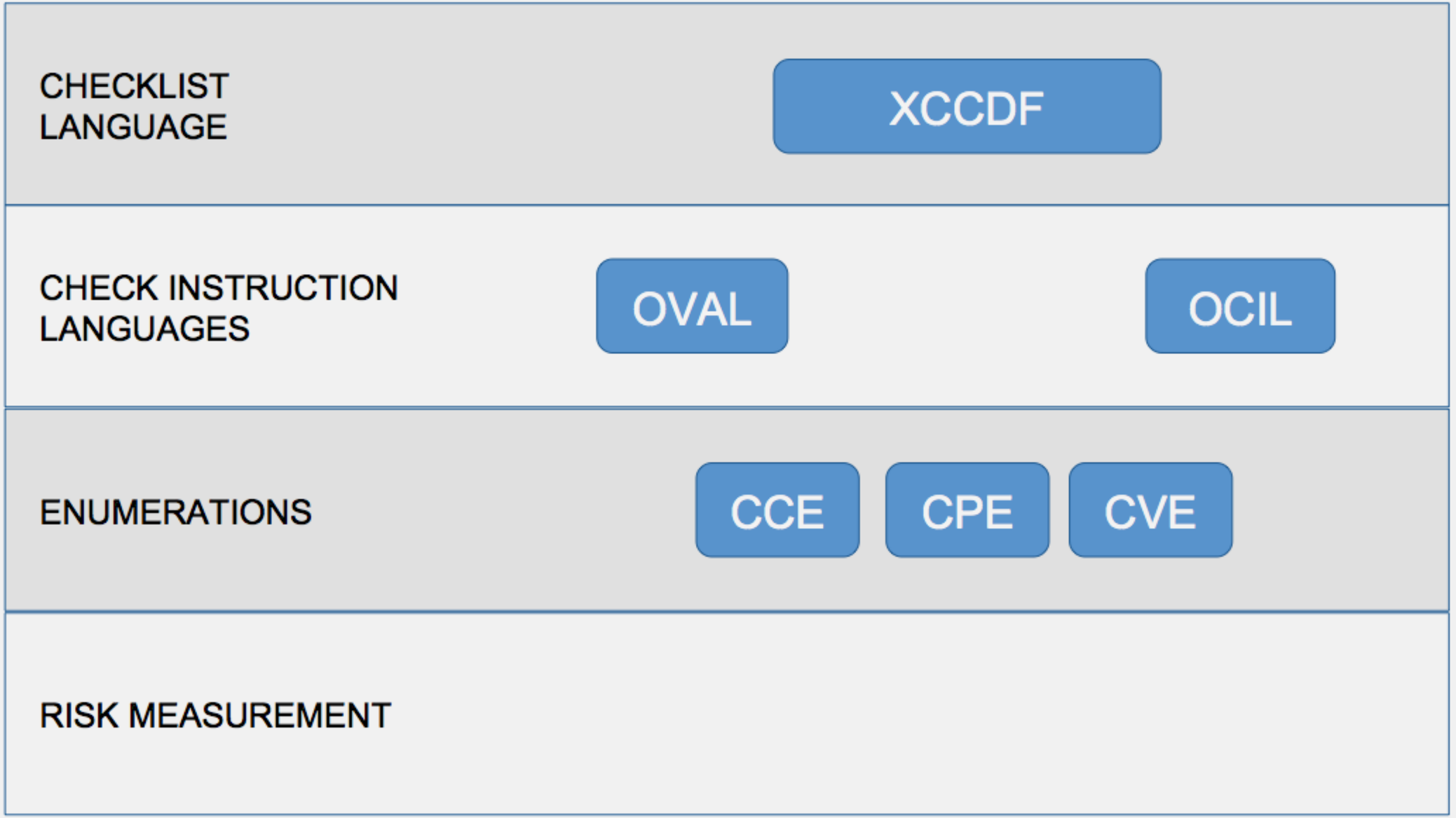
CHECK INSTRUCTION
LANGUAGES

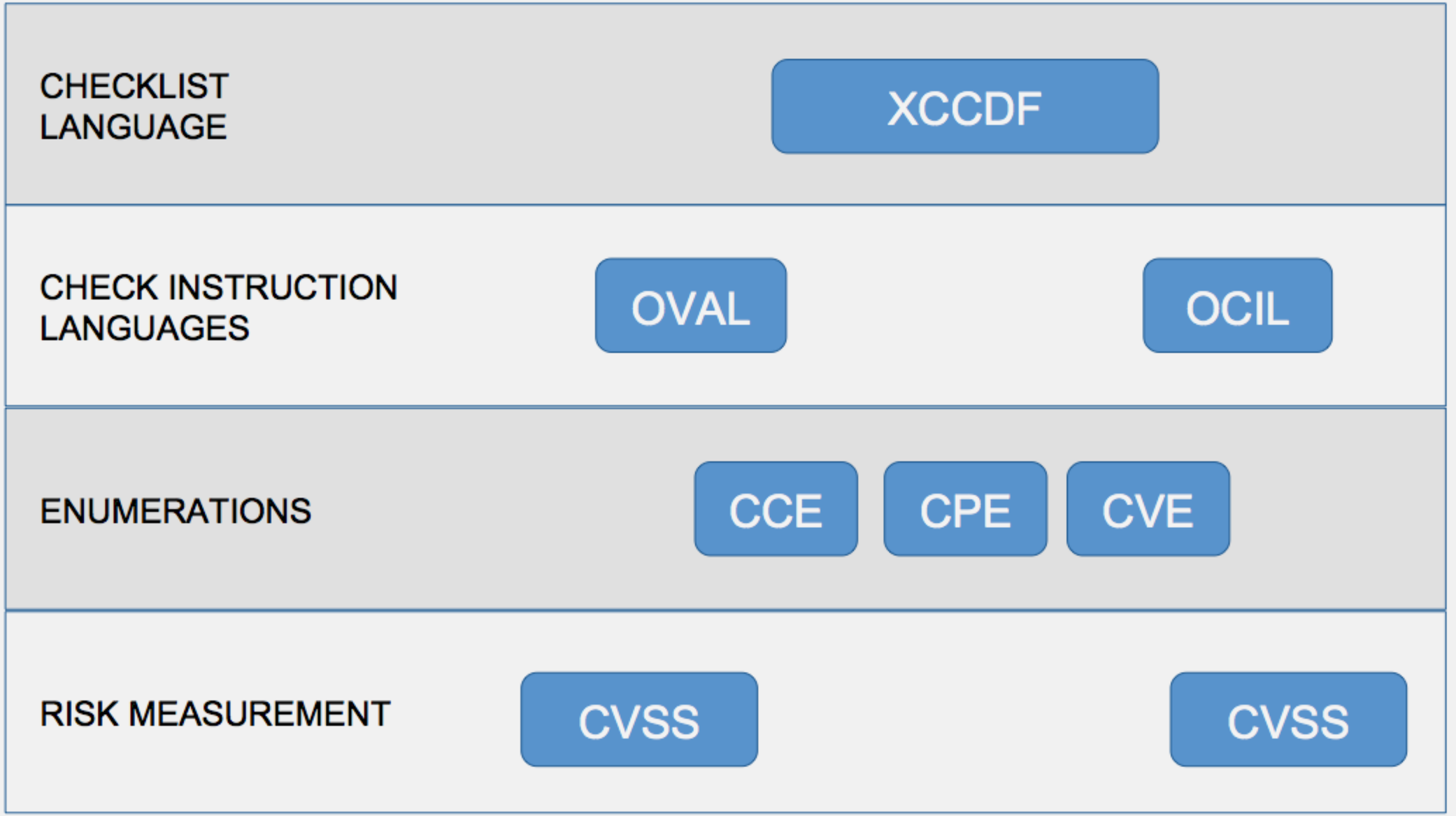
ENUMERATIONS

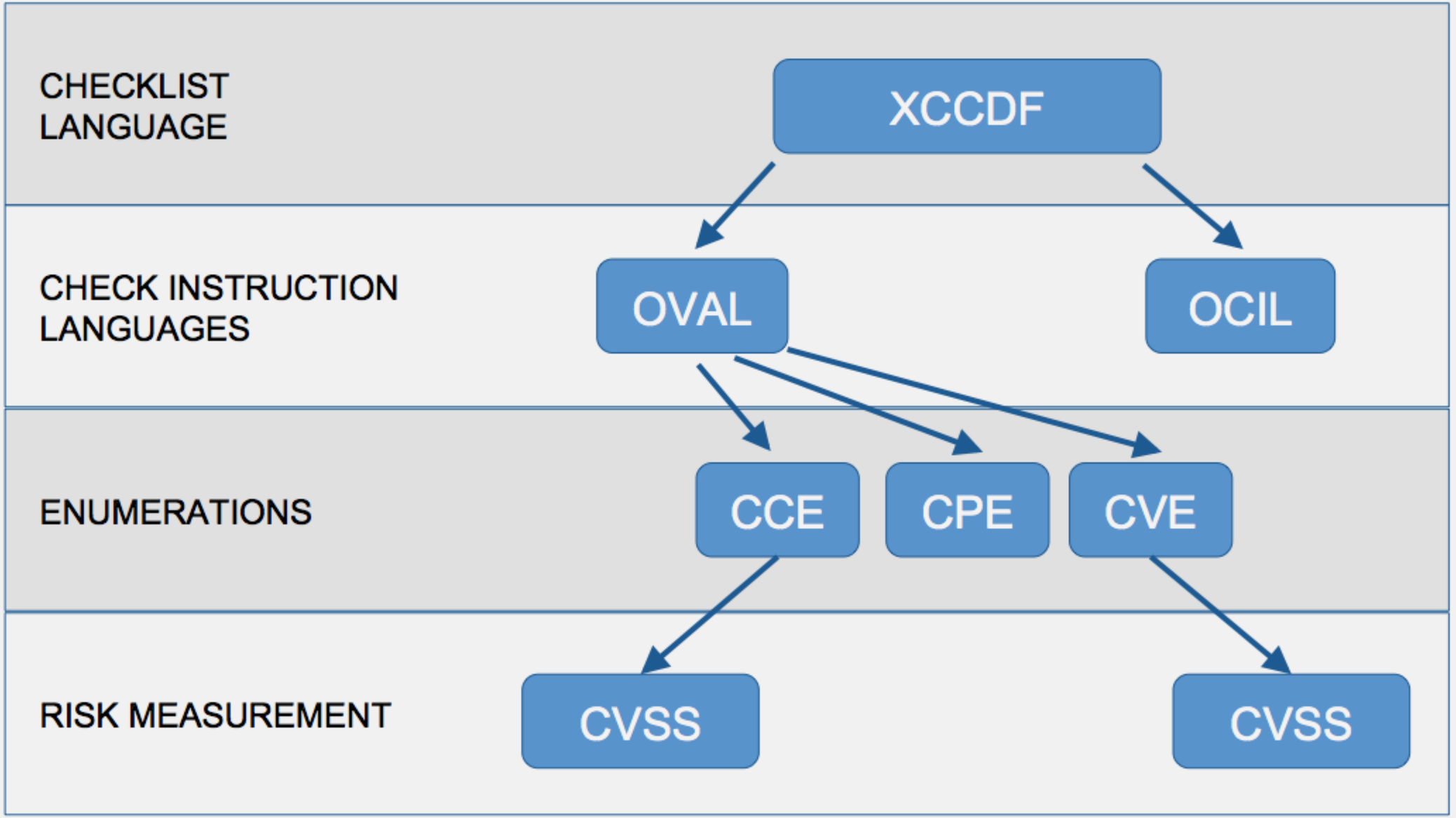
RISK MEASUREMENT


CHECKLIST
LANGUAGE
XCCDF
CHECK INSTRUCTION
LANGUAGES
ENUMERATIONS
RISK MEASUREMENT


CHECKLIST LANGUAGE
XCCDF
CHECK INSTRUCTION LANGUAGES
OVAL
OCIL
ENUMERATIONS
RISK MEASUREMENT


CHECKLIST LANGUAGE
XCCDF
CHECK INSTRUCTION LANGUAGES
OVAL
OCIL
ENUMERATIONS
CCE
CPE
CVE
RISK MEASUREMENT


CHECKLIST LANGUAGE
XCCDF
CHECK INSTRUCTION LANGUAGES
OVAL
OCIL
ENUMERATIONS
CCE
CPE
CVE
RISK MEASUREMENT
CVSS
CVSS

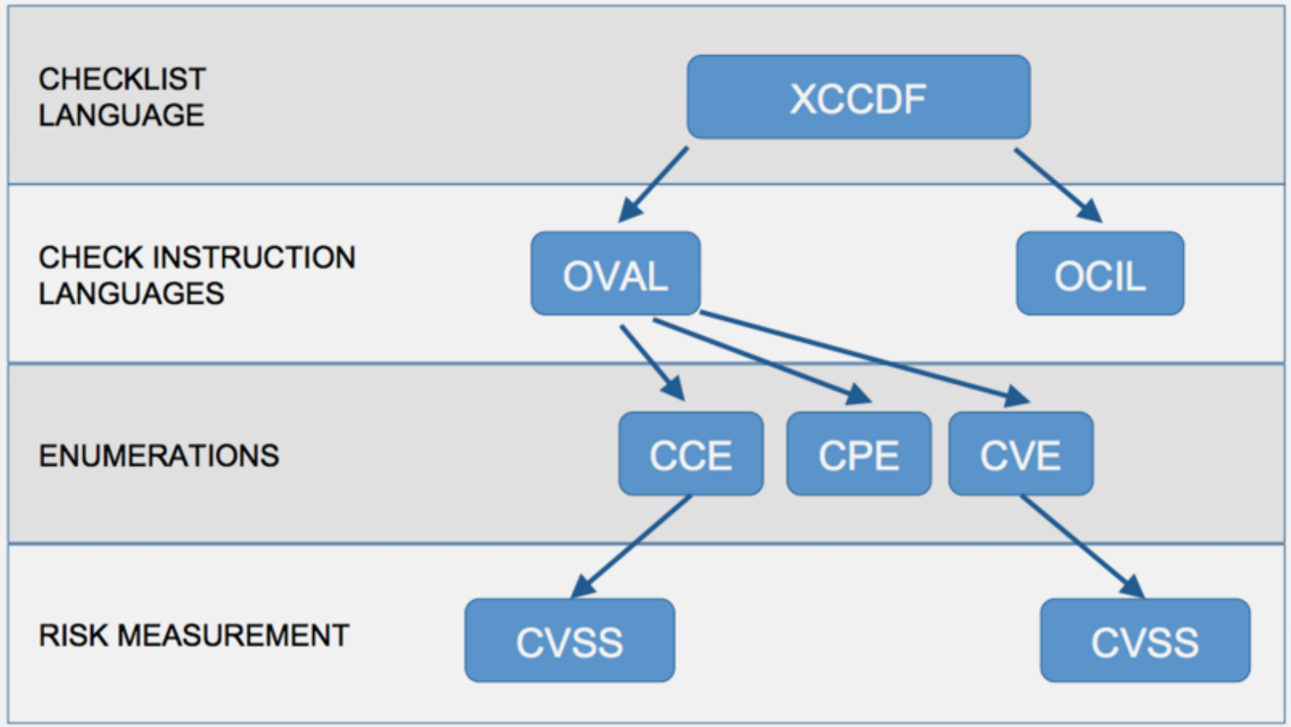

CHECKLIST LANGUAGE
XCCDF
CHECK INSTRUCTION LANGUAGES
OVAL
OCIL
ENUMERATIONS
CCE
CPE
CVE
RISK MEASUREMENT
CVSS
CVSS

Pop Quiz!

1. What assurances do I have that CVSS scores are accurate?

2. Who assigns CCEs?

3. Who reviews the CCE to NIST mappings?



OPEN SOURCE CONFRONTS THE C&A CHALLENGE:

OpenSCAP

OpenSCAP

Community created *portfolio* of tools and content
to assess systems for known vulnerabilities.

https://github.com/OpenSCAP

2008

First commit to OpenSCAP, execution capability for SCAP on Linux

```
commit 768d2d13c7b95736738ce2a48db7f2e528c161fe
Author: Peter Vrabec <pvrabec@wrabco.englab.brq.redhat.com>
Date:   Mon Nov 3 17:58:30 2008 +0100

    Initial commit
```

2008 First commit to OpenSCAP, execution capability for SCAP on Linux

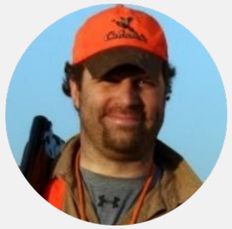
```
commit 768d2d13c7b95736738ce2a48db7f2e528c161fe
Author: Peter Vrabec <pvrabec@wrabco.englab.brq.redhat.com>
Date:   Mon Nov 3 17:58:30 2008 +0100

    Initial commit
```

2011 First commit to SCAP Security Guide, hardening guidance + policy references
Colloquially, “SCAP Content”

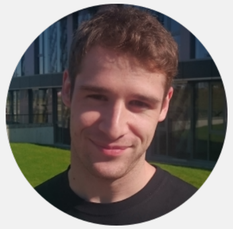
```
commit 540a78f26191a69651a167d256b5af47fd3eb983
Author: Jeff Blank <blank@eclipse.ncsc.mil>
Date:   Wed Jun 8 18:45:05 2011 -0400

    added a README
```



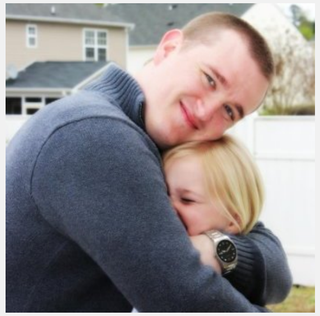



fedscoop
fedscoop
fedscoop







NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

CENTRAL INTELLIGENCE AGENCY
UNITED STATES OF AMERICA

LOCKHEED MARTIN

DEFENSE INFORMATION SYSTEMS AGENCY

TRESYS
TECHNOLOGY

ARL
U.S. Army Research Laboratory

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

HARRIS

Power of the Community

- RHEL7 STIG content, rebased in RHEL 7.3, reflects . . .
  - 6,180 commits from 95 people
  - 441,055 lines of code

- OpenSCAP interpreter contains . . .
  - 6,811 commits from 74 people
  - 157,775 lines of code

- “Security Button” in RHEL7 installer
  - 6 people, 90 days, 6,806 lines of code

OpenSCAP

SCAP
SECURITY GUIDE

SCAP
WORKBENCH

Foreman
OpenSCAP

Ruby Gem
OpenSCAP

Puppet
OpenSCAP

SCAPtimony

Keyboard Time!

Step 1: Download SSH keys

http://studentX.labs.redhatgov.io

Step 2: Login

$ ssh -i <key> ec2-user@studentX.labs.redhatgov.io

Step 3: Sudo to root

$ sudo bash

#1: INSTALL, REVIEW PROFILES

Install OpenSCAP and SCAP Content

```
$ sudo yum -y install openscap-scanner scap-security-guide
```

What default profiles exist?

```
$ oscap info /usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
….
Profiles:
   pci-dss
   rht-ccp
   common
   stig-rhel7-server-upstream
```

(p.s., we're changing that super long /usr/share/xml/… path in rhel 7.4)

#2: REVIEW HARDENING GUIDES

Review manpage

```
$ man scap-security-guide
```

Pop Quiz: Where are the files for the HTML guides located?

For the workshop:

http://studentX.labs.redhatgov.io → click on “SSG Docs”
we copied the files for easy viewing

#3: REVIEW POLICY MAPPINGS

In preparing for the workshop, I noticed we did not document the policy mapping tables in the man page. Fixing that for next RHEL release.

So for now, they're located under
/usr/share/doc/scap-security-guide/tables

For the workshop:
http://studentX.labs.redhatgov.io → click on "SSG Docs" → tables

View the "table-rhel7-nistrefs-ospp.html"

#4: LOCAL SCAN, REVIEW RESULTS

Perform Scan

```
$ sudo bash
# oscap xccdf eval \
--profile rht-ccp \
--results /var/www/html/scans/myscan-results.xml \
--report /var/www/html/scans/myscan-report.html \
/usr/share/xml/scap/ssg/content/ssg-rhel7-xccdf.xml
```

Review Results

http://studentX.labs.redhatgov.io/ → “Scan Results”

Select “myscan-report.html”

Quick Review

1. If we forget the OpenSCAP CLI syntax, where can we look for a reminder?

2. How do I tell what profiles are available?

    a) What if I want to read through the profile prior to a scan?

    b) Help! My security officer is asking for NIST 800-53 and DISA STIG mappings! Where are they?

Request for Feedback

Next rebase of OpenSCAP and SCAP Security Guide will be in RHEL 7.4.

What additional paperwork can we ship to help make accreditation easier?

Remediation!

Bash first

```
<fix system="urn:xccdf:fix:script:ansible">
        - name: Update file permissions on /var/www/
          become: yes
          command: chmod -R 755 /var/www/
</fix>
```

RHEL 7.3 + beyond

Now has support for Ansible, but limited content.

But we can show our upstream work
(estimated RHEL 7.4 release)

#5: Review Remediation

- Where do we find available profile IDs?
  (hint: `oscap info`)

- Extract DoD STIG Remediations for review

```
$ oscap xccdf generate fix \
--template urn:xccdf:fix:script:sh \
--profile <<profile ID>> \
--output /var/www/html/scans/remediation.sh.txt \
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
$ chmod 0755 /var/www/html/scans/remediation.sh.txt
```

Review Results

http://studentX.labs.redhatgov.io/ → "Scan Results" → remediation.sh.txt

“Online Remediation”

```
$ sudo bash
# oscap xccdf eval --remediate \
--profile <<your profile>>
--results scan-results.xml \
--report scan-report.html \
<<SCAP content >>
```

#6: STIG your VM

- Ensure you're root

```
$ sudo bash
```

- The profile ID is obtuse. 'oscap info' to give you something to copy/paste

```
# oscap info /usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

- Here's hoping for no bugs!

```
# oscap xccdf eval --remediate \
--profile <<STIG>> \
--results /var/www/html/scans/stig-results.xml \
--report /var/www/html/scans/stig-report.html \
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

SCAP WORKBENCH DEMO

Download SCAP Workbench

$ sudo yum -y install scap-workbench

For extra details, https://www.open-scap.org/tools/scap-workbench/

We’re done!

Thank you!