Practical Application of Software Assurance Assessment

Robert A. Martin - Sean Barnum - Daniel Wolf

4:15 PM - 5:00 PM

Wednesday April 30, 2008

MITRE

2007 InformationWeek/Accenture Global Information Security Survey

Cyber Threats to the Enterprise

2007 InformationWeek/Accenture Global Information Security Survey

Published July 16, 2007

2007 InformationWeek/Accenture Global Information Security Survey

Many Types of Attacks…

- known vulns in OS & packaged apps; misconfigured systems; unknown vulns in own apps; aimed at DB, applications, and web sites

Need to Master Many Technologies…

- firewalls; anti-virus; anti-spyware; app firewalls; IDS; SIMS; vulnerability scans; patching

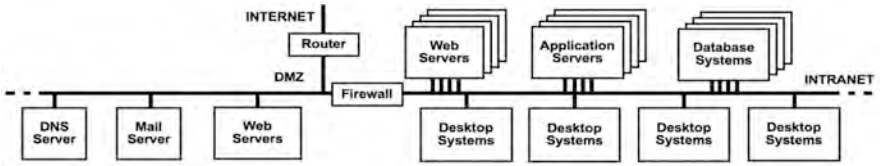
More Vulnerable Because of…

- exposed backend & homegrown apps; increased sophistication & volume of attacks; more malicious intent; lack of senior attention; incompatible security products; unable to adapt policies/configuration rules; outsourcing

Published July 16, 2007

MITRE

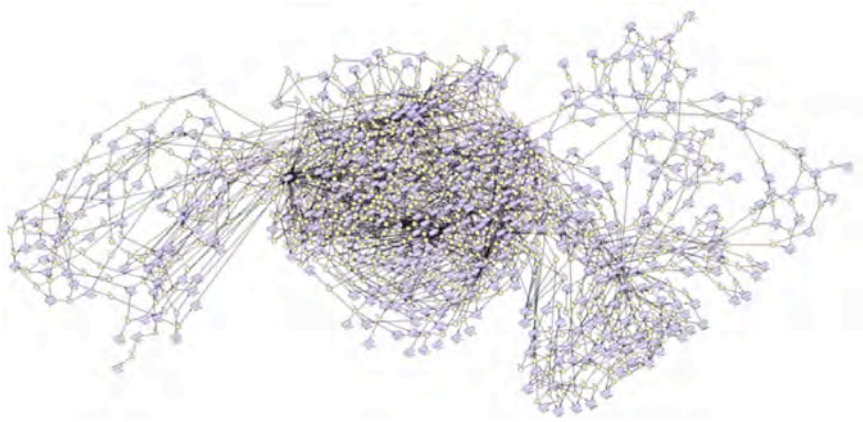
Enterprise Networks



Making Security Measurable

MITRE

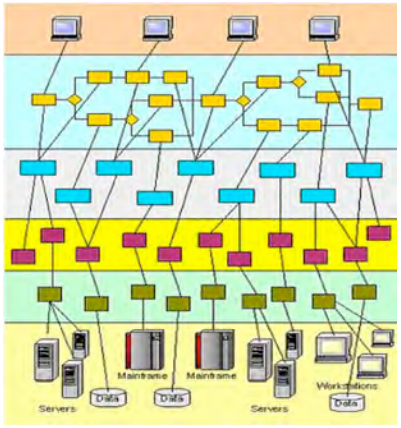
Real Enterprise Networks



Making Security Measurable

MITRE

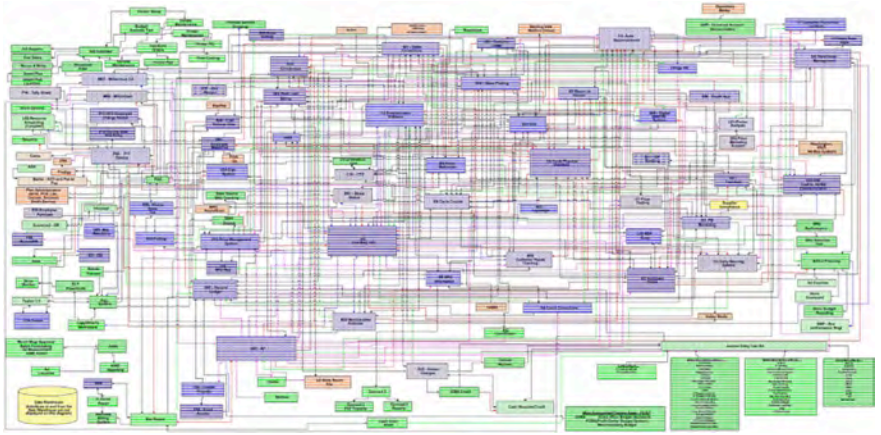
Information Technology-Based Business Capabilities As Conceived



Making Security Measurable

MITRE

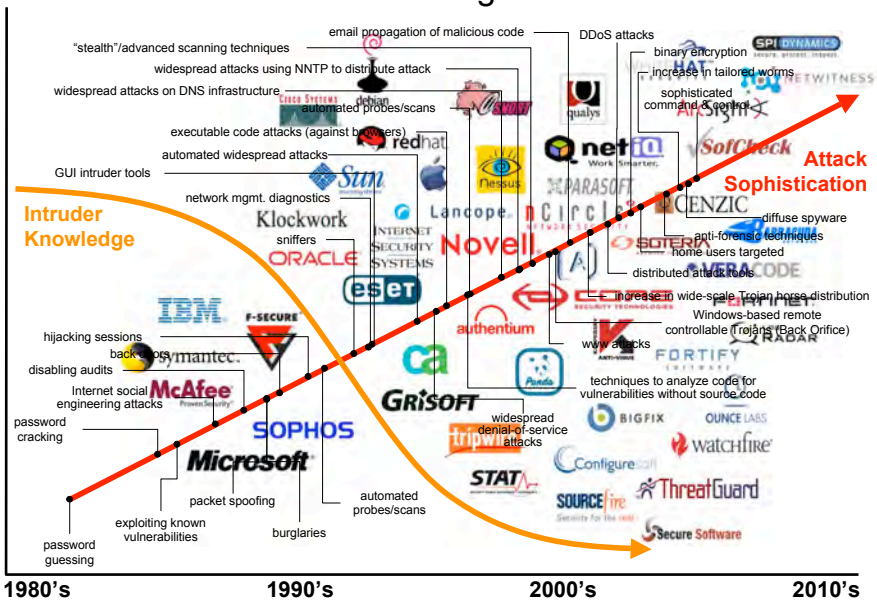
Reality



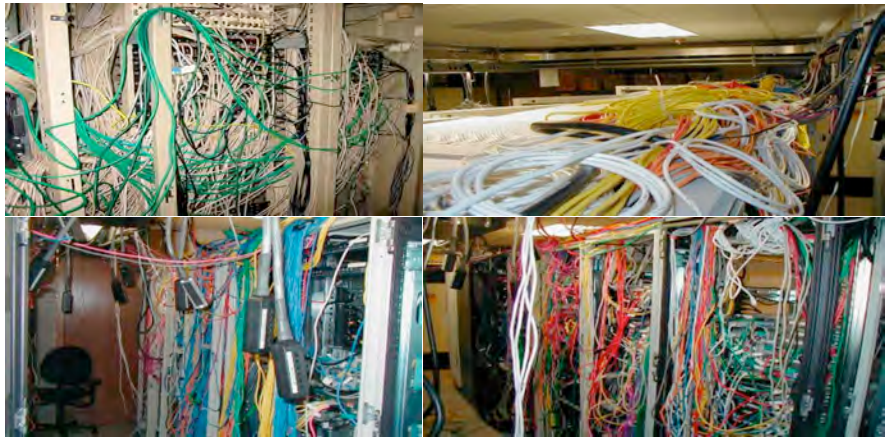
Making Security Measurable

MITRE

Solutions Also Emerged Over Time



Like Security - Networks Evolved



Each new solution had to integrate with the existing solutions -->>> every enterprise ends up with a "unique" tapestry of solutions

Making Security Measurable

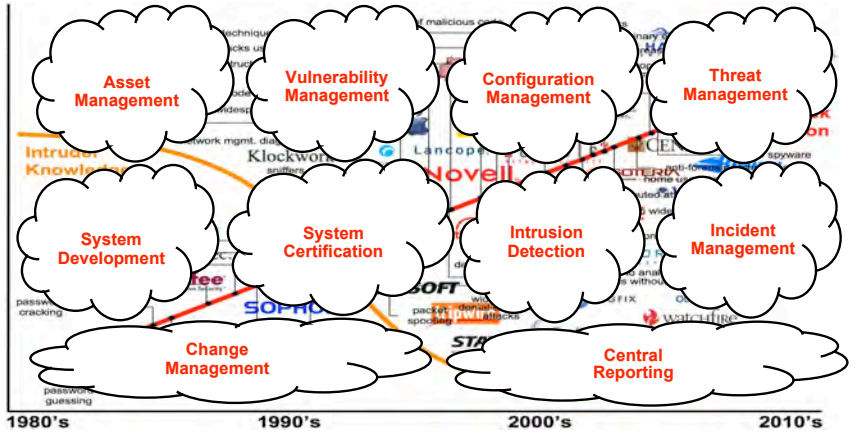
MITRE

But A More Supportable Solution Is Possible with Standards and Architecture Principles

Making Security Measurable

MITRE

Architecting Security



Making Security Measurable

MITRE

In Summary: Today Every Organization Has a Different Way of Doing Cyber Security…

- **Cyber security, tools, practices and technology have evolved dramatically over the last 10 years**
- **The result has been that most enterprises have been buying each new tool & training their people on it & integrating it as they realize they need to address a new area of Cyber Security…**
- **Then they buy another tool & train their people on that one too & integrate it with the other tools…**
- **Repeat for each "type" of security tool/challenge that appears…**
- **Result - each organization has a different tapestry of tools/processes integrated together trying to do the Cyber Security job…**
  - Assets, Configuration, Vulnerabilities, Patches, Intrusions, Malware, Malicious Code, etc.

Making Security Measurable™

Instead we should be architecting our security measurement and management method and get tools to implement and support it.

MITRE

What Do The Building Blocks for "Architecting Security" Look Like?

- Standard ways for enumerating "things we care about"
- Languages/Formats for encoding/carrying high fidelity content about the "things we care about"
- Repositories of this content for use in communities or individual organizations
- Adoption/branding and vetting programs to encourage adoption by tools and services

Making Security Measurable™

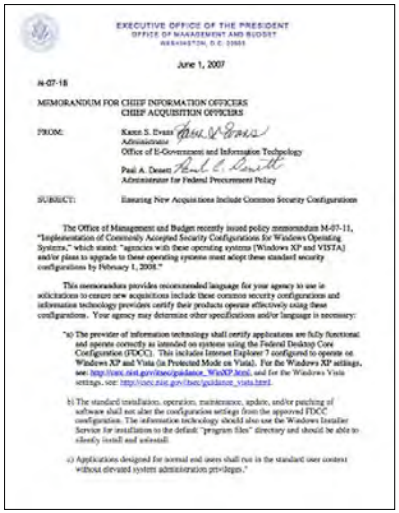
MITRE

The Building Blocks Are:

- Enumerations
  - **Catalog the fundamental entities in IA, Cyber Security, and Software Assurance**
    - **Vulnerabilities (CVE), misconfigurations (CCE), software packages (CPE), malware (CME), attack patterns (CAPEC), weaknesses in code/design/architecture (CWE)**
- Languages/Formats
  - **Support the creation of machine-readable state assertions, assessment results, and messages**
    - **Configuration/vulnerability/patch/asset patterns (XCCDF & OVAL), results from standards-based assessments (CRF), software security patterns (SBVR), event patterns (CEE), malware patterns (MAEC), risk of a vulnerability (CVSS), information messages (CAIF & *DEF)**
- Knowledge Repositories
  - **Packages of assertions supporting a specific application**
    - **Vulnerability advisories & alerts, (US-CERT Advisories/IAVAs), configuration assessment (NIST Checklists, CIS Benchmarks, NSA Configuration Guides, DISA STIGS), asset inventory (NIST/DHS NVD), code assessment & certification (NIST SAMATE, DoD DIACAP & eMASS)**

Tools

- **Interpret IA, Cyber Security, and SwA content in context of enterprise network**
- **Methods for assessing compliance to languages, formats, and enumerations**



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

June 1, 2007

M-07-18

MEMORANDUM FOR CHIEF INFORMATION OFFICERS
CHIEF ACQUISITION OFFICERS

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

Paul A. Denett
Administrator for Federal Procurement Policy

SUBJECT: Ensuring New Acquisitions Include Common Security Configurations

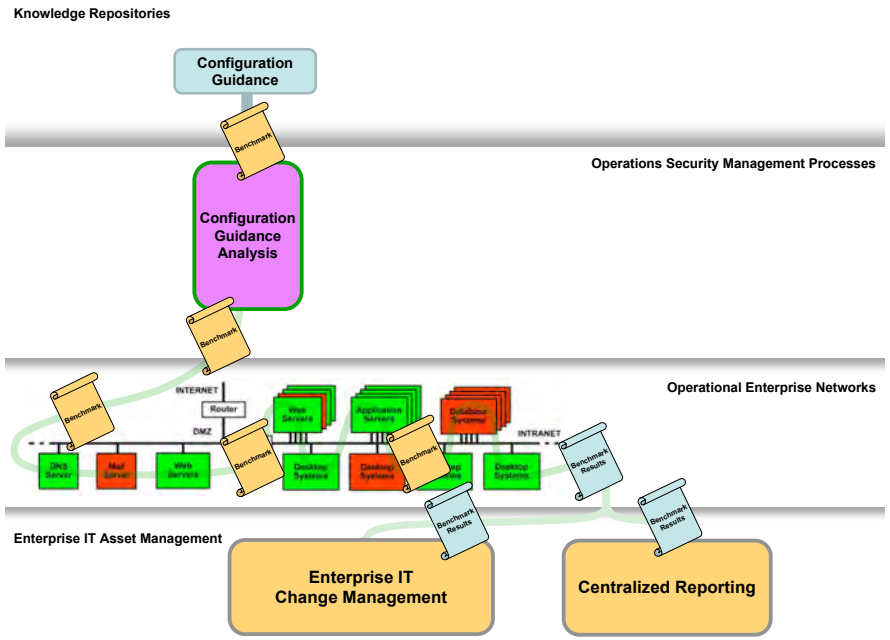
The Office of Management and Budget recently issued policy memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," which stated: "agencies with these operating systems [Windows XP and VISTA] and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008."

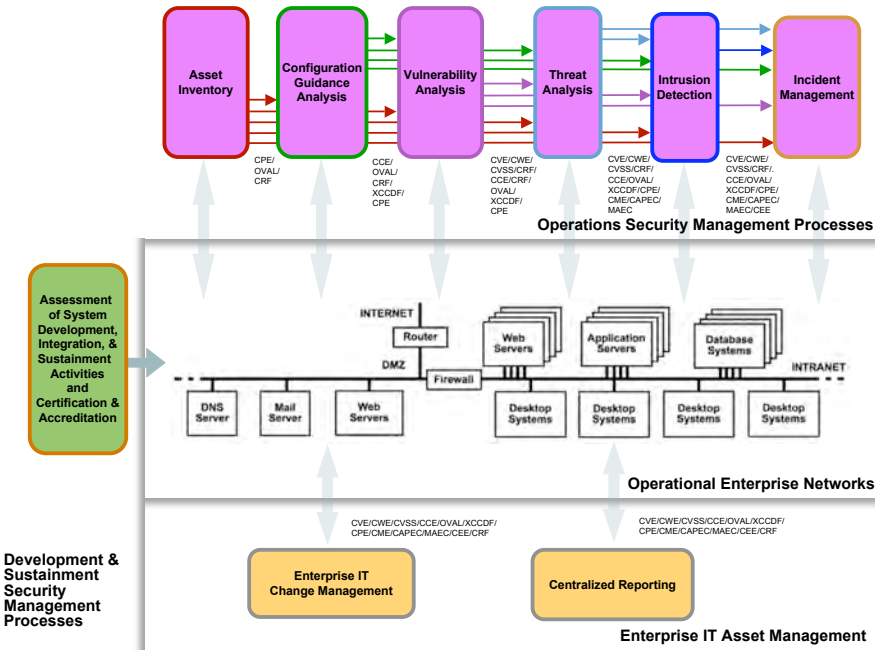
This memorandum provides recommended language for your agency to use in solicitations to ensure new acquisitions include these common security configurations and information technology providers certify their products operate effectively using these configurations. Your agency may determine other specifications and/or language is necessary:

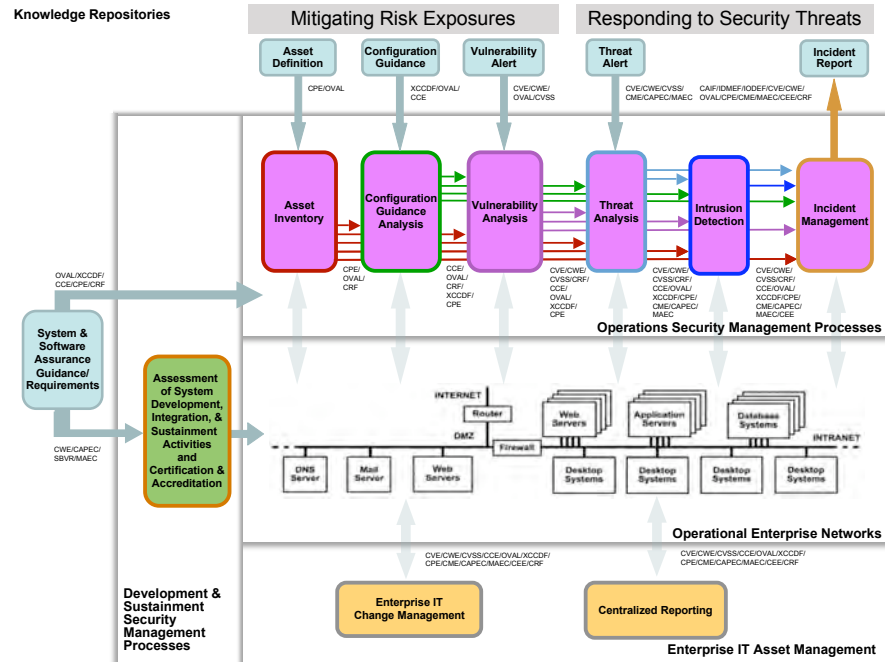
"a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista). For the Windows XP settings, see: http://csrc.nist.gov/itsec/guidance_WinXP.html, and for the Windows Vista settings, see: http://csrc.nist.gov/itsec/guidance_vista.html.

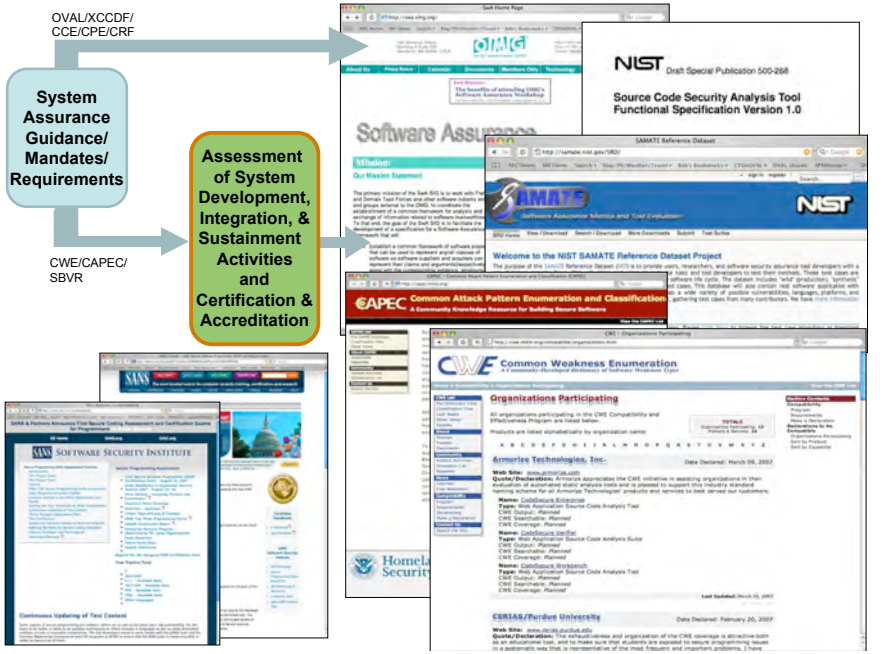
b) The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.

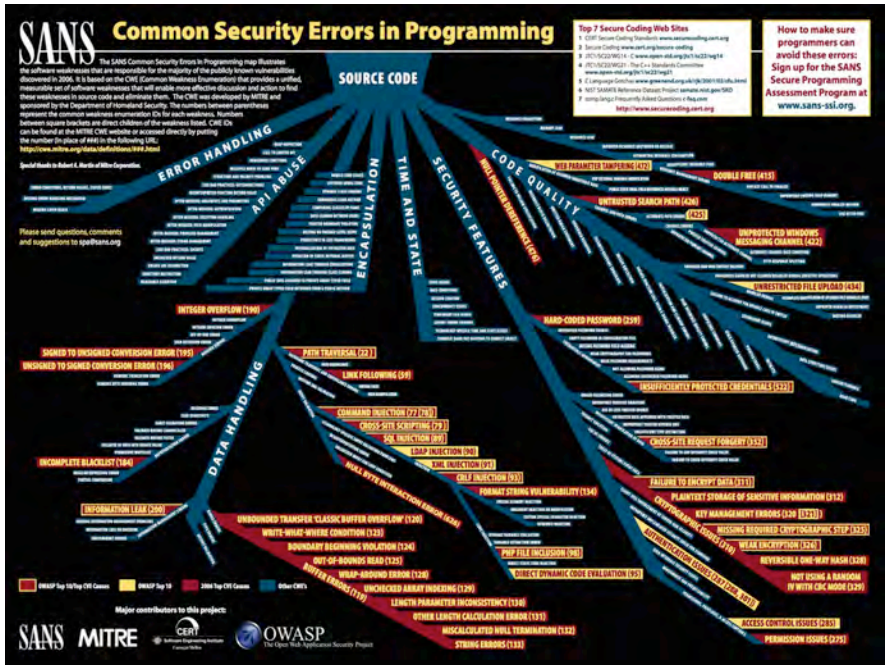
c) Applications designed for normal end users shall run in the standard user context without elevated system administration privileges."


Knowledge Repositories
Configuration Guidance
Benchmark
Operations Security Management Processes
Configuration Guidance Analysis
Benchmark
Operational Enterprise Networks
INTERNET
Router
DMZ
INTRANET
Benchmark Results
Enterprise IT Asset Management
Enterprise IT Change Management
Centralized Reporting

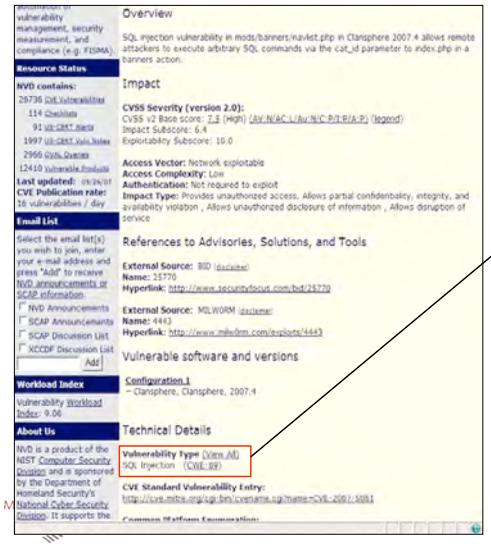

Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ CRF
CCE/ OVAL/ CRF/ XCCDF/ CPE
CVE/CWE/ CVSS/CRF/ CCE/CRF/ OVAL/ XCCDF/ CPE
CVE/CWE/ CVSS/CRF/ CCE/OVAL/ XCCDF/CPE/ CME/CAPEC/ MAEC
CVE/CWE/ CVSS/CRF/ CCE/OVAL/ XCCDF/CPE/ CME/CAPEC/ MAEC/CEE
Operations Security Management Processes
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
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
Operational Enterprise Networks
CVE/CWE/CVSS/CCE/OVAL/XCCDF/ CPE/CME/CAPEC/MAEC/CEE/CRF
CVE/CWE/CVSS/CCE/OVAL/XCCDF/ CPE/CME/CAPEC/MAEC/CEE/CRF
Development & Sustainment Security Management Processes
Enterprise IT Change Management
Centralized Reporting
Enterprise IT Asset Management


Knowledge Repositories
Mitigating Risk Exposures
Responding to Security Threats
Asset Definition
Configuration Guidance
Vulnerability Alert
Threat Alert
Incident Report
CPE/OVAL
XCCDF/OVAL/ CCE
CVE/CWE/ OVAL/CVSS
CVE/CWE/CVSS/ CME/CAPEC/MAEC
CAIF/IDMEF/IODEF/CVE/CWE/ OVAL/CPE/CME/MAEC/CEE/CRF
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ CRF
CCE/ OVAL/ CRF/ XCCDF/ CPE
CVE/CWE/ CVSS/CRF/ CCE/ OVAL/ XCCDF/ CPE
CVE/CWE/ CVSS/CRF/ CCE/OVAL/ XCCDF/CPE/ CME/CAPEC/ MAEC
CVE/CWE/ CVSS/CRF/ CCE/OVAL/ XCCDF/CPE/ CME/CAPEC/ MAEC/CEE
Operations Security Management Processes
OVAL/XCCDF/ CCE/CPE/CRF
System & Software Assurance Guidance/ Requirements
CWE/CAPEC/ SBVR/MAEC
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
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
Operational Enterprise Networks
CVE/CWE/CVSS/CCE/OVAL/XCCDF/ CPE/CME/CAPEC/MAEC/CEE/CRF
CVE/CWE/CVSS/CCE/OVAL/XCCDF/ CPE/CME/CAPEC/MAEC/CEE/CRF
Development & Sustainment Security Management Processes
Enterprise IT Change Management
Centralized Reporting
Enterprise IT Asset Management

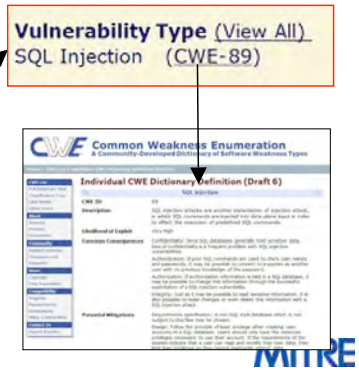

OVAL/XCCDF/ CCE/CPE/CRF
System Assurance Guidance/ Mandates/ Requirements
CWE/CAPEC/ SBVR
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
NIST
Draft Special Publication 500-268
Source Code Security Analysis Tool Functional Specification Version 1.0
Software Assurance
SAMATE
NIST
Welcome to the NIST SAMATE Reference Dataset Project
CAPEC
Common Attack Pattern Enumeration and Classification
CWE
Common Weakness Enumeration
Organizations Participating
SSI
Software Security Institute
Homeland Security



CWE Is Now A Part of the NVD CVE Information

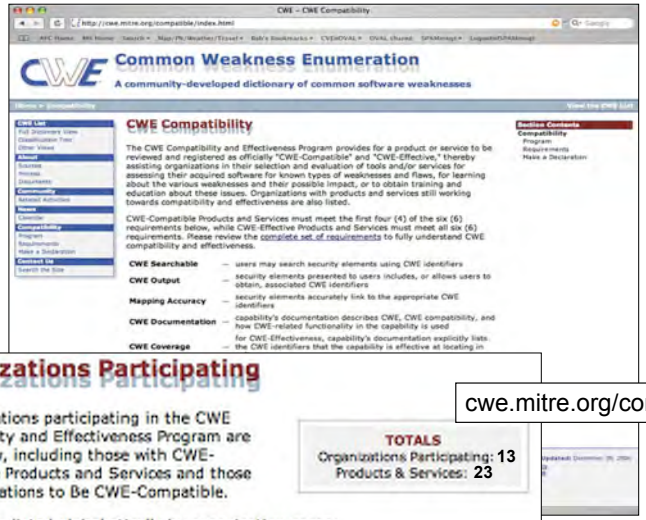


NVD XML feeds also include CWE



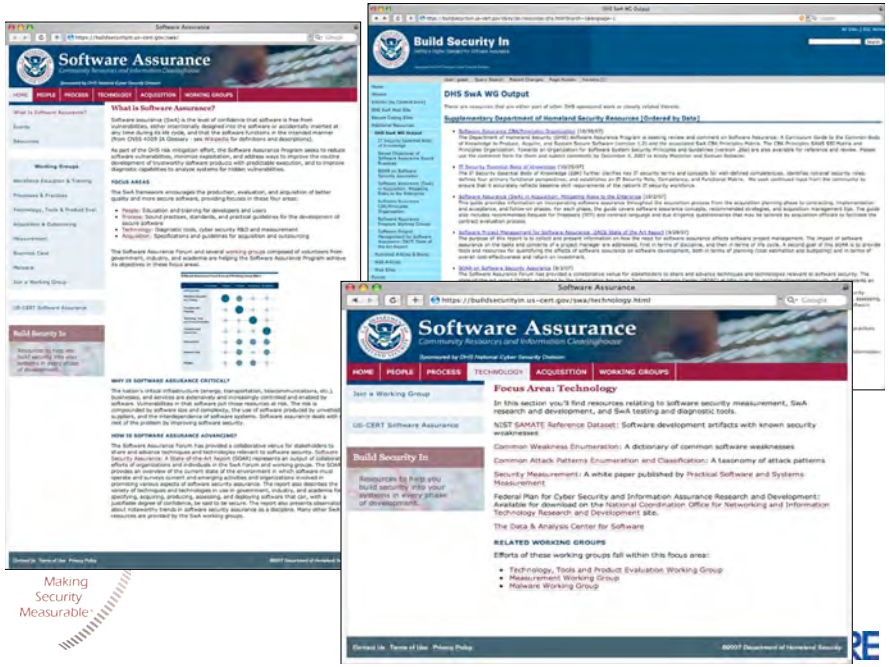
CWE Compatibility & Effectiveness Program

(launched Feb 2007)

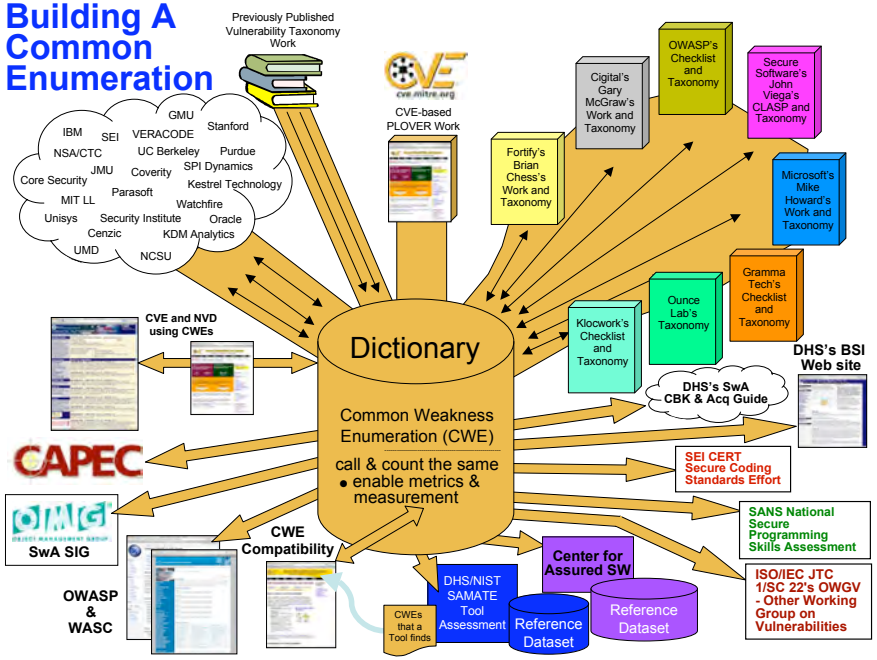


cwe.mitre.org/compatible/

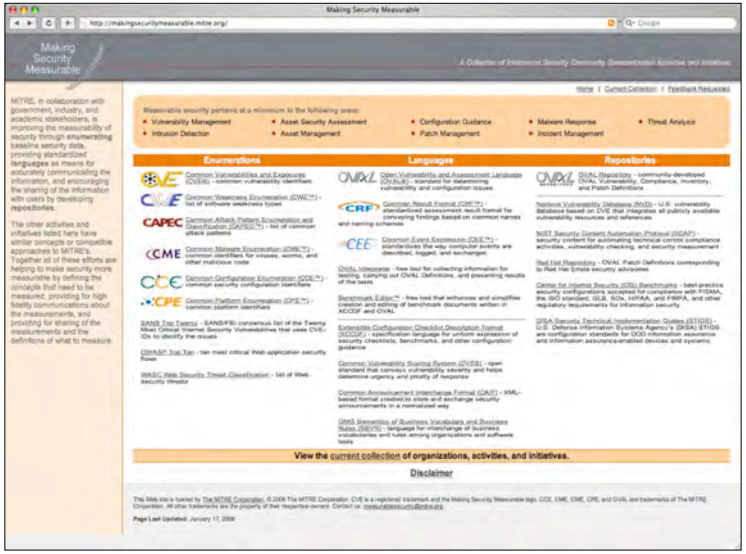
MITRE



Building A Common Enumeration



[makingsecuritymeasurable.mitre.org]



Making Security Measurable

MITRE