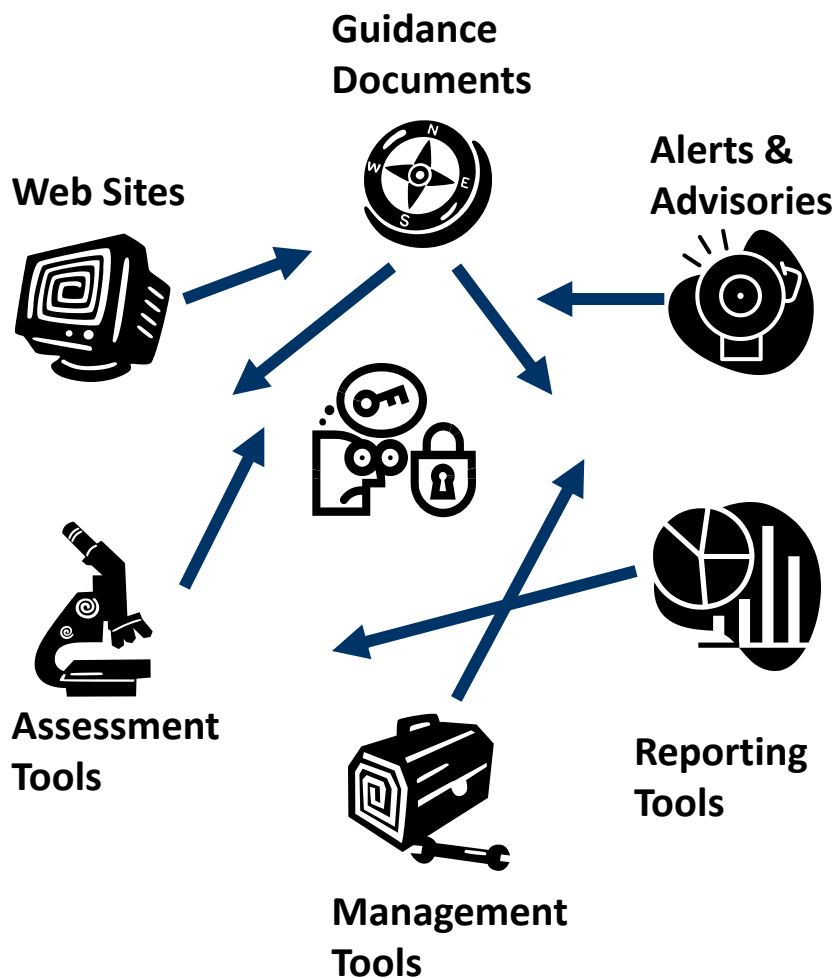


The Security Content Automation Protocol (SCAP)



Security Automation: The challenge



- “Tower of Babel”
 - Too much proprietary, incompatible information
 - Costly
 - Error prone
 - Difficult to scale
- Inefficient
 - Resources spent on “security hygiene”
 - Vulnerability management
 - Configuration management
 - Patch management
 - Compliance management

Security Automation: The solution



- **Standardization:**
 - Same Object, Same Name
 - Reporting
- **Automation:**
 - Efficiency
 - Accuracy
 - Resources re-tasked to harder problems:
 - Incident response
 - Infrastructure enhancement

What is SCAP?

The Security Content Automation Protocol

- Created to bring together existing specifications and to provide a standardized approach to maintaining the security of enterprise systems
- SCAP ...
 - provides a means to identify, express and measure security data in standardized ways
 - is a suite of individually maintained, open specifications
 - defines how these specification are used in concert
 - includes standardized reference data -- SCAP Content

What is SCAP?



Languages

Means of providing instructions

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



Metrics

Risk scoring framework

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











Enumerations

Convention for identifying and naming

- Community developed
- Product names
- Vulnerabilities
- Configuration settings



What is SCAP?

MITRE	 cve.mitre.org	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	 common platform enumeration	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
MITRE		OCIL	Open Checklist Interactive Language	Standard XML for human interaction
 Improving Security Together		CVSS	Common Vulnerability Scoring System	Standard for measuring the impact of vulnerabilities

Naming

Expressing

Assessing

Scoring

SCAP Use Cases

Configuration Management – determine whether system configuration settings comply with organizational policies

Vulnerability Management – detect and prioritize known vulnerabilities (software flaws) on a system

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, allowing zero day signature building for consumption by SCAP validated products

The Core SCAP Publications

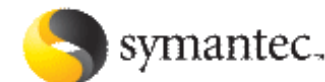
The NIST has publications on SCAP available on the Computer Security Resource Center (CSRC) website:

- **SP 800-117**: Guide to Adopting and Using SCAP, May 5, 2009
- **SP 800-126**: The Technical Specification for the SCAP 1.0, November 2009
- **SP 800-126 Rev 1**: The Technical Specification for the SCAP 1.1, Dec 15, 2009
- **IR-7511 Rev 1**: DRAFT SCAP Validation Program Test Requirements, Apr. 21, 2009

SCAP Products

SCAP Validated product vendors:

(as of 25 June 2010)





The National Vulnerability Database (NVD)

- Provides standardized reference for software vulnerabilities
- Over 39,000 CVE entries with the NVD Analysis Team evaluating over 6,000 vulnerabilities a year
- Product dictionary containing over 18,000 unique CPE based product names
- Machine readable data feeds
- Spanish and Japanese language translations



The National Checklist Program (NCP)

- U.S. Federal Government repository of publicly available security checklists
- Eases compliance management
- Checklists cover 178 products
- 17 SCAP expressed checklists (Tiers 3 and 4)
- Checklist contributors include:
 - Government organizations
 - Vendors
 - Nonprofit organizations

Looking Ahead

- SCAP

- Cloud computing – SCAP support
- Use of digital signatures to support trusted content

- Related Efforts

- Data aggregation and reporting
 - enterprise level compliance reporting
 - summarization of assessment results
- Remediation capabilities
- System and network events – Event Management Automation Protocol (EMAP)

Conclusion

Security Automation:

- Improves efficiency
- Promotes interoperability of data and security tools
- Enables standardized reporting across multiple views
- Provides enhanced situational awareness

Questions & Answers/ Feedback



David Waltermire

SCAP Architect

Computer Security Division

Information Technology Laboratory

National Institute of Standards and
Technology

david.waltermire@nist.gov

(301) 975-3390

More Information/Contacts

Information

NIST websites:

- SCAP Homepage: <http://scap.nist.gov>
- SCAP Validated Tools: <http://nvd.nist.gov/scaproducts.cfm>
- SCAP Validation Homepage: <http://nvd.nist.gov/validation.cfm>
- National Checklist Program: <http://checklists.nist.gov>
- National Vulnerability Database: <http://nvd.nist.gov>
- NIST Computer Security Resource Center (CRSC)
<http://csrc.nist.gov/publications/PubsSPs.html>

Why should I use SCAP?



To Minimize Effort

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



To Increase Interoperability

- Enable fast and accurate correlation within the enterprise and across organizations/agencies
- Allow security management components and data repositories to share data
- Foster shared situational awareness by enabling and facilitating data sharing, analysis and aggregation

Why should I use SCAP?



Economy of Scale and Reuse

- SCAP security content can be developed once and used by many
- National Checklist Program: publishing standardized content



Speed

- Shorten decision cycles by rapidly communicating:
 - Requirements (What/How to check)
 - Results (What was found)
- Rapidly identify vulnerabilities and improperly configured systems, communicate the degree of associated risk and take appropriate corrective action
- Zero day malware detection

What is SCAP?

