“Making Security Measurable”

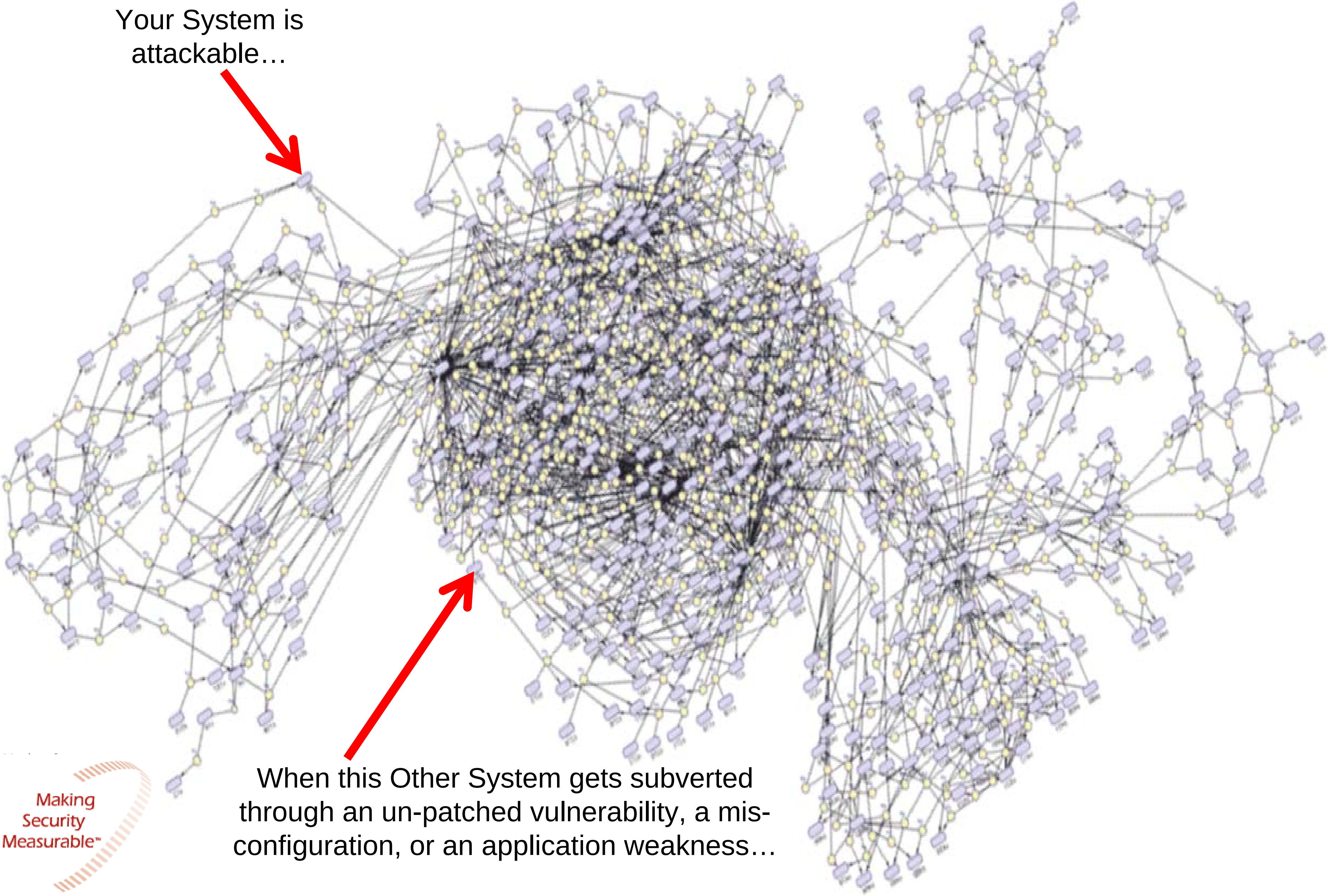
An Integrated Framework for Cyber Security and Incident Response

26 October 2009

Robert A. Martin

ramartin@mitre.org

Today Everything’s Connected



Your System is attackable…

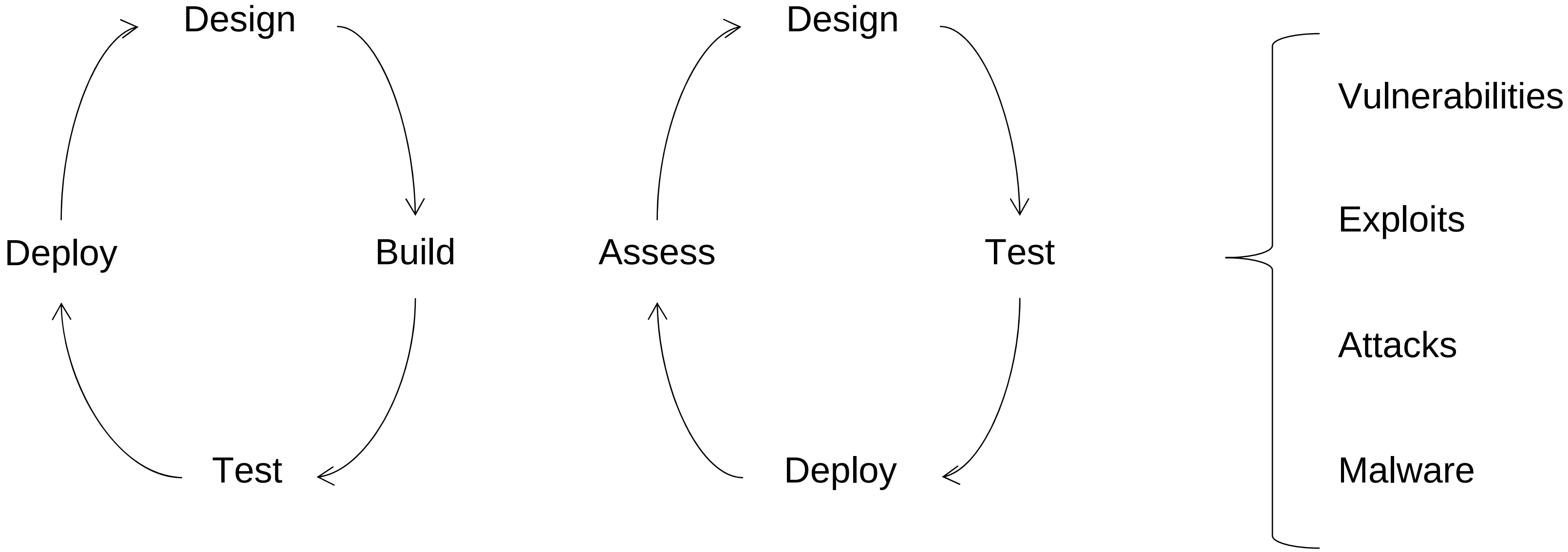
When this Other System gets subverted through an un-patched vulnerability, a mis-configuration, or an application weakness…

Making Security Measurable (MSM): You Are Here

Software Assurance

Enterprise Security Management

Threat Management



Design

Build

Test

Deploy

Design

Test

Deploy

Assess

Vulnerabilities

Exploits

Attacks

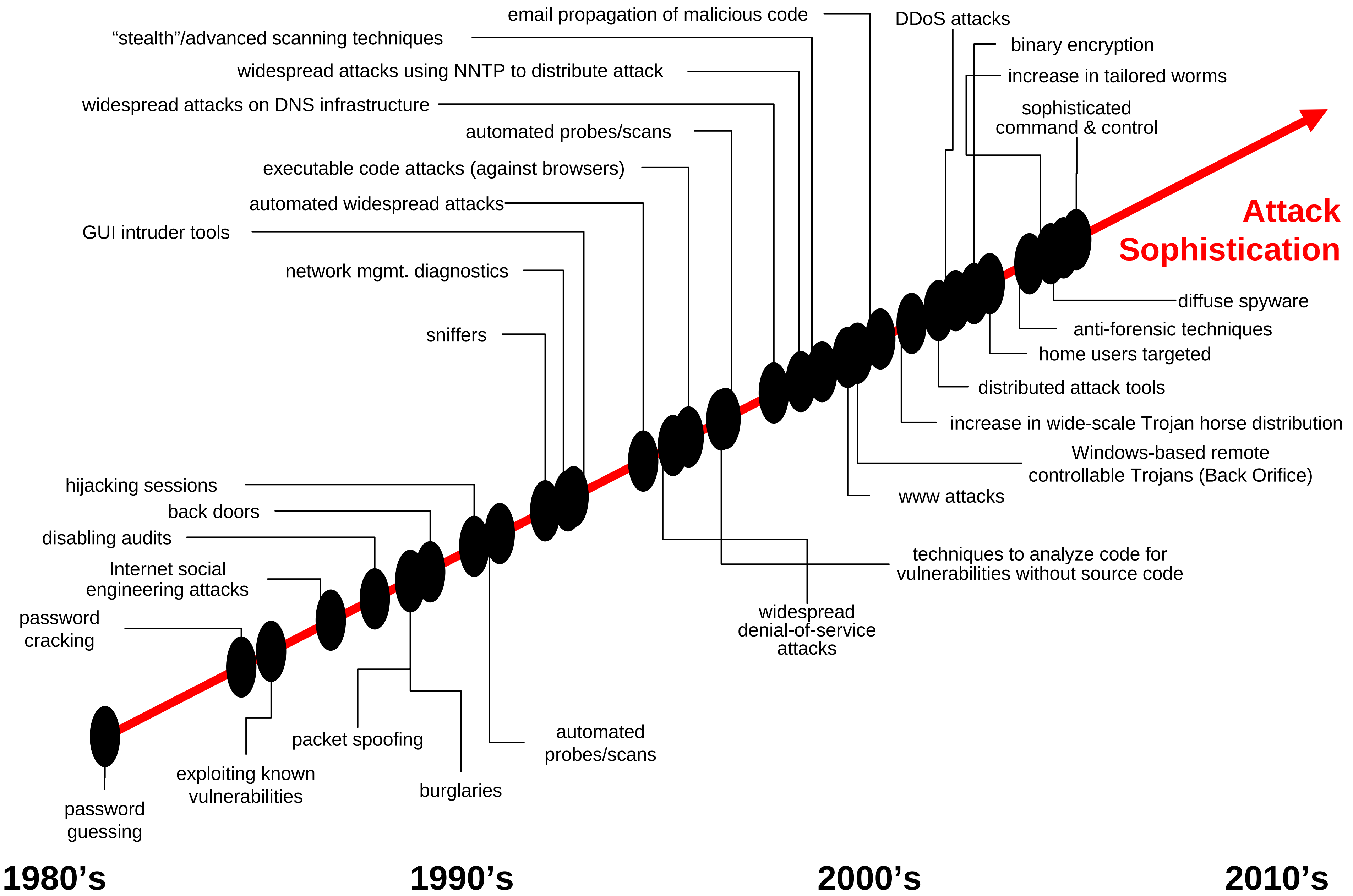
Malware

CWE, CAPEC

CPE, CCE, OVAL, XCCDF

CVE, CAPEC, MAEC

Cyber Threats Emerged Over Time



email propagation of malicious code

“stealth”/advanced scanning techniques

widespread attacks using NNTP to distribute attack

widespread attacks on DNS infrastructure

automated probes/scans

executable code attacks (against browsers)

automated widespread attacks

GUI intruder tools

network mgmt. diagnostics

sniffers

hijacking sessions

back doors

disabling audits

Internet social engineering attacks

password cracking

password guessing

exploiting known vulnerabilities

packet spoofing

burglaries

automated probes/scans

widespread denial-of-service attacks

techniques to analyze code for vulnerabilities without source code

www attacks

Windows-based remote controllable Trojans (Back Orifice)

increase in wide-scale Trojan horse distribution

distributed attack tools

home users targeted

anti-forensic techniques

diffuse spyware

DDoS attacks

binary encryption

increase in tailored worms

sophisticated command & control

Attack Sophistication

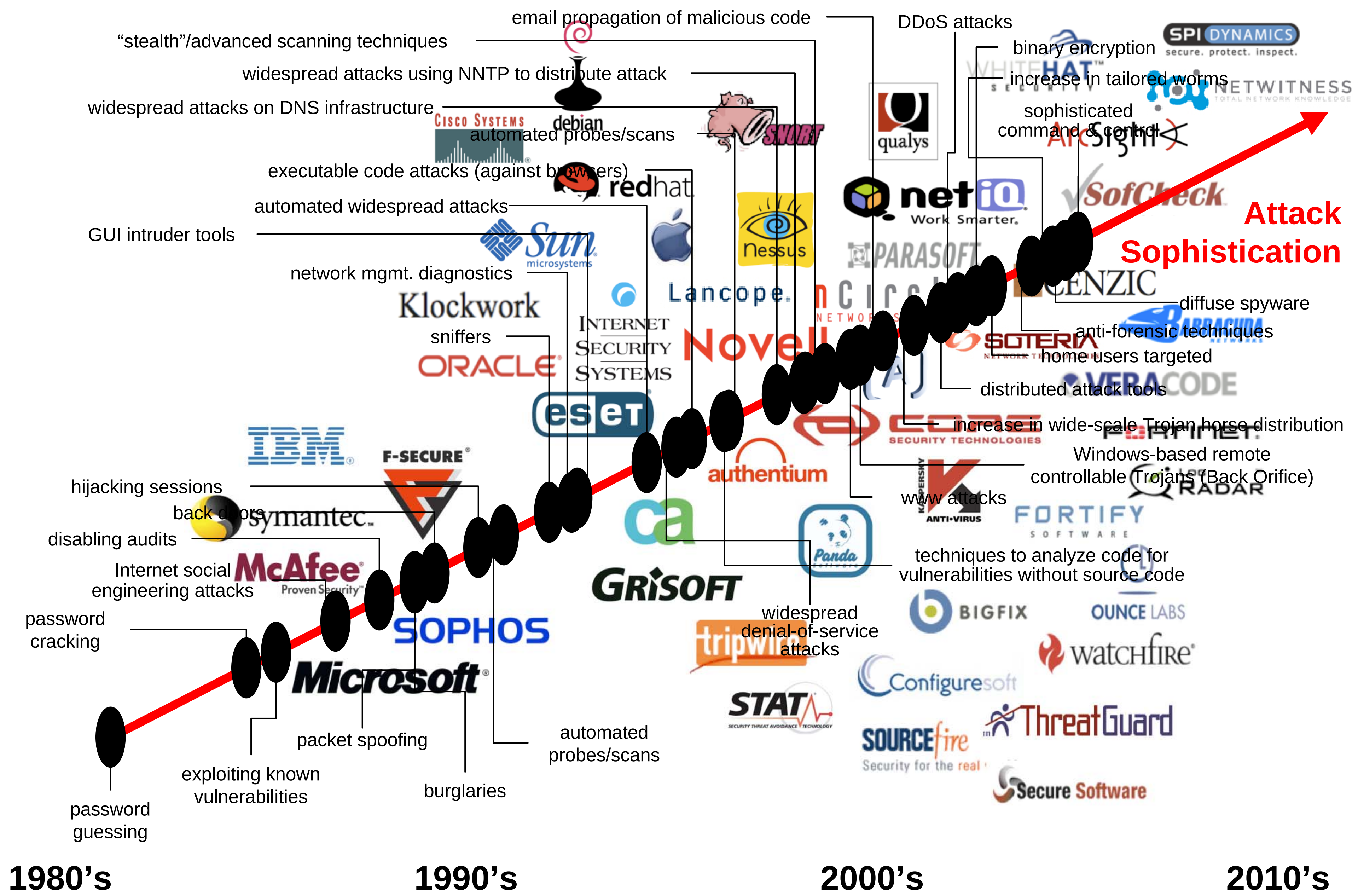
1980’s

1990’s

2000’s

2010’s

Solutions Also Emerged Over Time



password guessing

password cracking

exploiting known vulnerabilities

disabling audits

back doors

hijacking sessions

Internet social engineering attacks

packet spoofing

burglaries

automated probes/scans

sniffers

network mgmt. diagnostics

GUI intruder tools

automated widespread attacks

executable code attacks (against browsers)

automated probes/scans

widespread attacks on DNS infrastructure

widespread attacks using NNTP to distribute attack

“stealth”/advanced scanning techniques

email propagation of malicious code

DDoS attacks

widespread denial-of-service attacks

techniques to analyze code for vulnerabilities without source code

www attacks

Windows-based remote controllable Trojans (Back Orifice)

increase in wide-scale Trojan horse distribution

distributed attack tools

home users targeted

anti-forensic techniques

diffuse spyware

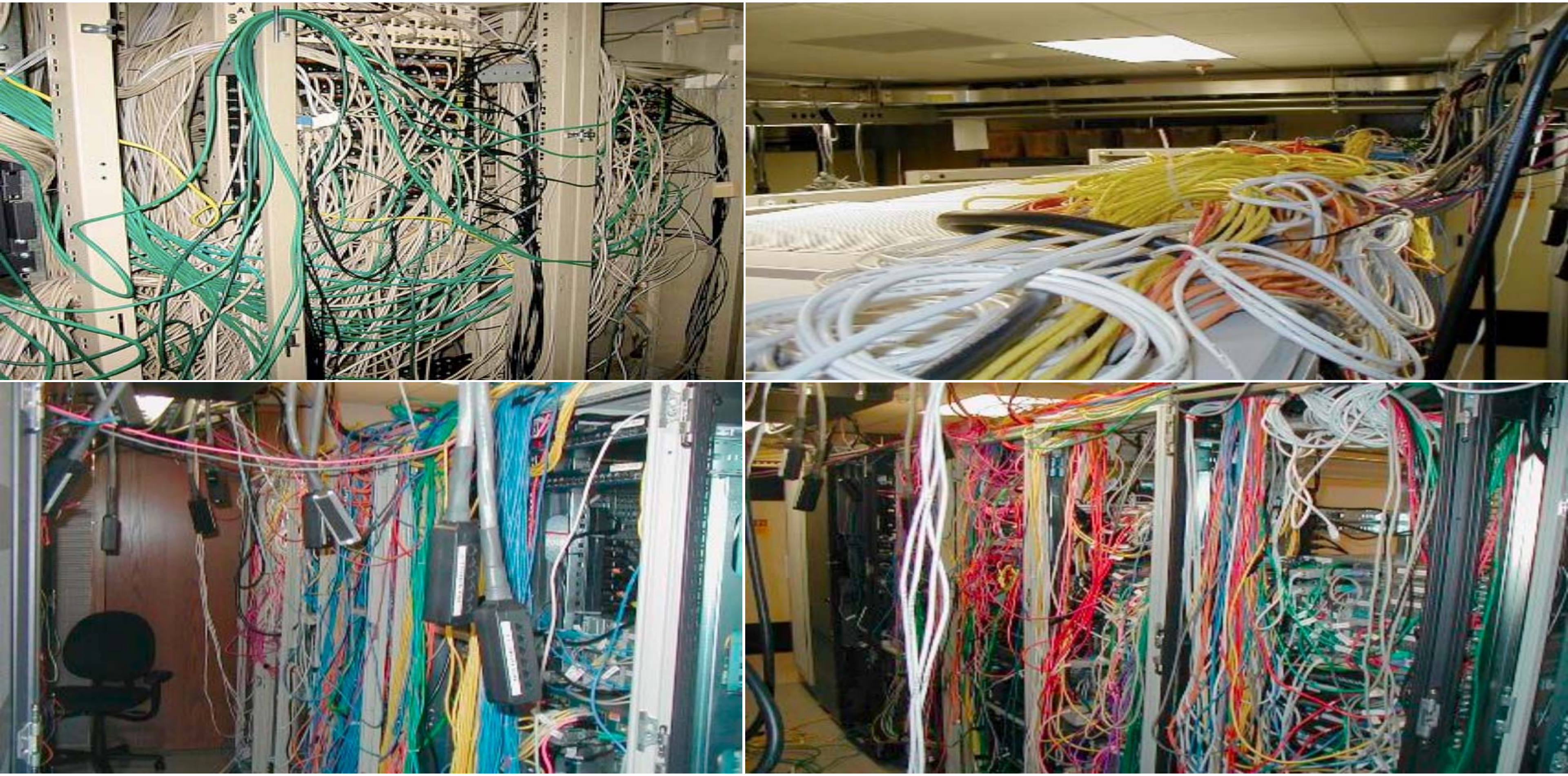
sophisticated command & control

increase in tailored worms

binary encryption

Attack Sophistication

Like Security - Networks Evolved



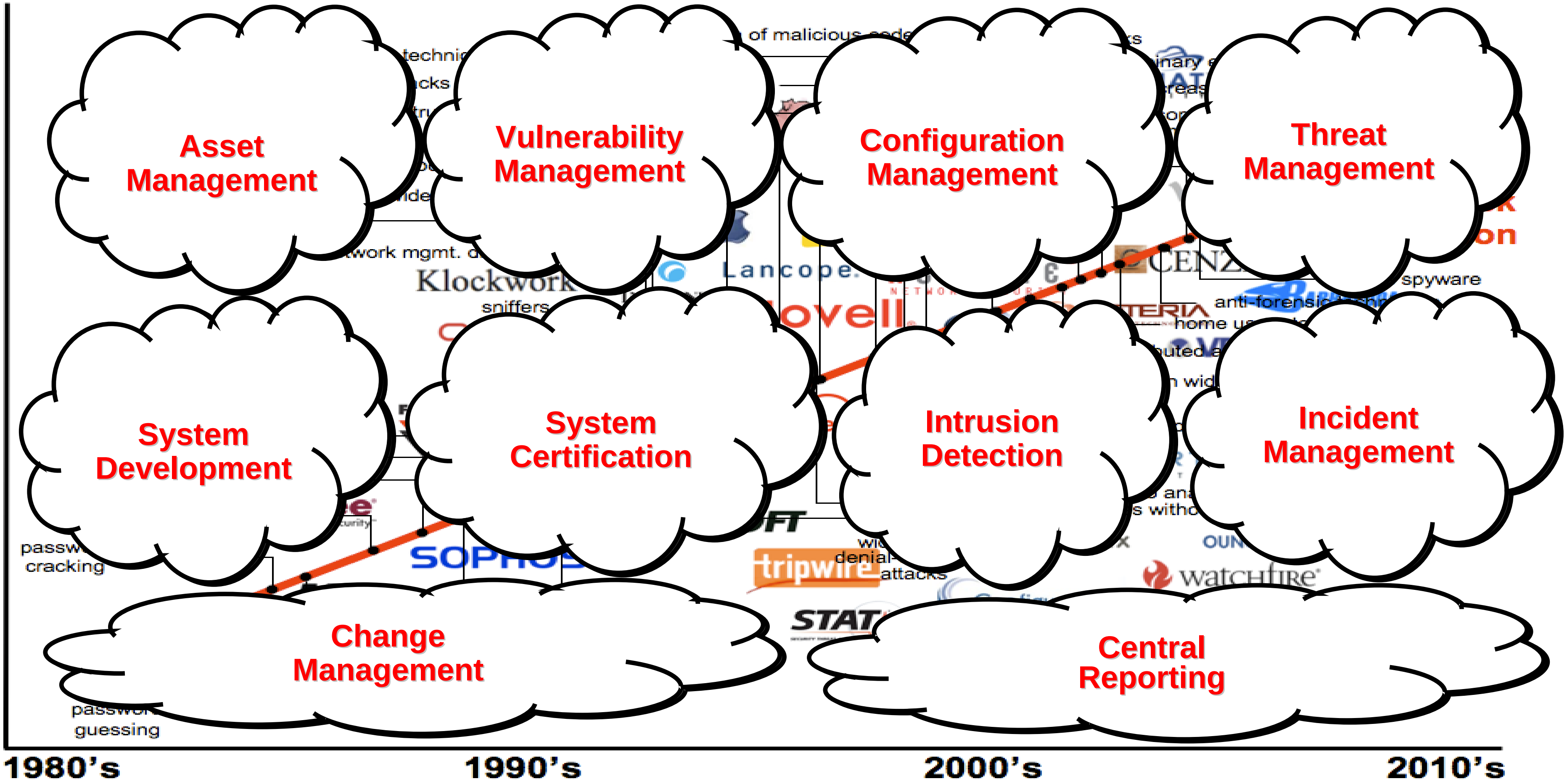
Each new solution had to integrate with the existing solutions -

->> every enterprise ends up learning as they go and has a “unique” tapestry of solutions with “local practices”

But A More Supportable Solution Is Possible with Standardized Approaches and the application of Architecting Principles

Making Security Measurable

Architecting Security with Information Standards for COIs



Asset Management

Vulnerability Management

Configuration Management

Threat Management

System Development

System Certification

Intrusion Detection

Incident Management

Change Management

Central Reporting

Making Security Measurable

What Do The Informational 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

The Building Blocks Are:

- Enumerations
  - **Catalog the fundamental entities in IA, Cyber Security, and Software Assurance**
    - **Vulnerabilities (CVE), configuration issues (CCE), software packages (CPE), 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), config risk (CCSS), weakness risk (CWSS), 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)**

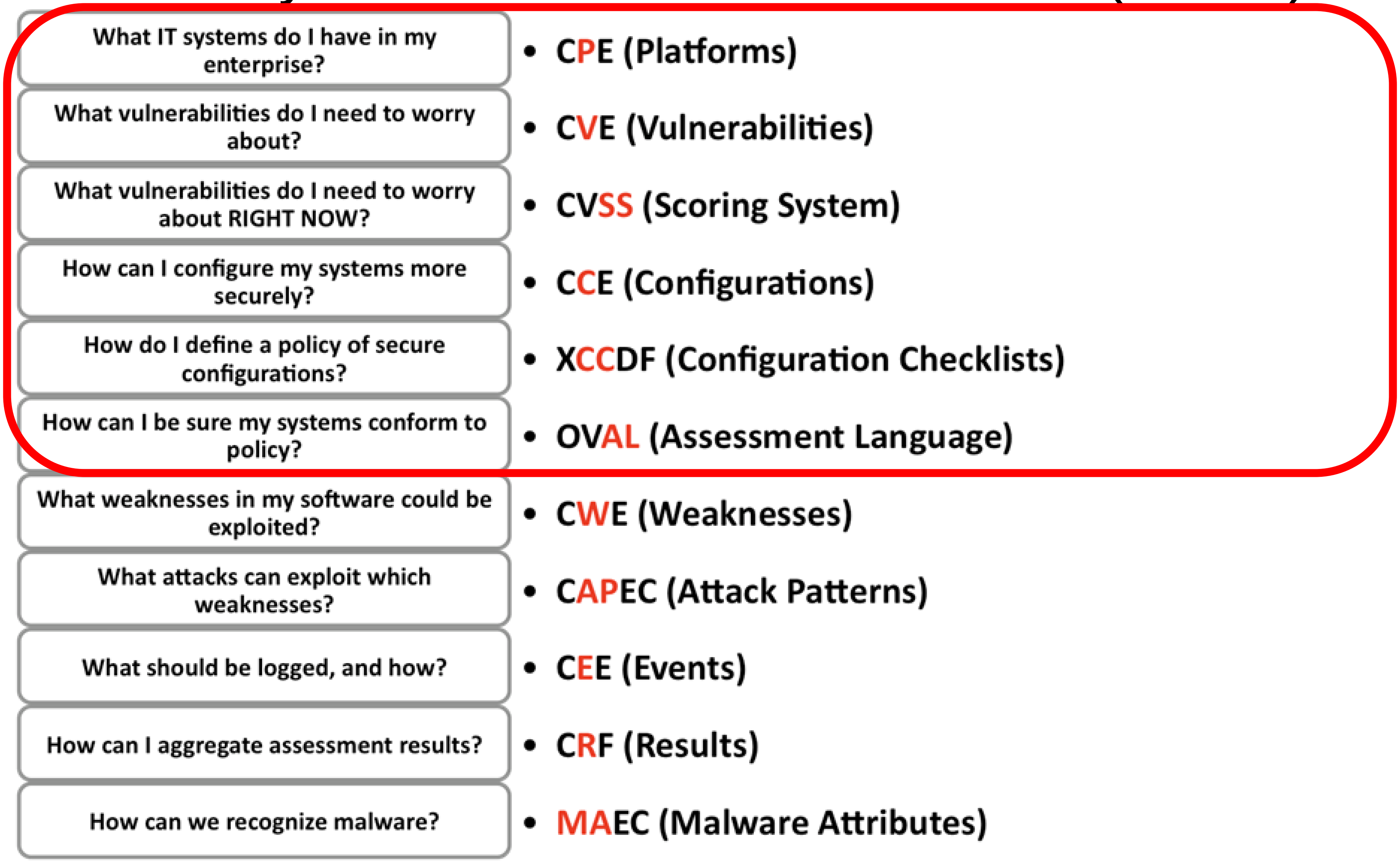
Tools

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

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)
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?	• CRF (Results)
How can we recognize malware?	• MAEC (Malware Attributes)

Standards included in 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)
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?	• CRF (Results)
How can we recognize malware?	• MAEC (Malware Attributes)

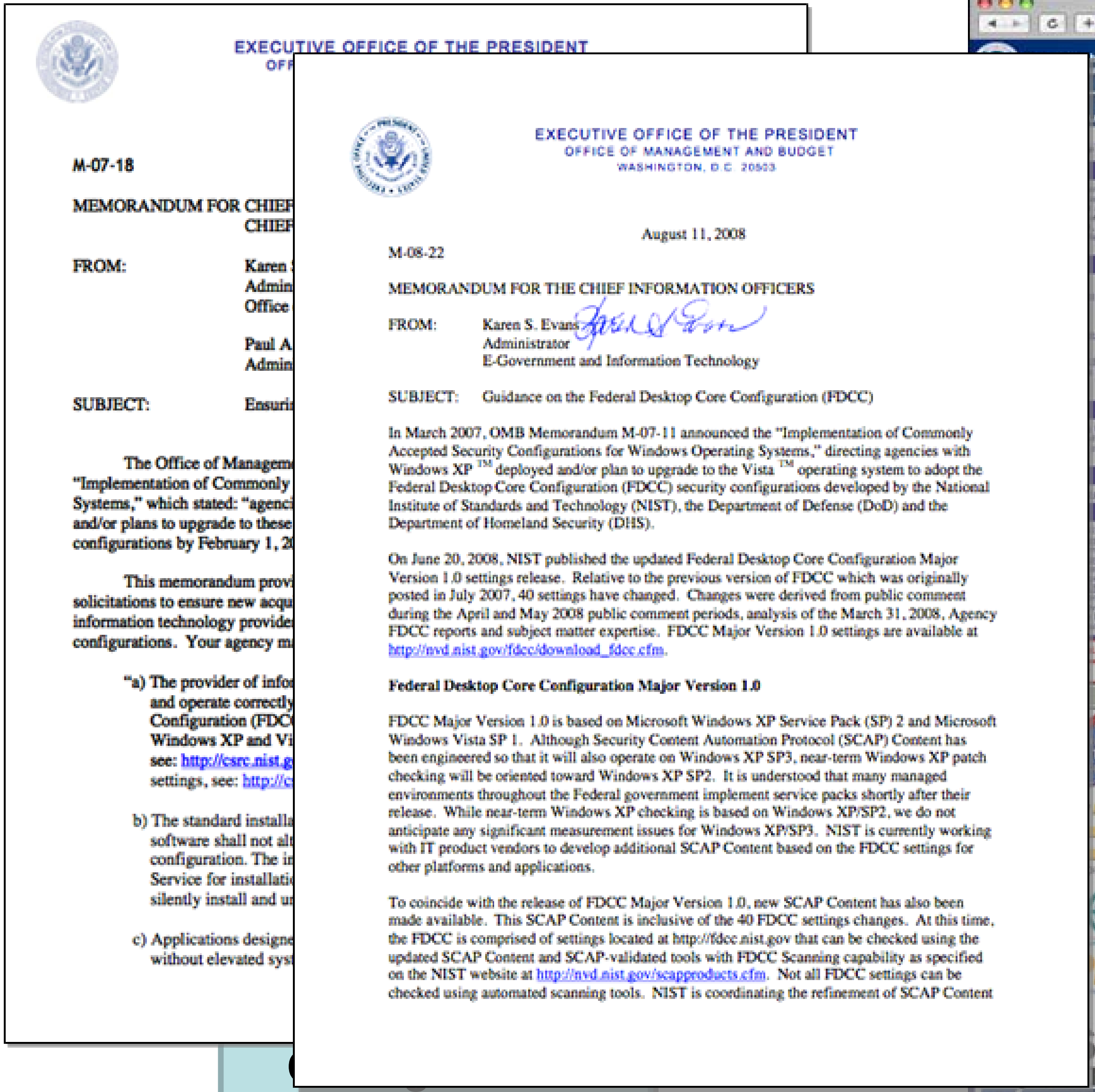
The Building Blocks Are:

- 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) , config risk (CCSS), weakness risk (CWSS), 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**

The Building Blocks Are:



EXECUTIVE OFFICE OF THE PRESIDENT
OFF

M-07-18

MEMORANDUM FOR CHIEF
CHIEF

FROM: Karen
Admin
Office

Paul A
Admin

SUBJECT: Ensuri

The Office of Managem
"Implementation of Commonly
Systems," which stated: "agenci
and/or plans to upgrade to these
configurations by February 1, 2

This memorandum provi
solicitations to ensure new acqu
information technology provide
configurations. Your agency m

"a) The provider of infor
and operate correctly
Configuration (FDC
Windows XP and Vi
see: http://csrc.nist.g
settings, see: http://c

b) The standard installa
software shall not alt
configuration. The in
Service for installatio
silently install and un

c) Applications designe
without elevated syst

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.

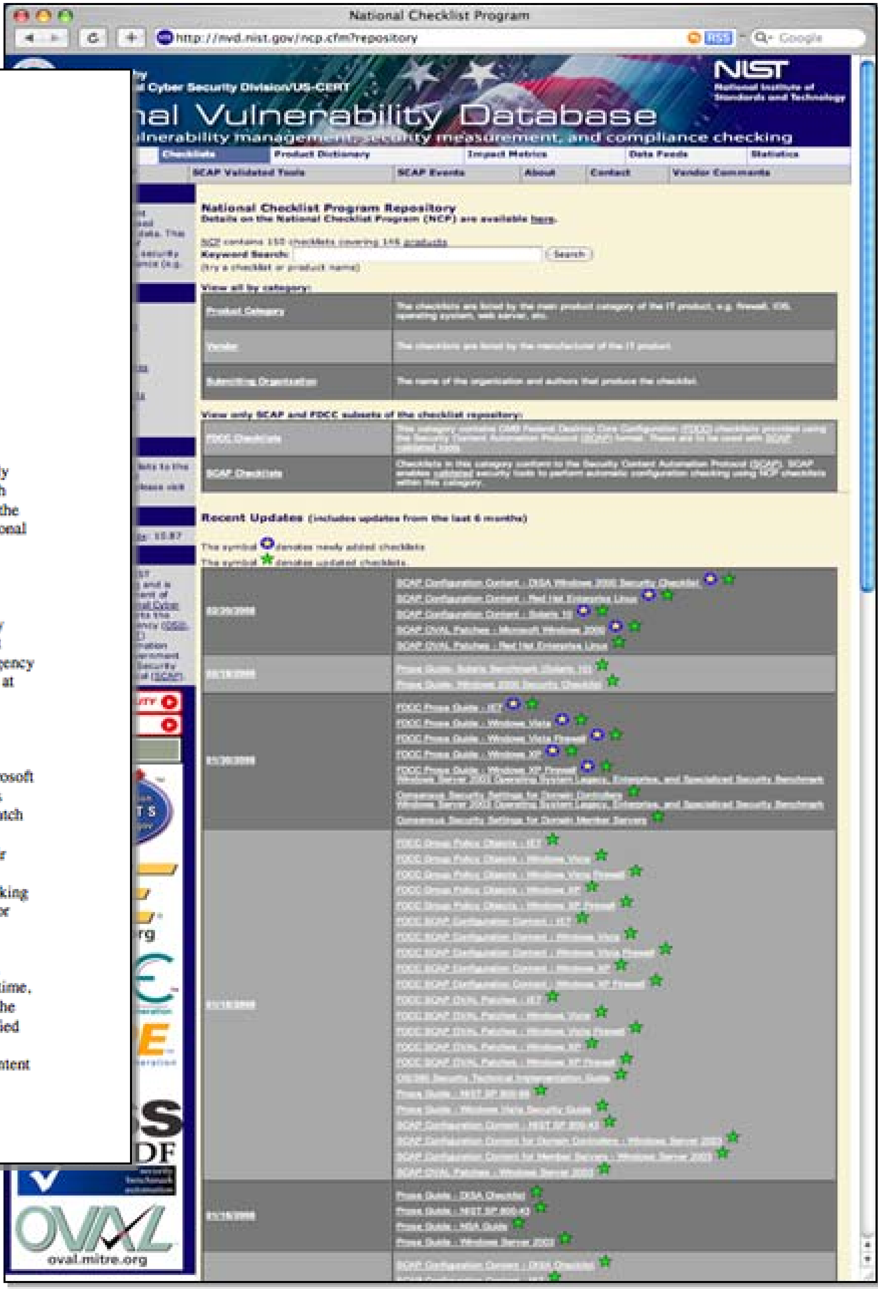
Federal Desktop Core Configuration Major Version 1.0

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

Guidance

Knowledge Repository



National Checklist Program

http://nvd.nist.gov/ncp.cfm?repository

al Cyber Security Division/US-CERT

nal Vulnerability Database

ulnerability management, security measurement, and compliance checking

NIST National Institute of Standards and Technology

Checklists | Product Dictionary | Impact Metrics | Data Feeds | Statistics

SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

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:

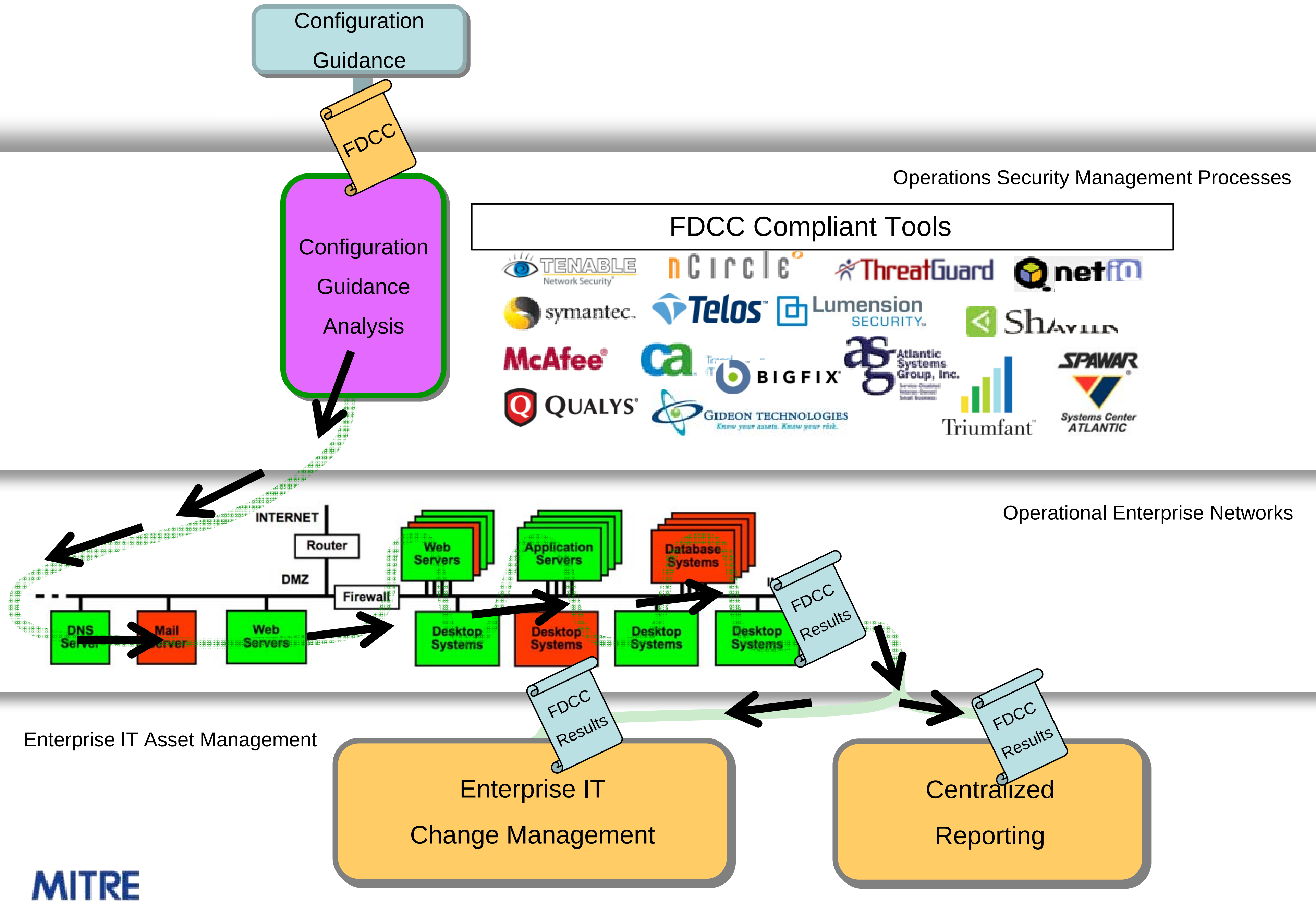
FDCC Checklists	This category contains OMB Federal Desktop Core Configuration (FDCC) checklists provided using the Security Content Automation Protocol (SCAP) format. These are to be used with SCAP validated tools.
SCAP Checklists	Checklists in this category conform to the Security Content Automation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

[illegible]	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 ★
[illegible]	Prose Guide - Solaris Benchmark (Solaris 10) ★ Prose Guide - Windows 2000 Security Checklist ★
[illegible]	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 ★
[illegible]	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 ★ DISA IIS 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 ★
[illegible]	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-Based FDCC Guidance



Configuration Guidance

Operations Security Management Processes

Configuration Guidance Analysis

FDCC Compliant Tools

Operational Enterprise Networks

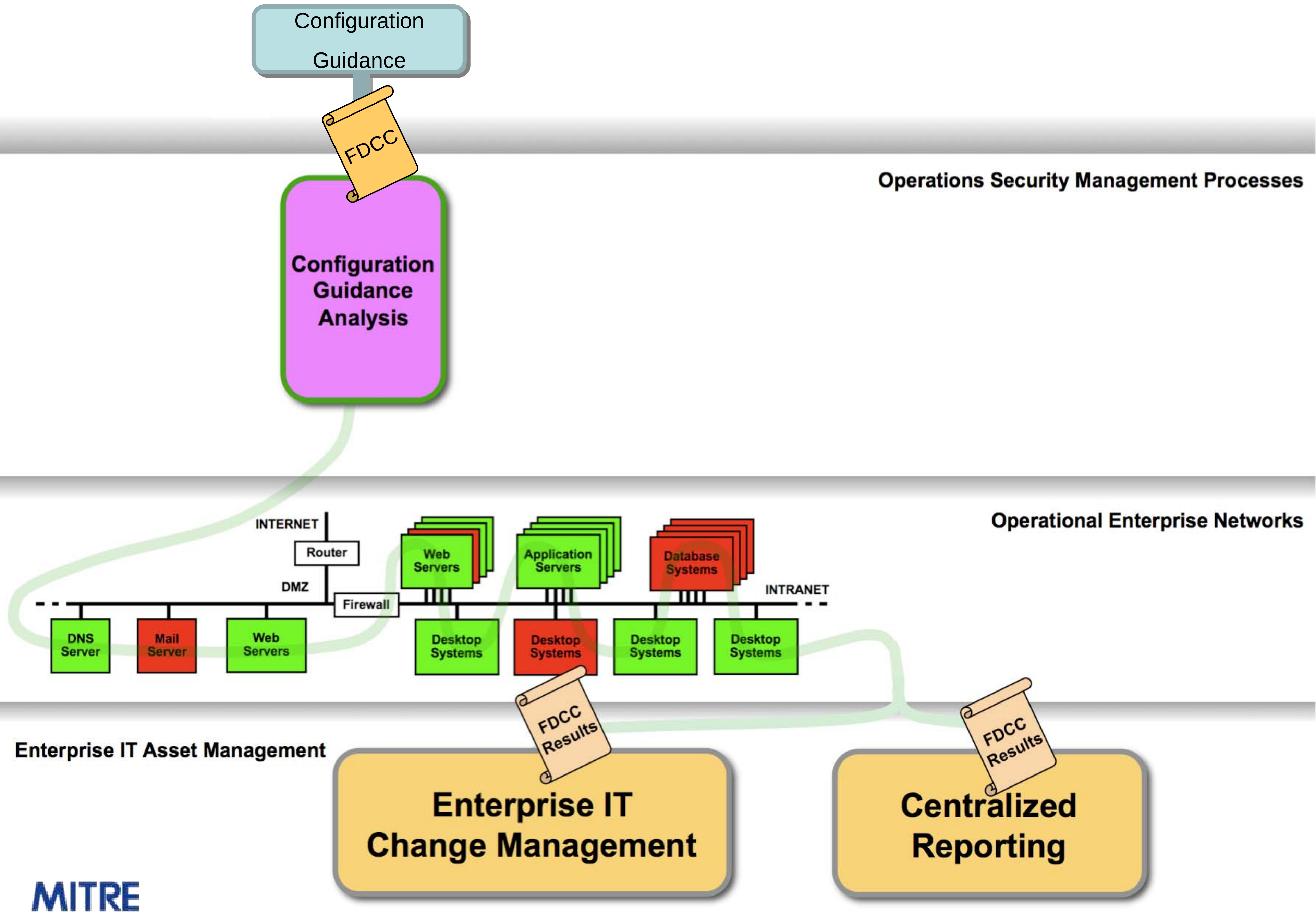
Enterprise IT Asset Management

Enterprise IT Change Management

Centralized Reporting

Knowledge Repositories

SCAP-Based FDCC Reporting



Configuration Guidance

FDCC

Operations Security Management Processes

Configuration Guidance Analysis

Operational Enterprise Networks

FDCC Results

FDCC Results

Enterprise IT Asset Management

Enterprise IT Change Management

Centralized Reporting

Sent: Wednesday, May 27, 2009 2:43 PM

Subject: Cyberspace Operations Culture Change

•
•
•

I have signed a directive memo making an unequivocal statement about the importance of compliance with network related technical orders. This guidance will improve safety and efficiency on the AF-GIG and provide commanders a clear enforcement/disciplinary mechanism. MTOs, NTOs, and CCOs issued by the AFNETOPS/CC now have the same authority as aircraft maintenance technical orders and lawful general orders.

•
•
•

This change is not easy, but compliance enables us to defend our networks - paramount in the face of increasing threats. Networks are a shared resource and a risk assumed by one is a risk exposed to all. Our Air Force must move to a system of tight network control, personal responsibility, and accountability as we execute our global mission on behalf of our Nation.

NORTON A. SCHWARTZ
General, USAF
Chief of Staff

The Building Blocks Are:

- Enumerations
  - **Catalog the fundamental entities in IA, Cyber Security, and Software Assurance**
    - **Vulnerabilities (CVE), configuration issues (CCE), software packages (CPE), 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), config risk (CCSS), weakness risk (CWSS), 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**

The Building Blocks Are:

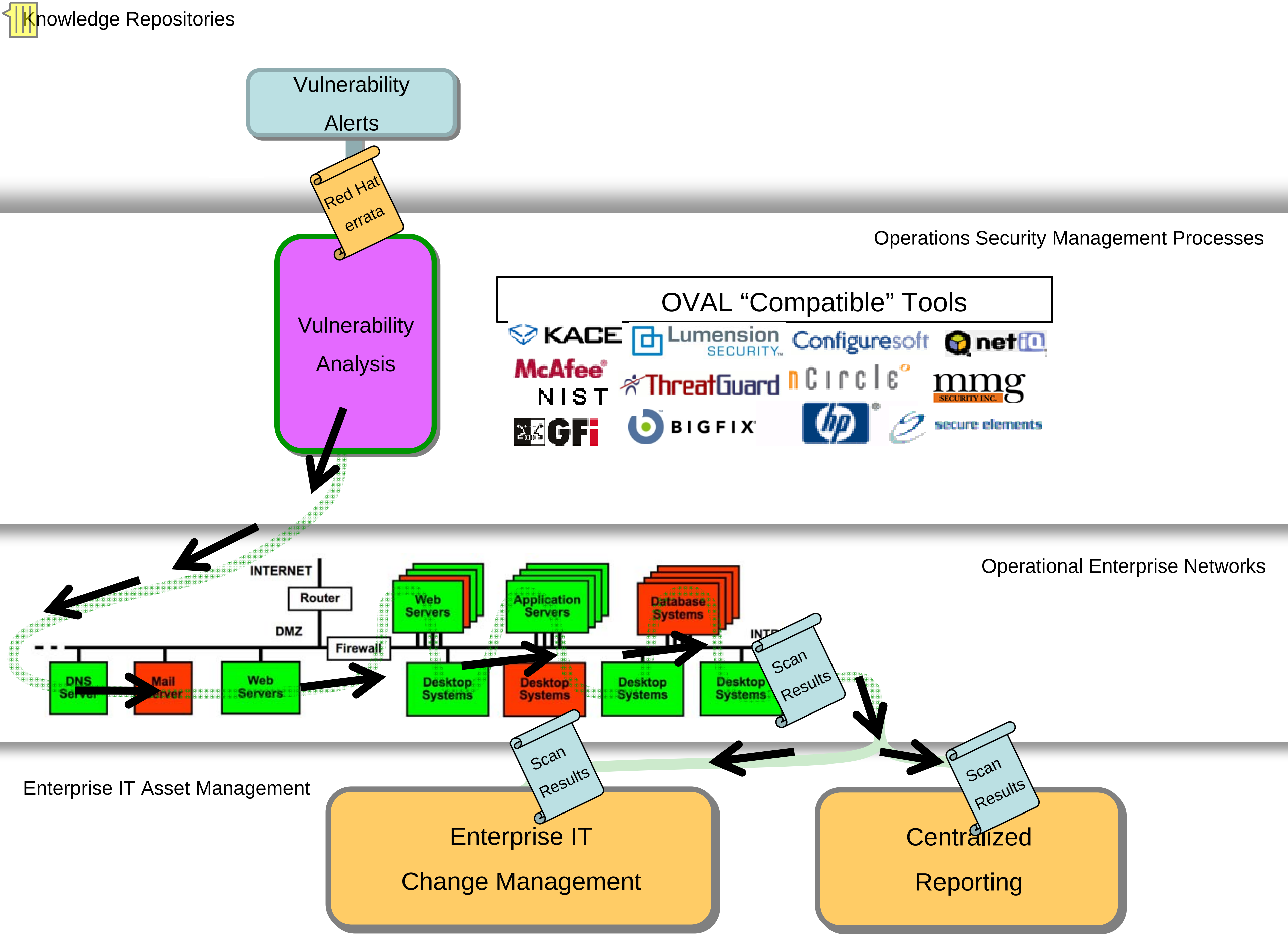
CVE

OVAL

NIST/DHS NVD

Vulnerability
Alerts

Knowledge Repository



Knowledge Repositories

Vulnerability Alerts

Red Hat errata

Operations Security Management Processes

Vulnerability Analysis

OVAL “Compatible” Tools

Operational Enterprise Networks

Enterprise IT Asset Management

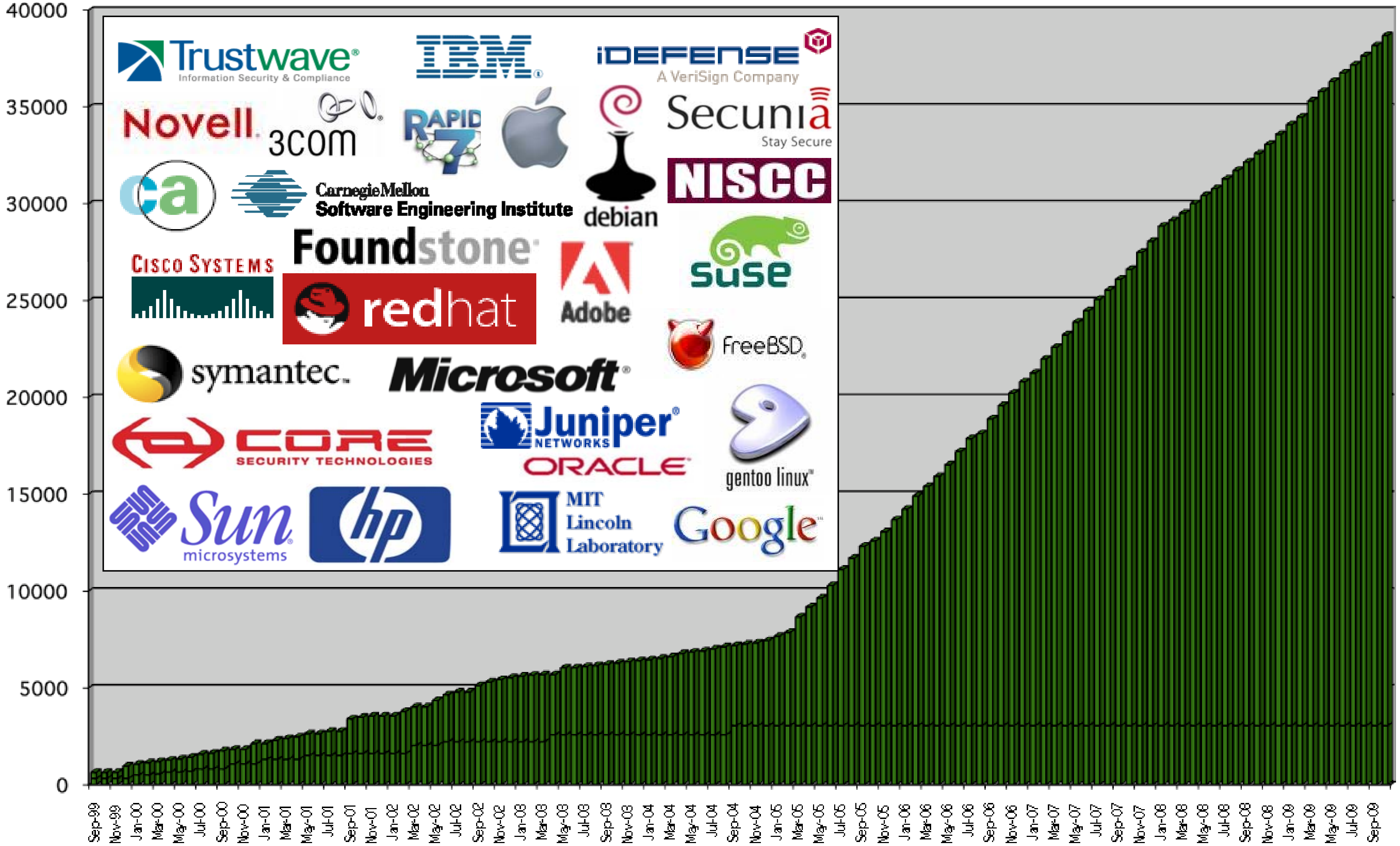
Scan Results

Enterprise IT Change Management

Scan Results

Centralized Reporting

CVE 1999 to 2009



CVE is Widely Used & Available
38,921 and climbing…

Arabic

Bulgarian

Catalan

Chinese

Croatian

Czech

Danish

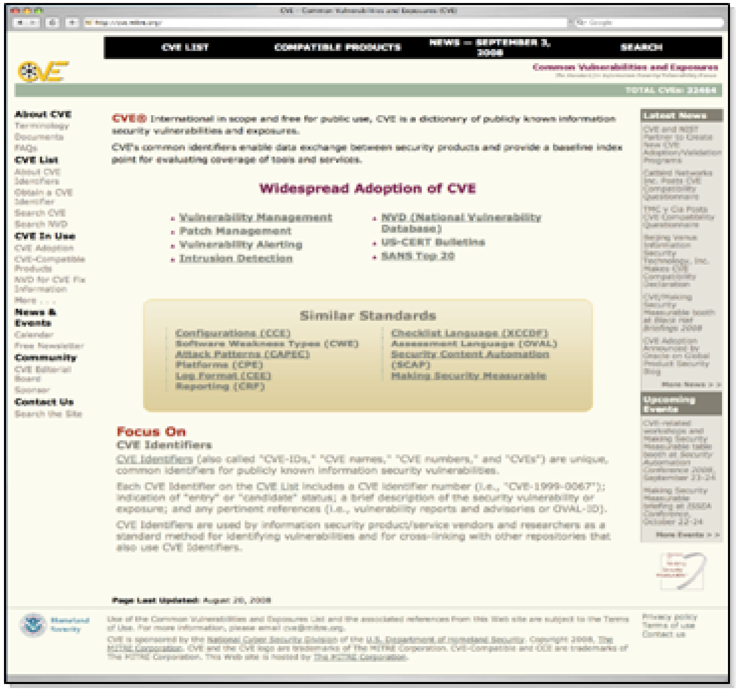
Dutch

Estonian

Finnish

French

German



CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures.

CVE's common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.

Widespread Adoption of CVE

- Vulnerability Management
- Patch Management
- Vulnerability Alerting
- Intrusion Detection
- NVD (National Vulnerability Database)
- US-CERT Bulletins
- SANS Top 20

Similar Standards

Configurations (CCE)
Software Weakness Types (CWE)
Attack Patterns (CAPEC)
Platforms (CPE)
Log Format (CEE)
Reporting (CRF)
Checklist Language (XCCDF)
Assessment Language (OVAL)
Security Content Automation (SCAP)
Making Security Measurable

Focus On
CVE Identifiers

CVE Identifiers (also called "CVE-IDs," "CVE names," "CVE numbers," and "CVEs") are unique, common identifiers for publicly known information security vulnerabilities.

Each CVE Identifier on the CVE List includes a CVE identifier number (i.e., "CVE-1999-0067"); indication of "entry" or "candidate" status; a brief description of the security vulnerability or exposure; and any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID).

CVE Identifiers are used by information security product/service vendors and researchers as a standard method for identifying vulnerabilities and for cross-linking with other repositories that also use CVE Identifiers.

Page Last Updated: August 20, 2008

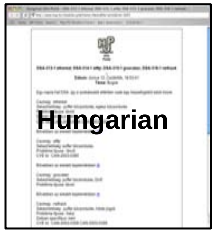
Use of the Common Vulnerabilities and Exposures List and the associated references from this Web site are subject to the Terms of Use. For more information, please email cve@mitre.org.

CVE is sponsored by the National Cyber Security Division of the U.S. Department of Homeland Security. Copyright 2008, The MITRE Corporation. CVE and the CVE logo are trademarks of The MITRE Corporation. CVE-Compatible and OCE are trademarks of The MITRE Corporation. This Web site is hosted by The MITRE Corporation.

Privacy policy
Terms of use
Contact us

Greek

Hebrew


Hungarian

Icelandic

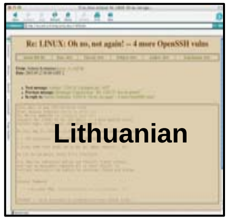
Indonesian

Italian

Japanese

Korean

Latvian


Re: LINUX: Oh no, not again! -- 4 more OpenSSH vulns

Lithuanian

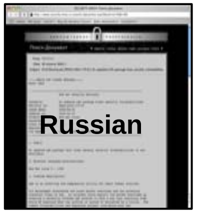
Norwegian

Polish

Dicionário CVE já possui mais de 2 mil registros

Portuguese

Romanian


Russian

Serbian

Slovak

Slovenian

Spanish

Swedish

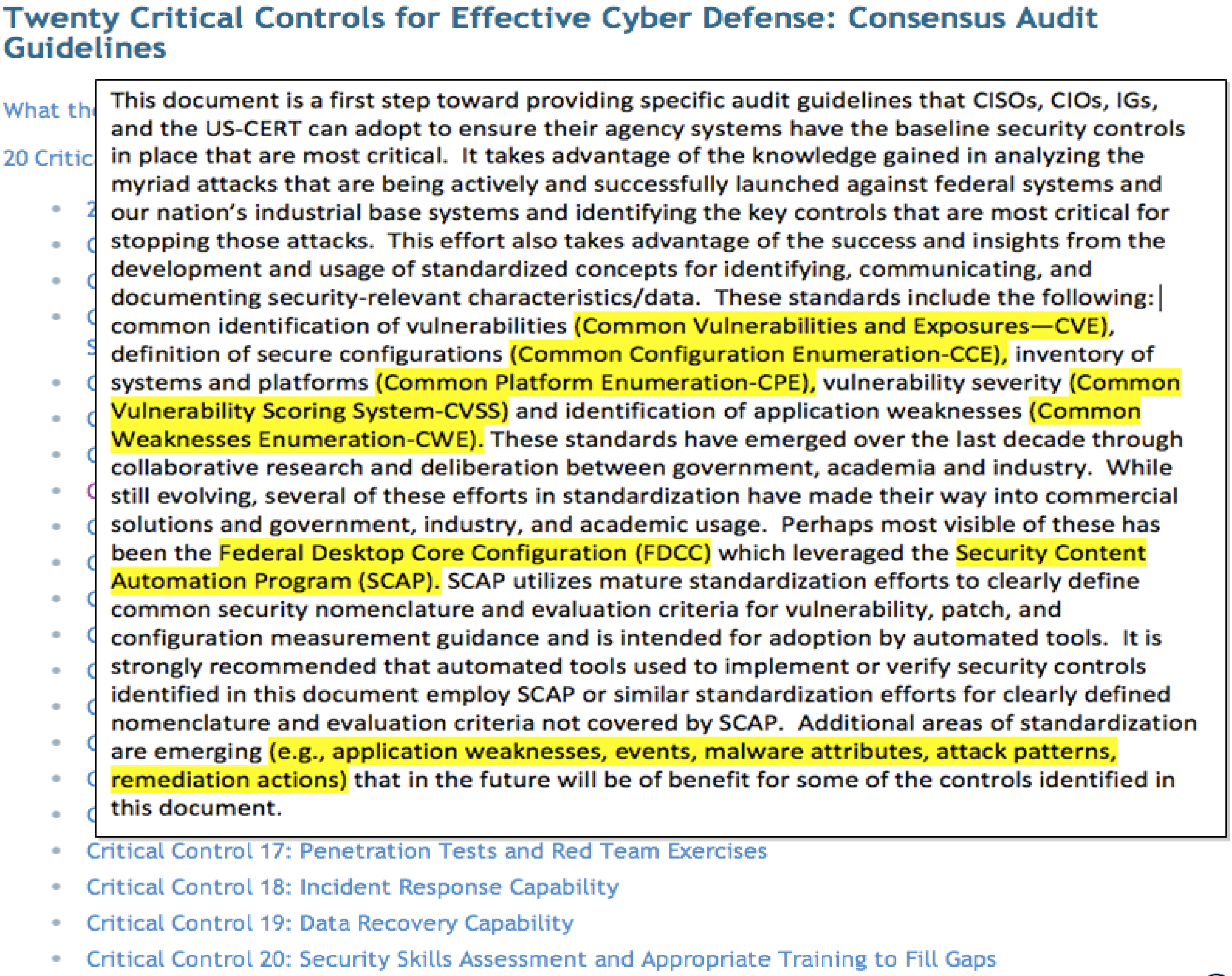
Turkish

CVE Vendor/Industry Penetration

Avocent
LANDesk
Trustwave
Information Security & Compliance
CertIST
GFI
Archer technologies
assuria
www.assuria.com
New paradigm
ZOHO
CERIAS
SecureInfo
THE INFORMATION ASSURANCE EXPERTS
skybox security
Soft Run
ca
Carnegie Mellon Software Engineering Institute
McAfee
netForensics
NSFOCUS
NIST
PATCHLINK
天融信 TOPSEC
ENTERASYS NETWORKS
Cisco Systems
redhat
APPLICATION SECURITY, INC.
KINGNET SECURITY INC.
Foundstone STRATEGIC SECURITY
SecurityReason
Our Reason is Security
TREND MICRO
SAINT
ArcSight
SANS INSTITUTE
SNORT
DragonSoft
www.dragonsoft.com
HARRIS
INTERNET SECURITY SYSTEMS
IBM
TENABLE Network Security
Intellitactics
symantec.
Critical Watch
Visibility . Measurability . Control
NETCRAFT
Nessus
netIQ
Work Smarter.
nCircle NETWORK SECURITY
(주)나일소프트
NileSOFT Ltd.
LOG RADAR
BlueLane
SECURITY DATABASE
KEEP A VIGILANT EYE ON YOUR DEFENSES
NETCLARITY
PREEMPTIVE, PROACTIVE PROTECTION
Beyond Security
榕基软件
RONGJI
im InformationRiskManagement
RUS CERT

252 PRODUCTS AND SERVICES FROM 142 ORGANIZATIONS IN 25 COUNTRIES

The Consensus Audit Guidelines – Aimed at Auditable Items



Twenty Critical Controls for Effective Cyber Defense: Consensus Audit Guidelines

What th

20 Critic

This document is a first step toward providing specific audit guidelines that CISOs, CIOs, IGs, and the US-CERT can adopt to ensure their agency systems have the baseline security controls in place that are most critical. It takes advantage of the knowledge gained in analyzing the myriad attacks that are being actively and successfully launched against federal systems and our nation's industrial base systems and identifying the key controls that are most critical for stopping those attacks. This effort also takes advantage of the success and insights from the development and usage of standardized concepts for identifying, communicating, and documenting security-relevant characteristics/data. These standards include the following: common identification of vulnerabilities (Common Vulnerabilities and Exposures—CVE), definition of secure configurations (Common Configuration Enumeration-CCE), inventory of systems and platforms (Common Platform Enumeration-CPE), vulnerability severity (Common Vulnerability Scoring System-CVSS) and identification of application weaknesses (Common Weaknesses Enumeration-CWE). These standards have emerged over the last decade through collaborative research and deliberation between government, academia and industry. While still evolving, several of these efforts in standardization have made their way into commercial solutions and government, industry, and academic usage. Perhaps most visible of these has been the Federal Desktop Core Configuration (FDCC) which leveraged the Security Content Automation Program (SCAP). SCAP utilizes mature standardization efforts to clearly define common security nomenclature and evaluation criteria for vulnerability, patch, and configuration measurement guidance and is intended for adoption by automated tools. It is strongly recommended that automated tools used to implement or verify security controls identified in this document employ SCAP or similar standardization efforts for clearly defined nomenclature and evaluation criteria not covered by SCAP. Additional areas of standardization are emerging (e.g., application weaknesses, events, malware attributes, attack patterns, remediation actions) that in the future will be of benefit for some of the controls identified in this document.

- Critical Control 17: Penetration Tests and Red Team Exercises
- Critical Control 18: Incident Response Capability
- Critical Control 19: Data Recovery Capability
- Critical Control 20: Security Skills Assessment and Appropriate Training to Fill Gaps

The Building Blocks Are:

- Enumerations
  - **Catalog the fundamental entities in IA, Cyber Security, and Software Assurance**
    - **Vulnerabilities (CVE), configuration issues (CCE), software packages (CPE), 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), config risk (CCSS), weakness risk (CWSS), 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**

The Building Blocks Are:

CCE

CPE

CAPEC

CV

XCCDF & OVAL

CRF

SB

MAEC

SS

CCSS

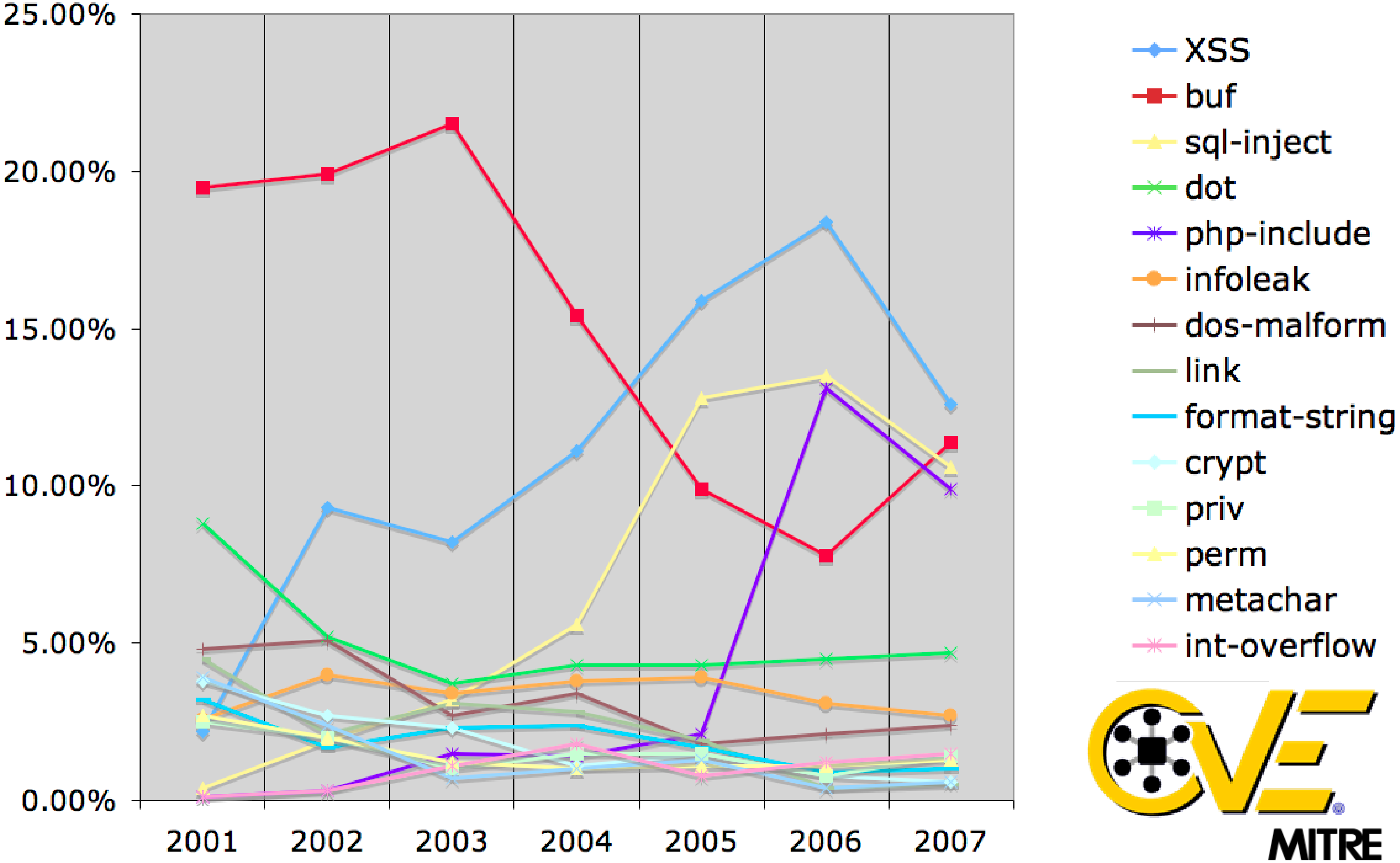
CWSS

DoD DIACAP & eMASS

e-MASS

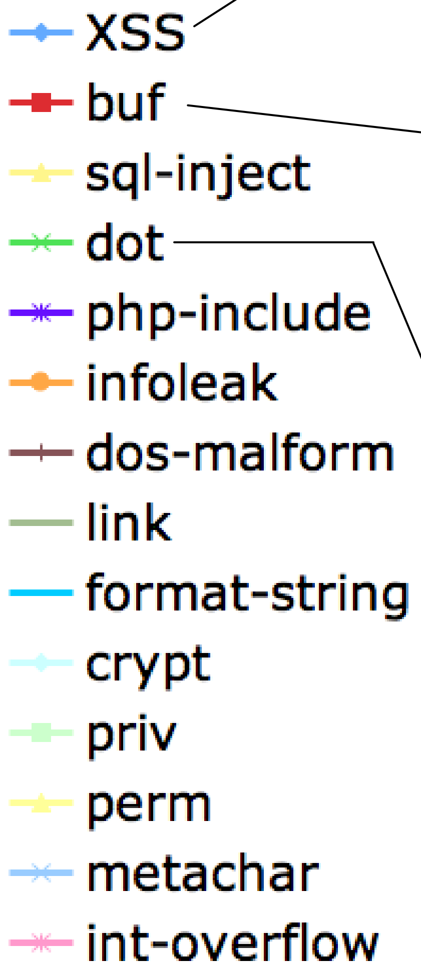
Knowledge Repository

Vulnerability Type Trends: A Look at the CVE List (2001 - 2007)



MITRE

Removing and Preventing the Vulnerabilities Requires More Specific Definitions…CWEs



Failure to Sanitize Directives in a Web Page (aka 'Cross-site scripting' (XSS)) (79)

- Failure to Sanitize Script-Related HTML Tags in a Web Page (Basic XSS) (80)
- Failure to Sanitize Directives in an Error Message Web Page (81)
- Failure to Sanitize Script in Attributes of IMG Tags in a Web Page (82)
- Failure to Sanitize Script in Attributes in a Web Page (83)
- Failure to Resolve Encoded URI Schemes in a Web Page (84)
- Doubled Character XSS Manipulations (85)
- Invalid Characters in Identifiers (86)
- Alternate XSS syntax (87)

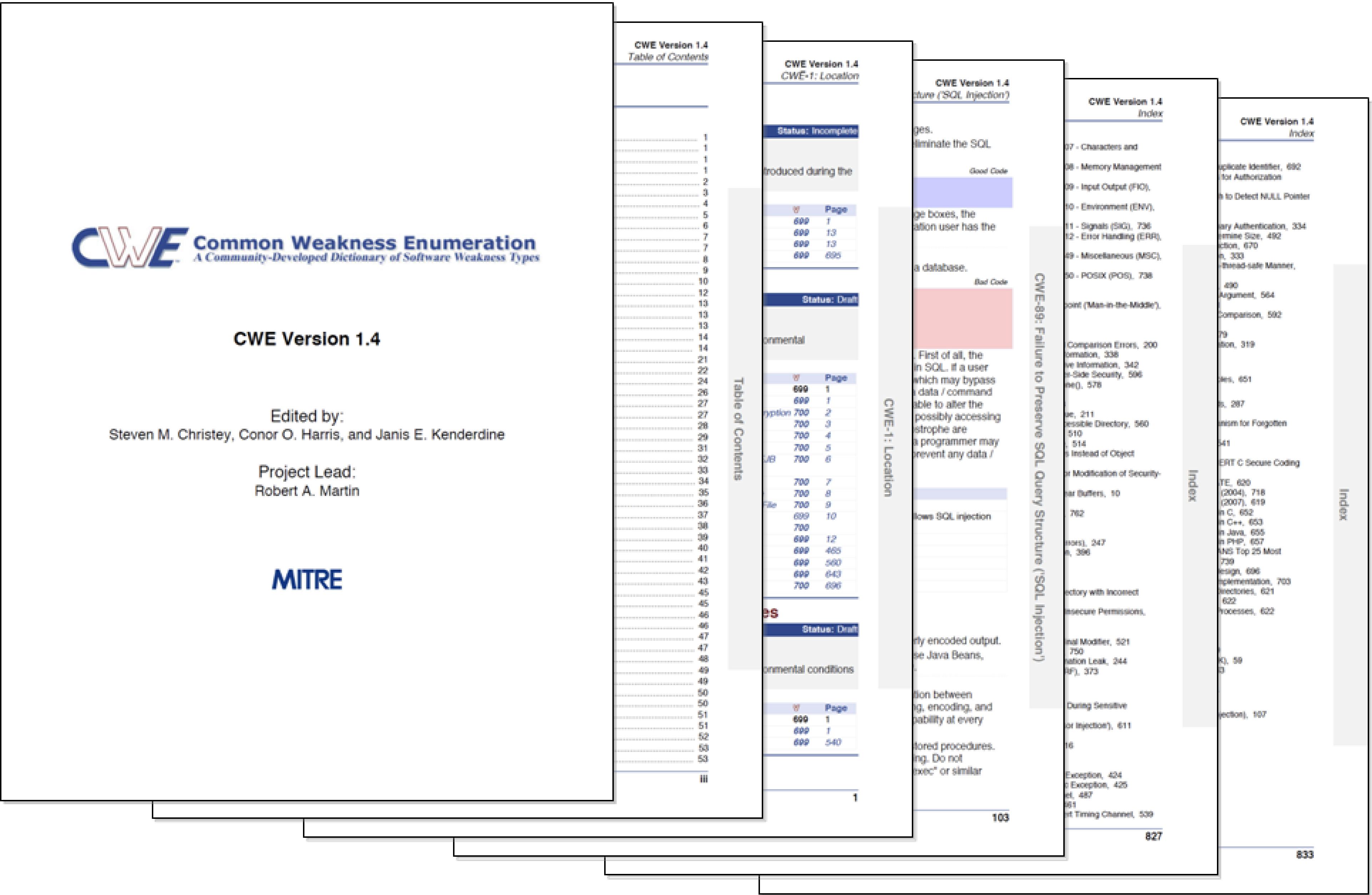
Failure to Constrain Operations within the Bounds of an Allocated Memory Buffer (119)

- Unbounded Transfer (‘Classic Buffer Overflow’) (120)
- Write-what-where Condition (123)
- Boundary Beginning Violation (’Buffer Underwrite') (124)
- Out-of-bounds Read (125)
- Wrap-around Error (128)
- Unchecked Array Indexing (129)
- Incorrect Calculation of Buffer Size (131)
- Miscalculated Null Termination (132)
- Return of Pointer Value Outside of Expected Range (466)

Path Traversal (22)

- Relative Path Traversal (23)
  - Path Traversal: '\..\filename' (29)
  - Path Traversal: '\dir\..\filename' (30)
  - Path Traversal: 'dir\..\filename' (31)
  - Path Traversal: '...' (Triple Dot) (32)
  - Path Traversal: '....' (Multiple Dot) (33)
  - Path Traversal: '....//' (34)
  - Path Traversal: '.../...//' (35)
- Absolute Path Traversal (36)
  - Path Traversal: '/absolute/pathname/here’ (37)
  - Path Traversal: '\absolute\pathname\here’ (38)
  - Path Traversal: 'C:dirname’ (39)
  - Path Traversal: '\\UNC\share\name\' (Windows UNC Share) (40)

Printable PDFs of Entire CWE Available



CWE Common Weakness Enumeration
A Community-Developed Dictionary of Software Weakness Types

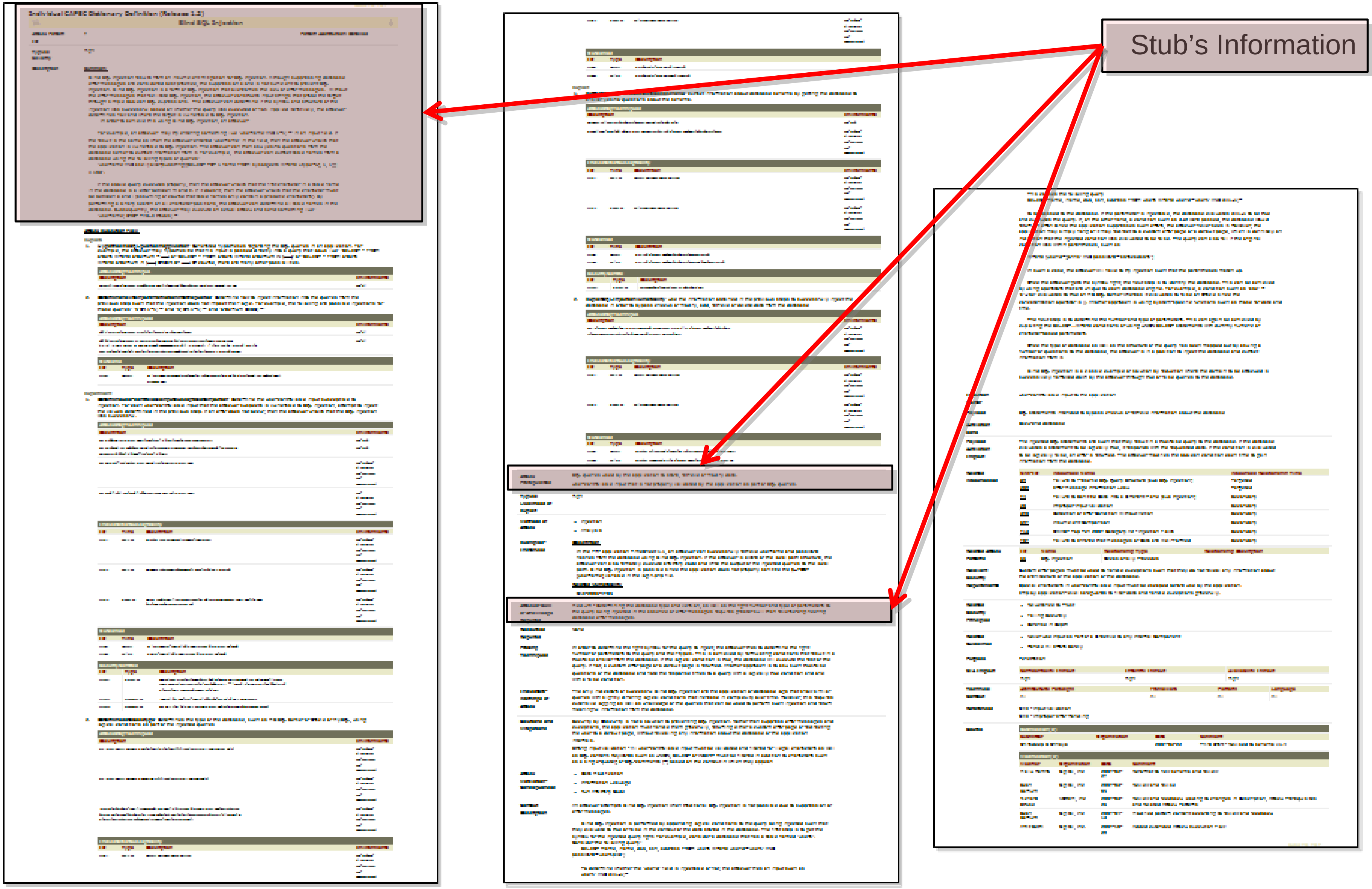
CWE Version 1.4

Edited by:
Steven M. Christey, Conor O. Harris, and Janis E. Kenderdine

Project Lead:
Robert A. Martin

MITRE

Complete CAPEC Entry Information



Individual CAPEC Dictionary Definition (Release 1.2)

Blind SQL Injection

Stub's Information

Individual CAPEC Dictionary Definition (Release 1.2)

Blind SQL Injection

Attack Pattern ID 7 **Pattern Abstraction: Detailed**

Typical Severity High

Description

Summary

Blind SQL Injection results from an insufficient mitigation for SQL Injection. Although suppressing database error messages are considered best practice, the suppression alone is not sufficient to prevent SQL Injection. Blind SQL Injection is a form of SQL Injection that overcomes the lack of error messages. Without the error messages that facilitate SQL Injection, the attacker constructs input strings that probe the target through simple Boolean SQL expressions. The attacker can determine if the syntax and structure of the injection was successful based on whether the query was executed or not. Applied iteratively, the attacker determines how and where the target is vulnerable to SQL Injection.

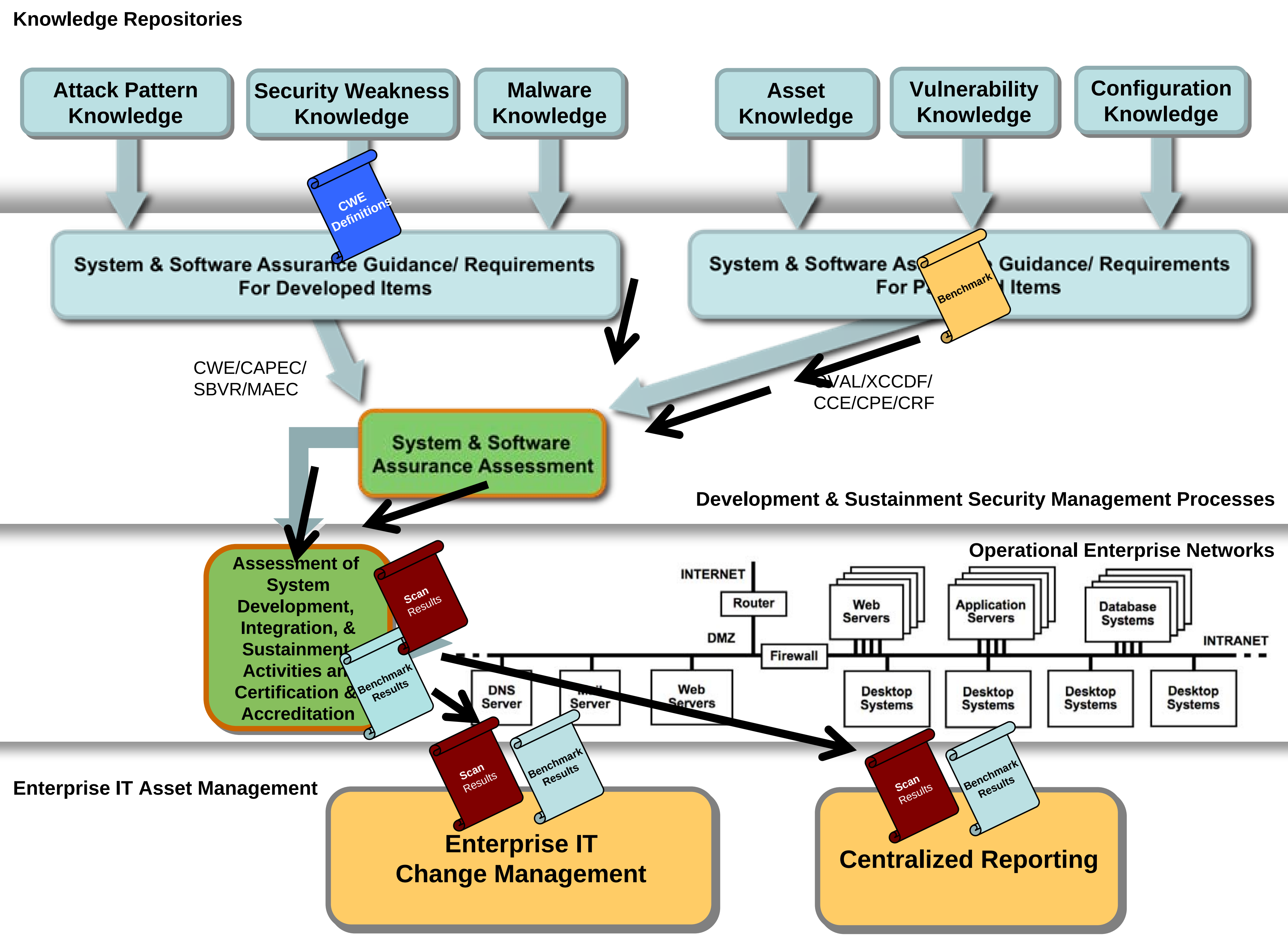
In order to achieve this using Blind SQL Injection, an attacker:

For example, an attacker may try entering something like "username' AND 1=1; --" in an input field. If the result is the same as when the attacker entered "username" in the field, then the attacker knows that the application is vulnerable to SQL Injection. The attacker can then ask yes/no questions from the database server to extract information from it. For example, the attacker can extract table names from a database using the following types of queries:

"username' AND ascii(lower(substring((SELECT TOP 1 name FROM sysobjects WHERE xtype='U'), 1, 1))) > 108".

If the above query executes properly, then the attacker knows that the first character in a table name in the database is a letter between m and z. If it doesn't, then the attacker knows that the character must be between a and l (assuming of course that table names only contain alphabetic characters). By performing a binary search on all character positions, the attacker can determine all table names in the database. Subsequently, the attacker may execute an actual attack and send something like:

"username'; DROP TABLE trades; --



Knowledge Repositories

Attack Pattern Knowledge

Security Weakness Knowledge

Malware Knowledge

Asset Knowledge

Vulnerability Knowledge

Configuration Knowledge

CWE Definitions

System & Software Assurance Guidance/ Requirements For Developed Items

System & Software As Guidance/ Requirements For P Items

Benchmark

CWE/CAPEC/ SBVR/MAEC

OVAL/XCCDF/ CCE/CPE/CRF

System & Software Assurance Assessment

Development & Sustainment Security Management Processes

Operational Enterprise Networks

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

Scan Results

Benchmark Results

Enterprise IT Asset Management

Scan Results

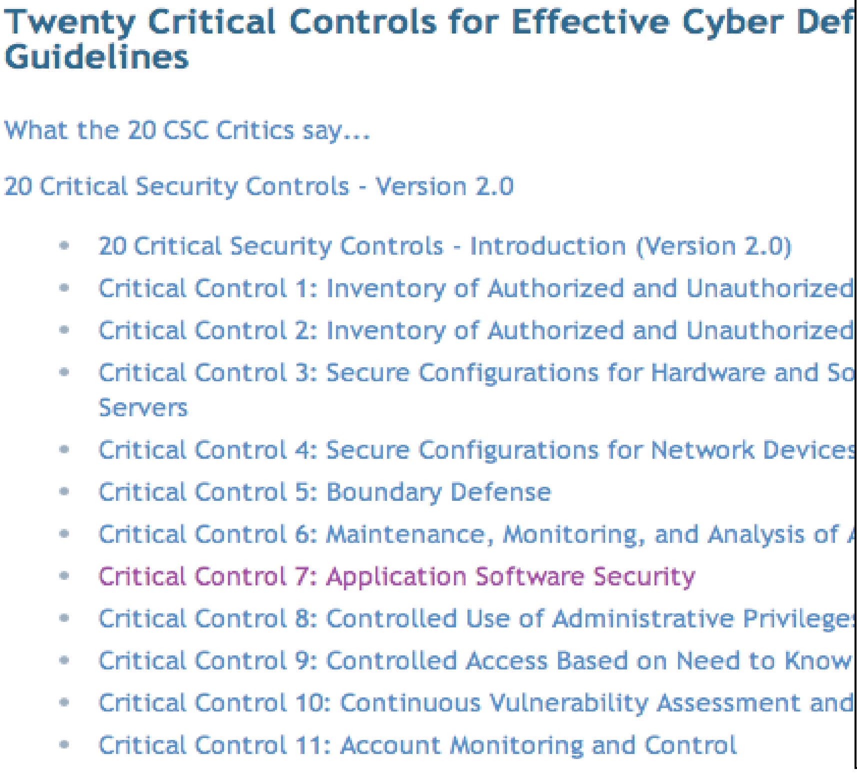
Benchmark Results

Enterprise IT Change Management

Scan Results

Benchmark Results

Centralized Reporting

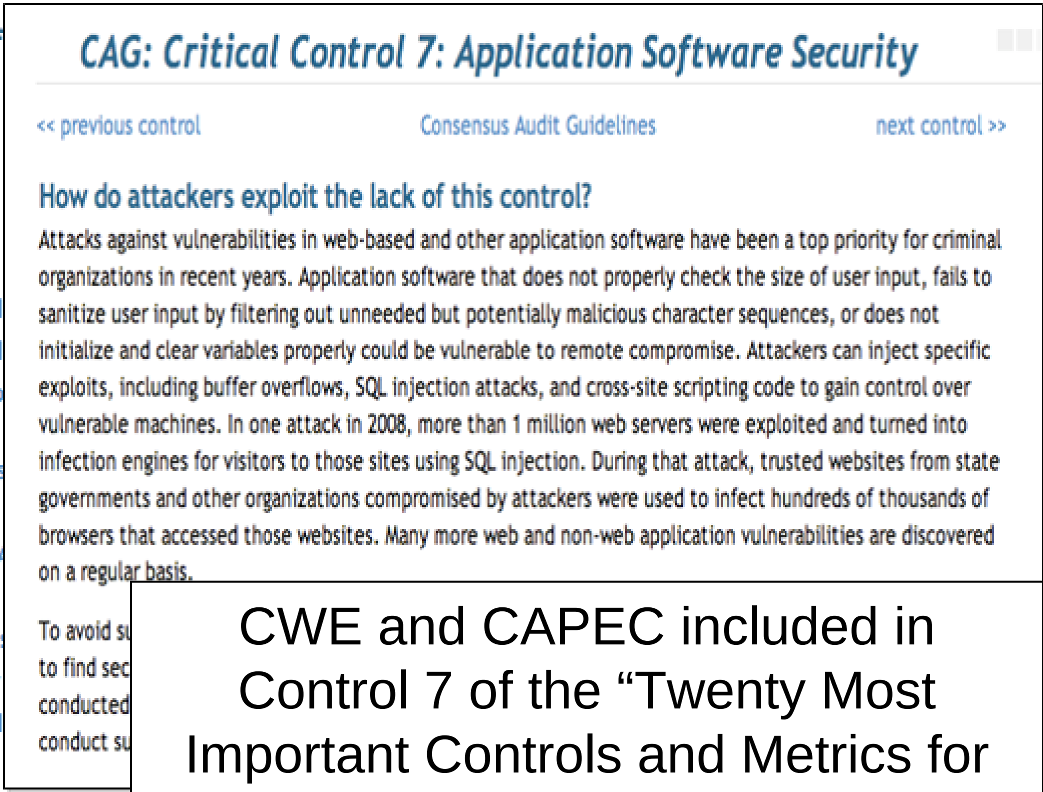


Twenty Critical Controls for Effective Cyber Def Guidelines

What the 20 CSC Critics say...

20 Critical Security Controls - Version 2.0

- 20 Critical Security Controls - Introduction (Version 2.0)
- Critical Control 1: Inventory of Authorized and Unauthorized
- Critical Control 2: Inventory of Authorized and Unauthorized
- Critical Control 3: Secure Configurations for Hardware and So Servers
- Critical Control 4: Secure Configurations for Network Devices
- Critical Control 5: Boundary Defense
- Critical Control 6: Maintenance, Monitoring, and Analysis of
- Critical Control 7: Application Software Security
- Critical Control 8: Controlled Use of Administrative Privileges
- Critical Control 9: Controlled Access Based on Need to Know
- Critical Control 10: Continuous Vulnerability Assessment and
- Critical Control 11: Account Monitoring and Control
- Critical
- Critical
- Critical
- Critical
- Critical
- Critical
- Critical
- Critical
- Critical



CAG: Critical Control 7: Application Software Security

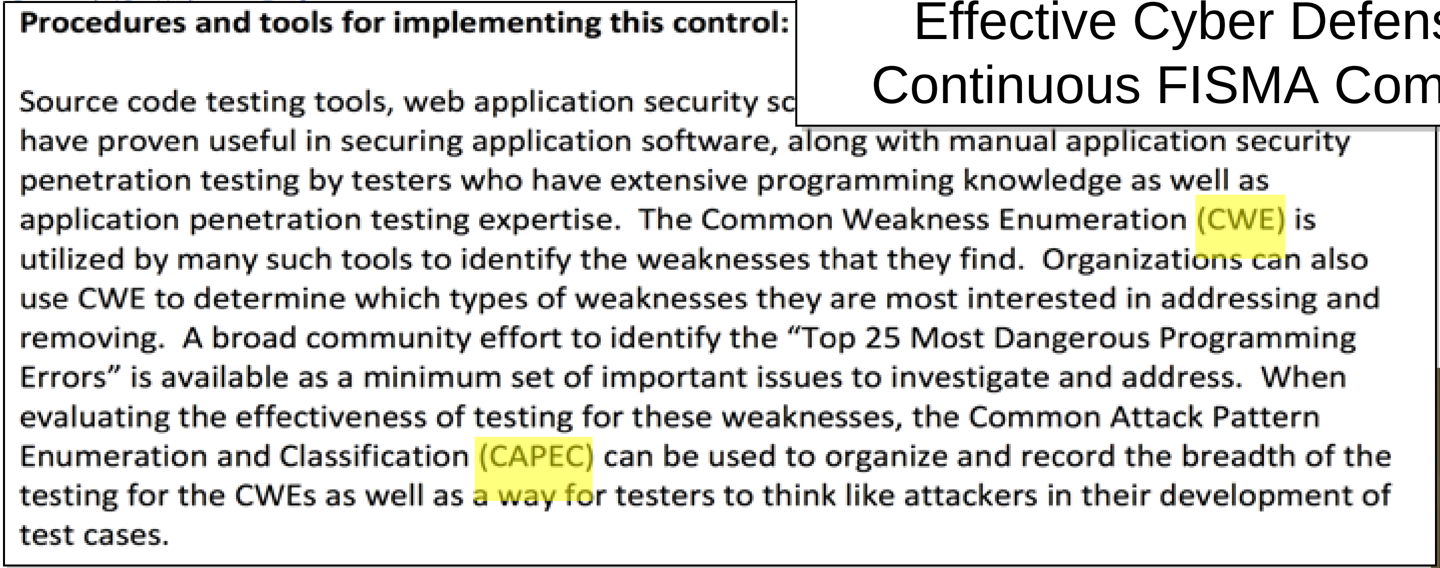
<< previous control   Consensus Audit Guidelines   next control >>

How do attackers exploit the lack of this control?

Attacks against vulnerabilities in web-based and other application software have been a top priority for criminal organizations in recent years. Application software that does not properly check the size of user input, fails to sanitize user input by filtering out unneeded but potentially malicious character sequences, or does not initialize and clear variables properly could be vulnerable to remote compromise. Attackers can inject specific exploits, including buffer overflows, SQL injection attacks, and cross-site scripting code to gain control over vulnerable machines. In one attack in 2008, more than 1 million web servers were exploited and turned into infection engines for visitors to those sites using SQL injection. During that attack, trusted websites from state governments and other organizations compromised by attackers were used to infect hundreds of thousands of browsers that accessed those websites. Many more web and non-web application vulnerabilities are discovered on a regular basis.

To avoid su
to find sec
conducted
conduct su

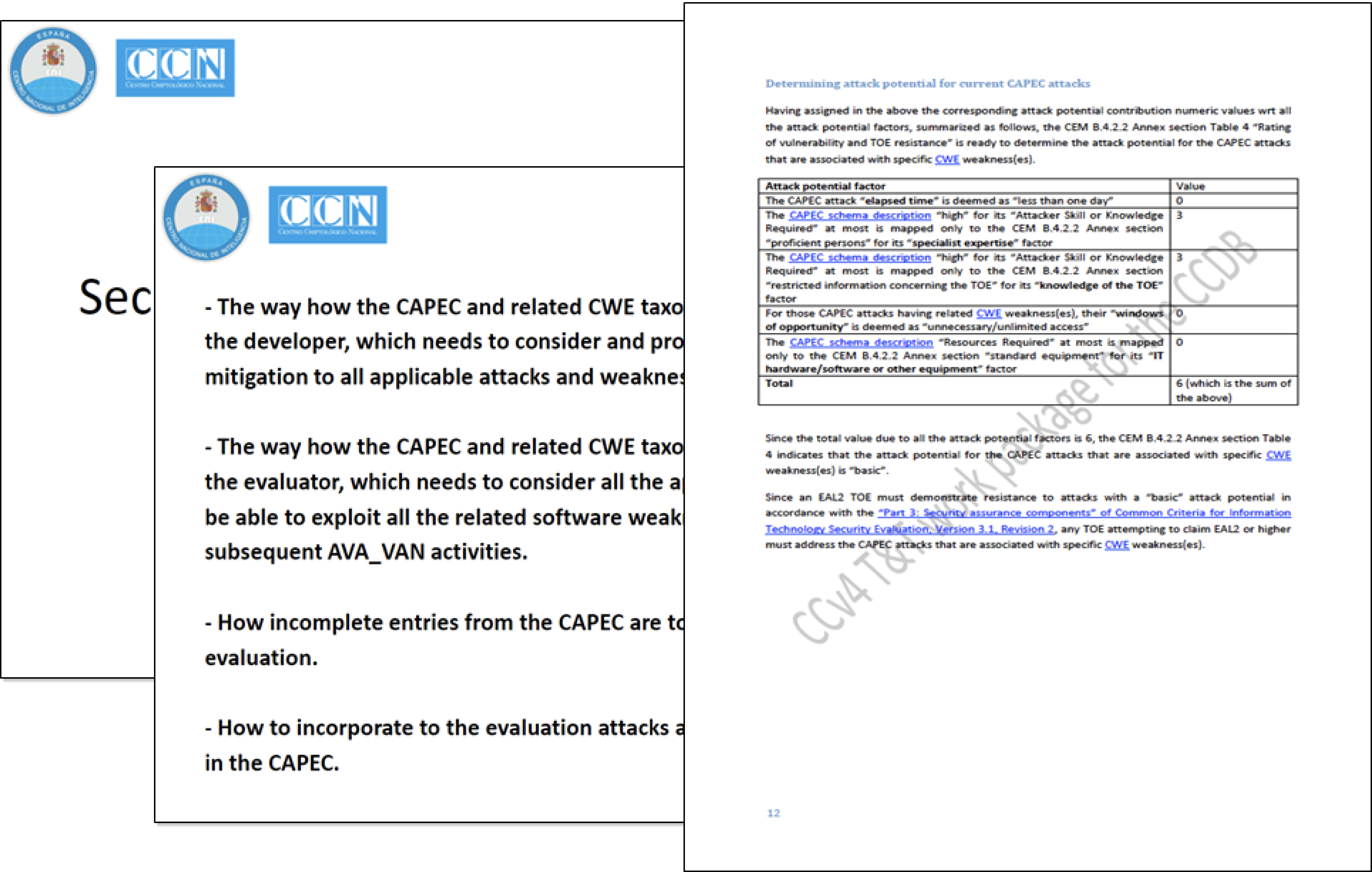
CWE and CAPEC included in Control 7 of the “Twenty Most Important Controls and Metrics for Effective Cyber Defense and Continuous FISMA Compliance”



Procedures and tools for implementing this control:

Source code testing tools, web application security sc have proven useful in securing application software, along with manual application security penetration testing by testers who have extensive programming knowledge as well as application penetration testing expertise. The Common Weakness Enumeration (CWE) is utilized by many such tools to identify the weaknesses that they find. Organizations can also use CWE to determine which types of weaknesses they are most interested in addressing and removing. A broad community effort to identify the “Top 25 Most Dangerous Programming Errors” is available as a minimum set of important issues to investigate and address. When evaluating the effectiveness of testing for these weaknesses, the Common Attack Pattern Enumeration and Classification (CAPEC) can be used to organize and record the breadth of the testing for the CWEs as well as a way for testers to think like attackers in their development of test cases.

Common Criteria version 4 will utilize CAPEC and CWE



CCN
Centro Criptológico Nacional
España
Centro Nacional de Inteligencia

Sec

- The way how the CAPEC and related CWE taxo
the developer, which needs to consider and pro
mitigation to all applicable attacks and weakne

- The way how the CAPEC and related CWE taxo
the evaluator, which needs to consider all the a
be able to exploit all the related software weak
subsequent AVA_VAN activities.

- How incomplete entries from the CAPEC are to
evaluation.

- How to incorporate to the evaluation attacks a
in the CAPEC.

Determining attack potential for current CAPEC attacks

Having assigned in the above the corresponding attack potential contribution numeric values wrt all the attack potential factors, summarized as follows, the CEM B.4.2.2 Annex section Table 4 "Rating of vulnerability and TOE resistance" is ready to determine the attack potential for the CAPEC attacks that are associated with specific CWE weakness(es).

Attack potential factor	Value
The CAPEC attack "**elapsed time**" is deemed as "less than one day"	0
The CAPEC schema description "high" for its "Attacker Skill or Knowledge Required" at most is mapped only to the CEM B.4.2.2 Annex section "proficient persons" for its "**specialist expertise**" factor	3
The CAPEC schema description "high" for its "Attacker Skill or Knowledge Required" at most is mapped only to the CEM B.4.2.2 Annex section "restricted information concerning the TOE" for its "**knowledge of the TOE**" factor	3
For those CAPEC attacks having related CWE weakness(es), their "**windows of opportunity**" is deemed as "unnecessary/unlimited access"	0
The CAPEC schema description "Resources Required" at most is mapped only to the CEM B.4.2.2 Annex section "standard equipment" for its "**IT hardware/software or other equipment**" factor	0
Total	6 (which is the sum of the above)

Since the total value due to all the attack potential factors is 6, the CEM B.4.2.2 Annex section Table 4 indicates that the attack potential for the CAPEC attacks that are associated with specific CWE weakness(es) is "basic".

Since an EAL2 TOE must demonstrate resistance to attacks with a "basic" attack potential in accordance with the "Part 3: Security assurance components" of Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, any TOE attempting to claim EAL2 or higher must address the CAPEC attacks that are associated with specific CWE weakness(es).

The Building Blocks Are:

- Enumerations
  - **Catalog the fundamental entities in IA, Cyber Security, and Software Assurance**
    - **Vulnerabilities (CVE), configuration issues (CCE), software packages (CPE), 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), config risk (CCSS), weakness risk (CWSS), 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**

The Building Blocks Are:

CVE

CPE

CW

CAPEC

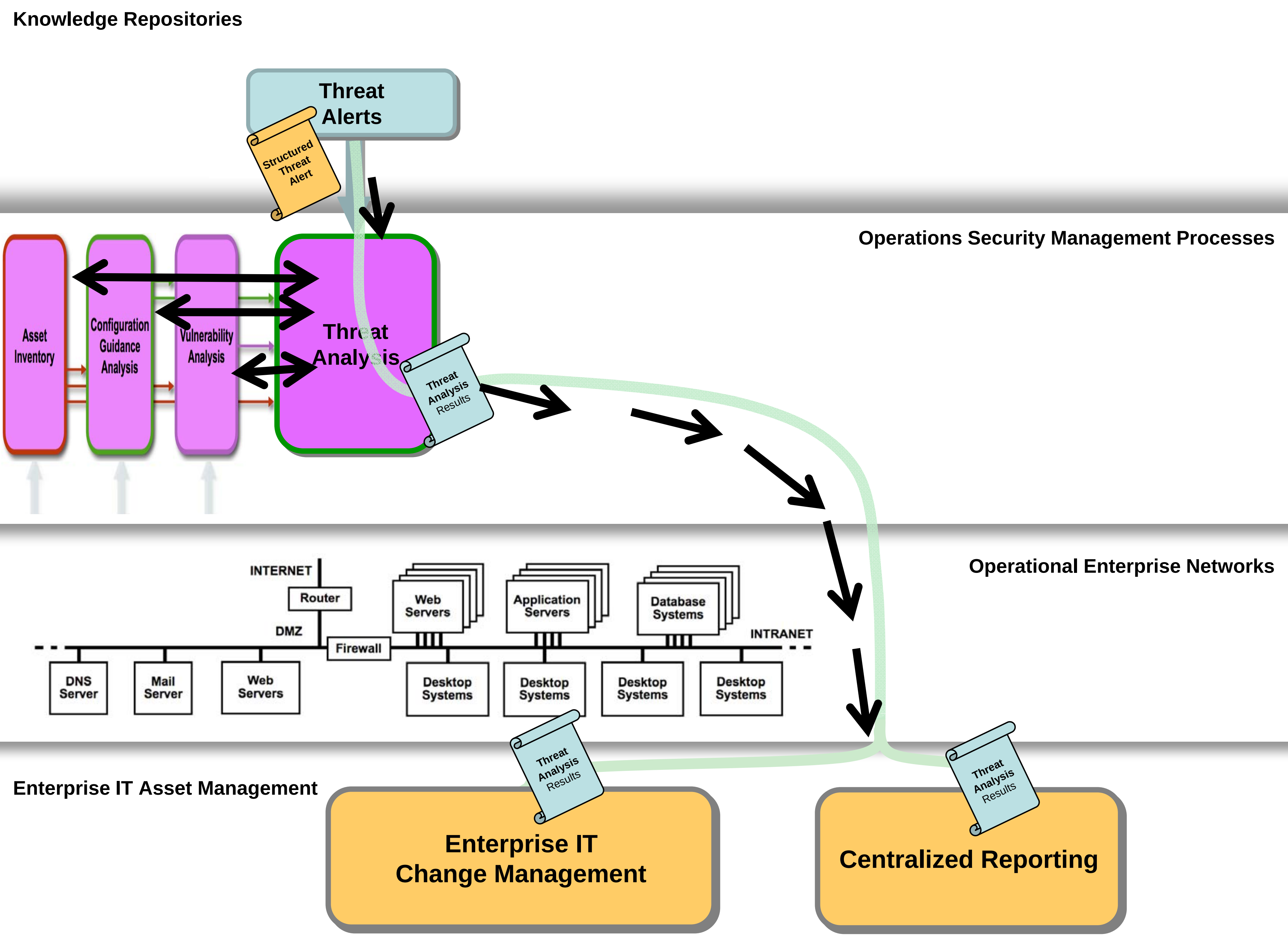
OVAL

CEE

NIST/DHS NVD

Threat
Alerts

Knowledge Repository



Knowledge Repositories

Threat Alerts

Structured Threat Alert

Operations Security Management Processes

Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

Threat Analysis

Threat Analysis Results

Operational Enterprise Networks

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

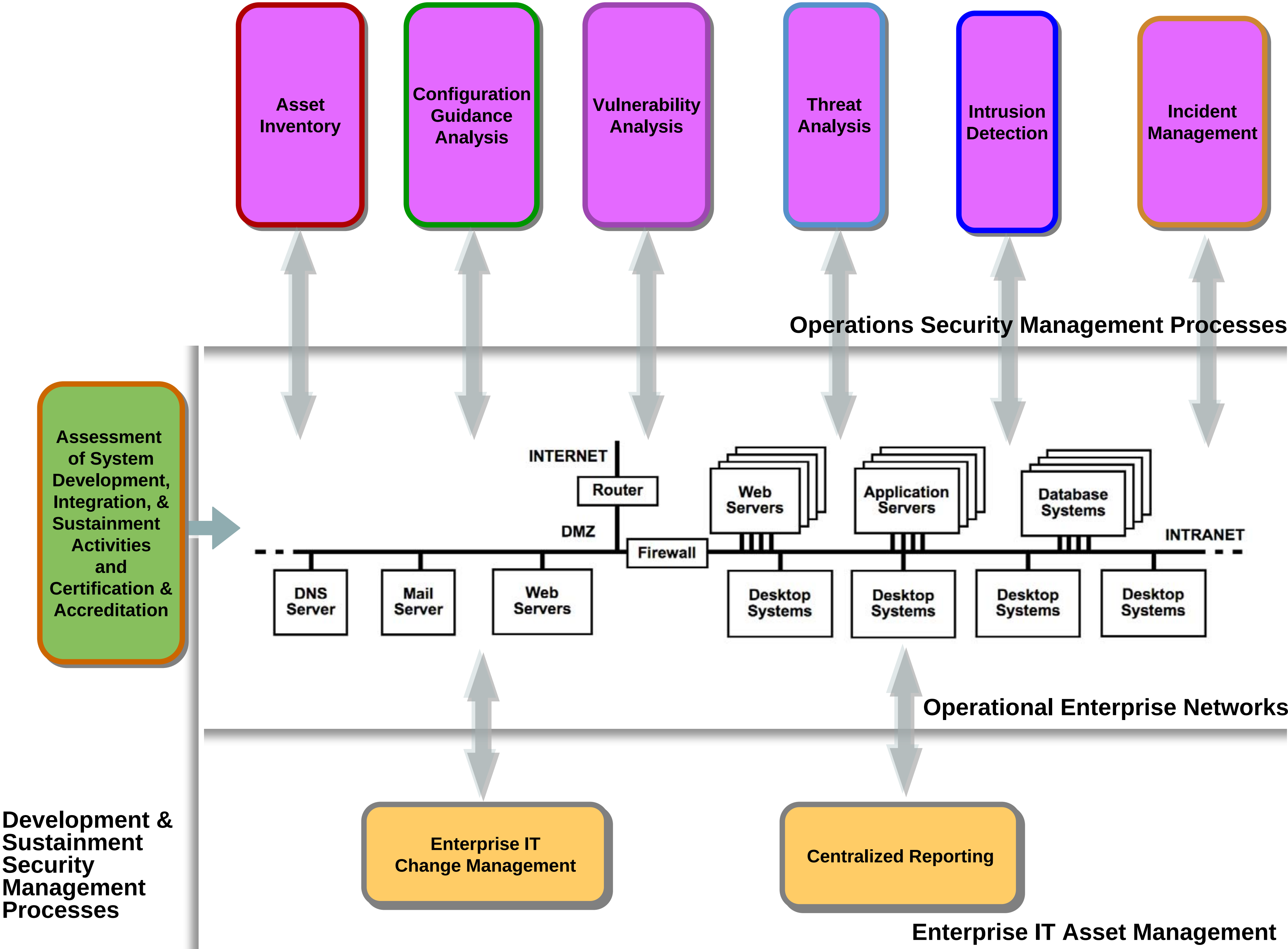
Enterprise IT Asset Management

Threat Analysis Results

Enterprise IT Change Management

Threat Analysis Results

Centralized Reporting



Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

Threat Analysis

Intrusion Detection

Incident Management

Operations Security Management Processes

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

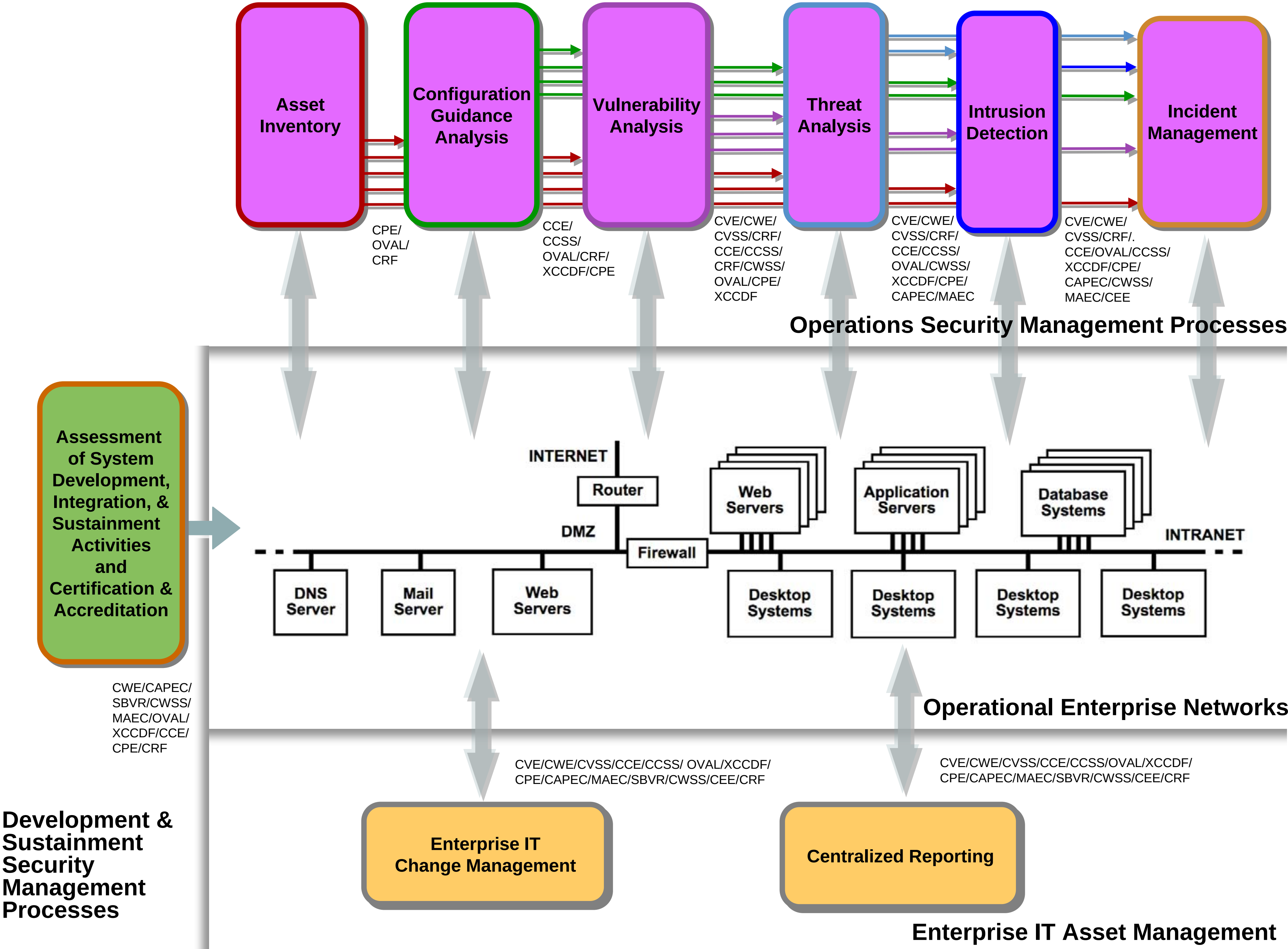
Operational Enterprise Networks

Development & Sustainment Security Management Processes

Enterprise IT Change Management

Centralized Reporting

Enterprise IT Asset Management



Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

Threat Analysis

Intrusion Detection

Incident Management

CPE/
OVAL/
CRF

CCE/
CCSS/
OVAL/CRF/
XCCDF/CPE

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

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

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

Operations Security Management Processes

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

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/CRF

Operational Enterprise Networks

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

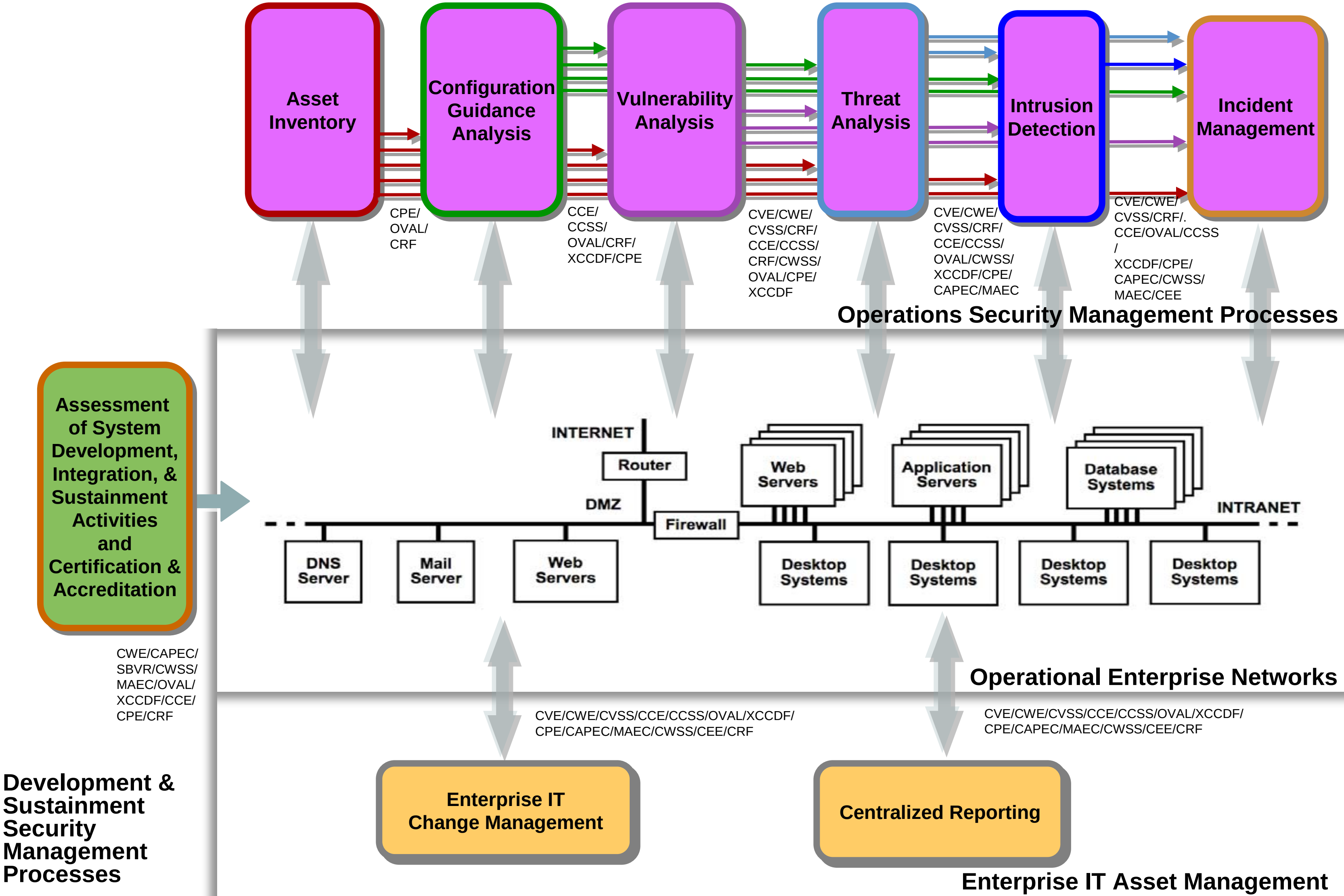
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/SBVR/CWSS/CEE/CRF

Enterprise IT Change Management

Centralized Reporting

Development & Sustainment Security Management Processes

Enterprise IT Asset Management



Asset Inventory

CPE/
OVAL/
CRF

Configuration Guidance Analysis

CCE/
CCSS/
OVAL/CRF/
XCCDF/CPE

Vulnerability Analysis

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

Threat Analysis

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

Intrusion Detection

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

Incident Management

Operations Security Management Processes

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

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/CRF

Operational Enterprise Networks

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

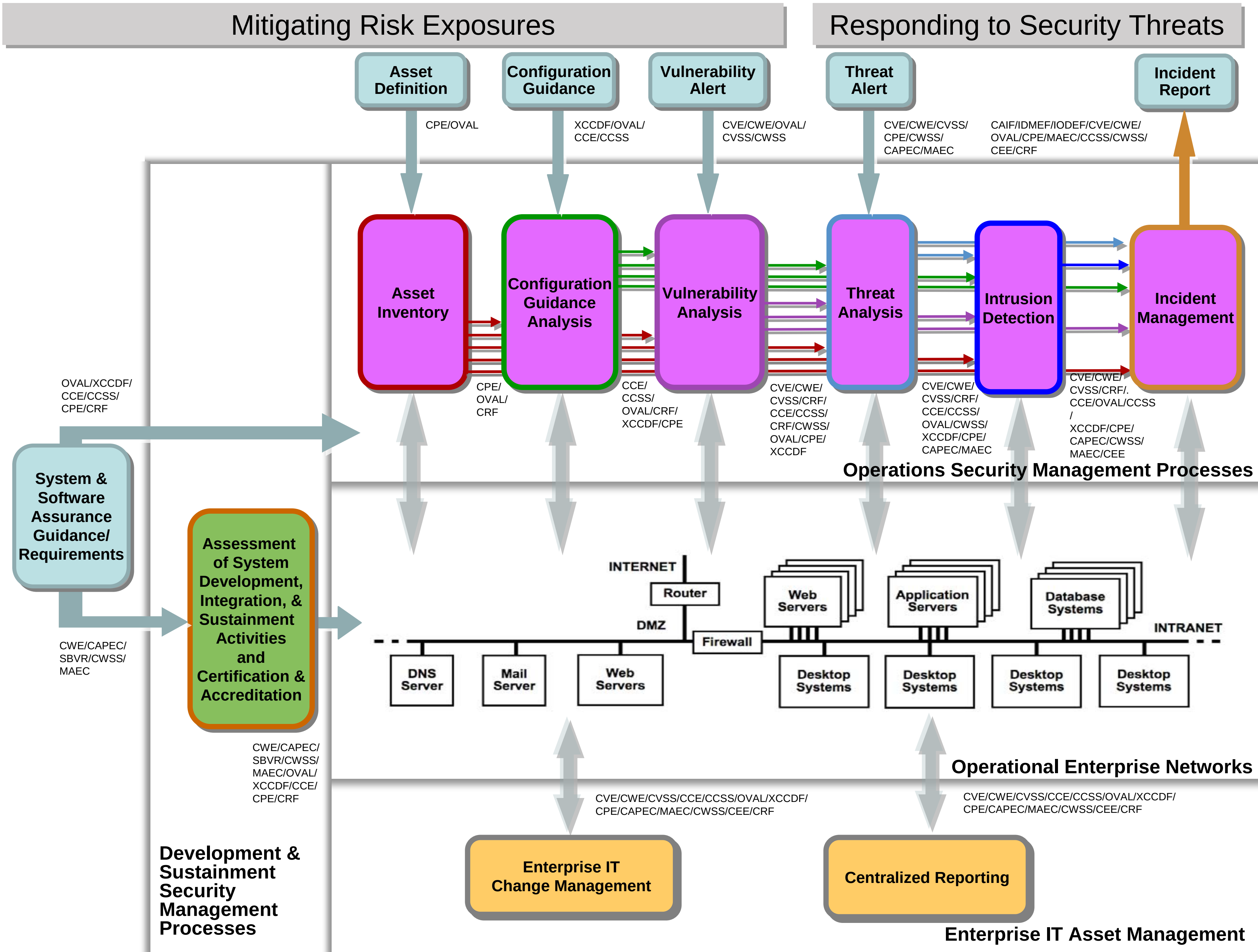
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

Enterprise IT Change Management

Centralized Reporting

Development & Sustainment Security Management Processes

Enterprise IT Asset Management



Mitigating Risk Exposures

Responding to Security Threats

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

Incident Report

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

Asset Inventory

CPE/
OVAL/
CRF

Configuration Guidance Analysis

CCE/
CCSS/
OVAL/CRF/
XCCDF/CPE

Vulnerability Analysis

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

Threat Analysis

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

Intrusion Detection

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

Incident Management

OVAL/XCCDF/
CCE/CCSS/
CPE/CRF

System & Software Assurance Guidance/ Requirements

CWE/CAPEC/
SBVR/CWSS/
MAEC

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

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/CRF

Operations Security Management Processes

Operational Enterprise Networks

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

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

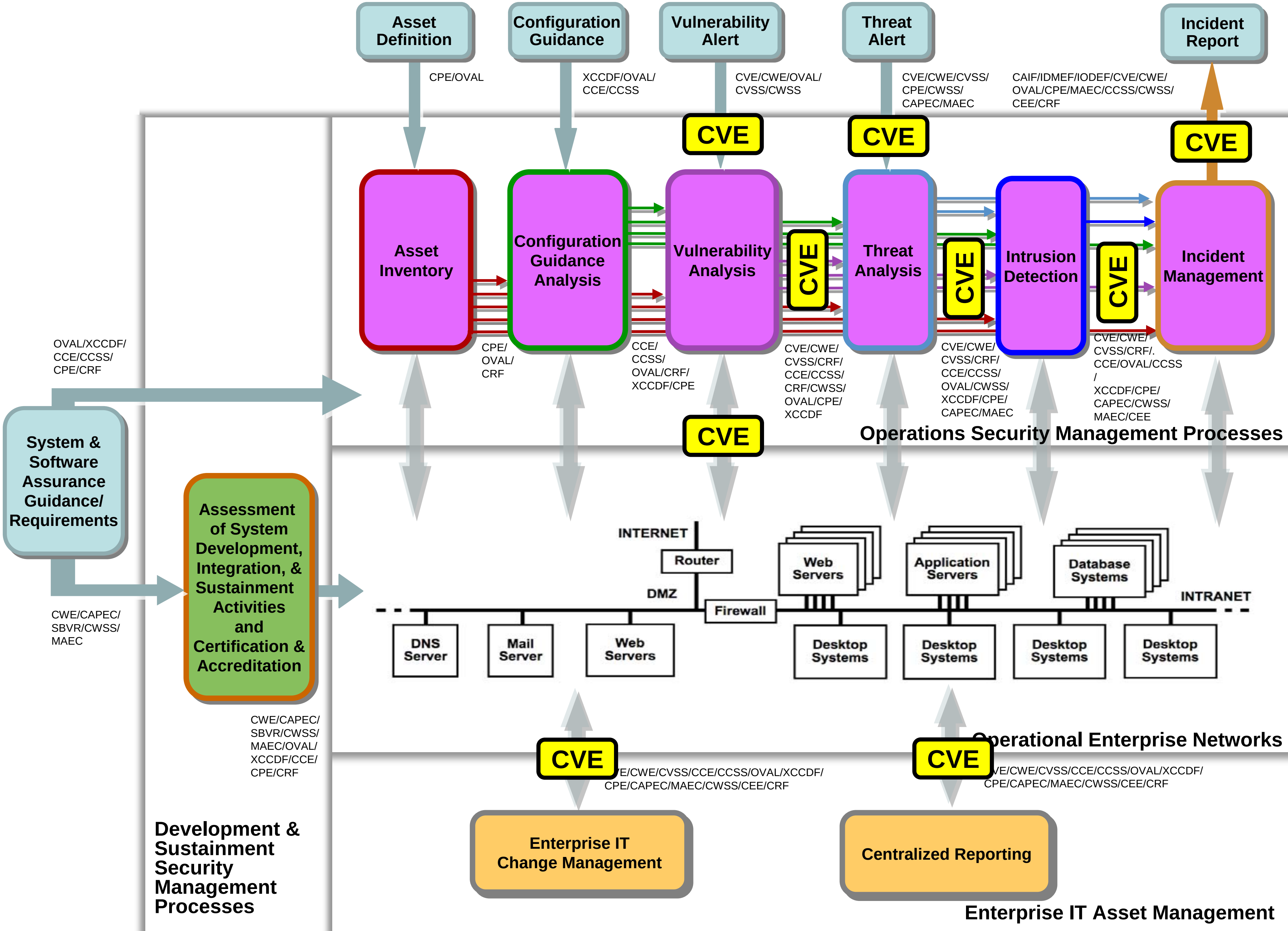
Enterprise IT Change Management

Centralized Reporting

Development & Sustainment Security Management Processes

Enterprise IT Asset Management

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/CRF

Incident Report

CVE

CVE

CVE

Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

CVE

Threat Analysis

CVE

Intrusion Detection

CVE

Incident Management

CPE/
OVAL/
CRF

CCE/
CCSS/
OVAL/CRF/
XCCDF/CPE

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

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

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

OVAL/XCCDF/
CCE/CCSS/
CPE/CRF

CVE

Operations Security Management Processes

System & Software Assurance Guidance/ Requirements

CWE/CAPEC/
SBVR/CWSS/
MAEC

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

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/CRF

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

Operational Enterprise Networks

CVE

E/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

CVE

VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

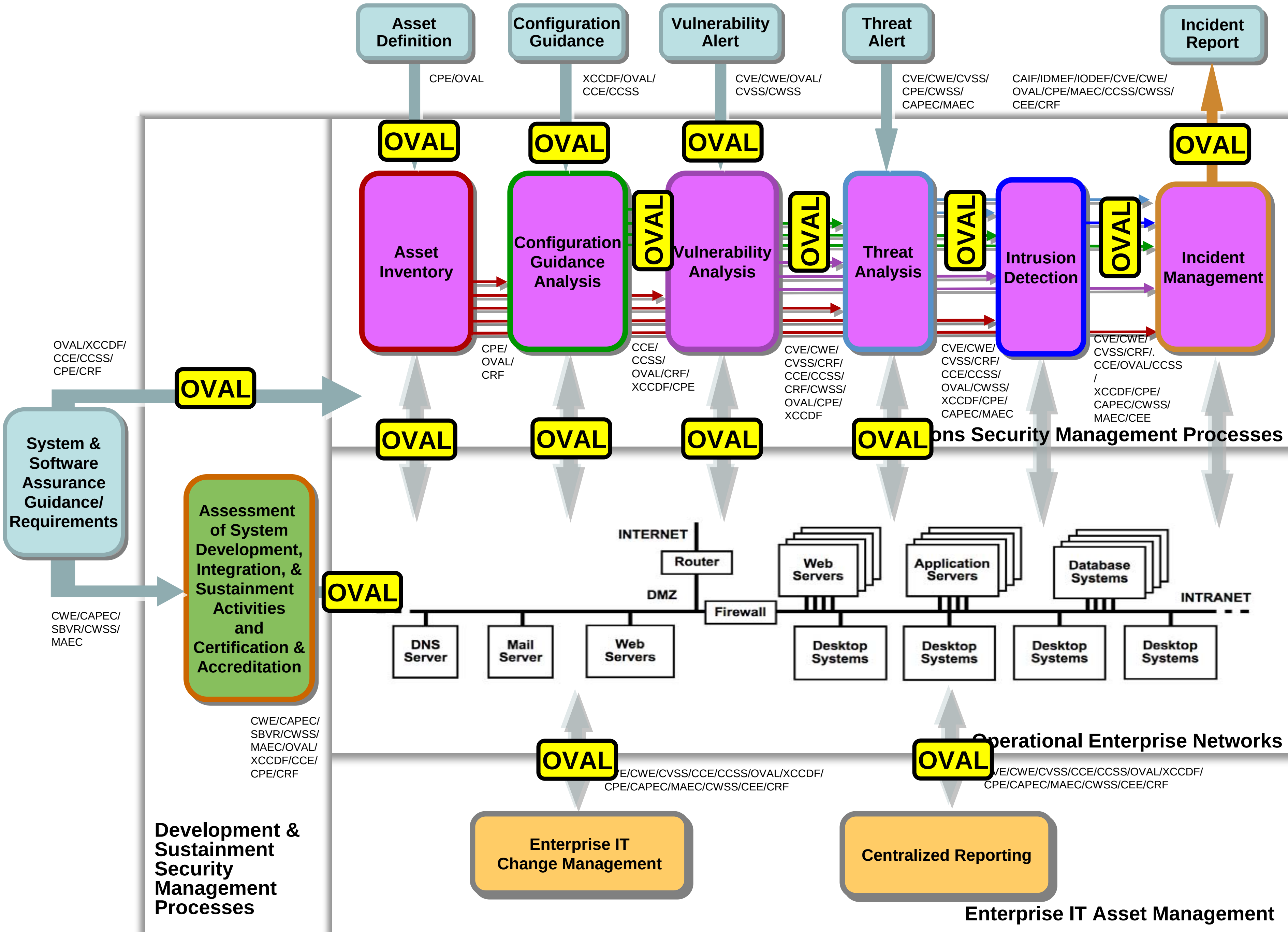
Enterprise IT Change Management

Centralized Reporting

Development & Sustainment Security Management Processes

Enterprise IT Asset Management

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/CRF

Incident Report

OVAL

OVAL

OVAL

OVAL

Asset Inventory

Configuration Guidance Analysis

OVAL

Vulnerability Analysis

OVAL

Threat Analysis

OVAL

Intrusion Detection

OVAL

Incident Management

CPE/
OVAL/
CRF

CCE/
CCSS/
OVAL/CRF/
XCCDF/CPE

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

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

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

OVAL/XCCDF/
CCE/CCSS/
CPE/CRF

OVAL

System & Software Assurance Guidance/ Requirements

OVAL

OVAL

OVAL

OVAL

ons Security Management Processes

CWE/CAPEC/
SBVR/CWSS/
MAEC

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

OVAL

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

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/CRF

perational Enterprise Networks

OVAL

E/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

OVAL

VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

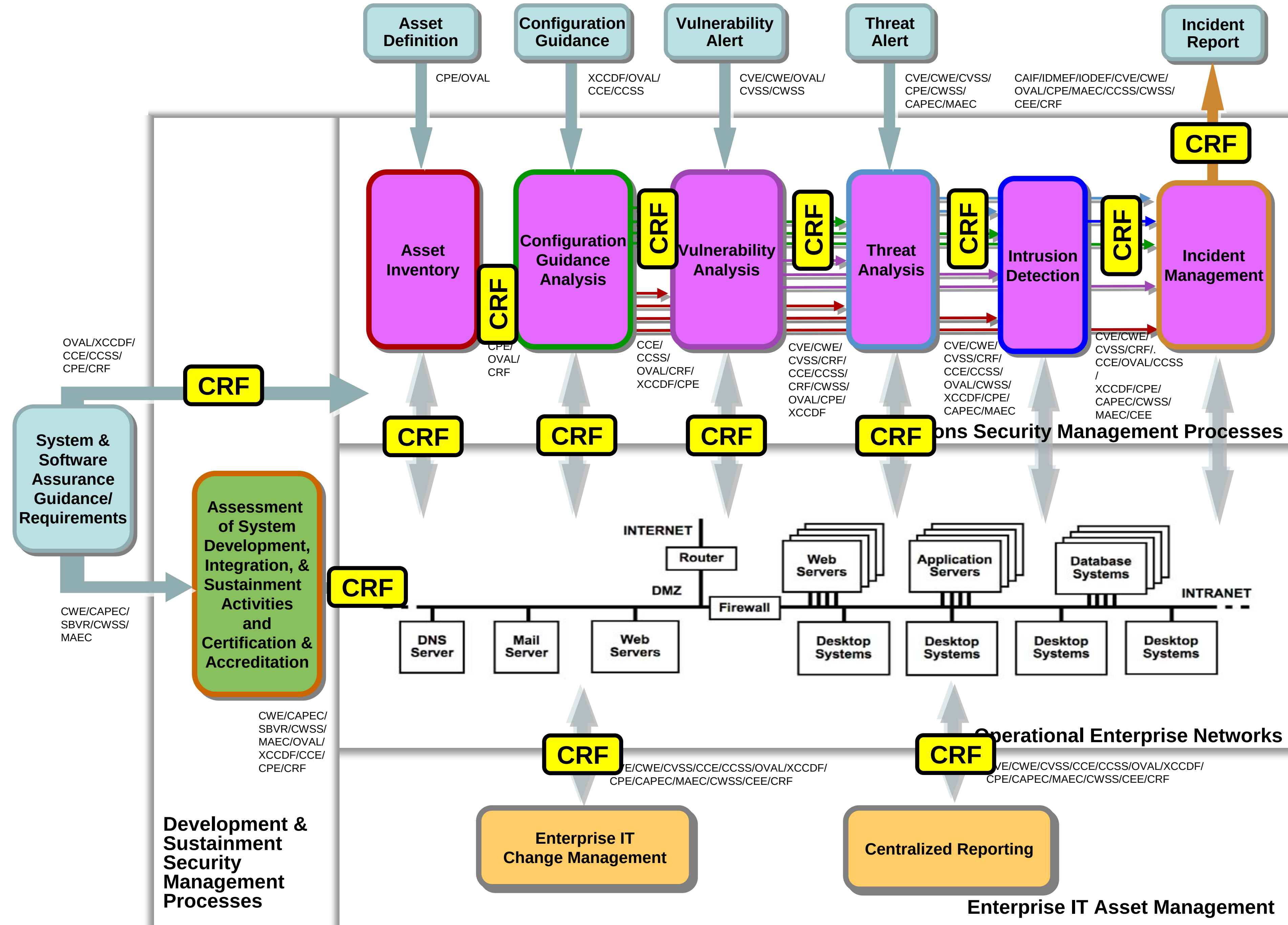
Development & Sustainment Security Management Processes

Enterprise IT Change Management

Centralized Reporting

Enterprise IT Asset Management

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

Incident Report

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

CRF

Asset Inventory

CRF

CPE/
OVAL/
CRF

Configuration Guidance Analysis

CRF

CCE/
CCSS/
OVAL/CRF/
XCCDF/CPE

Vulnerability Analysis

CRF

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

Threat Analysis

CRF

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

Intrusion Detection

CRF

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

Incident Management

OVAL/XCCDF/
CCE/CCSS/
CPE/CRF

CRF

CRF

CRF

CRF

CRF

ons Security Management Processes

System & Software Assurance Guidance/ Requirements

CWE/CAPEC/
SBVR/CWSS/
MAEC

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

CRF

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

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/CRF

Operational Enterprise Networks

CRF

E/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

CRF

VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

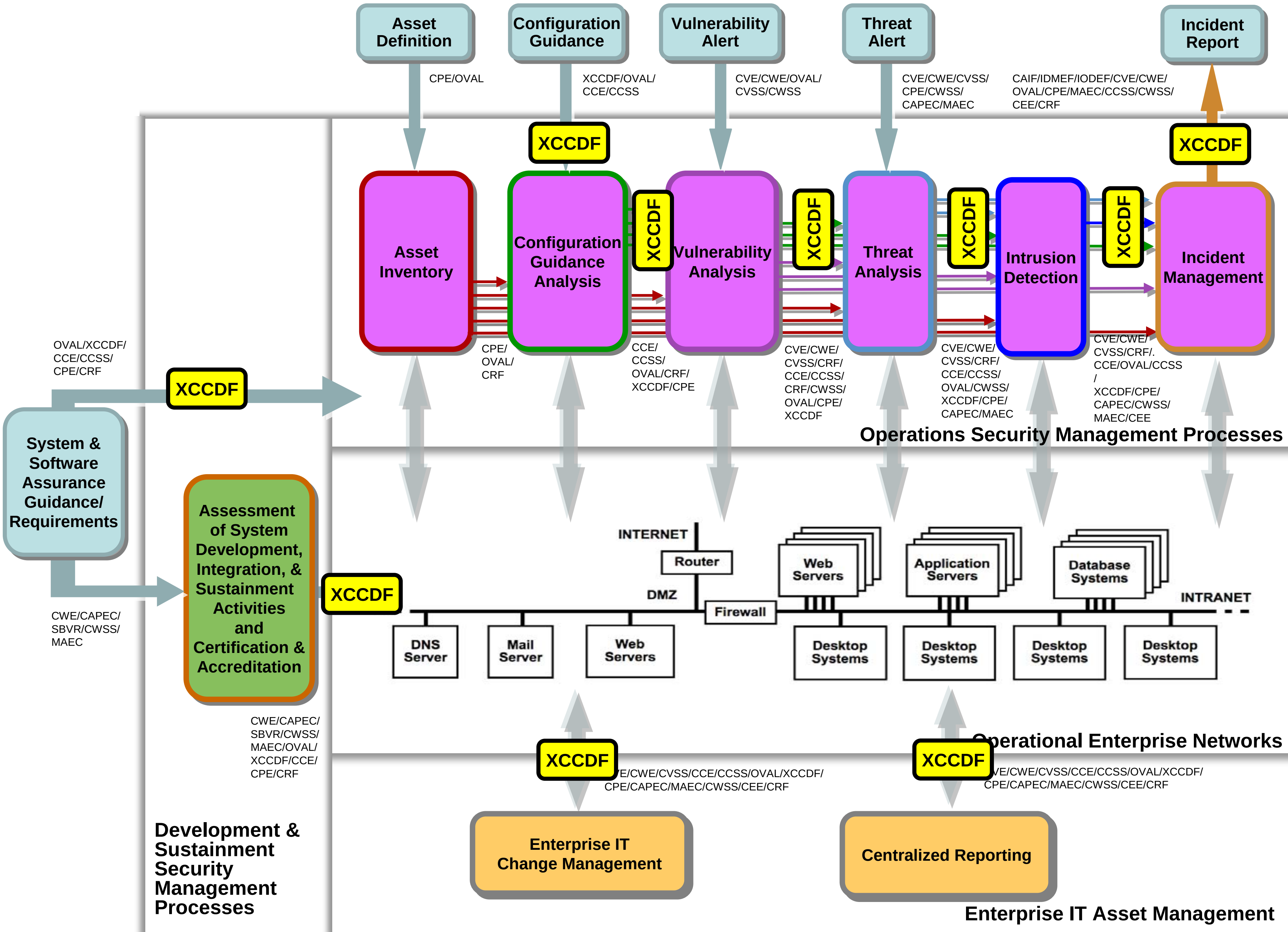
Enterprise IT Change Management

Centralized Reporting

Development & Sustainment Security Management Processes

Enterprise IT Asset Management

Knowledge Repositories



Asset Definition

Configuration Guidance

Vulnerability Alert

Threat Alert

Incident Report

CPE/OVAL

XCCDF/OVAL/
CCE/CCSS

CVE/CWE/OVAL/
CVSS/CWSS

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

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

XCCDF

XCCDF

Asset Inventory

Configuration Guidance Analysis

XCCDF

Vulnerability Analysis

XCCDF

Threat Analysis

XCCDF

Intrusion Detection

XCCDF

Incident Management

OVAL/XCCDF/
CCE/CCSS/
CPE/CRF

XCCDF

CPE/
OVAL/
CRF

CCE/
CCSS/
OVAL/CRF/
XCCDF/CPE

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

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

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

Operations Security Management Processes

System & Software Assurance Guidance/ Requirements

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

CWE/CAPEC/
SBVR/CWSS/
MAEC

XCCDF

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

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/CRF

Operational Enterprise Networks

XCCDF

E/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

XCCDF

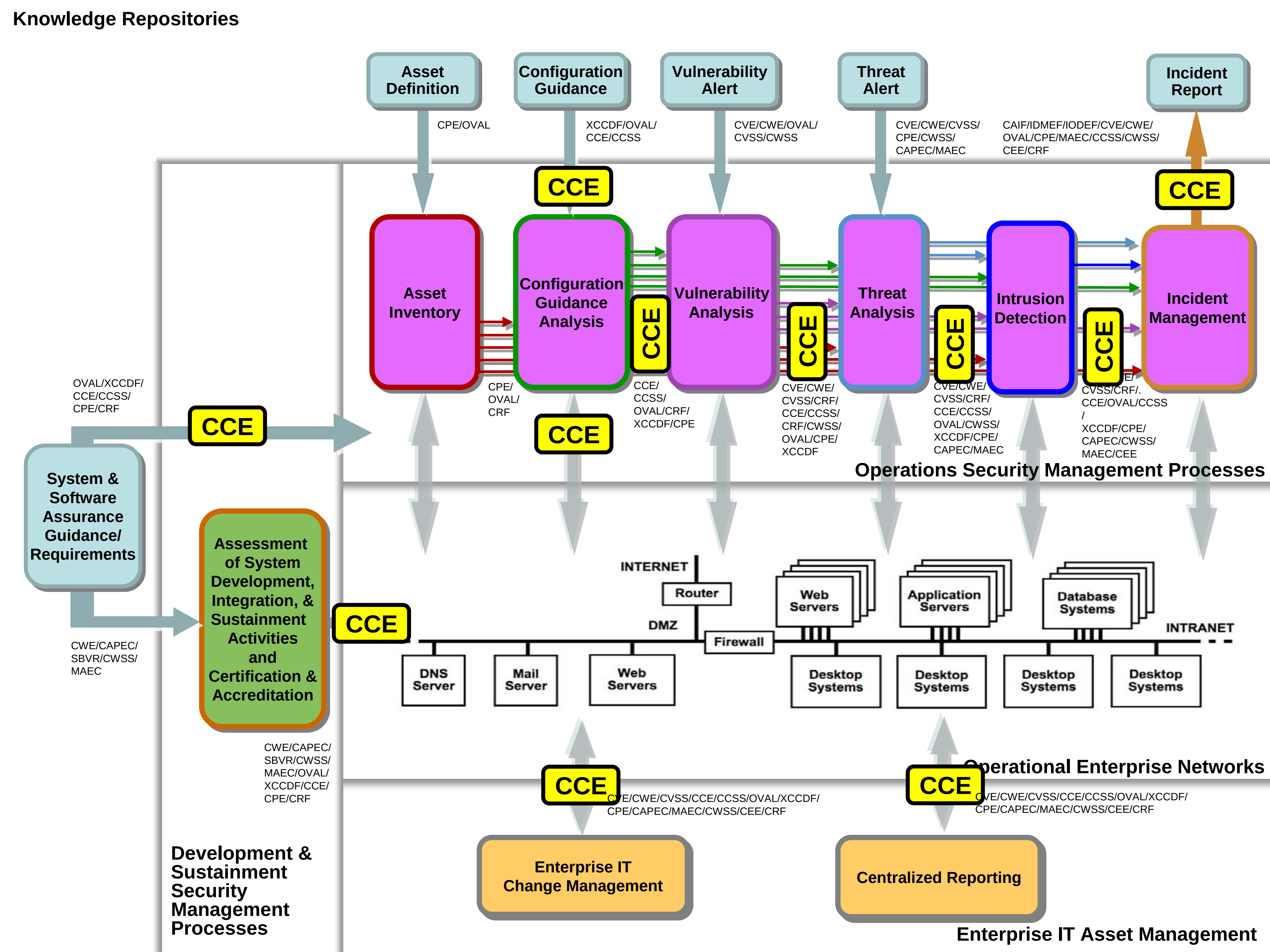
VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

Development & Sustainment Security Management Processes

Enterprise IT Change Management

Centralized Reporting

Enterprise IT Asset Management



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

Incident Report

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

CCE

CCE

Asset Inventory

Configuration Guidance Analysis

CCE

Vulnerability Analysis

CCE

Threat Analysis

CCE

Intrusion Detection

CCE

Incident Management

CPE/
OVAL/
CRF

CCE

CCE/
CCSS/
OVAL/CRF/
XCCDF/CPE

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

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

E/
CVSS/CRF/.
CCE/OVAL/CCSS
/
XCCDF/CPE/
CAPEC/CWSS/
MAEC/CEE

Operations Security Management Processes

OVAL/XCCDF/
CCE/CCSS/
CPE/CRF

CCE

System & Software Assurance Guidance/ Requirements

CWE/CAPEC/
SBVR/CWSS/
MAEC

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

CCE

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/CRF

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

Operational Enterprise Networks

CCE

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

CCE

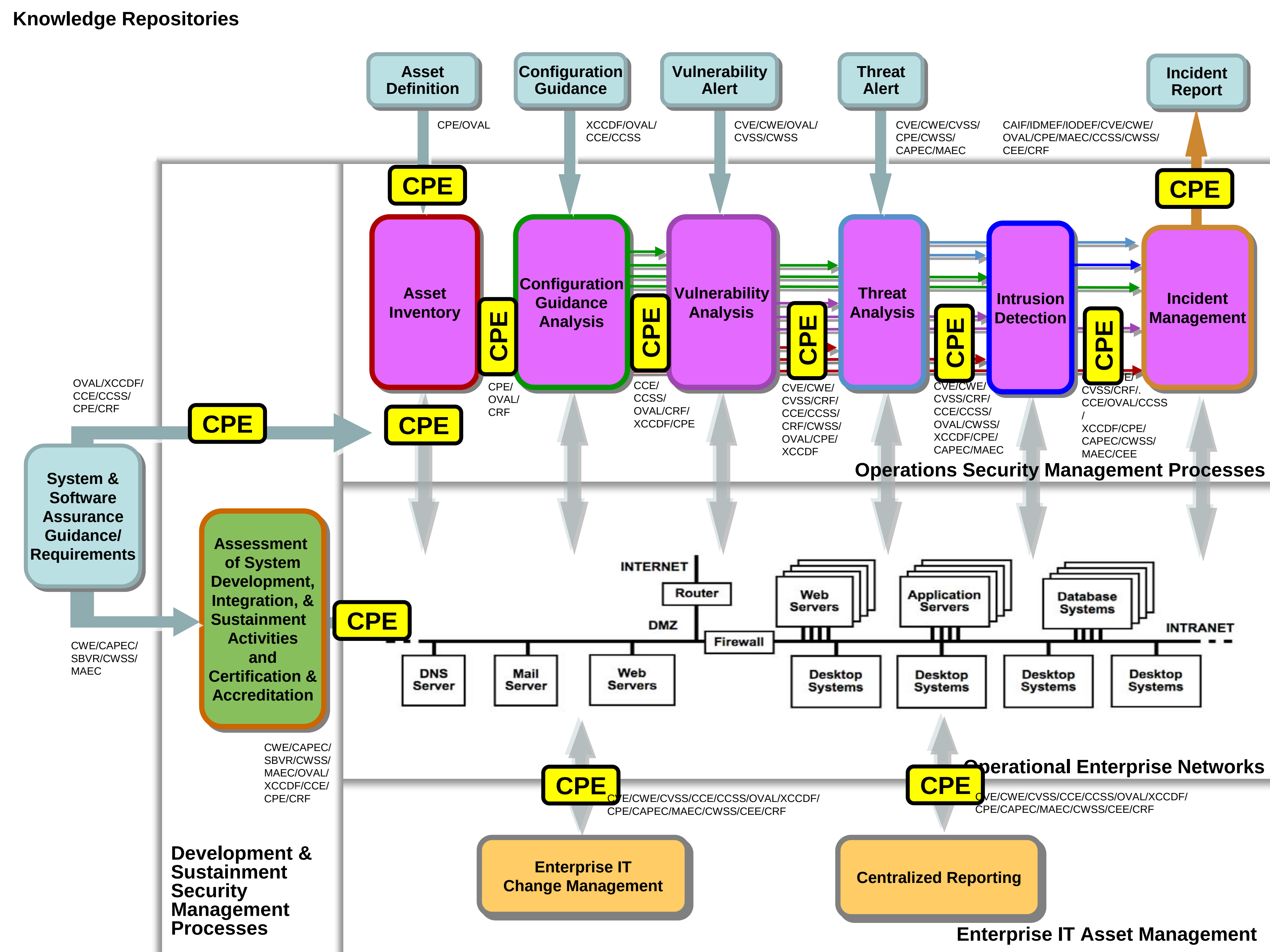
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

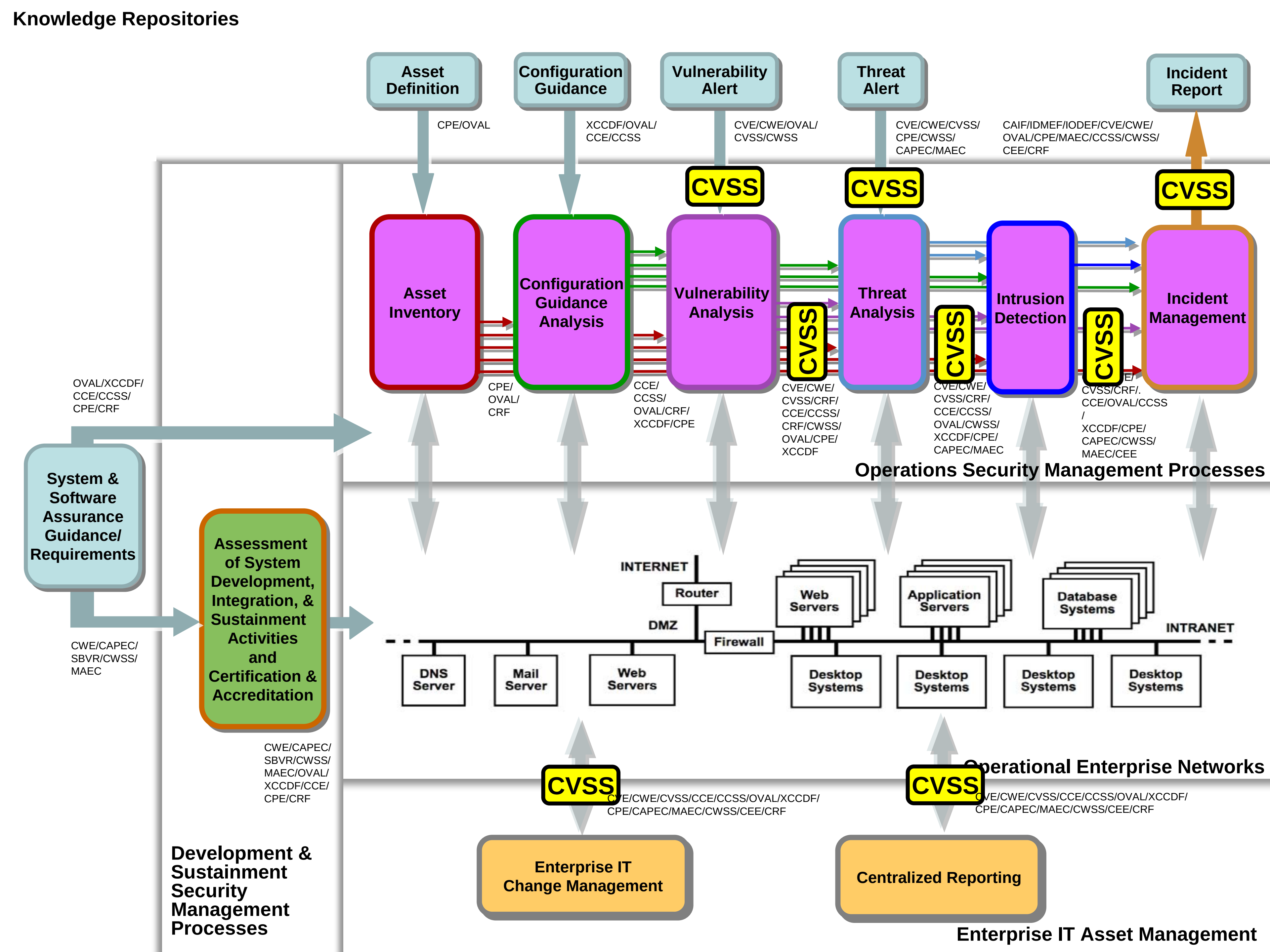
Development & Sustainment Security Management Processes

Enterprise IT Change Management

Centralized Reporting

Enterprise IT Asset Management


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
Incident Report
CAIF/IDMEF/IODEF/CVE/CWE/ OVAL/CPE/MAEC/CCSS/CWSS/ CEE/CRF
CPE
CPE
Asset Inventory
CPE
Configuration Guidance Analysis
CPE
Vulnerability Analysis
CPE
Threat Analysis
CPE
Intrusion Detection
CPE
Incident Management
CPE/ OVAL/ CRF
CCE/ CCSS/ OVAL/CRF/ XCCDF/CPE
CVE/CWE/ CVSS/CRF/ CCE/CCSS/ CRF/CWSS/ OVAL/CPE/ XCCDF
CVE/CWE/ CVSS/CRF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAEC
E/ CVSS/CRF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
OVAL/XCCDF/ CCE/CCSS/ CPE/CRF
CPE
CPE
Operations Security Management Processes
System & Software Assurance Guidance/ Requirements
CWE/CAPEC/ SBVR/CWSS/ MAEC
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
CPE
CWE/CAPEC/ SBVR/CWSS/ MAEC/OVAL/ XCCDF/CCE/ CPE/CRF
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
Operational Enterprise Networks
CPE
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/CRF
CPE
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/CRF
Development & Sustainment Security Management Processes
Enterprise IT Change Management
Centralized Reporting
Enterprise IT Asset Management



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

Incident Report

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

CVSS

CVSS

CVSS

Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

Threat Analysis

Intrusion Detection

Incident Management

CVSS

CVSS

CVSS

CPE/
OVAL/
CRF

CCE/
CCSS/
OVAL/CRF/
XCCDF/CPE

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

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

E/
CVSS/CRF/.
CCE/OVAL/CCSS
/
XCCDF/CPE/
CAPEC/CWSS/
MAEC/CEE

OVAL/XCCDF/
CCE/CCSS/
CPE/CRF

System & Software Assurance Guidance/ Requirements

CWE/CAPEC/
SBVR/CWSS/
MAEC

Operations Security Management Processes

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

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/CRF

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

Operational Enterprise Networks

CVSS

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

CVSS

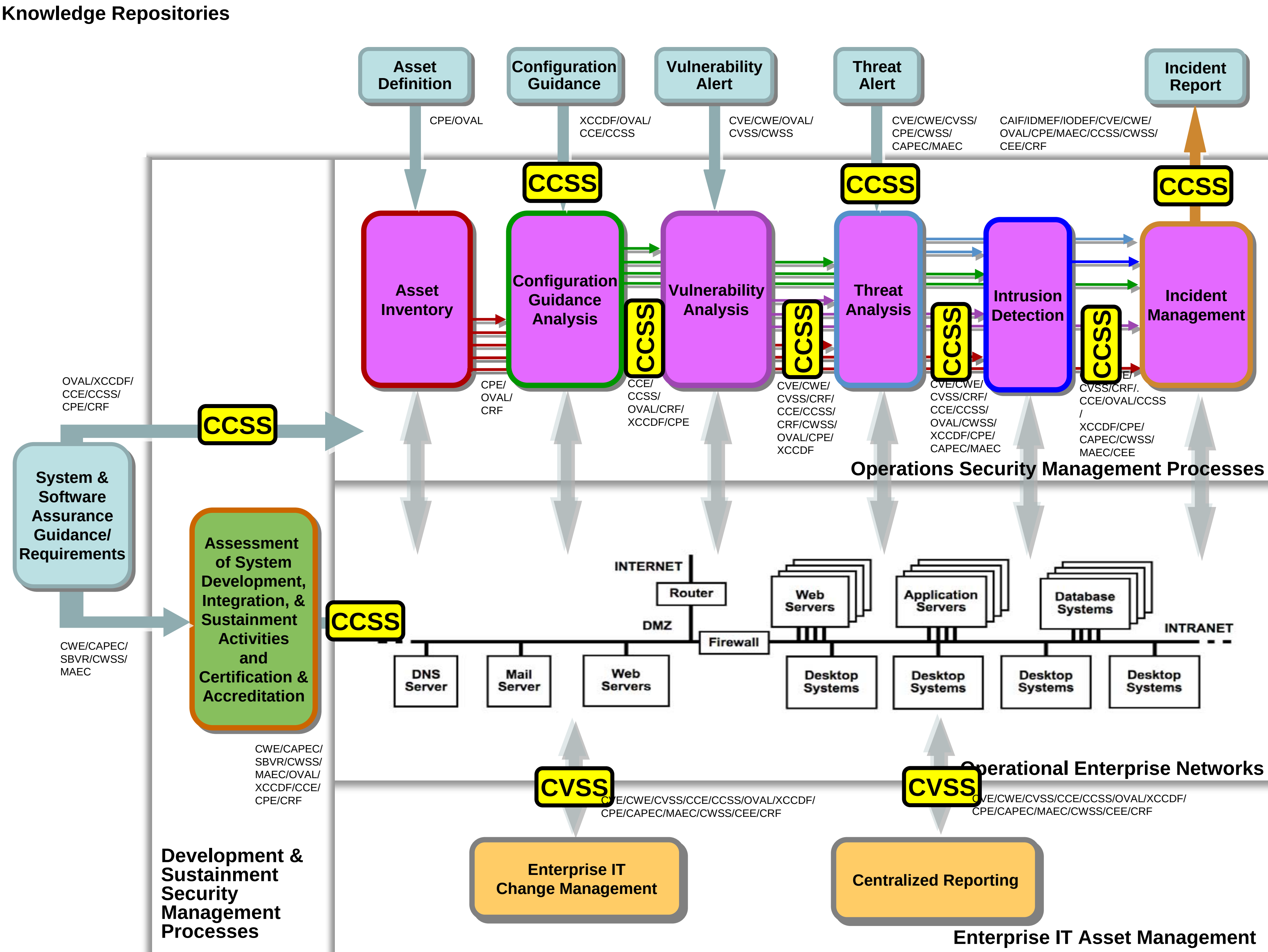
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

Development & Sustainment Security Management Processes

Enterprise IT Change Management

Centralized Reporting

Enterprise IT Asset Management



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

Incident Report

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

CCSS

CCSS

CCSS

Asset Inventory

CPE/
OVAL/
CRF

Configuration Guidance Analysis

CCSS

CCE/
CCSS/
OVAL/CRF/
XCCDF/CPE

Vulnerability Analysis

CCSS

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

Threat Analysis

CCSS

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

Intrusion Detection

CCSS

E/
CVSS/CRF/.
CCE/OVAL/CCSS
/
XCCDF/CPE/
CAPEC/CWSS/
MAEC/CEE

Incident Management

Operations Security Management Processes

OVAL/XCCDF/
CCE/CCSS/
CPE/CRF

CCSS

System & Software Assurance Guidance/ Requirements

CWE/CAPEC/
SBVR/CWSS/
MAEC

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

CCSS

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/CRF

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

Operational Enterprise Networks

CVSS

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

CVSS

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

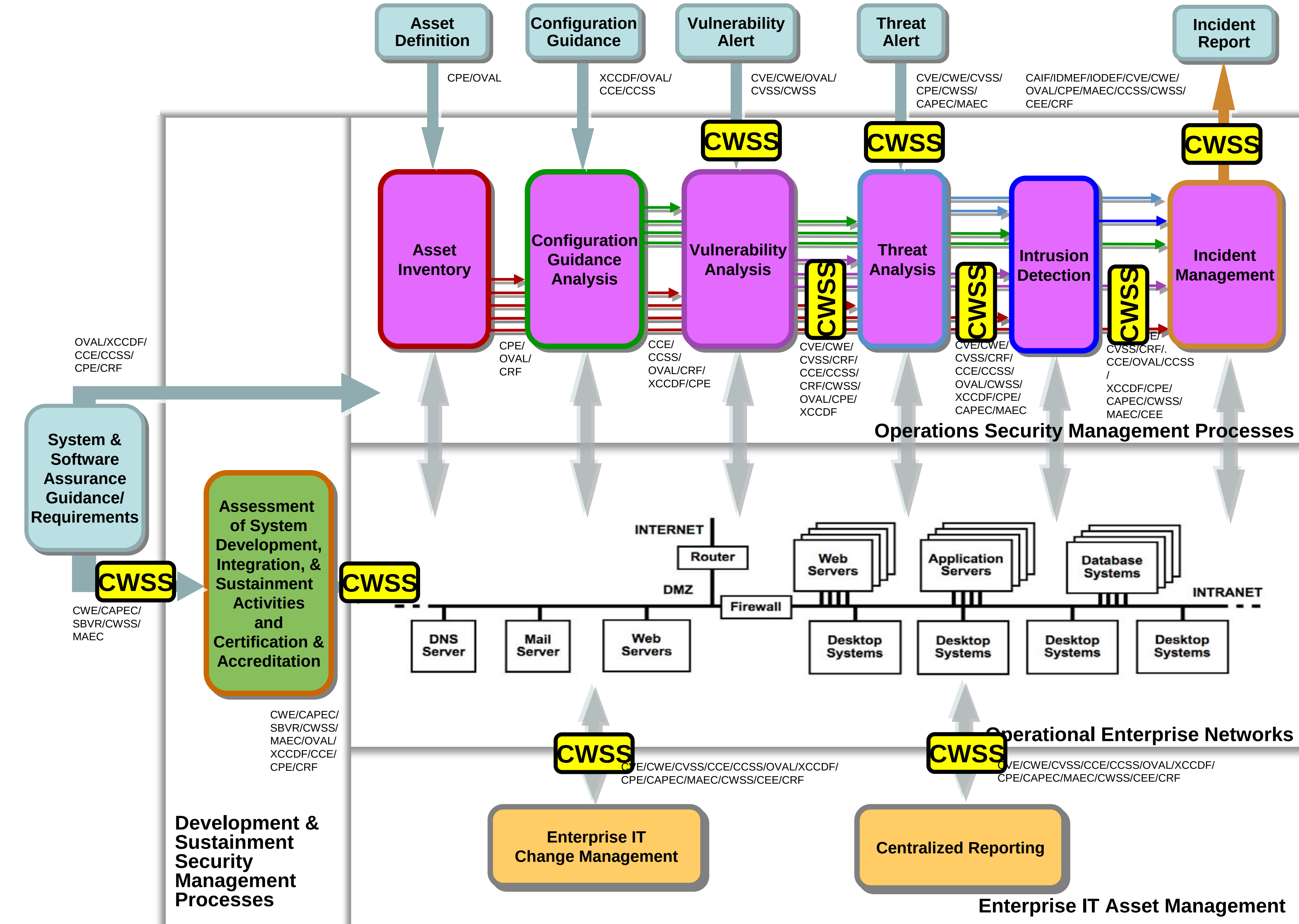
Development & Sustainment Security Management Processes

Enterprise IT Change Management

Centralized Reporting

Enterprise IT Asset Management

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/CRF

Incident Report

CWSS

CWSS

CWSS

Asset Inventory

CPE/
OVAL/
CRF

Configuration Guidance Analysis

CCE/
CCSS/
OVAL/CRF/
XCCDF/CPE

Vulnerability Analysis

CWSS

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

Threat Analysis

CWSS

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

Intrusion Detection

CWSS

E/
CVSS/CRF/.
CCE/OVAL/CCSS
/
XCCDF/CPE/
CAPEC/CWSS/
MAEC/CEE

Incident Management

OVAL/XCCDF/
CCE/CCSS/
CPE/CRF

Operations Security Management Processes

System & Software Assurance Guidance/ Requirements

CWSS

CWE/CAPEC/
SBVR/CWSS/
MAEC

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

CWSS

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/CRF

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

Operational Enterprise Networks

CWSS

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

CWSS

VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

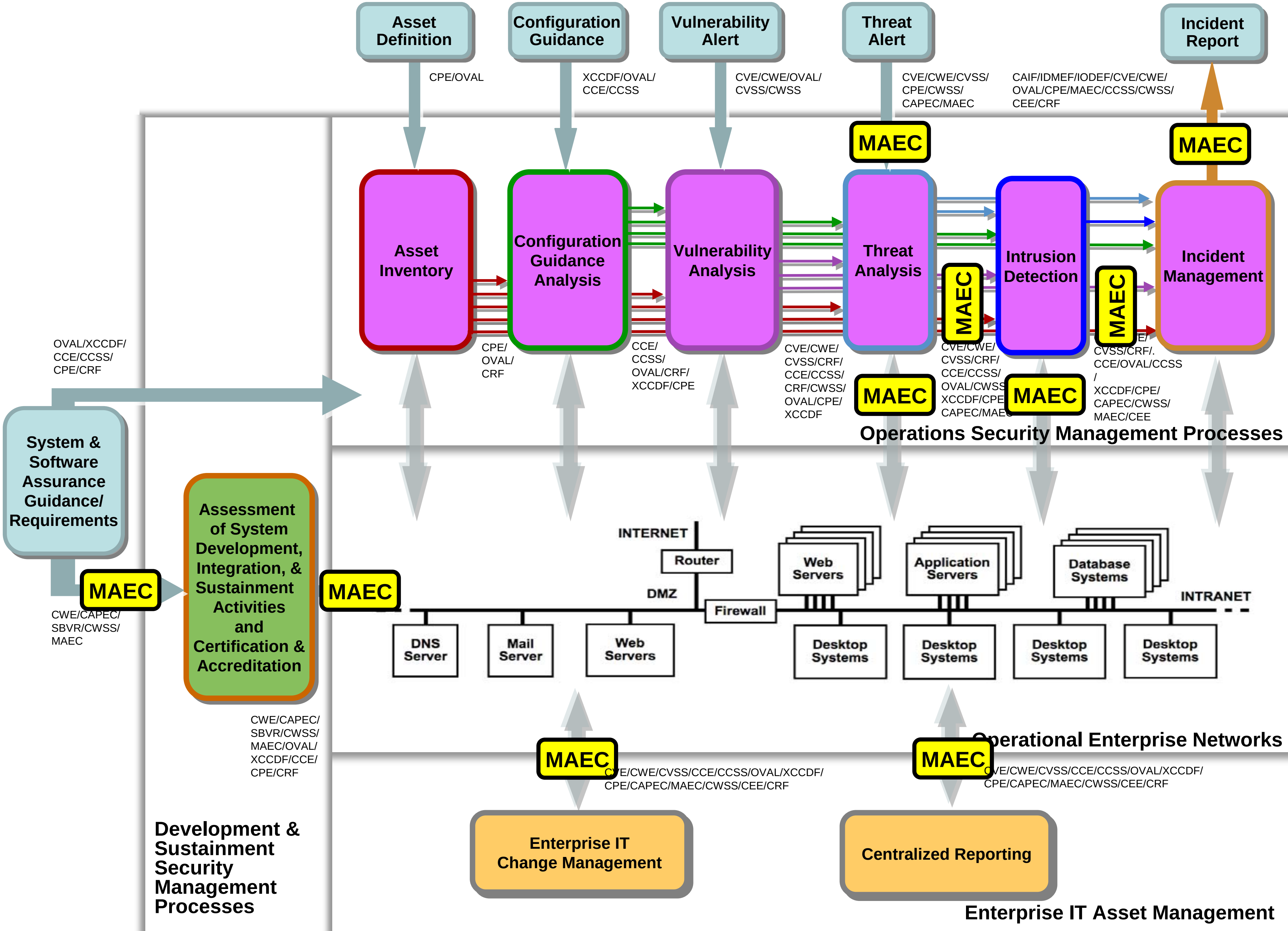
Development & Sustainment Security Management Processes

Enterprise IT Change Management

Centralized Reporting

Enterprise IT Asset Management

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/CRF

Incident Report

MAEC

MAEC

Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

Threat Analysis

Intrusion Detection

Incident Management

MAEC

MAEC

CPE/ OVAL/ CRF

CCE/ CCSS/ OVAL/CRF/ XCCDF/CPE

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

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

E/ CVSS/CRF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE

MAEC

MAEC

OVAL/XCCDF/ CCE/CCSS/ CPE/CRF

Operations Security Management Processes

System & Software Assurance Guidance/ Requirements

MAEC

CWE/CAPEC/ SBVR/CWSS/ MAEC

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

MAEC

CWE/CAPEC/ SBVR/CWSS/ MAEC/OVAL/ XCCDF/CCE/ CPE/CRF

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

Operational Enterprise Networks

MAEC

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

MAEC

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

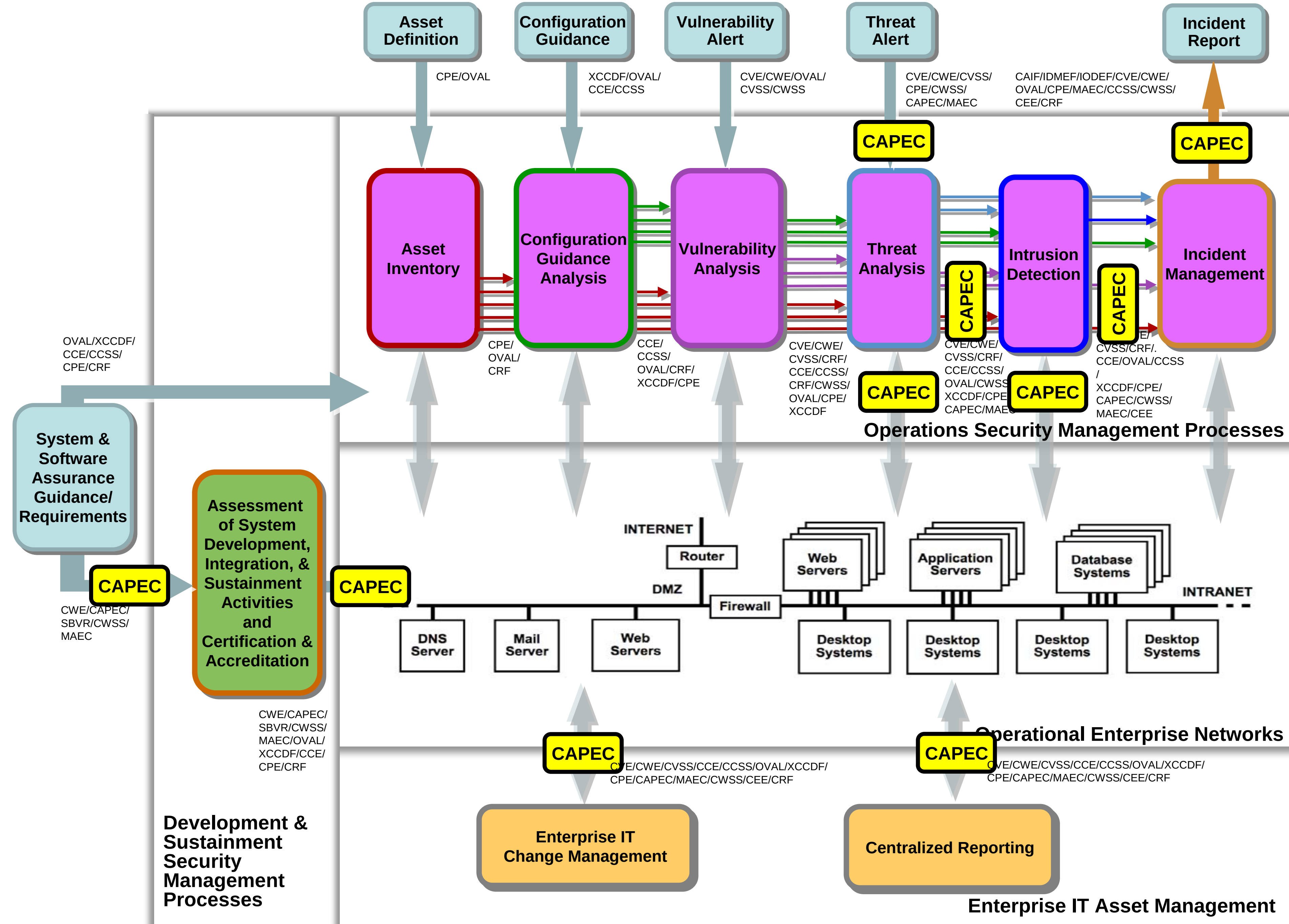
Development & Sustainment Security Management Processes

Enterprise IT Change Management

Centralized Reporting

Enterprise IT Asset Management

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

Incident Report
CAIF/IDMEF/IODEF/CVE/CWE/ OVAL/CPE/MAEC/CCSS/CWSS/ CEE/CRF

CAPEC

CAPEC

Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

Threat Analysis

Intrusion Detection

Incident Management

CAPEC

CAPEC

CPE/ OVAL/ CRF

CCE/ CCSS/ OVAL/CRF/ XCCDF/CPE

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

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

E/ CVSS/CRF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE

CAPEC

CAPEC

Operations Security Management Processes

OVAL/XCCDF/ CCE/CCSS/ CPE/CRF

System & Software Assurance Guidance/ Requirements

CAPEC

CWE/CAPEC/ SBVR/CWSS/ MAEC

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

CAPEC

CWE/CAPEC/ SBVR/CWSS/ MAEC/OVAL/ XCCDF/CCE/ CPE/CRF

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

Operational Enterprise Networks

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

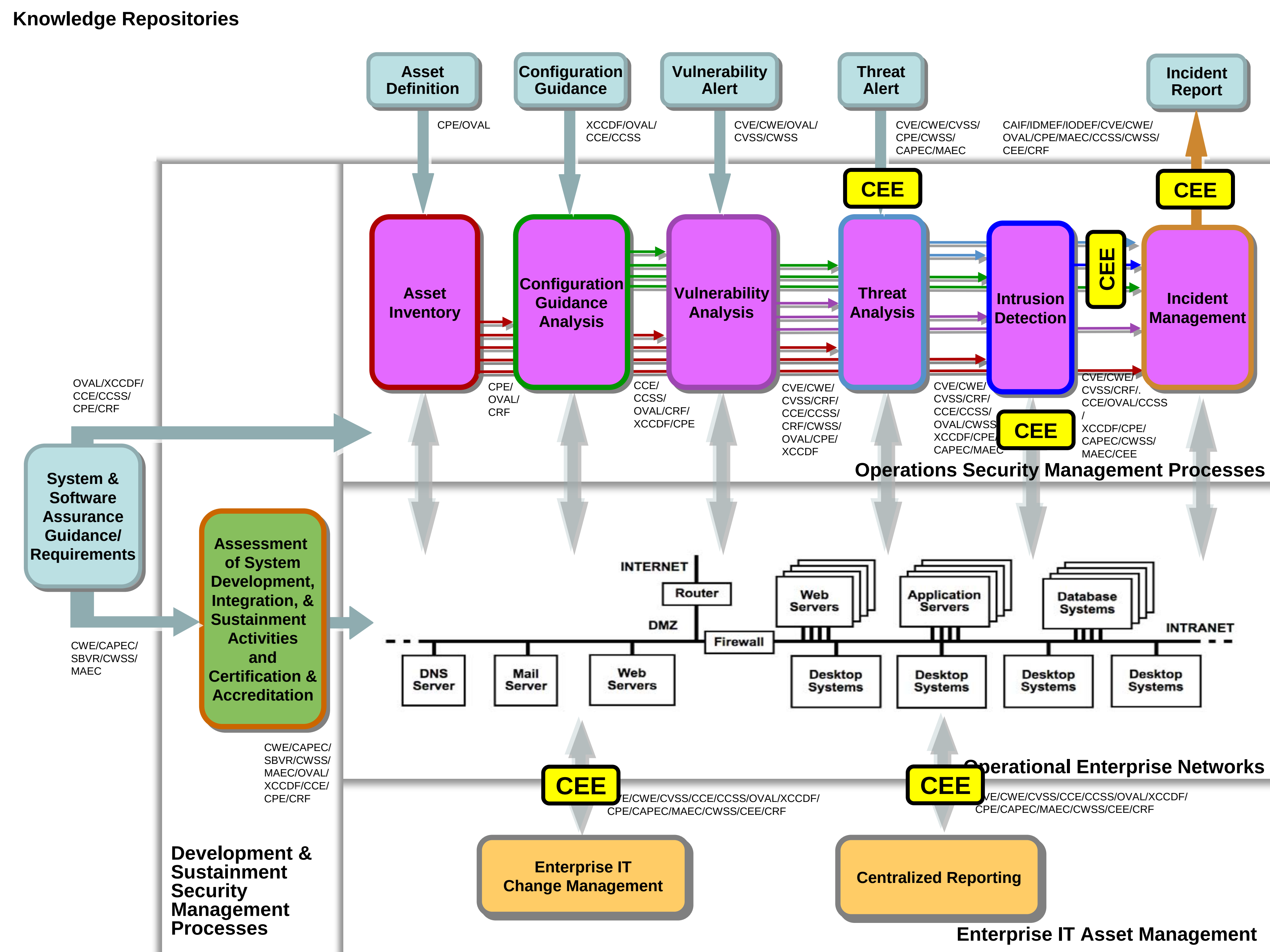
CAPEC
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/CRF

Enterprise IT Change Management

Centralized Reporting

Development & Sustainment Security Management Processes

Enterprise IT Asset Management



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

Incident Report

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

CEE

CEE

Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

Threat Analysis

Intrusion Detection

CEE

Incident Management

CPE/
OVAL/
CRF

CCE/
CCSS/
OVAL/CRF/
XCCDF/CPE

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

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

CEE

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

OVAL/XCCDF/
CCE/CCSS/
CPE/CRF

System & Software Assurance Guidance/ Requirements

CWE/CAPEC/
SBVR/CWSS/
MAEC

Operations Security Management Processes

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

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/CRF

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

Operational Enterprise Networks

CEE

VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

CEE

VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

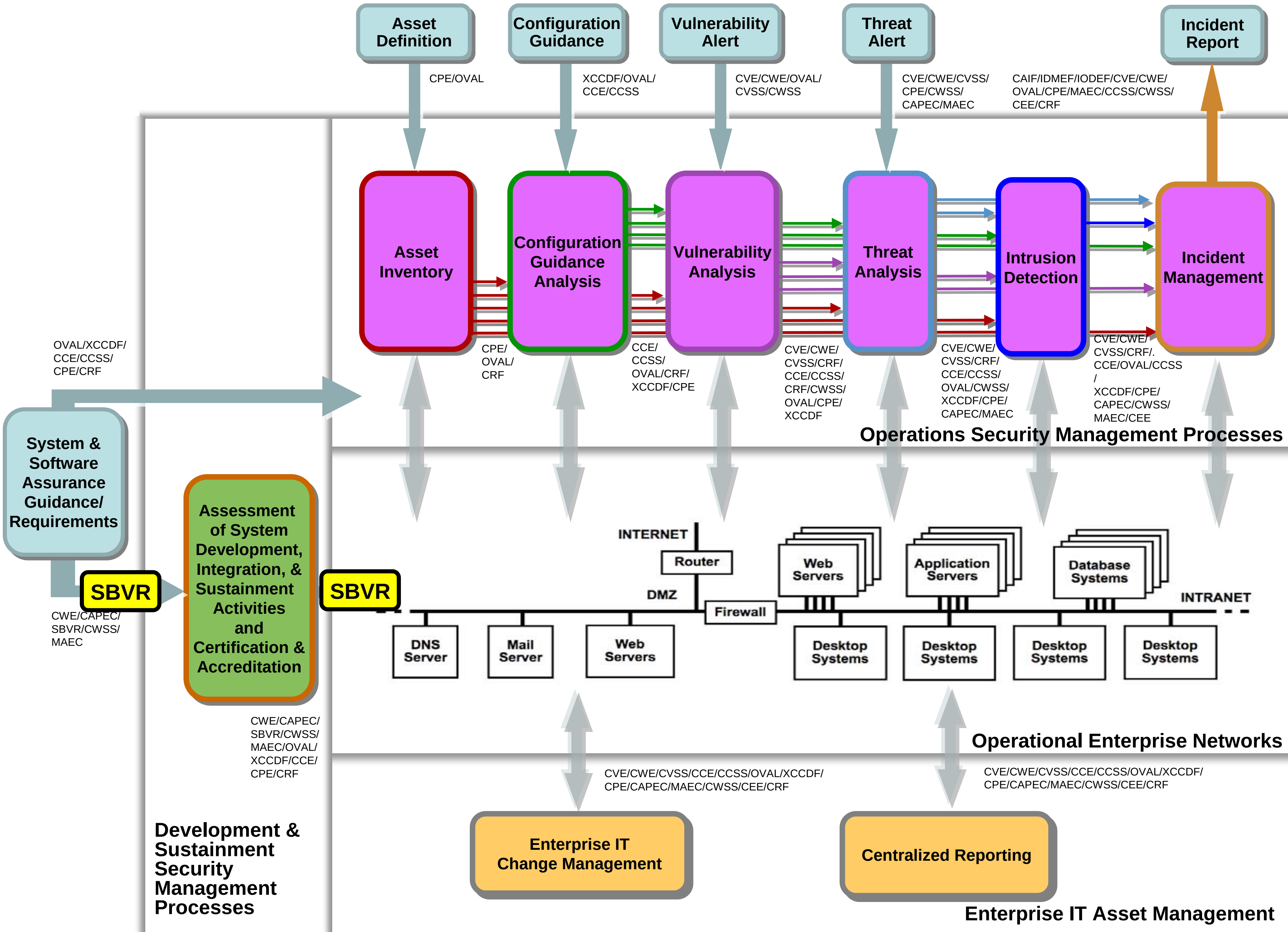
Development & Sustainment Security Management Processes

Enterprise IT Change Management

Centralized Reporting

Enterprise IT Asset Management

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/CRF

Incident Report

Asset Inventory

CPE/
OVAL/
CRF

Configuration Guidance Analysis

CCE/
CCSS/
OVAL/CRF/
XCCDF/CPE

Vulnerability Analysis

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

Threat Analysis

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

Intrusion Detection

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

Incident Management

Operations Security Management Processes

OVAL/XCCDF/
CCE/CCSS/
CPE/CRF

System & Software Assurance Guidance/ Requirements

SBVR

CWE/CAPEC/
SBVR/CWSS/
MAEC

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

SBVR

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/CRF

Operational Enterprise Networks

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

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

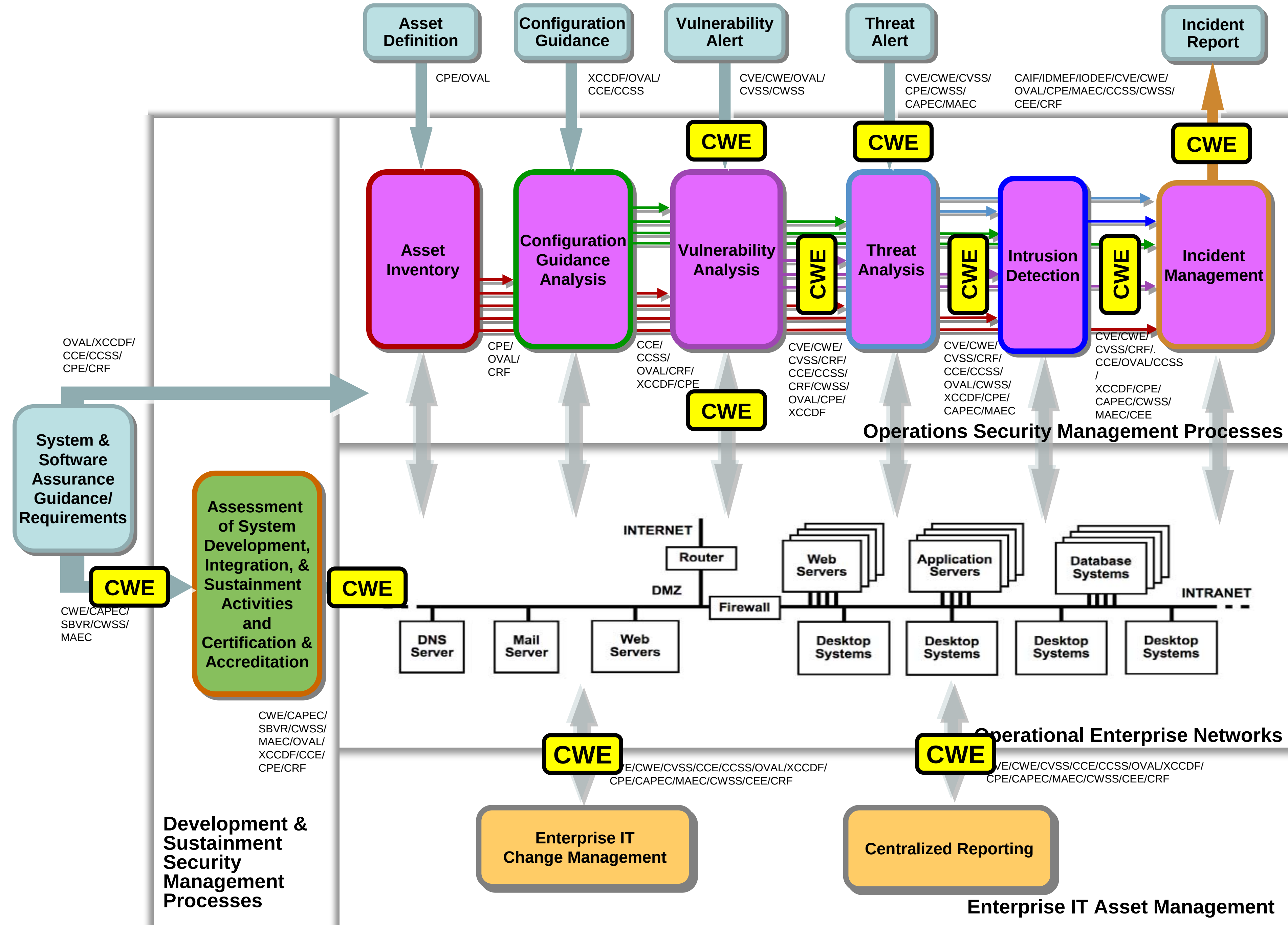
Development & Sustainment Security Management Processes

Enterprise IT Change Management

Centralized Reporting

Enterprise IT Asset Management

Knowledge Repositories



Asset Definition

Configuration Guidance

Vulnerability Alert

Threat Alert

Incident Report

CPE/OVAL

XCCDF/OVAL/
CCE/CCSS

CVE/CWE/OVAL/
CVSS/CWSS

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

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

CWE

CWE

CWE

Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

CWE

Threat Analysis

CWE

Intrusion Detection

CWE

Incident Management

OVAL/XCCDF/
CCE/CCSS/
CPE/CRF

CPE/
OVAL/
CRF

CCE/
CCSS/
OVAL/CRF/
XCCDF/CPE

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

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

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

CWE

Operations Security Management Processes

System & Software Assurance Guidance/ Requirements

CWE

CWE/CAPEC/
SBVR/CWSS/
MAEC

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

CWE

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/CRF

Operational Enterprise Networks

CWE

E/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

CWE

VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

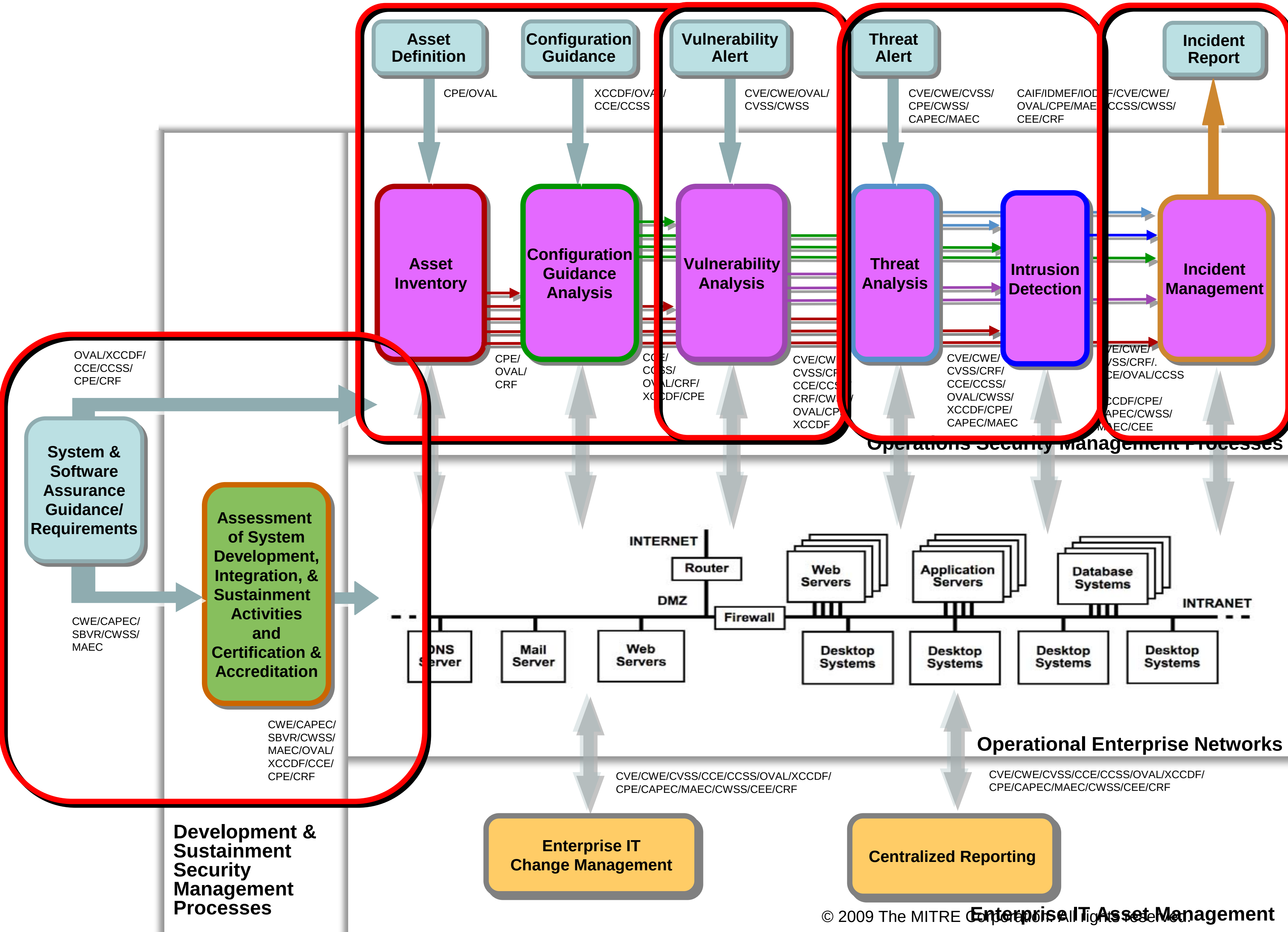
Enterprise IT Change Management

Centralized Reporting

Development & Sustainment Security Management Processes

Enterprise IT Asset Management

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/CRF

Incident Report

Asset Inventory

Configuration Guidance Analysis

Vulnerability Analysis

Threat Analysis

Intrusion Detection

Incident Management

CPE/
OVAL/
CRF

CCE/
CCSS/
OVAL/CRF/
XCCDF/CPE

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

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

CVE/CWE/
CVSS/CRF/.
CCE/OVAL/CCSS

XCCDF/CPE/
CAPEC/CWSS/
MAEC/CEE

Operations Security Management Processes

OVAL/XCCDF/
CCE/CCSS/
CPE/CRF

System & Software Assurance Guidance/ Requirements

CWE/CAPEC/
SBVR/CWSS/
MAEC

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

CWE/CAPEC/
SBVR/CWSS/
MAEC/OVAL/
XCCDF/CCE/
CPE/CRF

Operational Enterprise Networks

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

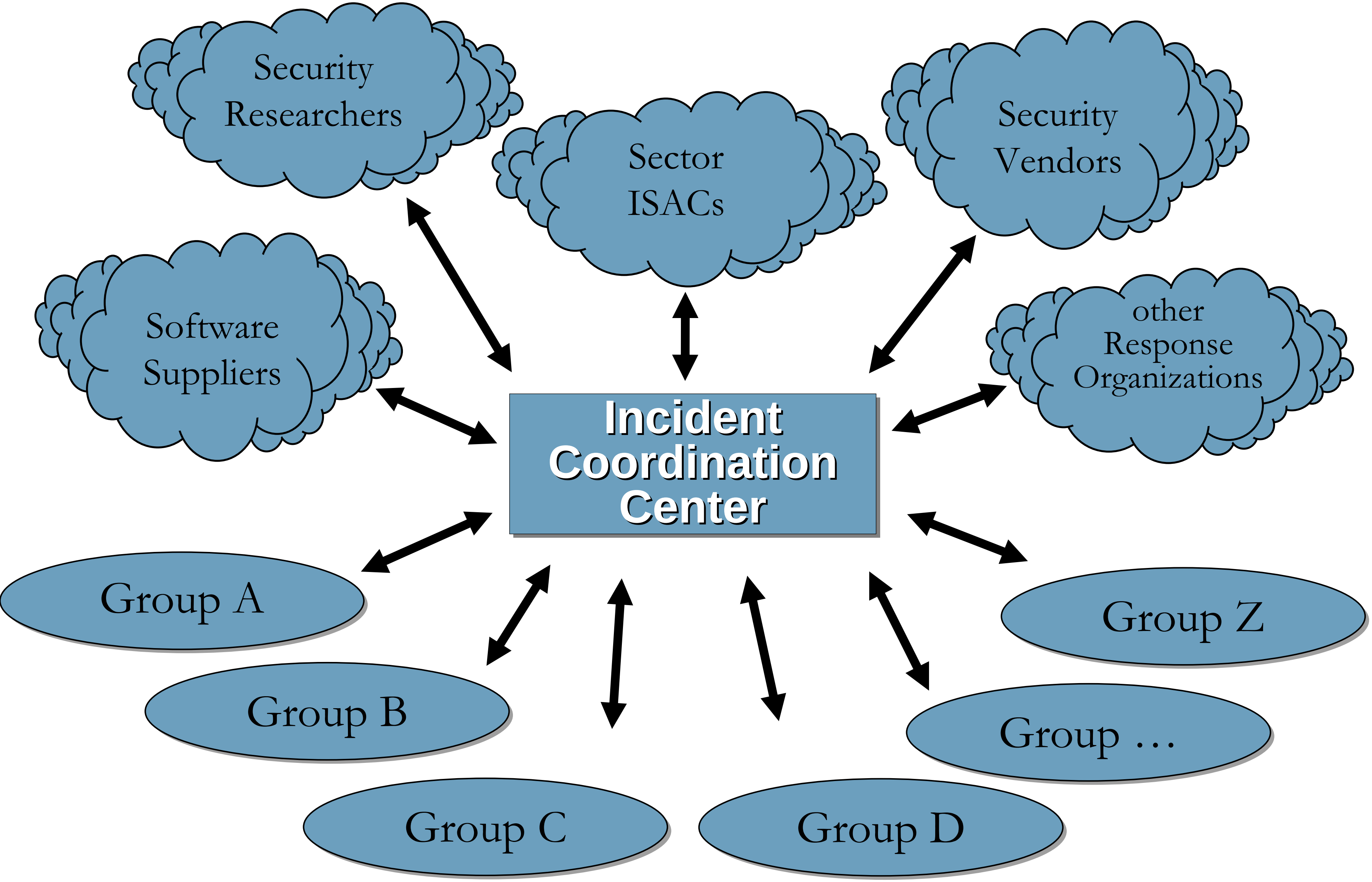
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/
CPE/CAPEC/MAEC/CWSS/CEE/CRF

Development & Sustainment Security Management Processes

Enterprise IT Change Management

Centralized Reporting

Enterprise IT Asset Management



Security Researchers

Sector ISACs

Security Vendors

Software Suppliers

other Response Organizations

Incident Coordination Center

Group A

Group B

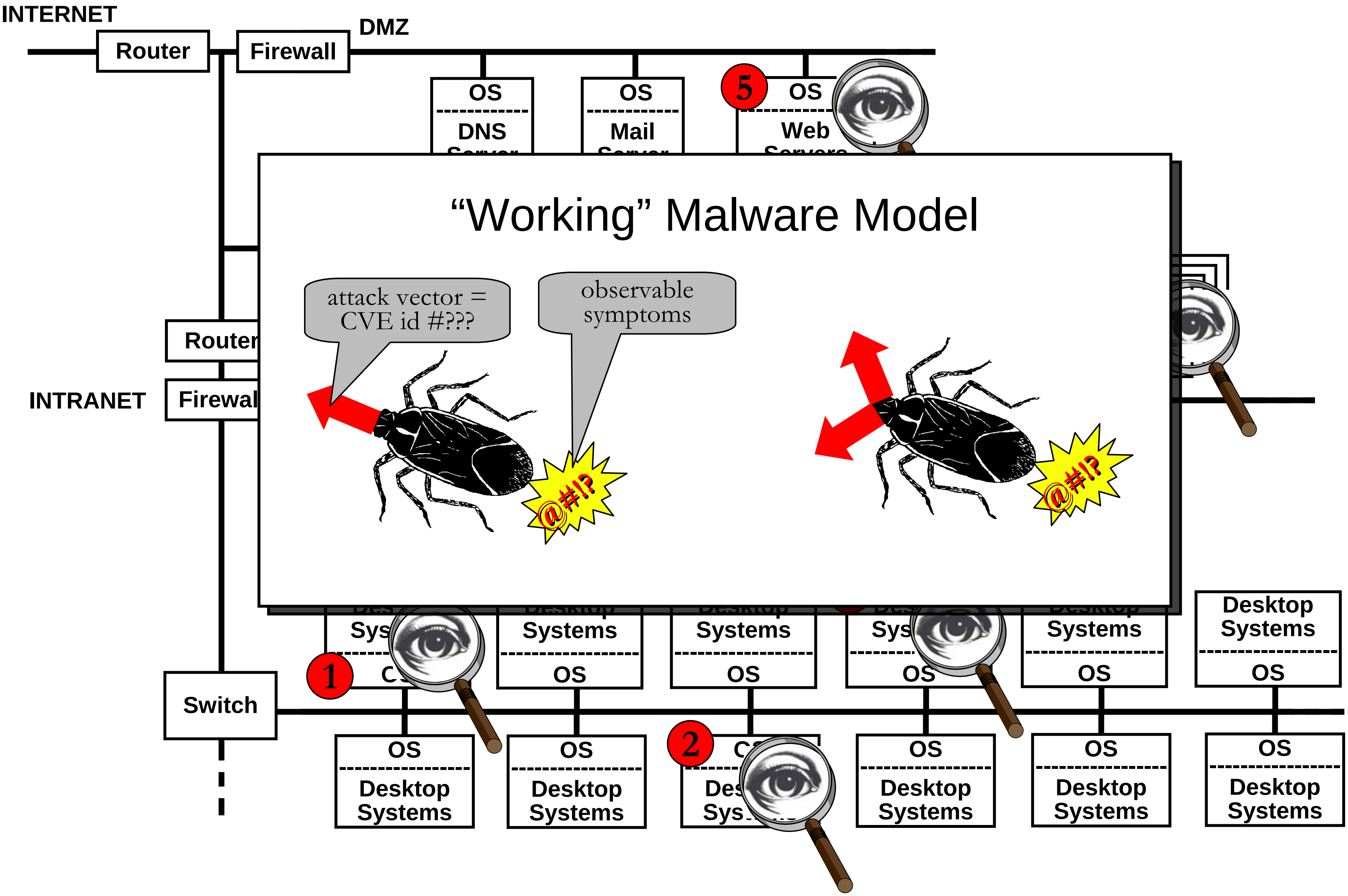
Group C

Group D

Group …

Group Z

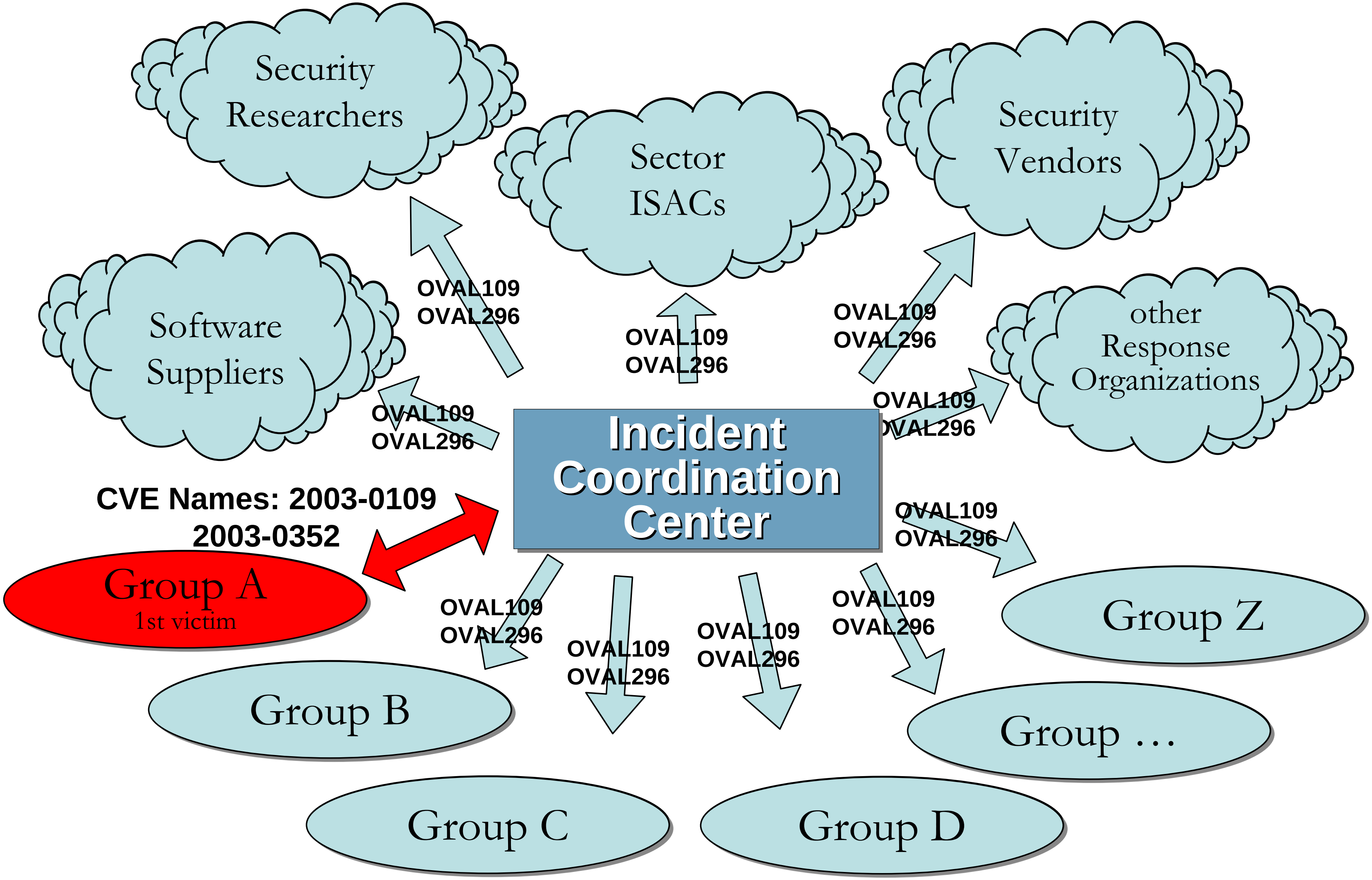
“Working” Malware Model



“Group A” Network

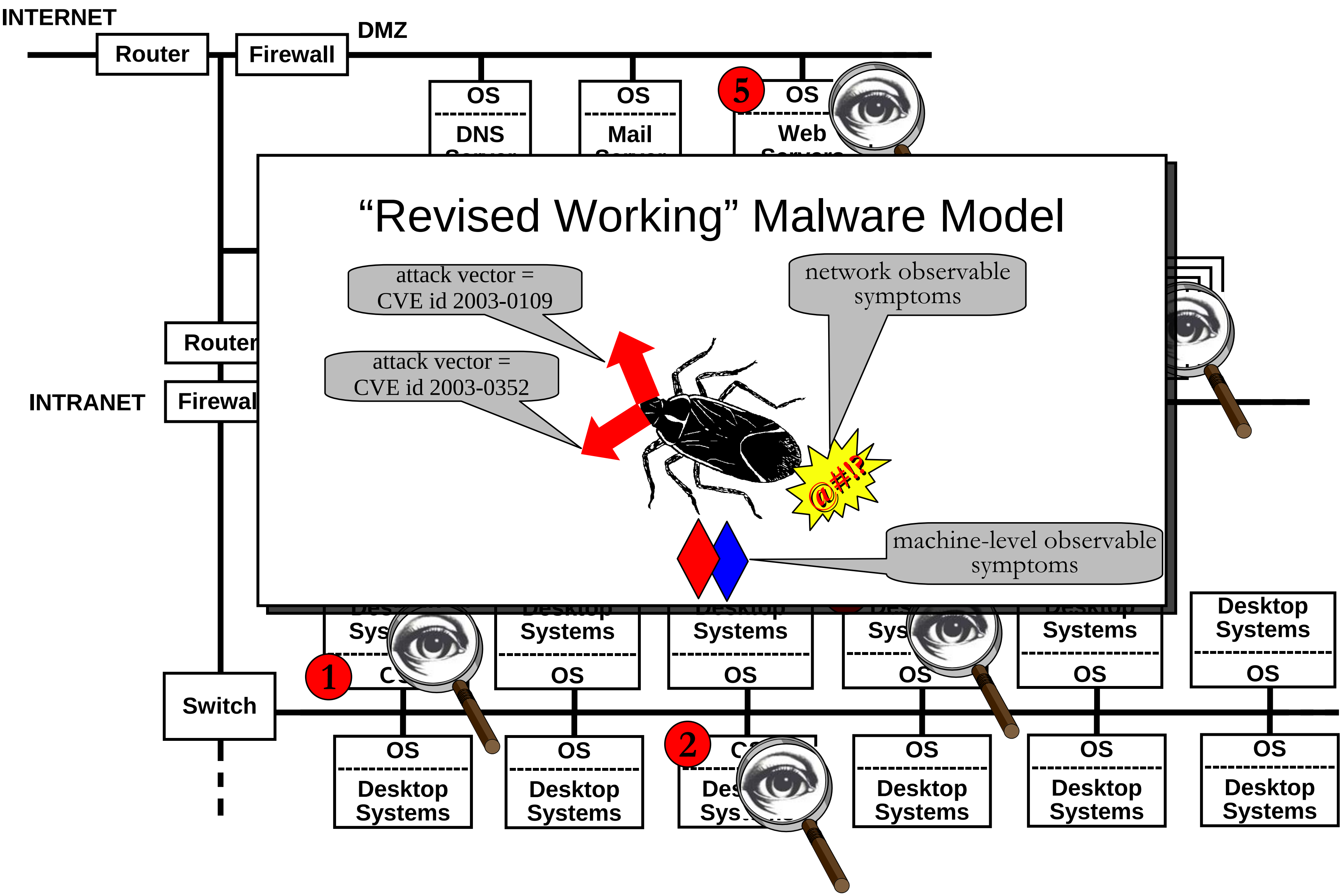
First Level Vulnerability Examination Results

	CVE Name: 2003-0109 OVAL109	CVE Name: 2003-0352 OVAL296	CVE Name: 2003-0223 OVAL66	CVE Name: 2003-0228 OVAL321	CVE Name: 2003-0660 OVAL198
System 1 10.0.0.121	**no**	**yes**	**no**	**yes**	**yes**
System 2 10.0.0.122	**no**	**yes**	**no**	**no**	**no**
System 3 10.0.0.123	**no**	**yes**	**no**	**yes**	**no**
System 4 10.0.1.124	**yes**	**no**	**yes**	**no**	**yes**
System 5 10.0.2.125	**yes**	**no**	**no**	**no**	**no**



Security Researchers
Sector ISACs
Security Vendors
Software Suppliers
other Response Organizations
OVAL109 OVAL296
OVAL109 OVAL296
OVAL109 OVAL296
OVAL109 OVAL296
OVAL109 OVAL296
Incident Coordination Center
CVE Names: 2003-0109 2003-0352
Group A
1st victim
OVAL109 OVAL296
OVAL109 OVAL296
OVAL109 OVAL296
OVAL109 OVAL296
OVAL109 OVAL296
Group Z
Group B
Group …
Group C
Group D

“Revised Working” Malware Model



INTERNET

Router

Firewall

DMZ

OS

DNS

OS

Mail

5

OS

Web

Router

Firewall

INTRANET

Switch

1

2

Desktop Systems

OS

attack vector = CVE id 2003-0109

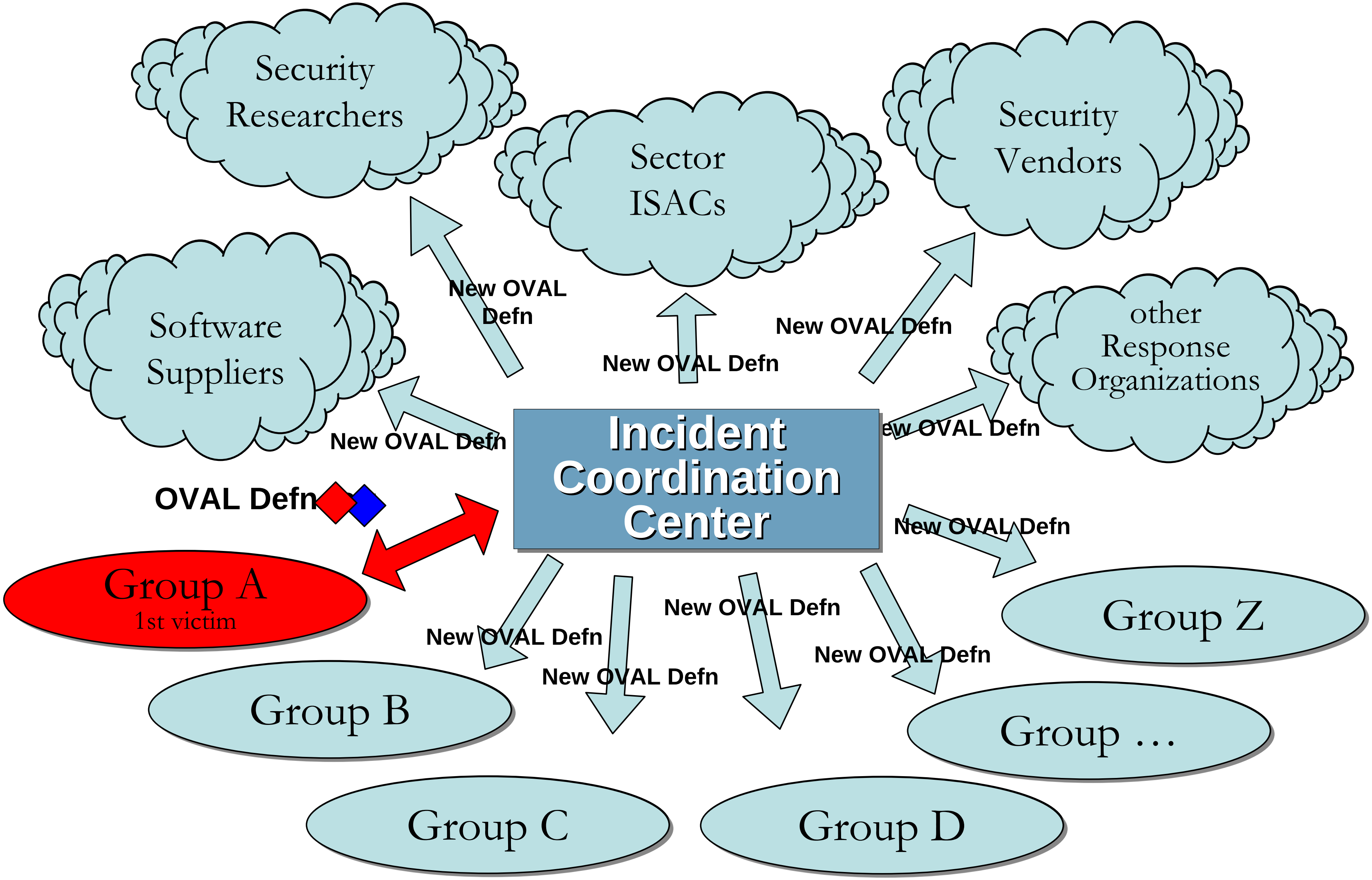
attack vector = CVE id 2003-0352

network observable symptoms

@#!?

machine-level observable symptoms

“Group A” Network



Security Researchers

Sector ISACs

Security Vendors

Software Suppliers

other Response Organizations

New OVAL Defn

New OVAL Defn

New OVAL Defn

New OVAL Defn

New OVAL Defn

ew OVAL Defn

Incident Coordination Center

OVAL Defn

Group A
1st victim

New OVAL Defn

New OVAL Defn

New OVAL Defn

New OVAL Defn

New OVAL Defn

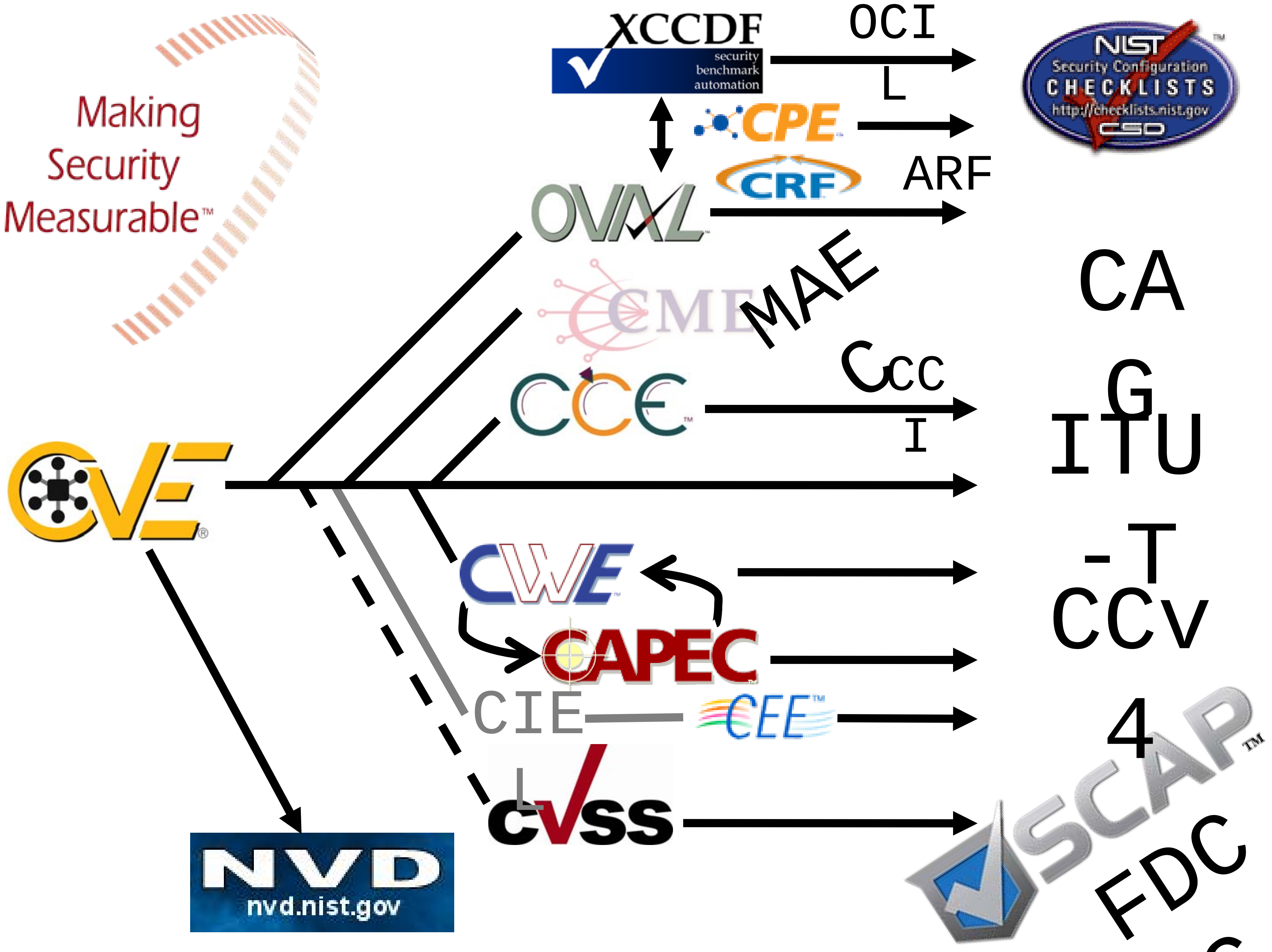
Group Z

Group B

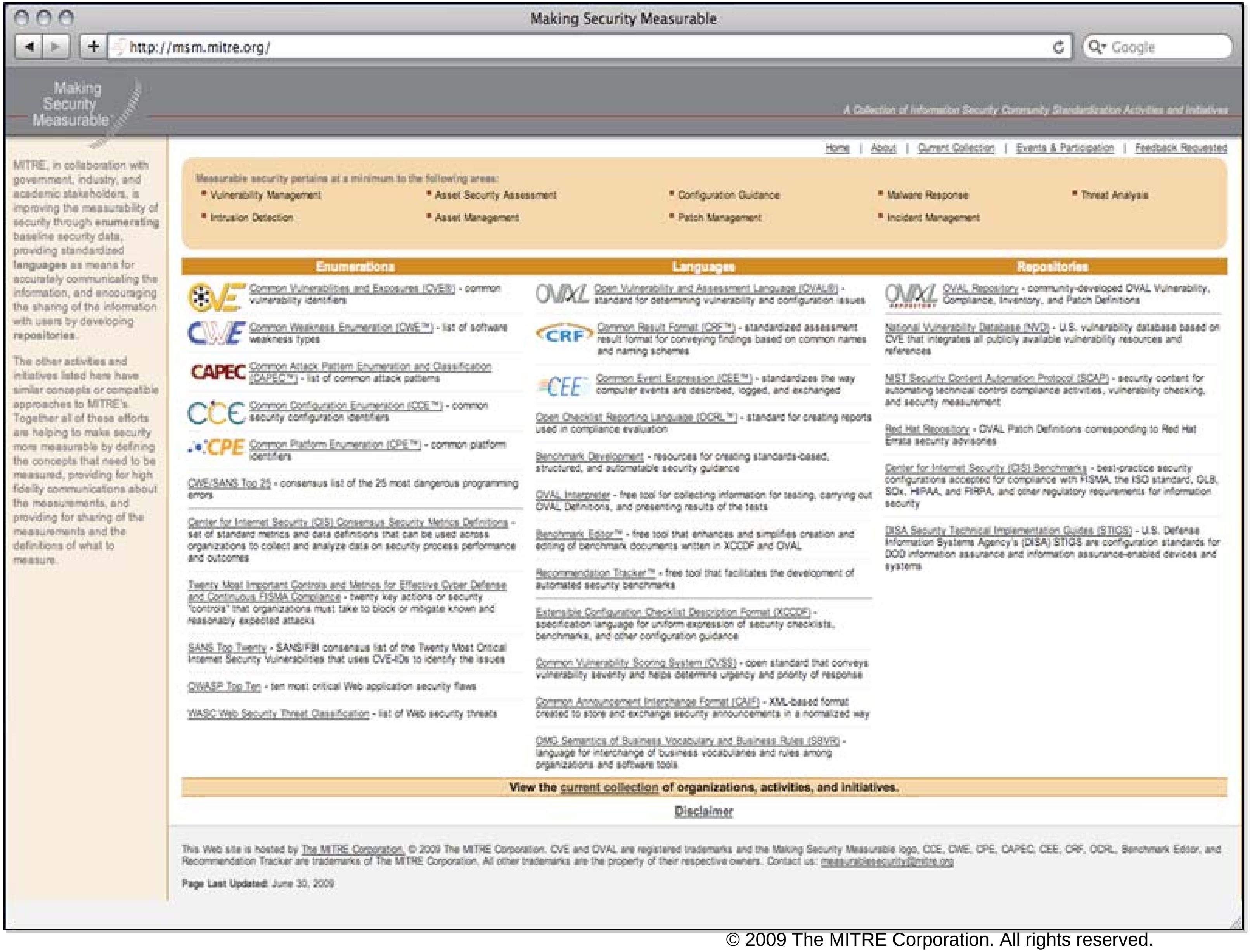
Group …

Group C

Group D


Making
Security
Measurable™
XCCDF
security benchmark automation
OCI
L
NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD
CPE
CRF
ARF
OVAL
CME
MAE
CA
G
CCE
Ccc
I
ITU
-T
CVE
CWE
CCv
CAPEC
CIE
CEE™
4
SCAP™
L
cvss
NVD
nvd.nist.gov
FDC
C

[makingsecuritymeasurable.mitre.org]



A Collection of Information Security Community Standardization Activities and Initiatives

Home | About | Current Collection | 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
- Asset Security Assessment
- Configuration Guidance
- Malware Response
- Threat Analysis
- Intrusion Detection
- Asset Management
- Patch Management
- Incident Management

Enumerations

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

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

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

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

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

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

Common Result Format (CRF™) - standardized assessment result format for conveying findings based on common names and naming schemes

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

Open Checklist Reporting Language (OCRL™) - standard for creating reports used in compliance evaluation

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

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

Common Announcement Interchange Format (CAIF) - XML-based format created to store and exchange security announcements in a normalized way

OMG Semantics of Business Vocabulary and Business Rules (SBVR) - language for interchange of business vocabularies and rules among organizations and software tools

Repositories

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

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

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

Disclaimer

This Web site is hosted by The MITRE Corporation. © 2009 The MITRE Corporation. CVE and OVAL are registered trademarks and the Making Security Measurable logo, CCE, CWE, CPE, CAPEC, CEE, CRF, OCRL, 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: June 30, 2009

Making Security Measurable

Questions?