HS SEDI
Homeland Security Systems Engineering and Development Institute

Jon Baker
November 1, 2011

Homeland Security

OVAL Overview

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.

- **Open Vulnerability and Assessment Language**
  - A community-developed open standard
  - Since December 2002
  - Enables automated assessment and compliance checking
- **OVAL Language**
  - XML-based framework for making logical assertions about a system
    - Vulnerable, Compliant, Installed application, Patched
  - OVAL Interpreter
    - An open source reference implementation
- **OVAL Repository**
  - A collection of community contributed OVAL Definitions
- **OVAL Adoption**
  - Educate vendors, receive constructive technical feedback, and lists adopters

MITRE's Role in OVAL

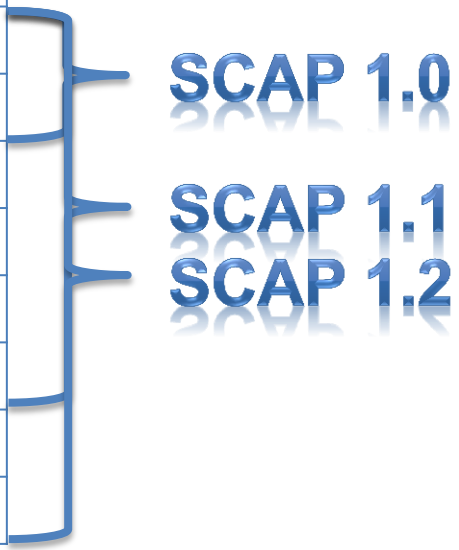
- **MITRE is a not-for-profit corporation, chartered to work solely in the public interest.**
  - MITRE operates Federally Funded Research and Development Centers (FFRDCs).
  - Non-compete charter fosters "trusted moderator" status.
  - Work in the public interest.
  - Government sponsored.

- **OVAL Moderator**
  - Help drive consensus between government customers and greater community with technical solutions and changes.
  - Promote the **growth and adoption** of OVAL.
  - **Listen** to the community and guide the development of OVAL.
  - **Facilitate** the OVAL Board.
  - **Moderate** the OVAL Repository.
  - **Balance different perspectives** to arrive at the consensus solution that is best for OVAL and the public interest.

OVAL Releases

- Minor releases add tests, minor capabilities, and critical fixes.
- Releases occur as needed by the community (approx. 2 per year).
- All releases are approved by the OVAL Board.

Version	Release Date
OVAL 5.0	June 16, 2006
OVAL 5.1	November 6, 2006
OVAL 5.2	January 31, 2007
OVAL 5.3	June 27, 2007
OVAL 5.4	April 10, 2008
OVAL 5.5	October 1, 2008
OVAL 5.6	September 11, 2009
OVAL 5.7	May 12, 2010
OVAL 5.8	September 15, 2010
OVAL 5.9	February 2, 2011
OVAL 5.10	September 14, 2011



SCAP's Use of OVAL

- **OVAL provides the low level system assessment capability.**
  - SCAP Validated products use OVAL Definitions as the basis for system assessments (patched, vulnerable, compliant, compromised, application installed).

- **OVAL's Use Cases**
  1. **Security Advisory Distribution** - Defining the conditions under which the issue exists.
  2. **Vulnerability Assessment** - Detecting the presence of the issue.
  3. **Patch Management** - Determining if the patch can be installed.
  4. **Configuration Management** - Defining the desired configuration and monitoring systems.
  5. **System Inventory** - Describing how to detect an installed application.
  6. **Malware and Threat Indicator Sharing** - Describing the possible locations of malware or threat artifacts and indicators.
  7. **Network Access Control (NAC)** – Defining the policy for network access.
  8. **Auditing and Centralized Audit Validation** - Representing detailed system assessment results over time.
  9. **Security Information Management Systems (SIMS)** - Standardized assessment result format for consumption and fusion with other sensor inputs.

What's new for OVAL 5.9?

- **A bug fix release.**
  - Corrected invalid XML Schema construct
  - Corrected Schematron defects
  - Documentation corrections and clarifications

OVAL 5.10 - Goals

- **Vetting current tests:**
  - Linux support based upon test results of USGCB for Red Hat EL5.
  - Mac OS X support to ensure Apple baseline is automatable.
  - Address 64 bit issues on Windows
- **Identifying and implementing capabilities that will improve maintainability, extensibility, and reduce implementation burden.**
- **Address open bug and feature requests as appropriate.**
- **Identify and deprecate any unneeded capabilities.**
- **Publish an OVAL Language specification.**

OVAL 5.10 Highlights

- **Refactored RPM related tests to support Red Hat EL 5 USGCB settings.**
- **Enhanced Mac OSX support with plist510_test to better support assessing Macs in future configuration baselines.**
- **Enhanced Microsoft Windows support with the addition of the cmdlet_test to enable assessments of many newer Microsoft applications.**
- **Improved schema documentation.**
- **Added unique and count functions.**
- **Enhanced support for 64 bit Windows.**
- **Published the OVAL Language Specification.**
  - Developing component schema specifications now.
  - Much more documentation on the way…
  - Included in ITU-T x.cybex in which is planned to be finalized in February 2012.
- **Addressed defects with the mask and variable_instance attributes.**
- **Added 'applicability_check' attribute to simplify results processing.**
- **Added capabilities to better support artifact hunting.**

Community Participation

- Developer List
  - 638 Messages
  - 664 Subscribers
- 2 Face-to-face meetings
- 4 Teleconferences

OVAL Test Content

- **A collection of test OVAL Definitions.**
  1. **Developers** use the content to help guide the development of new tools.
  2. **Users** use the content as part of your product evaluations.
  3. **Content authors** use the content as a reference for writing new content.

- **Currently supports core constructs and platform specific tests for Linux, Solaris, Mac, and Windows.**

- **OVAL Adoption program will soon require vendors to show evaluation results.**

- **Migrating to SoureForge.net this fall**
  - Public access to issue trackers
  - Public access to SVN repository to simplify community contributions and make corrections and additions available as they are committed.

https://oval.mitre.org/repository/about/testcontent.html

OVAL Repository

The central meeting place for the community to discuss, analyze, store, and disseminate OVAL Definitions.

- **Active community contributing OVAL Definitions for the latest vulnerabilities.**
- **Coverage for a diverse set of applications and operating systems**
  - Microsoft, Debian, Mozilla, Solaris, Adobe, Apple, and more...
- **12,000 Definition Milestone – October 2011**

Other Public Repositories of OVAL content

debian NIST Novell redhat secpod Security Simplified

OVAL Repository Least Version Support

- **Previous practice:**
  - On the official release date of a given OVAL Language version, all OVAL Repository content was updated.

- **Moving forward:**
  1. Content will only be upgraded if there is a need.
  2. Content authors can write content sing the latest version of the language and we will automatically calculate the least version required for the content when it is submitted.
  3. OVAL Repository downloads will then be made available by lowest required schema version.

- **Currently support OVAL Version 5.9 and Version 5.10.**
- **Support for OVAL versions going back to 5.3 or earlier is being developed.**

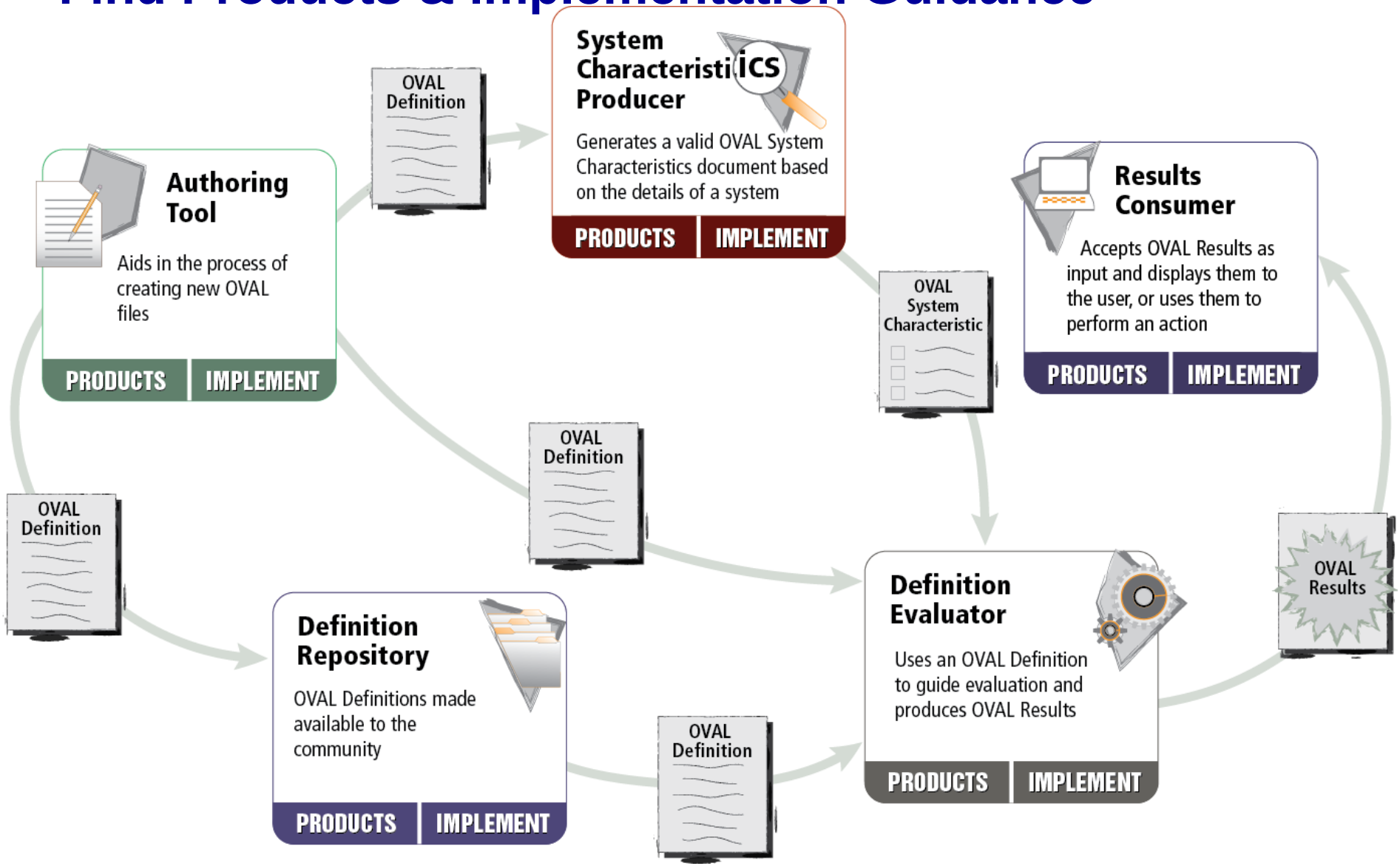
OVAL Adoption Program

Total Participants:
Organizations: 31
Products & Services: 45

- **Provides a channel to both educate organizations about OVAL and receive constructive technical feedback to evolve the standard.**
  - Best practice usage guidance
  - Vendor formal self-assertions
  - Provides MITRE deeper insight into how OVAL is or could be used

- **Defines requirements for how to use OVAL.**
  - Authoring Tool
  - Definition Evaluator
  - Definition Repository
  - Result Consumer
  - System Characteristics Producer

OVAL Adoption Program: Find Products & Implementation Guidance



OVAL Board

- **Actively Engaged**
  - Outreach efforts
  - Release planning and approval
- **Diverse**
  - 27 Organizations from Government, Academia, and Industry
- **Responsibilities**
  - Attend the quarterly board meetings
  - Provide input into strategic direction
  - Actively follow both community forums
  - Provide expert advice about OVAL
  - Look for opportunities to advocate OVAL

Get Involved!

- **Join the OVAL mailing lists**
  - **OVAL-Announce** – General news and announcements about OVAL
  - **OVAL Developer's Forum** – Public forum for discussing the OVAL Language, addressing OVAL implementation issues, and for assisting other developers with OVAL.
  - **OVAL Repository Forum** – Public forum for discussing OVAL Repository content.

    https://oval.mitre.org/community/registration.html

- **Participate in the OVAL Adoption Program**
  - Help shape the effort

    https://oval.mitre.org/adoption/