

UNCLASSIFIED



Security Content Automation Protocol and Health Information Technology

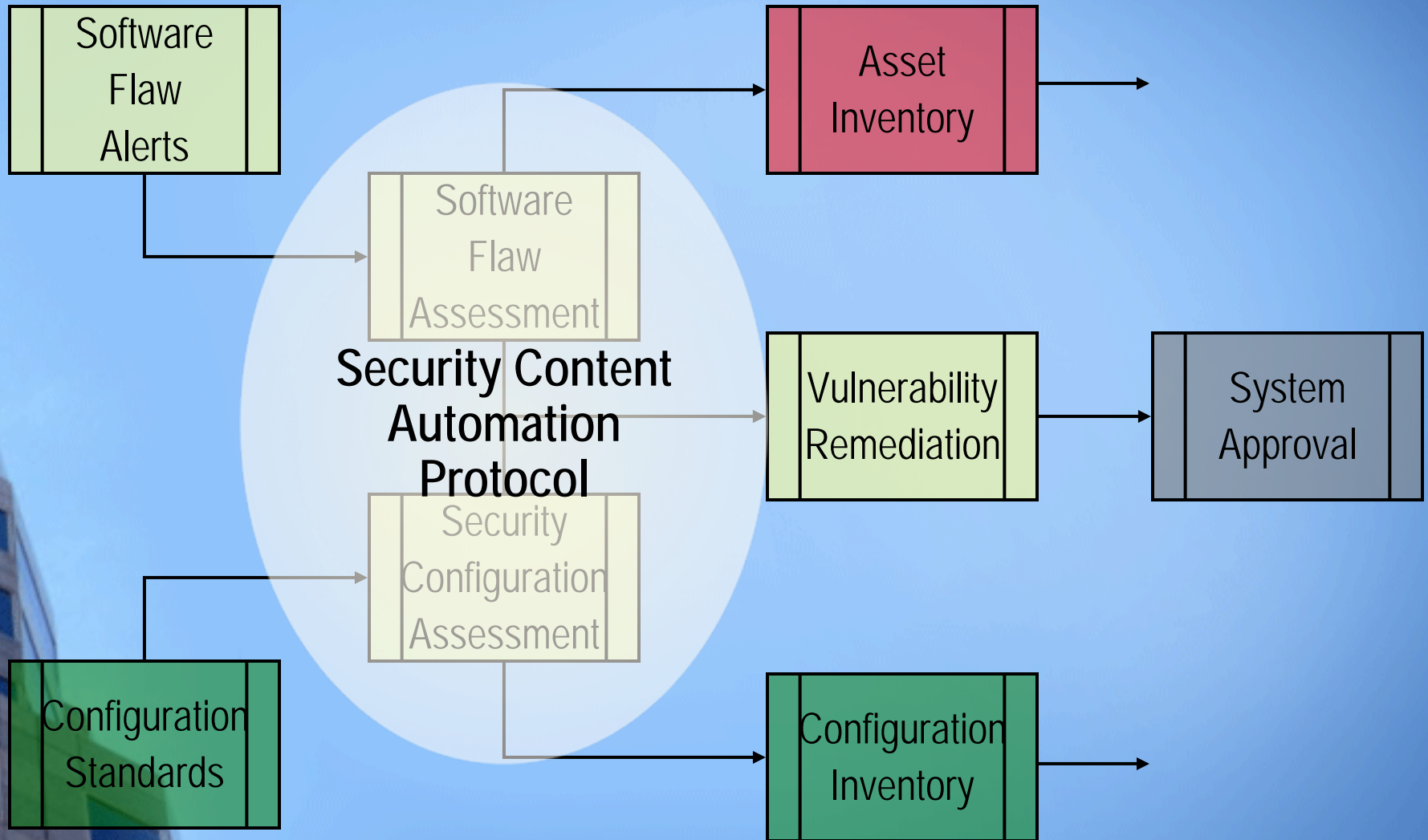
presented by:

Matt Barrett, Project Manager, Security Content Automation Protocol
The National Institute of Standards and Technology

UNCLASSIFIED



Enterprise Information Security Reporting Flow Diagram

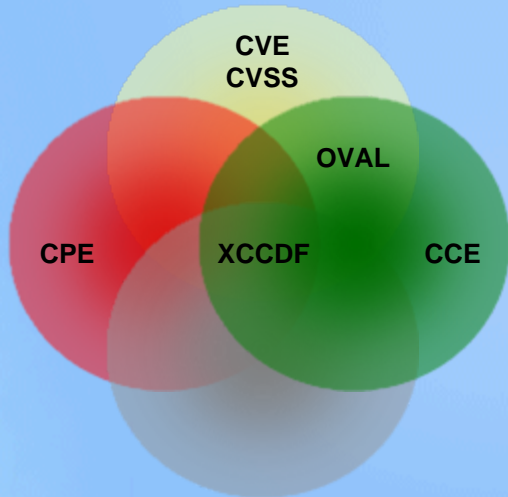


What is SCAP?

How

Standardizing the format by which we communicate

Protocol



What

Standardizing the information we communicate

Content



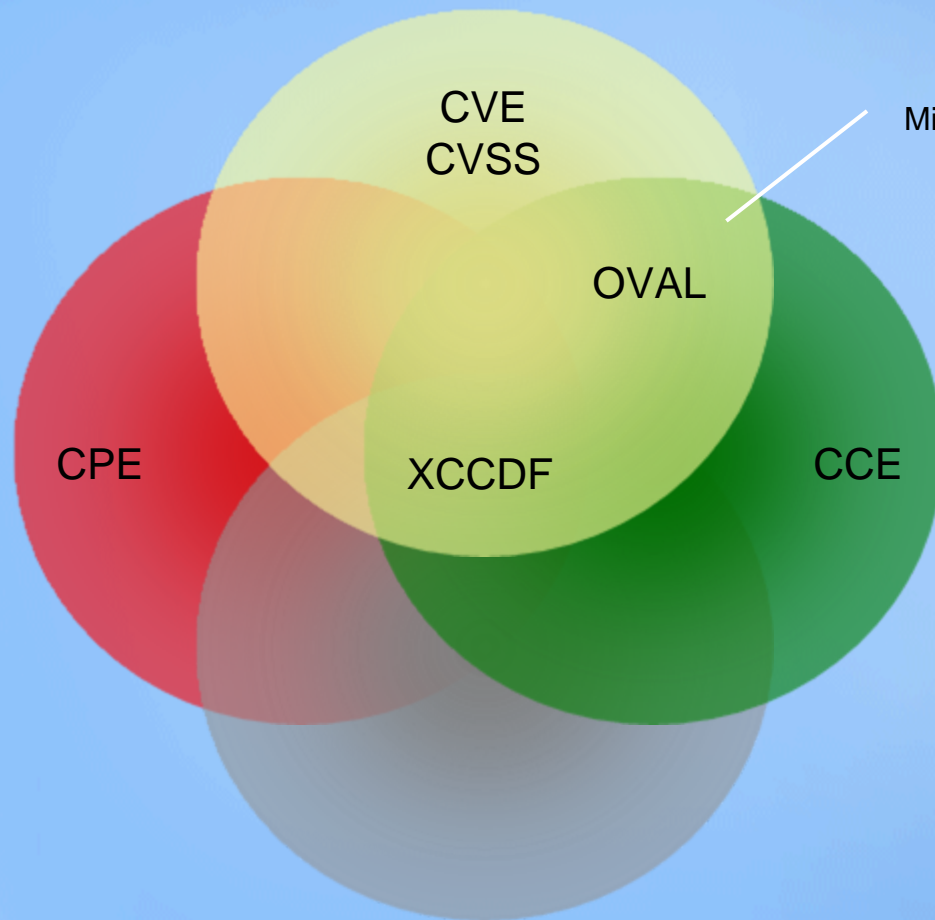
<http://nvd.nist.gov>

<http://checklists.nist.gov>

- 70 million hits per year
- 20 new vulnerabilities per day, over 6,000 per year
- Mis-configuration cross references
- Reconciles software flaws from US CERT and MITRE repositories
- Spanish translation
- Produces XML feed for NVD content

Integrating IT and IT Security Through SCAP

Vulnerability Management



Misconfiguration

Asset Management

Configuration Management

Compliance Management

- CVE Common Vulnerability and Exposures
- CPE Common Platform Enumeration
- CCE Common Configuration Enumeration
- XCCDF eXtensible Checklist Configuration Description Format
- OVAL Open Vulnerability and Assessment Language
- CVSS Common Vulnerability Scoring System

Linking Configuration to Compliance

REFERENCES

IA-5 - Authenticator Management

NIST 800-26: 15.1.6, 15.1.7, 15.1.9, 15.1.10, 15.1.11,
15.1.12, 15.1.13, 16.1.3, 16.2.3

GAO FISCAM: AC-3.2

DOD 8500.2: IAKM-1, IATS-1

DCID 6/3: 4.B.2.a(7), 4.B.3.a(11)

CobIT DS5

ISO/IEC 17799: 11.5.2, 11.5.3

HIPAA SR 164.312(a)(1) Access Control

PCI Data Security Standard v1.1 8.5.10

800-68 Section 6.1 - Table A-1.4

DISA STIG Section 5.4.1.3

DISA Gold Disk ID 7082

PDI IAIA-12B

NSA Chapter 4 - Table 1 Row 4

CCE-100 - minimum-password-length

Operational Efficiency

- Map it up-front
- Map it only once
- Map it with expertise - let technologists be technologists
- Support standardized builds
- Communicate clearly and definitively
- Communicate broadly

Slogans

- A "Scan Once, Report Many" technology
- Make compliance a by-product of security

RULE

CCE-100 - minimum-password-length




test procedures...

800-53 Controls with Automated Checking

Tool Set	Automation	Control Count	Control Percent	Control Example
Framework Tools	Full Automation	-	-	-
	Partial Automation	49	30%	PL-2 System Security Plan
Security Content Automation Protocol	Full Automation	31	19%	AC-11 Session Lock
	Partial Automation	39	24%	AC-8 System Use Notification
Future Automation Techniques or No Automation		44	27%	AC-1 Access Control Policy and Procedures
Total Controls		163	100%	

SCAP Use Cases

UNCLASSIFIED

	FDCC	The Office of Management and Budget Federal Desktop Core Configuration <i>Repeatable Assessments and Uniform Reporting</i> Implementing and measuring standardized security configurations
	CND	The Office of Secretary of Defense Computer Network Defense Data Pilot <i>Integrated and Timely Situational Awareness</i> Connecting vulnerability, threat, event, incident, and asset repositories
	PCI	The Payment Card Industry Requirements for Approved Scanning Vendors <i>Standardized Software Flaw Content and Severity Scores</i> Leveraging gold standard NIST reference data

Noteworthy use case dialogs:

- .Department of Homeland Security US Computer Emergency Readiness Team Technical Cyber Security Alerts
- .Joint Task Force Global Network Operations Information Assurance Vulnerability Management Alerts
- .Federal Information Security Management Act Implementation

UNCLASSIFIED



SCAP Validation Program Status

*As of 6 January 2009,
11 months of operation...*

- 10 Accredited labs

Validated Products

- 13 vendors
- 19 products
- 68 capabilities-based validations
- 13 standards-based validations
- All 13 vendors and 17/19 products are FDCC Scanner validated



*...and more to come in
2009.*

SCAP Documentation

- **SP800-117**: DRAFT Adopting and Using Security Content Automation Protocol
- *COMING SOON* **SP800-126**: Security Content Automation Protocol Specification
- **SP800-70 Rev 1**: DRAFT National Checklist Program for IT Products-
-Guidelines for Checklist Users and Developers
- **IR-7511**: DRAFT Security Content Automation Protocol (SCAP)
Validation Program Test Requirements
- **IR-7435**: The Common Vulnerability Scoring System (CVSS) and Its
Applicability to Federal Agency Systems
- **IR-7275 Rev 3**: Specification for the Extensible Configuration
Checklist Description Format (XCCDF) Version 1.1.4
- **IR-7502**: DRAFT The Common Configuration Scoring System (CCSS)

Questions?

Presenter:

Matt Barrett

matthew.barrett@nist.gov



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

SCAP Validation 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>