SCAP™

Security Content Automation

Tim Grance, Program Manager, Cyber and Network Security Program
The National Institute of Standards and Technology

October 27, 2009

Agenda

- Current State
- What is SCAP, how is it used?
- What's next?
- How can you help?

Thoughts on Current State of Vulnerability and Configuration Management

- *Automation and communication is normally limited to a single discipline* - vulnerability, compliance, configuration, and asset management remain compartmentalized
- *Automation and communication usually occurs through proprietary methods* - therefore data sharing, analysis, aggregation, etc. is typically only possible within a product line
- *Increasing number of mandates* - means increasing number of frameworks, standards, regulations, guidelines, sometimes these documents conflict
- *Relatively static number of security configurations*
- *Increasing number and complexity of vulnerabilities and threats*

Security Content Automation Protocol

Naming	CVE	Common Vulnerability Enumeration	Standard nomenclature and dictionary of security related software flaws
	CCE	Common Configuration Enumeration	Standard nomenclature and dictionary of software misconfigurations
	CPE	Common Platform Enumeration	Standard nomenclature and dictionary for product naming
Expressing	XCCDF	eXtensible Checklist Configuration Description Format	Standard XML for specifying checklists and for reporting results of checklist evaluation
Assessing	OVAL	Open Vulnerability and Assessment Language	Standard XML for test procedures
Scoring	CVSS	Common Vulnerability Scoring System	Standard for measuring the impact of vulnerabilities

Cisco, Qualys, Symantec, Carnegie Mellon University

SCAP™

Languages

Means of providing instructions

- Community developed
- Machine readable XML
- Reporting
- Representing security checklists
- Detecting machine state

XCCDF security benchmark automation

OVAL™ Open Vulnerability and Assessment Language

Metrics

Risk scoring framework

- Community developed
- Transparent
- Metrics
  - Base
  - Temporal
  - Environmental

CVSS

Enumerations

Convention for identifying and naming

- Community developed
- Product names
- Vulnerabilities
- Configuration settings

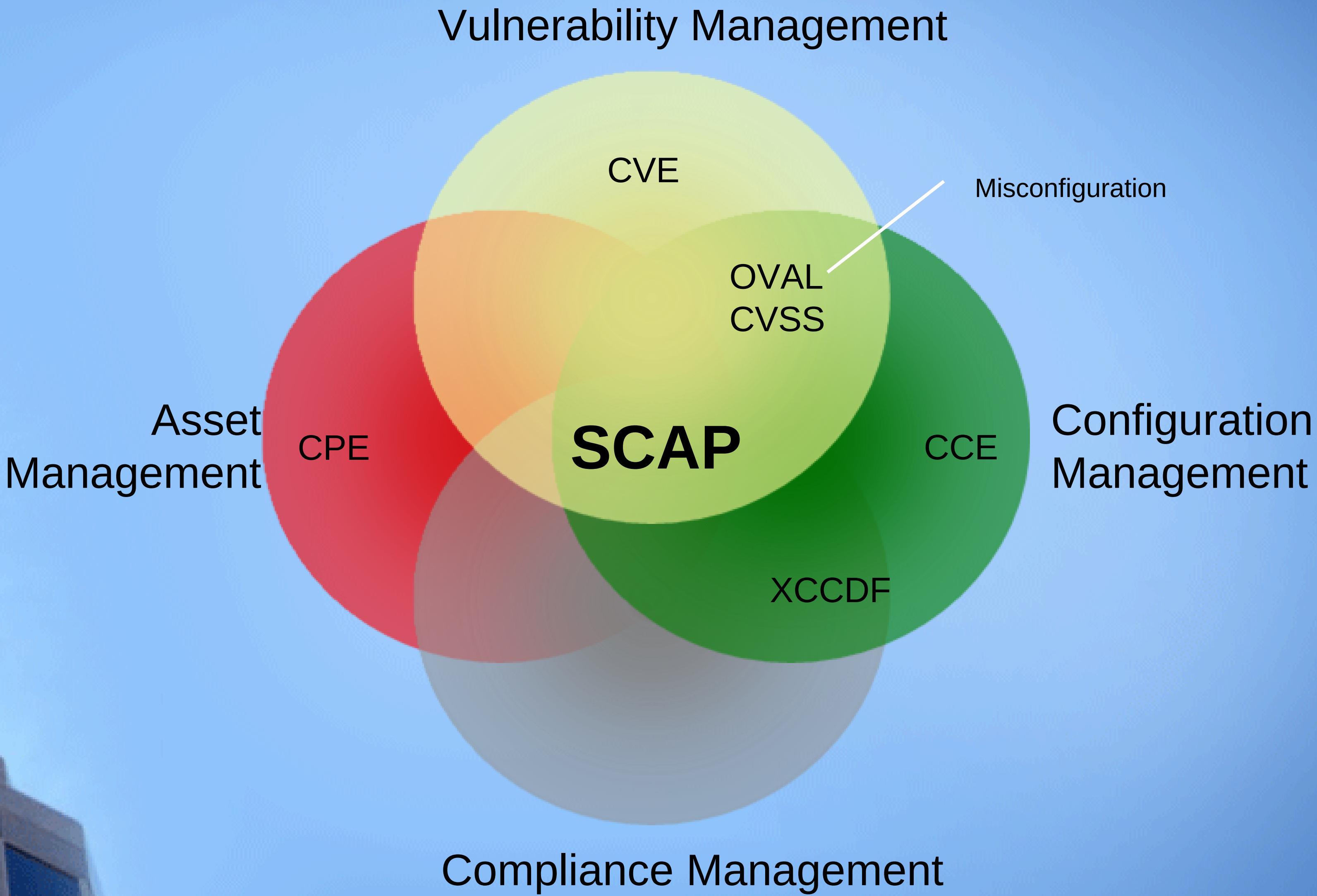
CVE cve.mitre.org

CCE™

CPE™ common platform enumeration

NIST

Integrating IT and IT Security Through SCAP



What are we trying to achieve with SCAP?

Minimize Effort

- Reduce the time and effort of manual assessment and remediation
- Provide a more comprehensive assessment of system state

Increase Interoperability

- Enable fast and accurate correlation within the enterprise and across organizations/agencies
- Shorten decision cycles by rapidly communicating:
  - Requirements (What/How to check)
  - Results (What was found)
- Allow diverse tool suites and repositories to share data
- Foster shared situational awareness by enabling and facilitating data sharing, analysis, and aggregation

What are we trying to achieve with SCAP?

Economy of scale and reuse

SCAP security content can be developed once and used by many

- National Checklist Program: publishing standardized content

Speed

Rapidly identify vulnerabilities and improperly configured systems, communicate the degree of associated risk, and take appropriate corrective action

- Zero day malware detection

Current SCAP Use Cases

- Vulnerability Management – detect, prioritize, and remediate vulnerabilities (software flaws) on a system

- Configuration Verification – determine whether system configuration settings comply with organizational policies

- Patch Compliance – determine whether appropriate patches have been applied on a system

- System Inventory – identify products installed on the system (e.g., hardware, operating system, and applications)

- Malware Detection – detect presence of malware on a system
  - Zero day signature building for consumption by SCAP validated products

Using SCAP

- Define the computing environment, architecture, components, related threats, vulnerabilities, and metrics, and appropriate security baselines consistent with industry recommended practices (NIST impact levels, vendors, providers, and VoIP/IT Healthcare/cloud/validation standard bodies)
- Collaborate with vendors and providers to produce configuration guides that meet the general security requirements and industry recommended practices
- Work with configuration tool vendors to support the configuration guide in SCAP
- Leverage validated tools as part of the SCAP program

Challenges in Cloud Computing Environment

- Complex hosted infrastructure
  - Composition of diverse technologies, e.g., compute, storage, network, virtualization, OS, services, applications, and data
  - Dynamic hosted environment and dynamic workloads
  - Security transparency in multi-tenancy and internationally hosted environment
  - Express security service level requirements
  - Compliance and governance

SCAP Cloud Use Case

- SCAP in the IaaS, PaaS, and SaaS environment
  - Manage the asset inventory, e.g., compute, storage, services, etc.
  - Identify and manage the vulnerabilities and configurations
  - Express security policy and higher level framework compliance
  - Assess the components in the stack
- SCAP across diverse clouds
  - Express security level agreements for dynamic hosted environments
  - Encapsulate dynamic workloads
  - Assess and measure the hosted platforms according to the security requirements

What has SCAP accomplished?

At Present

- Fully functional, broadly tested security protocol with applicability in vulnerability and technical compliance management
- High level benefits of interoperability, repeatability, uniform decision material, uniform reporting format
- Self-documenting compliance
- Currently delivers:
  - Repeatable assessments and uniform reporting - OMB's FDCC
  - Standardized software flaw and impact measurement - PCI DSS v1.2

…significantly and positively affecting both public and private sectors

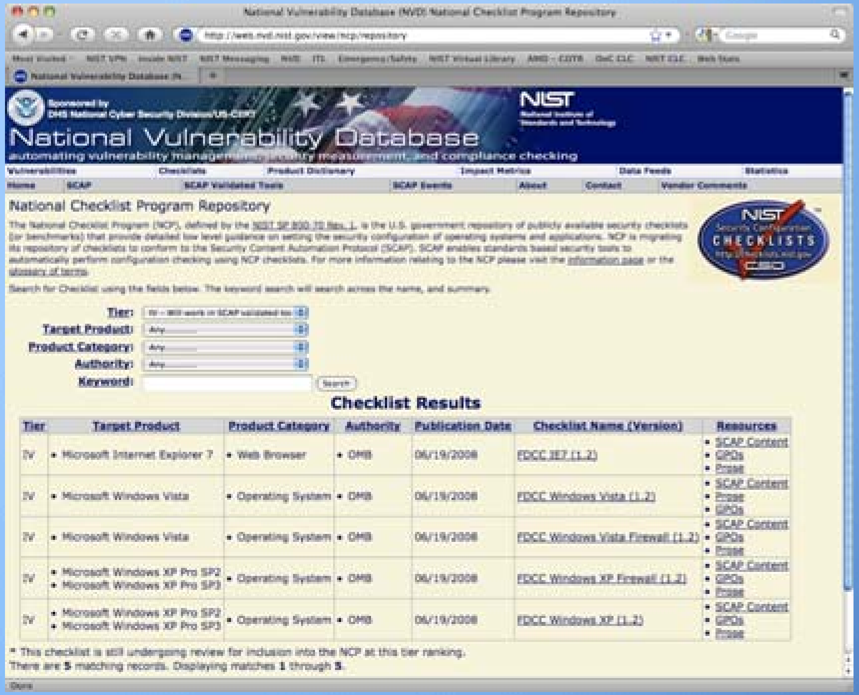
At Our Current Trajectory

- All of these things set the stage for significant security automation
- Build actuarial data for information security
- Net effect of which will be enhanced security posture, delivered in less time and with less expense

National Checklist Program Website

U.S. Government repository of publicly available security checklists

- 129 checklists currently published on the website
- 17 SCAP-expressed checklists
- Additional SCAP-expressed checklists planned for FY2010
- Checklists cover 178 products
- Checklist contributors include
  - Government organizations
  - Vendors
  - Non-profit organizations


National Vulnerability Database (NVD) National Checklist Program Repository
http://web.nvd.nist.gov/view/ncp/repository
Most Visited
NIST VPN
Inside NIST
NIST Messaging
NVD
ITL
Emergency/Safety
NIST Virtual Library
AMD - COTR
OoC CLC
NIST CLC
Web Stats
National Vulnerability Database (N…
Sponsored by
DHS National Cyber Security Division/US-CERT
NIST
National Institute of Standards and Technology
National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking
Vulnerabilities
Checklists
Product Dictionary
Impact Metrics
Data Feeds
Statistics
Home
SCAP
SCAP Validated Tools
SCAP Events
About
Contact
Vendor Comments
NIST Security Configuration CHECKLISTS
Search
Done

National Checklist Program Repository

The National Checklist Program (NCP), defined by the NIST SP 800-70 Rev. 1, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications. NCP is migrating its repository of checklists to conform to the Security Content Automation Protocol (SCAP). SCAP enables standards based security tools to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the information page or the glossary of terms.

Search for Checklist using the fields below. The keyword search will search across the name, and summary.

Tier: IV - Will work in SCAP validated to…
Target Product: Any
Product Category: Any
Authority: Any
Keyword:

Checklist Results

Tier	Target Product	Product Category	Authority	Publication Date	Checklist Name (Version)	Resources
IV	• Microsoft Internet Explorer 7	• Web Browser	• OMB	06/19/2008	FDCC IE7 (1.2)	• SCAP Content • GPOs • Prose
IV	• Microsoft Windows Vista	• Operating System	• OMB	06/19/2008	FDCC Windows Vista (1.2)	• SCAP Content • Prose • GPOs
IV	• Microsoft Windows Vista	• Operating System	• OMB	06/19/2008	FDCC Windows Vista Firewall (1.2)	• SCAP Content • GPOs • Prose
IV	• Microsoft Windows XP Pro SP2 • Microsoft Windows XP Pro SP3	• Operating System	• OMB	06/19/2008	FDCC Windows XP Firewall (1.2)	• SCAP Content • GPOs • Prose
IV	• Microsoft Windows XP Pro SP2 • Microsoft Windows XP Pro SP3	• Operating System	• OMB	06/19/2008	FDCC Windows XP (1.2)	• SCAP Content • GPOs • Prose

* This checklist is still undergoing review for inclusion into the NCP at this tier ranking.
There are **5** matching records. Displaying matches **1** through **5**.

National Vulnerability Database

- NVD is the U.S. government repository of public vulnerability management information.
- XML data feeds for SCAP reference data
- Used by government, industry and academia
- 39,000 CVE entries with the NVD Analysis Team evaluating over 6,000 vulnerabilities a year
- Product dictionary containing 18,000 unique product names
- CCE to 800-53 control mapping data feed
- Spanish and Japanese language translations

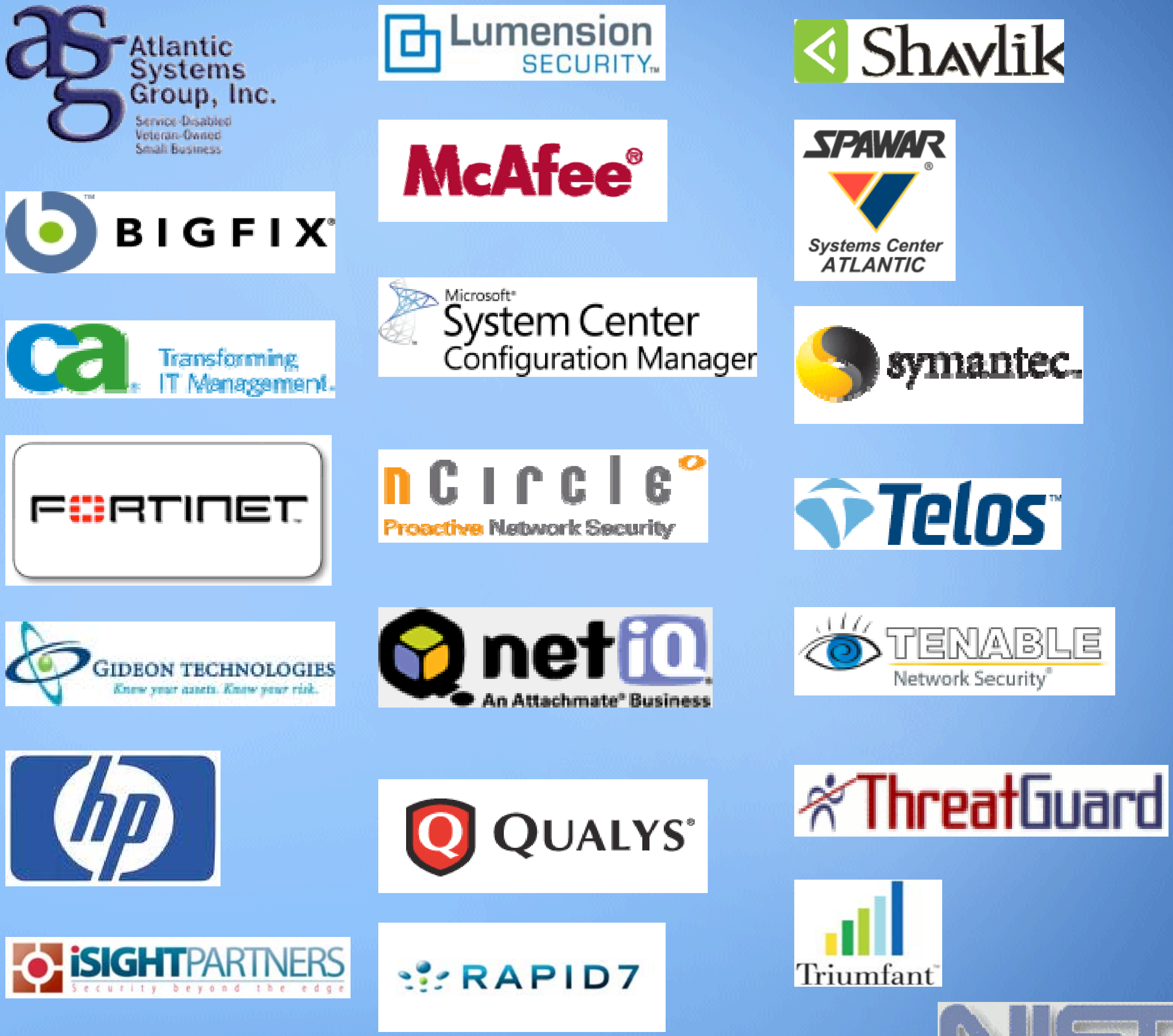
SCAP Validation Program Status

As of 21 October 2009,

- 10 Accredited labs

Validated Products

- 21 vendors
- 28 products
- 89 capabilities-based validations
- 17 standards-based validations


Atlantic Systems Group, Inc.
Service-Disabled Veteran-Owned Small Business
BIGFIX
ca Transforming IT Management
FORTINET
GIDEON TECHNOLOGIES Know your assets. Know your risk.
hp
iSIGHTPARTNERS Security beyond the edge
Lumension SECURITY
McAfee
Microsoft System Center Configuration Manager
nCircle Proactive Network Security
netIQ An Attachmate Business
QUALYS
RAPID7
Shavlik
SPAWAR Systems Center ATLANTIC
symantec.
Telos
TENABLE Network Security
ThreatGuard
Triumfant

DRAFT SCAP/Validation Roadmap

2010 – SCAP 1.0

- SP 800-126 and IR 7511 rev 2
- Content Validation

2011 – SCAP 1.1

- SP 800-126 rev 1 and IR 7511 rev 3
  - OCIL 2.0
  - OVAL 5.6

2012 – SCAP 1.2

  - SP 800-126 rev 2 and IR 7511 rev 4
  - OVAL 5.X OS and application support
  - Digitally trusted content
- Remediation Validation Program

2013 – SCAP 1.3

- SP 800-126 rev 3 and IR 7511 rev 5
- Digitally trusted reporting
- SCAP Remediation

2014 – SCAP 2.0

- SP 800-126 rev 4 and IR 7511 rev 6
- First major revision of SCAP
- XCCDF 2.0
- OVAL 6.X
- Expanded remediation capabilities
- Expanded product naming capabilities

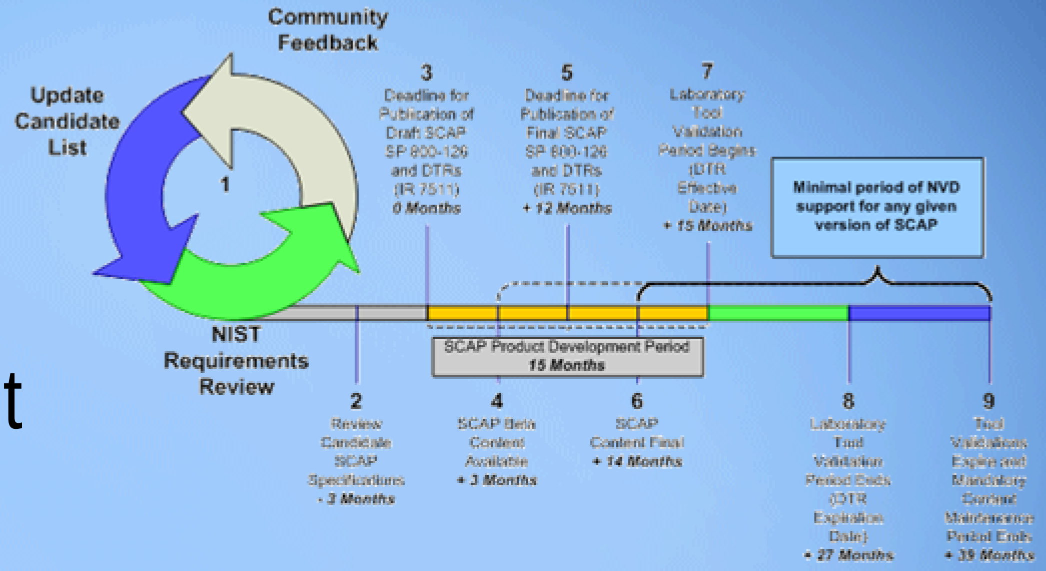
2015 – SCAP 2.1

Process Formalization

- Roadmap

- Vendor and GOTS Software Development Planning

- Predictable Validation Cycle


Community Feedback
Update Candidate List
1
NIST Requirements Review
3
Deadline for Publication of Draft SCAP SP 800-126 and DTRs (IR 7511)
0 Months
5
Deadline for Publication of Final SCAP SP 800-126 and DTRs (IR 7511)
+ 12 Months
7
Laboratory Tool Validation Period Begins (DTR Effective Date)
+ 15 Months
Minimal period of NVD support for any given version of SCAP
SCAP Product Development Period
15 Months
2
Review Candidate SCAP Specifications
- 3 Months
4
SCAP Beta Content Available
+ 3 Months
6
SCAP Content Final
+ 14 Months
8
Laboratory Tool Validation Period Ends (DTR Expiration Date)
+ 27 Months
9
Tool Validations Expire and Mandatory Content Maintenance Period Ends
+ 39 Months

Where are we going, what are we going to do?

- Formalize SCAP development lifecycle
- Address additional security domains and functions
  - Remediation
  - Auditing and events
  - SCAP within cloud computing/virtualization
  - Software assurance
- Metrics
  - Evidence-based approach to security decision making
  - Automated methods of collecting security measurements
- Establish an SCAP Content Validation Program
- Enterprise SCAP
  - •Trusted content
  - •Compliance Reporting
- Emerging specifications (e.g., OCIL, OCRL, CCSS, CMSS)
- Security ontologies

What do we want folks to do?

- IT Vendors
  - Produce checklists in SCAP and submit to National Checklist Program
  - Produce CPE, CCE, and CVE’s for your products
  - Produce vulnerability alerts using SCAP
- Buy and use SCAP Validated products
- Engagement and feedback, e.g., healthcare, smart grid, VoIP, cloud computing, etc.
- Innovate, e.g., energy saving, performance, etc.

Conference Acknowledgements

- Government Sponsors
    - NSA, DHS, DISA, NIST
- Corporate Sponsors
    - Platinum: Symantec, Intel
    - Gold: Red Seal, Qualys
    - Silver: Trend Micro
- Conference Special Recognitions
    - Track Leads
    - Mitre

Resources

SCAP Homepage: http://scap.nist.gov

SCAP Validation Tools: http://nvd.nist.gov/scapproducts.cfm

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

National Checklist Program: http://checklists.nist.gov

National Vulnerability Database: http://nvd.nist.gov