

The logo features the text "SCAP" in large, bold, white letters with a metallic sheen, and "VALIDATED" in smaller, bold, black letters below it. To the right of the text is a 3D rendering of several interlocking silver gears. The background of the logo is dark blue with a subtle grid pattern.

SCAP
VALIDATED

Authenticated Vulnerability and Patch Scanner

SCAP Validation and GSA SmartBUY

Peter Mell, SCAP Validation Program Manager
John Banghart, SCAP Validation Project Lead

Agenda

- Overview of SCAP Validation
- GSA SmartBUY and SCAP Validation
- OMB FDCC and SCAP Validation
- SCAP Reference Implementation
 - Open source NIST XCCDF interpreter
 - Open source MITRE OVAL interpreter
- SCAP Validation Details
 - New CVE, OVAL, and XCCDF validations
- New SCAP Validation Testing Platforms
 - Red Hat Enterprise Linux 5
 - Solaris 10

SCAP Validation Program

- Provides product conformance testing for Security Content Automation Protocol (SCAP) and the SCAP component standards
- <http://nvd.nist.gov/validation.cfm> (Validation Program)
- <http://nvd.nist.gov/scaproducts.cfm> (Validated Products)

SCAP is a suite of vulnerability management standards that together enable standardization and automation of vulnerability management, measurement, and technical policy compliance checking (soon remediation) along with enhanced product and database integration capabilities.

Security Content Automation Protocol (SCAP)

Standardizing How We Communicate

MITRE



CVE

Common
Vulnerability
Enumeration

Standard nomenclature and dictionary of security related software flaws

MITRE



CCE

Common
Configuration
Enumeration

Standard nomenclature and dictionary of software misconfigurations

MITRE



CPE

Common Platform
Enumeration

Standard nomenclature and dictionary for product naming



XCCDF

eXtensible Checklist
Configuration
Description Format

Standard XML for specifying checklists and for reporting results of checklist evaluation

MITRE



OVAL

Open Vulnerability
and Assessment
Language

Standard XML for test procedures



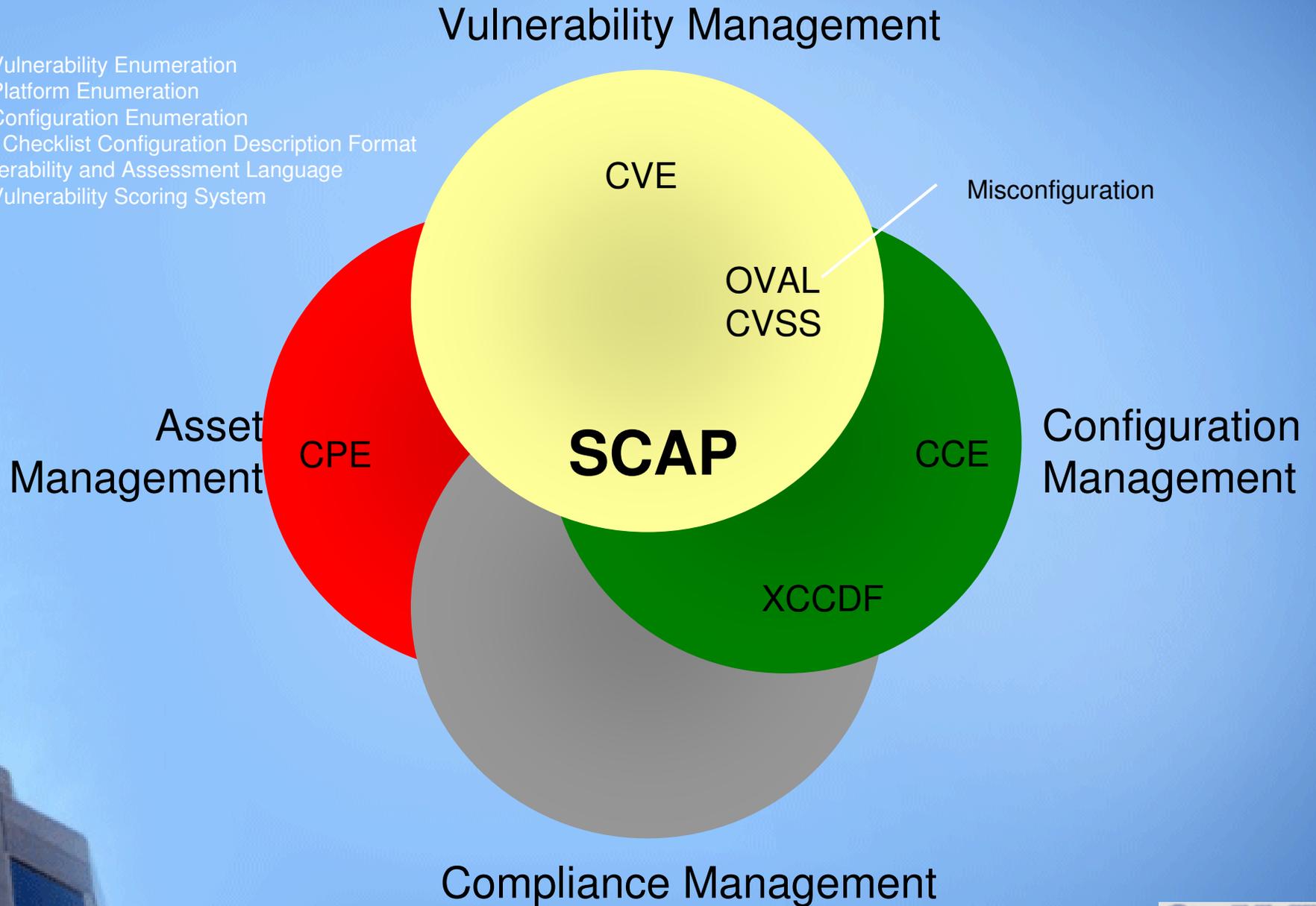
CVSS

Common
Vulnerability Scoring
System

Standard for measuring the impact of vulnerabilities

Integrating IT and IT Security Through SCAP

Common Vulnerability Enumeration
Common Platform Enumeration
Common Configuration Enumeration
eXtensible Checklist Configuration Description Format
Open Vulnerability and Assessment Language
Common Vulnerability Scoring System



SCAP Validation Capabilities

Currently being validated	Currently on list, not yet being validated
FDCC Scanner	Intrusion Detection and Prevention Systems (IDPS)*
Authenticated Vulnerability and Patch Scanner	Patch Remediation*
Authenticated Configuration Scanner	Malware Tool*
Unauthenticated Vulnerability Scanner	Asset Scanner*
Mis-configuration Remediation	
Vulnerability Database	
Mis-configuration Database	

SCAP Component Standards

Common Vulnerabilities and Exposures (CVE)	http://cve.mitre.org
Common Configuration Enumeration (CCE)	http://cce.mitre.org
Common Platform Enumeration (CPE)*	http://cpe.mitre.org
Common Vulnerability Scoring System (CVSS)	http://www.first.org/cvss/index.html
eXtensible Configuration Checklist Document Format (XCCDF)	http://nvd.nist.gov/xccdf.cfm
Open Vulnerability Assessment Language (OVAL)	http://oval.mitre.org

* Not currently available for validation

17 SCAP Validated Products from 11 Vendors



SCAP Validation Program was started only 8 months ago

9 Accredited Independent Laboratories Perform SCAP Product Testing

- AEGISOLVE
- ATSEC
- COACT
- Cygnacom
- DOMUS
- EWA – Canada
- ICSA Labs
- InfoGard
- SAIC
- Testing is black box
- Tests are either easily human verifiable or automated
- NIST provides labs a reference SCAP implementation
- Tests documented in NIST IR-7511

Technology Services

National Voluntary Laboratory Accreditation Program

NIST

National Institute of
Standards and Technology

NVLAP
Home

Accredited
Laboratories

Fields of
Accreditation

Publications/
Applications

Mutual Recognition
Arrangements

Assessor
Resources

Contact
NVLAP

NIST

GSA SmartBUY and SCAP Validation

- Information System Security Line of Business (ISSLOB)
 - Situational Awareness and Incident Response (SAIR) working group
- SmartBUY
 - consolidated purchasing program
- ISSLOB SAIR partnered with GSA SmartBUY
- SmartBUY is conducting enterprise wide Blanket Purchase Agreements (BPAs) for SAIR requirements.

Objective of ISSLOB SAIR SmartBUY



U.S. General Services Administration

- “The objective is to obtain a collection of cost effective information security tools. Additionally these products shall:
 - Give government agencies security products with ability to check for and report **FDCC compliance** and prove ability to scan for FDCC compliance
 - Enable all federal government agencies to purchase security products that are, at a minimum, **compliant with current NIST SCAP guidelines.**
 - Provide products via a GSA SmartBuy BPA that perform **Network Mapping and Discovery, Baseline Configuration Management, and Vulnerability Assessment”**

SAIR SCAP Validation Requirements

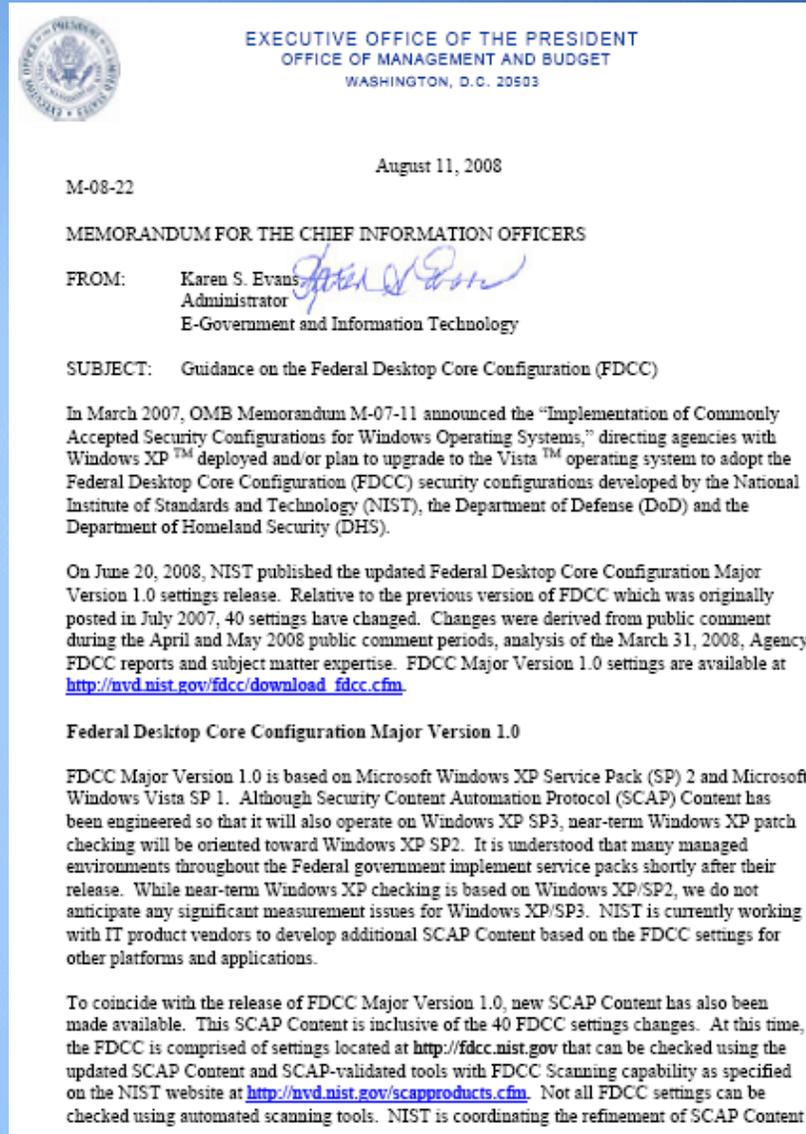


U.S. General Services Administration

- SAIR - Baseline Configuration Management Requirements for **Configuration Scanners**
 - (D92) ‘The product shall be **validated** under the NIST Security Content Automation Protocol (SCAP) validation program as having all of the following capabilities: “**Federal Desktop Core Configuration (FDCC) Scanner**” and “**Authenticated Configuration Scanner.**”’
- SAIR Vulnerability Assessment Management Requirements for **Vulnerability Scanners**
 - (D92) ‘The product shall be **validated** under the NIST Security Content Automation Program (SCAP) as having at least one of the following capabilities: “**Authenticated Vulnerability and Patch Scanner**” or “**Unauthenticated Vulnerability Scanner**”.’

OMB and SCAP Validation

- OMB Memorandum M-08-22
 - Released August 11, 2008
 - <http://www.whitehouse.gov/omb/memoranda/fy2008/m08-22.pdf>
- “Industry and government IT providers must use SCAP validated tools with FDCC Scanner capability”
- “Agencies will use SCAP tools to scan for... FDCC configurations”



MITRE SCAP Adoption Program and SCAP Validation

MITRE

- MITRE runs adoption programs for vendors
 - Educate vendors on how to implement and use the standards
 - Complements the SCAP Validation Program
- Covers CVE, CCE, OVAL, and CPE
- Paper on MITRE Adoption Program and SCAP Validation
 - http://cve.mitre.org/adoption/Adoption_and_Validation_August2008.pdf
- CVE Adoption: <http://cve.mitre.org/adoption/index.html>
- CCE Adoption: <http://cce.mitre.org/adoption/index.html>
- CPE Adoption: <http://cpe.mitre.org/adoption/index.html>
- OVAL Adoption: <http://oval.mitre.org/adoption/index.html>



SCAP Validation: New Component Standard Validations

- CVE
 - Adapted from MITRE compatibility program
 - Grandfathering products for 1 year
- OVAL
 - Adapted from MITRE compatibility program
 - Separate matrix to define capabilities
 - Grandfathering products for 1 year
- XCCDF
 - Based on explicit and implicit use cases from XCCDF specification v1.1.4.
 - Separate matrix to define capabilities



New SCAP Validation Test Platforms



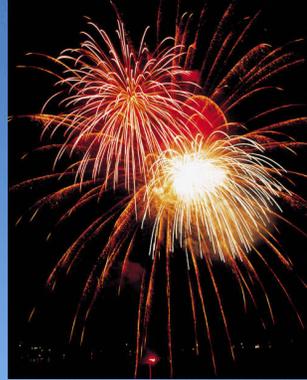
- SCAP Validation is Expanding to Unix!!
 - Red Hat Enterprise Linux 5
 - Solaris 10
 - Beta SCAP content exists
- Windows XP (already available)
- Windows Vista (already available)

SCAP Validation Testing: Raising the Bar

- SCAP is evolving and we are improving how we test it
- Requirements will be updated every January
- Vendors must revalidate once a year to maintain their validation
 - Vendors can not “skip” updated requirements by re-validating early
- Test requirements published in NIST IR-7511
- <http://csrc.nist.gov/publications/drafts/nistir-7511/Draft-NISTIR-7511.pdf>

XCCDF Reference Implementation

- Announcing the **XCCDF interpreter** created here at NIST
- Open source BSD license (same as MITRE OVALDI)
- Java based
- Uses the MITRE OVALDI for OVAL parsing
- Tested on Windows XP Professional SP2 and Windows Vista
- Currently being ported to Unix (RHEL, Solaris) in near future
- Planned release in October 2008



SCAP Validation Program Contacts

Peter Mell

SCAP Validation Program Manager

mell@nist.gov

John Banghart

SCAP Validation Project Lead

john.banghart@nist.gov



SCAP Validation Tools: <http://nvd.nist.gov/scaproducts.cfm>

SCAP Validation Homepage: <http://nvd.nist.gov/validation.cfm>