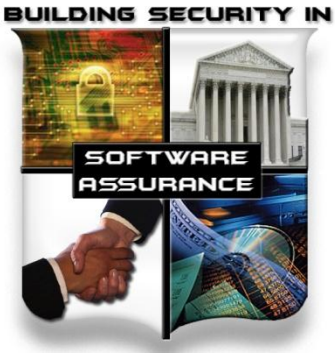
Homeland Security

Commerce

National Defense



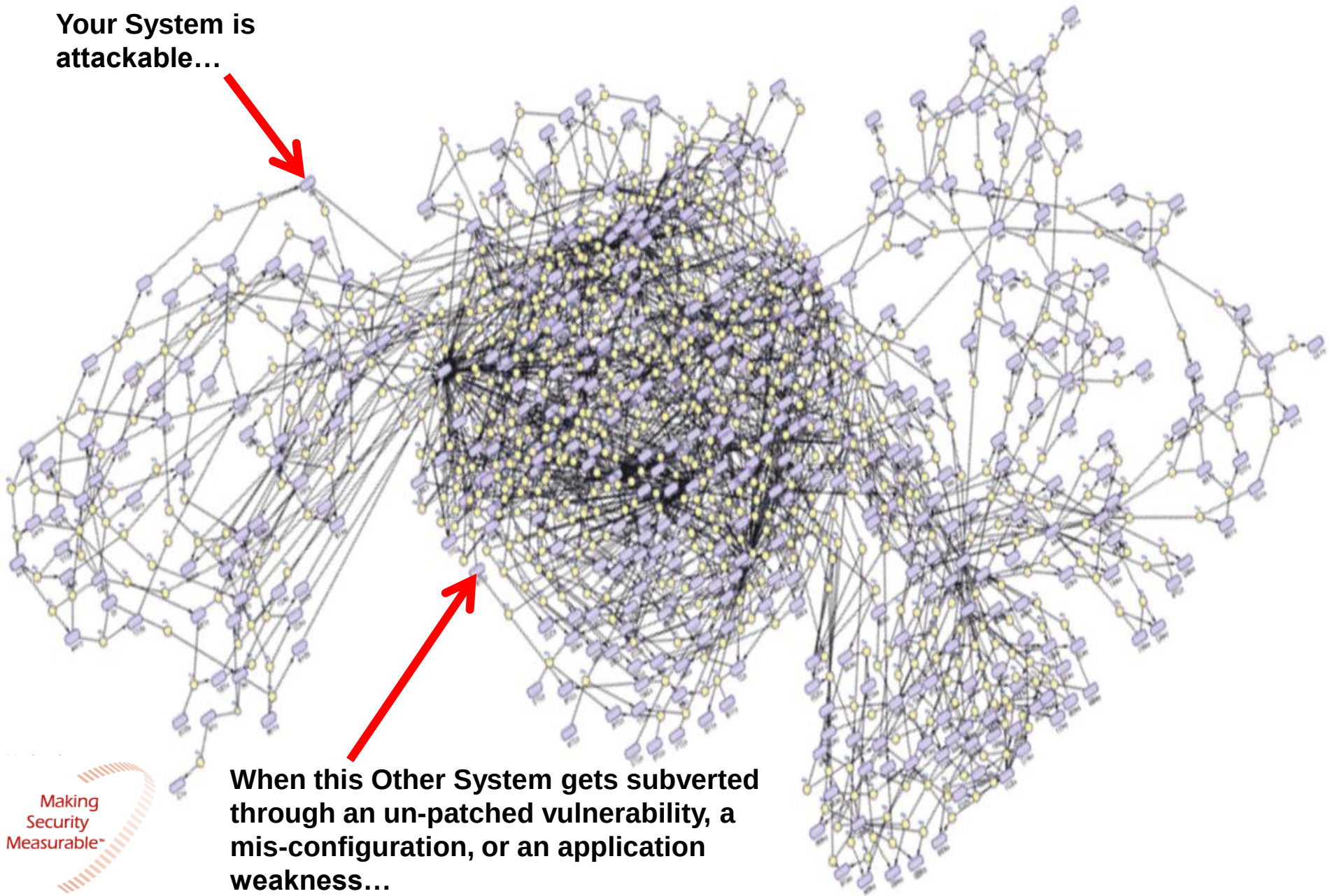
The Cybersecurity Ecosystem & Making Security Measurable

Making Security Measurable™

Robert A. Martin
28 Feb 2011

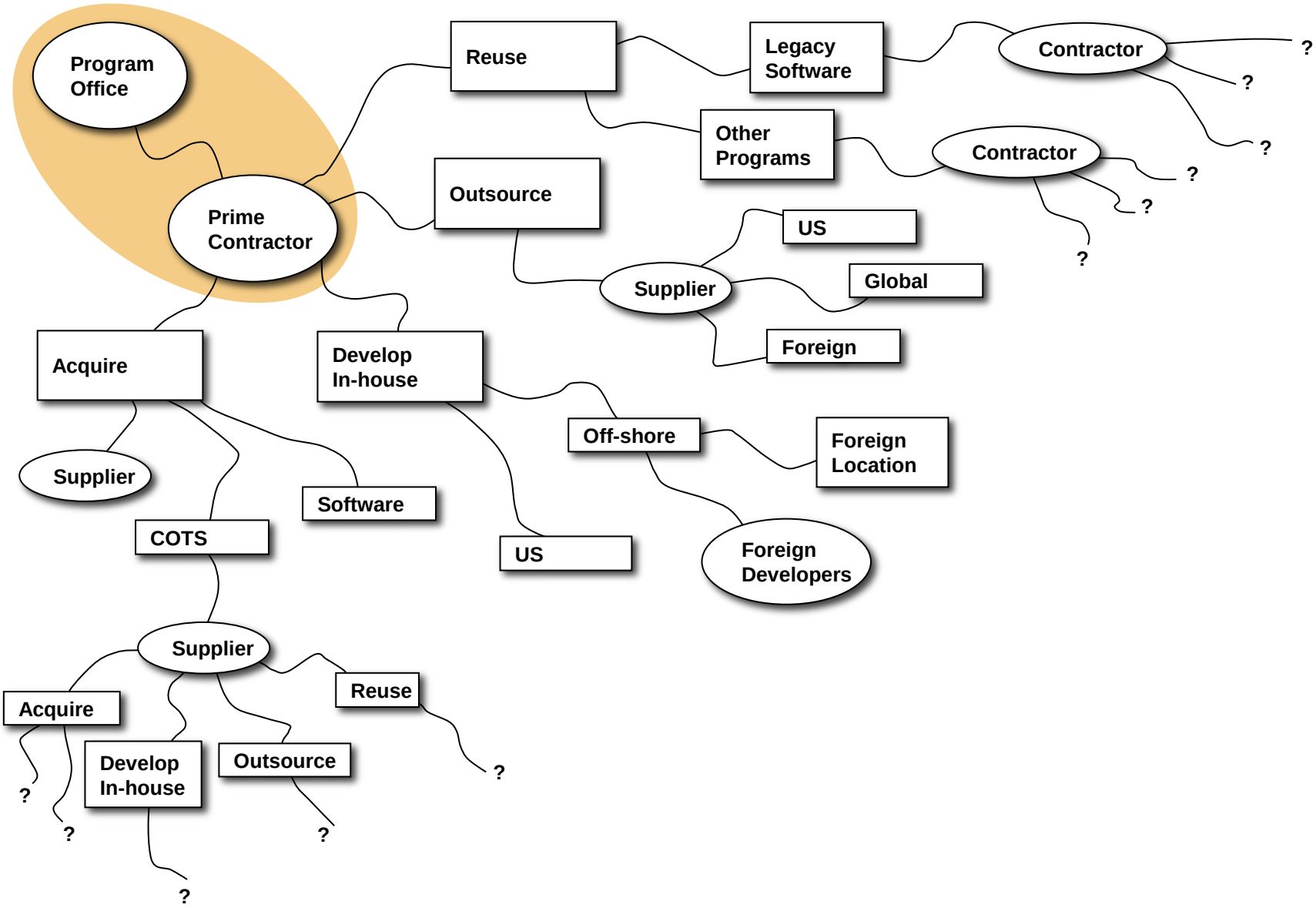
MITRE

Today Everything's Connected



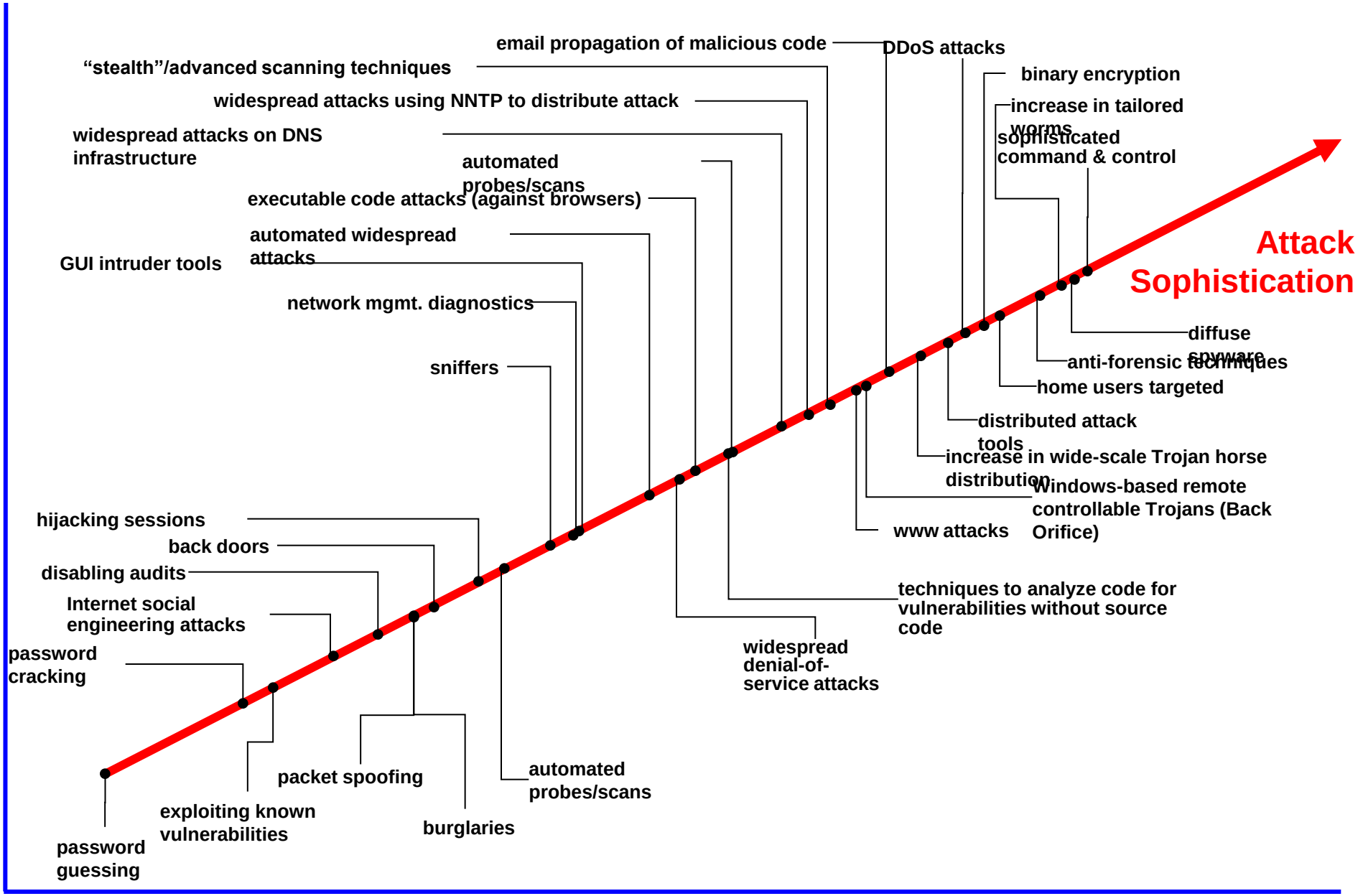
Making Security Measurable™

The Software Supply Chain

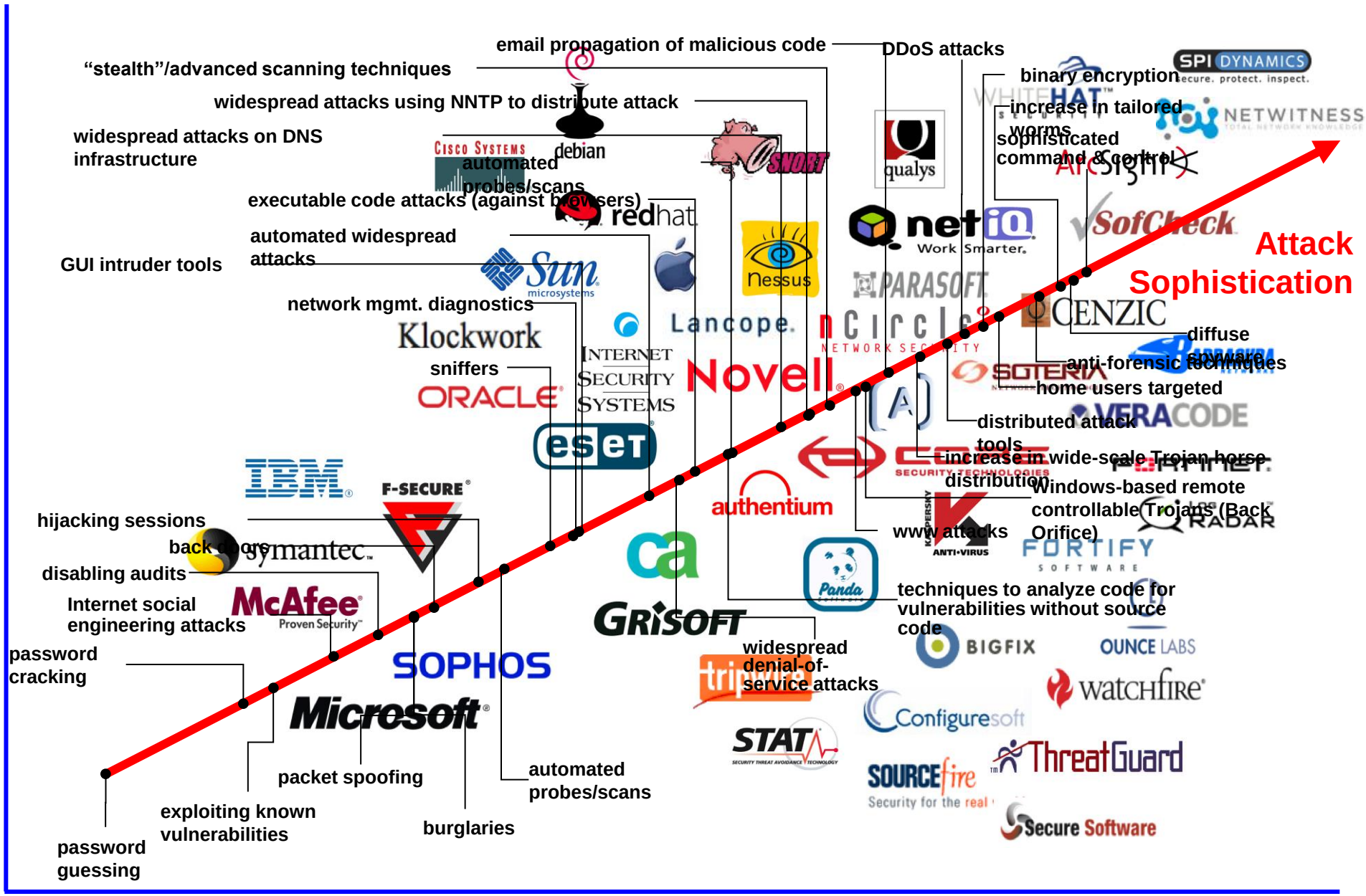


* "Scope of Supplier Expansion and Foreign Involvement" graphic in DACS www.softwaretechnews.com Secure Software Engineering, July 2005 article "Software Development Security: A Risk Management Perspective" synopsis of May 2004 GAO-04-678 report "Defense Acquisition: Knowledge of Software Suppliers Needed to Manage Risks"

Cyber Threats Emerged Over Time



Solutions Also Emerged Over Time

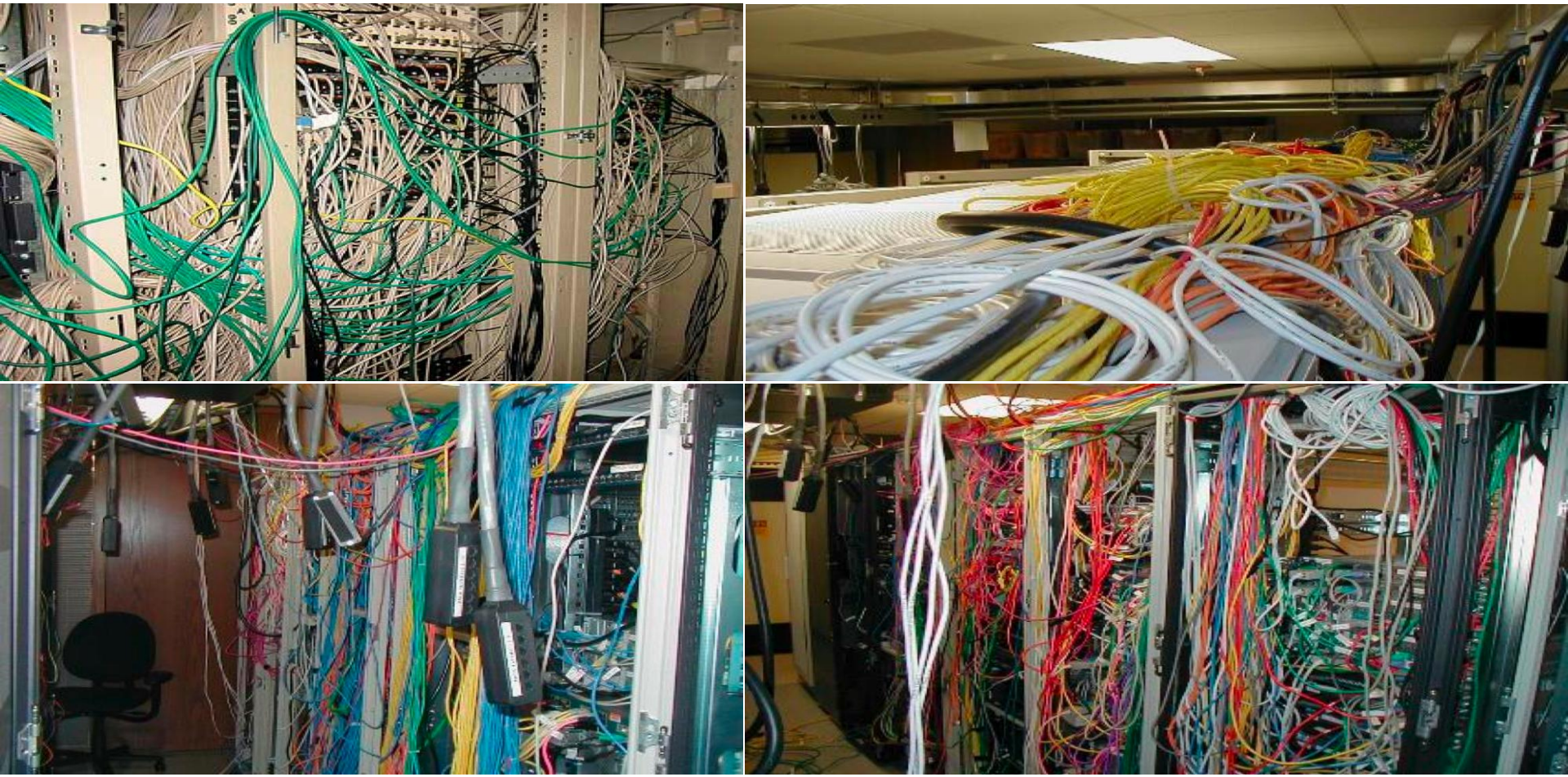


Why Should We Re-Architect Cybersecurity?

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



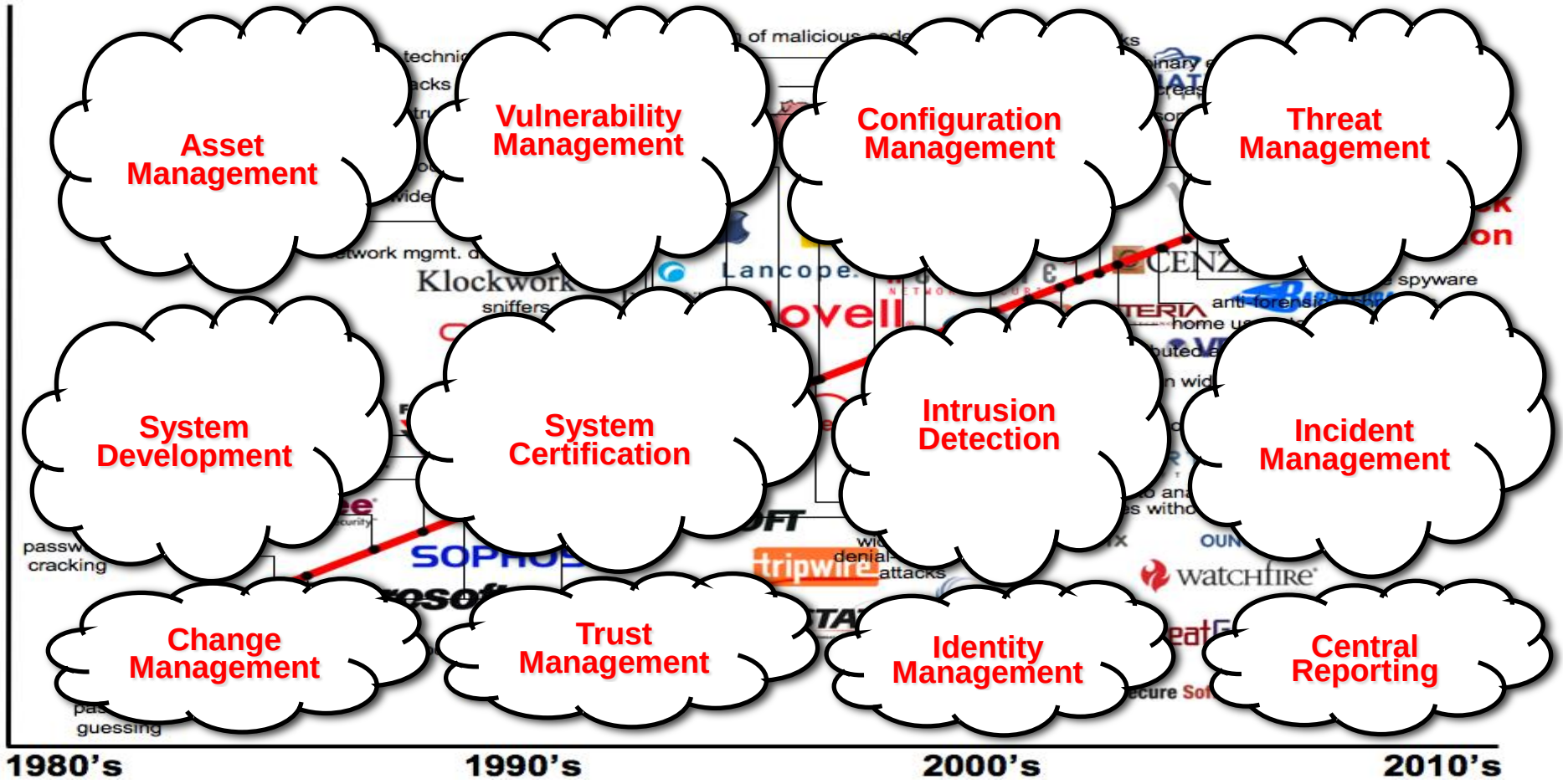
Each new solution had to integrate with the existing solutions

-->> 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

Making Security Measurable™

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

Making Security Measurable™

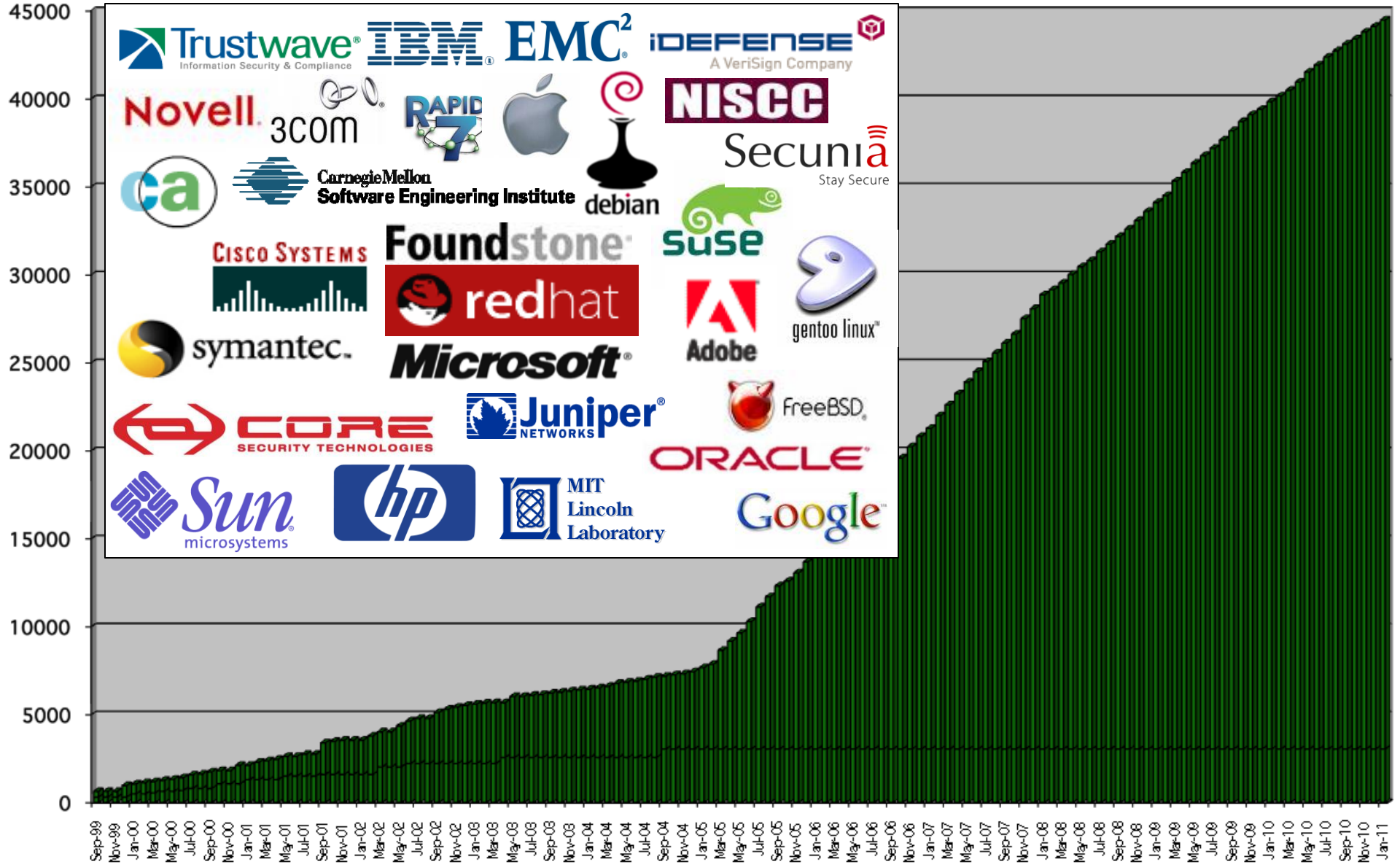
The Building Blocks Are:

- 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 (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)**

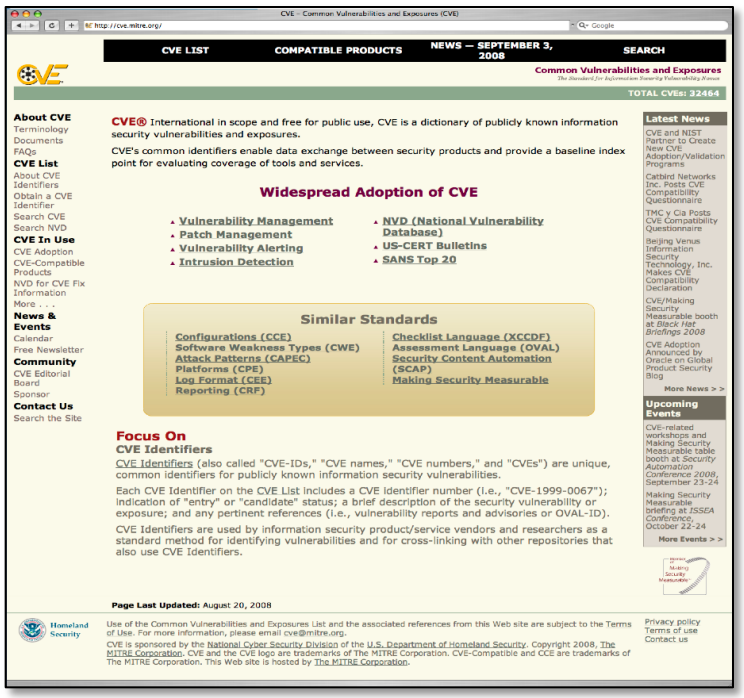
Tools

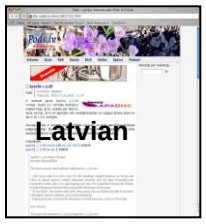
- **Interpret IA, Cyber Security, and SwA content in context of enterprise network**
- **Methods for assessing compliance to languages, formats, and enumerations**

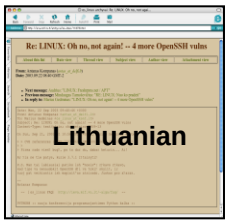
CVE 1999 to 2011

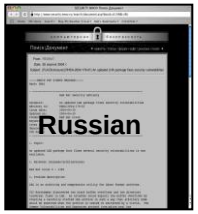


CVE is Widely Used & Available
45,218 and climbing…









CVE Vendor/Industry Engagement

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:

CVE

OVAL

NIST/DHS NVD

Vulnerability Alerts

Knowledge Repository

Knowledge Repositories

Vulnerability Alerts

Red Hat errata

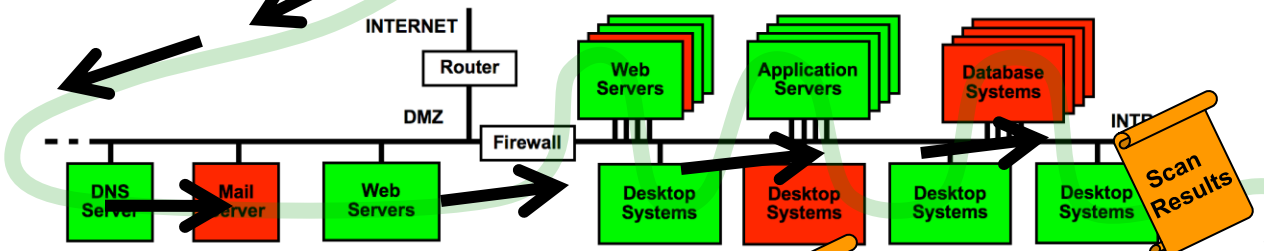
Vulnerability Analysis

Operations Security Management Processes

OVAL "Compatible" Tools

MODULO Solutions for GRC · QUALYS · McAfee · NIST National Institute of Standards and Technology · ca · bmcsoftware · Greenbone · G2 · Microsoft System Center Configuration Manager · Shavlik · ThreatGuard · Configuresoft · BIGFIX · INVERSE PATH · Telos · FORTINET · Lumension SECURITY · tripwire TAKE CONTROL · CERDEC · SAINT · the CENTER for INTERNET SECURITY · PRISM MICROSYSTEMS · netiq · SPAWAR · LANDesk · symantec · SignaCert · hp · redhat · Novell · nCircle · catbird · GIDEON TECHNOLOGIES · Triumfant · Systems Center ATLANTIC · Atlantic Systems Group, Inc.

Operational Enterprise Networks



Enterprise IT Asset Management

Scan Results

Scan Results

Enterprise IT Change Management

Centralized Reporting

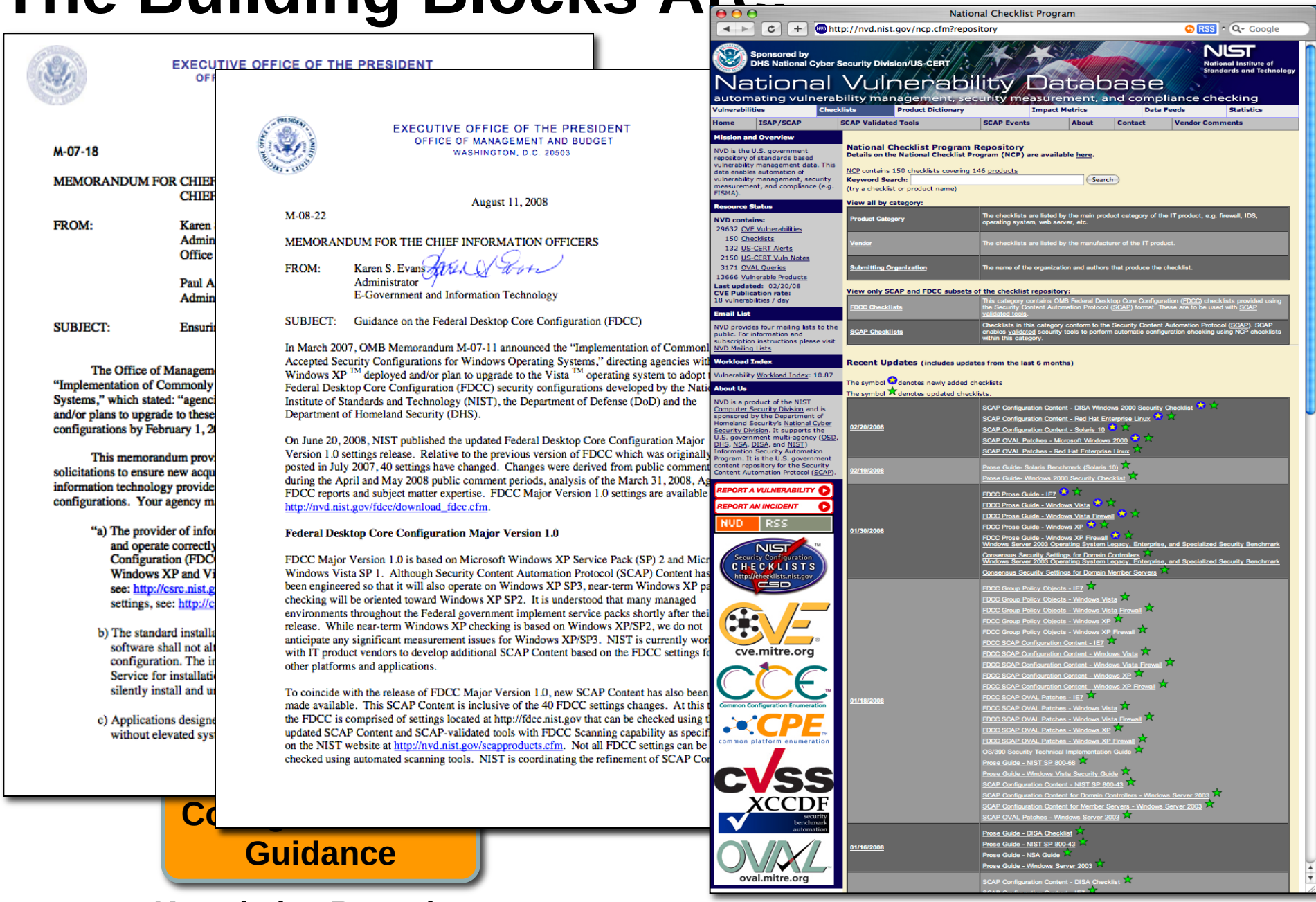
The Building Blocks Are:

- 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:



Guidance

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

FDCC

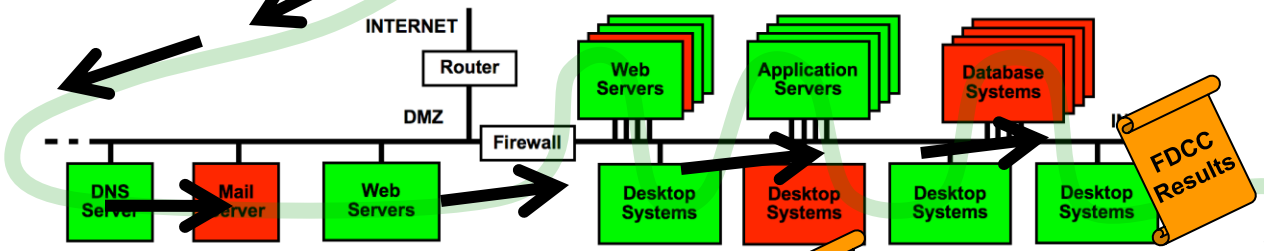
Configuration Guidance Analysis

Operations Security Management Processes

FDCC Compliant Tools

TENABLE Network Security, nCircle, ThreatGuard, netIQ, SignaCert, hp, symantec., Telos, Lumension SECURITY, Shavlik, tripwire TAKE CONTROL., LANDesk SOFTWARE, the CENTER for INTERNET SECURITY, ca, bmcsoftware, ag Atlantic Systems Group, Inc. Service-Disabled Veteran-Owned Small Business, McAfee, BIGFIX, FORTINET, eEye Digital Security, QUALYS, GIDEON TECHNOLOGIES Know your assets. Know your risk., PRISM MICROSYSTEMS, Triumfant, Systems Center ATLANTIC, Microsoft System Center Configuration Manager

Operational Enterprise Networks



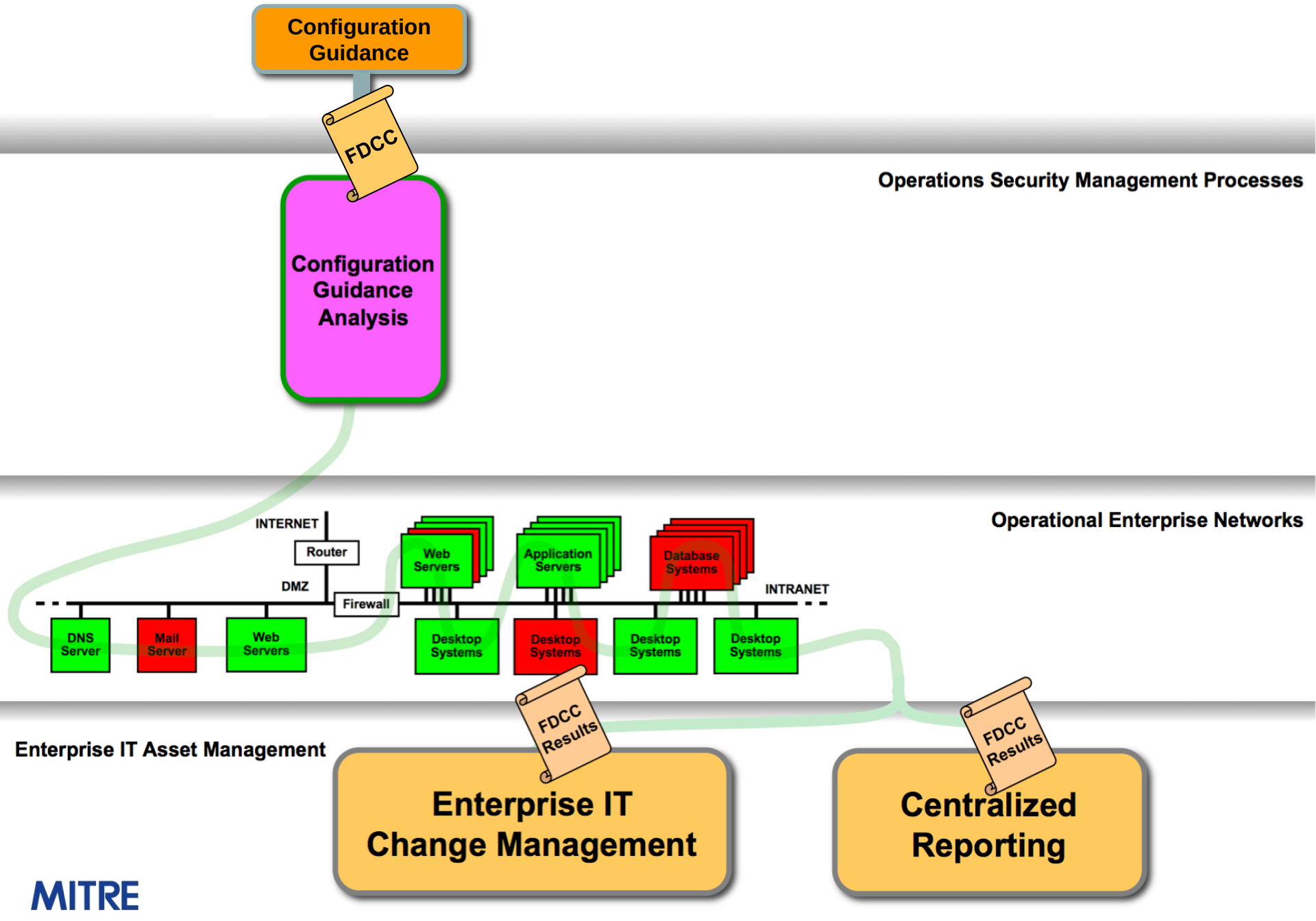
Enterprise IT Asset Management

Enterprise IT Change Management

Centralized Reporting

MITRE

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:

CPE

CAPEC

CCE

XCCDF & OVAL

ARF

CVSS

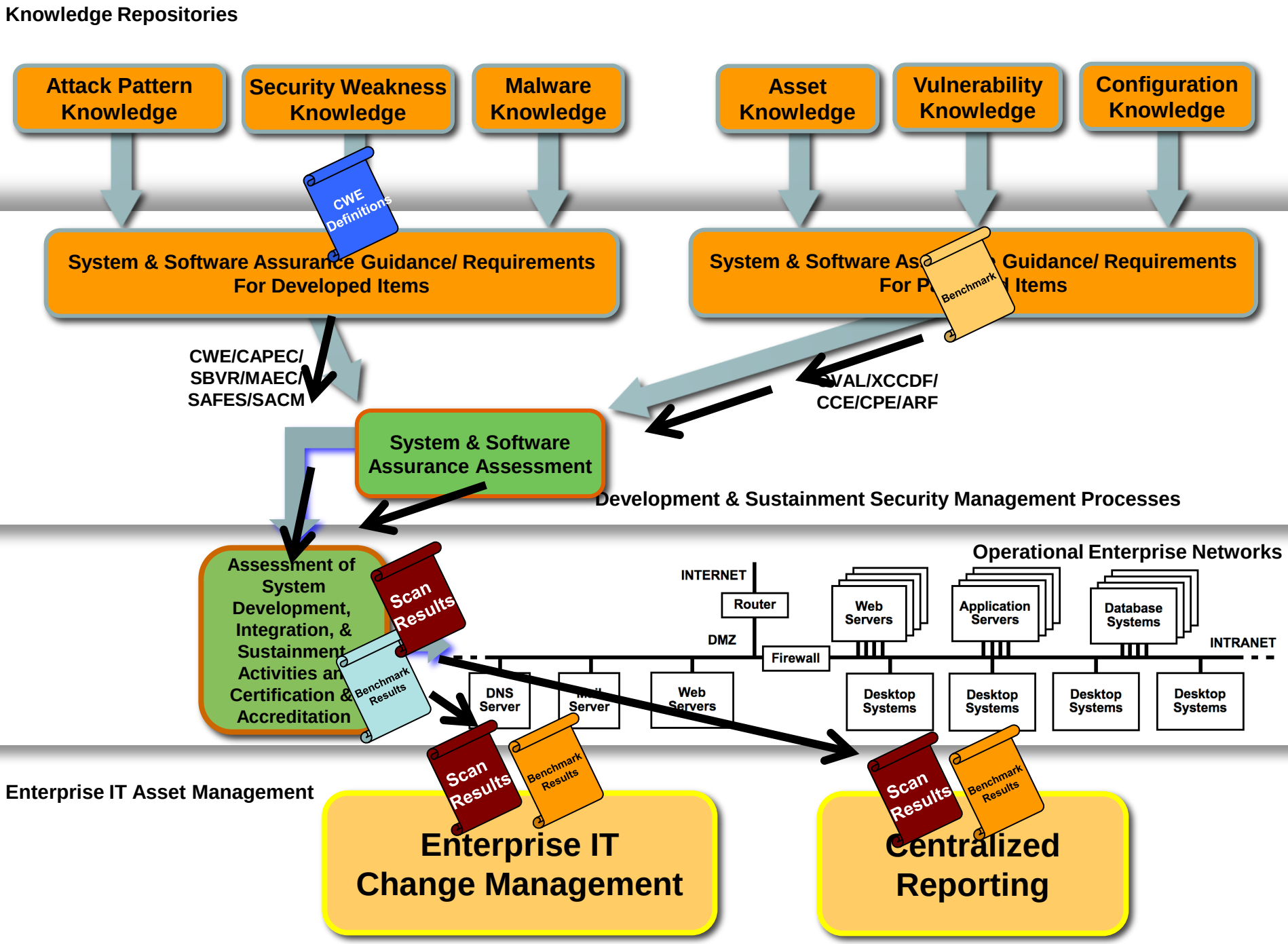
CCSS

SAFES/SACM

DoD DIACAP & eMASS

e-MASS

Knowledge Repository


Knowledge Repositories
Attack Pattern Knowledge
Security Weakness Knowledge
Malware Knowledge
Asset Knowledge
Vulnerability Knowledge
Configuration Knowledge
CWE Definitions
Benchmark
System & Software Assurance Guidance/ Requirements For Developed Items
CWE/CAPEC/ SBVR/MAEC/ SAFES/SACM
VAL/XCCDF/ CCE/CPE/ARF
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
INTERNET
Router
DMZ
Firewall
Web Servers
Application Servers
Database Systems
INTRANET
DNS Server
Web Servers
Desktop Systems
Desktop Systems
Desktop Systems
Desktop Systems
Enterprise IT Asset Management
Enterprise IT Change Management
Centralized Reporting
© 2011 MITRE

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:

CVE

CPE

CAPEC

OVAL

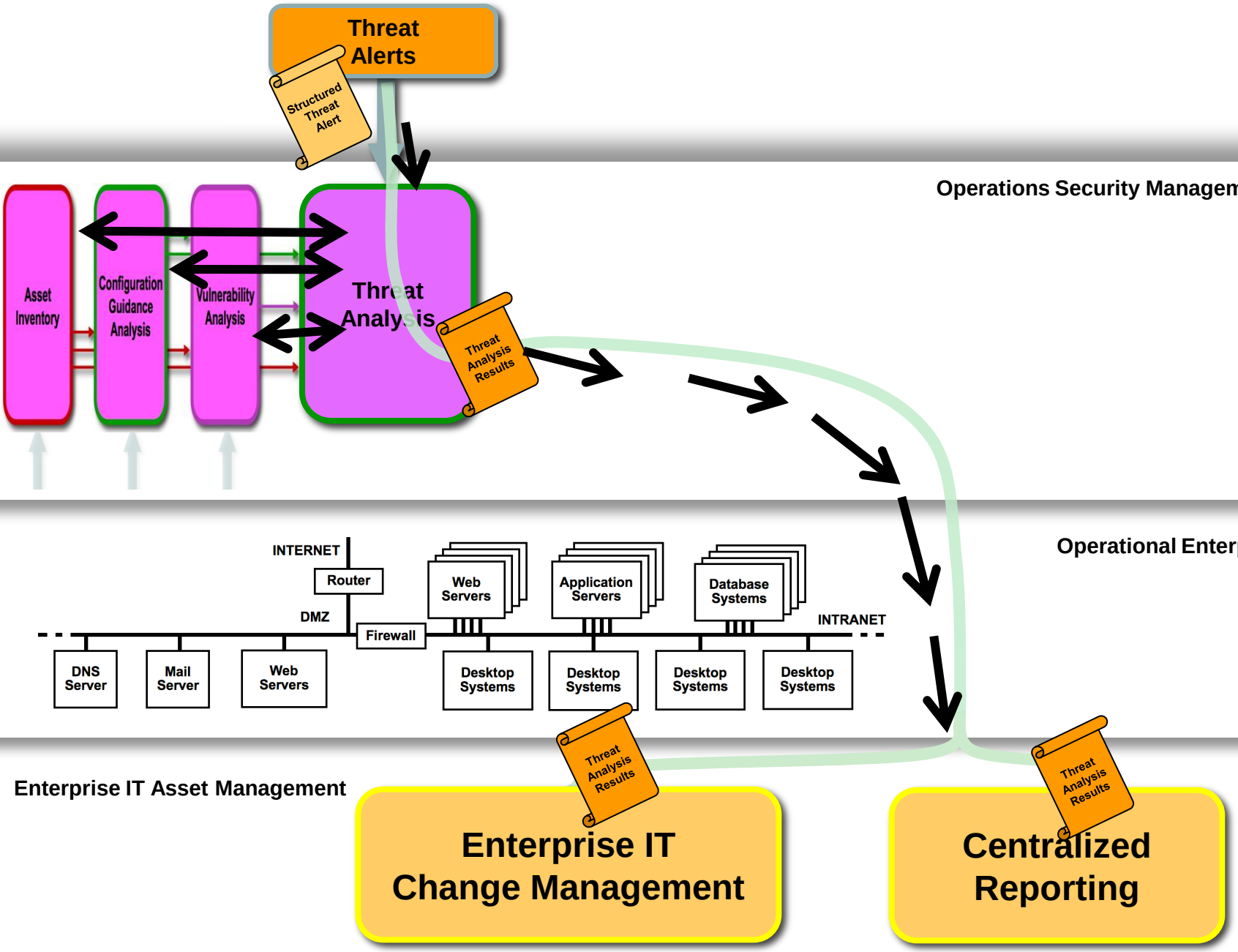
CEE

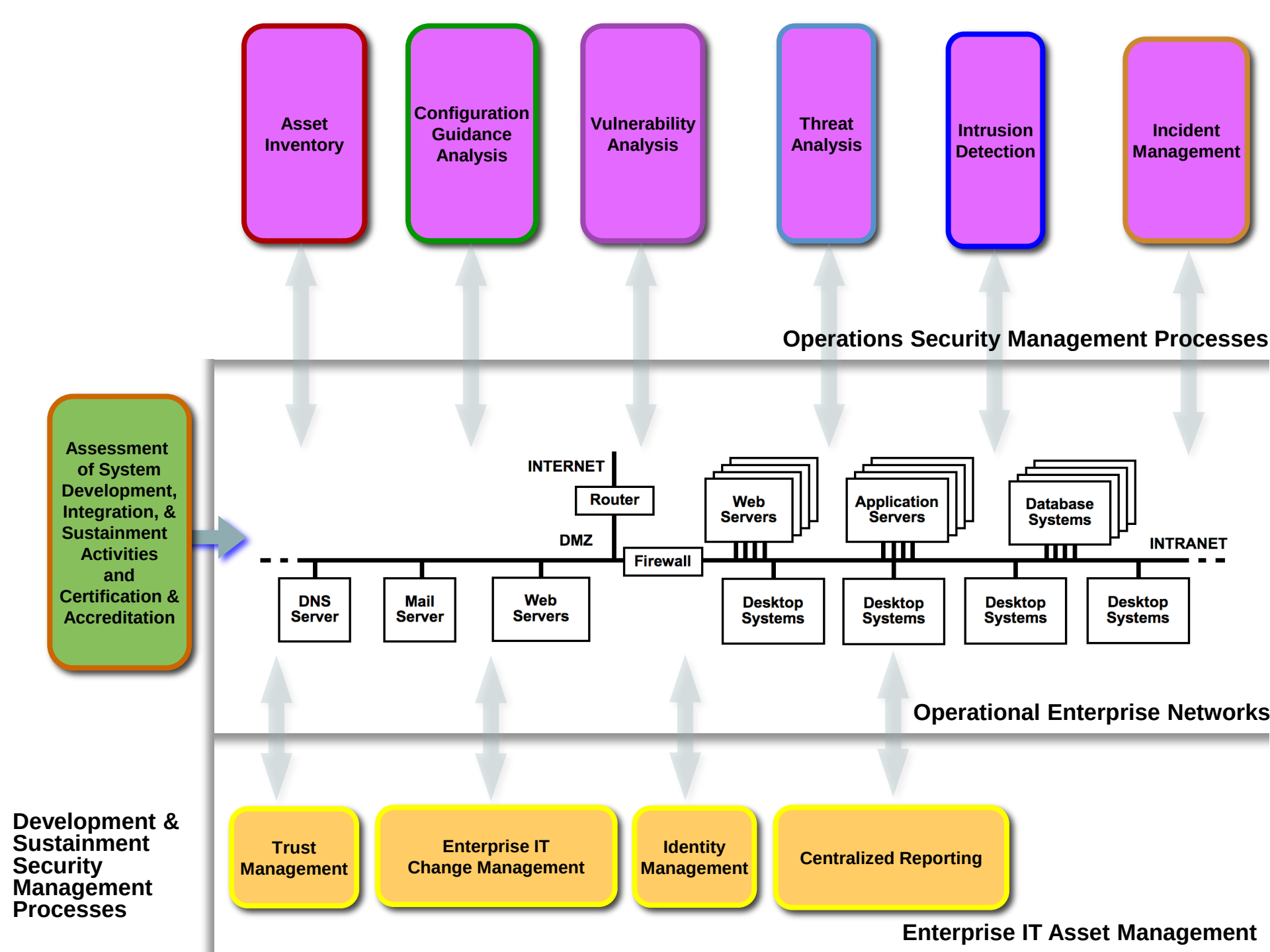
NIST/DHS NVD

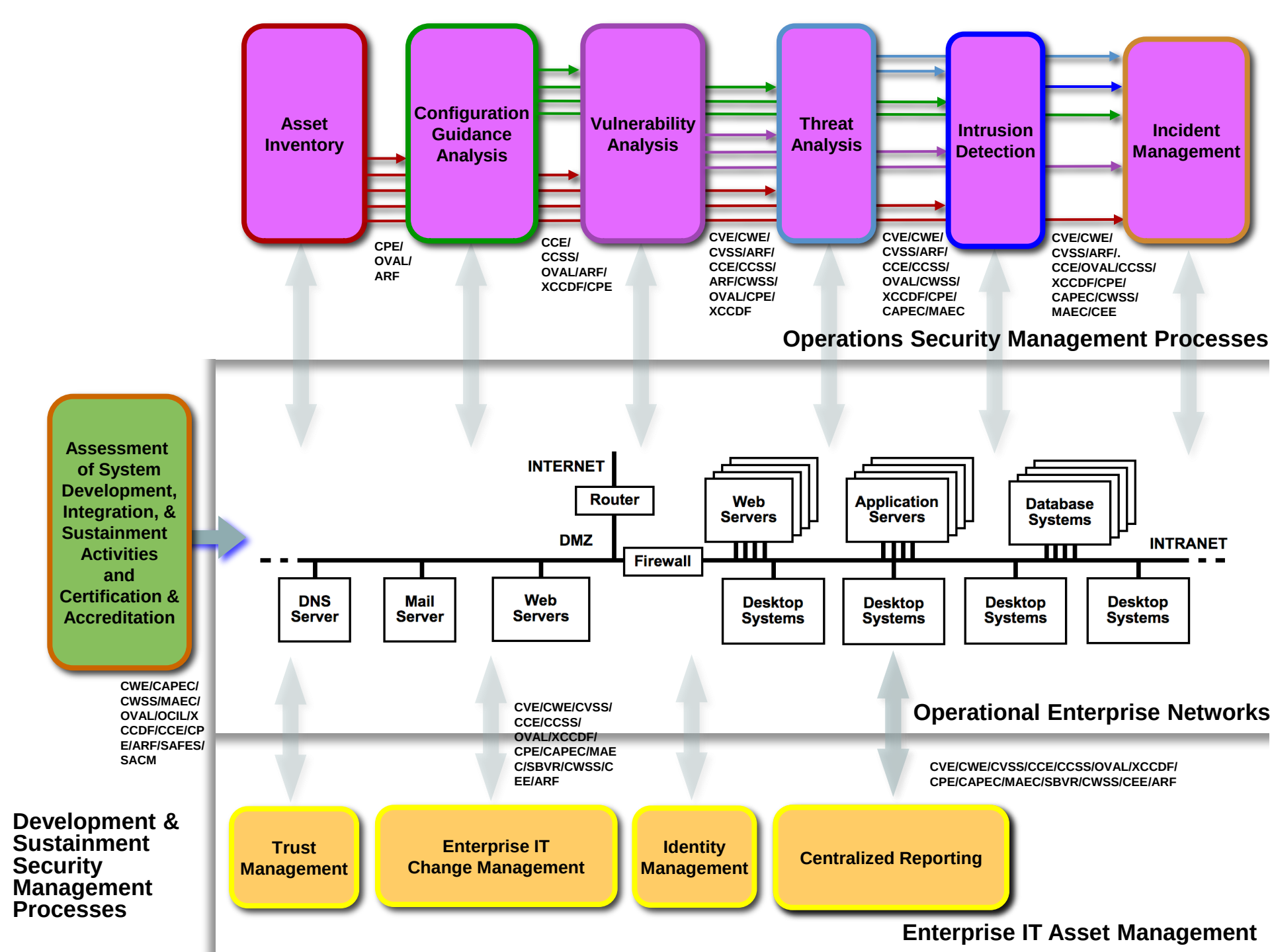
Threat Alerts

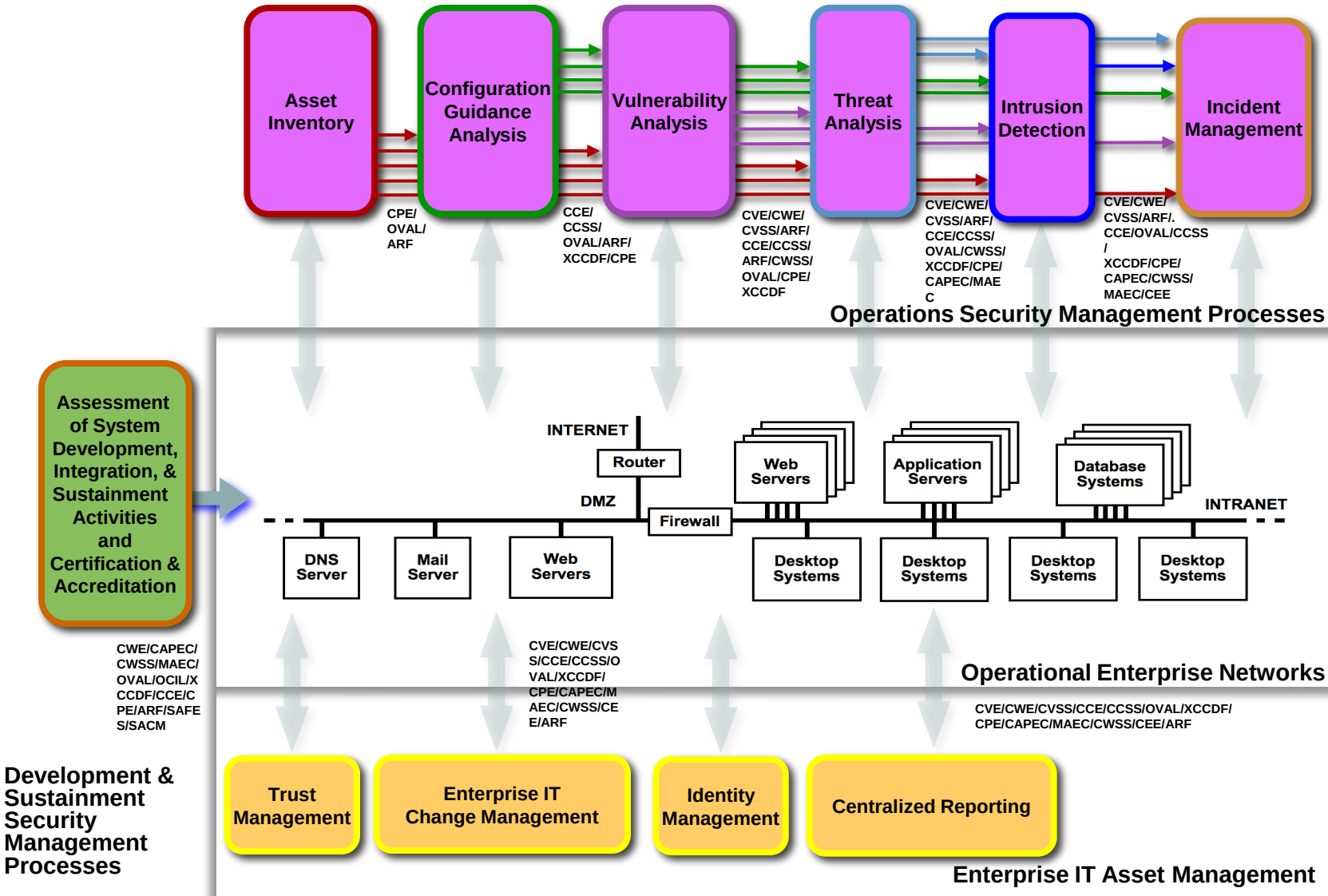
Knowledge Repository

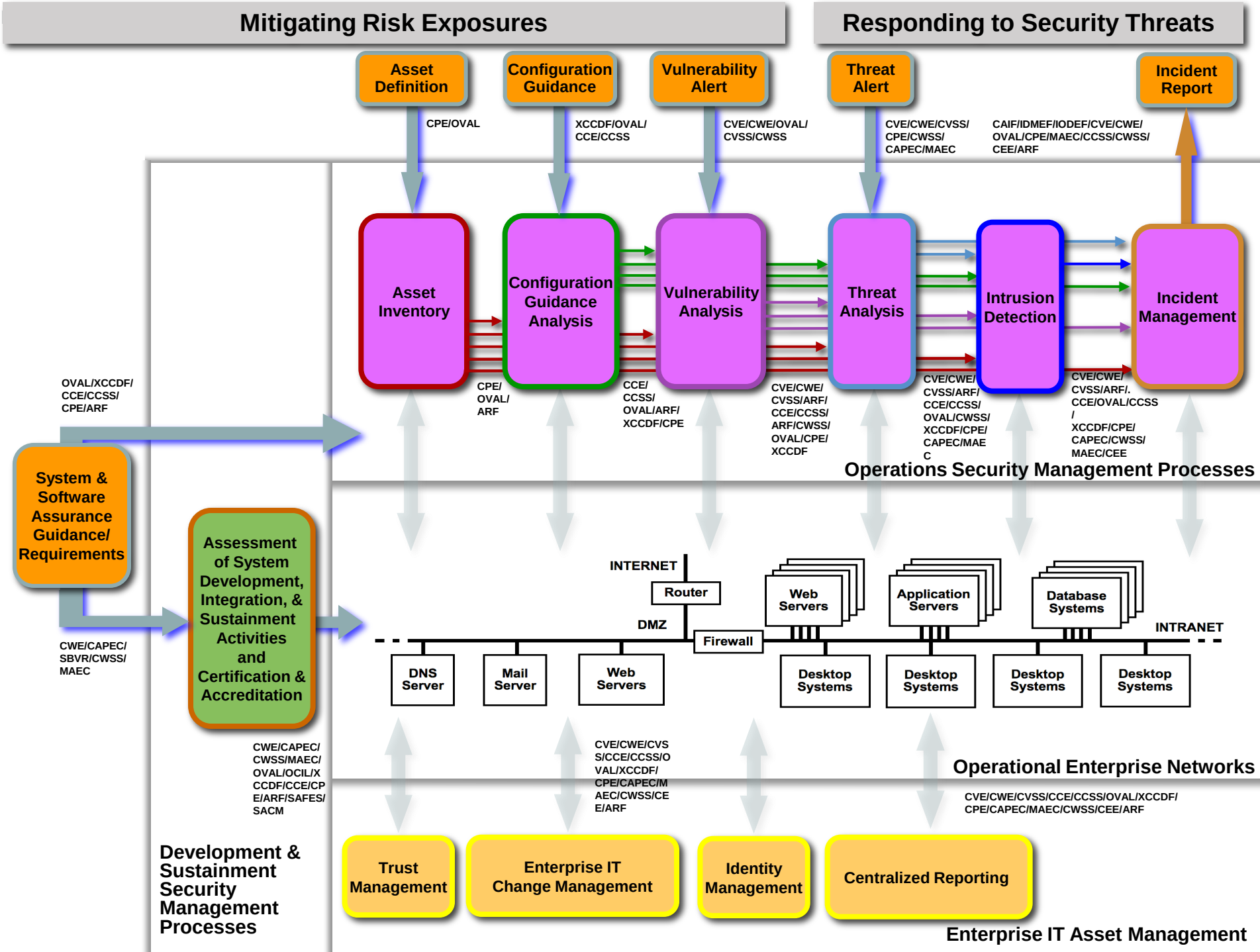
Knowledge Repositories

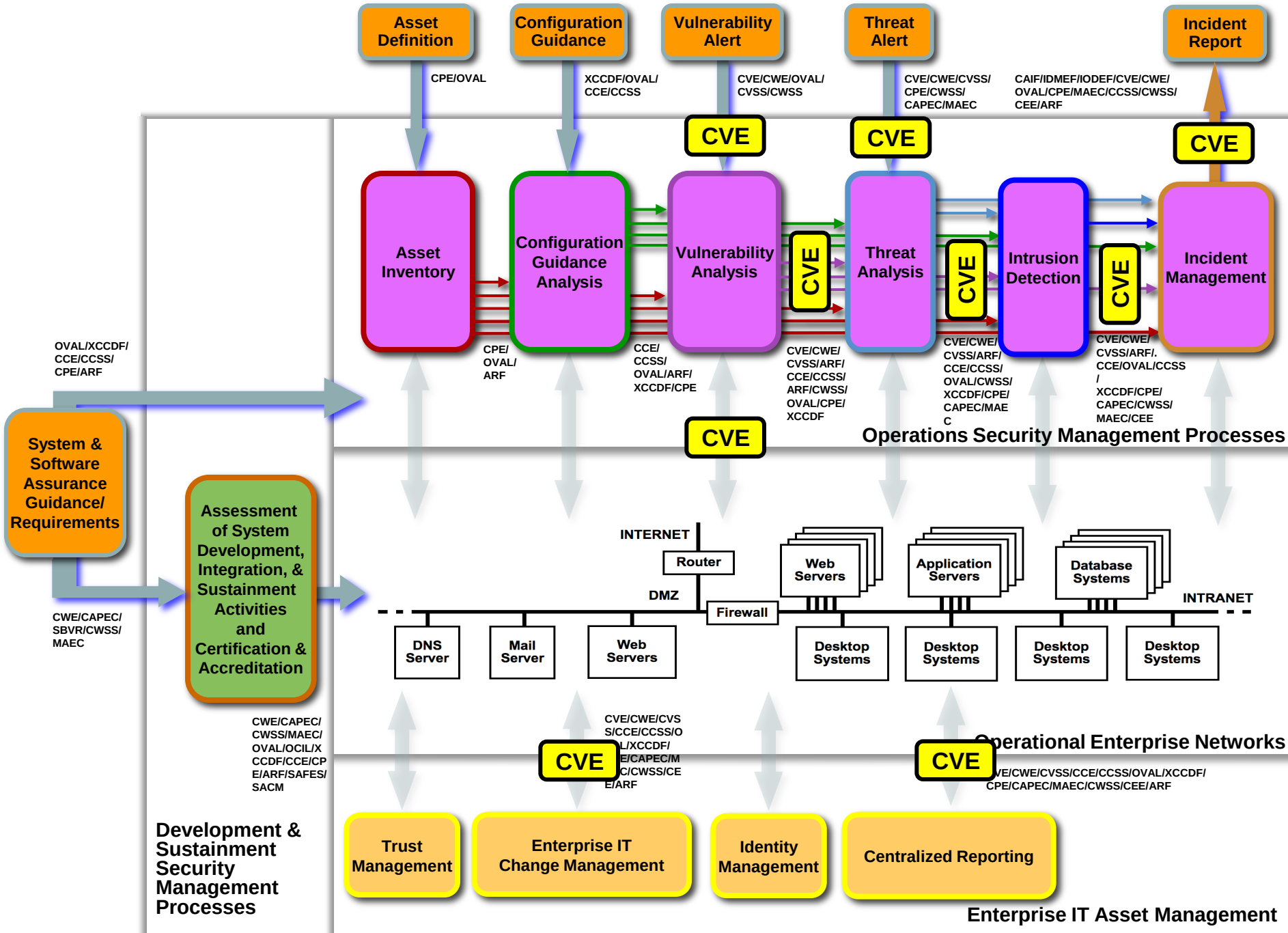


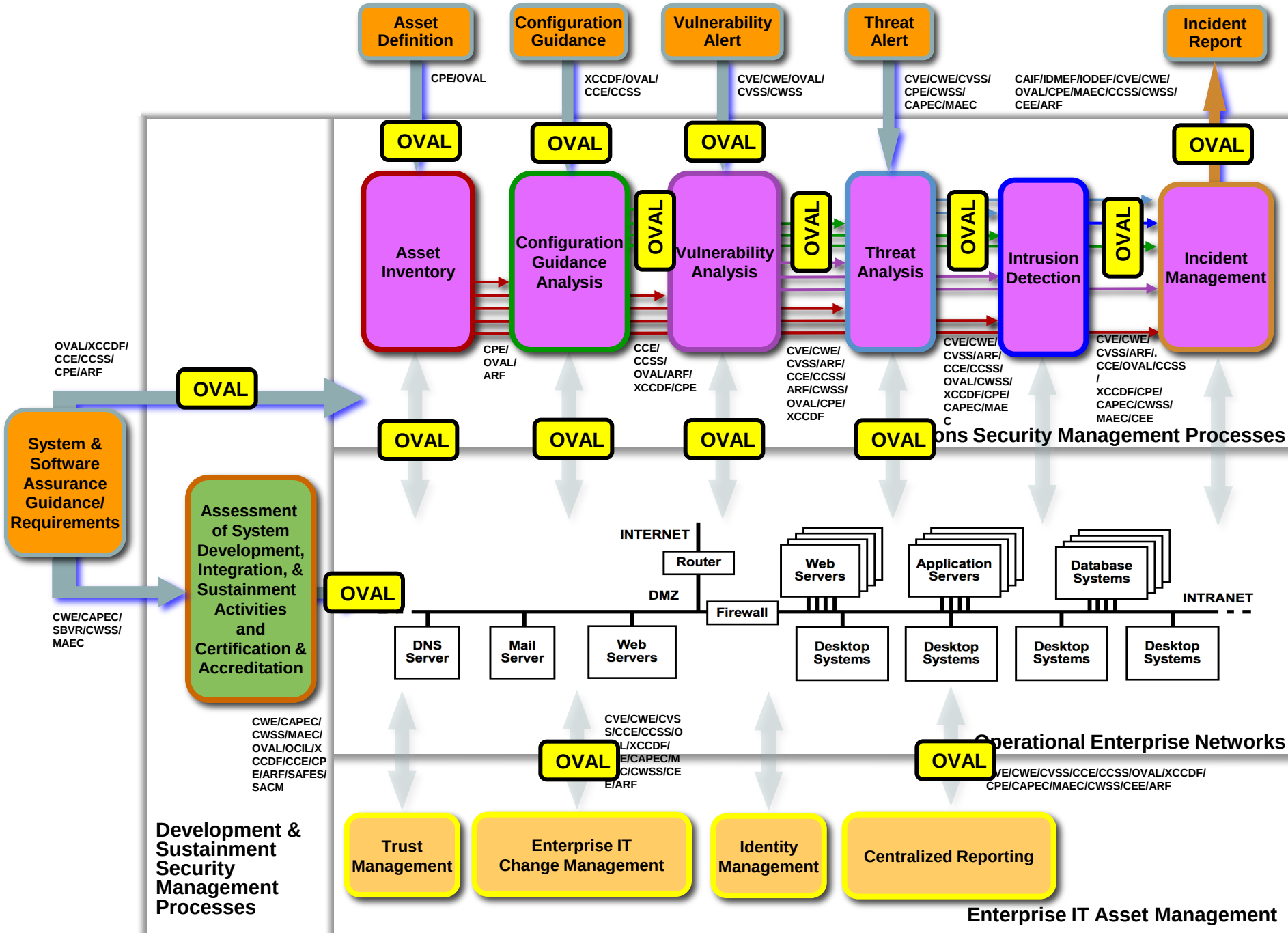

Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
Operations Security Management Processes
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
INTERNET
Router
DMZ
Firewall
Web Servers
Application Servers
Database Systems
INTRANET
DNS Server
Mail Server
Web Servers
Desktop Systems
Desktop Systems
Desktop Systems
Desktop Systems
Operational Enterprise Networks
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management

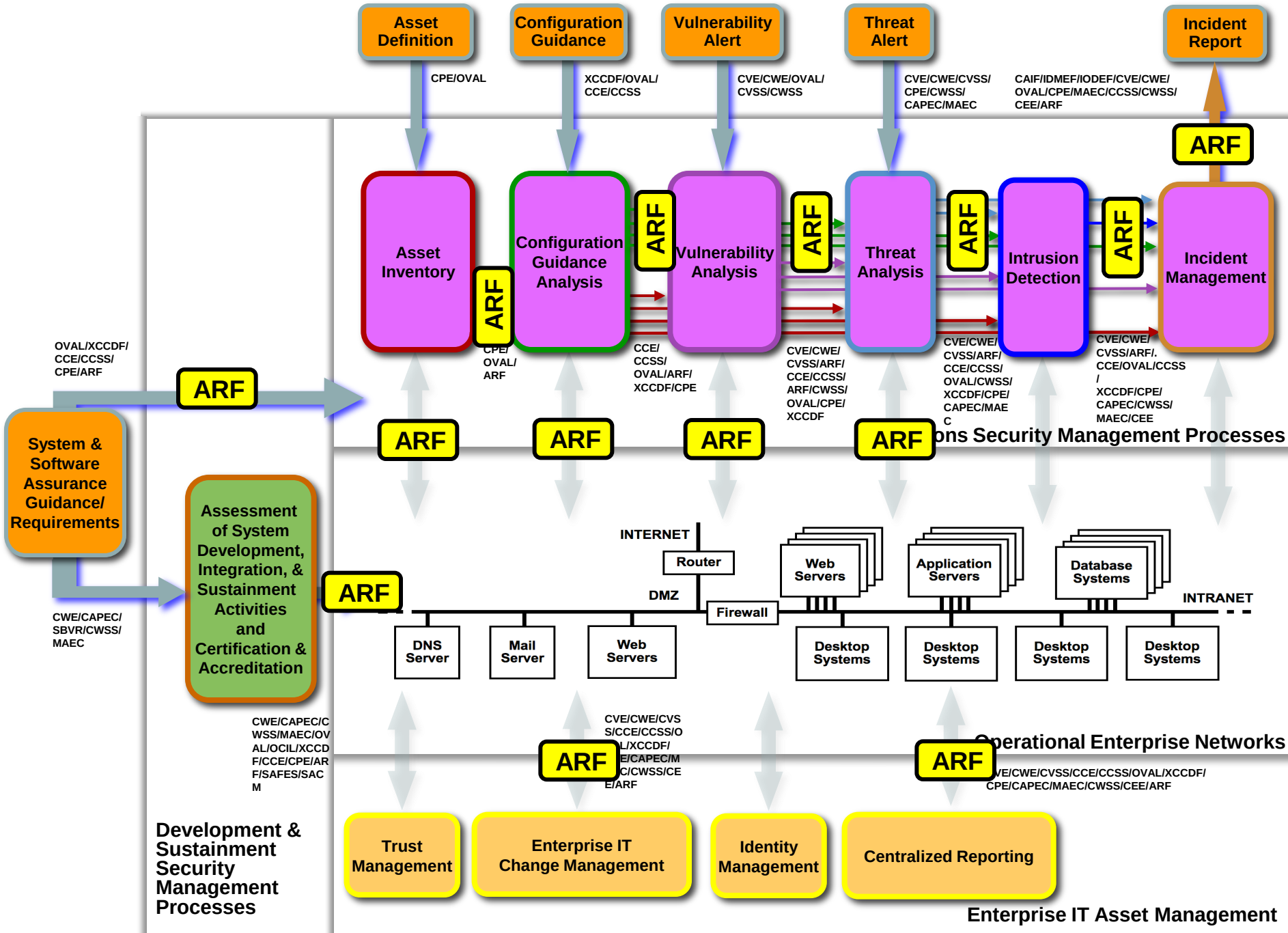

Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAEC
CVE/CWE/ CVSS/ARF/. CCE/OVAL/CCSS/ XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
Operations Security Management Processes
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
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/ CWSS/MAEC/ OVAL/OCIL/X CCDF/CCE/CP E/ARF/SAFES/ SACM
CVE/CWE/CVSS/ CCE/CCSS/ OVAL/XCCDF/ CPE/CAPEC/MAE C/SBVR/CWSS/C EE/ARF
Operational Enterprise Networks
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/SBVR/CWSS/CEE/ARF
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management


Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAE C
CVE/CWE/ CVSS/ARF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
Operations Security Management Processes
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
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/ CWSS/MAEC/ OVAL/OCIL/X CCDF/CCE/C PE/ARF/SAFE S/SACM
CVE/CWE/CVS S/CCE/CCSS/O VAL/XCCDF/ CPE/CAPEC/M AEC/CWSS/CE E/ARF
Operational Enterprise Networks
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/ARF
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management

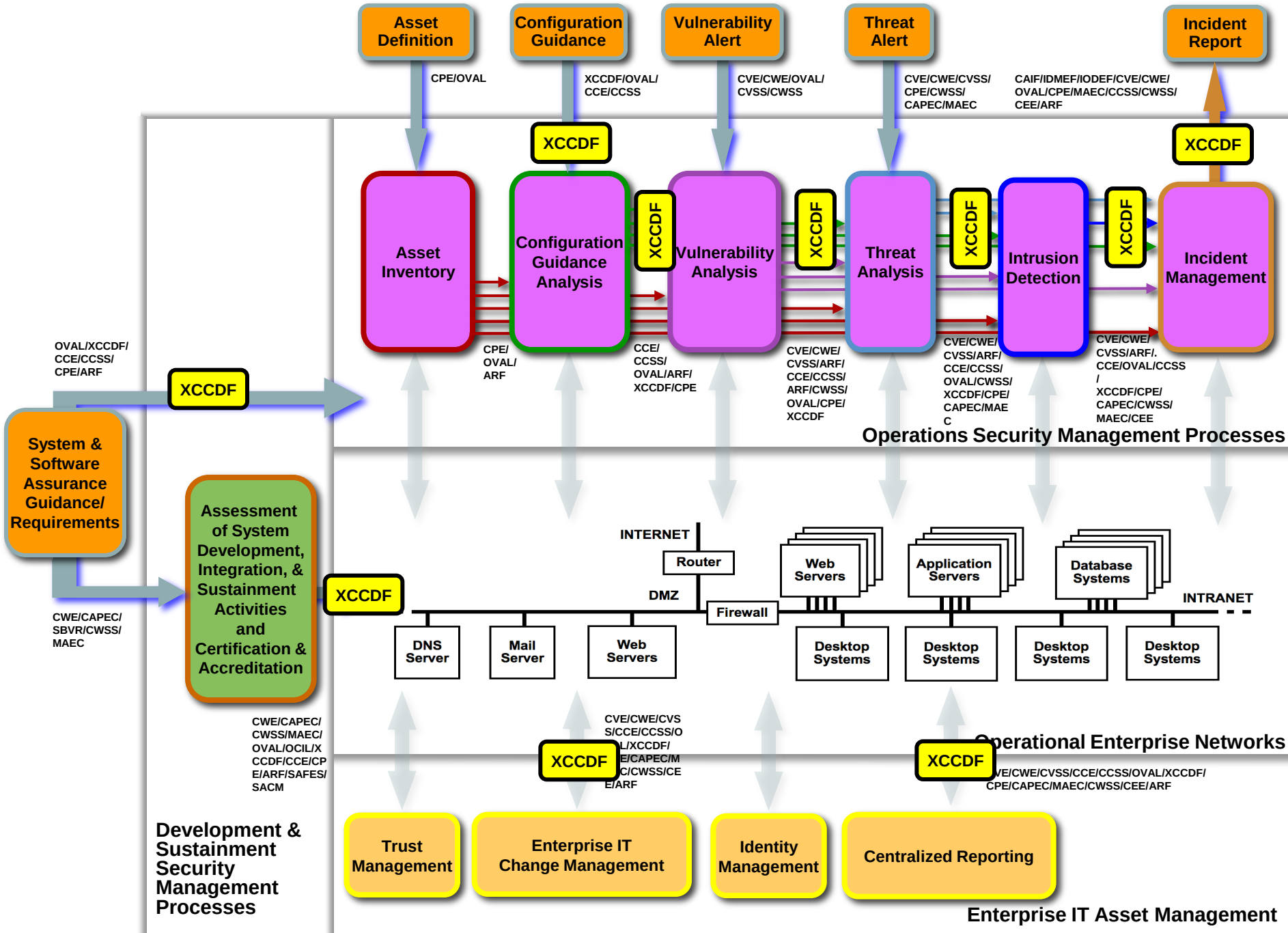

Mitigating Risk Exposures
Responding to Security Threats
Asset Definition
Configuration Guidance
Vulnerability Alert
Threat Alert
Incident Report
CPE/OVAL
XCCDF/OVAL/ CCE/CCSS
CVE/CWE/OVAL/ CVSS/CWSS
CVE/CWE/CVSS/ CPE/CWSS/ CAPEC/MAEC
CAIF/IDMEF/IODEF/CVE/CWE/ OVAL/CPE/MAEC/CCSS/CWSS/ CEE/ARF
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAE C
CVE/CWE/ CVSS/ARF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
OVAL/XCCDF/ CCE/CCSS/ CPE/ARF
Operations Security Management Processes
System & Software Assurance Guidance/ Requirements
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
CWE/CAPEC/ SBVR/CWSS/ MAEC
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/ CWSS/MAEC/ OVAL/OCIL/X CCDF/CCE/CP E/ARF/SAFES/ SACM
CVE/CWE/CVS S/CCE/CCSS/O VAL/XCCDF/ CPE/CAPEC/M AEC/CWSS/CE E/ARF
Operational Enterprise Networks
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/ARF
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management


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/ARF
CVE
CVE
CVE
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CVE
CVE
CVE
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAE C
CVE/CWE/ CVSS/ARF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
OVAL/XCCDF/ CCE/CCSS/ CPE/ARF
CVE
Operations Security Management Processes
System & Software Assurance Guidance/ Requirements
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
CWE/CAPEC/ SBVR/CWSS/ MAEC
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/ CWSS/MAEC/ OVAL/OCIL/X CCDF/CCE/CP E/ARF/SAFES/ SACM
CVE/CWE/CVS S/CCE/CCSS/O L/XCCDF/ E/CAPEC/M C/CWSS/CE E/ARF
CVE
CVE
Operational Enterprise Networks
VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/ARF
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management

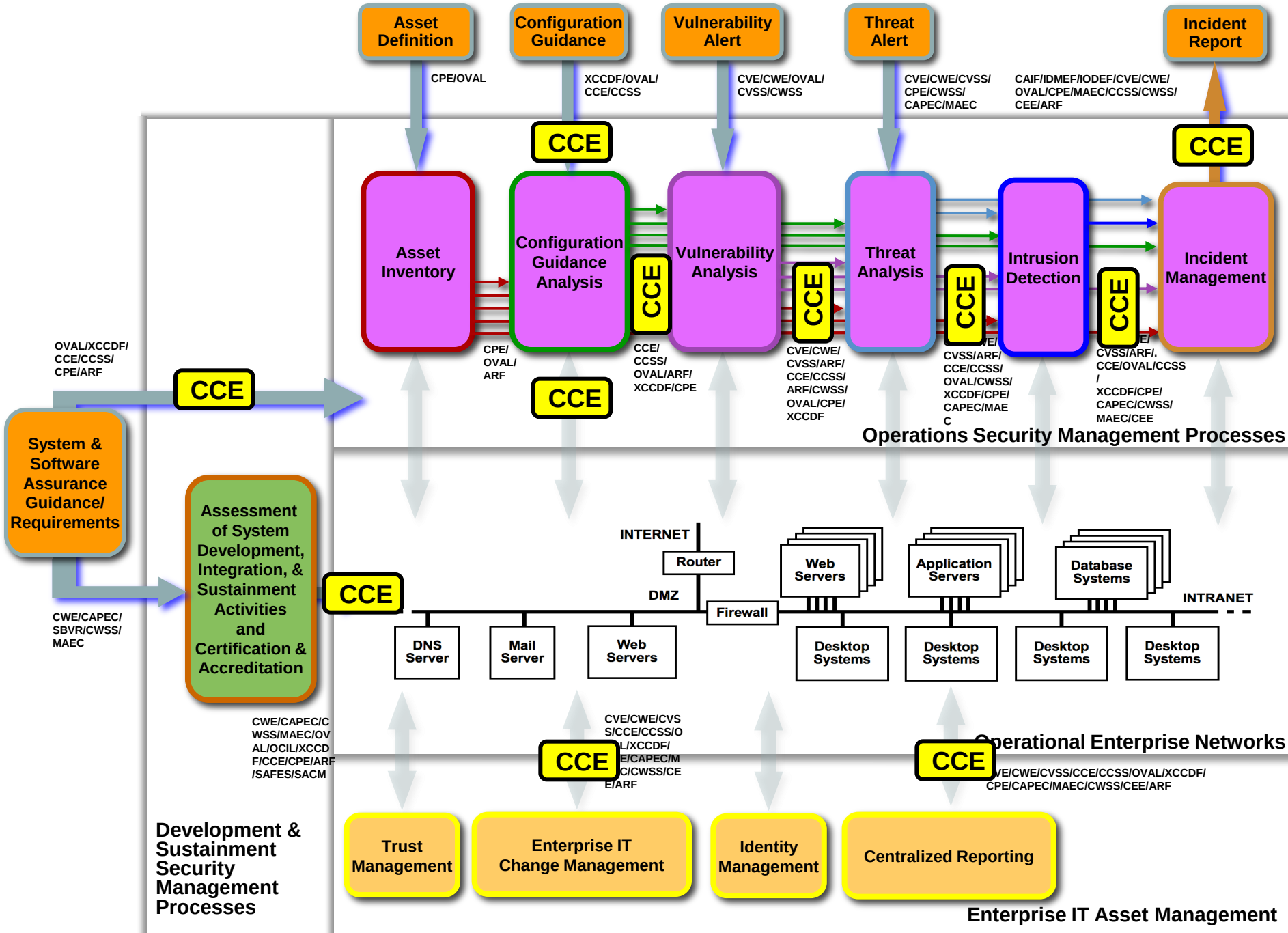

Asset Definition
Configuration Guidance
Vulnerability Alert
Threat Alert
Incident Report
CPE/OVAL
XCCDF/OVAL/ CCE/CCSS
CVE/CWE/OVAL/ CVSS/CWSS
CVE/CWE/CVSS/ CPE/CWSS/ CAPEC/MAEC
CAIF/IDMEF/IODEF/CVE/CWE/ OVAL/CPE/MAEC/CCSS/CWSS/ CEE/ARF
OVAL
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAE C
CVE/CWE/ CVSS/ARF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
OVAL/XCCDF/ CCE/CCSS/ CPE/ARF
System & Software Assurance Guidance/ Requirements
CWE/CAPEC/ SBVR/CWSS/ MAEC
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
CWE/CAPEC/ CWSS/MAEC/ OVAL/OCIL/X CCDF/CCE/CP E/ARF/SAFES/ SACM
Development & Sustainment Security Management Processes
ons Security Management Processes
INTERNET
Router
DMZ
Firewall
Web Servers
Application Servers
Database Systems
INTRANET
DNS Server
Mail Server
Web Servers
Desktop Systems
Desktop Systems
Desktop Systems
Desktop Systems
CVE/CWE/CVS S/CCE/CCSS/O L/XCCDF/ E/CAPEC/M C/CWSS/CE E/ARF
perational Enterprise Networks
VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/ARF
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management

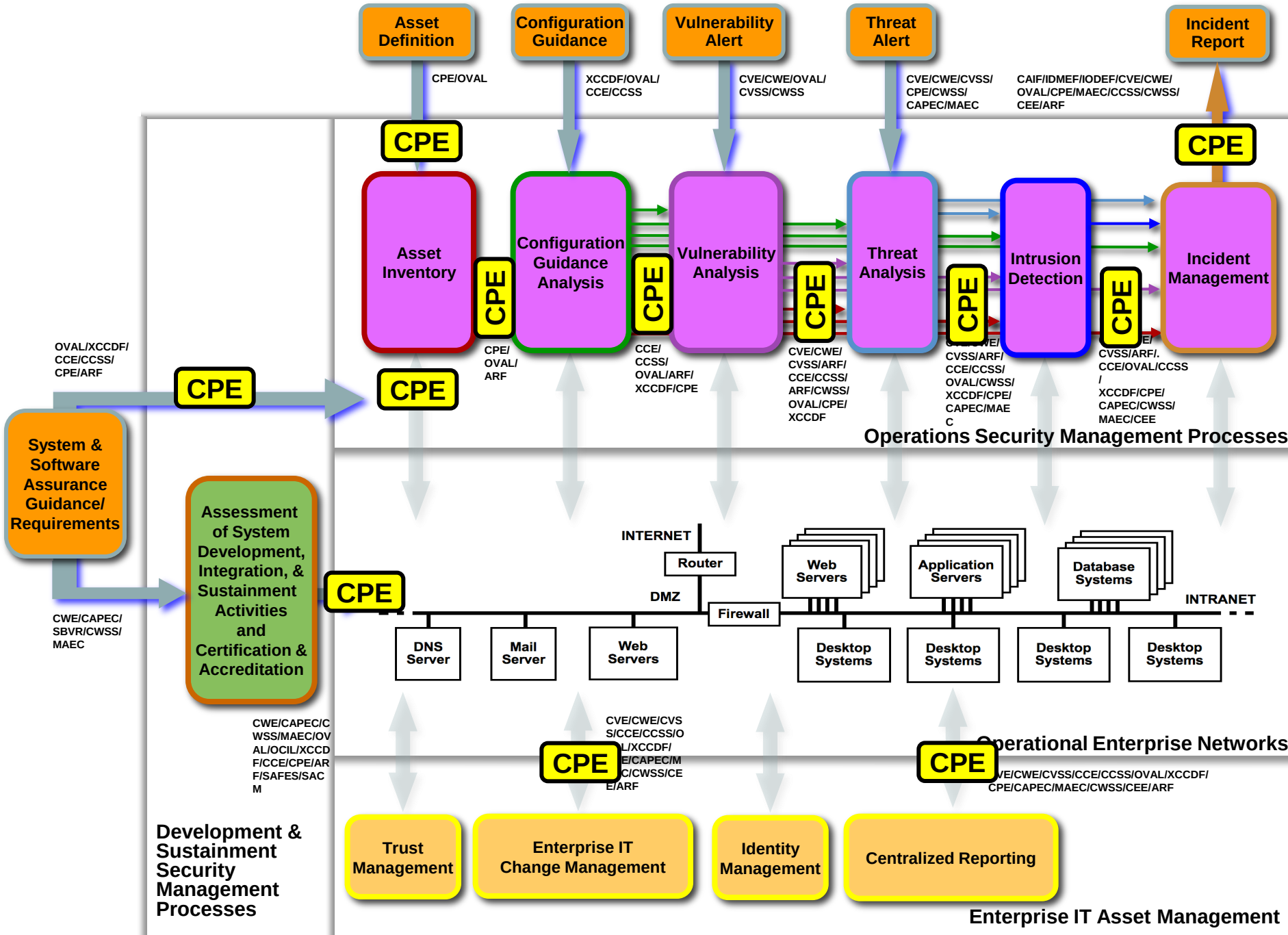

Asset Definition
Configuration Guidance
Vulnerability Alert
Threat Alert
Incident Report
CPE/OVAL
XCCDF/OVAL/ CCE/CCSS
CVE/CWE/OVAL/ CVSS/CWSS
CVE/CWE/CVSS/ CPE/CWSS/ CAPEC/MAEC
CAIF/IDMEF/IODEF/CVE/CWE/ OVAL/CPE/MAEC/CCSS/CWSS/ CEE/ARF
ARF
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAE C
CVE/CWE/ CVSS/ARF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
OVAL/XCCDF/ CCE/CCSS/ CPE/ARF
System & Software Assurance Guidance/ Requirements
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
CWE/CAPEC/ SBVR/CWSS/ MAEC
CWE/CAPEC/C WSS/MAEC/OV AL/OCIL/XCCD F/CCE/CPE/AR F/SAFES/SAC M
Operations Security Management Processes
INTERNET
Router
DMZ
Firewall
INTRANET
Web Servers
Application Servers
Database Systems
DNS Server
Mail Server
Web Servers
Desktop Systems
Desktop Systems
Desktop Systems
Desktop Systems
CVE/CWE/CVS S/CCE/CCSS/O L/XCCDF/ E/CAPEC/M C/CWSS/CE E/ARF
Operational Enterprise Networks
VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/ARF
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management

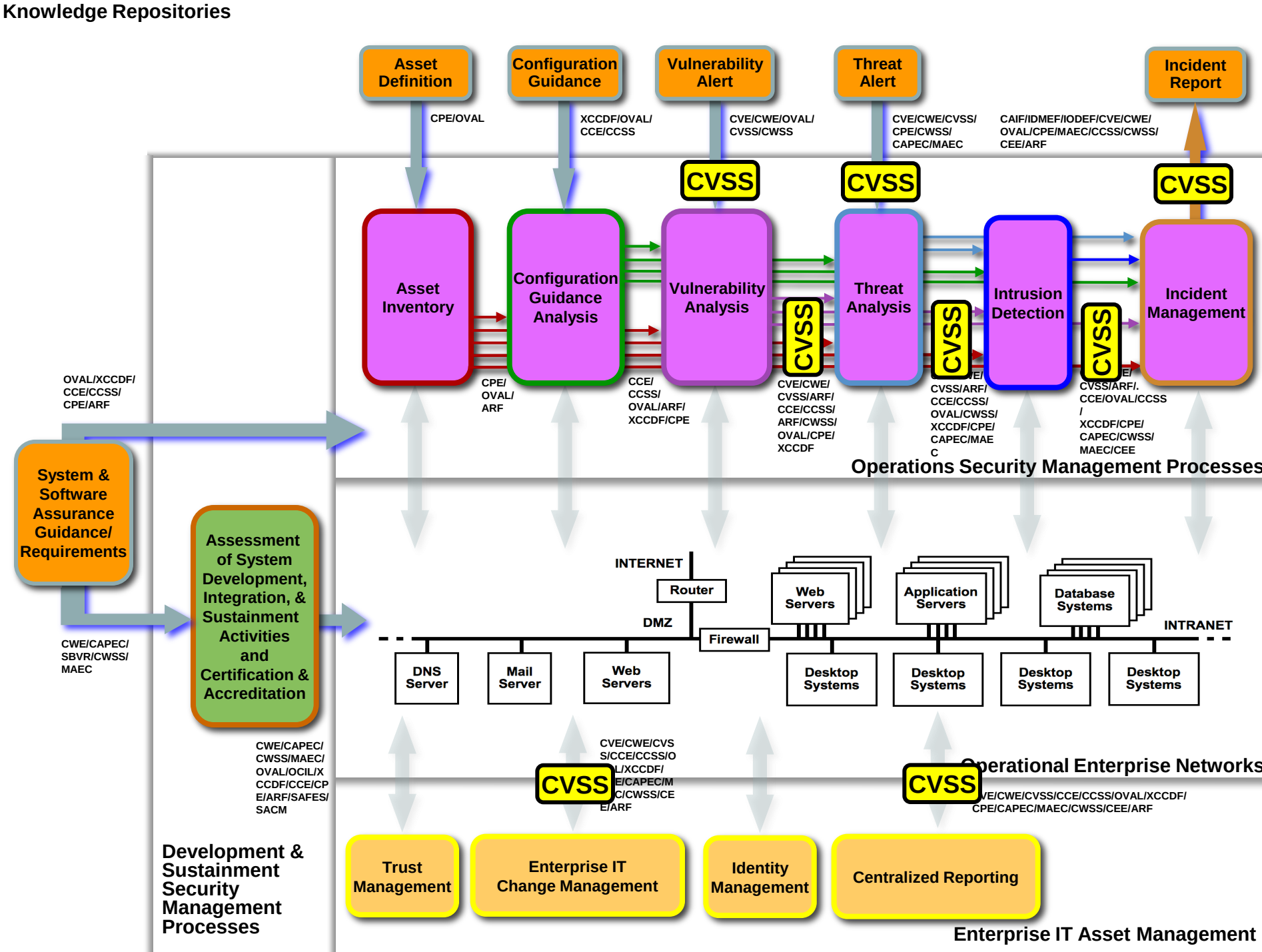
Knowledge Repositories

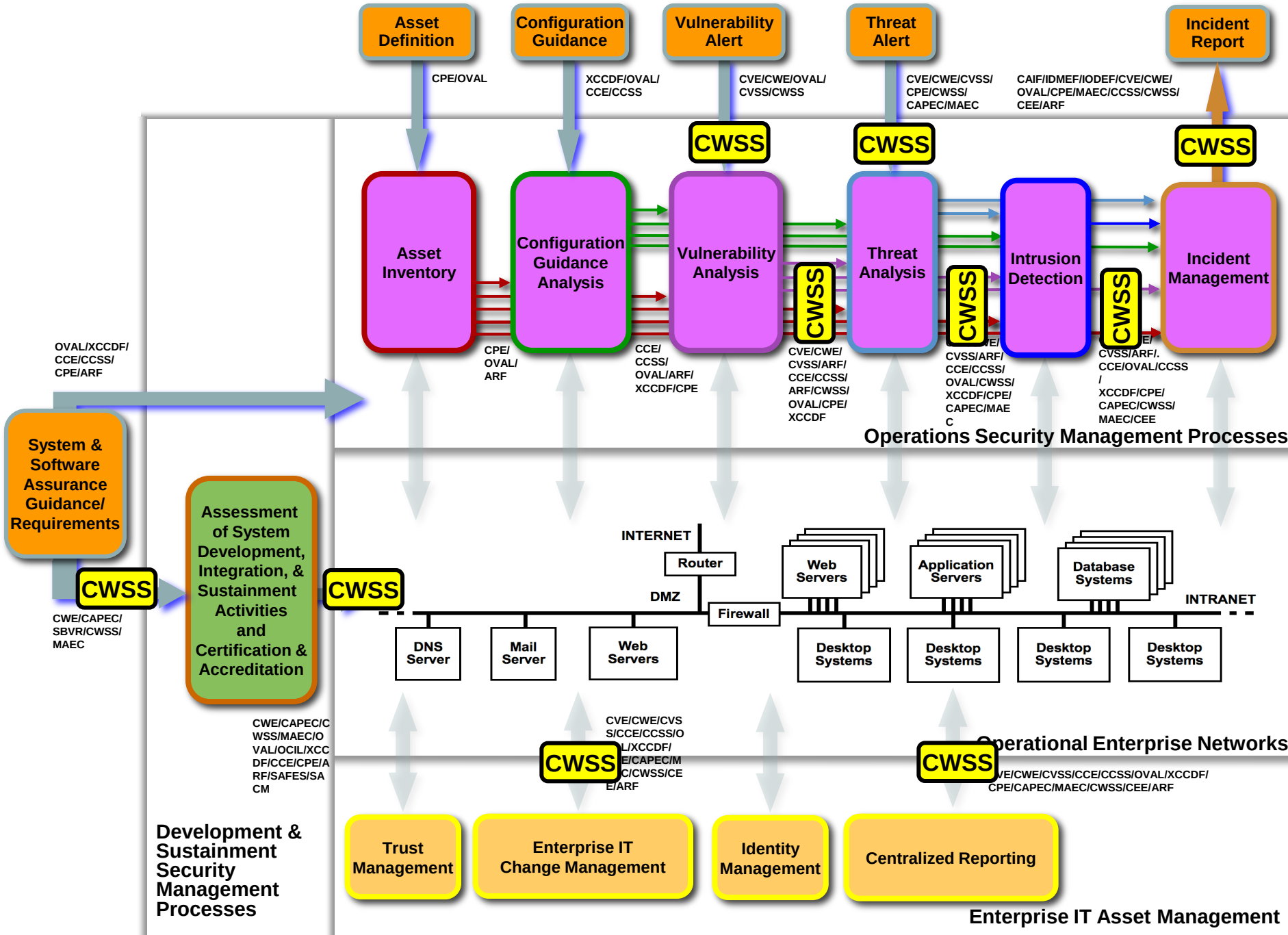


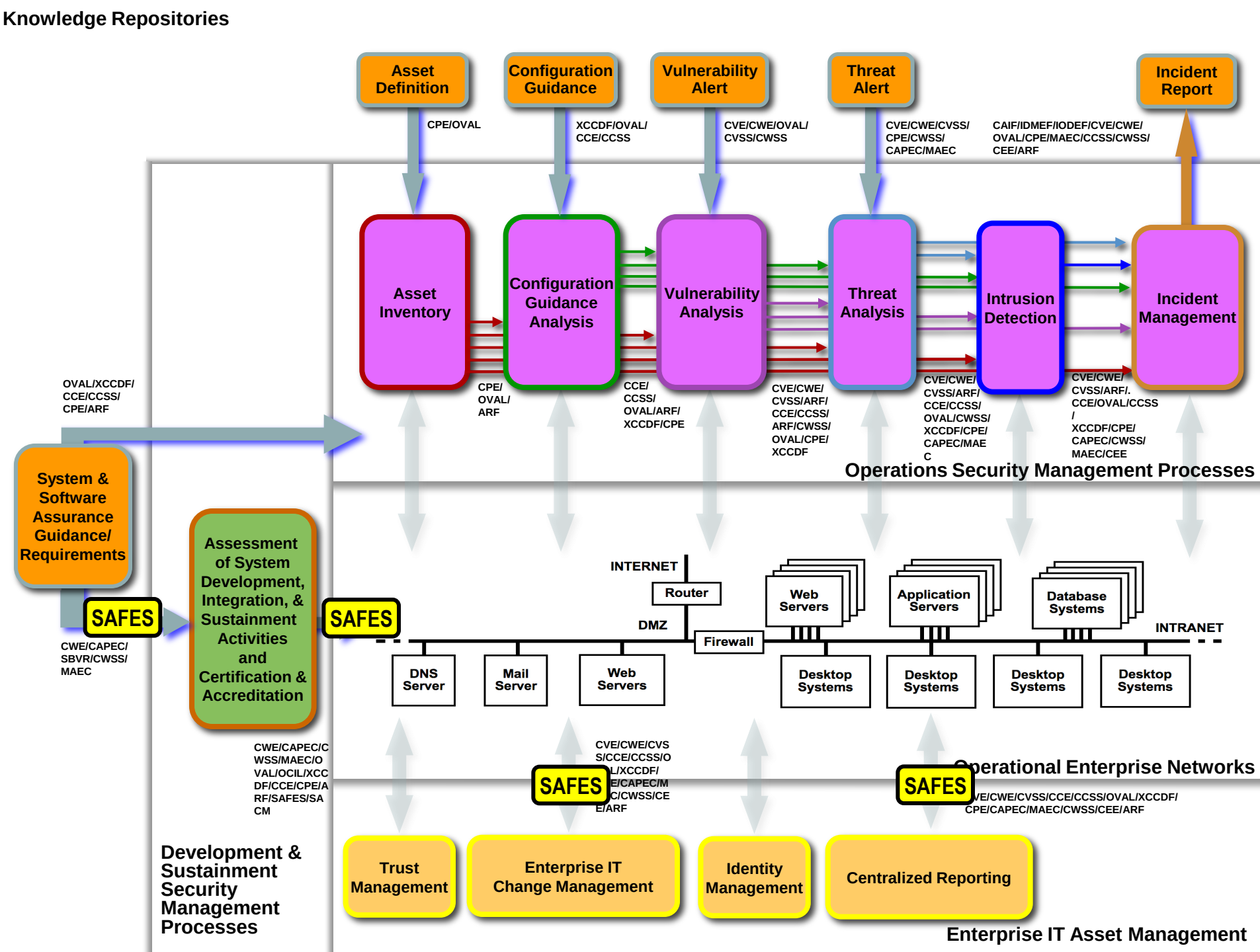
Knowledge Repositories

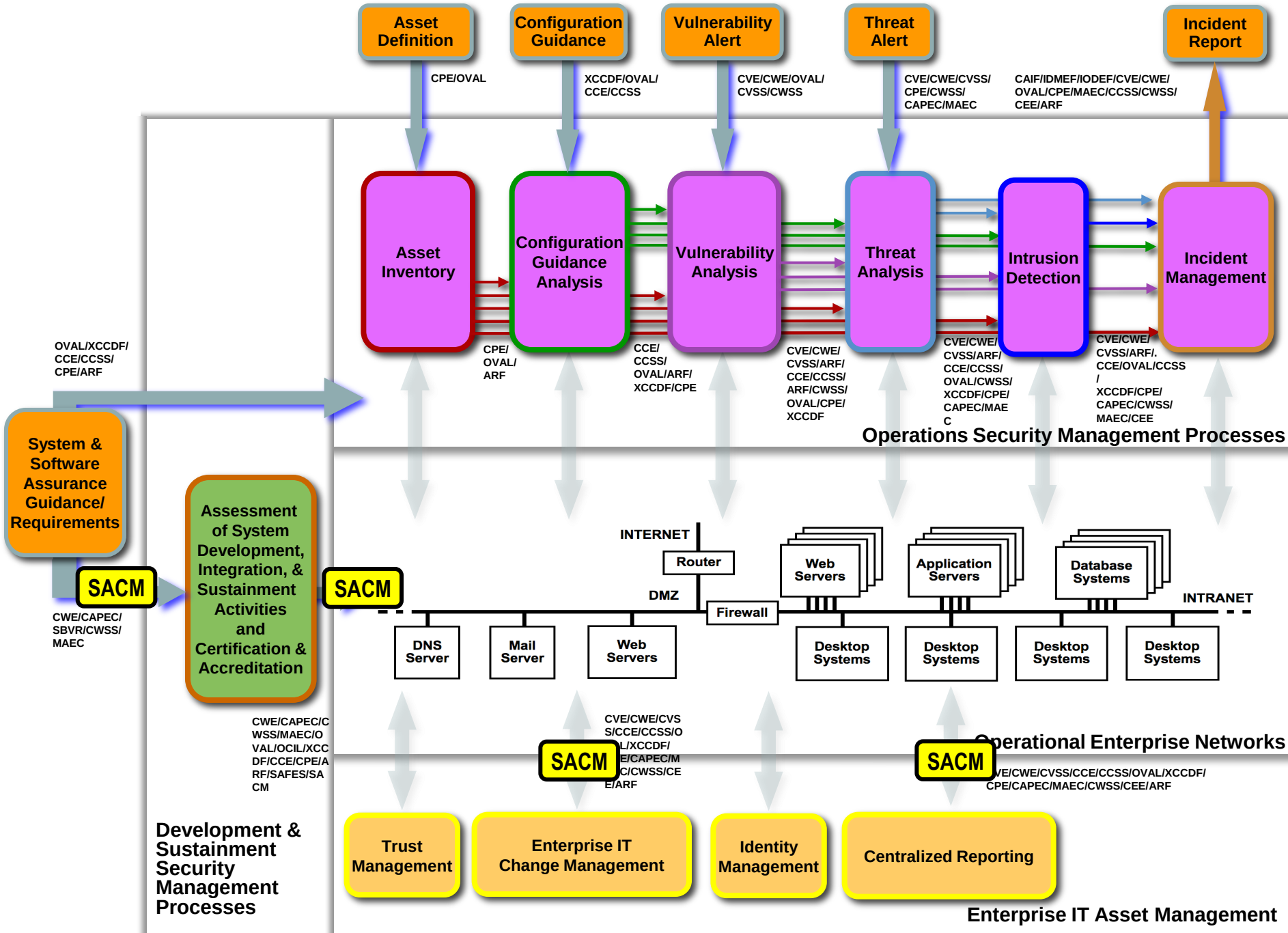


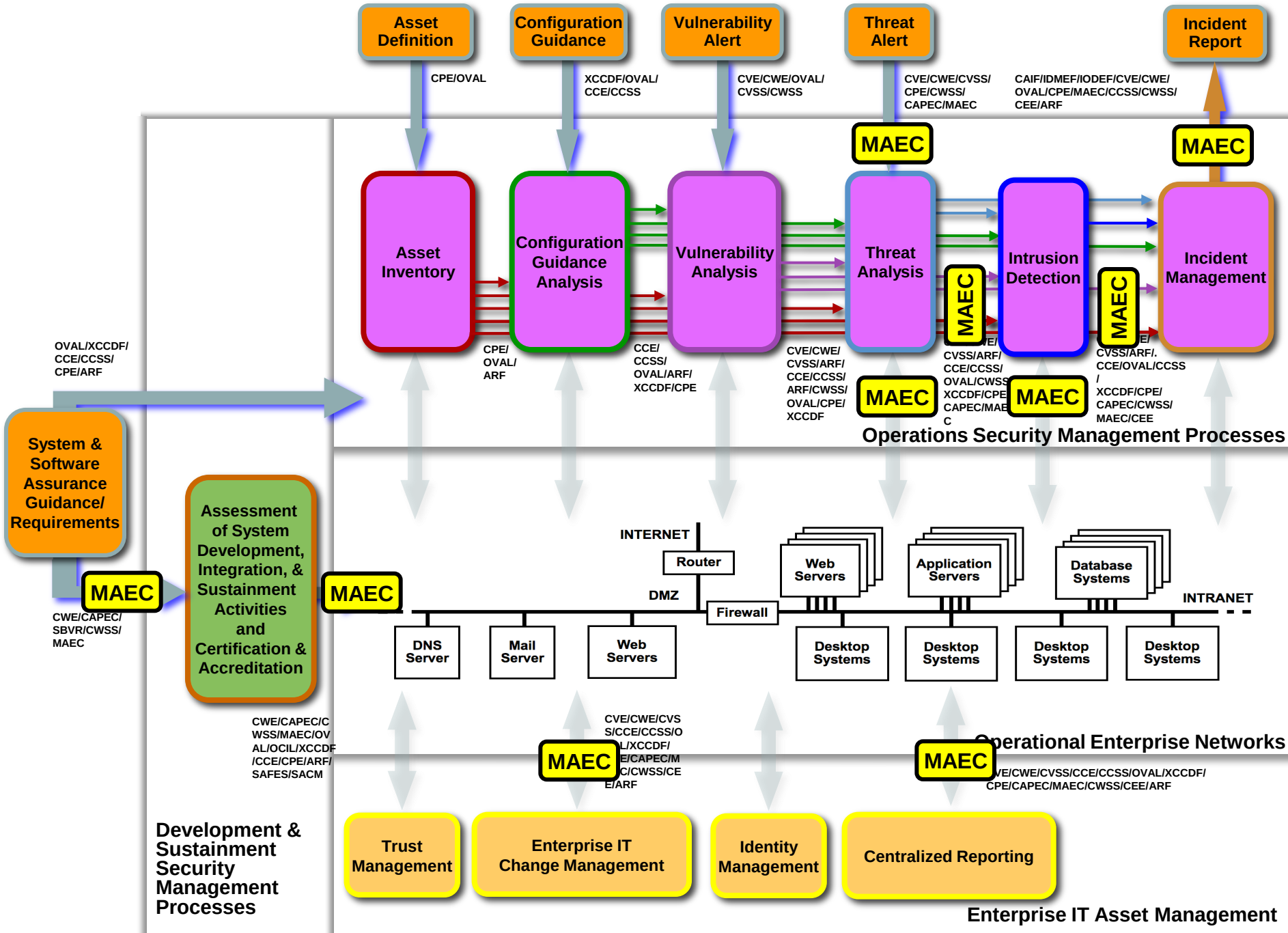

Asset Definition
Configuration Guidance
Vulnerability Alert
Threat Alert
Incident Report
CPE/OVAL
XCCDF/OVAL/ CCE/CCSS
CVE/CWE/OVAL/ CVSS/CWSS
CVE/CWE/CVSS/ CPE/CWSS/ CAPEC/MAEC
CAIF/IDMEF/IODEF/CVE/CWE/ OVAL/CPE/MAEC/CCSS/CWSS/ CEE/ARF
CPE
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAE C
CVSS/ARF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
OVAL/XCCDF/ CCE/CCSS/ CPE/ARF
System & Software Assurance Guidance/ Requirements
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
CWE/CAPEC/ SBVR/CWSS/ MAEC
CWE/CAPEC/C WSS/MAEC/OV AL/OCIL/XCCD F/CCE/CPE/AR F/SAFES/SAC M
Operations Security Management Processes
INTERNET
Router
DMZ
Firewall
Web Servers
Application Servers
Database Systems
INTRANET
DNS Server
Mail Server
Web Servers
Desktop Systems
Desktop Systems
Desktop Systems
Desktop Systems
CVE/CWE/CVS S/CCE/CCSS/O L/XCCDF/ E/CAPEC/M C/CWSS/CE E/ARF
Operational Enterprise Networks
VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/ARF
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management

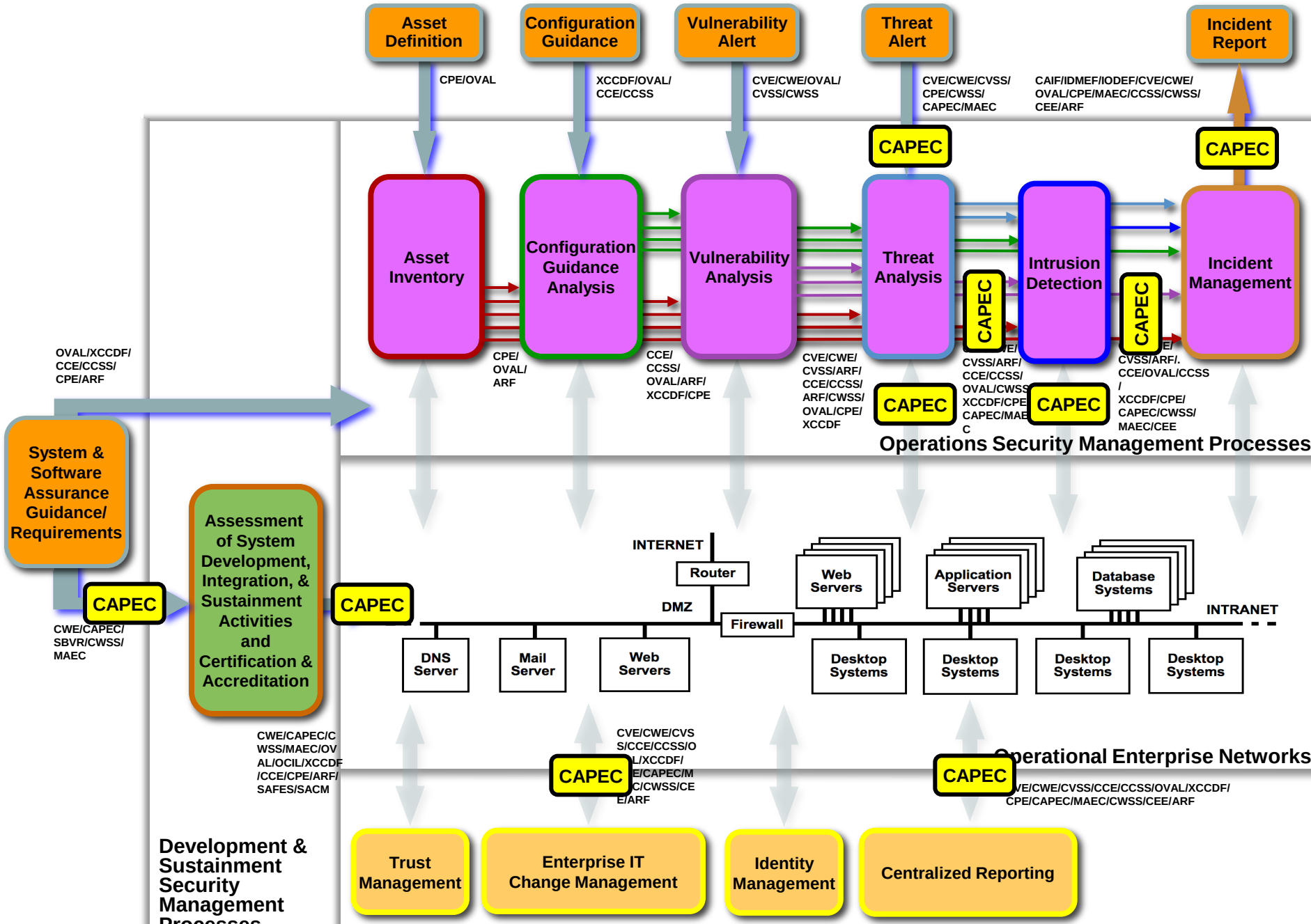

Knowledge Repositories
Asset Definition
Configuration Guidance
Vulnerability Alert
Threat Alert
Incident Report
CPE/OVAL
XCCDF/OVAL/ CCE/CCSS
CVE/CWE/OVAL/ CVSS/CWSS
CVE/CWE/CVSS/ CPE/CWSS/ CAPEC/MAEC
CAIF/IDMEF/IODEF/CVE/CWE/ OVAL/CPE/MAEC/CCSS/CWSS/ CEE/ARF
CVSS
CVSS
CVSS
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAE C
CVSS/ARF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
OVAL/XCCDF/ CCE/CCSS/ CPE/ARF
Operations Security Management Processes
System & Software Assurance Guidance/ Requirements
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
CWE/CAPEC/ SBVR/CWSS/ MAEC
INTERNET
Router
DMZ
Firewall
INTRANET
Web Servers
Application Servers
Database Systems
DNS Server
Mail Server
Web Servers
Desktop Systems
Desktop Systems
Desktop Systems
Desktop Systems
CWE/CAPEC/ CWSS/MAEC/ OVAL/OCIL/X CCDF/CCE/CP E/ARF/SAFES/ SACM
CVE/CWE/CVS S/CCE/CCSS/O L/XCCDF/ E/CAPEC/M C/CWSS/CE E/ARF
CVSS
CVSS
Operational Enterprise Networks
VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/ARF
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management


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/ARF
CWSS
CWSS
CWSS
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAE C
CVSS/ARF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
OVAL/XCCDF/ CCE/CCSS/ CPE/ARF
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
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/C WSS/MAEC/O VAL/OCIL/XCC DF/CCE/CPE/A RF/SAFES/SA CM
CVE/CWE/CVS S/CCE/CCSS/O L/XCCDF/ E/CAPEC/M C/CWSS/CE E/ARF
CWSS
CWSS
Operational Enterprise Networks
VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/ARF
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management

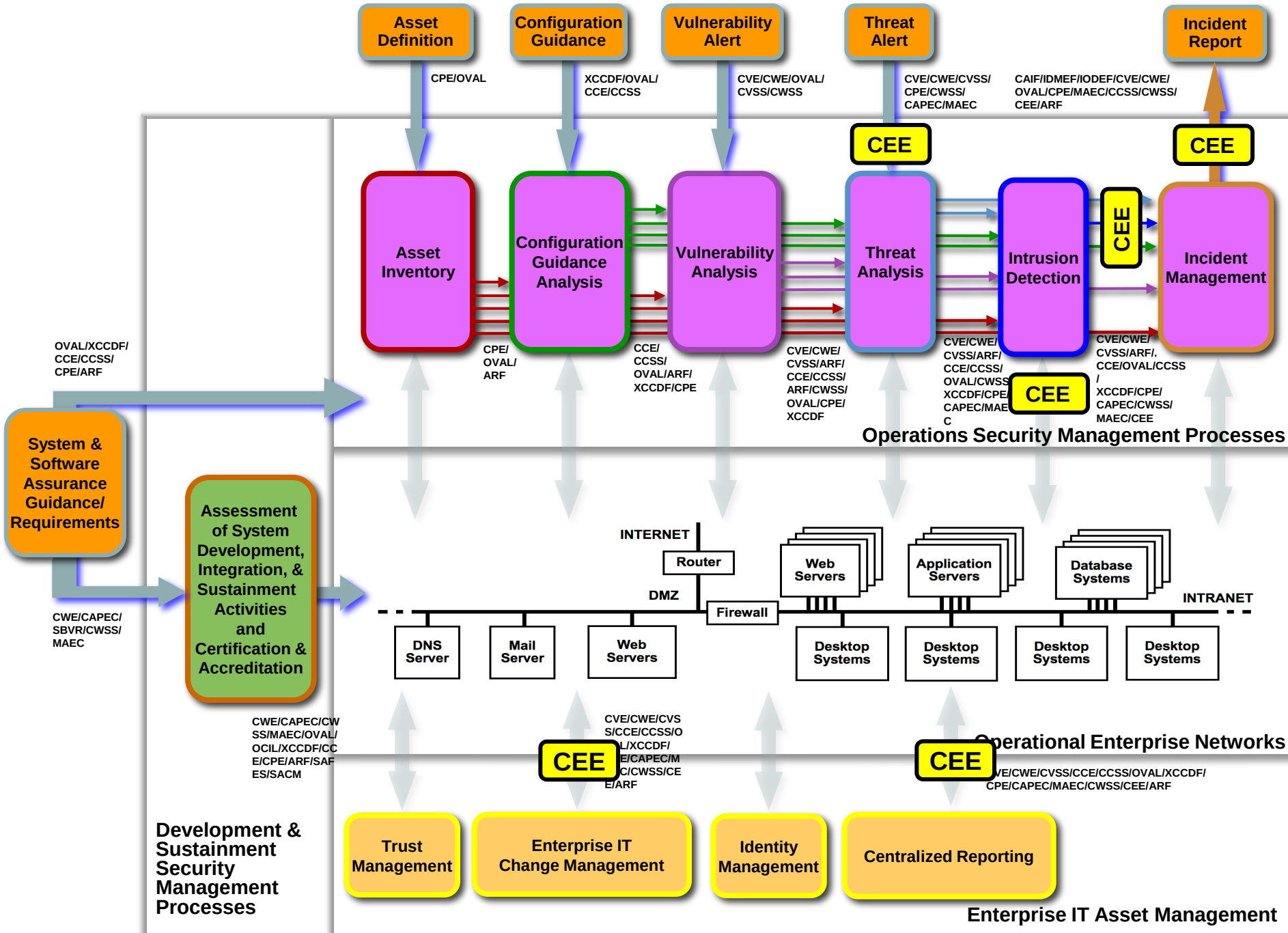

Knowledge Repositories
Asset Definition
Configuration Guidance
Vulnerability Alert
Threat Alert
Incident Report
CPE/OVAL
XCCDF/OVAL/ CCE/CCSS
CVE/CWE/OVAL/ CVSS/CWSS
CVE/CWE/CVSS/ CPE/CWSS/ CAPEC/MAEC
CAIF/IDMEF/IODEF/CVE/CWE/ OVAL/CPE/MAEC/CCSS/CWSS/ CEE/ARF
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAE C
CVE/CWE/ CVSS/ARF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
OVAL/XCCDF/ CCE/CCSS/ CPE/ARF
Operations Security Management Processes
System & Software Assurance Guidance/ Requirements
SAFES
CWE/CAPEC/ SBVR/CWSS/ MAEC
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
SAFES
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/C WSS/MAEC/O VAL/OCIL/XCC DF/CCE/CPE/A RF/SAFES/SA CM
CVE/CWE/CVS S/CCE/CCSS/O L/XCCDF/ E/CAPEC/M C/CWSS/CE E/ARF
SAFES
Operational Enterprise Networks
SAFES
VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/ARF
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management

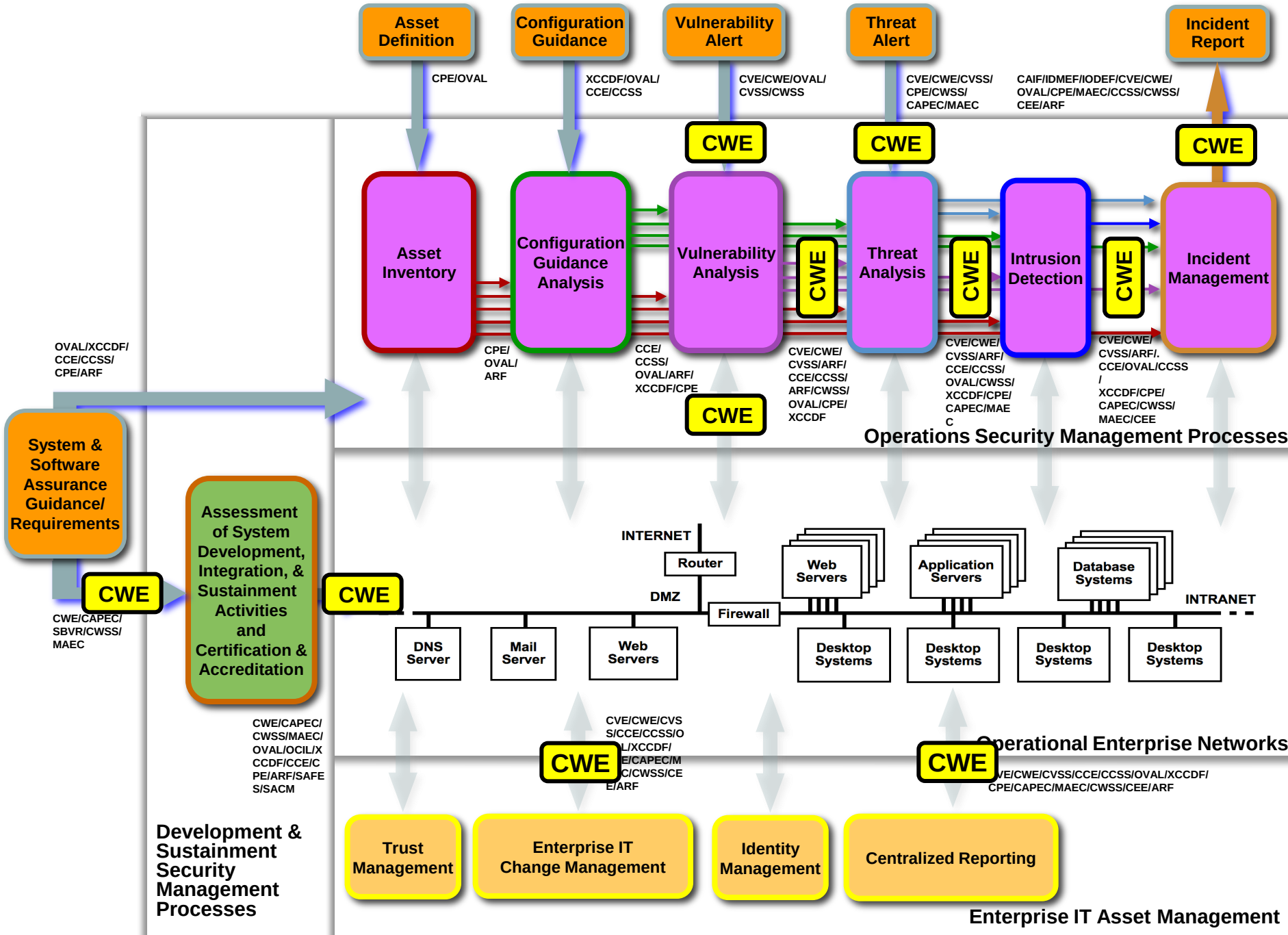

Asset Definition
Configuration Guidance
Vulnerability Alert
Threat Alert
Incident Report
CPE/OVAL
XCCDF/OVAL/ CCE/CCSS
CVE/CWE/OVAL/ CVSS/CWSS
CVE/CWE/CVSS/ CPE/CWSS/ CAPEC/MAEC
CAIF/IDMEF/IODEF/CVE/CWE/ OVAL/CPE/MAEC/CCSS/CWSS/ CEE/ARF
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
OVAL/XCCDF/ CCE/CCSS/ CPE/ARF
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAE C
CVE/CWE/ CVSS/ARF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
Operations Security Management Processes
System & Software Assurance Guidance/ Requirements
SACM
CWE/CAPEC/ SBVR/CWSS/ MAEC
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
SACM
INTERNET
Router
DMZ
Firewall
Web Servers
Application Servers
Database Systems
INTRANET
DNS Server
Mail Server
Web Servers
Desktop Systems
Desktop Systems
Desktop Systems
Desktop Systems
CWE/CAPEC/C WSS/MAEC/O VAL/OCIL/XCC DF/CCE/CPE/A RF/SAFES/SA CM
SACM
CVE/CWE/CVS S/CCE/CCSS/O L/XCCDF/ E/CAPEC/M C/CWSS/CE E/ARF
SACM
VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/ARF
Operational Enterprise Networks
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management

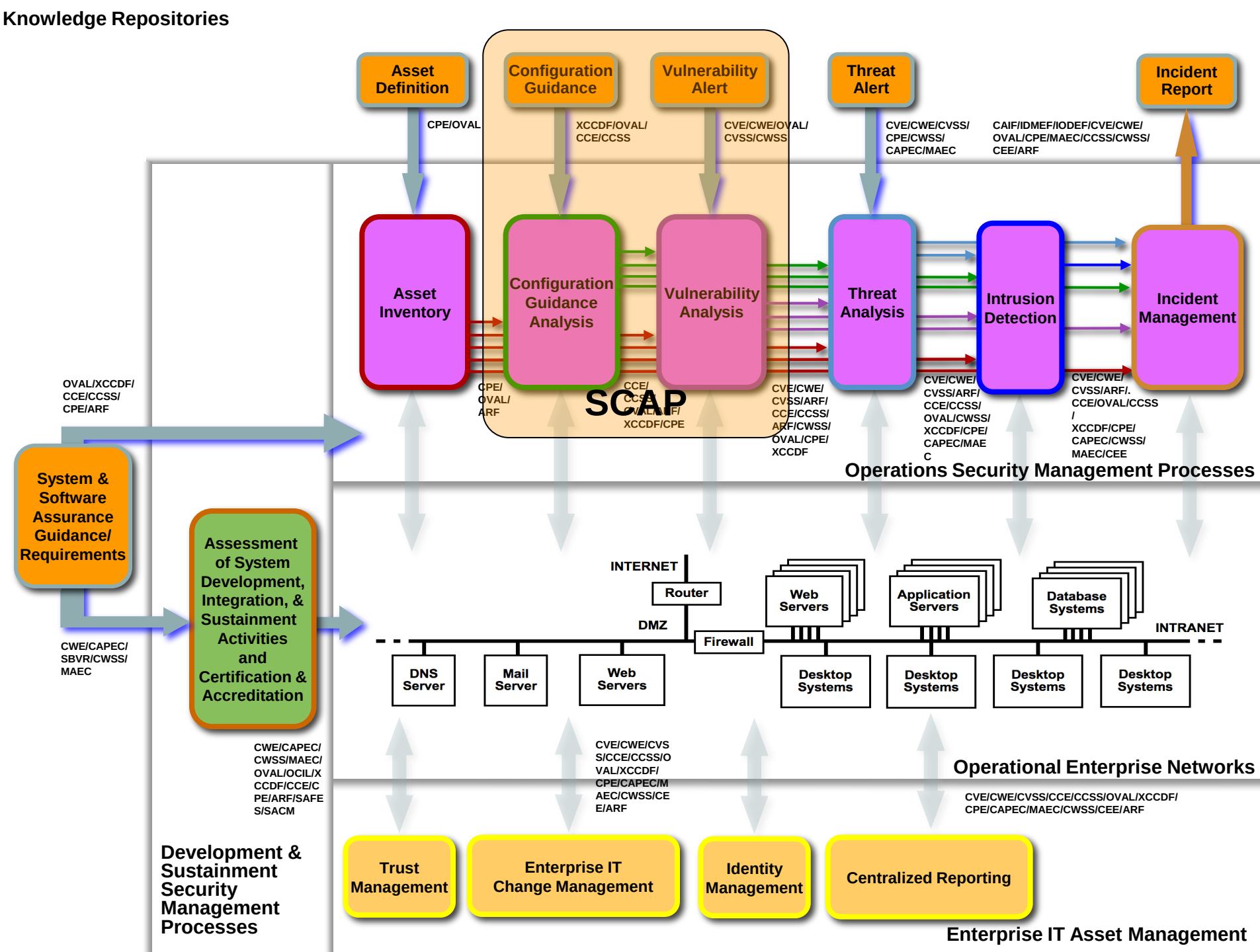

Asset Definition
Configuration Guidance
Vulnerability Alert
Threat Alert
Incident Report
CPE/OVAL
XCCDF/OVAL/ CCE/CCSS
CVE/CWE/OVAL/ CVSS/CWSS
CVE/CWE/CVSS/ CPE/CWSS/ CAPEC/MAEC
CAIF/IDMEF/IODEF/CVE/CWE/ OVAL/CPE/MAEC/CCSS/CWSS/ CEE/ARF
MAEC
MAEC
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVSS/ARF/ CCE/CCSS/ OVAL/CWSS XCCDF/CPE CAPEC/MAEC
CVSS/ARF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
MAEC
MAEC
MAEC
OVAL/XCCDF/ CCE/CCSS/ CPE/ARF
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
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/C WSS/MAEC/OV AL/OCIL/XCCDF /CCE/CPE/ARF/ SAFES/SACM
MAEC
CVE/CWE/CVS S/CCE/CCSS/O L/XCCDF/ E/CAPEC/M C/CWSS/CE E/ARF
MAEC
VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/ARF
Operational Enterprise Networks
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management

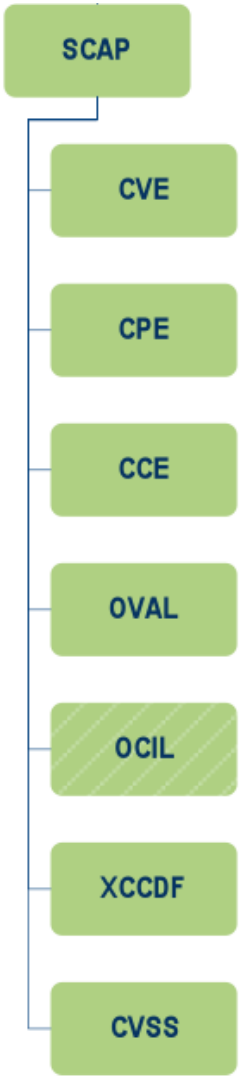

Asset Definition
Configuration Guidance
Vulnerability Alert
Threat Alert
Incident Report
CPE/OVAL
XCCDF/OVAL/ CCE/CCSS
CVE/CWE/OVAL/ CVSS/CWSS
CVE/CWE/CVSS/ CPE/CWSS/ CAPEC/MAEC
CAIF/IDMEF/IODEF/CVE/CWE/ OVAL/CPE/MAEC/CCSS/CWSS/ CEE/ARF
CAPEC
CAPEC
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CAPEC
CAPEC
CAPEC
CAPEC
CVSS/ARF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
OVAL/XCCDF/ CCE/CCSS/ CPE/ARF
Operations Security Management Processes
System & Software Assurance Guidance/ Requirements
CAPEC
CWE/CAPEC/ SBVR/CWSS/ MAEC
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
CAPEC
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/C WSS/MAEC/OV AL/OCIL/XCCDF /CCE/CPE/ARF/ SAFES/SACM
CAPEC
CVE/CWE/CVS S/CCE/CCSS/O L/XCCDF/ E/CAPEC/M C/CWSS/CE E/ARF
CAPEC
VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/ARF
Operational Enterprise Networks
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity 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/ARF
CWE
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAE C
CVE/CWE/ CVSS/ARF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
Operations Security Management Processes
OVAL/XCCDF/ CCE/CCSS/ CPE/ARF
System & Software Assurance Guidance/ Requirements
CWE/CAPEC/ SBVR/CWSS/ MAEC
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
CWE/CAPEC/ CWSS/MAEC/ OVAL/OCIL/X CCDF/CCE/C PE/ARF/SAFE S/SACM
INTERNET
Router
DMZ
Firewall
Web Servers
Application Servers
Database Systems
INTRANET
DNS Server
Mail Server
Web Servers
Desktop Systems
Desktop Systems
Desktop Systems
Desktop Systems
CVE/CWE/CVS S/CCE/CCSS/O L/XCCDF/ E/CAPEC/M C/CWSS/CE E/ARF
Operational Enterprise Networks
VE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/ARF
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management


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/ARF
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAE C
CVE/CWE/ CVSS/ARF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
SCAP
OVAL/XCCDF/ CCE/CCSS/ CPE/ARF
Operations Security Management Processes
System & Software Assurance Guidance/ Requirements
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
CWE/CAPEC/ SBVR/CWSS/ MAEC
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/ CWSS/MAEC/ OVAL/OCIL/X CCDF/CCE/C PE/ARF/SAFE S/SACM
CVE/CWE/CVS S/CCE/CCSS/O VAL/XCCDF/ CPE/CAPEC/M AEC/CWSS/CE E/ARF
Operational Enterprise Networks
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/ARF
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management



SCAP 1.1 uses the following specifications:

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

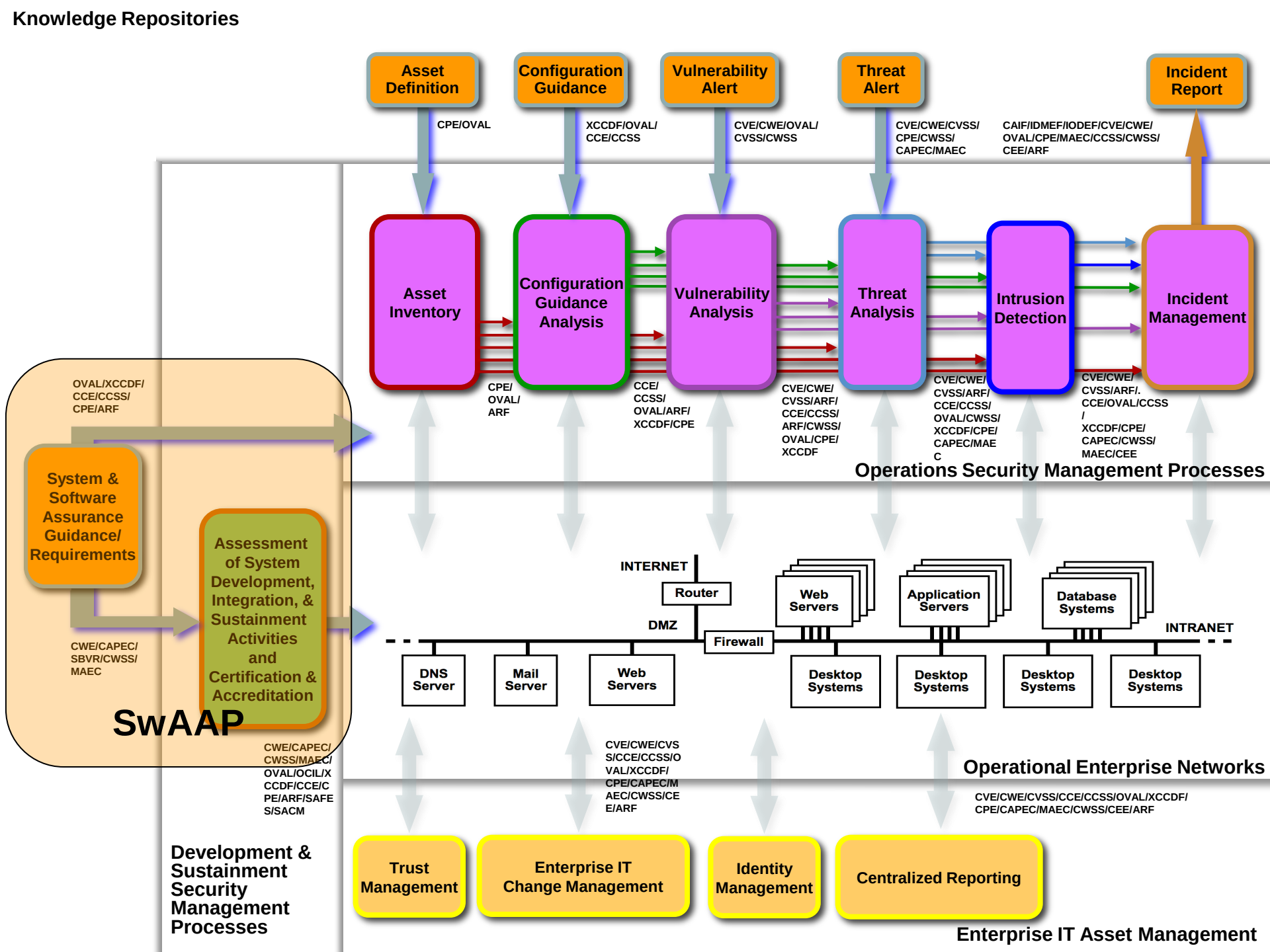
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-126
Revision 1 (DRAFT)

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

Recommendations of the National Institute of Standards and Technology

Stephen Quinn
David Waltermire
Christopher Johnson
Karen Scarfone
John Banghart


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/ARF
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
CPE/ OVAL/ ARF
CCE/ CCSS/ OVAL/ARF/ XCCDF/CPE
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ ARF/CWSS/ OVAL/CPE/ XCCDF
CVE/CWE/ CVSS/ARF/ CCE/CCSS/ OVAL/CWSS/ XCCDF/CPE/ CAPEC/MAE C
CVE/CWE/ CVSS/ARF/. CCE/OVAL/CCSS / XCCDF/CPE/ CAPEC/CWSS/ MAEC/CEE
Operations Security Management Processes
OVAL/XCCDF/ CCE/CCSS/ CPE/ARF
System & Software Assurance Guidance/ Requirements
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
CWE/CAPEC/ SBVR/CWSS/ MAEC
SwAAP
CWE/CAPEC/ CWSS/MAEC/ OVAL/OCIL/X CCDF/CCE/C PE/ARF/SAFE S/SACM
INTERNET
Router
DMZ
Firewall
Web Servers
Application Servers
Database Systems
INTRANET
DNS Server
Mail Server
Web Servers
Desktop Systems
Desktop Systems
Desktop Systems
Desktop Systems
CVE/CWE/CVS S/CCE/CCSS/O VAL/XCCDF/ CPE/CAPEC/M AEC/CWSS/CE E/ARF
Operational Enterprise Networks
CVE/CWE/CVSS/CCE/CCSS/OVAL/XCCDF/ CPE/CAPEC/MAEC/CWSS/CEE/ARF
Development & Sustainment Security Management Processes
Trust Management
Enterprise IT Change Management
Identity Management
Centralized Reporting
Enterprise IT Asset Management

SwAAP

CWE

CAPEC

MAEC

CWSS

OMG SACM

OMG XRG

SAFES

"Food Label"

OMG SMM

ISO 15026

OMG KDM

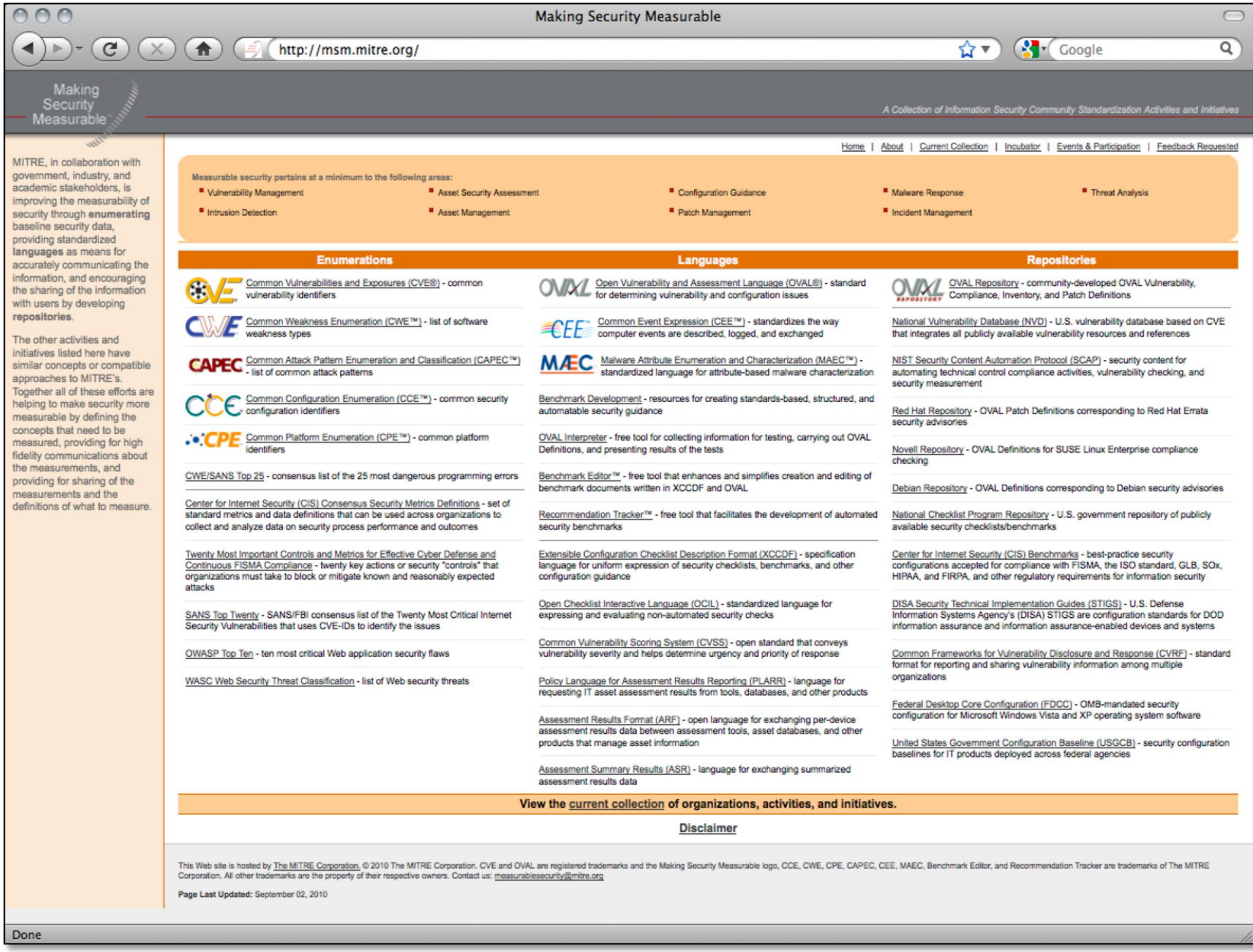
OMG ASTM

- **Software Assurance Automation Protocol (SwAAP)**
  - **For measuring & enumerating software weaknesses and the assurance cases.**

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™


Questions?
ramartin@mitre.org