



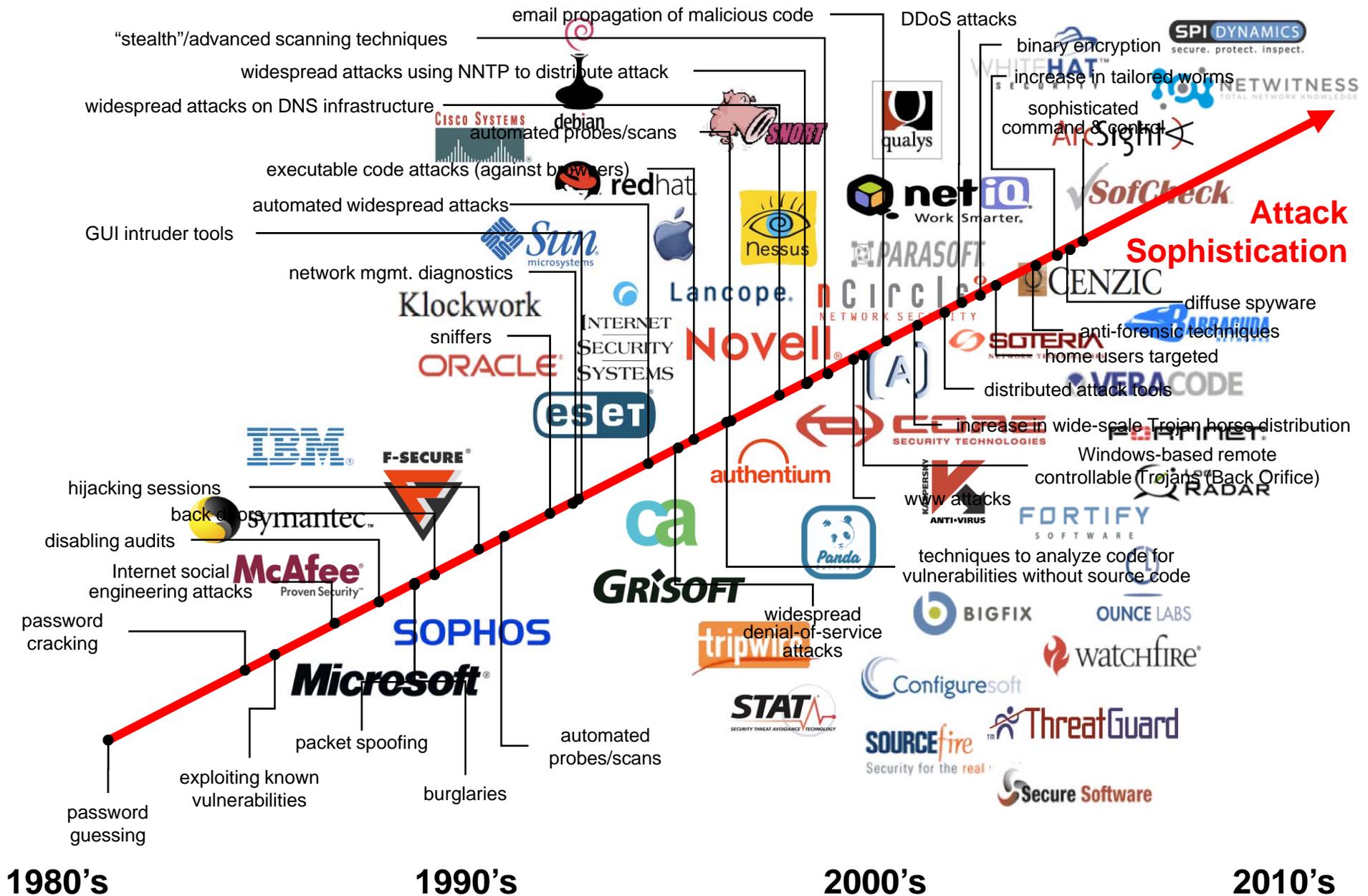
“Making Security Measurable”



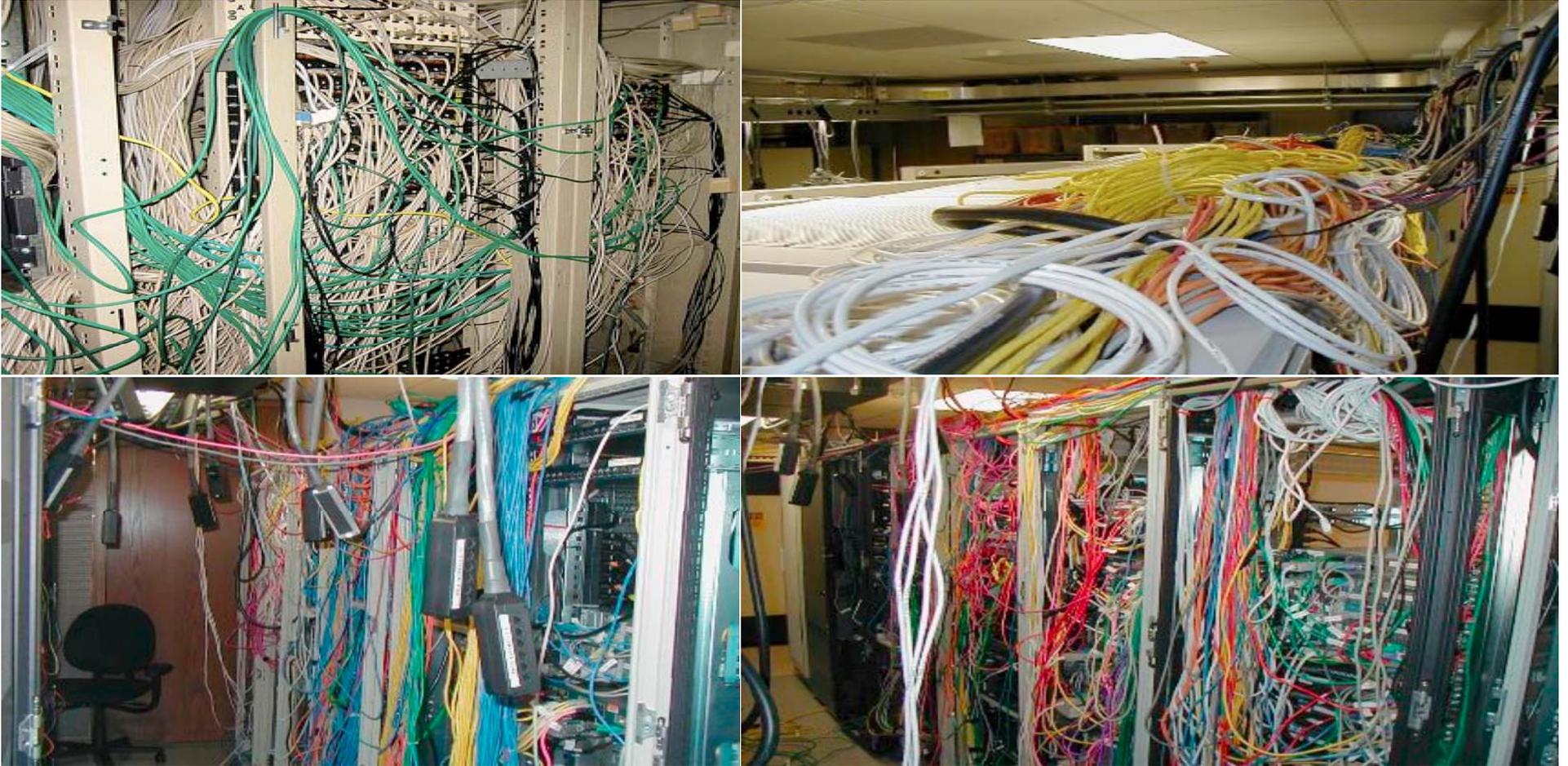
Homeland
Security

MITRE

Solutions Also Emerged Over Time



Like Security - Networks Evolved

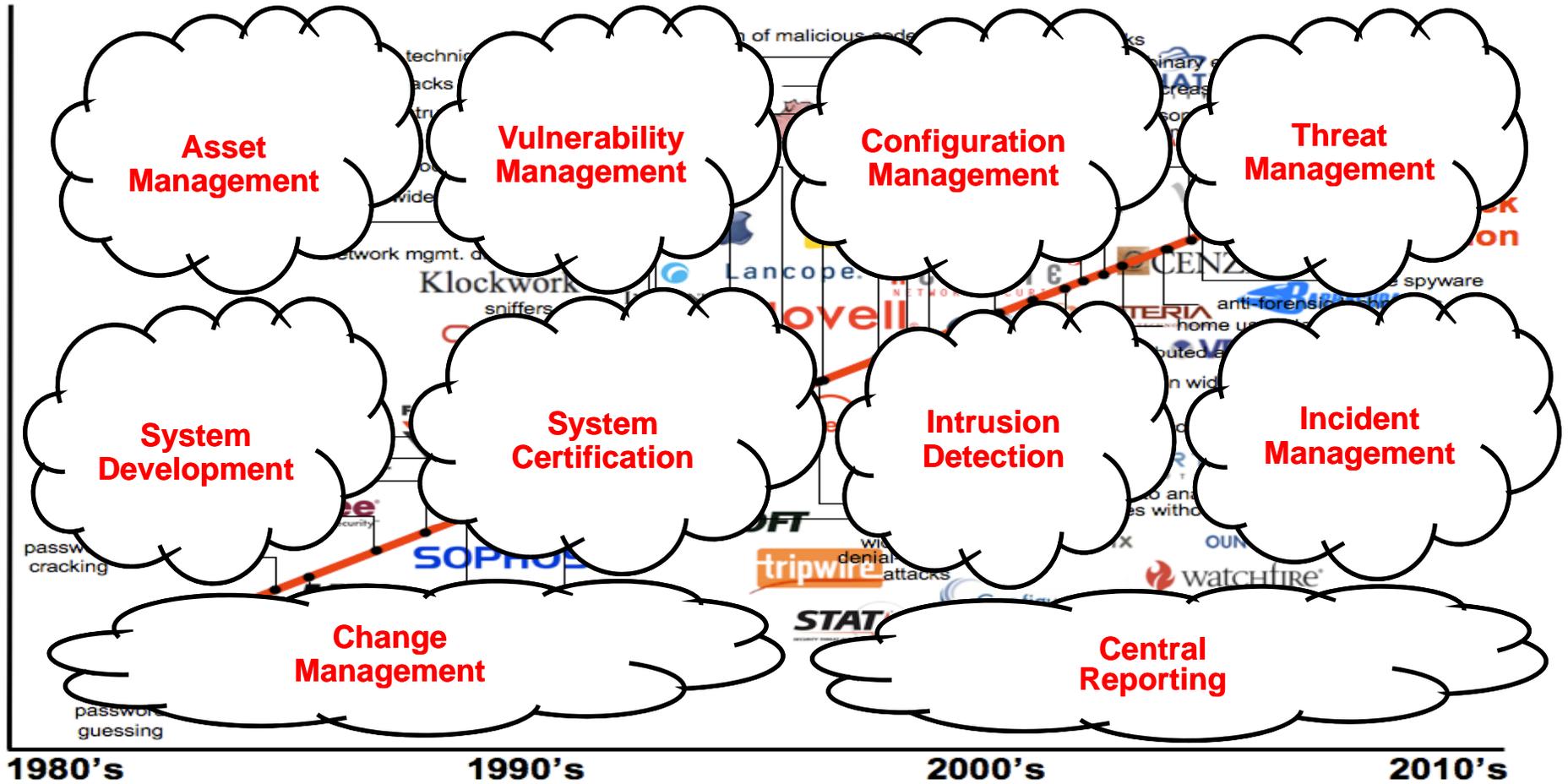


Each new solution had to integrate with the existing solutions -->> every enterprise ends up with a “unique” tapestry of solutions

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



Architecting Security



Making Security Measurable™

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



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/NWD), 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:



OVAL

NIST/DHS NVD



Knowledge Repository

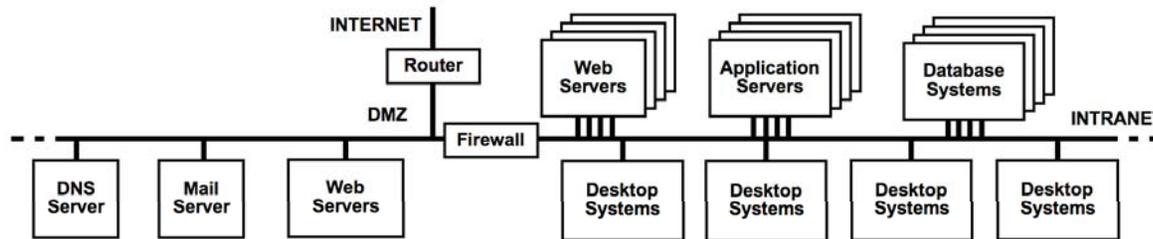
Knowledge Repositories

Vulnerability Alerts

Vulnerability Analysis

Operations Security Management Processes

Operational Enterprise Networks



Enterprise IT Asset Management

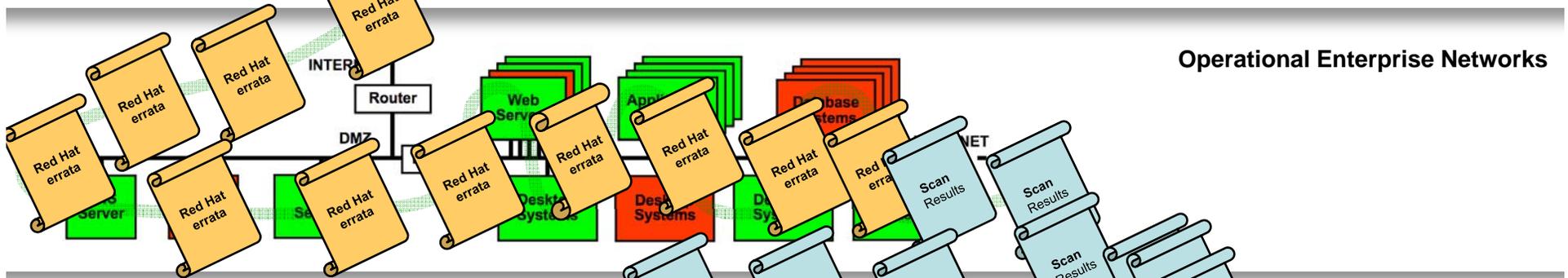
Enterprise IT Change Management

Centralized Reporting

Knowledge Repositories



Operations Security Management Processes



Operational Enterprise Networks

Enterprise IT Asset Management



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, CISE Benchmarks, NSA Configuration Guides, DISA STIGS), asset inventory (NIST/DHS NWD), 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
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

M-07-18

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

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

SUBJECT: Ensuring the security of information systems

August 11, 2008

MEMORANDUM FOR THE CHIEF INFORMATION OFFICERS

FROM: 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/fdccc/download_fdccc.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

The Office of Management and Budget (OMB) Memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," which stated: "agencies and/or plans to upgrade to these configurations by February 1, 2008."

This memorandum provides information technology providers with information to ensure new acquisitions and configurations provide the necessary security settings. Your agency must:

- The provider of information technology must ensure that the software and hardware configurations are set up to operate correctly and securely. For Windows XP and Vista, see: <http://csrc.nist.gov> for more information on security settings, see: <http://fdcc.nist.gov>
- The standard installation of software shall not alter the configuration. The information technology provider shall ensure that the software is installed and updated silently install and update.
- Applications designed to be installed and updated without elevated system privileges.

Guidance

Knowledge Repository

National Checklist Program

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

NIST National Institute of Standards and Technology

National Vulnerability Database

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

View all by category:

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

View only SCAP and FDCC subsets of the checklist repository:

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

Recent Updates (includes updates from the last 6 months)

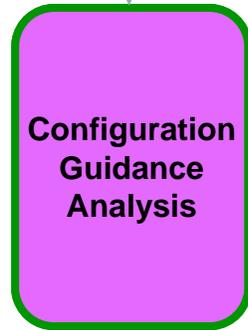
The symbol denotes newly added checklists
The symbol denotes updated checklists.

02/20/2008	<ul style="list-style-type: none"> SCAP Configuration Content - DISA Windows 2000 Security Checklist SCAP Configuration Content - Red Hat Enterprise Linux SCAP Configuration Content - Solaris 10 SCAP OVAL Patches - Microsoft Windows 2000 SCAP OVAL Patches - Red Hat Enterprise Linux
02/19/2008	<ul style="list-style-type: none"> Prose Guide - Solaris Benchmark (Solaris 10) Prose Guide - Windows 2000 Security Checklist
01/30/2008	<ul style="list-style-type: none"> FDCC Prose Guide - IET FDCC Prose Guide - Windows Vista FDCC Prose Guide - Windows Vista Firewall FDCC Prose Guide - Windows XP FDCC Prose Guide - Windows XP Firewall FDCC Prose Guide - Windows XP Firewall, Enterprise, and Specialized Security Benchmark Consensus Security Settings for Domain Controllers Windows Server 2003 Operating System Legacy, Enterprise, and Specialized Security Benchmark Consensus Security Settings for Domain Member Servers
01/18/2008	<ul style="list-style-type: none"> FDCC Group Policy Objects - IET FDCC Group Policy Objects - Windows Vista FDCC Group Policy Objects - Windows Vista Firewall FDCC Group Policy Objects - Windows XP FDCC SCAP Configuration Content - IET 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 - IET FDCC SCAP OVAL Patches - Windows Vista FDCC SCAP OVAL Patches - Windows Vista Firewall FDCC SCAP OVAL Patches - Windows XP FDCC SCAP OVAL Patches - Windows XP Firewall OS/390 Security Technical Implementation Guide Prose Guide - NIST SP 800-53 Prose Guide - Windows Vista Security Guide SCAP Configuration Content - NIST SP 800-43 SCAP Configuration Content for Domain Controllers - Windows Server 2003 SCAP Configuration Content for Member Servers - Windows Server 2003 SCAP OVAL Patches - Windows Server 2003
01/16/2008	<ul style="list-style-type: none"> Prose Guide - DISA Checklist Prose Guide - NIST SP 800-43 Prose Guide - NSA Guide Prose Guide - Windows Server 2003 SCAP Configuration Content - DISA Checklist

DFCS security benchmark automation

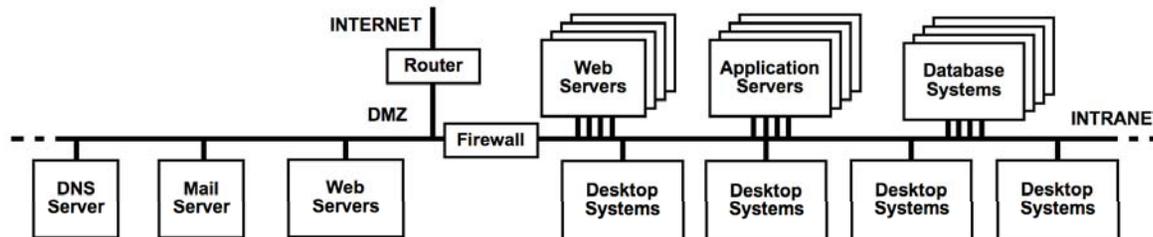
oval.mitre.org

Knowledge Repositories



Operations Security Management Processes

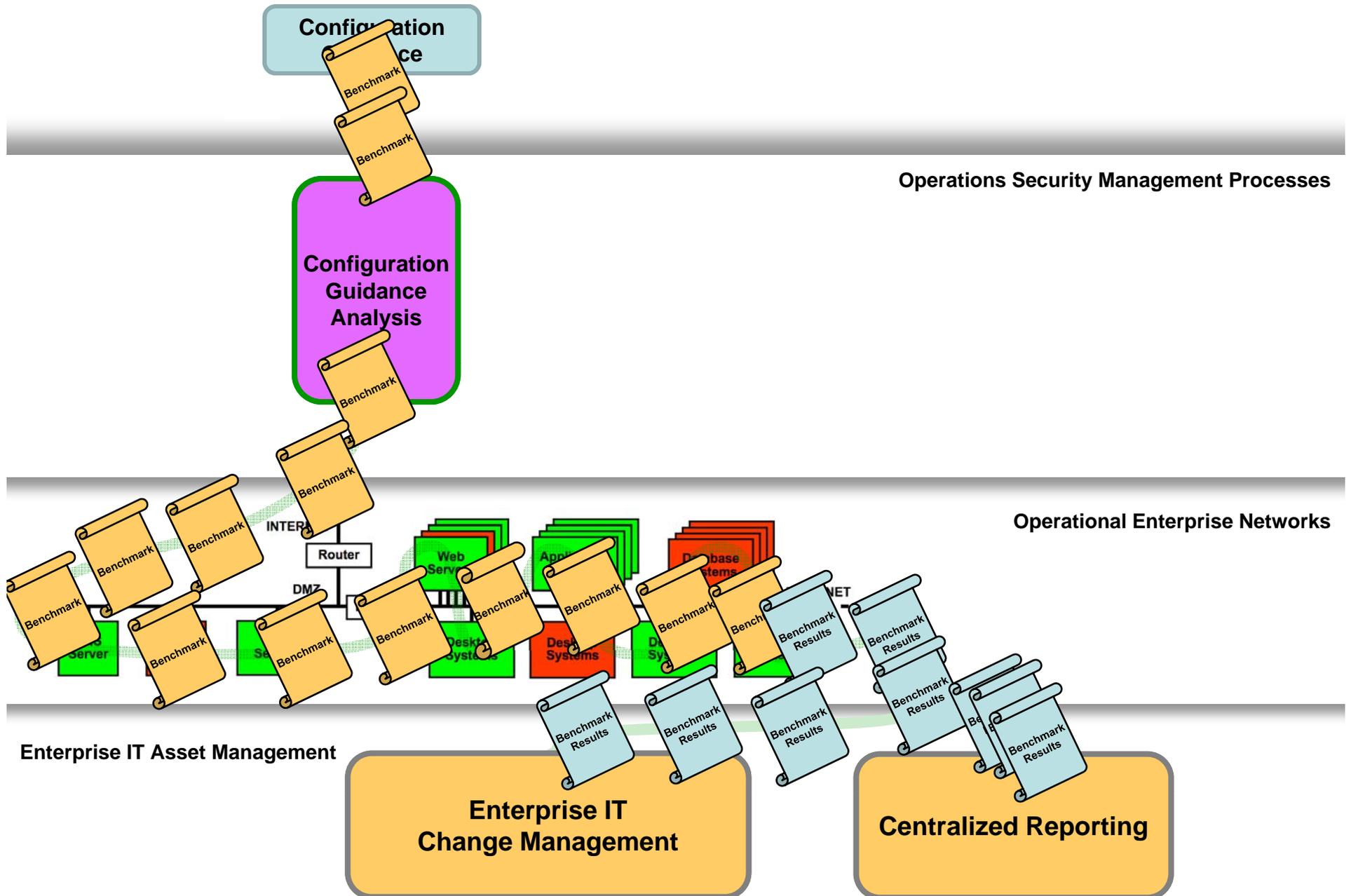
Operational Enterprise Networks



Enterprise IT Asset Management



Knowledge Repositories



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 (~~SBWR~~), event patterns (CEE), malware patterns (~~MAPEC~~), risk of a vulnerability (~~CVSS~~), config risk (~~CCSS~~), weakness risk (~~CMSS~~), 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 & eWASS~~)

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:



CPE
CIS

CAPEC

CCE

SE

SS

CRF

XCCDF & OVAL

MAEC

CCSS

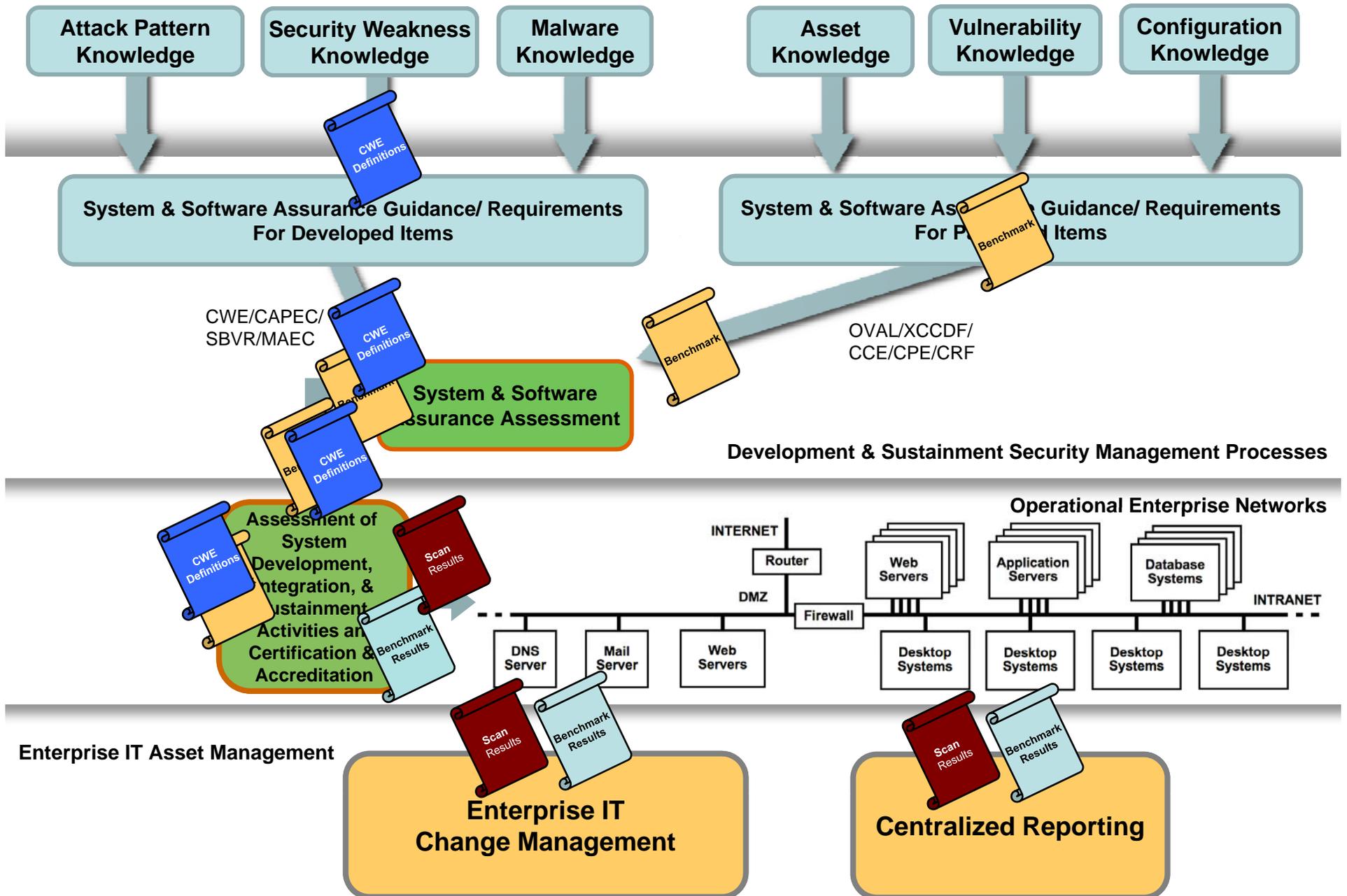
CWSS

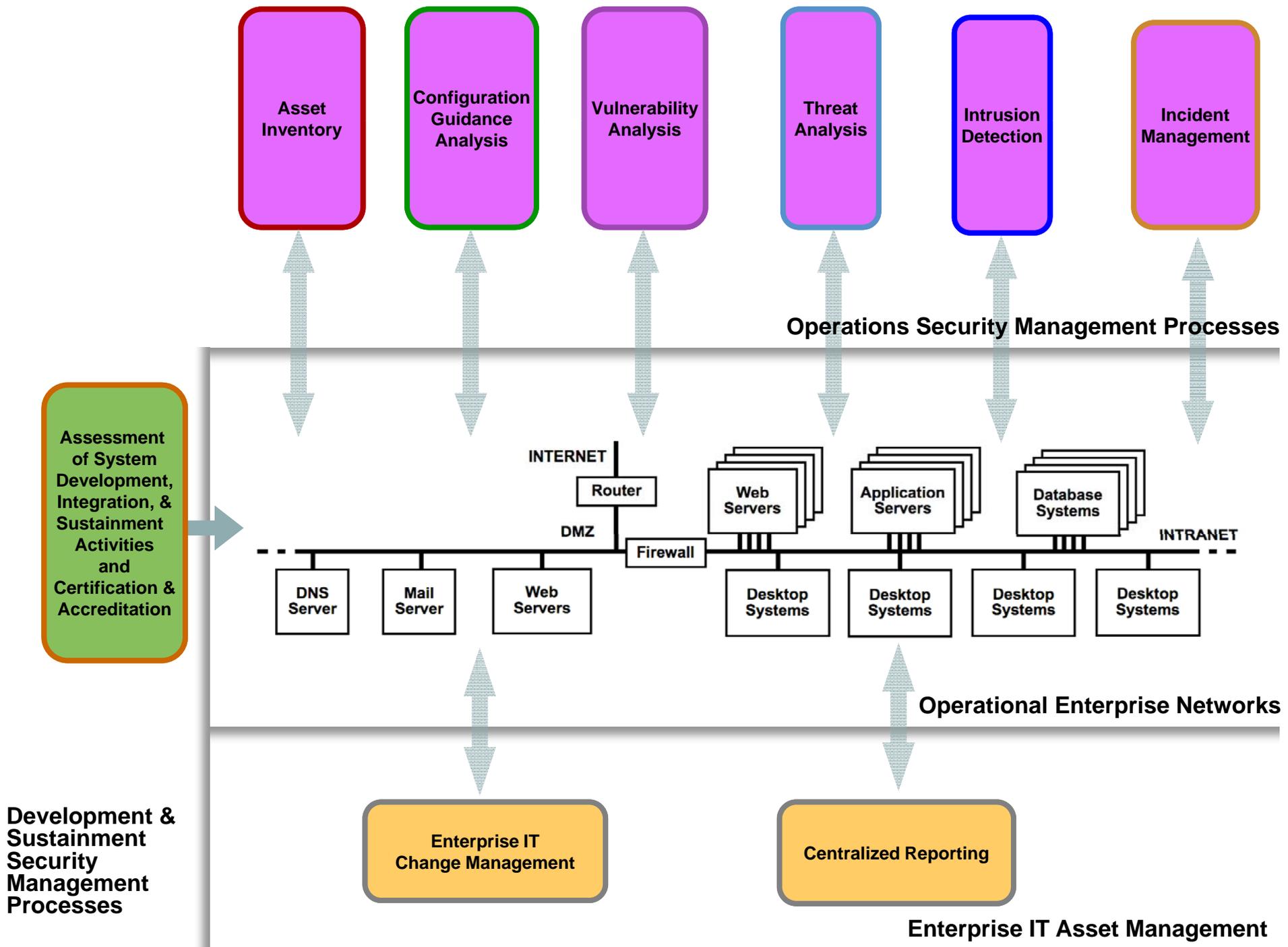
DoD DIACAP & eMASS

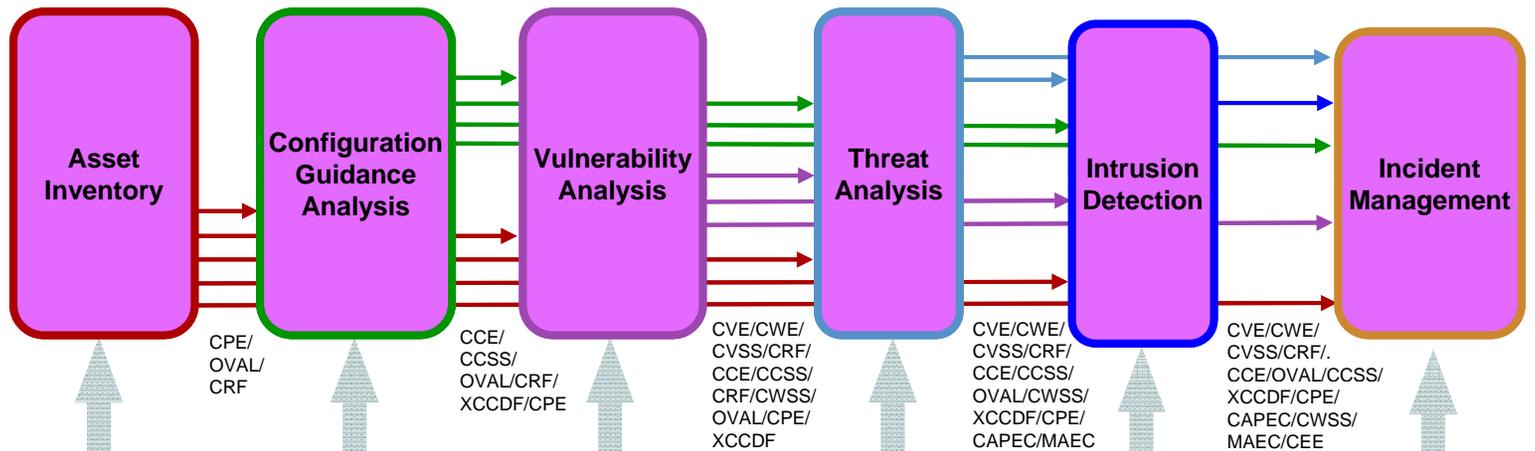


Knowledge Repository

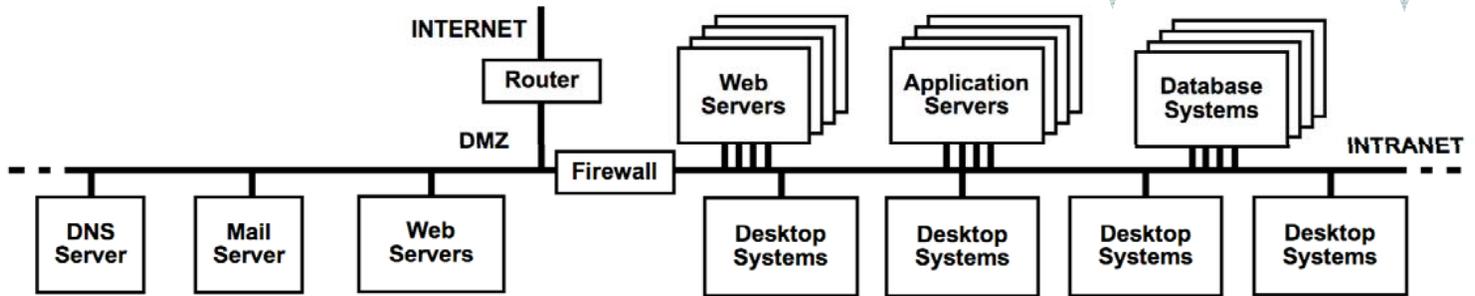
Knowledge Repositories







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



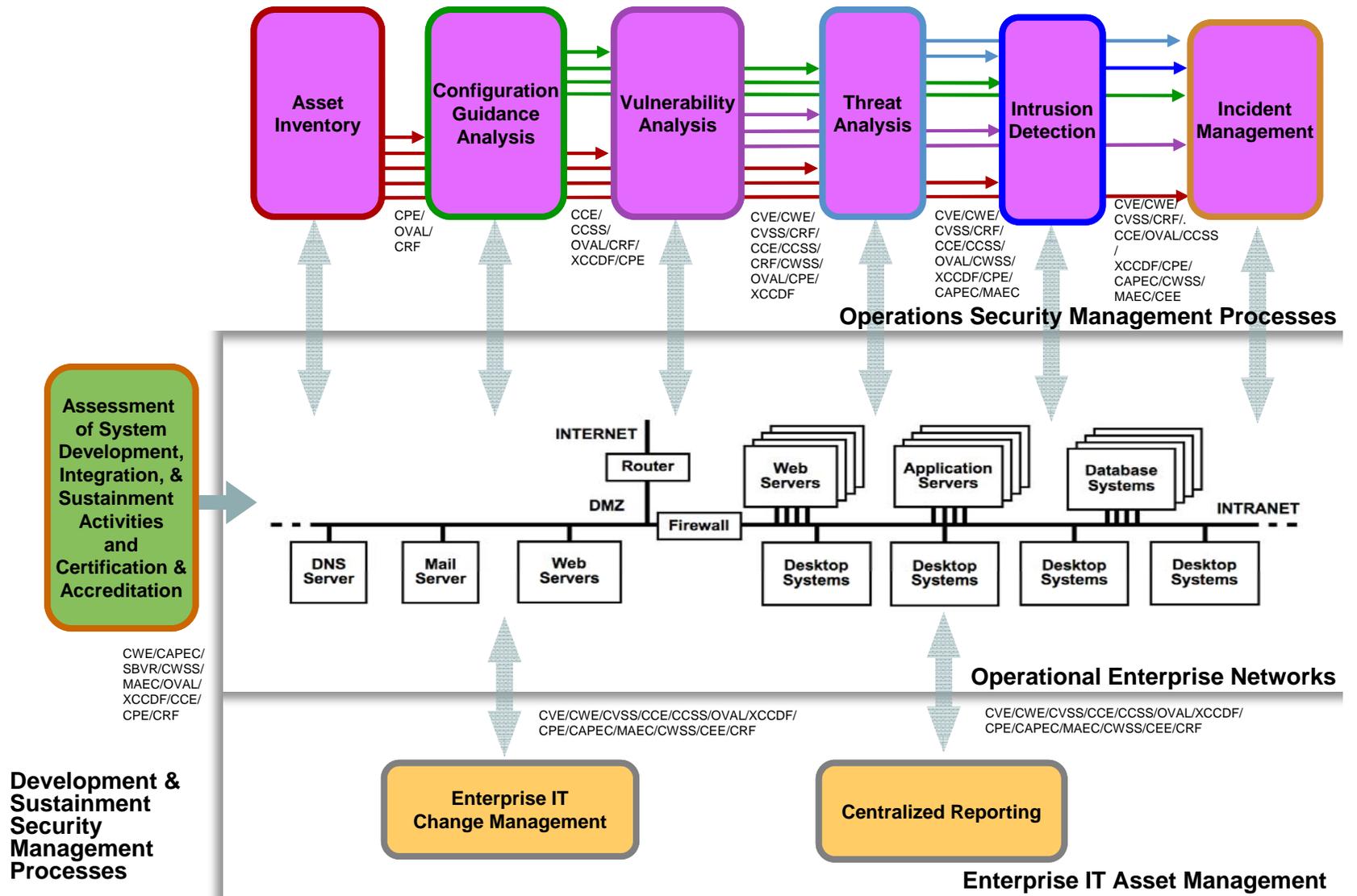
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/CPE/CAPEC/MAEC/SBVR/CWSS/CEE/CRF

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

Development & Sustainment Security Management Processes

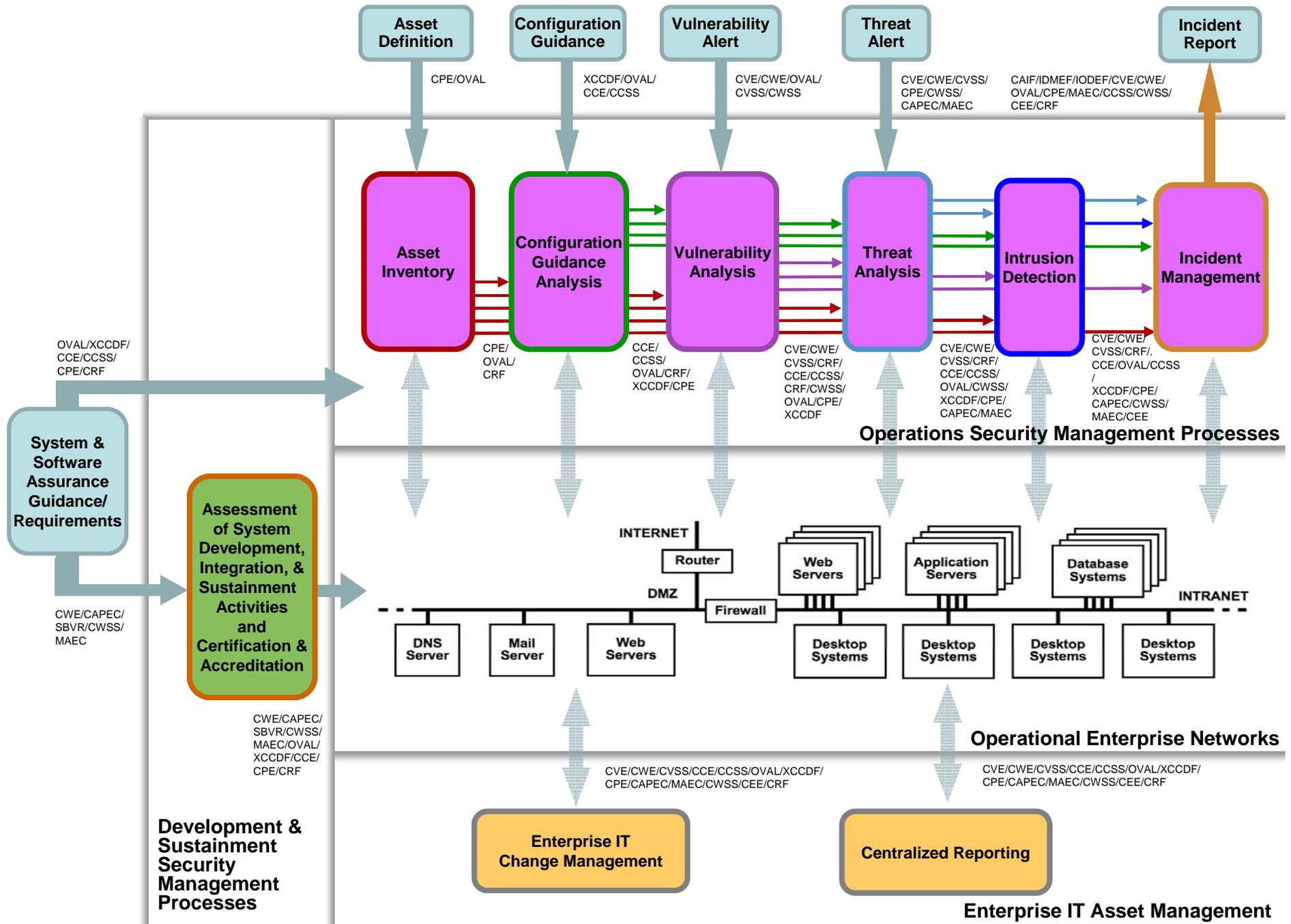


Enterprise IT Asset Management

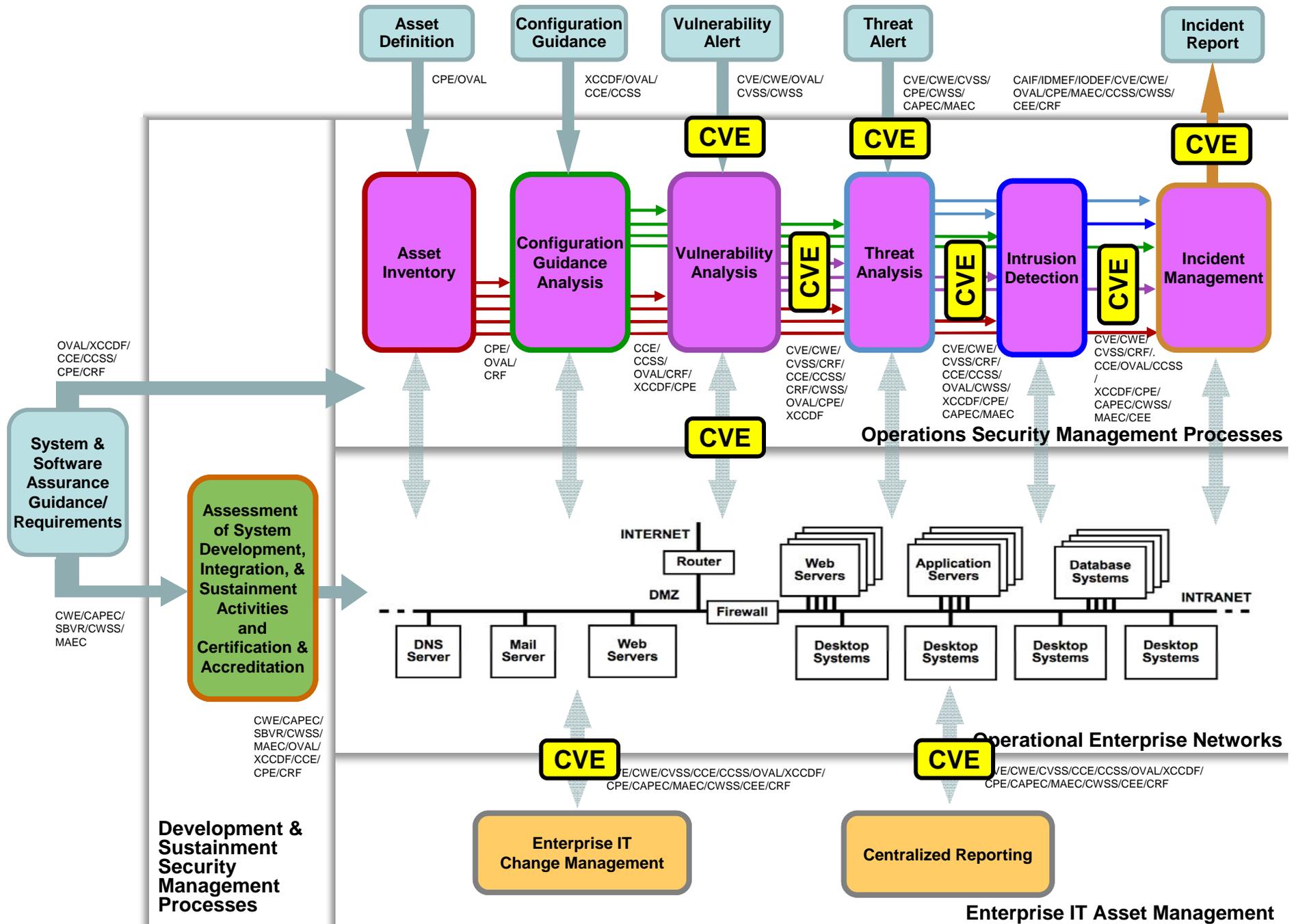


Mitigating Risk Exposures

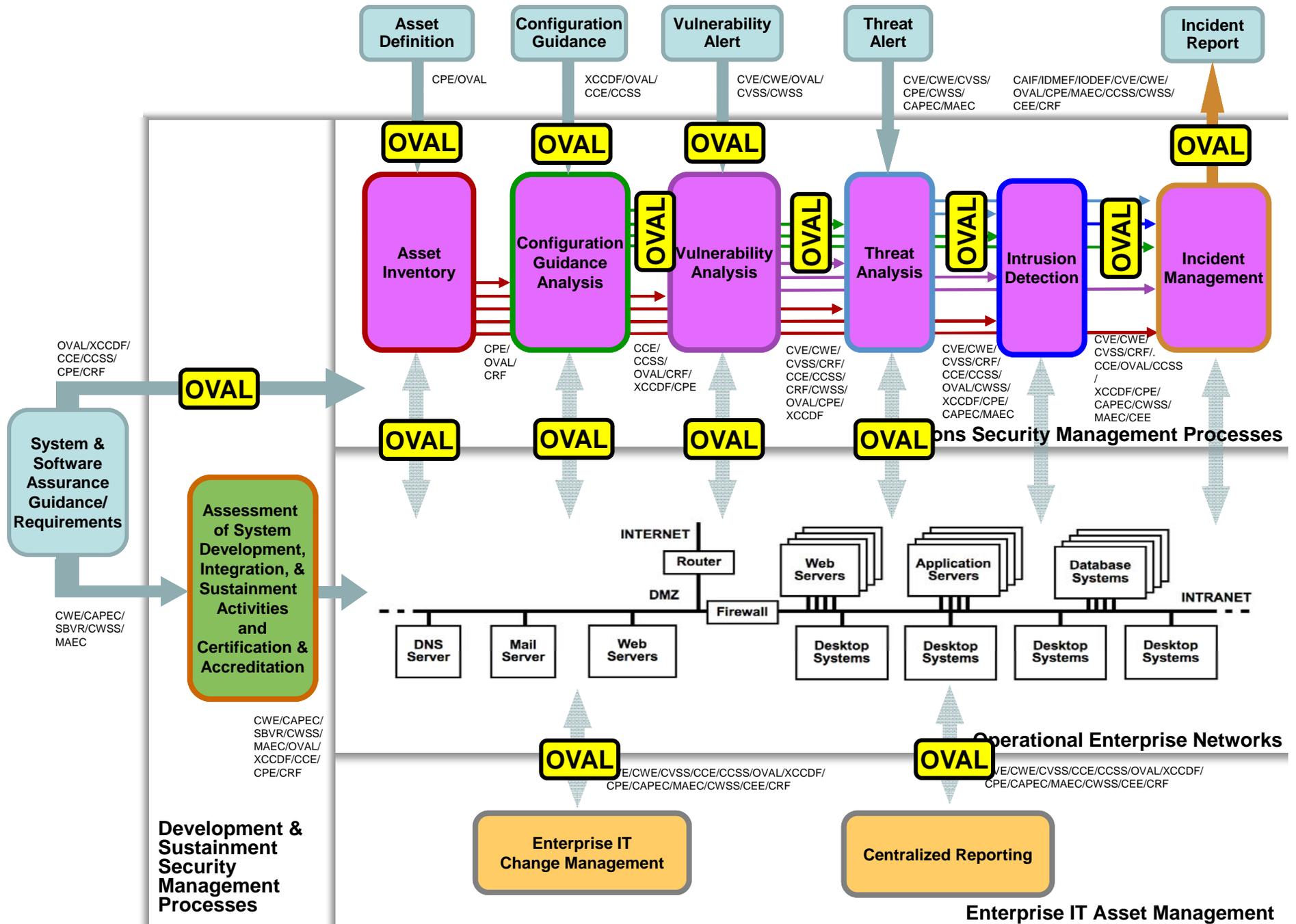
Responding to Security Threats



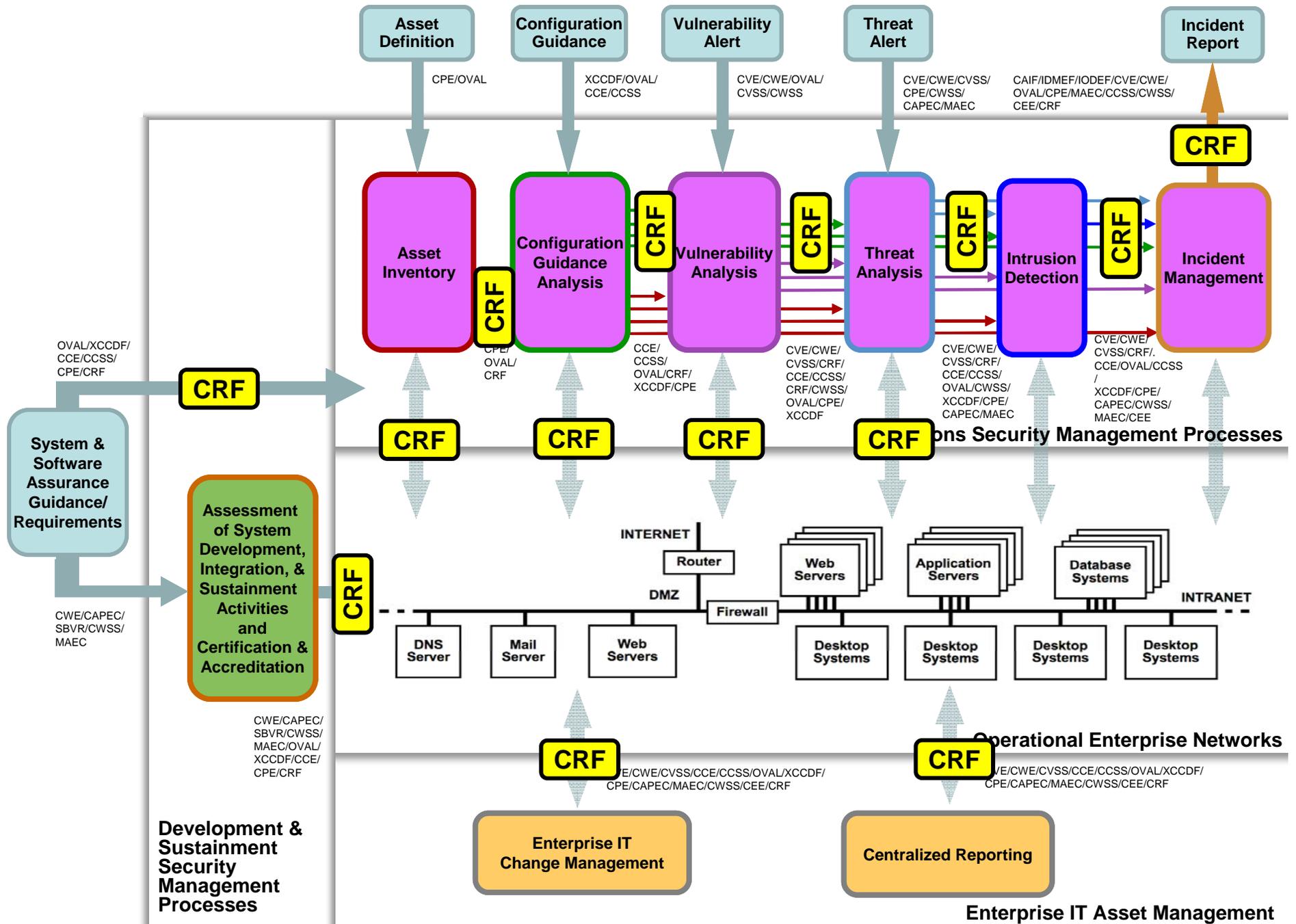
Knowledge Repositories



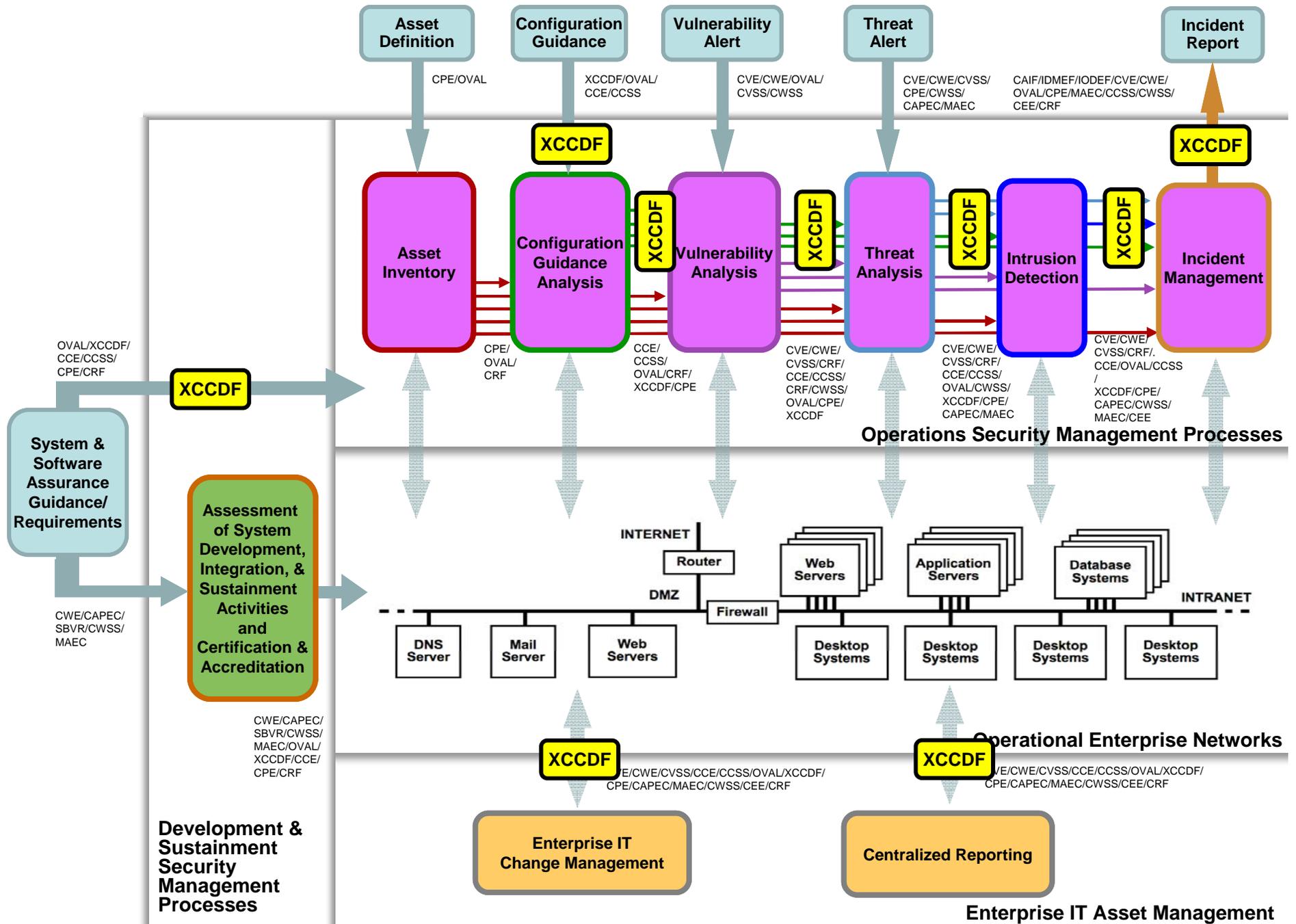
Knowledge Repositories



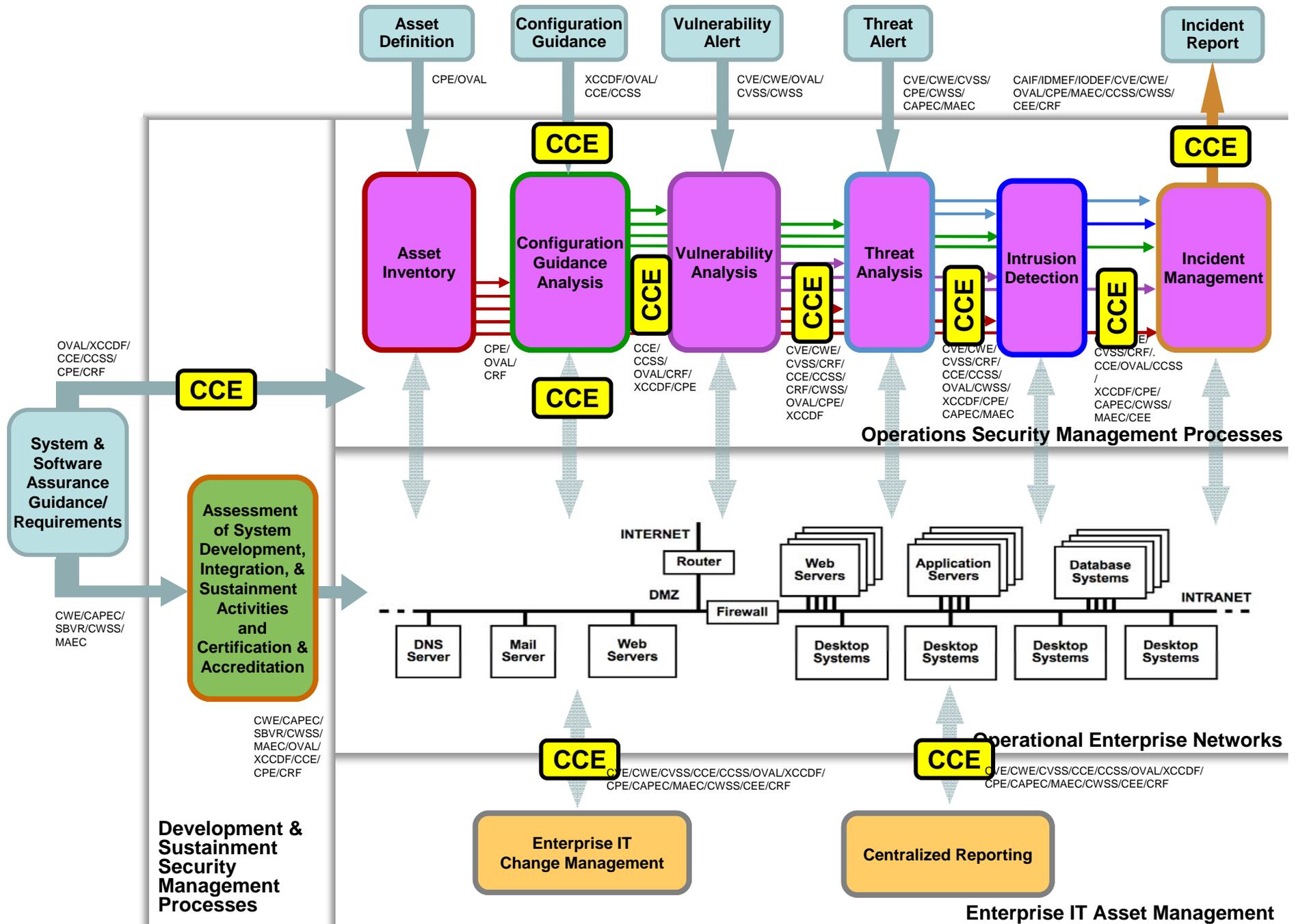
Knowledge Repositories



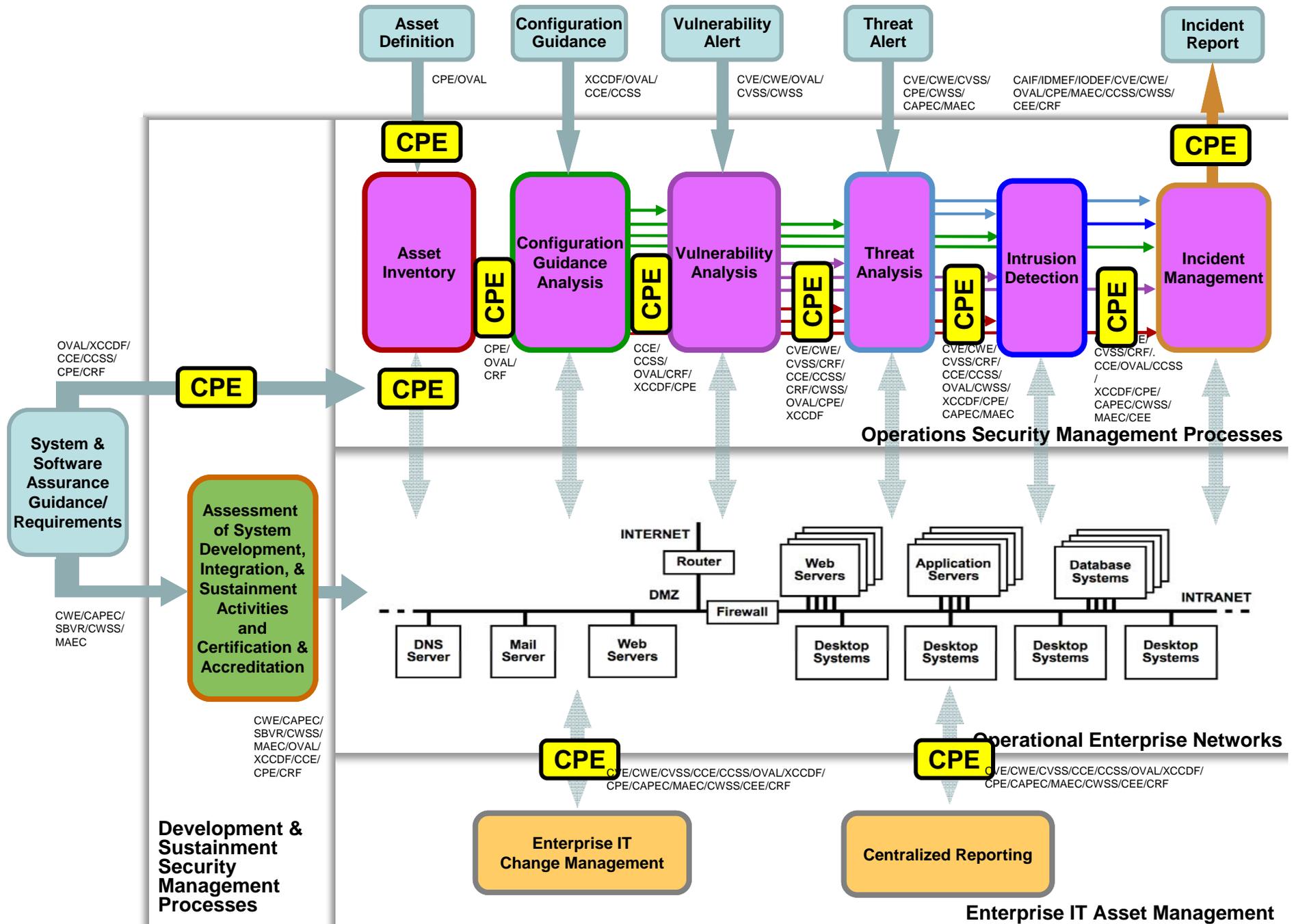
Knowledge Repositories



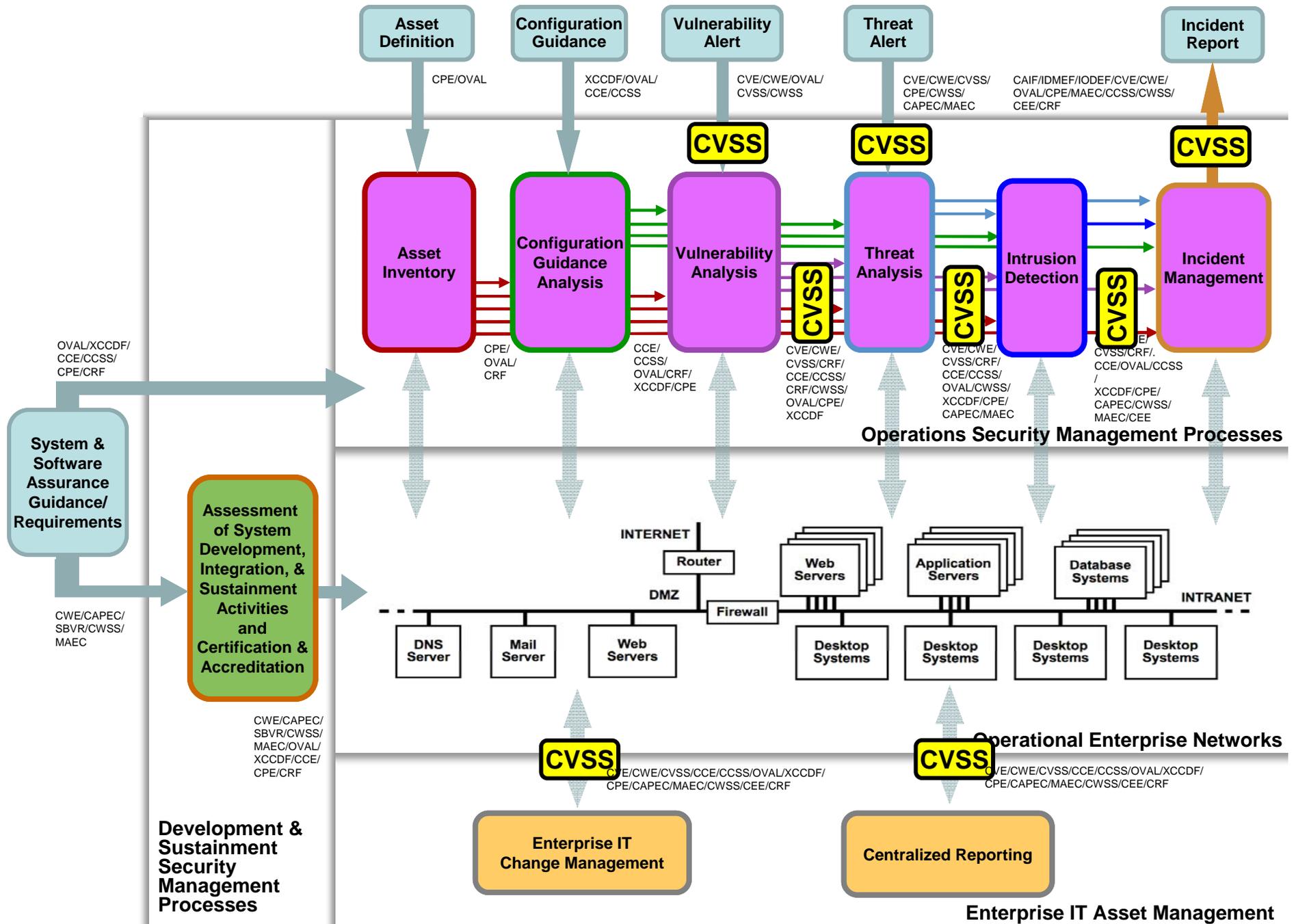
Knowledge Repositories



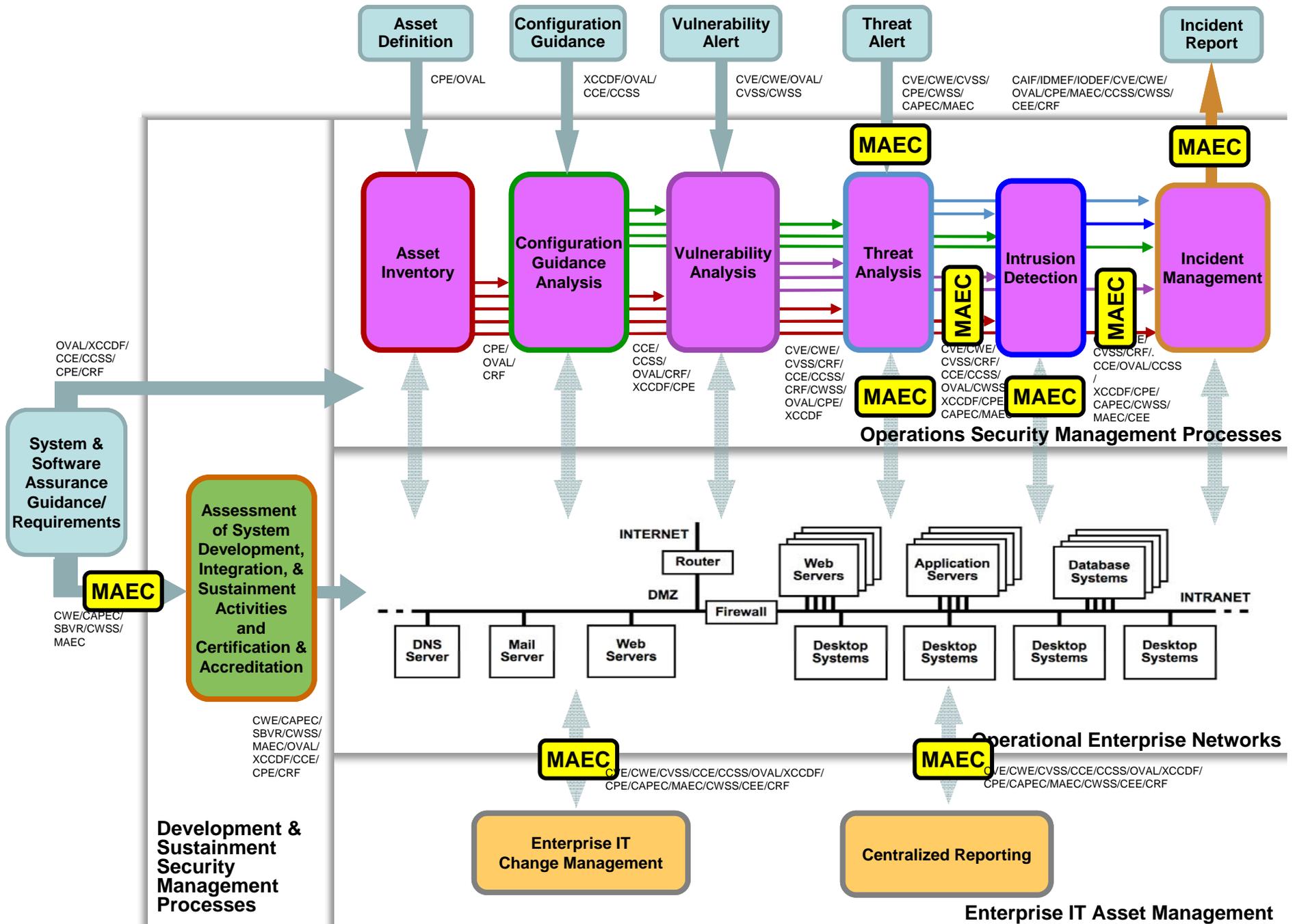
Knowledge Repositories



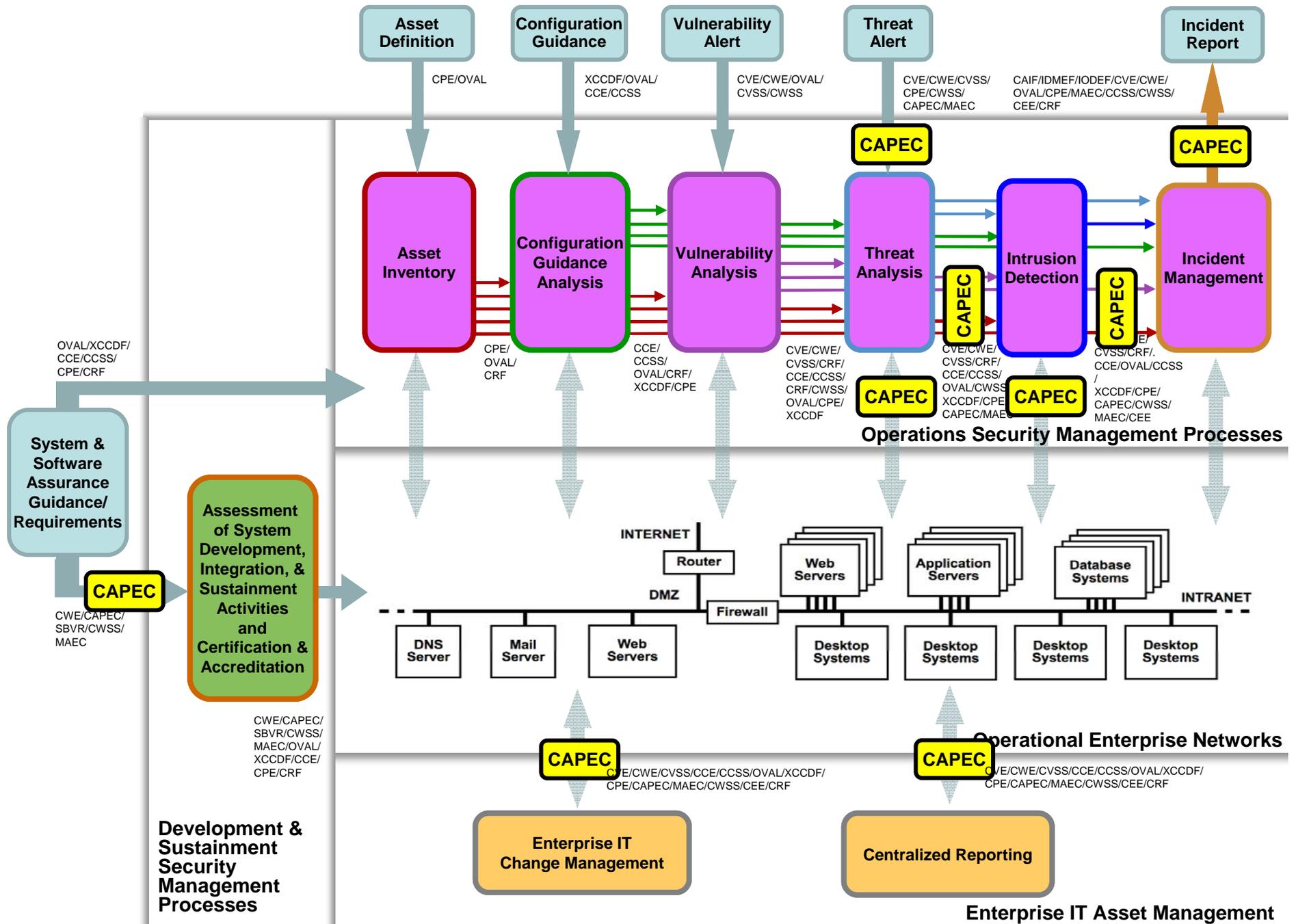
Knowledge Repositories



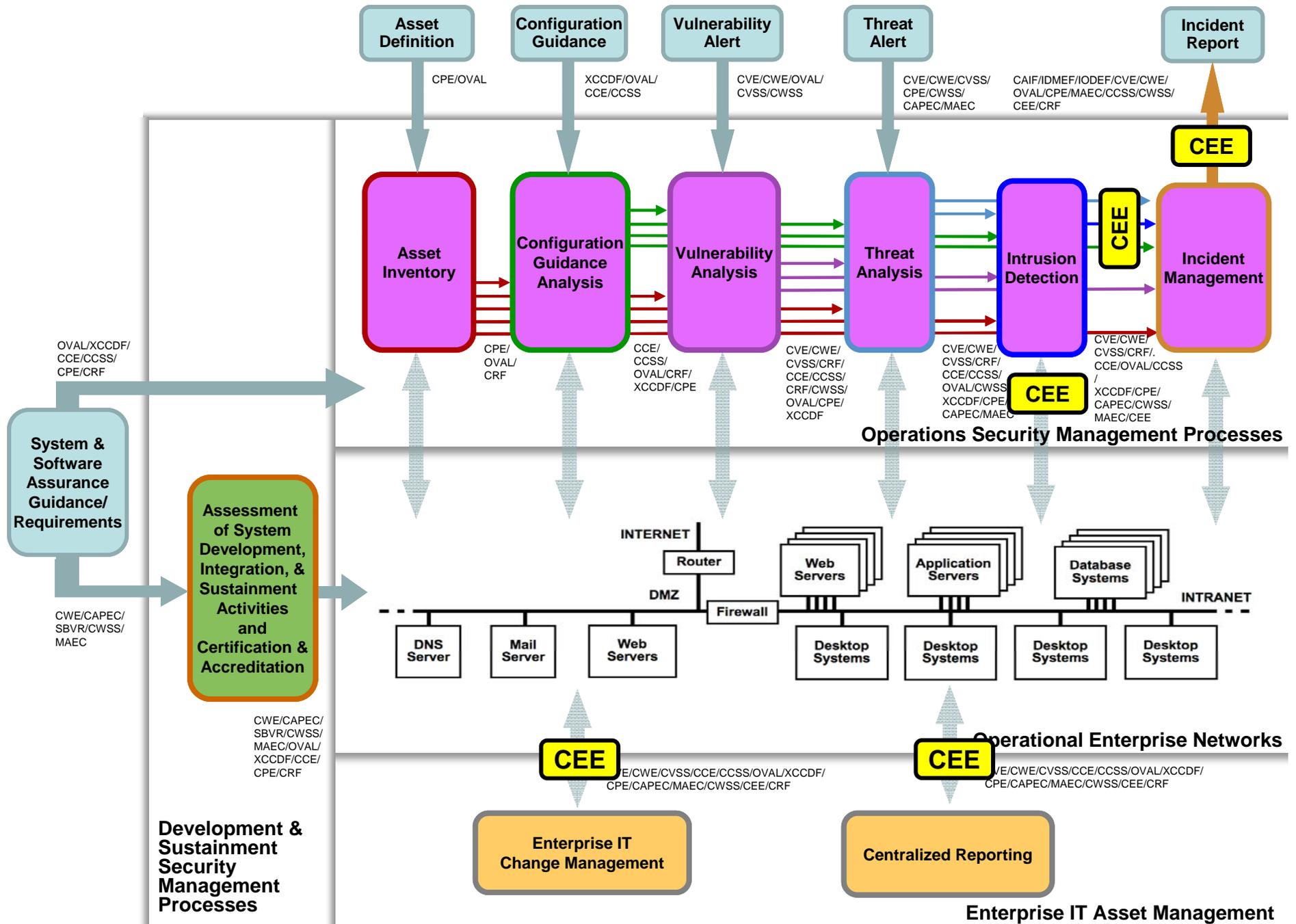
Knowledge Repositories



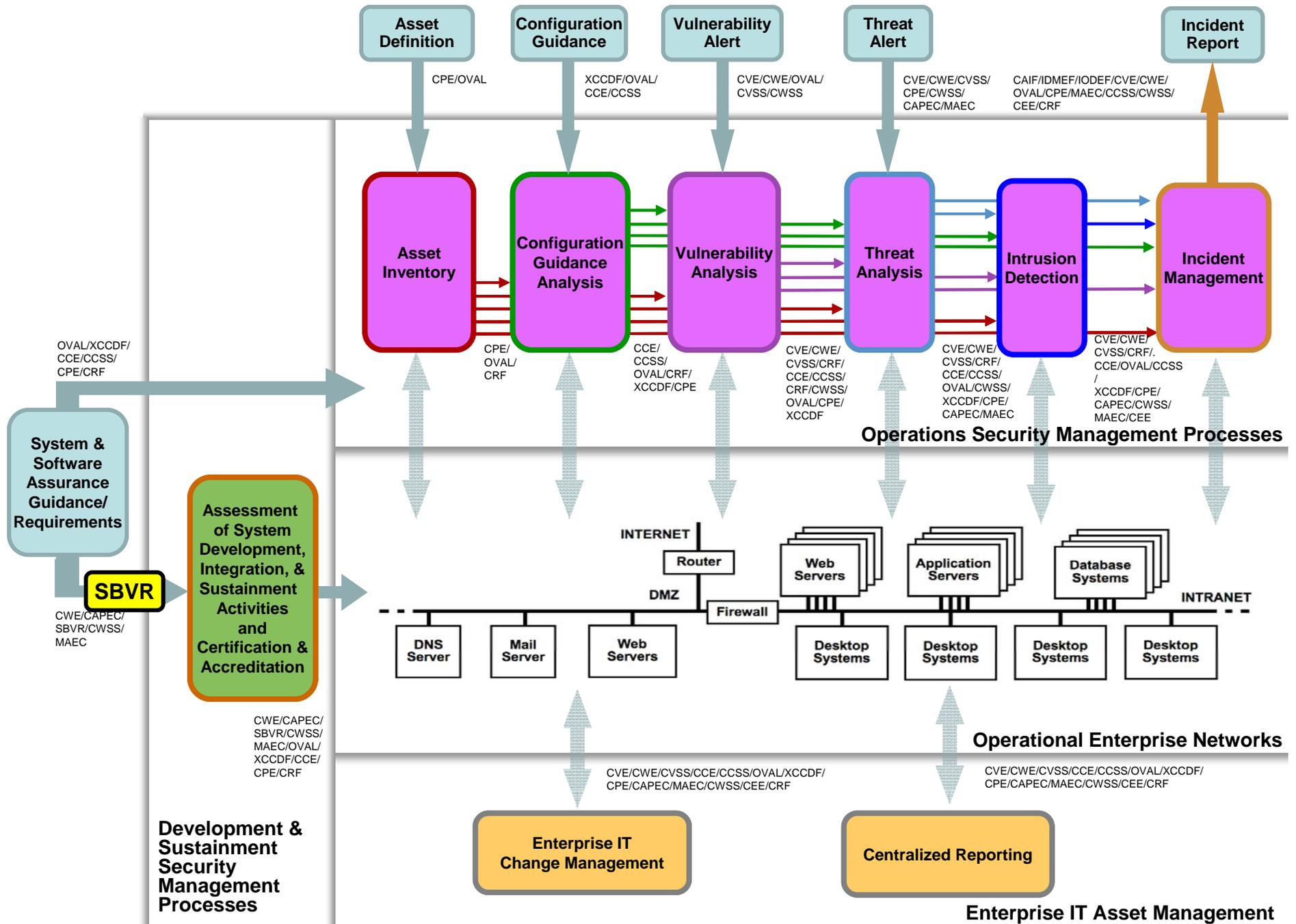
Knowledge Repositories



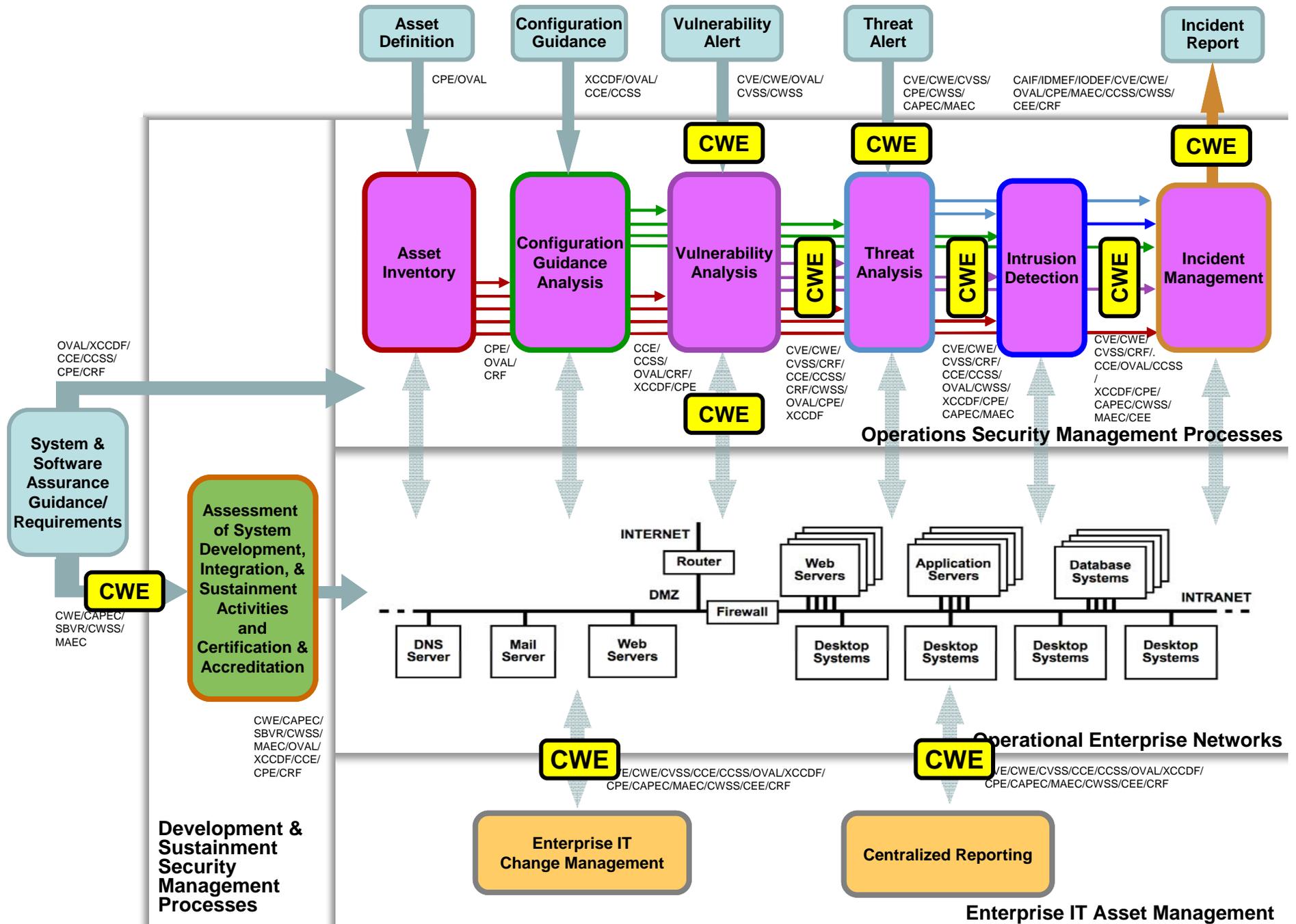
Knowledge Repositories



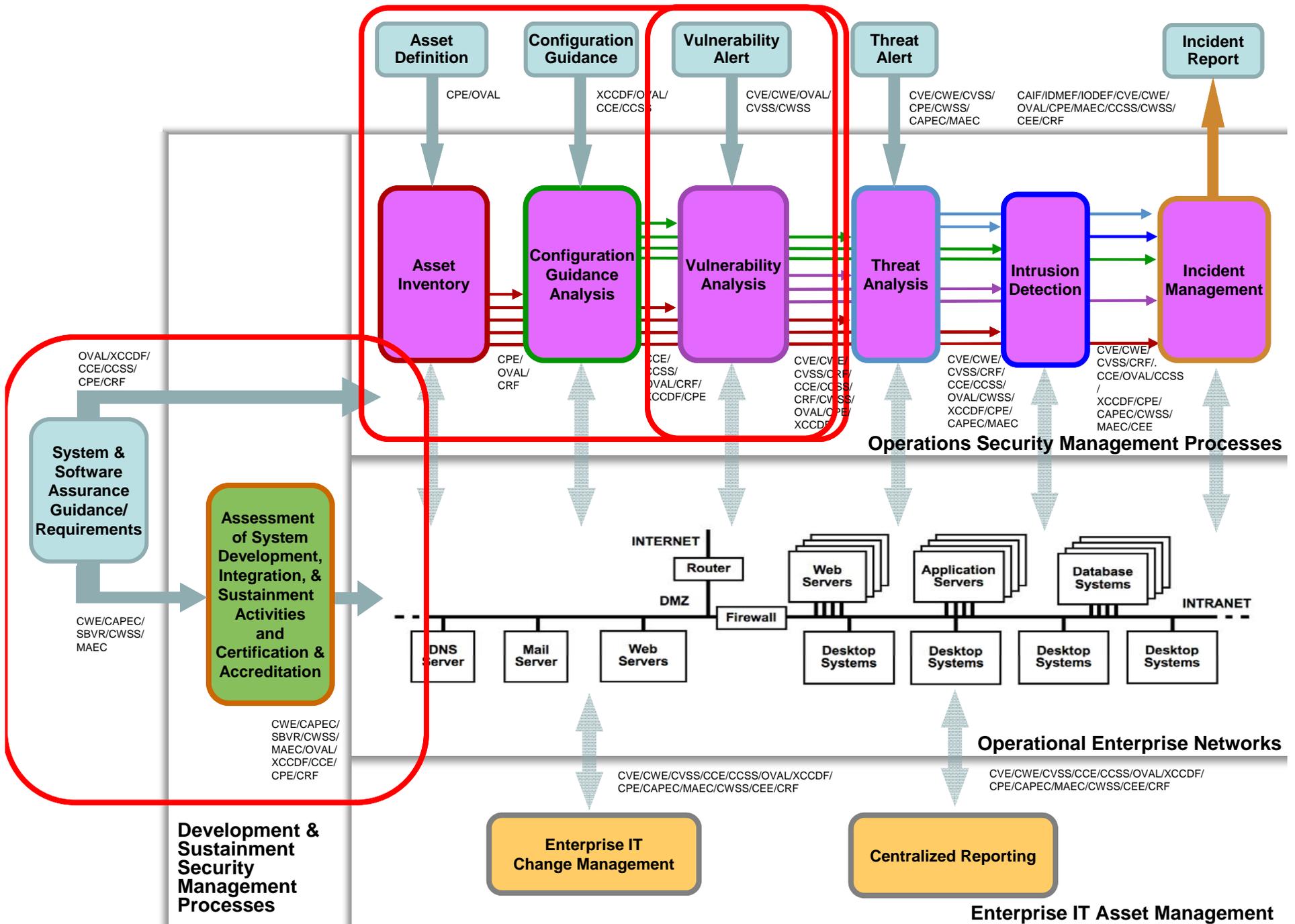
Knowledge Repositories



Knowledge Repositories



Knowledge Repositories



[makingsecuritymeasurable.mitre.org]

Making Security Measurable

A Collection of Information Security Community Standardization Activities and Initiatives

Home | Current Collection | Feedback Requested

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

- CVE** Common Vulnerabilities and Exposures (CVE®) - common vulnerability identifiers
- CWE** Common Weakness Enumeration (CWE™) - list of software weakness types
- CAPEC** Common Attack Pattern Enumeration and Classification (CAPEC™) - list of common attack patterns
- CCE** Common Configuration Enumeration (CCE™) - common security configuration identifiers
- CPE** Common Platform Enumeration (CPE™) - common platform identifiers
- SANS Top Twenty** - SANS/FBI consensus list of the Twenty Most Critical Internet Security Vulnerabilities that uses CVE-IDs to identify the issues
- OWASP Top Ten** - ten most critical Web application security flaws
- WASC Web Security Threat Classification** - list of Web security threats

Languages

- OVAL** Open Vulnerability and Assessment Language (OVAL®) - standard for determining vulnerability and configuration issues
- CRF** Common Result Format (CRF™) - standardized assessment result format for conveying findings based on common names and naming schemes
- CEE** Common Event Expression (CEE™) - standardizes the way computer events are described, logged, and exchanged
- 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
- 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 (CAIE)** - 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](#). © 2008 The MITRE Corporation. CVE is a registered trademark and the Making Security Measurable logo, CCE, CME, CWE, CPE, and OVAL are trademarks of The MITRE Corporation. All other trademarks are the property of their respective owners. Contact us: measurablesecurity@mitre.org

Page Last Updated: January 17, 2008

