Introduction to OVAL

"Open Vulnerability and Assessment Language"

Agenda

- What is OVAL?
- MITRE’s Role
- Components of the OVAL Language
- OVAL Process
- OVAL ID Structure
- OVAL Versioning
- OVAL Roadmap

What is OVAL?

an international, information security, community standard to promote open and publicly available security content, and to standardize the transfer of this information across the entire spectrum of security tools and services.

- Three main components to OVAL
  - XML language for expressing machine state & reference implementation
    - checking system
  - Repository of content written in OVAL
  - Compatibility Program

OVAL Language

- Community developed standard
- Standardizes the three main steps of the assessment process
  - Representing configuration information of systems for testing
  - Analyzing the system for the presence of a specified machine state
  - Reporting the results of the assessment
- Can describe many different machine states
  - Vulnerable
  - Non-compliant
  - Installed asset
  - Patched

http://oval.mitre.org/language

OVAL Interpreter

- freely available reference implementation
- demonstrates usability of the OVAL Language
- drives the development of the OVAL Language
- validate & test content
- reduce the cost of OVAL adoption

http://oval.mitre.org/language/download/interpreter

OVAL Repository

- What are the goals?
  - promote open and publicly available
  - **free** to use
  - bring together the knowledge in the community to create the best possible content

- What is covered?
  - Vulnerability, Inventory, and Patch Definitions
  - Windows, Solaris, OpenSuse, ...

http://oval.mitre.org/repository

OVAL Compatibility Program

- develop consistency of use and implementation
- established a set of guidelines that help enforce a standard implementation
- provide assurance that a product’s implementation of OVAL coincides with the standard set forth

http://oval.mitre.org/compatible

MITRE's role in OVAL ...

MITRE is an FFRDC

not for profit -

work in the public interest -

Government contracts -

OVAL Moderator

promote growth -

guide development of language -

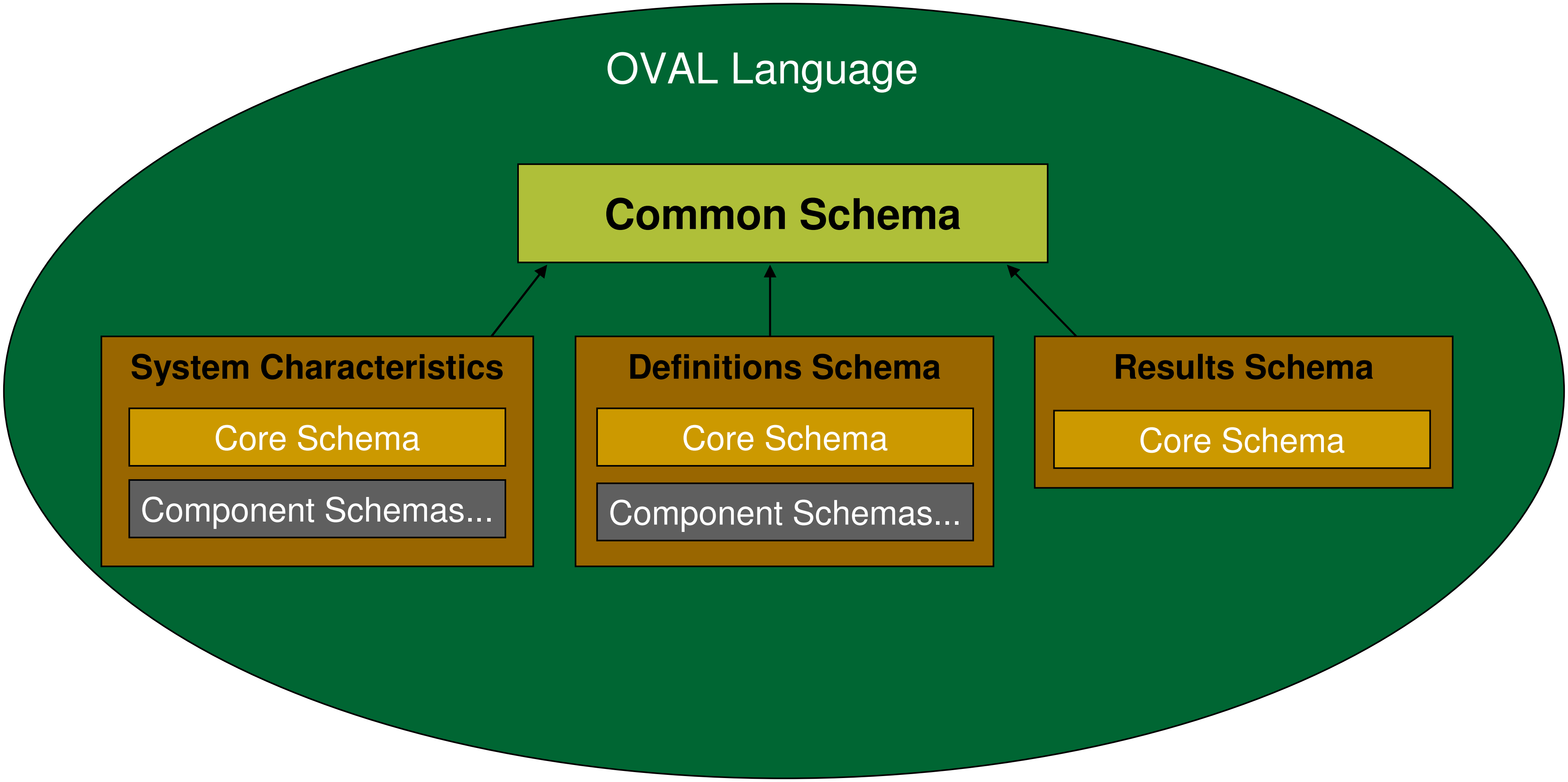
facilitate OVAL Board -

compatibility program -

OVAL Language: 3 Core Schemas

- OVAL Definitions Schema
  - framework for logical assertions about a system
- OVAL System Characteristics Schema
  - encoding of the details of a system
- OVAL Results Schema
  - encoding of the detailed results of an analysis

Core schemas relationships


OVAL Language

Common Schema

System Characteristics

Core Schema

Component Schemas...

Definitions Schema

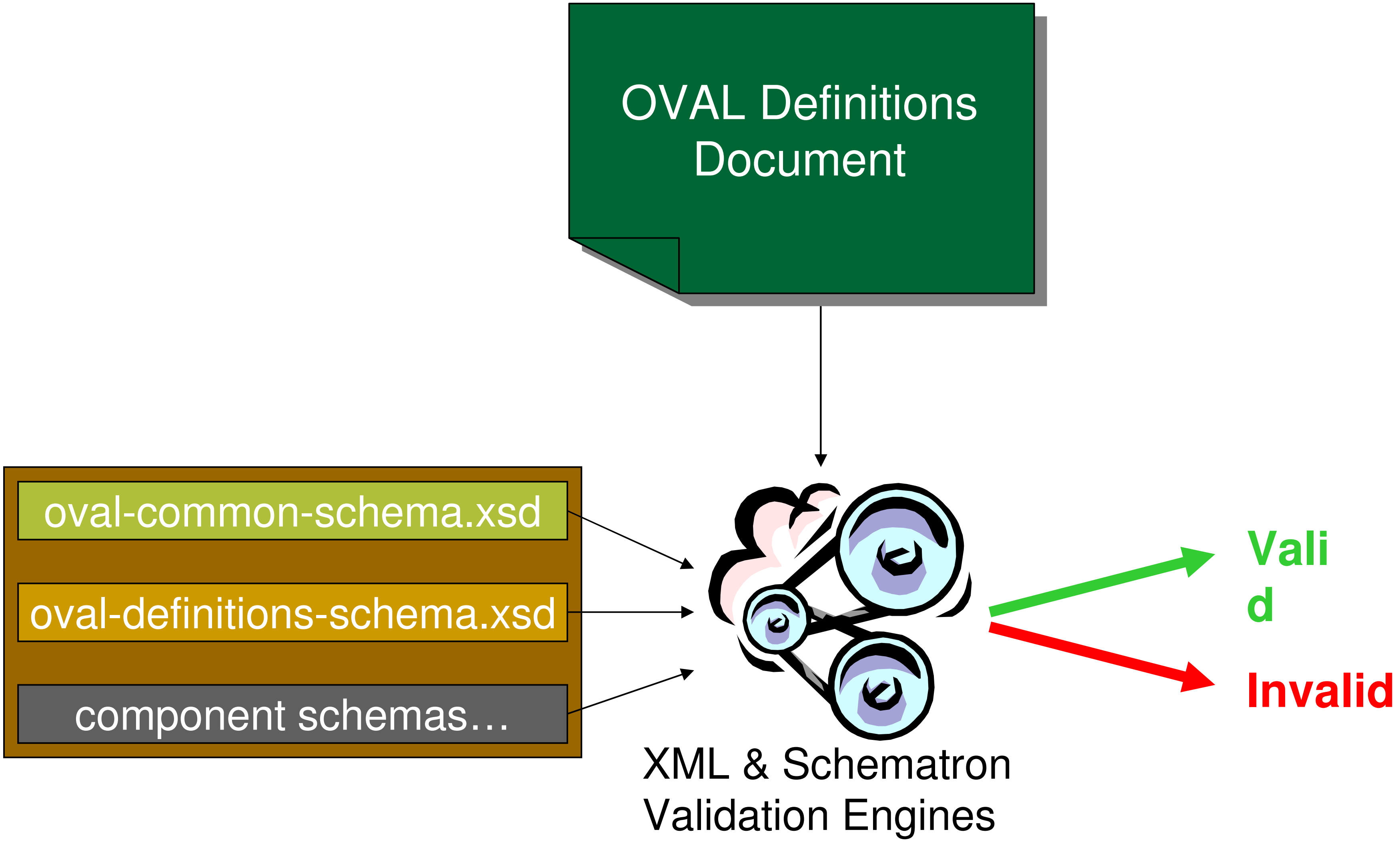
Core Schema

Component Schemas...

Results Schema

Core Schema

OVAL Document Validation Process



OVAL Definitions Document

oval-common-schema.xsd

oval-definitions-schema.xsd

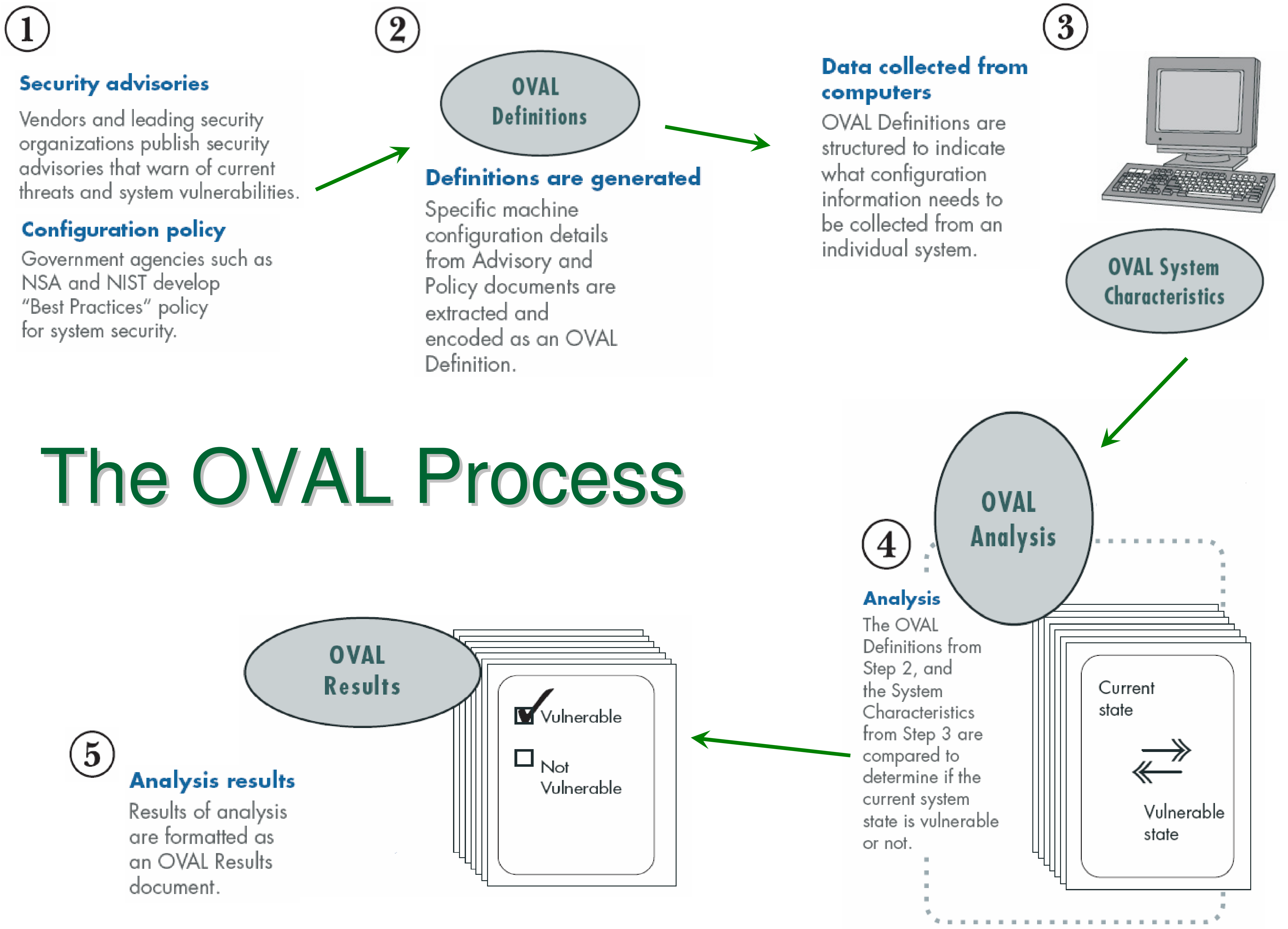
component schemas…

XML & Schematron Validation Engines

Vali
d

Invalid

The OVAL Process



1

Security advisories

Vendors and leading security organizations publish security advisories that warn of current threats and system vulnerabilities.

Configuration policy

Government agencies such as NSA and NIST develop "Best Practices" policy for system security.

2

Definitions are generated

Specific machine configuration details from Advisory and Policy documents are extracted and encoded as an OVAL Definition.

3

Data collected from computers

OVAL Definitions are structured to indicate what configuration information needs to be collected from an individual system.

4

Analysis

The OVAL Definitions from Step 2, and the System Characteristics from Step 3 are compared to determine if the current system state is vulnerable or not.

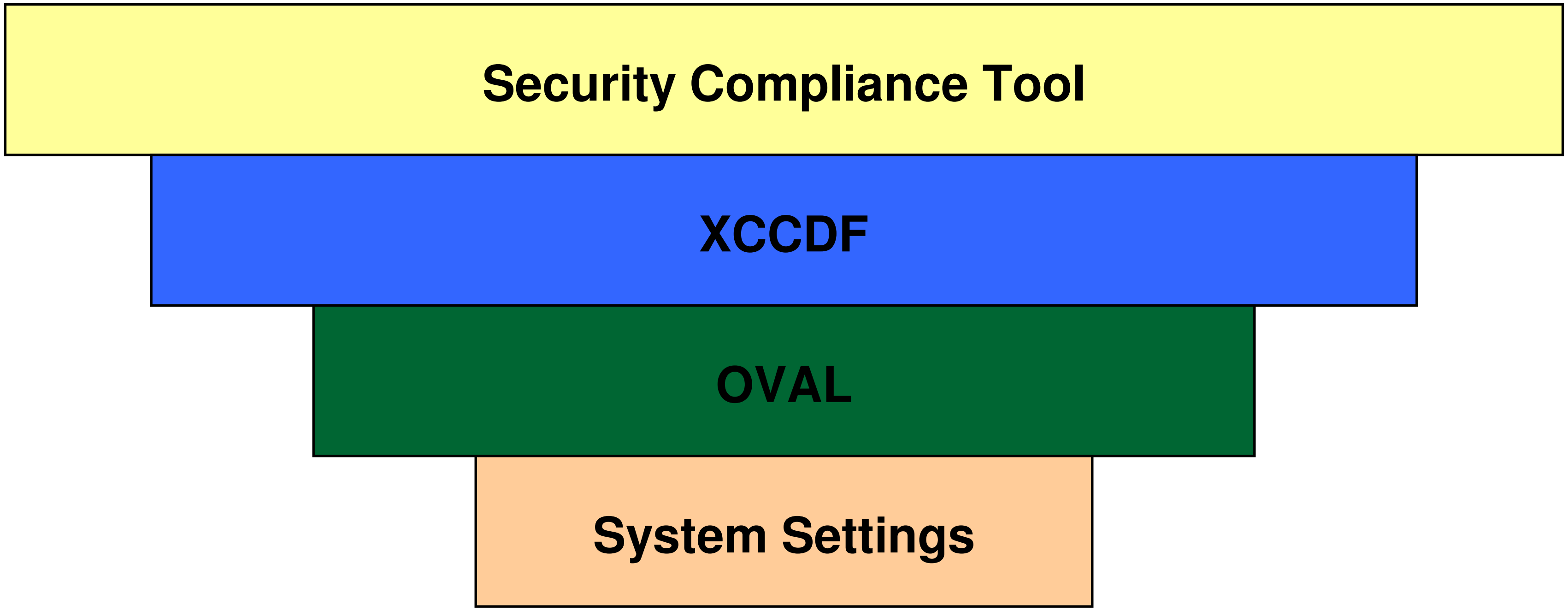
5

Analysis results

Results of analysis are formatted as an OVAL Results document.

XCCDF And OVAL

OVAL is how XCCDF "talks" to the system that a guide is written for.



Each layer is built on top of the layer below it.

OVAL ID Format

- **Globally unique urn**
  - oval : org.mitre.oval : def : 123
- **four parts**
  - prefix ‘oval’
  - organization DNS name (reverse order)
  - ID type (def, tst, ste, obj, var)
  - ID value (unique integer)
- **use the same organization DNS for every id in the repository**
  - OVAL Repository - org.mitre.oval
  - Red Hat - com.redhat
  - SCAP - gov.nist.scap (???)

Creating New IDs

- OVAL Repository content
  - request valid ID from MITRE
    - web service
  - use your own
    - organizational DNS name and ID value
    - we will convert to an org.mitre.oval ID
- External Repository content
  - responsible for id uniqueness

Versioning Process

- 4 phases identified
  - Planning
  - Draft
  - Release Candidate
  - Official

- Time interval between each phase depends on the magnitude of the release and the amount of community activity.

Versioning Process - Minor

- Backward compatible
- Generally only additions
  - New tests
  - New component schemas
  - New behaviors
- No changes to xmlns

Versioning Process - Major

- Not Backward compatible
- Requires retesting of OVAL Compatible tools

- Changes xmlns
  - For version 5.x base xmlns is:

    `http://oval.mitre.org/XMLSchema/oval-definitions-5`
  - For version 6.x base xmlns will be:

    `http://oval.mitre.org/XMLSchema/oval-definitions-6`

- For more information see:

  http://oval.mitre.org/language/about/versioning.html

OVAL Roadmap

- OVAL Language Plans
  - Minor
    - Plan on 3-4 per year.
  - Major
    - No date set
    - Collecting data now
    - Likely to see serious development in 2008
- OVAL Repository Plans
  - Incremental improvements to content access
  - Growth
    - Plan to support all of NIST's OVAL content
    - Plan to support definitions for CPE
    - Several orgs have promised large amounts of content
- Other Repositories on the way
- Compatibility
  - Rewrite to coincide with next major version.

OVAL Resources

- Web site: http://oval.mitre.org
- Mailing list registration: http://oval.mitre.org/community/registration.html
- oval-developer-list
  - The place to discuss the standard itself
- oval-discussion-list
  - The place to discuss the content in the OVAL Repository
- Mailing list archives: http://oval.mitre.org/community/archives/

Questions?