



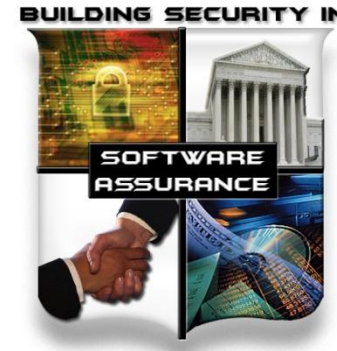
Homeland
Security



Commerce



National
Defense



The Cybersecurity Ecosystem & Making Security Measurable

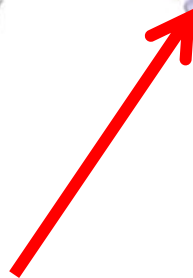
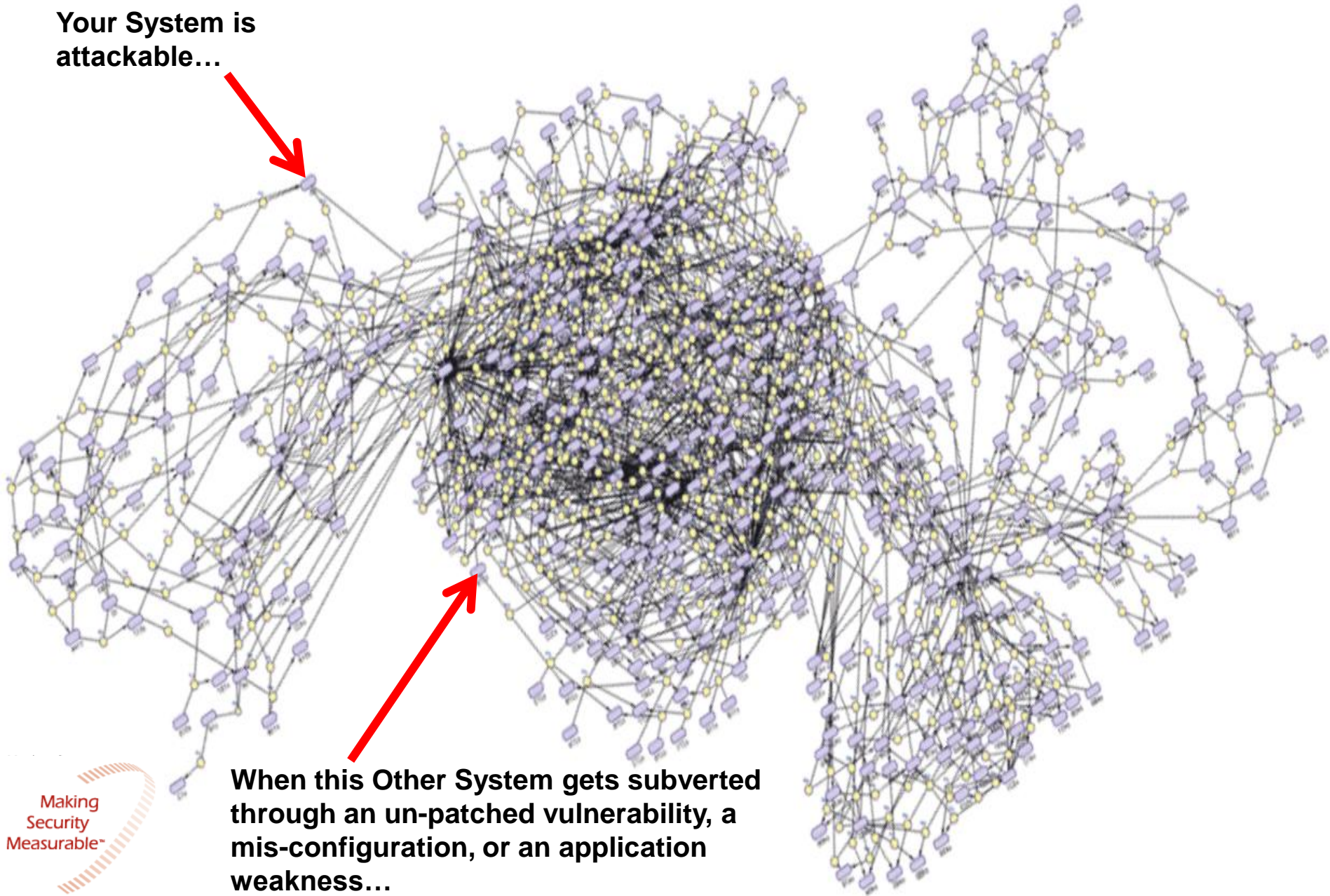


Robert A. Martin
28 Feb 2011

MITRE

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...

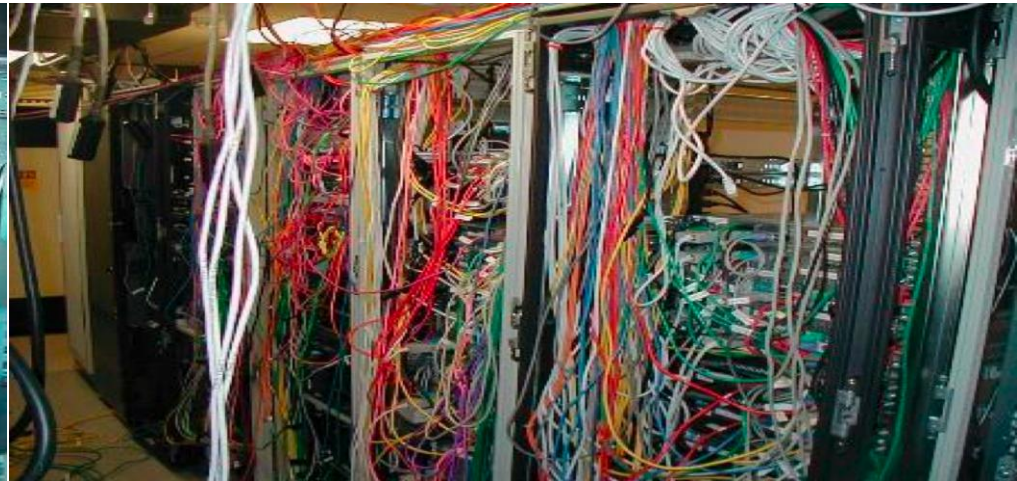
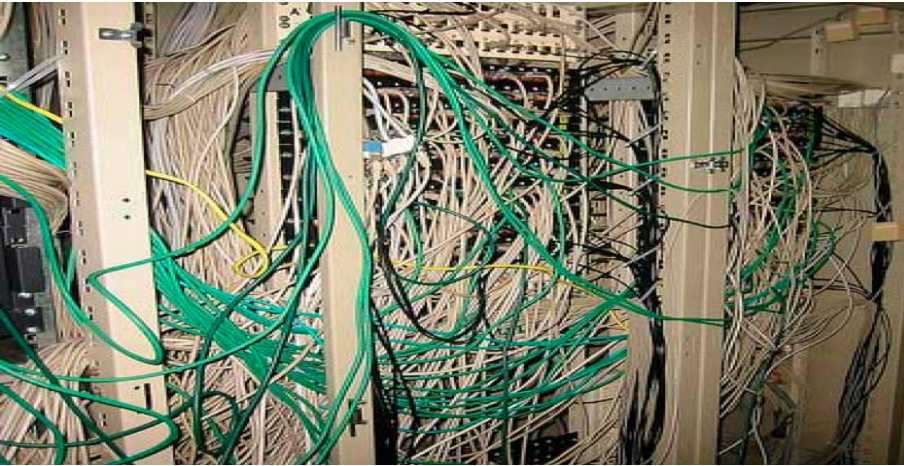


Why Should We Re-Architect Cybersecurity?

Proposition: The divergent and unique manner in which each of our enterprises have implemented their cybersecurity capabilities, we as a community can not easily leverage each others efforts and experiences in coming up with practical and widely applicable approaches to:

- Acquisition
- Training
- Software Security Engineering
- Software Assurance Analysis
- Secure Software Operations

Like Security - Networks Evolved

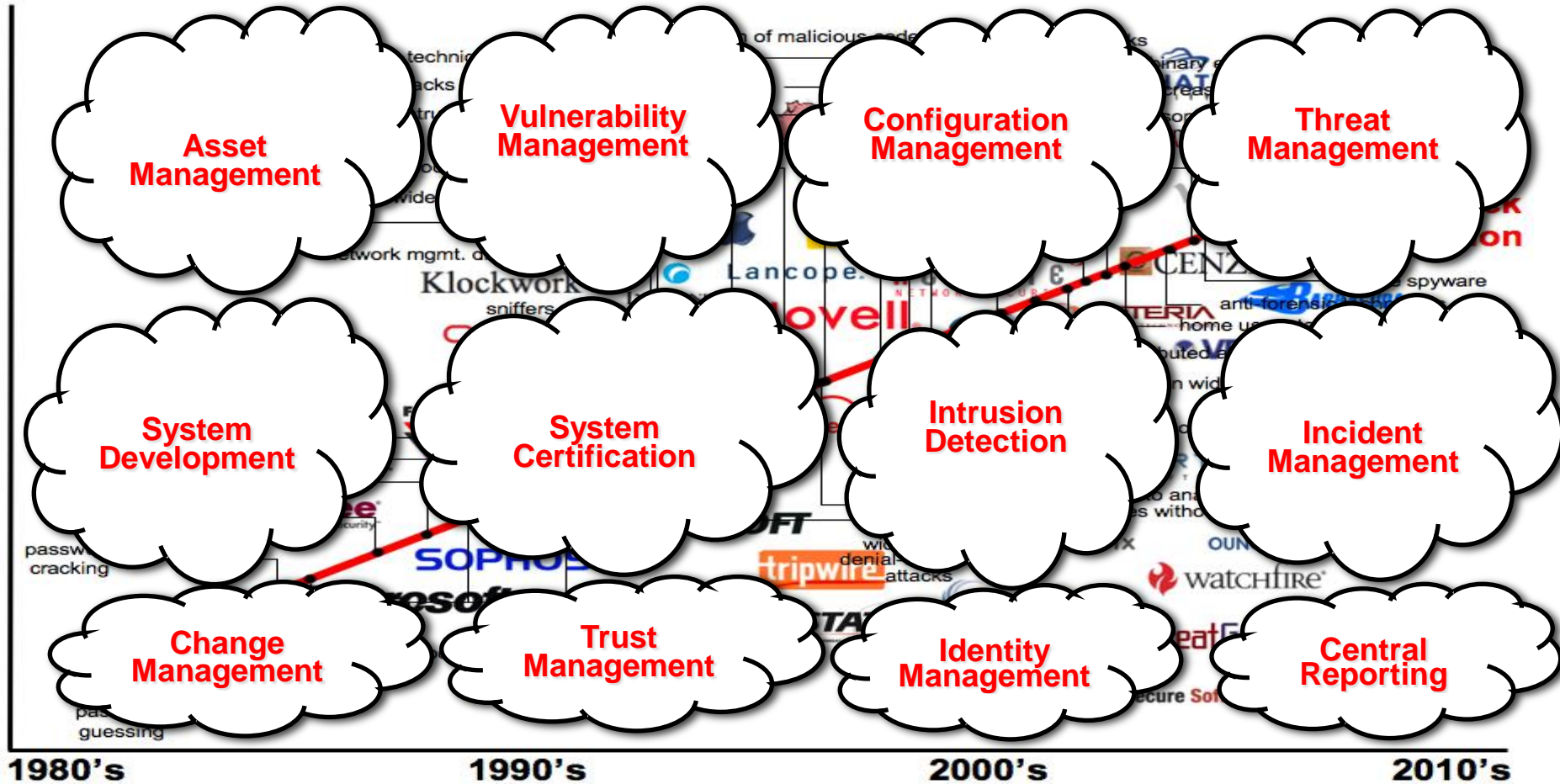


**Each new solution had to integrate with the existing solutions
-->> every enterprise ends up learning as they go and has a
“unique” tapestry of solutions with “local practices”**

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



Architecting Security with Information Standards for COIs



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



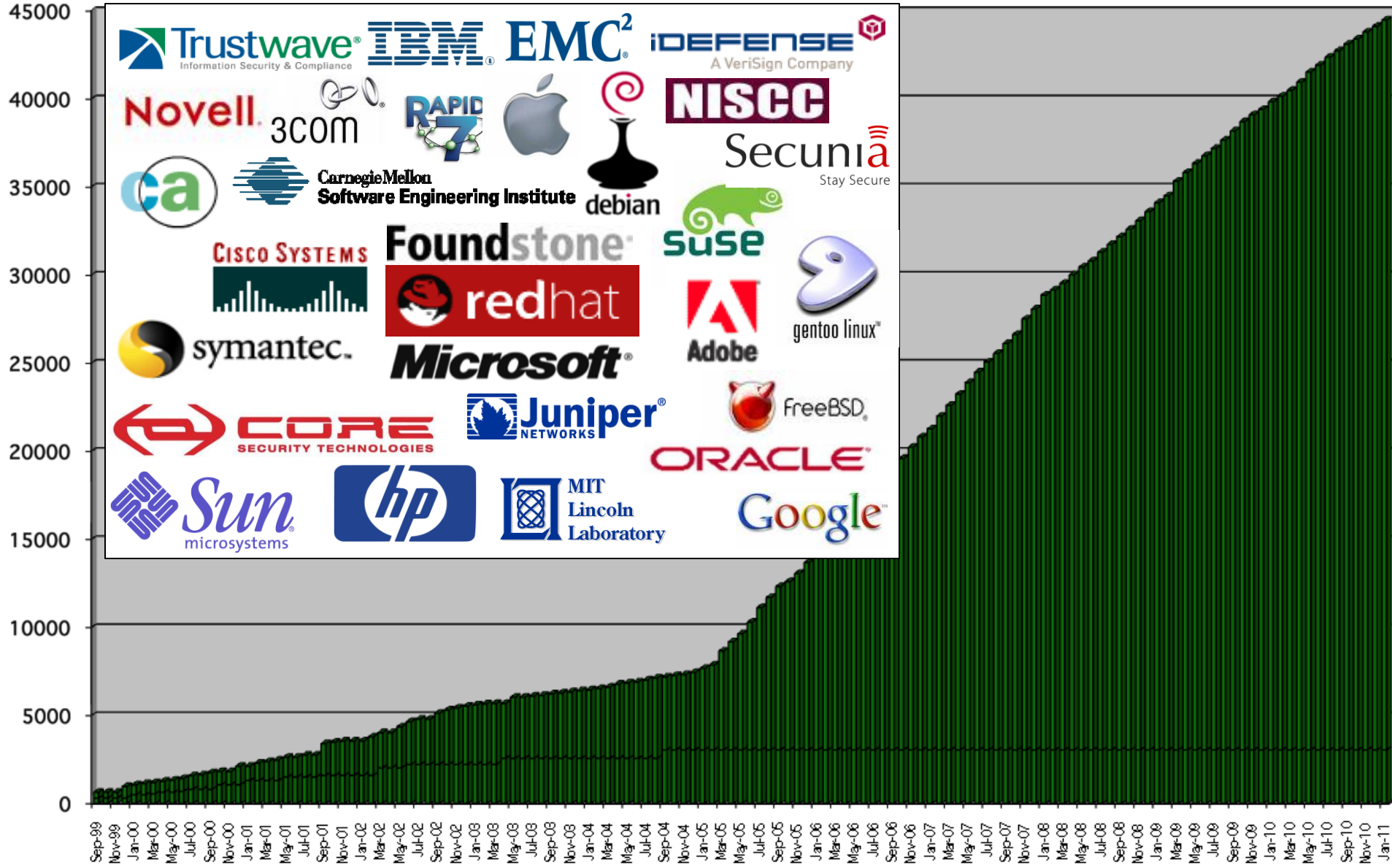
The Building Blocks Are:

- 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 (ARF), event patterns (CEE), malware patterns (MAEC), risk of a vulnerability (CVSS), config risk (CCSS), weakness risk (CWSS), assessment findings (SAFES/SACM), information messages (CYBEX/IODEF)**
- 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**

CVE 1999 to 2011



CVE is Widely Used & Available 45,218 and climbing...

Arabic

Bulgarian

Catalan

Chinese

Croatian

Czech

Danish

Dutch

Estonian

Finnish

French

German

Greek

Hebrew

Hungarian

Icelandic

Indonesian

Italian

Japanese

Korean

Latvian

Lithuanian

Norwegian

Polish

Portuguese

Romanian

Russian

Serbian

Slovak

Slovenian

Spanish

Swedish

Turkish

English Version Content:

CVE LIST COMPATIBLE PRODUCTS NEWS - SEPTEMBER 3, 2008 SEARCH

Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Reporting
TOTAL CVEs: 32464

Latest News
CVE and NIST Partner to Create New CVE Advisory Validation Programs
Caldent Networks Inc. Posts CVE Compatibility Questionnaire
TMC v Ca Posts CVE Compatibility Questionnaire
Being Venus Information Security Technology, Inc. Makes CVE Compatibility Declaration
City Housing Security Measureable south at Black Hat Briefings 2008
CVE Adoption Announced by Oracle on Global Product Security Blog
More News >>

Upcoming Events
CVE-related workshops and Making Security Measureable table being at BSUSA Conference, October 22-24
More Events >>

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.

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 (CRP)
- Checklist Language (XCCDF)
- Assessment Language (OVAL)
- Security Content Automation (SCAP)
- Making Security Measurable

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 CCE are trademarks of The MITRE Corporation. This Web site is hosted by The MITRE Corporation.

CVE Vendor/Industry Engagement



278 PRODUCTS AND SERVICES FROM 152 ORGANIZATIONS IN 26 COUNTRIES

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 (ARF), event patterns (CEE), malware patterns (MAEC), risk of a vulnerability (CVSS), config risk (CCSS), weakness risk (CWSS), assessment findings (SAFES/SACM), information messages (CYBEX/IODEF)**
- 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:



OVAL

NIST/DHS NVD

**Vulnerability
Alerts**

Knowledge Repository

Vulnerability Alerts

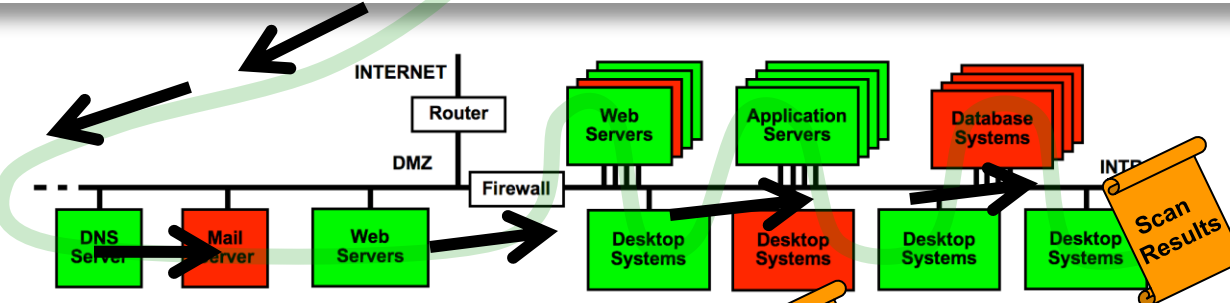


Vulnerability Analysis

Operations Security Management Processes

OVAL "Compatible" Tools

Operational Enterprise Networks



Enterprise IT Asset Management

Enterprise IT Change Management

Centralized Reporting

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 (ARF), event patterns (CEE), malware patterns (MAEC), risk of a vulnerability (CVSS), config risk (CCSS), weakness risk (CWSS), assessment findings (SAFES/SACM), information messages (CYBEX/IODEF)**
- 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
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

DATE: August 11, 2008

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 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, AFDCC reports and subject matter expertise. FDCC Major Version 1.0 settings are available 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 patching 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 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

National Checklist Program

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

Sponsored by DHS National Cyber Security Division/US-CERT

National Vulnerability Database
automating vulnerability management, security measurement, and compliance checking

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

Home | ISAP/SCAP | SCAP Validated Tools | SCAP Events | About | Contact | Vendor Comments

Mission and Overview

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

Resource Status

NVD contains:
29632 CVE Vulnerabilities
150 Checklists
132 US-CERT Alerts
2150 US-CERT Vuln Notes
3171 OVAL Queries
13666 Vulnerable Products

Last updated: 02/20/08
CVE Publication rate: 18 vulnerabilities / day

Email List

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

Workload Index

Vulnerability Workload Index: 10.87

About Us

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

REPORT A VULNERABILITY
REPORT AN INCIDENT

NVD RSS

NIST Security Configuration CHECKLISTS
<http://checklists.nist.gov>

cve.mitre.org

CCE
Common Configuration Enumeration

CPE
common platform enumeration

CVSS XCCDF
security benchmark automation

OVAL
oval.mitre.org

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

NCP contains 150 checklists covering 146 products

Keyword 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 assisted 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 the category.

Recent Updates (includes updates from the last 6 months)

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

02/20/2008	SCAP Configuration Content - DISA Windows 2000 Security Checklist
	SCAP Configuration Content - Real Hat Enterprise Linux
	SCAP Configuration Content - Solaris 10
	SCAP OVAL Patches - Microsoft Windows 2000
	SCAP OVAL Patches - Real Hat Enterprise Linux
02/18/2008	Prose Guide - Solaris Benchmark (Solaris 10)
	Prose Guide - Windows 2000 Security Checklist
01/30/2008	FDCC Prose Guide - IE7
	FDCC Prose Guide - Windows Vista
	FDCC Prose Guide - Windows Vista Firewall
	FDCC Prose Guide - Windows XP
	FDCC Prose Guide - Windows XP Firewall
	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
	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
01/18/2008	FDCC SCAP OVAL Patches - IE7
	FDCC SCAP OVAL Patches - Windows Vista
	FDCC SCAP OVAL Patches - Windows Vista Firewall
	FDCC SCAP OVAL Patches - Windows XP
	FDCC SCAP OVAL Patches - Windows XP Firewall
	OS/390 Security Technical Implementation Guide
	Prose Guide - NIST SP 800-68
	Prose Guide - Windows Vista Security Guide
	SCAP Configuration Content - NIST SP 800-43
	SCAP Configuration Content for Domain Controllers - Windows Server 2003
	SCAP Configuration Content for Member Servers - Windows Server 2003
	SCAP OVAL Patches - Windows Server 2003
01/16/2008	Prose Guide - DISA Checklist
	Prose Guide - NIST SP 800-43
	Prose Guide - NSA Guide
	Prose Guide - Windows Server 2003
	SCAP Configuration Content - DISA Checklist

Knowledge Repository

Remembering the Acronyms

What IT systems do I have in my enterprise?

- **CPE** (Platforms)

What vulnerabilities do I need to worry about?

- **CVE** (Vulnerabilities)

What vulnerabilities do I need to worry about
RIGHT NOW?

- **CVSS** (Scoring System)

How can I configure my systems more
securely?

- **CCE** (Configurations)

How do I define a policy of secure
configurations?

- **XCCDF** (Configuration Checklists)

How can I be sure my systems conform to
policy?

- **OVAL** (Assessment Language)

How can I be sure the operation of my systems
conforms to policy?

- **OCIL** (Interactive Language)

What weaknesses in my software could be
exploited?

- **CWE** (Weaknesses)

What attacks can exploit which weaknesses?

- **CAPEC** (Attack Patterns)

What should be logged, and how?

- **CEE** (Events)

How can I aggregate assessment results?

- **ARF** (Results)

How can we recognize malware?

- **MAEC** (Malware Attributes)

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

What IT systems do I have in my enterprise?

- **CPE** (Platforms)

What vulnerabilities do I need to worry about?

- **CVE** (Vulnerabilities)

What vulnerabilities do I need to worry about
RIGHT NOW?

- **CVSS** (Scoring System)

How can I configure my systems more
securely?

- **CCE** (Configurations)

How do I define a policy of secure
configurations?

- **XCCDF** (Configuration Checklists)

How can I be sure my systems conform to
policy?

- **OVAL** (Assessment Language)

How can I be sure the operation of my systems
conforms to policy?

- **OCIL** (Interactive Language)

What weaknesses in my software could be
exploited?

- **CWE** (Weaknesses)

What attacks can exploit which weaknesses?

- **CAPEC** (Attack Patterns)

What should be logged, and how?

- **CEE** (Events)

How can I aggregate assessment results?

- **ARF** (Results)

How can we recognize malware?

- **MAEC** (Malware Attributes)

SCAP-Based FDCC Guidance

Configuration Guidance

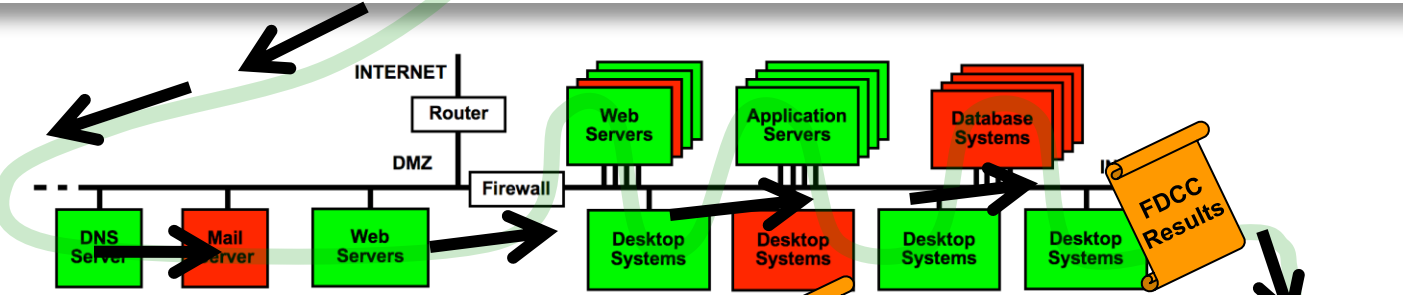


Configuration Guidance Analysis

Operations Security Management Processes

FDCC Compliant Tools

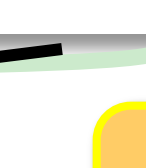
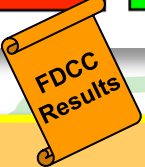
Operational Enterprise Networks



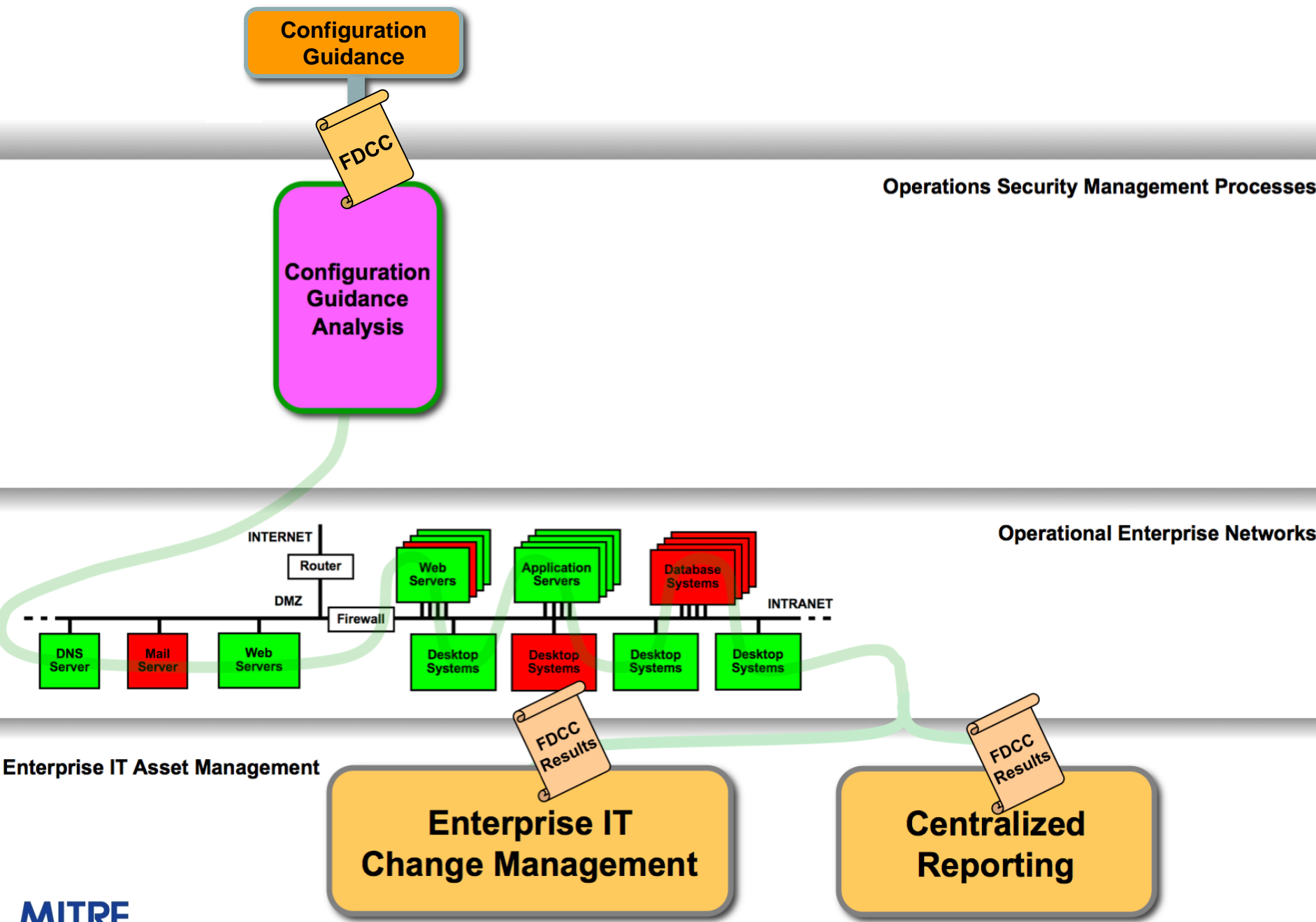
Enterprise IT Asset Management

Enterprise IT Change Management

Centralized Reporting



SCAP-Based FDCC Reporting



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 (ARF), event patterns (CEE), malware patterns (MAEC), risk of a vulnerability (CVSS), config risk (CCSS), weakness risk (CWSS), assessment findings (SAFES/SACM), information messages (CYBEX/IODEF)**
- 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:



CAPEC

CCE

XCCDF & OVAL

ARF

CVSS

CCSS

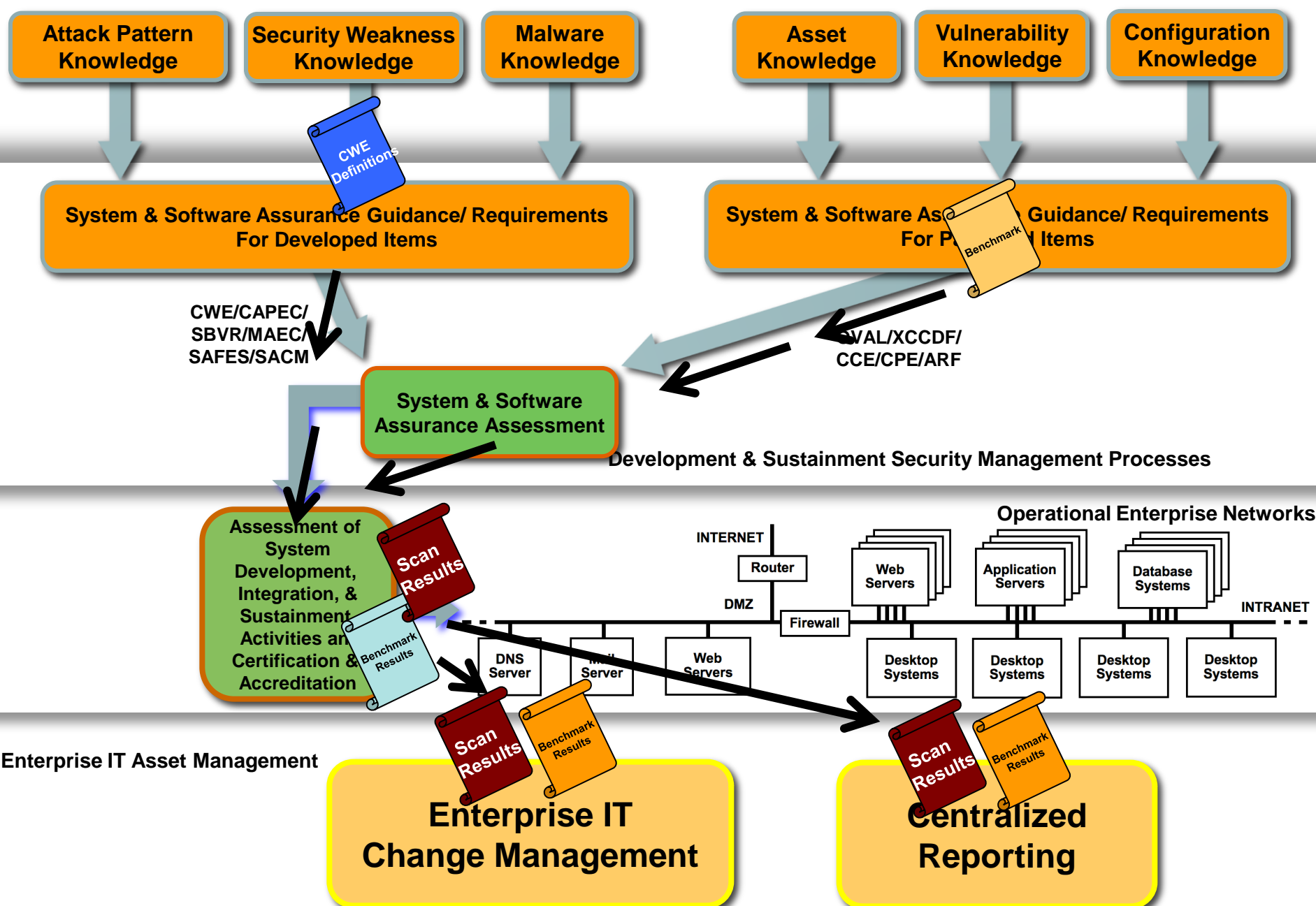
SAFES/SACM

DoD DIACAP & eMASS

e-MASS

Knowledge Repository

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 (ARF), event patterns (CEE), malware patterns (MAEC), risk of a vulnerability (CVSS), config risk (CCSS), weakness risk (CWSS), assessment findings (SAFES/SACM), information messages (CYBEX/IODEF)**
- 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:



CPE
CV

CVE

CAPEC

OVAL

CEE

NIST/DHS NVD

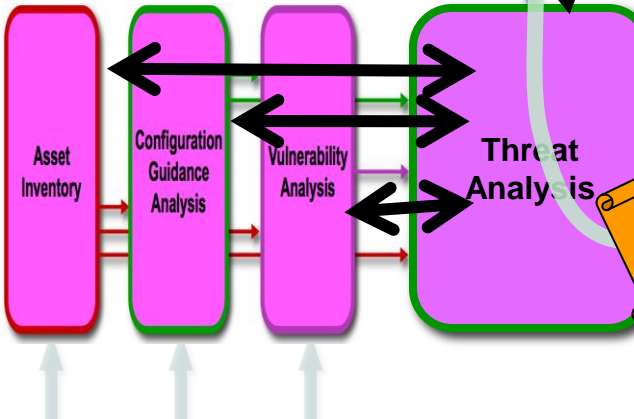


Knowledge Repository

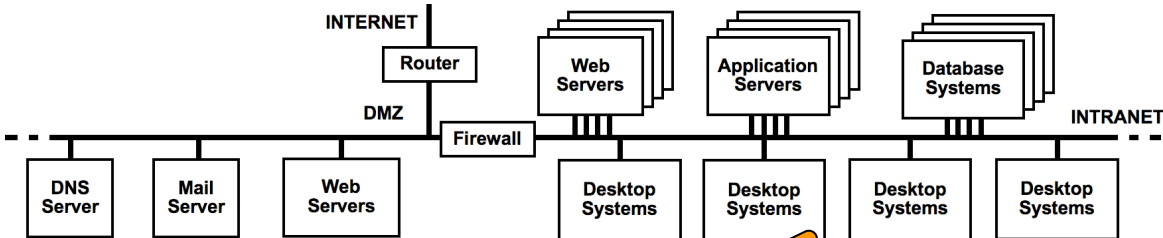
Knowledge Repositories



Operations Security Management Processes

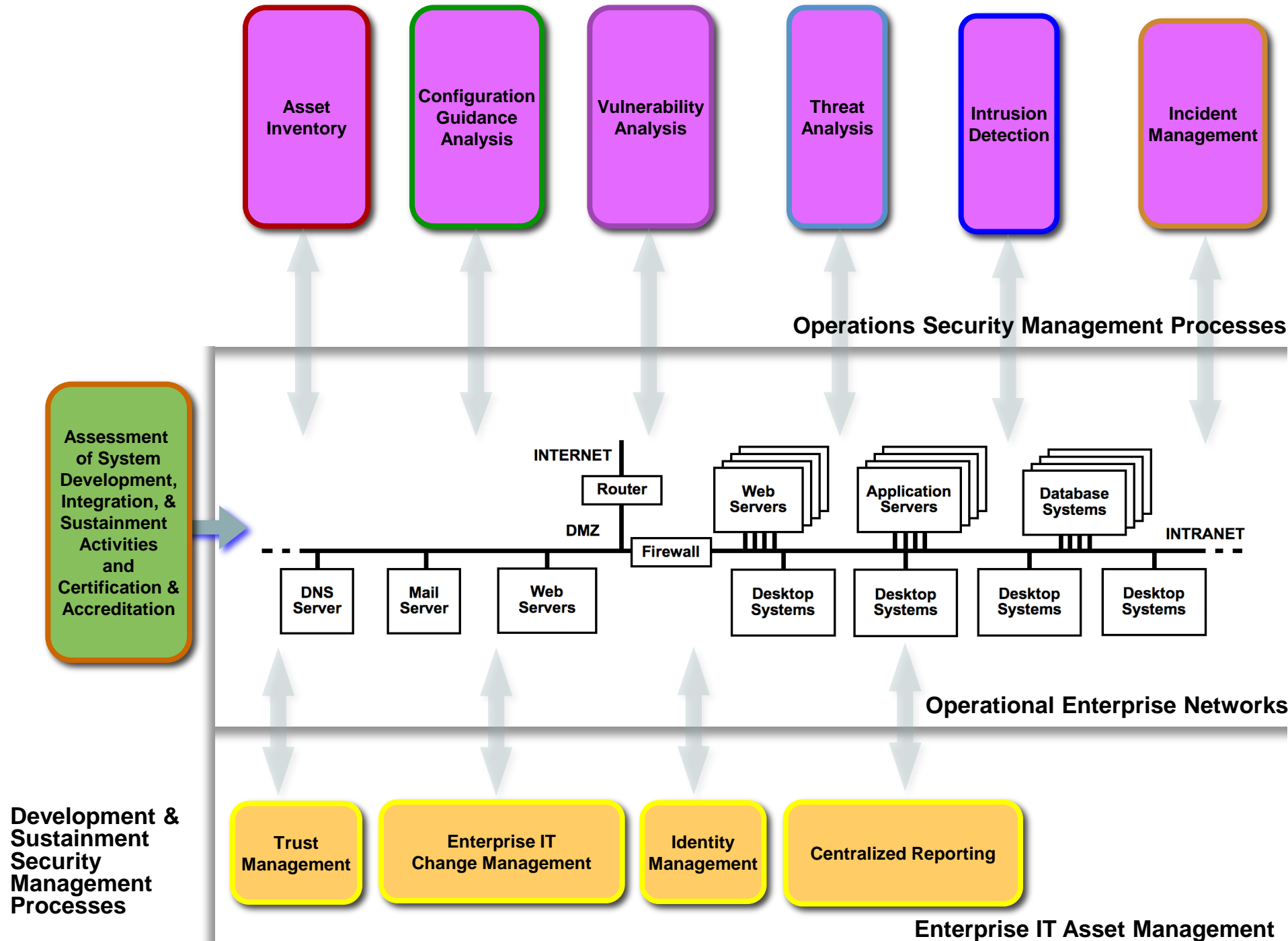


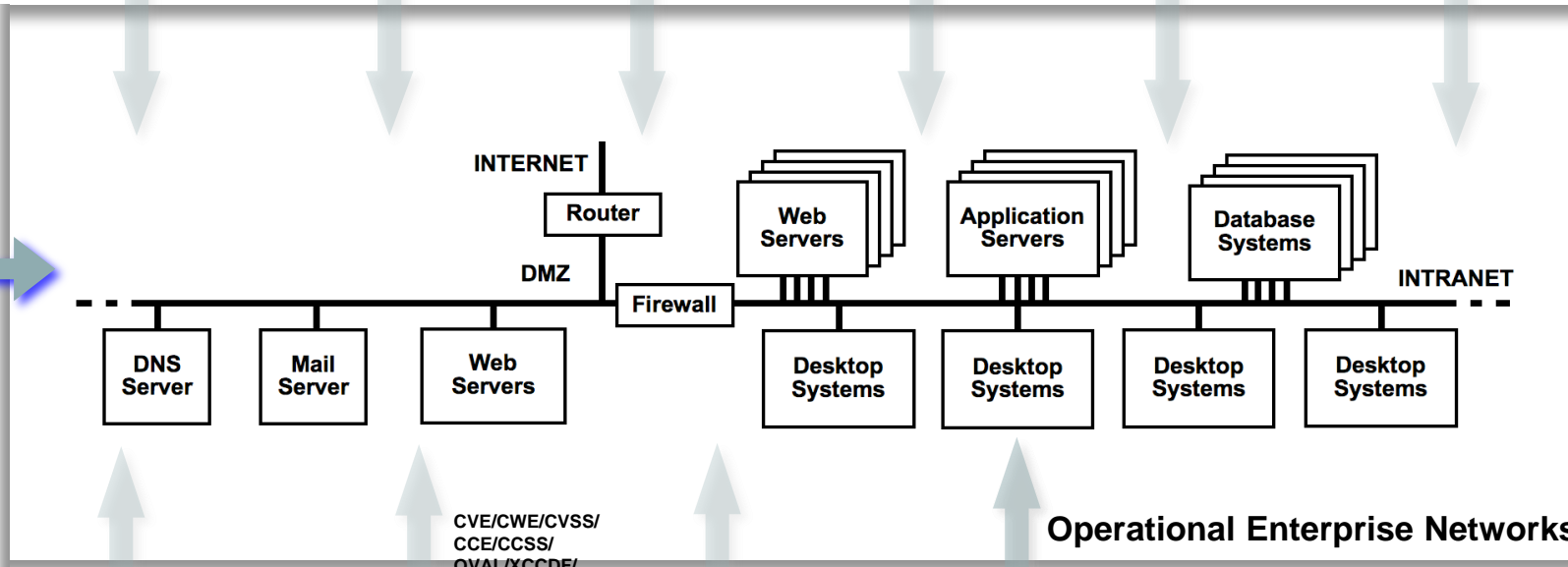
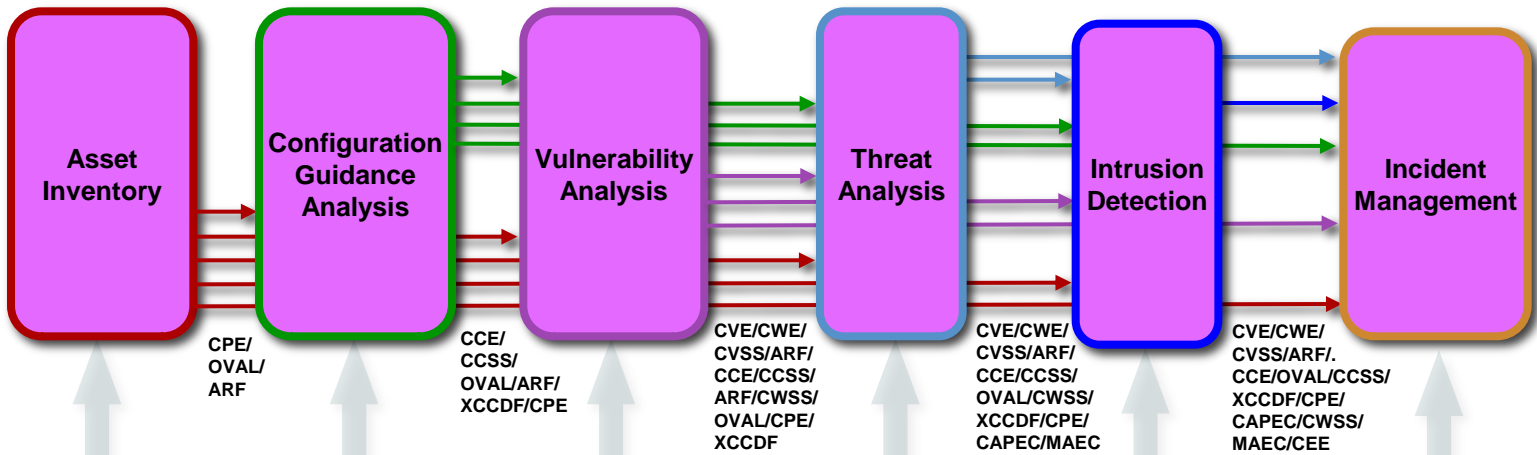
Operational Enterprise Networks



Enterprise IT Asset Management







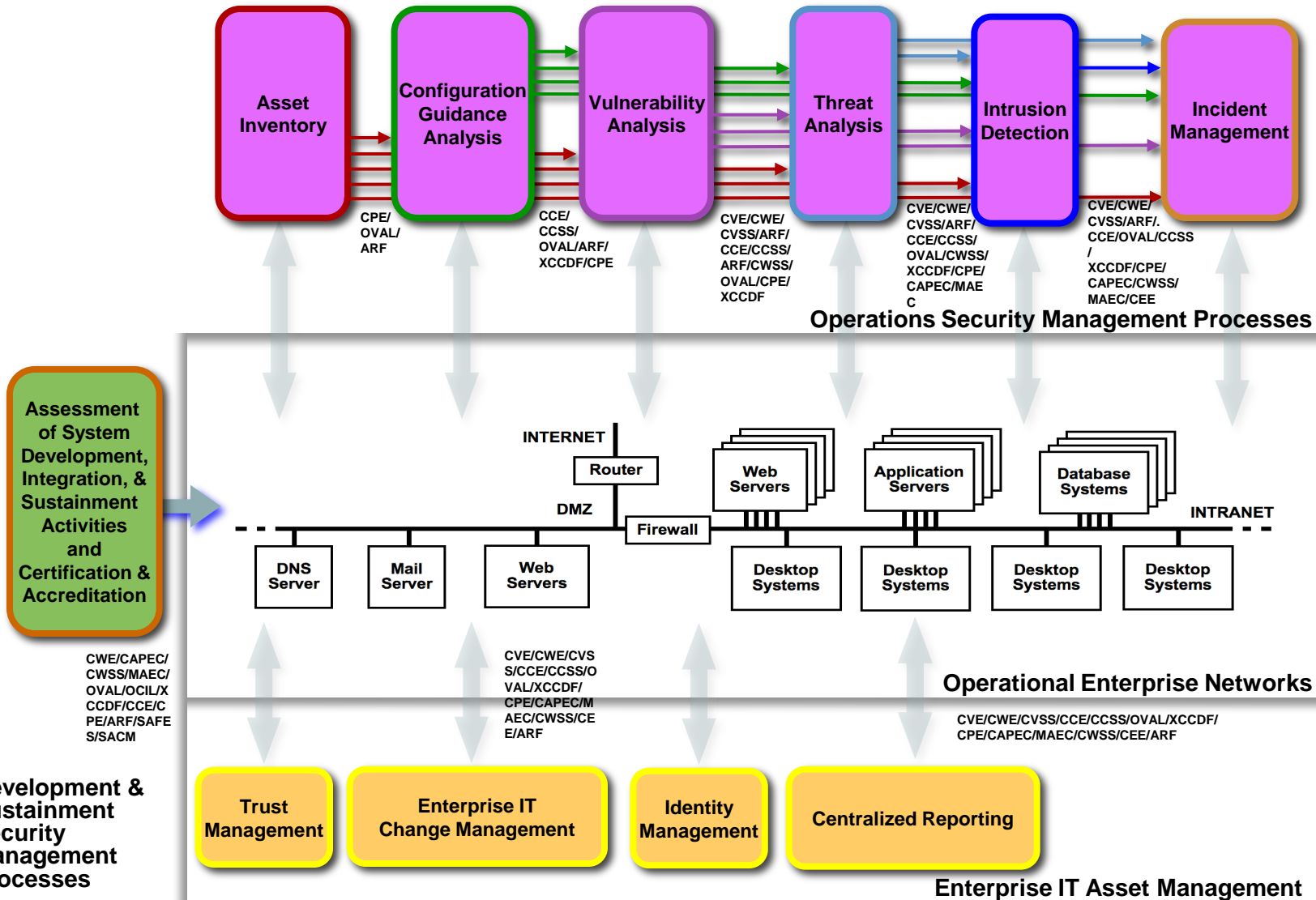
Development & Sustainment Security Management Processes

CWE/CAPEC/CWSS/MAEC/OVAL/OCIL/XCCDF/CCE/CP E/ARF/SAFES/SACM

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

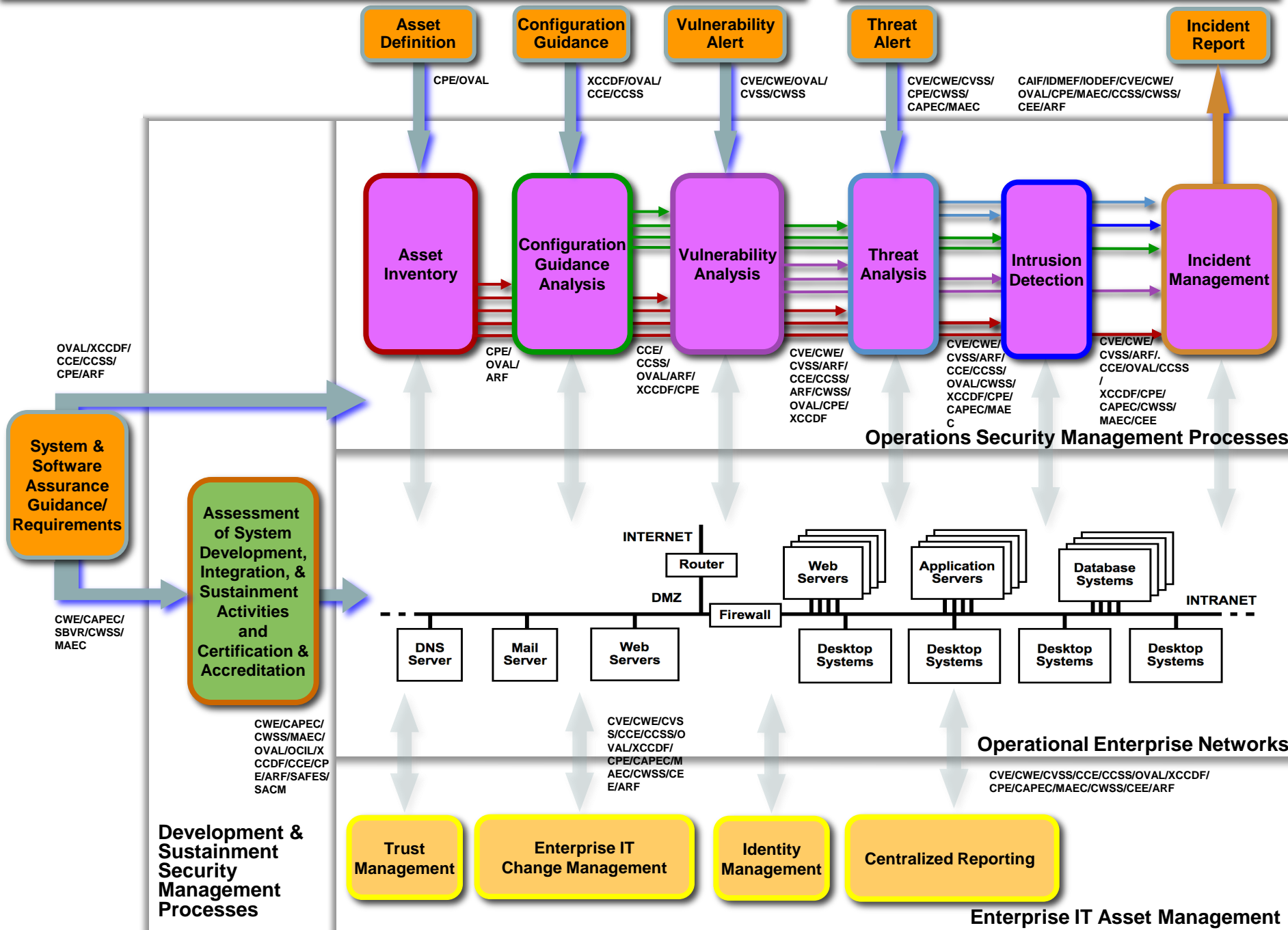
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/CPE/CAPEC/MAEC/SBVR/CWSS/CEE/ARF

Enterprise IT Asset Management

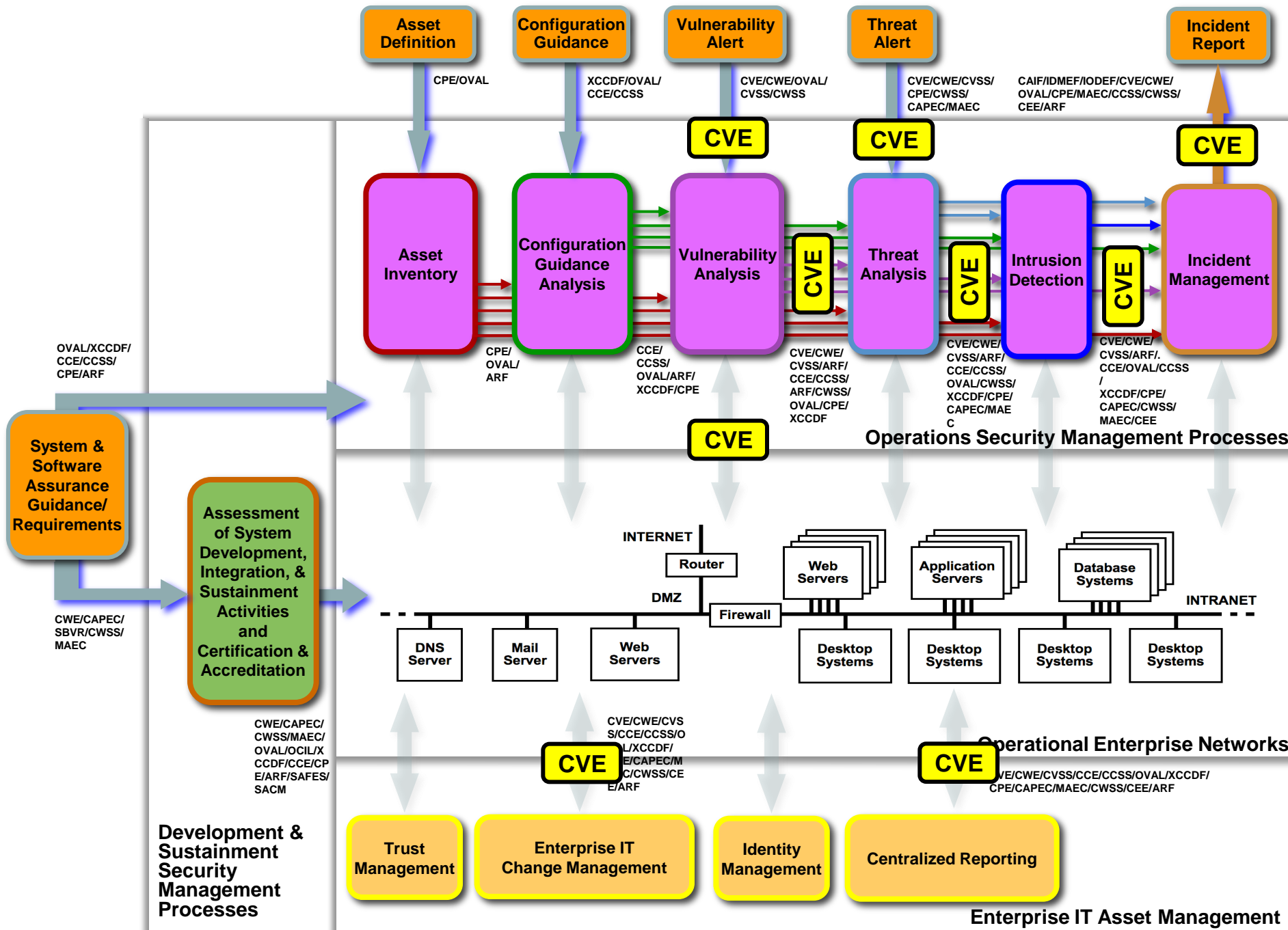


Mitigating Risk Exposures

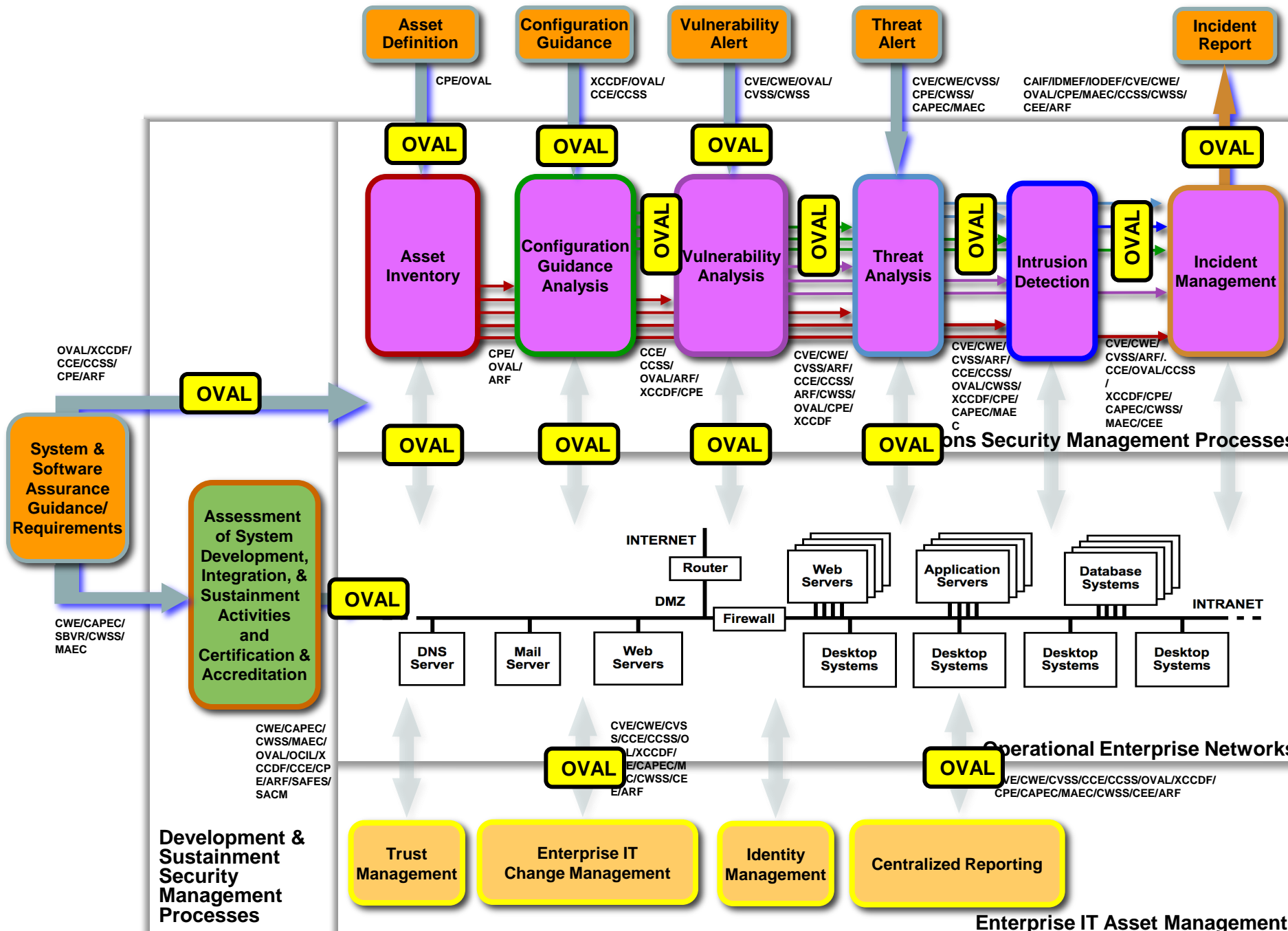
Responding to Security Threats



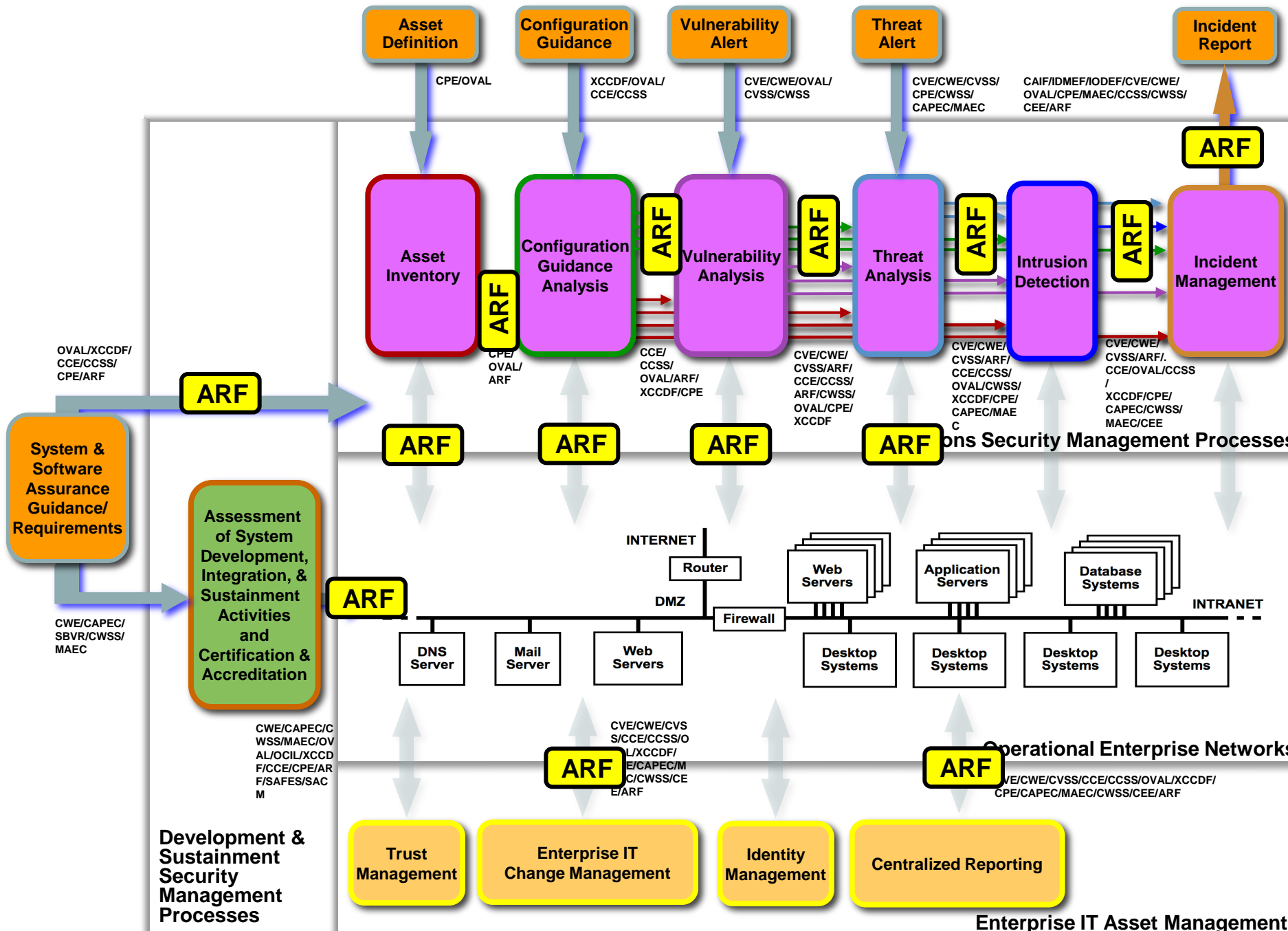
Knowledge Repositories



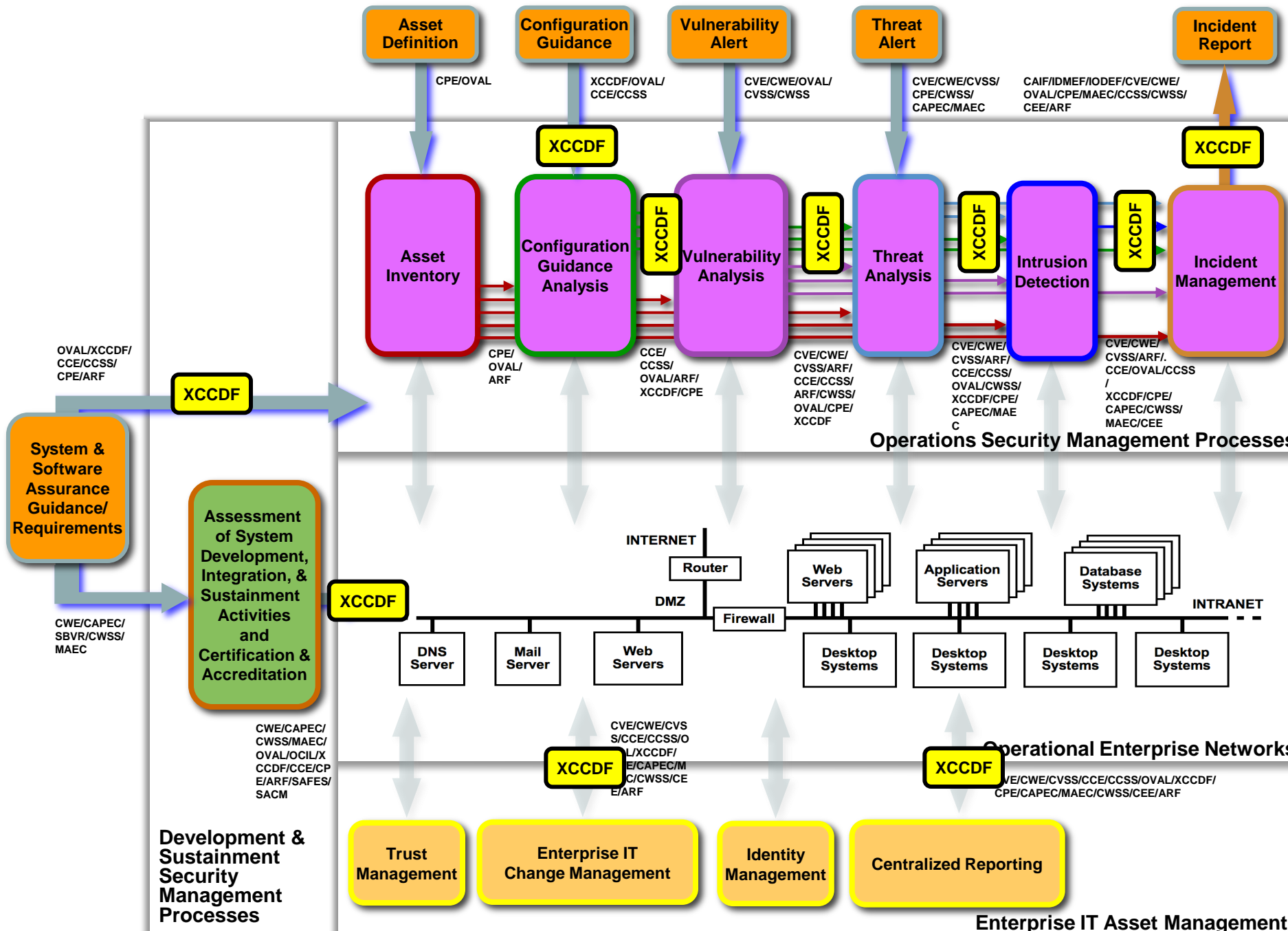
Knowledge Repositories



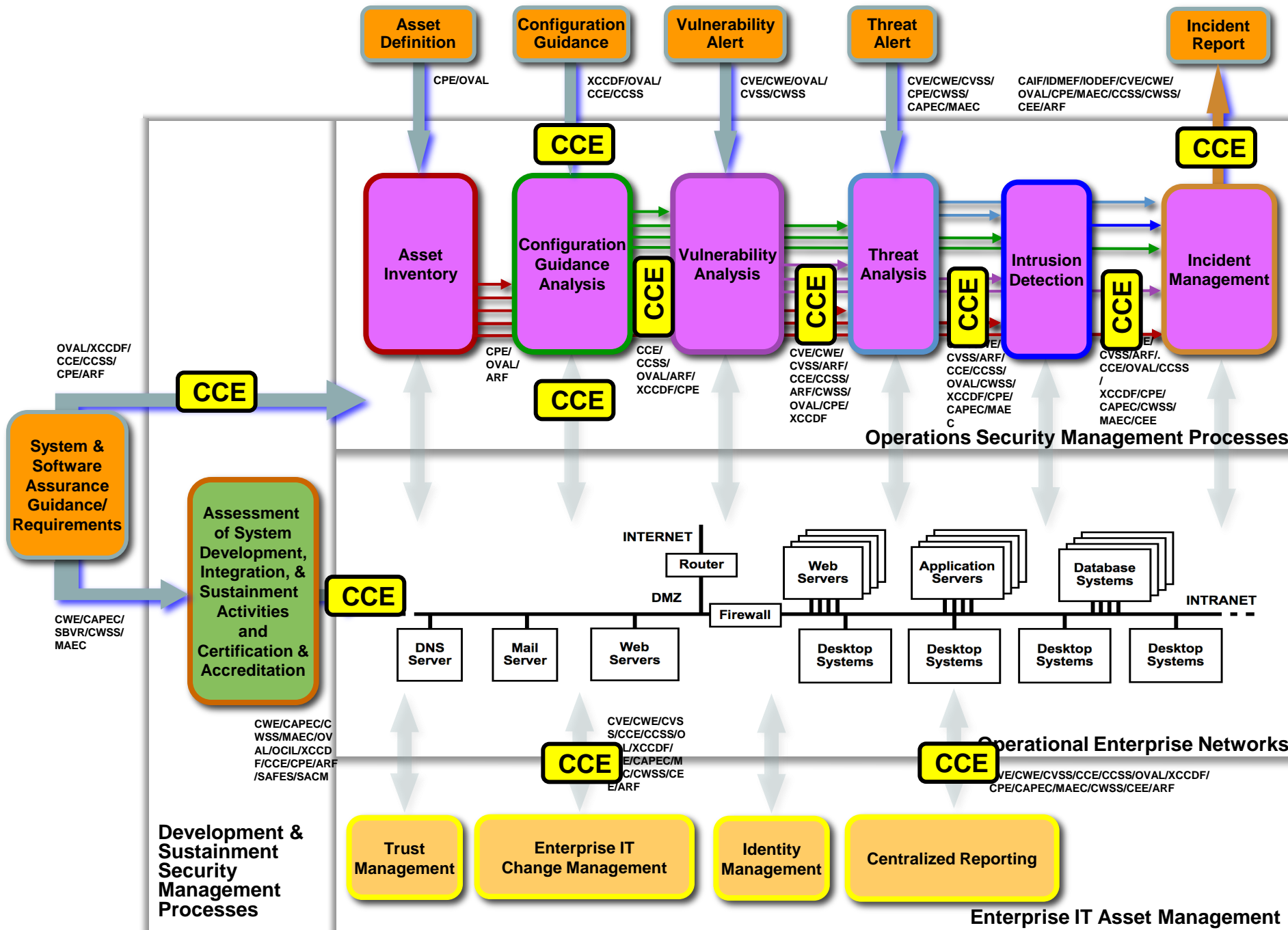
Knowledge Repositories



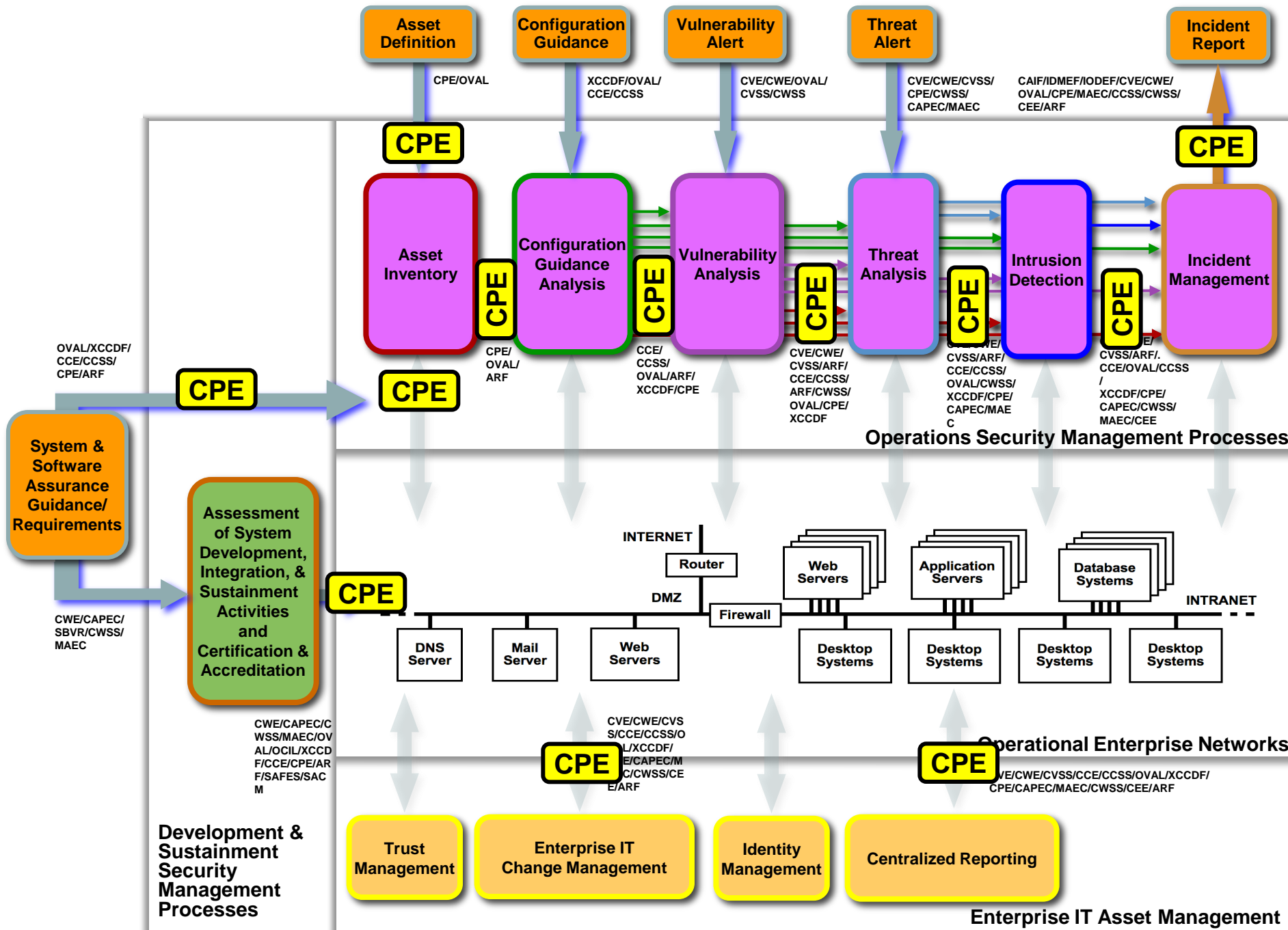
Knowledge Repositories



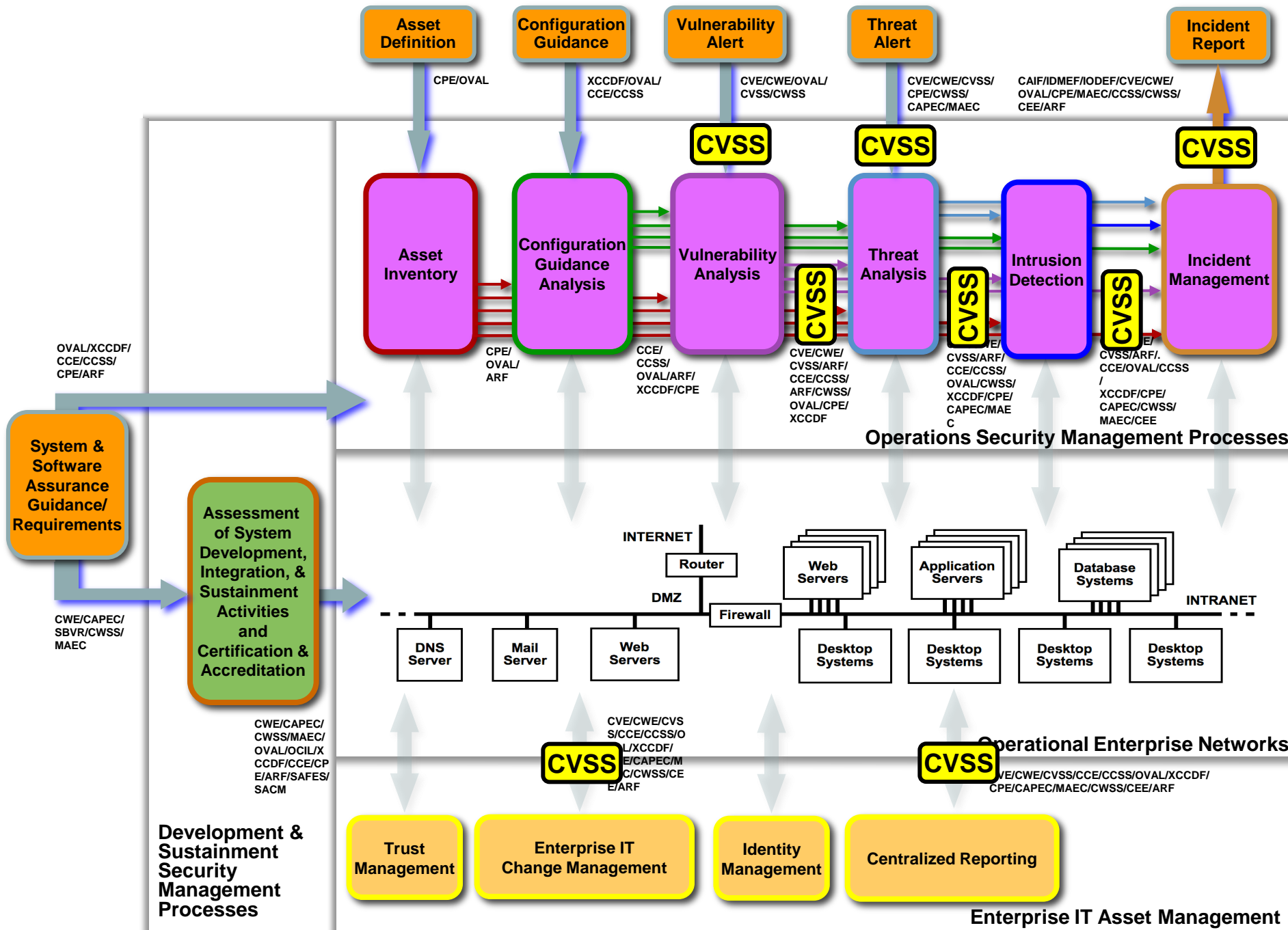
Knowledge Repositories



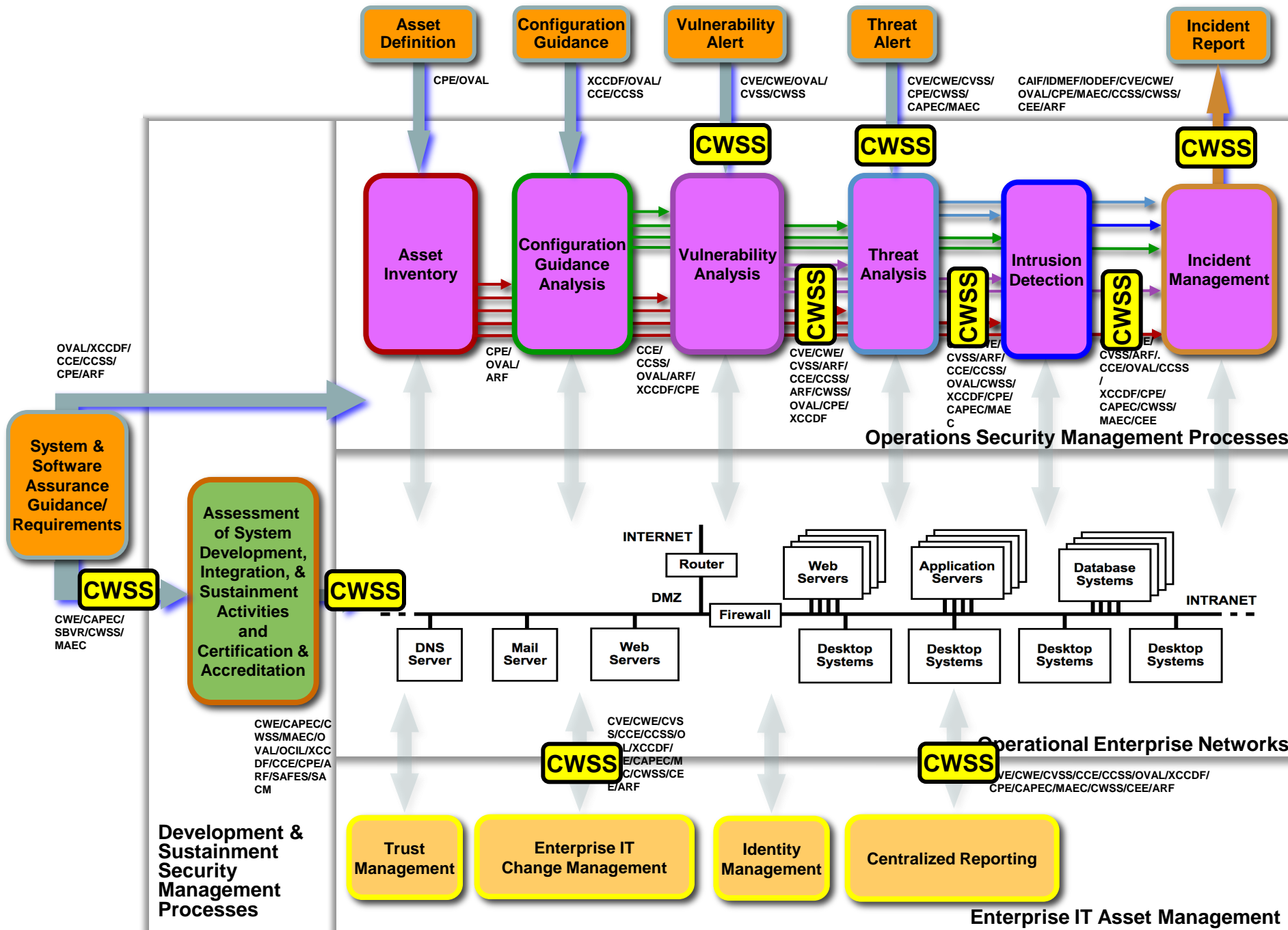
Knowledge Repositories



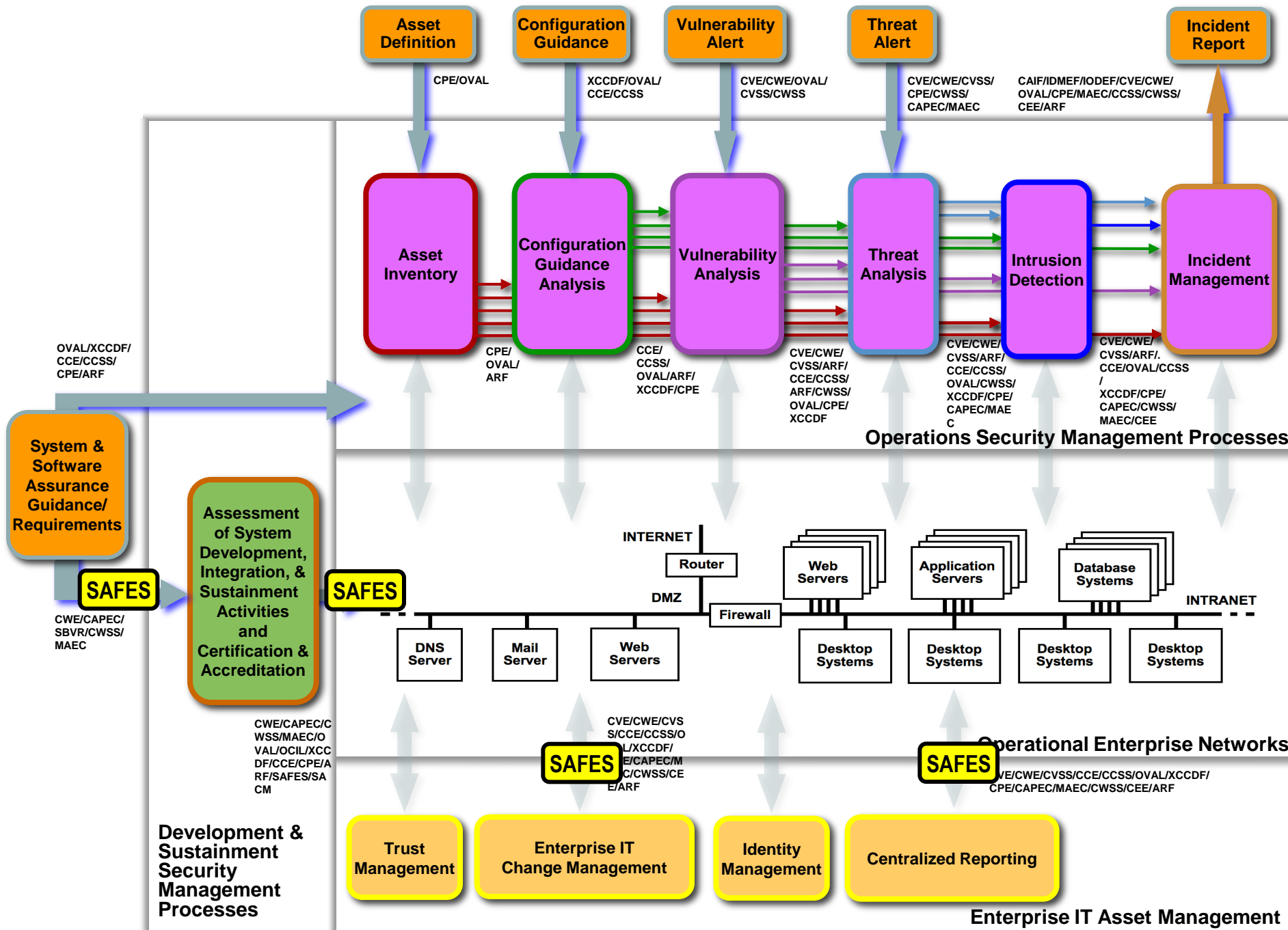
Knowledge Repositories



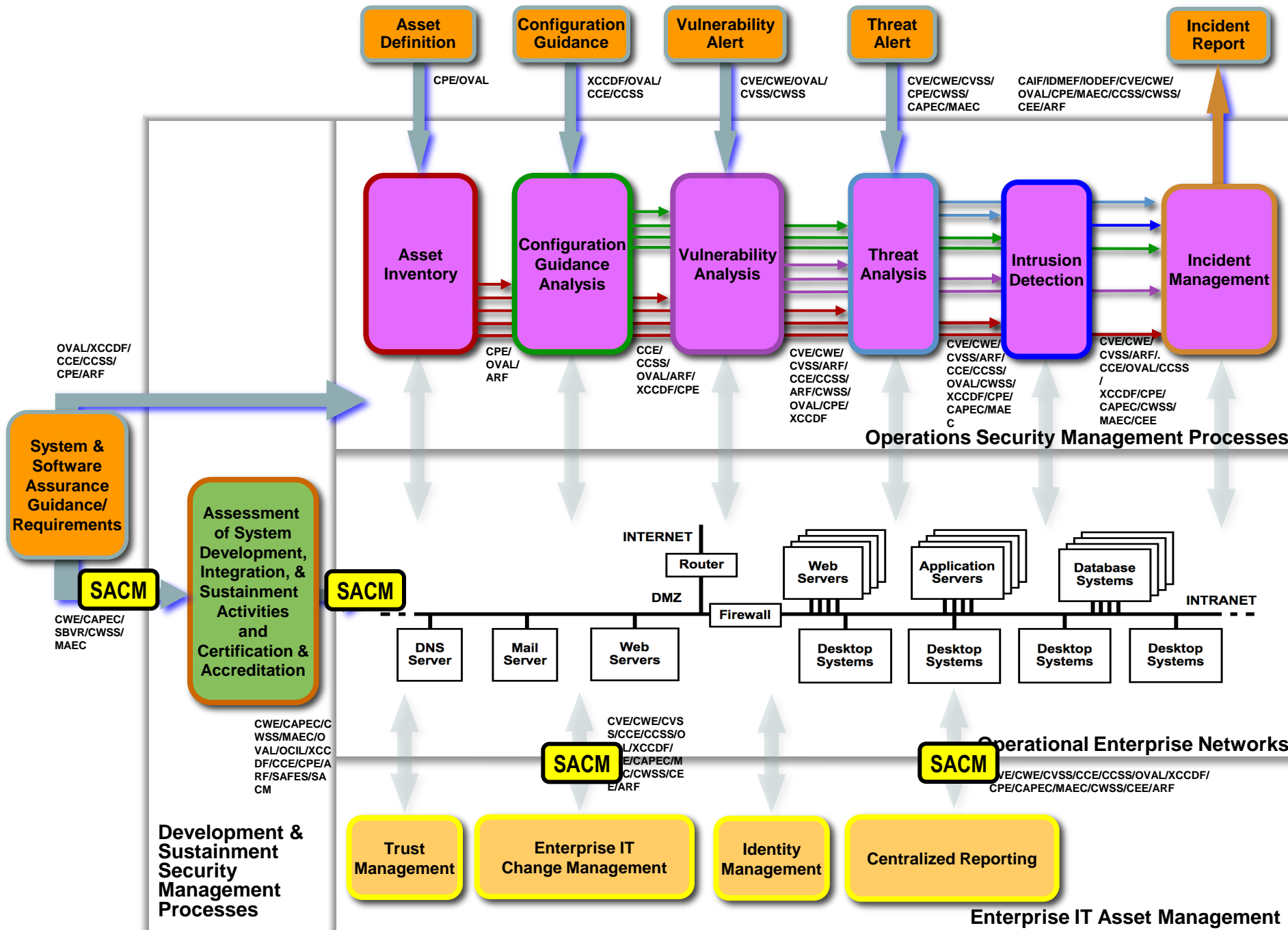
Knowledge Repositories



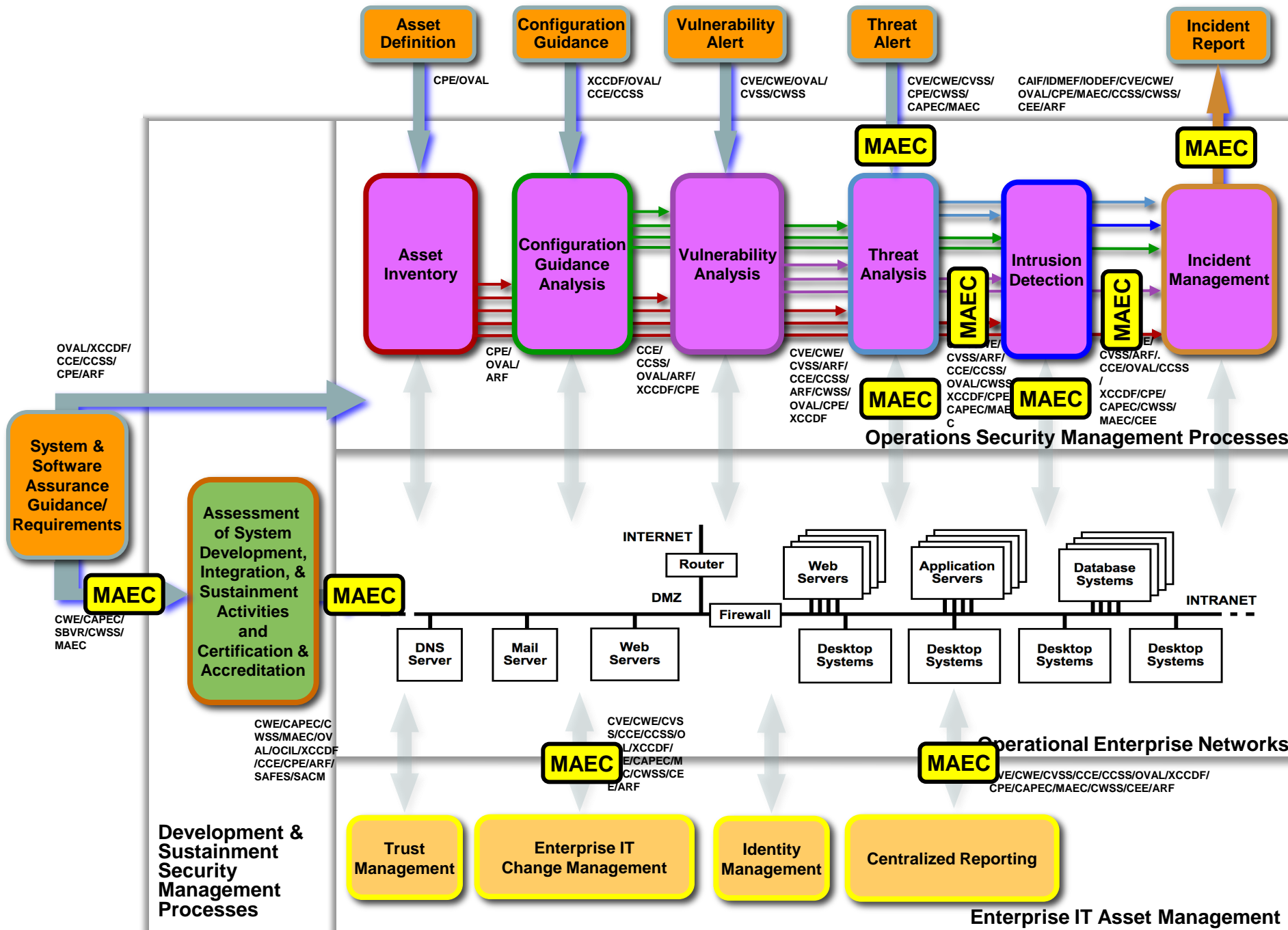
Knowledge Repositories



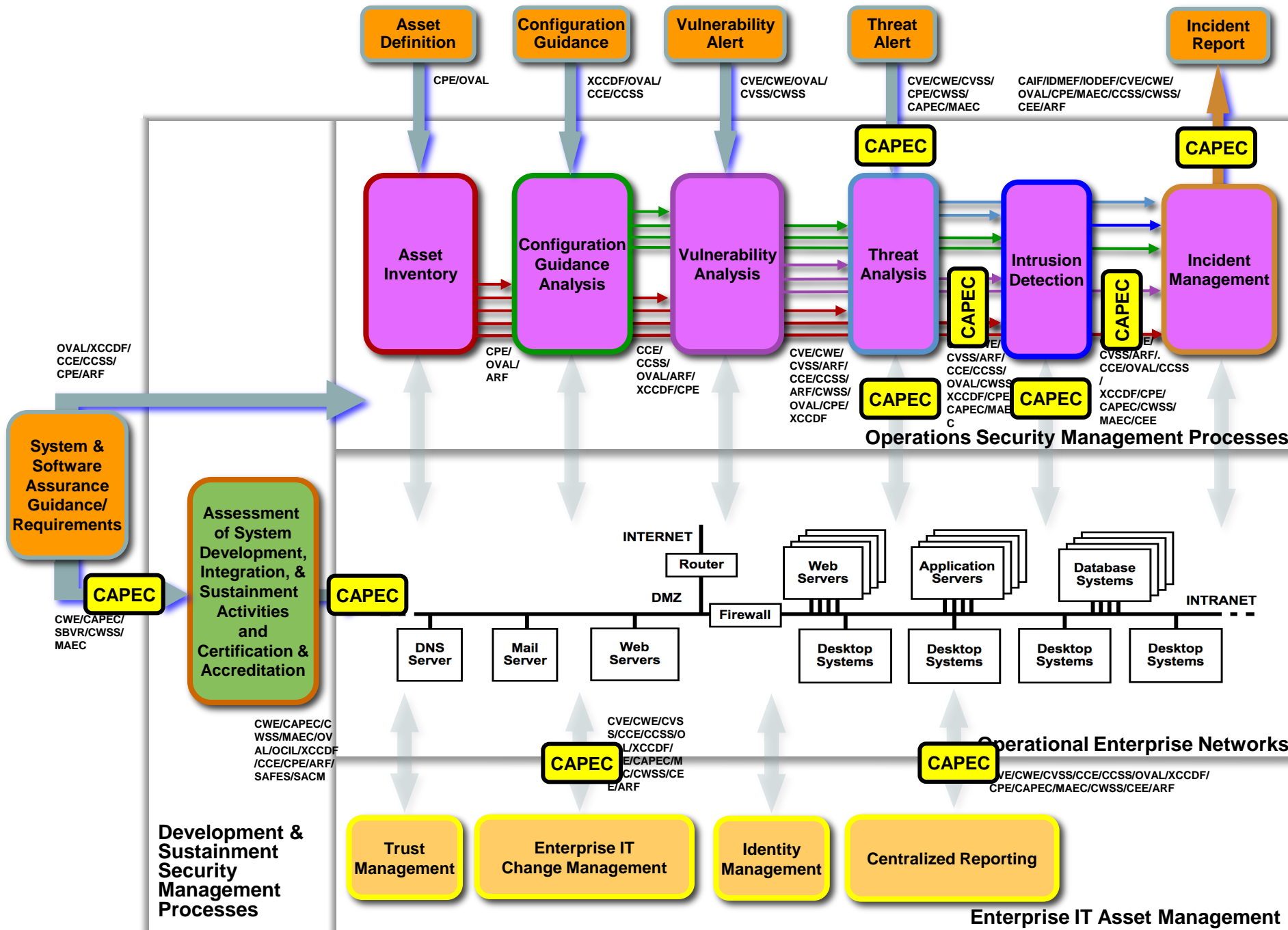
Knowledge Repositories



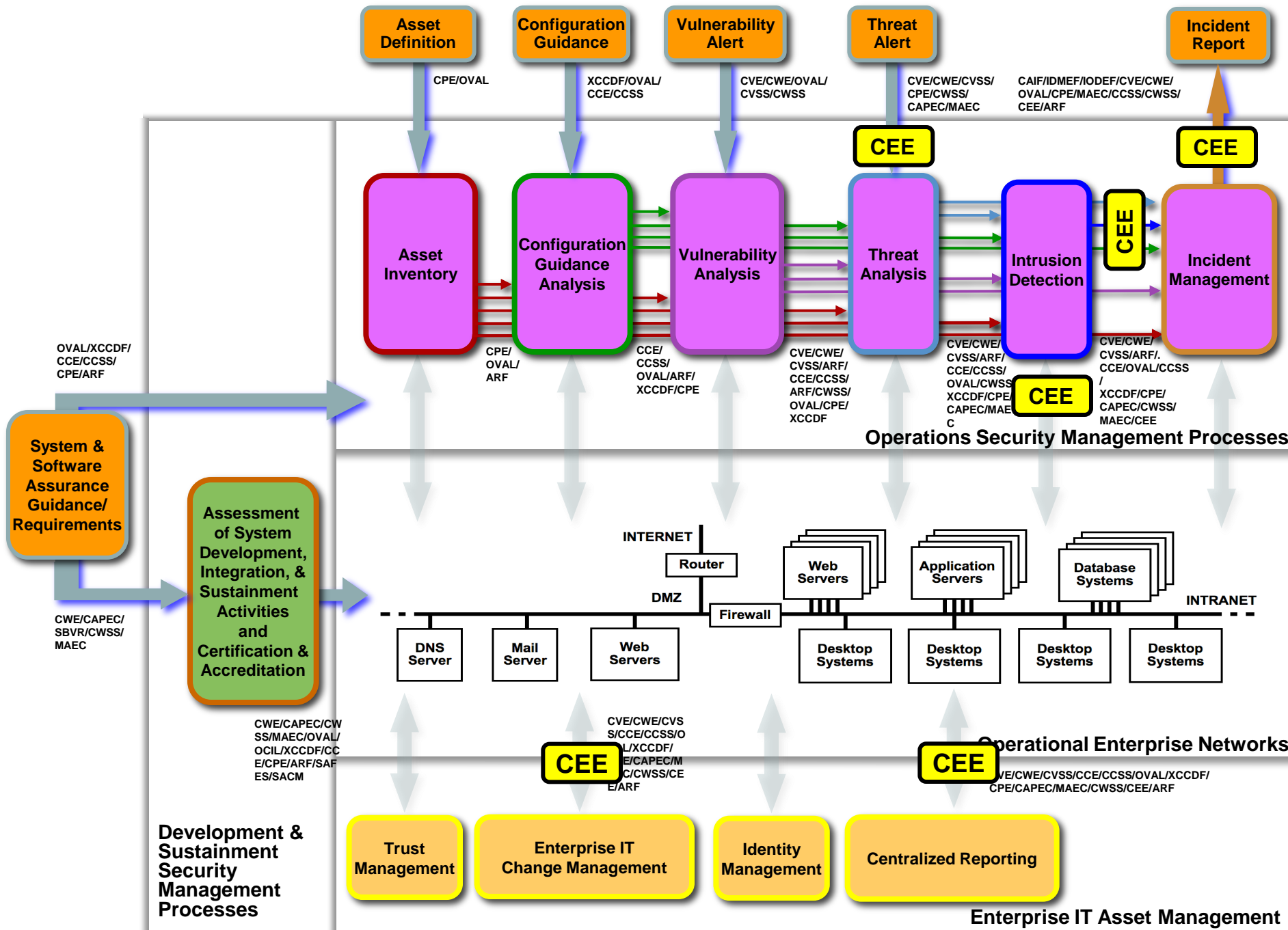
Knowledge Repositories



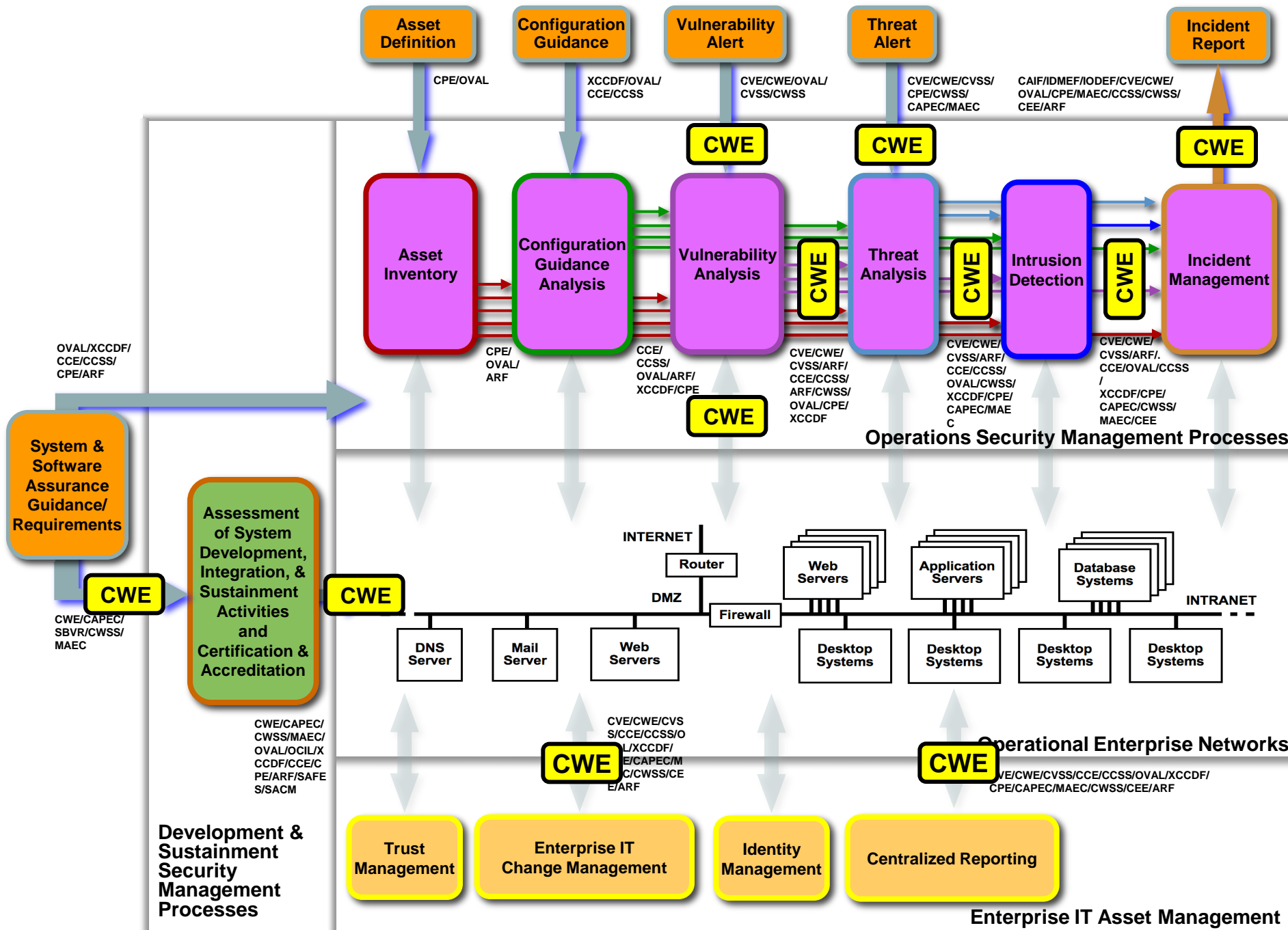
Knowledge Repositories



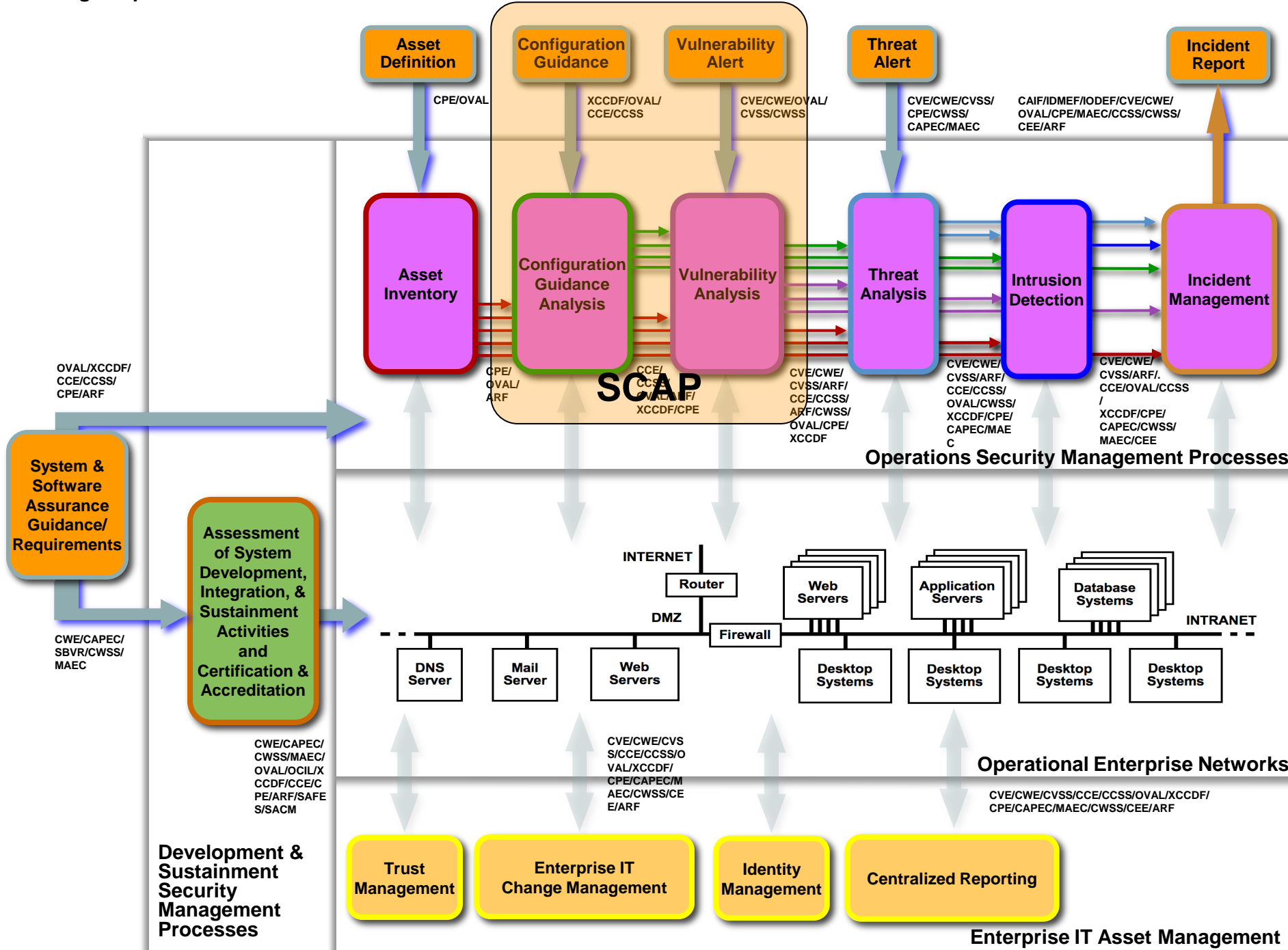
Knowledge Repositories



Knowledge Repositories



Knowledge Repositories





SCAP 1.1 uses the following specifications:

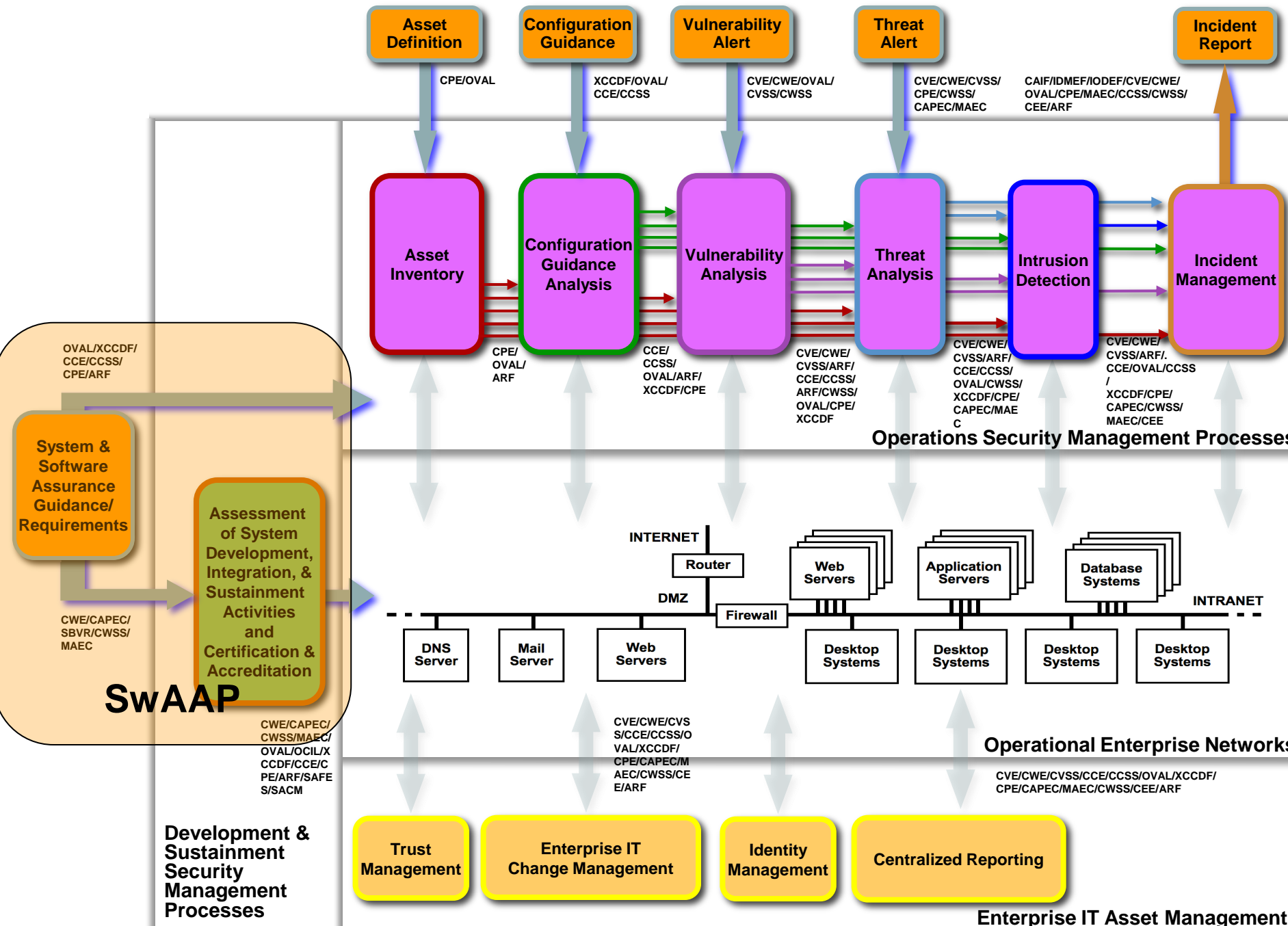
- Extensible Configuration Checklist Description Format (XCCDF) 1.1.4, a language for authoring security checklists/benchmarks and for reporting results of checklist evaluation [QUI08]
- Open Vulnerability and Assessment Language (OVAL) 5.6, a language for representing system configuration information, assessing machine state, and reporting assessment results
- Open Checklist Interactive Language (OCIL) 2.0, a language for representing security checks that requires human feedback
- Common Platform Enumeration (CPE) 2.2, a nomenclature and dictionary of hardware, operating systems, and applications [BUT09]
- Common Configuration Enumeration (CCE) 5, a nomenclature and configurations
- Common Vulnerabilities and Exposures (CVE), a nomenclature and software flaws⁹
- Common Vulnerability Scoring System (CVSS) 2.0, an open specification for the severity of software flaw vulnerabilities [MEL07].

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

Recommendations of the National Institute
of Standards and Technology

Stephen Quinn
David Waltermire
Christopher Johnson
Karen Scarfone
John Banghart

Knowledge Repositories



● Software Assurance Automation Protocol (SwAAP)

- For measuring & enumerating software weaknesses and the assurance cases.

CWE

CAPEC

MAEC

CWSS

OMG SACM

OMG ARG

SAFES

"Food Label"

OMG SMM

ISO 15026

OMG KDM

OMG ASTM

Common Weakness Enumeration (CWE),

Common Attack Pattern Enumeration & Classification (CAPEC),

Malware Attribute Enumeration & Characterization (MAEC),

Common Weakness Scoring System (CWSS),

OMG Structured Assurance Case Metamodel (OMG SACM),

Software Assurance Findings Expression Schema (SAFES),

NIST SAMATE's "Food Label",

OMG Structured Metrics Metamodel (OMG SMM),

ISO "Assurance Case" 15026 (ISO 15026),

OMG Knowledge Discovery Metamodel (OMG KDM),

OMG Abstract Syntax Tree Metamodel (OMG ASTM)

- plus SCAP to capture "accredited" system CPEs and CCE settings?
- OVAL checks for capturing "finger print" of software applications to address supply-chain risk measurement?

[makingsecuritymeasurable.mitre.org]

Making Security Measurable

http://msm.mitre.org/

Home | About | Current Collection | Incubator | Events & Participation | 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	Languages	Repositories
<p>CVE Common Vulnerabilities and Exposures (CVE®) - common vulnerability identifiers</p> <p>CWE Common Weakness Enumeration (CWE™) - list of software weakness types</p> <p>CAPEC Common Attack Pattern Enumeration and Classification (CAPEC™) - list of common attack patterns</p> <p>CCE Common Configuration Enumeration (CCE™) - common security configuration identifiers</p> <p>CPE Common Platform Enumeration (CPE™) - common platform identifiers</p> <p>CWE/SANS Top 25 - consensus list of the 25 most dangerous programming errors</p> <p>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</p> <p>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</p> <p>SANS Top Twenty - SANS/FBI consensus list of the Twenty Most Critical Internet Security Vulnerabilities that uses CVE-IDs to identify the issues</p> <p>OWASP Top Ten - ten most critical Web application security flaws</p> <p>WASC Web Security Threat Classification - list of Web security threats</p>	<p>OVAXL Open Vulnerability and Assessment Language (OVAXL®) - standard for determining vulnerability and configuration issues</p> <p>CEE Common Event Expression (CEE™) - standardizes the way computer events are described, logged, and exchanged</p> <p>MAEC Malware Attribute Enumeration and Characterization (MAEC™) - standardized language for attribute-based malware characterization</p> <p>Benchmark Development - resources for creating standards-based, structured, and automatable security guidance</p> <p>OVAL Interpreter - free tool for collecting information for testing, carrying out OVAL Definitions, and presenting results of the tests</p> <p>Benchmark Editor™ - free tool that enhances and simplifies creation and editing of benchmark documents written in XCCDF and OVAL</p> <p>Recommendation Tracker™ - free tool that facilitates the development of automated security benchmarks</p> <p>Extensible Configuration Checklist Description Format (XCCDF) - specification language for uniform expression of security checklists, benchmarks, and other configuration guidance</p> <p>Open Checklist Interactive Language (OCIL) - standardized language for expressing and evaluating non-automated security checks</p> <p>Common Vulnerability Scoring System (CVSS) - open standard that conveys vulnerability severity and helps determine urgency and priority of response</p> <p>Policy Language for Assessment Results Reporting (PLARR) - language for requesting IT asset assessment results from tools, databases, and other products</p> <p>Assessment Results Format (ARF) - open language for exchanging per-device assessment results data between assessment tools, asset databases, and other products that manage asset information</p> <p>Assessment Summary Results (ASR) - language for exchanging summarized assessment results data</p>	<p>OVAXL REPOSITORY OVAL Repository - community-developed OVAL Vulnerability, Compliance, Inventory, and Patch Definitions</p> <p>National Vulnerability Database (NVD) - U.S. vulnerability database based on CVE that integrates all publicly available vulnerability resources and references</p> <p>NIST Security Content Automation Protocol (SCAP) - security content for automating technical control compliance activities, vulnerability checking, and security measurement</p> <p>Red Hat Repository - OVAL Patch Definitions corresponding to Red Hat Errata security advisories</p> <p>Novell Repository - OVAL Definitions for SUSE Linux Enterprise compliance checking</p> <p>Debian Repository - OVAL Definitions corresponding to Debian security advisories</p> <p>National Checklist Program Repository - U.S. government repository of publicly available security checklists/benchmarks</p> <p>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</p> <p>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</p> <p>Common Frameworks for Vulnerability Disclosure and Response (CVDR) - standard format for reporting and sharing vulnerability information among multiple organizations</p> <p>Federal Desktop Core Configuration (FDCC) - OMB-mandated security configuration for Microsoft Windows Vista and XP operating system software</p> <p>United States Government Configuration Baseline (USGCB) - security configuration baselines for IT products deployed across federal agencies</p>

[View the current collection of organizations, activities, and initiatives.](#)

[Disclaimer](#)

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

Page Last Updated: September 02, 2010

Done

Questions?

