Homeland Security

Commerce

National Defense

BUILDING SECURITY IN
SOFTWARE ASSURANCE

The Cybersecurity Ecosystem

SCAP, SwAAP, et.al.

Making Security Measurable™

Robert A. Martin
28 Feb 2011

MITRE

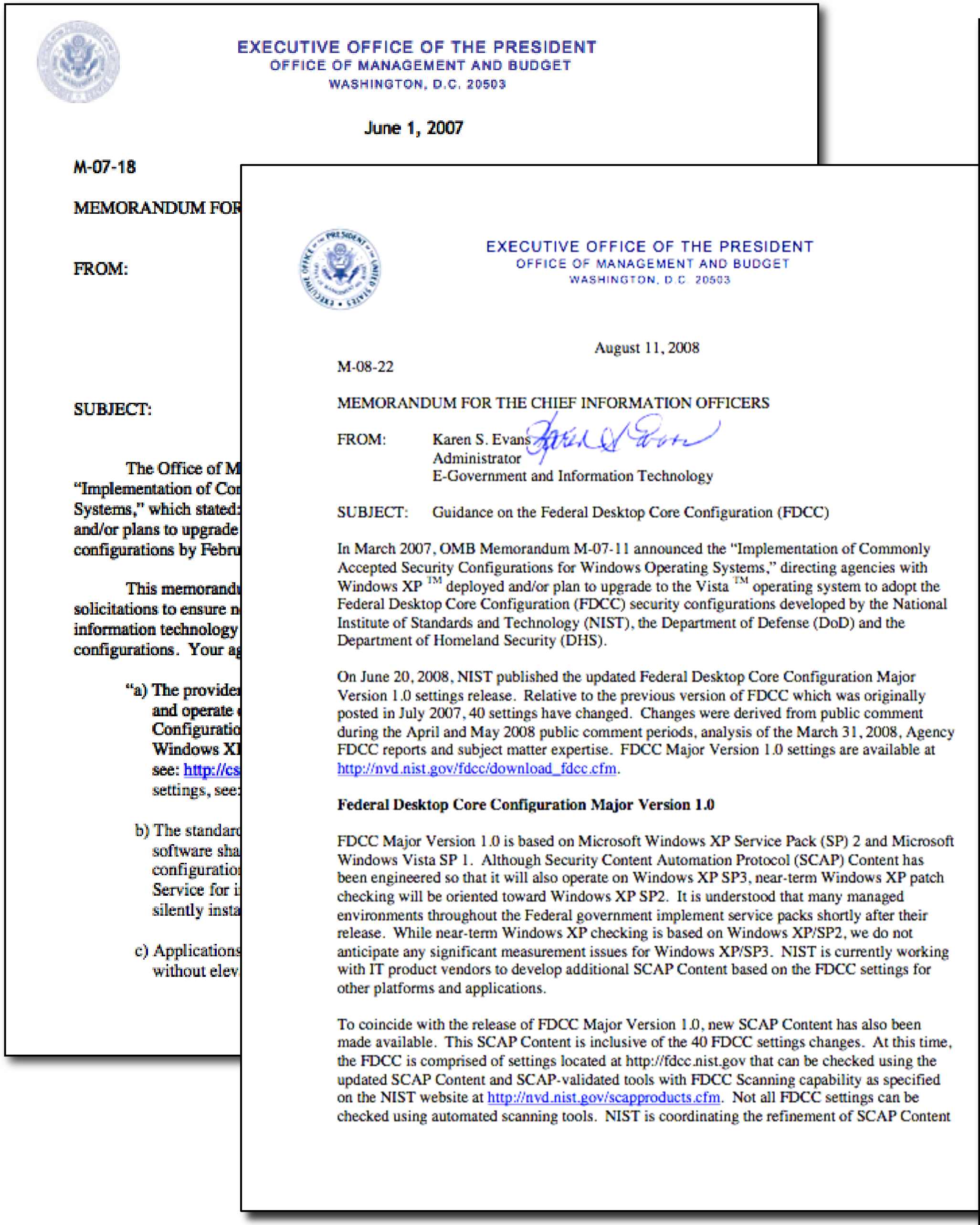
Remembering the Acronyms

What IT systems do I have in my enterprise?	CPE (Platforms)
What vulnerabilities do I need to worry about?	CVE (Vulnerabilities)
What vulnerabilities do I need to worry about RIGHT NOW?	CVSS (Scoring System)
How can I configure my systems more securely?	CCE (Configurations)
How do I define a policy of secure configurations?	XCCDF (Configuration Checklists)
How can I be sure my systems conform to policy?	OVAL (Assessment Language)
How can I be sure the operation of my systems conforms to policy?	OCIL (Interactive Language)
What weaknesses in my software could be exploited?	CWE (Weaknesses)
What attacks can exploit which weaknesses?	CAPEC (Attack Patterns)
What should be logged, and how?	CEE (Events)
How can I aggregate assessment results?	ARF (Results)
How can we recognize malware?	MAEC (Malware Attributes)

Standardization Efforts leveraged by the Security Content Automation Protocol (SCAP)

What IT systems do I have in my enterprise?	• CPE (Platforms)
What vulnerabilities do I need to worry about?	• CVE (Vulnerabilities)
What vulnerabilities do I need to worry about RIGHT NOW?	• CVSS (Scoring System)
How can I configure my systems more securely?	• CCE (Configurations)
How do I define a policy of secure configurations?	• XCCDF (Configuration Checklists)
How can I be sure my systems conform to policy?	• OVAL (Assessment Language)
How can I be sure the operation of my systems conforms to policy?	• OCIL (Interactive Language)
What weaknesses in my software could be exploited?	• CWE (Weaknesses)
What attacks can exploit which weaknesses?	• CAPEC (Attack Patterns)
What should be logged, and how?	• CEE (Events)
How can I aggregate assessment results?	• ARF (Results)
How can we recognize malware?	• MAEC (Malware Attributes)

SCAP – FDCC and USGCB



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

June 1, 2007

M-07-18

MEMORANDUM FOR

FROM:

SUBJECT:

The Office of M
"Implementation of Co
Systems," which stated
and/or plans to upgrade
configurations by Febru

This memorand
solicitations to ensure n
information technology
configurations. Your a

"a) The provider
and operate
Configuratio
Windows XI
see: http://cs
settings, see

b) The standard
software sha
configuratio
Service for i
silently insta

c) Applications
without elev

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

August 11, 2008

M-08-22

MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS

FROM: Karen S. Evans Karen S Evans
Administrator
E-Government and Information Technology

SUBJECT: Guidance on the Federal Desktop Core Configuration (FDCC)

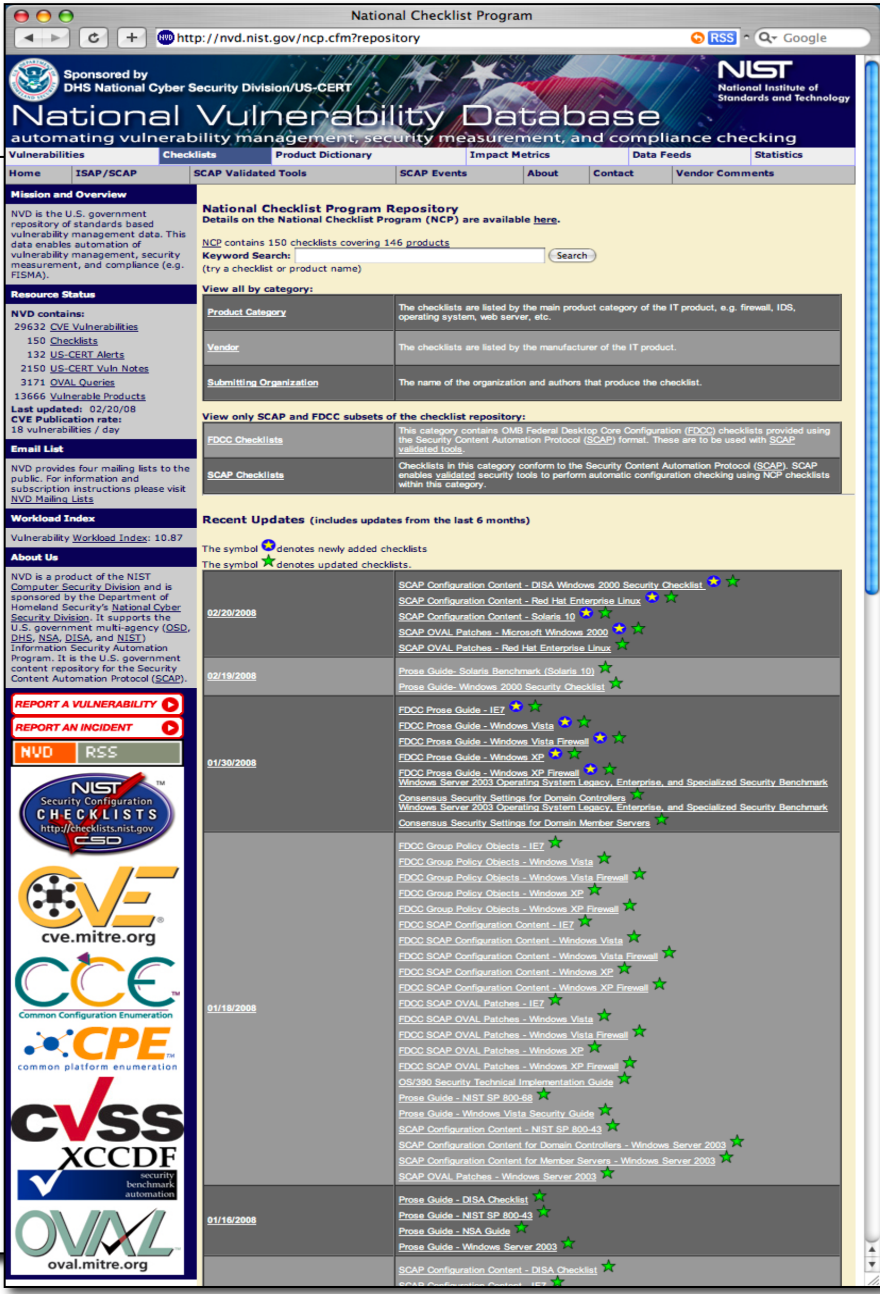
In March 2007, OMB Memorandum M-07-11 announced the "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," directing agencies with Windows XP ™ deployed and/or plan to upgrade to the Vista ™ operating system to adopt the Federal Desktop Core Configuration (FDCC) security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DoD) and the Department of Homeland Security (DHS).

On June 20, 2008, NIST published the updated Federal Desktop Core Configuration Major Version 1.0 settings release. Relative to the previous version of FDCC which was originally posted in July 2007, 40 settings have changed. Changes were derived from public comment during the April and May 2008 public comment periods, analysis of the March 31, 2008, Agency FDCC reports and subject matter expertise. FDCC Major Version 1.0 settings are available at http://nvd.nist.gov/fdcc/download_fdcc.cfm.

Federal Desktop Core Configuration Major Version 1.0

FDCC Major Version 1.0 is based on Microsoft Windows XP Service Pack (SP) 2 and Microsoft Windows Vista SP 1. Although Security Content Automation Protocol (SCAP) Content has been engineered so that it will also operate on Windows XP SP3, near-term Windows XP patch checking will be oriented toward Windows XP SP2. It is understood that many managed environments throughout the Federal government implement service packs shortly after their release. While near-term Windows XP checking is based on Windows XP/SP2, we do not anticipate any significant measurement issues for Windows XP/SP3. NIST is currently working with IT product vendors to develop additional SCAP Content based on the FDCC settings for other platforms and applications.

To coincide with the release of FDCC Major Version 1.0, new SCAP Content has also been made available. This SCAP Content is inclusive of the 40 FDCC settings changes. At this time, the FDCC is comprised of settings located at http://fdcc.nist.gov that can be checked using the updated SCAP Content and SCAP-validated tools with FDCC Scanning capability as specified on the NIST website at http://nvd.nist.gov/scapproducts.cfm. Not all FDCC settings can be checked using automated scanning tools. NIST is coordinating the refinement of SCAP Content



National Checklist Program
http://nvd.nist.gov/ncp.cfm?repository
RSS
Google
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
ISAP/SCAP
SCAP Validated Tools
SCAP Events
About
Contact
Vendor Comments
REPORT A VULNERABILITY
REPORT AN INCIDENT
NVD RSS
NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD
CVE cve.mitre.org
CCE Common Configuration Enumeration
CPE common platform enumeration
CVSS
XCCDF security benchmark automation
OVAL oval.mitre.org

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:
29632 CVE Vulnerabilities
150 Checklists
132 US-CERT Alerts
2150 US-CERT Vuln Notes
3171 OVAL Queries
13666 Vulnerable Products
Last updated: 02/20/08
CVE Publication rate:
18 vulnerabilities / day

Email List

NVD provides four mailing lists to the public. For information and subscription instructions please visit NVD Mailing Lists

Workload Index

Vulnerability Workload Index: 10.87

About Us

NVD is a product of the NIST Computer Security Division and is sponsored by the Department of Homeland Security's National Cyber Security Division. It supports the U.S. government multi-agency (OSD, DHS, NSA, DISA, and NIST) Information Security Automation Program. It is the U.S. government content repository for the Security Content Automation Protocol (SCAP).

National Checklist Program Repository
Details on the National Checklist Program (NCP) are available here.

NCP contains 150 checklists covering 146 products
Keyword Search: Search
(try a checklist or product name)

View all by category:

Product Category	The checklists are listed by the main product category of the IT product, e.g. firewall, IDS, operating system, web server, etc.
Vendor	The checklists are listed by the manufacturer of the IT product.
Submitting Organization	The name of the organization and authors that produce the checklist.

View only SCAP and FDCC subsets of the checklist repository:

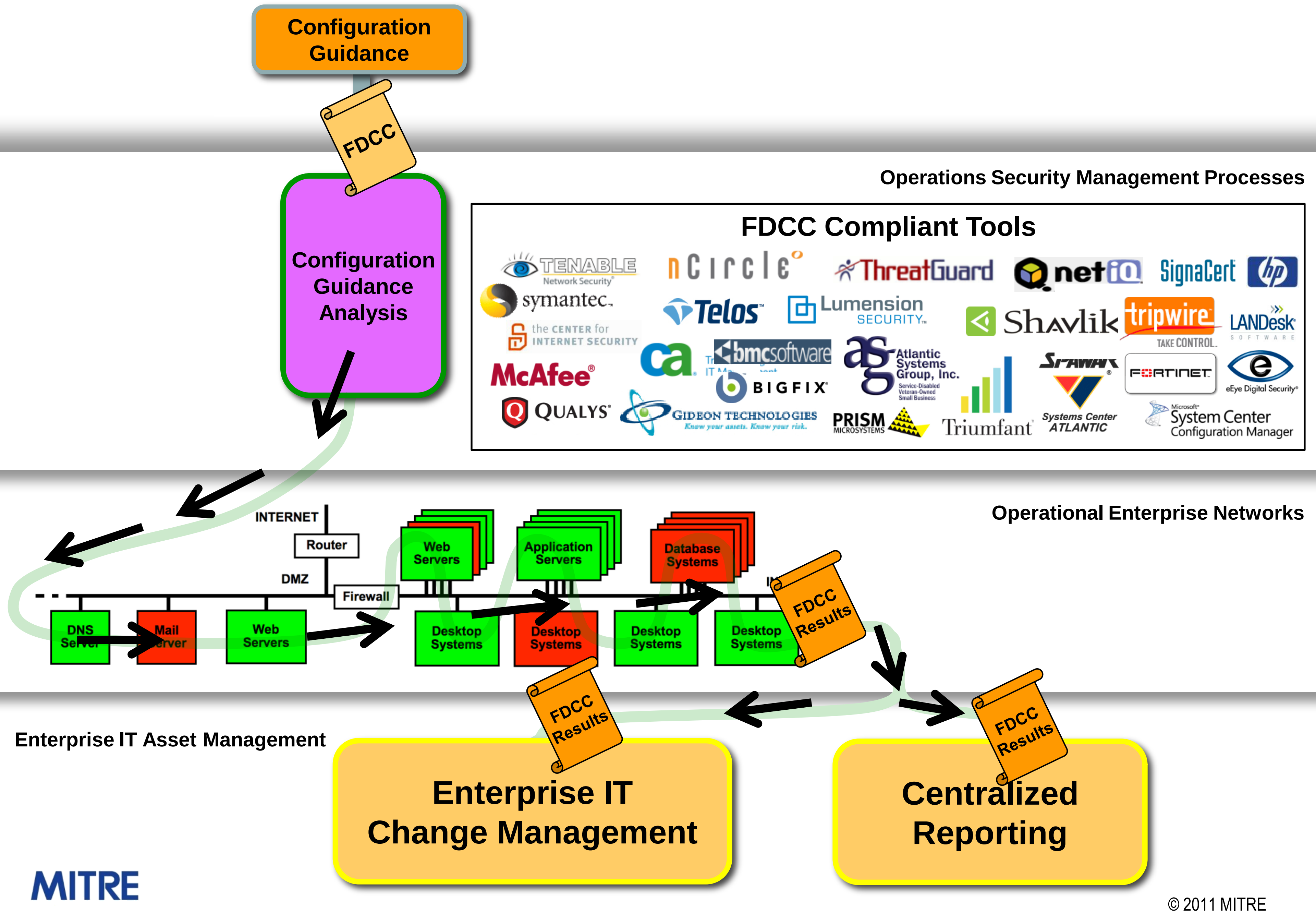
FDCC Checklists	This category contains OMB Federal Desktop Core Configuration (FDCC) checklists provided using the Security Content Automation Protocol (SCAP) format. These are to be used with SCAP validated tools.
SCAP Checklists	Checklists in this category conform to the Security Content Automation Protocol (SCAP). SCAP enables validated security tools to perform automatic configuration checking using NCP checklists within this category.

Recent Updates (includes updates from the last 6 months)

The symbol ✪ denotes newly added checklists
The symbol ★ denotes updated checklists.

02/20/2008	SCAP Configuration Content - DISA Windows 2000 Security Checklist ✪ ★ SCAP Configuration Content - Red Hat Enterprise Linux ✪ ★ SCAP Configuration Content - Solaris 10 ✪ ★ SCAP OVAL Patches - Microsoft Windows 2000 ✪ ★ SCAP OVAL Patches - Red Hat Enterprise Linux ★
02/19/2008	Prose Guide- Solaris Benchmark (Solaris 10) ★ Prose Guide- Windows 2000 Security Checklist ★
01/30/2008	FDCC Prose Guide - IE7 ✪ ★ FDCC Prose Guide - Windows Vista ✪ ★ FDCC Prose Guide - Windows Vista Firewall ✪ ★ FDCC Prose Guide - Windows XP ✪ ★ FDCC Prose Guide - Windows XP Firewall ✪ ★ Windows Server 2003 Operating System Legacy, Enterprise, and Specialized Security Benchmark Consensus Security Settings for Domain Controllers ★ Windows Server 2003 Operating System Legacy, Enterprise, and Specialized Security Benchmark Consensus Security Settings for Domain Member Servers ★
01/18/2008	FDCC Group Policy Objects - IE7 ★ FDCC Group Policy Objects - Windows Vista ★ FDCC Group Policy Objects - Windows Vista Firewall ★ FDCC Group Policy Objects - Windows XP ★ FDCC Group Policy Objects - Windows XP Firewall ★ FDCC SCAP Configuration Content - IE7 ★ FDCC SCAP Configuration Content - Windows Vista ★ FDCC SCAP Configuration Content - Windows Vista Firewall ★ FDCC SCAP Configuration Content - Windows XP ★ FDCC SCAP Configuration Content - Windows XP Firewall ★ FDCC SCAP OVAL Patches - IE7 ★ FDCC SCAP OVAL Patches - Windows Vista ★ FDCC SCAP OVAL Patches - Windows Vista Firewall ★ FDCC SCAP OVAL Patches - Windows XP ★ FDCC SCAP OVAL Patches - Windows XP Firewall ★ OS/390 Security Technical Implementation Guide ★ Prose Guide - NIST SP 800-68 ★ Prose Guide - Windows Vista Security Guide ★ SCAP Configuration Content - NIST SP 800-43 ★ SCAP Configuration Content for Domain Controllers - Windows Server 2003 ★ SCAP Configuration Content for Member Servers - Windows Server 2003 ★ SCAP OVAL Patches - Windows Server 2003 ★
01/16/2008	Prose Guide - DISA Checklist ★ Prose Guide - NIST SP 800-43 ★ Prose Guide - NSA Guide ★ Prose Guide - Windows Server 2003 ★
	SCAP Configuration Content - DISA Checklist ★ SCAP Configuration Content - IE7 ★

SCAP-Based FDCC Guidance



Knowledge Repositories

Configuration Guidance

Configuration Guidance Analysis

Operations Security Management Processes

FDCC Compliant Tools

Operational Enterprise Networks

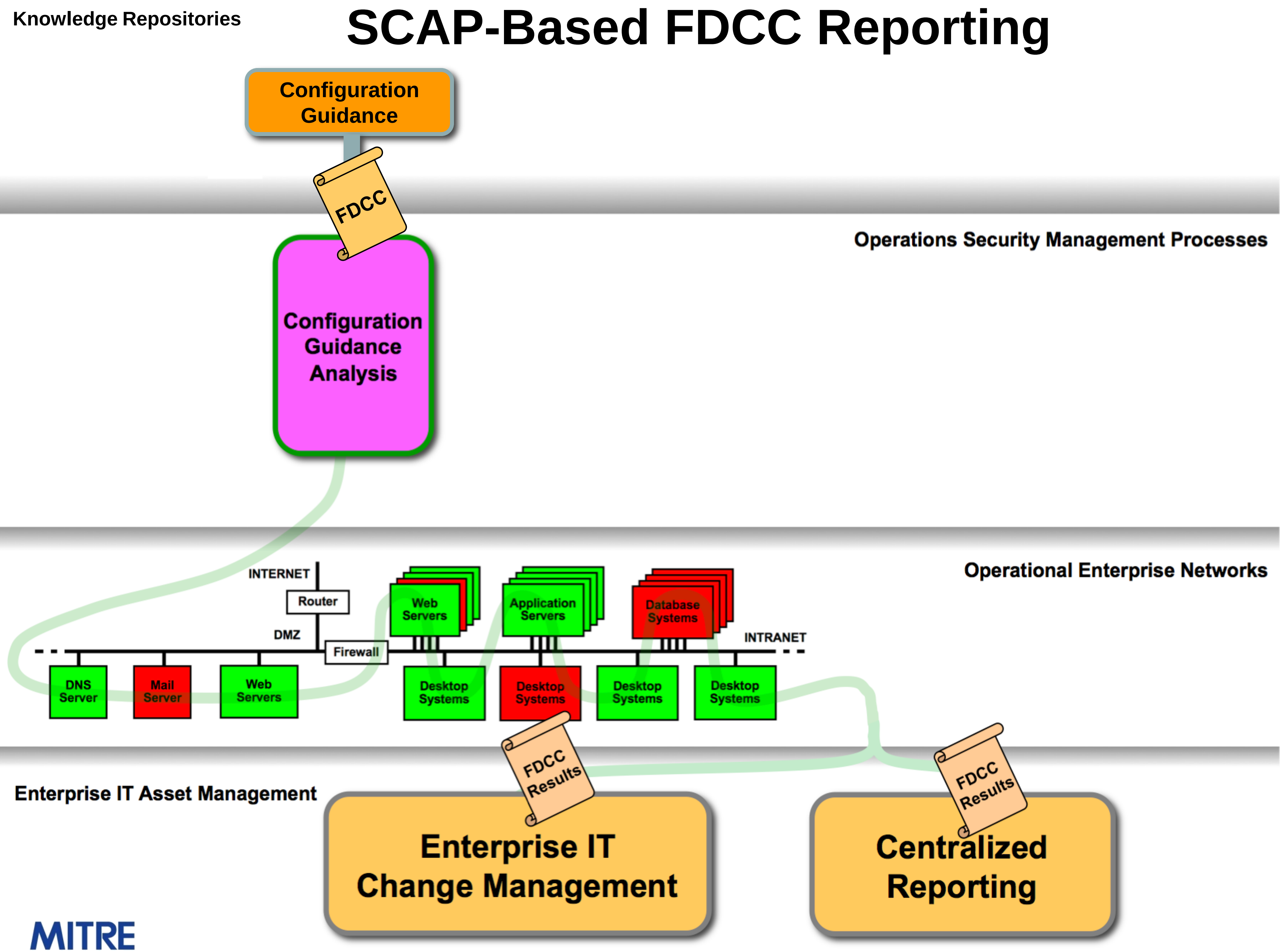
Enterprise IT Asset Management

Enterprise IT Change Management

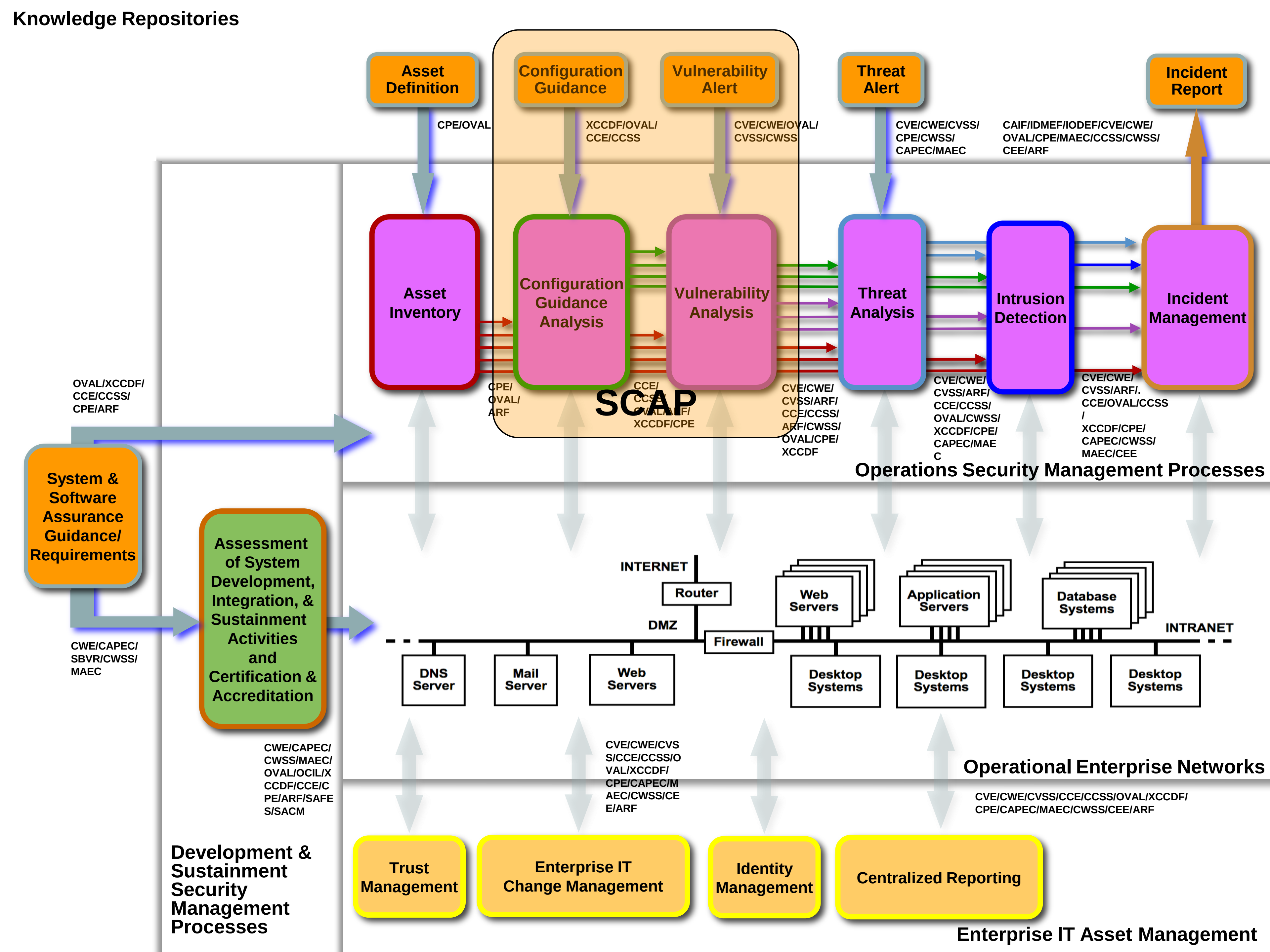
Centralized Reporting

MITRE

SCAP-Based FDCC Reporting



MITRE



Knowledge Repositories

Asset Definition

CPE/OVAL

Configuration Guidance

XCCDF/OVAL/
CCE/CCSS

Vulnerability Alert

CVE/CWE/OVAL/
CVSS/CWSS

Threat Alert

CVE/CWE/CVSS/
CPE/CWSS/
CAPEC/MAEC

CAIF/IDMEF/IODEF/CVE/CWE/
OVAL/CPE/MAEC/CCSS/CWSS/
CEE/ARF

Incident Report

Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

Threat Analysis

Intrusion Detection

Incident Management

CPE/
OVAL/
ARF

SCAP

CCE/
CCSS/
OVAL/ARF/
XCCDF/CPE

CVE/CWE/
CVSS/ARF/
CCE/CCSS/
ARF/CWSS/
OVAL/CPE/
XCCDF

CVE/CWE/
CVSS/ARF/
CCE/CCSS/
OVAL/CWSS/
XCCDF/CPE/
CAPEC/MAE
C

CVE/CWE/
CVSS/ARF/.
CCE/OVAL/CCSS
/
XCCDF/CPE/
CAPEC/CWSS/
MAEC/CEE

Operations Security Management Processes

OVAL/XCCDF/
CCE/CCSS/
CPE/ARF

System & Software Assurance Guidance/ Requirements

CWE/CAPEC/
SBVR/CWSS/
MAEC

Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation

CWE/CAPEC/
CWSS/MAEC/
OVAL/OCIL/X
CCDF/CCE/C
PE/ARF/SAFE
S/SACM

INTERNET

Router

DMZ

Firewall

Web Servers

Application Servers

Database Systems

INTRANET

DNS Server

Mail Server

Web Servers

Desktop Systems

Desktop Systems

Desktop Systems

Desktop Systems

CVE/CWE/CVS
S/CCE/CCSS/O
VAL/XCCDF/
CPE/CAPEC/M
AEC/CWSS/CE
E/ARF

Operational Enterprise Networks

CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/ARF

Development & Sustainment Security Management Processes

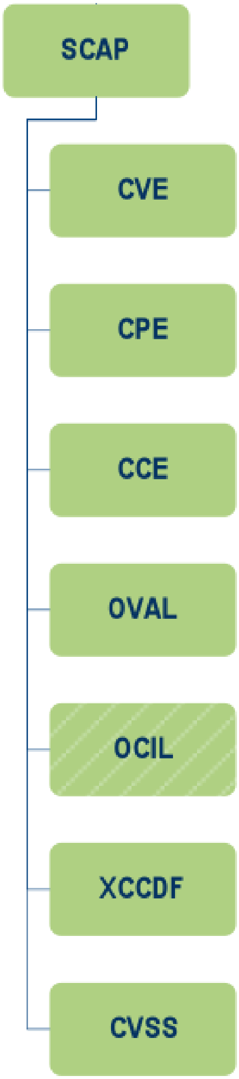
Trust Management

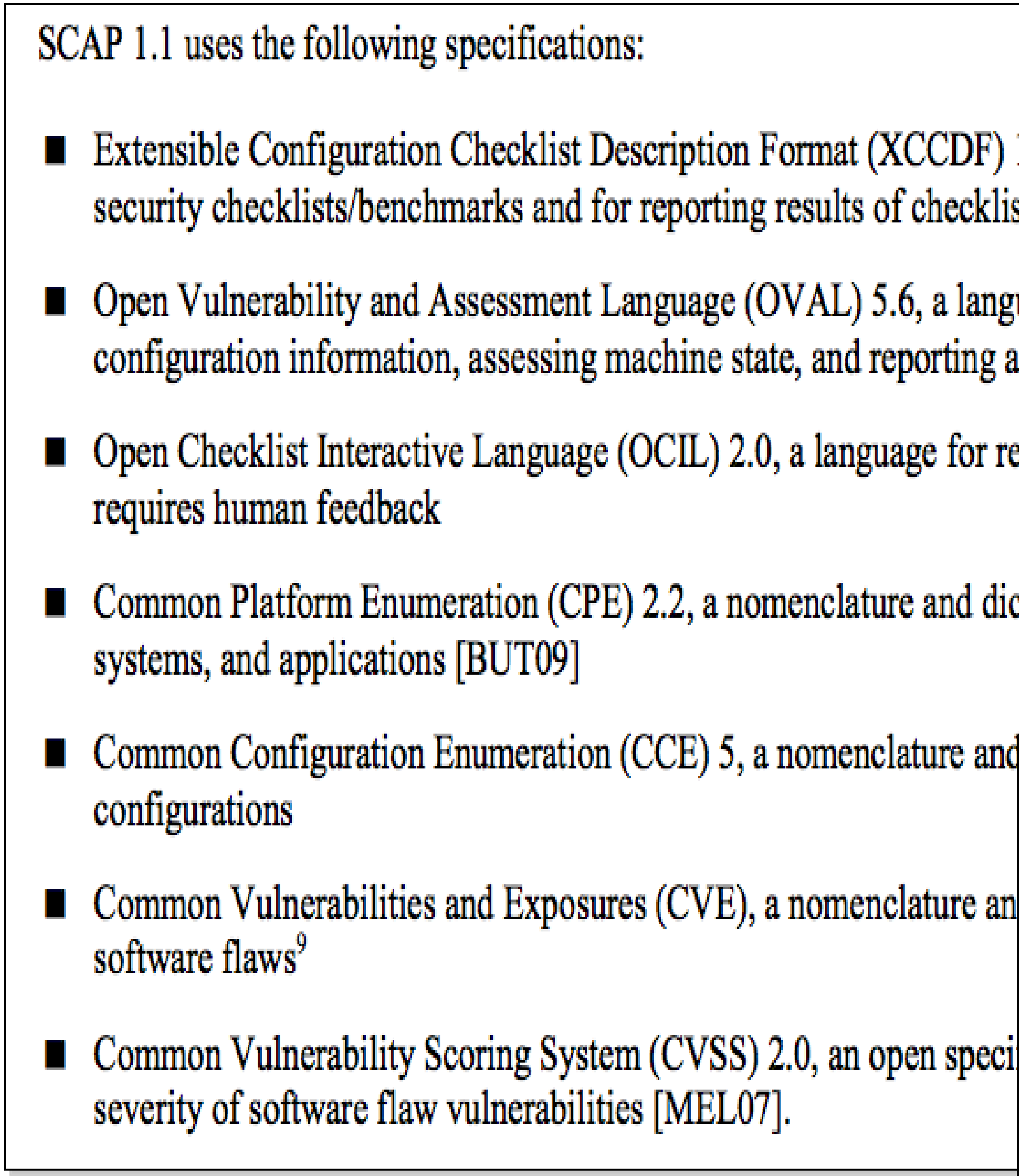
Enterprise IT Change Management

Identity Management

Centralized Reporting

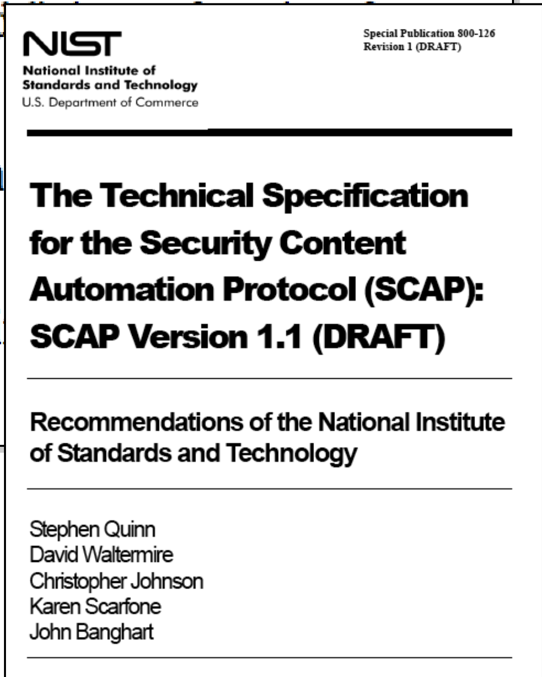
Enterprise IT Asset Management





SCAP 1.1 uses the following specifications:

- Extensible Configuration Checklist Description Format (XCCDF) 1.1.4, a language for authoring security checklists/benchmarks and for reporting results of checklist evaluation [QUI08]
- Open Vulnerability and Assessment Language (OVAL) 5.6, a language for representing system configuration information, assessing machine state, and reporting assessment results
- Open Checklist Interactive Language (OCIL) 2.0, a language for representing security checks that requires human feedback
- Common Platform Enumeration (CPE) 2.2, a nomenclature and dictionary of hardware, operating systems, and applications [BUT09]
- Common Configuration Enumeration (CCE) 5, a nomenclature and configurations
- Common Vulnerabilities and Exposures (CVE), a nomenclature an software flaws[9]
- Common Vulnerability Scoring System (CVSS) 2.0, an open speci severity of software flaw vulnerabilities [MEL07].



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-126
Revision 1 (DRAFT)

The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1 (DRAFT)

Recommendations of the National Institute of Standards and Technology

Stephen Quinn
David Waltermire
Christopher Johnson
Karen Scarfone
John Banghart

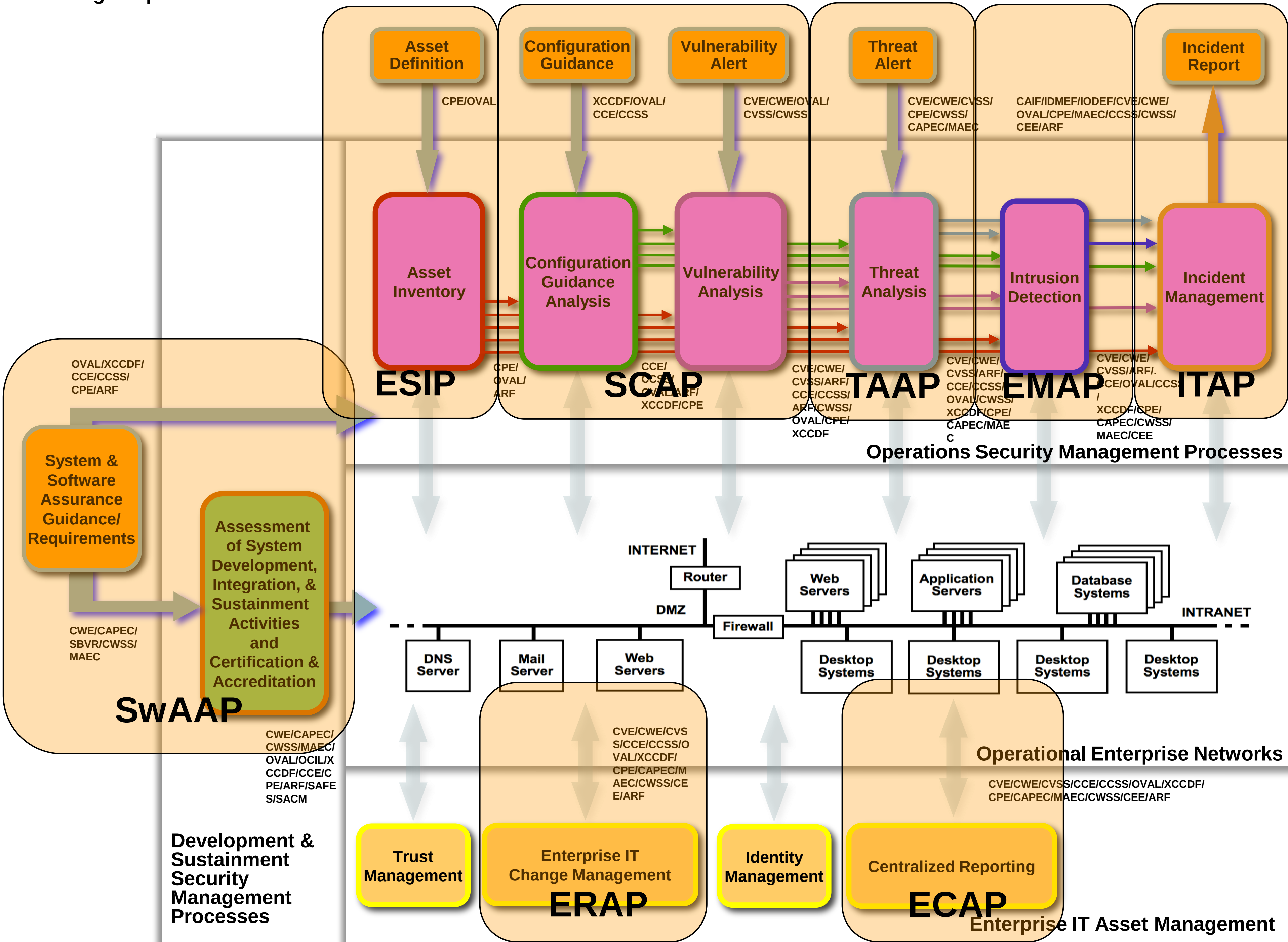
Other Automation Protocols Can Capture the Government Use Cases…

- **Enterprise System Information Protocol (ESIP)**
  - For reporting of asset inventory information. Common Platform Enumeration (CPE), etc.
- **Threat Analysis Automation Protocol (TAAP)**
  - For reporting and sharing structured threat information. Malware Attribute Enumeration & Characterization (MAEC), Common Attack Pattern Enumeration & Classification (CAPEC), Common Platform Enumeration (CPE), Common Weakness Enumeration (CWE), Open Vulnerability and Assessment Language (OVAL), Common Configuration Enumeration (CCE), and Common Vulnerabilities and Exposures (CVE).
- **Event Management Automation Protocol (EMAP)**
  - For reporting of security events. Common Event Expression (CEE), Malware Attribute Enumeration & Characterization (MAEC), and Common Attack Pattern Enumeration & Classification (CAPEC).

Other Automation Protocols Can Capture the Government Use Cases…(concluded)

- **Incident Tracking and Assessment Protocol (ITAP)**
  - For tracking, reporting, managing and sharing incident information. Open Vulnerability and Assessment Language (OVAL), Common Platform Enumeration (CPE), Common Configuration Enumeration (CCE), Common Vulnerabilities and Exposures (CVE), Common Vulnerability Scoring System (CVSS), Malware Attribute Enumeration & Characterization (MAEC), Common Attack Pattern Enumeration & Classification (CAPEC), Common Weakness Enumeration (CWE), Common Event Expression (CEE), Incident Object Description Exchange Format (IODEF), National Information Exchange Model (NIEM), and Cybersecurity Information Exchange Format (CYBEX).
- **Enterprise Remediation Automation Protocol (ERAP)**
  - For automated remediation of mis-configuration & missing patches. Common Remediation Enumeration (CRE), Extended Remediation Information (ERI), Open Vulnerability and Assessment Language (OVAL), Common Platform Enumeration (CPE), and Common Configuration Enumeration (CCE).
- **Enterprise Compliance Automation Protocol (ECAP)**
  - For reporting configuration compliance. Asset Reporting Format (ARF), Open Checklist Reporting Language (OCRL), etc.

Knowledge Repositories



Asset Definition

CPE/OVAL

Configuration Guidance

XCCDF/OVAL/
CCE/CCSS

Vulnerability Alert

CVE/CWE/OVAL/
CVSS/CWSS

Threat Alert

CVE/CWE/CVSS/
CPE/CWSS/
CAPEC/MAEC

CAIF/IDMEF/IODEF/CVE/CWE/
OVAL/CPE/MAEC/CCSS/CWSS/
CEE/ARF

Incident Report

Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

Threat Analysis

Intrusion Detection

Incident Management

ESIP

SCAP

TAAP

EMAP

ITAP

CPE/
OVAL/
ARF

CCE/
CCSS/
OVAL/ARF/
XCCDF/CPE

CVE/CWE/
CVSS/ARF/
CCE/CCSS/
ARF/CWSS/
OVAL/CPE/
XCCDF

CVE/CWE/
CVSS/ARF/
CCE/CCSS/
OVAL/CWSS/
XCCDF/CPE/
CAPEC/MAE
C

CVE/CWE/
CVSS/ARF/.
CCE/OVAL/CCSS
/
XCCDF/CPE/
CAPEC/CWSS/
MAEC/CEE

Operations Security Management Processes

OVAL/XCCDF/
CCE/CCSS/
CPE/ARF

System & Software Assurance Guidance/ Requirements

Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation

CWE/CAPEC/
SBVR/CWSS/
MAEC

SwAAP

CWE/CAPEC/
CWSS/MAEC/
OVAL/OCIL/X
CCDF/CCE/C
PE/ARF/SAFE
S/SACM

INTERNET

Router

DMZ

Firewall

INTRANET

DNS Server

Mail Server

Web Servers

Web Servers

Application Servers

Database Systems

Desktop Systems

Desktop Systems

Desktop Systems

Desktop Systems

CVE/CWE/CVS
S/CCE/CCSS/O
VAL/XCCDF/
CPE/CAPEC/M
AEC/CWSS/CE
E/ARF

Operational Enterprise Networks

CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/ARF

Development & Sustainment Security Management Processes

Trust Management

Enterprise IT Change Management

ERAP

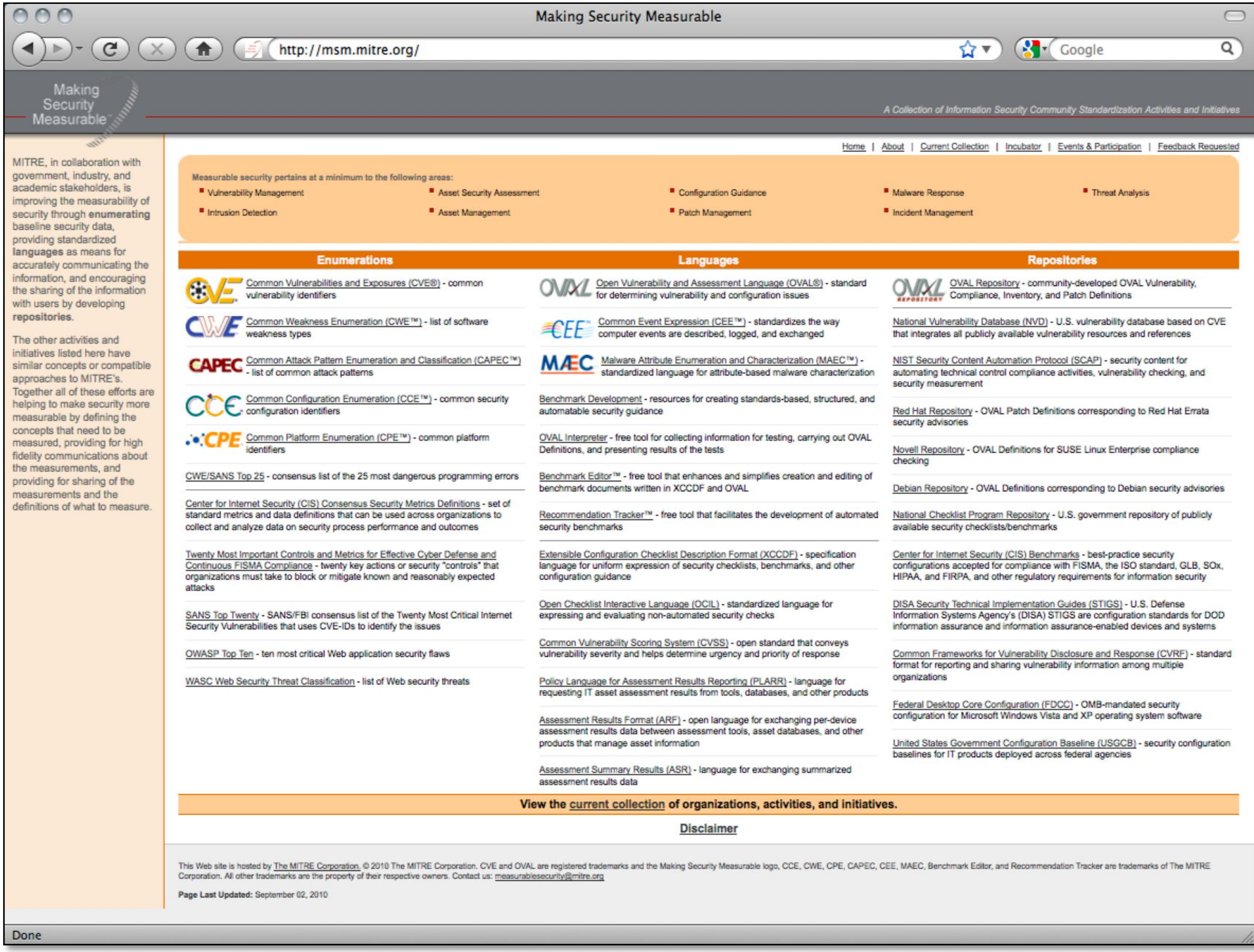
Identity Management

Centralized Reporting

ECAP

Enterprise IT Asset Management

[makingsecuritymeasurable.mitre.org]



Making Security Measurable™

A Collection of Information Security Community Standardization Activities and Initiatives

Home | About | Current Collection | Incubator | Events & Participation | Feedback Requested

MITRE, in collaboration with government, industry, and academic stakeholders, is improving the measurability of security through **enumerating** baseline security data, providing standardized **languages** as means for accurately communicating the information, and encouraging the sharing of the information with users by developing **repositories**.

The other activities and initiatives listed here have similar concepts or compatible approaches to MITRE's. Together all of these efforts are helping to make security more measurable by defining the concepts that need to be measured, providing for high fidelity communications about the measurements, and providing for sharing of the measurements and the definitions of what to measure.

Measurable security pertains at a minimum to the following areas:

- Vulnerability Management
- Intrusion Detection
- Asset Security Assessment
- Asset Management
- Configuration Guidance
- Patch Management
- Malware Response
- Incident Management
- Threat Analysis

Enumerations

CVE – Common Vulnerabilities and Exposures (CVE®) - common vulnerability identifiers

CWE – Common Weakness Enumeration (CWE™) - list of software weakness types

CAPEC – Common Attack Pattern Enumeration and Classification (CAPEC™) - list of common attack patterns

CCE – Common Configuration Enumeration (CCE™) - common security configuration identifiers

CPE – Common Platform Enumeration (CPE™) - common platform identifiers

CWE/SANS Top 25 - consensus list of the 25 most dangerous programming errors

Center for Internet Security (CIS) Consensus Security Metrics Definitions - set of standard metrics and data definitions that can be used across organizations to collect and analyze data on security process performance and outcomes

Twenty Most Important Controls and Metrics for Effective Cyber Defense and Continuous FISMA Compliance - twenty key actions or security "controls" that organizations must take to block or mitigate known and reasonably expected attacks

SANS Top Twenty - SANS/FBI consensus list of the Twenty Most Critical Internet Security Vulnerabilities that uses CVE-IDs to identify the issues

OWASP Top Ten - ten most critical Web application security flaws

WASC Web Security Threat Classification - list of Web security threats

Languages

OVAL – Open Vulnerability and Assessment Language (OVAL®) - standard for determining vulnerability and configuration issues

CEE – Common Event Expression (CEE™) - standardizes the way computer events are described, logged, and exchanged

MAEC – Malware Attribute Enumeration and Characterization (MAEC™) - standardized language for attribute-based malware characterization

Benchmark Development - resources for creating standards-based, structured, and automatable security guidance

OVAL Interpreter - free tool for collecting information for testing, carrying out OVAL Definitions, and presenting results of the tests

Benchmark Editor™ - free tool that enhances and simplifies creation and editing of benchmark documents written in XCCDF and OVAL

Recommendation Tracker™ - free tool that facilitates the development of automated security benchmarks

Extensible Configuration Checklist Description Format (XCCDF) - specification language for uniform expression of security checklists, benchmarks, and other configuration guidance

Open Checklist Interactive Language (OCIL) - standardized language for expressing and evaluating non-automated security checks

Common Vulnerability Scoring System (CVSS) - open standard that conveys vulnerability severity and helps determine urgency and priority of response

Policy Language for Assessment Results Reporting (PLARR) - language for requesting IT asset assessment results from tools, databases, and other products

Assessment Results Format (ARF) - open language for exchanging per-device assessment results data between assessment tools, asset databases, and other products that manage asset information

Assessment Summary Results (ASR) - language for exchanging summarized assessment results data

Repositories

OVAL REPOSITORY – OVAL Repository - community-developed OVAL Vulnerability, Compliance, Inventory, and Patch Definitions

National Vulnerability Database (NVD) - U.S. vulnerability database based on CVE that integrates all publicly available vulnerability resources and references

NIST Security Content Automation Protocol (SCAP) - security content for automating technical control compliance activities, vulnerability checking, and security measurement

Red Hat Repository - OVAL Patch Definitions corresponding to Red Hat Errata security advisories

Novell Repository - OVAL Definitions for SUSE Linux Enterprise compliance checking

Debian Repository - OVAL Definitions corresponding to Debian security advisories

National Checklist Program Repository - U.S. government repository of publicly available security checklists/benchmarks

Center for Internet Security (CIS) Benchmarks - best-practice security configurations accepted for compliance with FISMA, the ISO standard, GLB, SOx, HIPAA, and FIRPA, and other regulatory requirements for information security

DISA Security Technical Implementation Guides (STIGS) - U.S. Defense Information Systems Agency's (DISA) STIGS are configuration standards for DOD information assurance and information assurance-enabled devices and systems

Common Frameworks for Vulnerability Disclosure and Response (CVRF) - standard format for reporting and sharing vulnerability information among multiple organizations

Federal Desktop Core Configuration (FDCC) - OMB-mandated security configuration for Microsoft Windows Vista and XP operating system software

United States Government Configuration Baseline (USGCB) - security configuration baselines for IT products deployed across federal agencies

View the current collection of organizations, activities, and initiatives.

Disclaimer

This Web site is hosted by The MITRE Corporation. © 2010 The MITRE Corporation. CVE and OVAL are registered trademarks and the Making Security Measurable logo, CCE, CWE, CPE, CAPEC, CEE, MAEC, Benchmark Editor, and Recommendation Tracker are trademarks of The MITRE Corporation. All other trademarks are the property of their respective owners. Contact us: measurablesecurity@mitre.org

Page Last Updated: September 02, 2010

Making Security Measurable™

Questions?

ramartin@mitre.org