RED HAT SUMMIT

Practical OpenSCAP

Security Standard Compliance and Reporting

Robin Price II – Senior Solutions Architect
Martin Preisler – Senior Software Engineer

INTRODUCTION

AGENDA

- Review some slides
- Follow along demostration
- Deconstruction of each lab step
- Leave feeling informed and enabled

WHY ARE WE HERE?

WHY ARE WE HERE?

- Computer security has become increasingly important
- Two major approaches can be recognized in computer security:
  - Reactive
  - Proactive
- The **reactive** approach is involved in disaster recover plans
  - Eliminating the threat
  - Switching to alternate systems
  - Attack surface analysis
  - Investigation
  - Remediation of compromised systems
- The **proactive** approach consists of any actions that reduce the risk of damage or compromise.

WHY ARE WE HERE?

- To be able to mitigate consequences of possible attack, the assets at risk must be recognized prior to the attack.

- To properly implement security guidance, target computers need to be hardened and continuously monitored during their lifecycle.

- The major focus of this work is to accommodate compliance audit in large infrastructure deployments using open source software.

- The objective is to enable users to perform the security audit on multiple remote systems from a single, centralized environments.

WHAT IS SCAP?

WHAT IS SCAP?

- **Security Content Automation Protocol** (SCAP) is a collection of standards managed by **National Institute of Standards and Technology** (NIST). It was created to provide a standardized approach to maintaining the security of enterprise systems, such as automatically verifying the presence of patches, checking system security configuration settings, and examining systems for signs of compromise.

- The key step in the implementation of SCAP within the organization is having the security policy in the form of SCAP.

- It is a collection of data formats.

WHAT IS SCAP?

- For each of the SCAP components mentioned, the standard defines a document format with syntax and semantics of the internal data structures.

- All the component standards are based on **Extensible Markup Language** (XML) and each component standard defines its own XML namespace.

- Any tool which is certified against SCAP 1.2 is **required** to understand all of the previous versions of the component standards.

SCAP COMPONENTS

- SCAP encompassed several underlying standards. The component standards of SCAP include:
  - Languages:
    - **OVAL®**: A language for making logical assertions about the state of an endpoint system.
    - **XCCDF**: A language to express, organize, and manage security guidance that references OVAL.
    - **OCIL**: Open Checklist Interactive Language: a language to provide a standard way of querying a human user.
    - **ARF**: Asset Reporting Format: a language to express the transport format of information about assets, and the relationships between assets and reports.
  - Enumerations:
    - **CCETM**: Common Configuration Enumeration: an enumeration of security-relevant configuration elements for applications and operating systems
    - **CPETM**: Common Platform Enumeration: a structured naming scheme used to identify information technology systems, platforms, and packages.
    - **CVE®**: Common Vulnerabilities and Exposures: an enumeration of security-relevant configuration elements for applications and operating systems.

SCAP COMPONENTS

- SCAP encompassed several underlying standards. The component standards of SCAP include (cont.):
  - Metrics:
    - **CVSS**: Common Vulnerability Scoring System: metrics to assign a score to software vulnerabilities to help users prioritize risk.
    - **CCSS**: Common Configuration Scoring System: metrics to assign a score to security-relevant configuration elements to help users prioritize responses.

WHAT IS OPENSCAP?

WHAT IS OPENSCAP?

- A **framework** of **libraries** and **tools** to improve the accessibility of SCAP and enhance the usability of the information it represents.

- OpenSCAP components:
  - **Library** - OpenSCAP library provides API to SCAP document processing and evaluation.

  - **Toolkit** – SCAP scanner (**oscap**) is a command line tool that provides various SCAP capabilities; for instance: configuration scanner, vulnerability scanner, SCAP content validation and transformation etc.

- On 04/29/2014 OpenSCAP project received SCAP 1.2 certification from NIST.
  - **http://nvd.nist.gov/scapproducts.cfm**

WHAT IS OPENSCAP?

- The **OpenSCAP Tool (oscap)** was developed after the OpenSCAP library was mature enough to perform the scan and was the only missing piece (thanks, Peter Vrabec!).

- The **shared library** offers wide selection of SCAP functionality, however only a limited set of features is needed in day-to-day use of SCAP.

- The **oscap** command-line utility is a simple front-end to the **OpenSCAP library**, it groups its functionality into sub-commands called modules.
  - “xccdf eval”
  - “generate fix”

WHAT TOOLING IS AVAILABLE FOR SCAP?

- **OpenSCAP**: suite of open source tools and libraries for security automation
- **OpenSCAP Scanner**: command line tool for configuration and vulnerability measurements
- **SCAP Workbench**: a GUI tool for scanning and content tailoring, GUI front-end for OpenSCAP
- **SCAP Security Guide**: The project provides pre-built profiles for common configuration requirements, such as DoD STIG, PCI, CJIS, and the Red Hat Certified Cloud Provider standards.
- **OSCAP Anaconda**: An add-on for the Anaconda installer that enables administrators to feed security policy into the installation process and ensure that systems are compliant from the very first boot.
- **Red Hat Satellite**: Centralized systems life-cycle manager with enterprise vulnerability measurements.
- **Red Hat CloudForms**: to manage security through the full life cycle of systems and apps in open hybrid cloud environments (want to scan Amazon AMIs?).
- **Red Hat Atomic:** The ability to scan Docker container images.

WHAT TOOLING IS AVAILABLE FOR SCAP?

- **OpenSCAP**: suite of open source tools and libraries for security automation
- **OpenSCAP Scanner**: command line tool for configuration and vulnerability measurements
- **SCAP Workbench**: a GUI tool for scanning and content tailoring, GUI front-end for OpenSCAP
- **SCAP Security Guide**: The project provides pre-built profiles for common configuration requirements, such as DoD STIG, PCI, CJIS, and the Red Hat Certified Cloud Provider standards.
- **OSCAP Anaconda**: An add-on for the Anaconda installer that enables administrators to feed security policy into the installation process and ensure that systems are compliant from the very first boot.
- **Red Hat Satellite**: Centralized systems life-cycle manager with enterprise vulnerability measurements.
- **Red Hat CloudForms**: to manage security through the full life cycle of systems and apps in open hybrid cloud environments (want to scan Amazon AMIs?).
- **Red Hat Atomic:** The ability to scan Docker container images.

LAB: Part 1

Language Standards
(data formats)

Check Language - OVAL

WHAT IS OVAL?

- OVAL - The **Open Vulnerability Assessment Language**

- OVAL is an open specification to represent the technical aspects of evauluating compliance with a security guidance line item such as the installation of a specific patch.

- The main goal of the **OVAL** standard is to enable interchangeability among security products.

- OVAL checks are intended to be used by automated assessment tools to **evaluate a system's compliance** without requiring user input or intervention.

- OVAL can be used to assess a system's compilance with a configuration settings, perform an inventory of software that is install on a system, identify missing patches on a system, and determine when a system has a specific vulerability present.

WHAT IS OVAL?

- Unlike other tools or custom scripts, the **OVAL** language describes a desired state of resources in declarative manner.
- The declarative character of **OVAL** language ensures that the state of assessed system will not be accidentally modified, which is important as security scanners are often run with highest possible privileges.
- The **OVAL** file contains definitions.
  - These definitions have unique IDs assigned.
  - Each definition evaluates to true or false or it fails to evaluate at all.
- While it is possible to use **OVAL** without **XCCDF**, you don't get nice titles, nice descriptions and nice IDs.

Checklist Language - XCCDF

WHAT IS XCCDF?

- XCCDF - **The eXtensible Configuration Checklist Description Format**
- XCCDF is a document format to support integration with multiple underlying configuration checking 'engines'.
- The primary uses of a checklist language standard are **authoring checklists** and **executing checklists**(evaluating a system based on the crteria defined in a checklist).
- XCCDF is a checklist language **most often used** for security checklists.
- It is meant to be transformed into human readable prose guides.

WHAT IS XCCDF?

- Initial purpose was to facilitate the **transmission**, **distribution**, and **automated** use of security checklists.

- **Before** the advent of XCCDF, checklists were **created by individuals** in various document formats such as **text documents** and **spreadsheets**.

- XCCDF enables sharing of checklists among organizations and enables the use of those checklists within various assessment tools through the use of a standard, open format for representing security check to be performed.

- XCCDF uses XML file format for presenting configuration requirements. This format is vendor and platform independent and is freely available.

- While it is possible to use **XCCDF** without **OVAL**, this will not evaluate the rules and you are stuck with just a nice descriptive hierarchy of rules.

Asset Language - ARF

WHAT IS ARF?

- ARF – the **Asset Reporting Format**

- Asset language standards provide **framework for documenting information** related to a variety of assests, including computers, networks, software, and hardware.

- Asset Reporting Format defines how to express information (results or compliance status) about assets in a way that can be transported from one computer to another, including standardized reporting formats.

WHAT ARE DATASTREAMS?

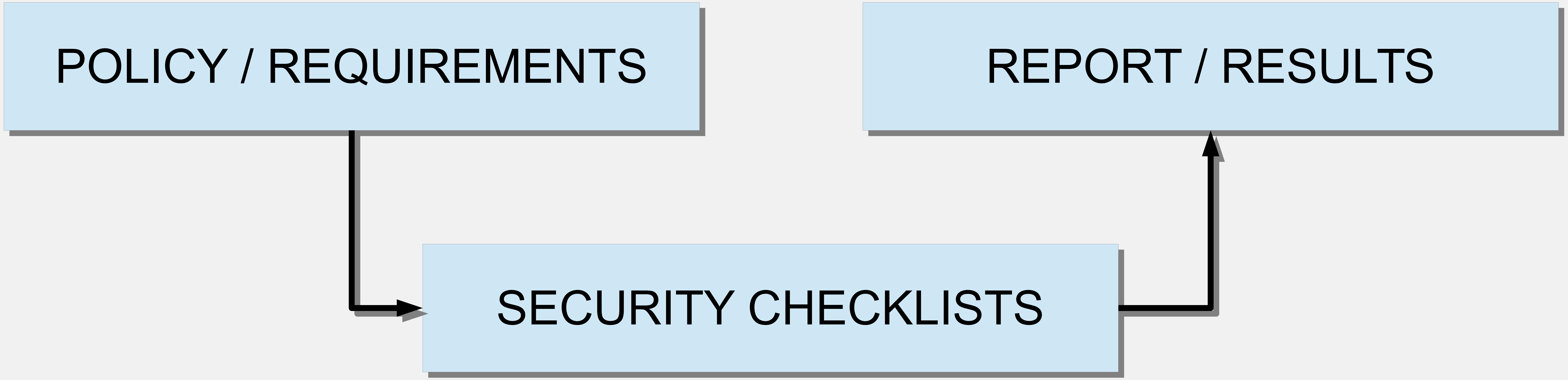
WHAT ARE DATASTREAMS?

- Source DataStream is a new file format introduced by SCAP 1.2 specification
  (Its sole purpose is to bundle other SCAP component files into a single file)

- That is based on the insight that one file is much easier to deploy when compared to a group of files.

- And it supports digital signatures. This will allow us to ship signed content in the future.

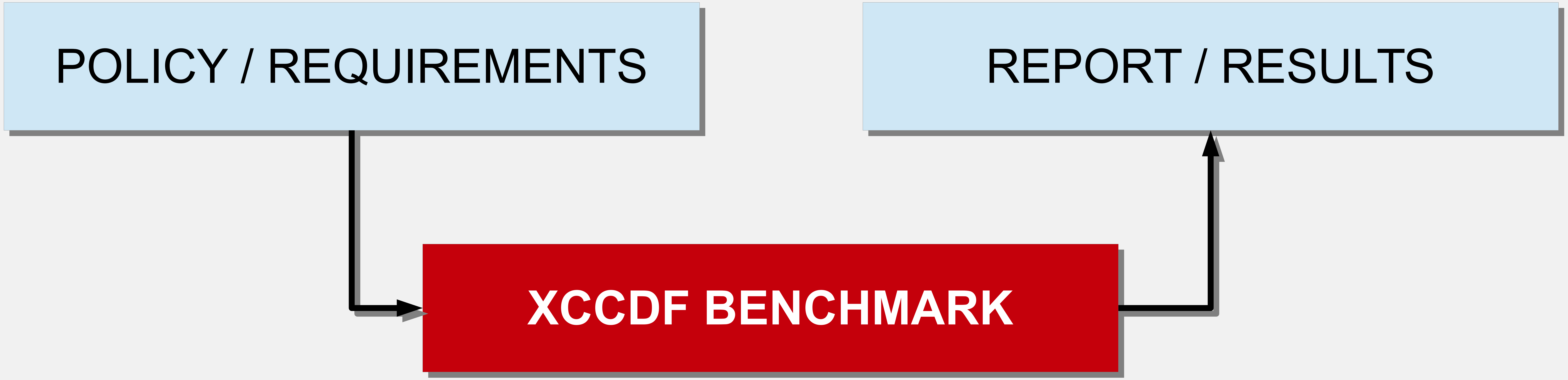
Checklist and Check language interaction



POLICY / REQUIREMENTS

SECURITY CHECKLISTS

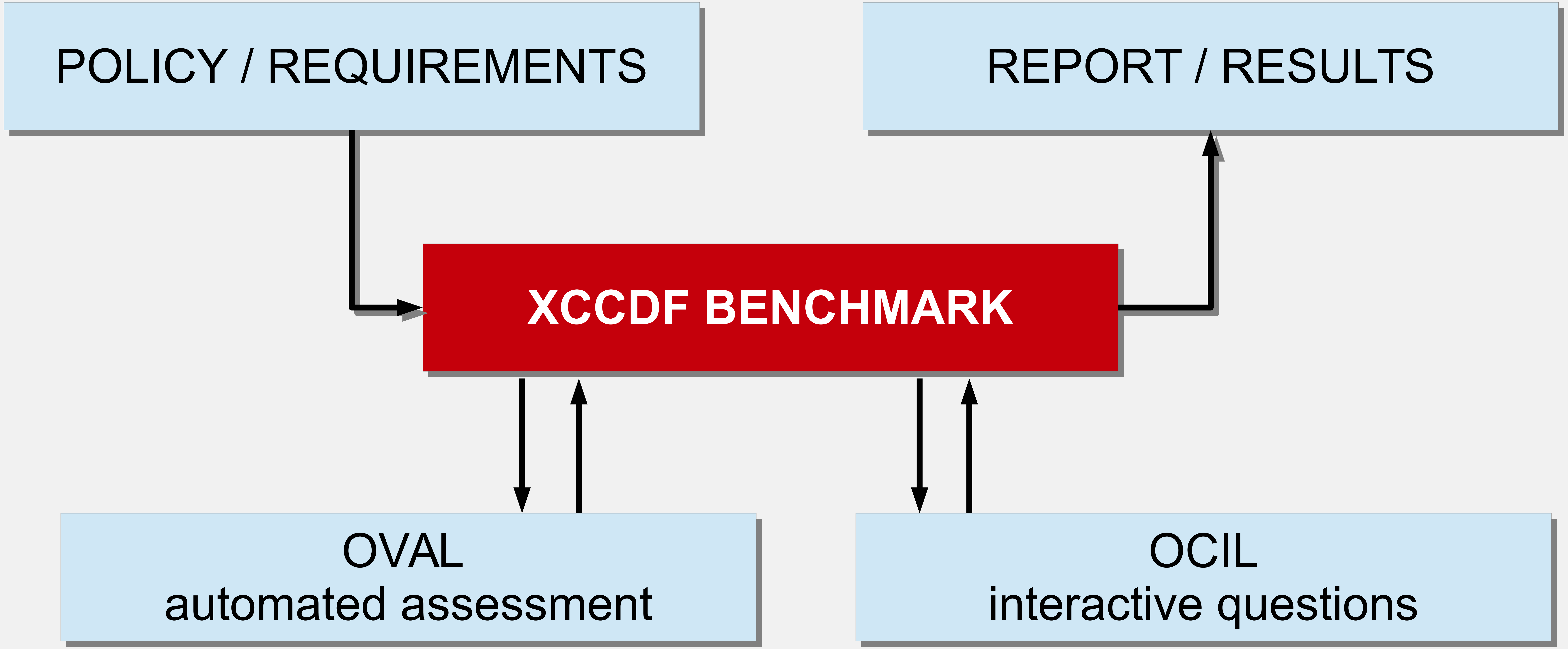
REPORT / RESULTS



POLICY / REQUIREMENTS

XCCDF BENCHMARK

REPORT / RESULTS



POLICY / REQUIREMENTS

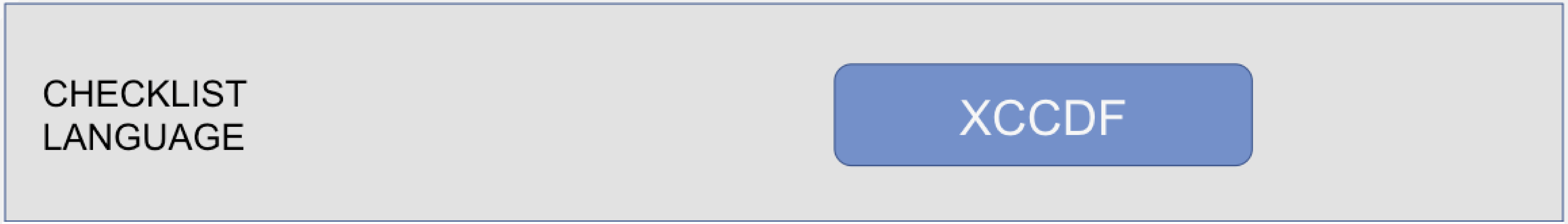
REPORT / RESULTS

XCCDF BENCHMARK

OVAL
automated assessment

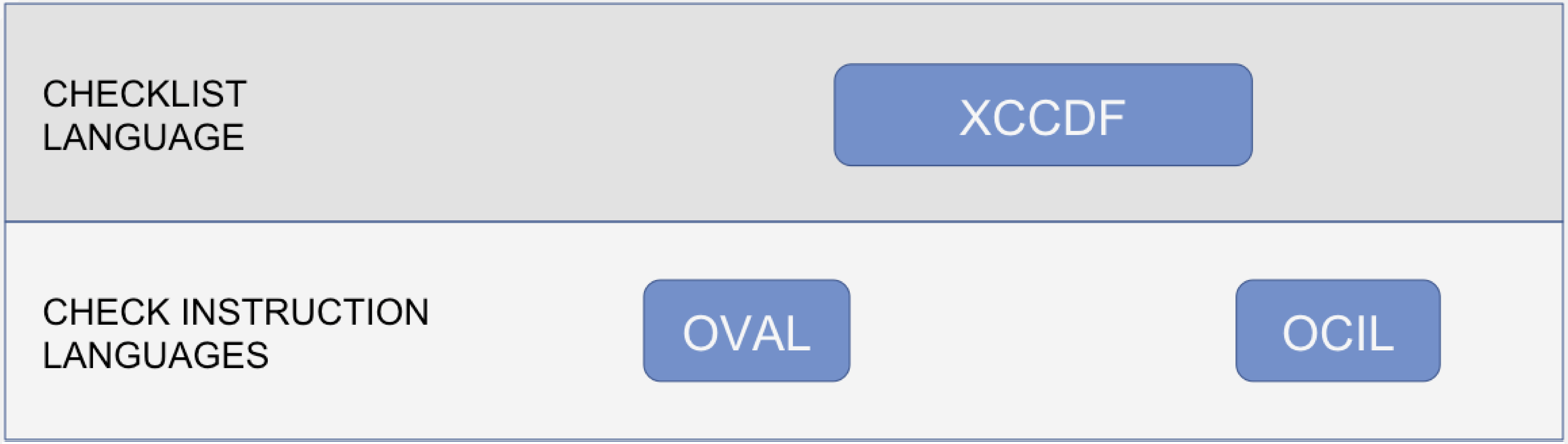
OCIL
interactive questions

SCAP component interaction



CHECKLIST LANGUAGE

XCCDF



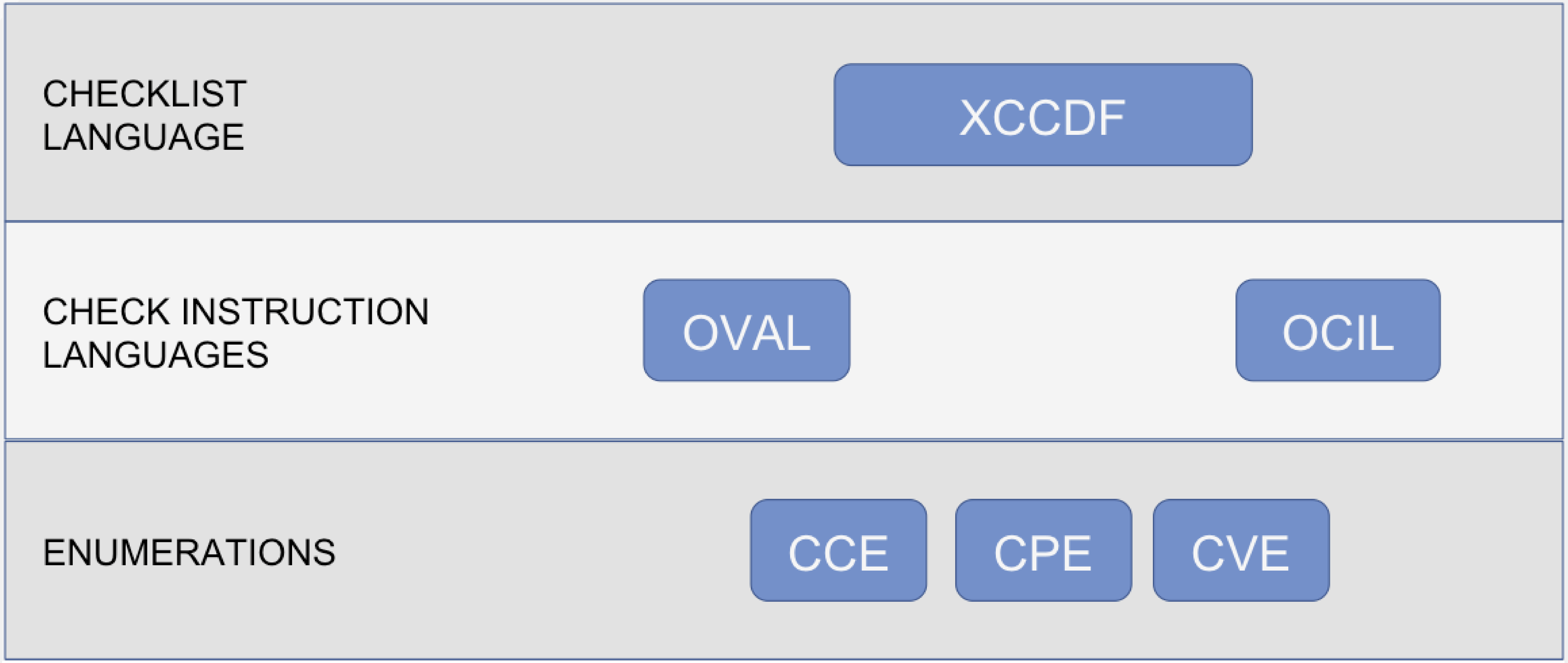
CHECKLIST LANGUAGE

XCCDF

CHECK INSTRUCTION LANGUAGES

OVAL

OCIL



CHECKLIST LANGUAGE

XCCDF

CHECK INSTRUCTION LANGUAGES

OVAL

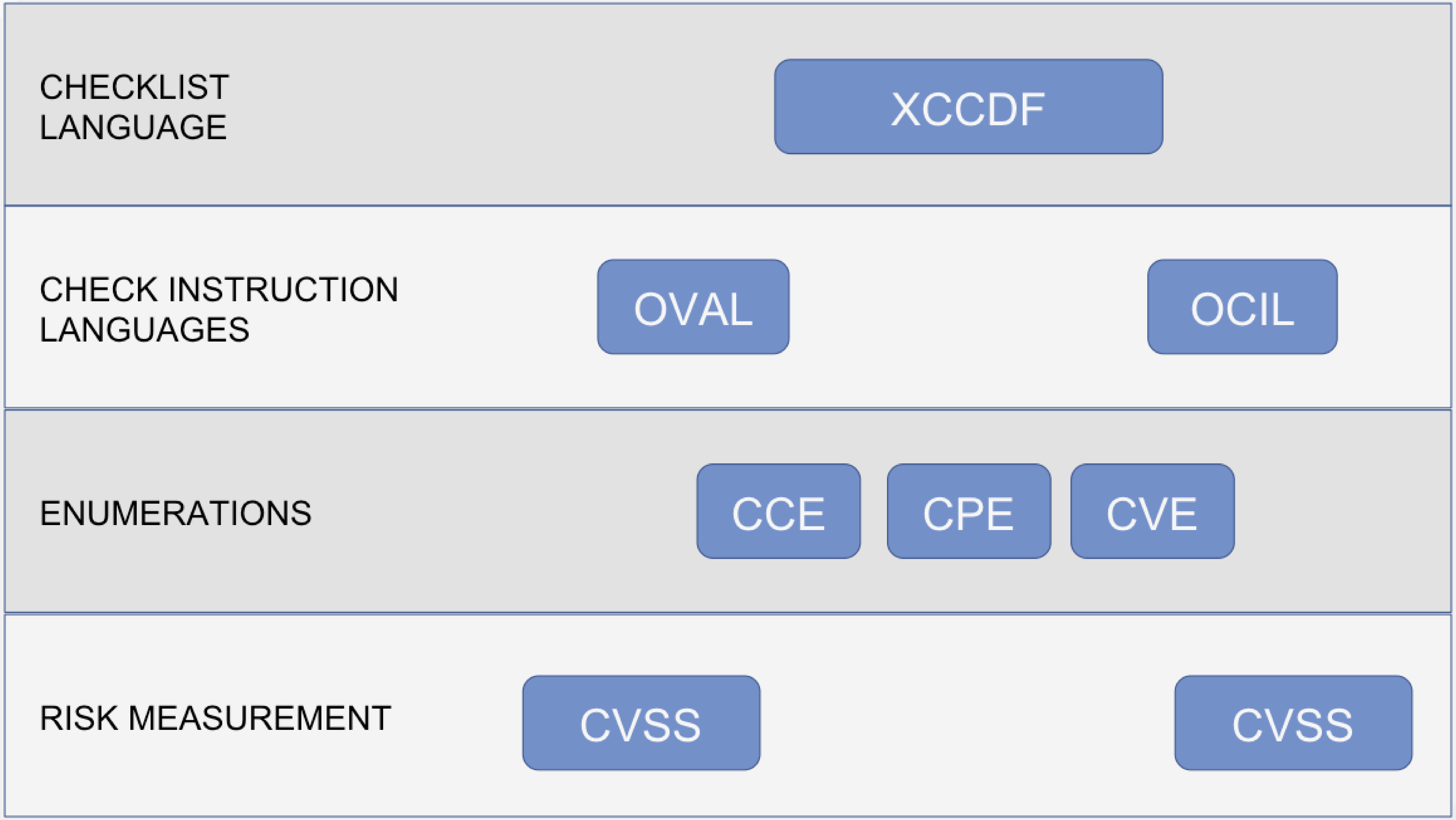
OCIL

ENUMERATIONS

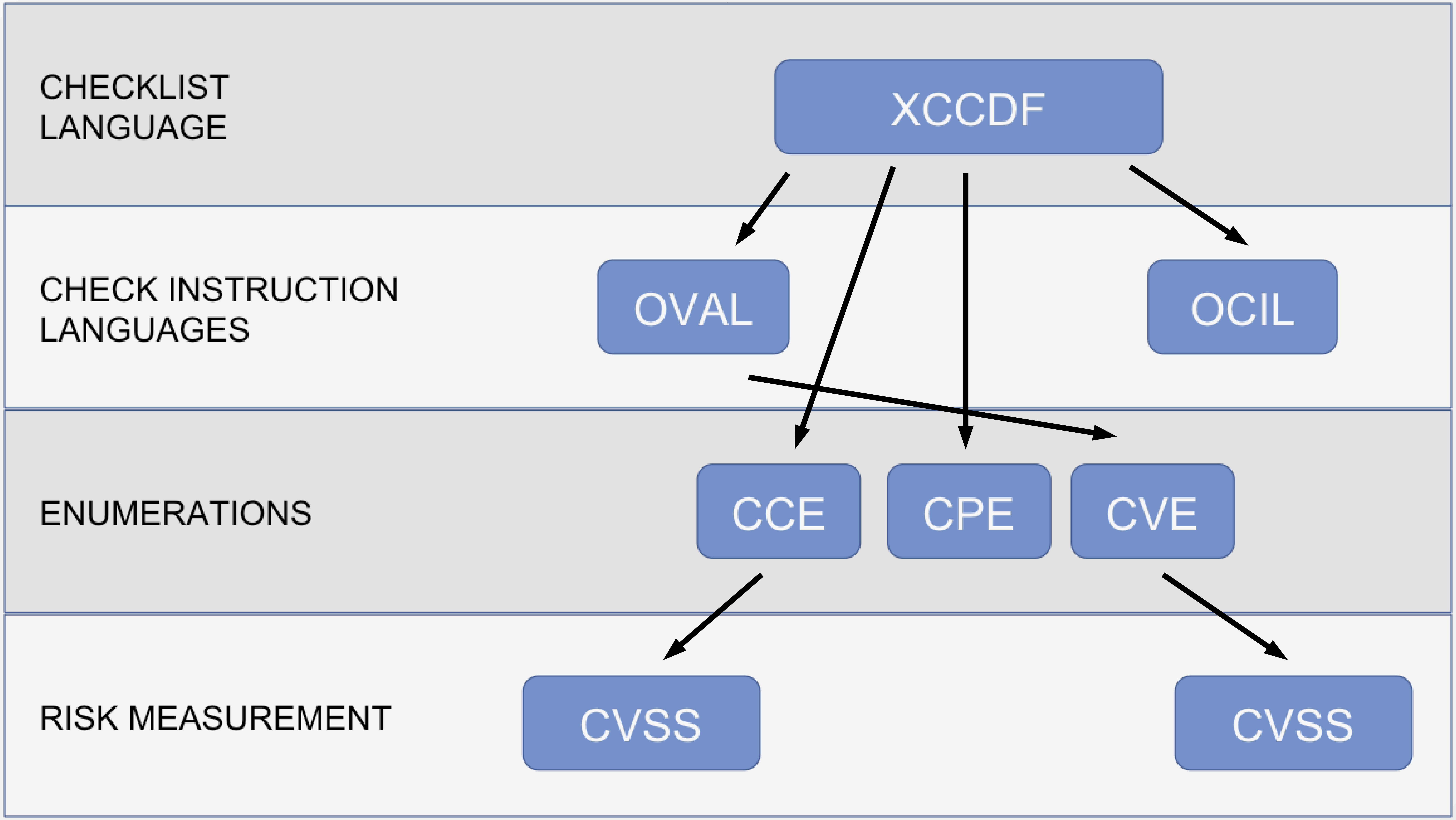
CCE

CPE

CVE



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

SCAP SECURITY GUIDE

WHAT IS SCAP SECURITY GUIDE?

- The project provides practical security hardening advice for Red Hat products and also links it to compliance requirements in order to ease deployment activities, such as certification and accreditation.

- The project started in 2011 as open collaboration of U.S. Government bodies to develop next generation of **United States Government Baseline** (USGCB) available for Red Hat Enterprise Linux 6.

- In addition to the policy for Red Hat Enterprise Linux 6 and 7, there are policies growing for other Red Hat products (JBoss Application Server , Java, Webmin, Tomcat/Apache pending)

- Take policy requirements and present them as machine readable formats.

LAB: Part 2

SCAP WORKBENCH?

WHAT IS SCAP WORKBENCH?

- **SCAP Workbench** is a GUI tool that serves as an SCAP scanner and provides tailoring functionality for SCAP content.
- It uses the **OpenSCAP library** and its oscap tool to do all evaluation.
- SCAP Workbench only scans a single machine.
- The assumption is that this is enough for users who want to scan a few machines and users with huge amount of machines to scan will just use **`scap-workbench`** to test or hand-tune their content before deploying it with more advanced tools like **Red Hat Satellite** or **Red Hat Cloudforms**.

WHAT IS SCAP WORKBENCH?

- Feature highlights include:
  - Linux, Windows, MacOS X support
    - Windows support – including a native MSI installer
    - MacOS X support – including a native dmg image
  - Evaluation of local machine
  - Evaluation of remote machine (using ssh)
  - Profile customization support - selection and unselection of rules, value changes
  - Exporting content as RPM or into a directory

SPECIAL THANKS

- Special Thanks to the following people for helping us along the way:
  - https://github.com/OpenSCAP/openscap/graphs/contributors
  - https://github.com/OpenSCAP/scap-security-guide/graphs/contributors
    - Šimon Lukašík
    - Jan Lieskovsky
    - Jan Černý
    - Zbyněk Moravec
    - Josh Bressers
    - Eric Christensen
    - Kurt Seifried
    - Shawn Wells
    - Jeff Blank
  - https://github.com/OpenSCAP/scap-security-guide/wiki/Collateral-and-References
  - https://www.open-scap.org

RED HAT SUMMIT

LEARN. NETWORK.
EXPERIENCE OPEN SOURCE.