SCAP Validation

John Banghart

September 29, 2010

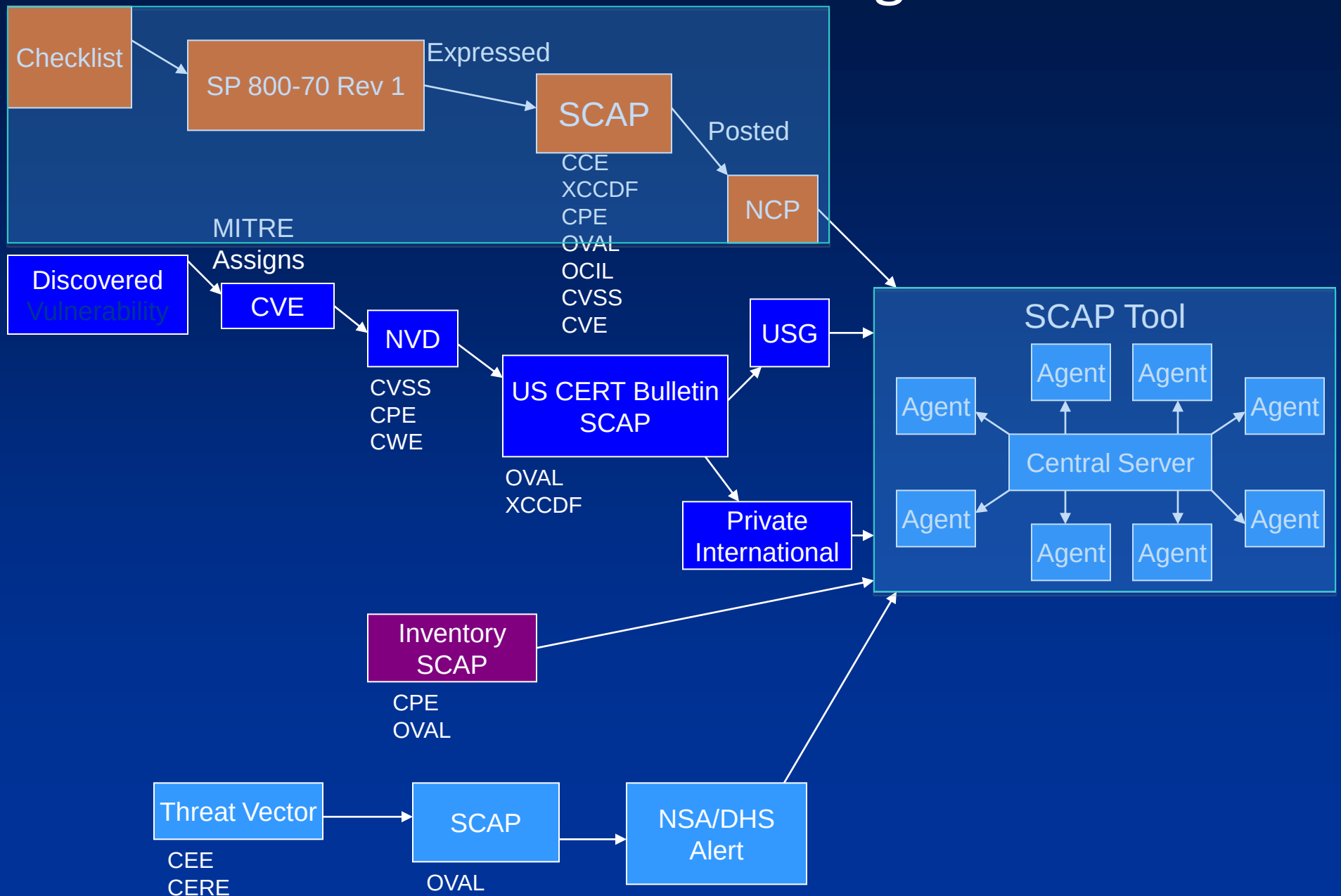
Agenda

- SCAP Validation Program Summary
  - What, Why, Who, Where, How
- Derived Test Requirements
  - Relationship to SCAP Specification
  - Importance to stakeholders
- Looking Ahead
  - USGCB
  - SCAP Roadmap
  - Validation Model
- Open Discussion

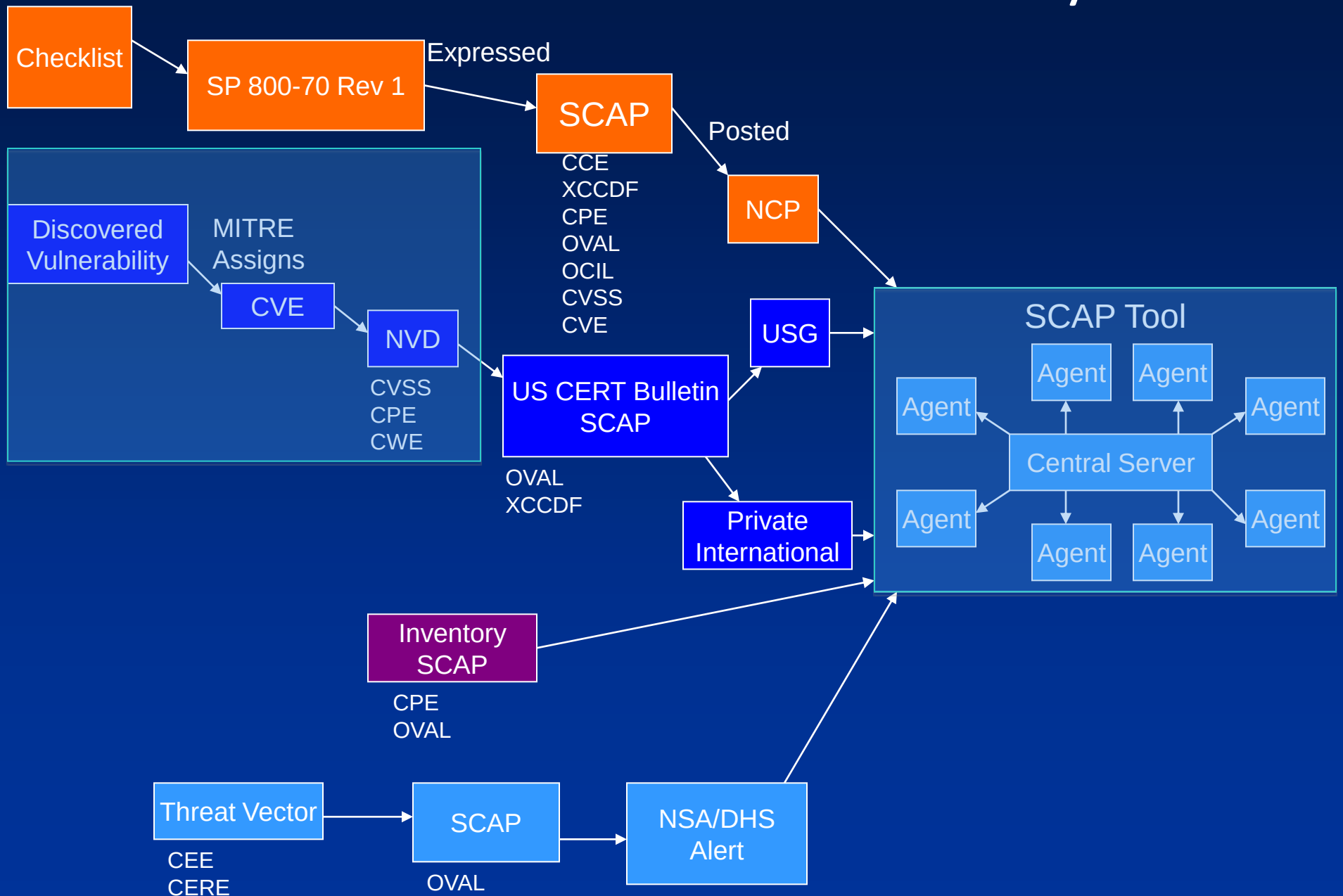
What is it?

- **Supports Business Decisions**
- Provides product conformance testing for Security Content Automation Protocol (SCAP)
  - Awards use case specific validations to products. For example:
    - Configuration assessment
    - Vulnerability assessment

SCAP Use Cases - Configuration



SCAP Use Cases - Vulnerability



Why?

- Originally formed in response to Office of Management and Budget (OMB) directive based on Federal Desktop Core Configuration (FDCC) initiative
- Supports the broader security automation initiative by enabling vendors and organizations a path to adoption and procurement

Who's involved?

- NIST Computer Security Division (CSD)
  - Provides SCAP subject matter expertise
  - Develops test requirements and procedures
  - Reviews test reports and recommends validation
- National Voluntary Laboratory Accreditation Program (NVLAP)
  - Accredits independent testing laboratories
  - 9 labs currently accredited for SCAP testing
- Product vendors seeking validation

SCAP Accredited Labs

http://nvd.nist.gov/scapproducts.cfm

AEGISOLVE

CYGNACOM SOLUTIONS

ICSA labs
An Independent Division of Verizon Business

@SECE

DOMUS
IT Security Laboratory

INFOGARD

COACT INC.

EWA
Enabling a More Secure Future

SAIC
From Science to Solutions

NVLAP

SCAP Validated Products

http://nvd.nist.gov/scapproducts.cfm

Where is it?

- CSD and NVLAP at NIST campus in Gaithersburg, MD

- Labs in Canada and US

How does it work?

- Vendors work with a lab to submit their product for testing
  - NIST does not set cost or duration of testing
- Derived Test Requirements
  - Guide the labs on what tests to perform and what results to expect
- Lab submits test report to NIST CSD for review and approval
- Validated product is listed on web site

Questions/Discussion

Presenter:
John Banghart
john.banghart@nist.gov

Derived Test Requirements (DTR)

- NIST Interagency Report (IR) 7511
- Defines the “bar” that products must meet to be awarded SCAP validation
- Derived from NIST Special Publication (SP) 800-126, the SCAP Specification*
- Examples

* *Maybe not so much*

DTR – Documentation Example

- **XCCDF.R.2: The vendor must assert that the product implements the XCCDF specification and provide a high-level summary of the implementation approach.**
- **Required Vendor Information**
  - XCCDF.V.2: The vendor shall provide a 150 to 500 word English language document to the lab that asserts that the product implements the XCCDF specification and provides a high-level summary of the implementation approach. This content will be used on NIST web pages to explain details about each validated product and thus must contain only information that is to be publicly released.
- **Required Test Procedures**
  - XCCDF.T.2.1: The tester shall inspect the provided documentation to verify that the documentation asserts that the product implements the XCCDF specification and provides a high-level summary of the implementation approach. This test does not judge the quality or accuracy of the documentation, nor does it test how thoroughly the product implements XCCDF.
  - XCCDF.T.2.2: The tester shall verify that the provided documentation is an English language document consisting of 150 to 500 words.

DTR – Technical Example

- **FDCC.R.2: The product shall be able to produce specified FDCC results (both the human and machine-readable versions).**
- **Required Vendor Information**
  - FDCC.V.2: None
- **Required Test Procedure**
  - FDCC.T.2.1: The tester shall validate the XCCDF results produced, on the target platform by the product, against the FDCC reporting Schematron stylesheet and must verify that no validation errors are produced.
  - FDCC.T.2.2: The product documentation shall indicate to the user how they can access the product output as defined in FDCC.T.2.1. The product interface shall make this output available through the product GUI or other user interface.
  - FDCC.T.2.3: The tester shall validate that the human-readable FDCC assessment results provide the CCE ID and the associated pass/fail status corresponding to the XCCDF results required in FDCC.T.2.1. The required result format is the CCE ID, followed by a comma, followed by the words “pass” or “fail” followed by a new line.

DTR – Derived from SCAP Specification

- Future SCAP Specification will contain conformance guidance
  - Test Requirements will map back this conformance guidance to ensure accuracy and completeness
  - Will ensure consistency
  - Really will be “derived”

DTR – Stakeholders

- End user organizations
  - Government and private sector
  - Supports procurement though validation verification
    - For example: “FDCC Scanner”
- Product Vendors/Software Developers
  - What does my product need to do?
- Laboratories
  - How do I test a product?

Questions/Discussion

Presenter:
John Banghart
john.banghart@nist.gov

Looking Ahead - USGCB

- US Government Configuration Baseline (USGCB)
  - Windows 7/IE8
- Following in the footsteps of FDCC, but more of true baseline
- Planned for January, 2011
  - Dependent on finished content
- Future Platforms
  - Red Hat Enterprise Linux 5
  - Others…

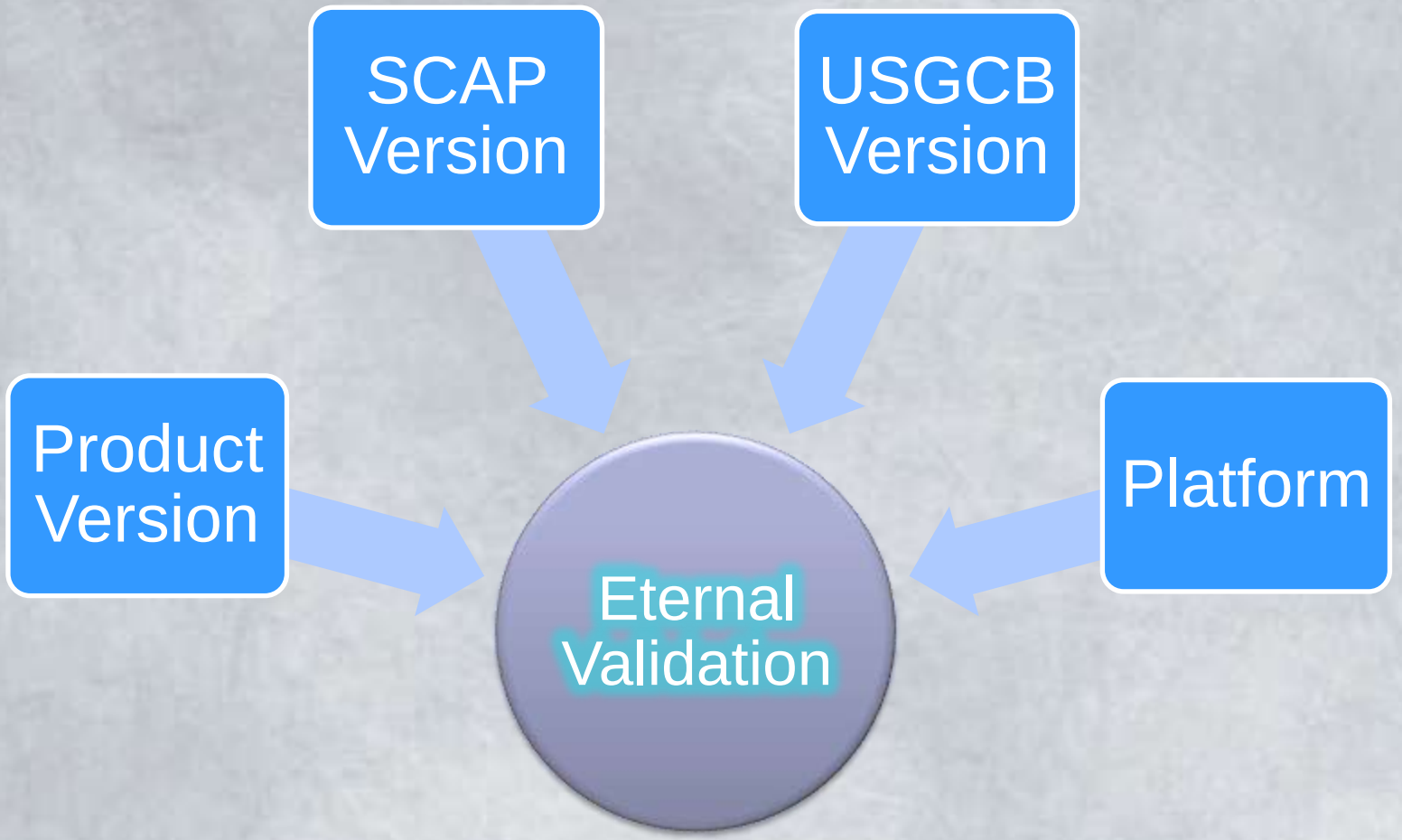
USGCB/FDCC Process

Looking Ahead – SCAP Roadmap

	SCAP 1.0	SCAP 1.1	SCAP 1.2
Scheduled Release Date	Currently Final	Q4, 2010 – Final Version	Q1, 2011 – Initial Draft
Included Specifications	• CVE • CCE 5.0 • CPE 2.2 • XCCDF 1.1.4 • OVAL 5.3, 5.4 • CVSS 2.0	• CVE • CCE 5.0 • CPE 2.2 • XCCDF 1.1.4 • OVAL 5.3, 5.4, 5.5, 5.6, 5.7, 5.8 • CVSS 2.0 • OCIL 2.0	• CVE • CCE 5.0 • CPE 2.3 • XCCDF 1.2 • OVAL 5.3, 5.4, 5.5, 5.6, 5.7, 5.8 • CVSS 2.0 • OCIL 2.0 • ARF 1.0 • AI 1.0

** The release dates of future SCAP revisions and the inclusion of specific component specifications is tentative and subject to change.*

Looking Ahead – Validation Model



Validation Model – Con't

Product Version	• Full or modular? • Major/minor versions?
SCAP Version	• When to validate? • Component parts?
USGCB Version	• Yes
Platform	• Level of specificity? • e.g. RH or all Linux?

Conformance Suite

- Content bundles to exercise all defined SCAP features for a given platform
  - For example, all Windows OVAL tests
  - Specific checklists are subsets
- Public version for pre-validation development and testing
  - Include testing guide
  - Enable end user testing
- More robust reference implementations

Validation Database

- Searchable list of all past and current validations
  - Platform
  - Capability
  - FDCC/USGCB Version
  - Product Name
  - Vendor Name

Questions/Discussion

Presenter:
John Banghart
john.banghart@nist.gov