

What Do The Building Blocks for Measuring Assurance 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

The Building Blocks Are:

- Enumerations
 - **Catalog the fundamental entities in 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), software security patterns (SBVR), event patterns (CEE), malware patterns (MAEC), risk of a vulnerability (CVSS), config risk (CCSS), weakness risk (CWSS), information messages (CAIF & *DEF)**
- Knowledge Repositories
 - **Packages of assertions supporting a specific application**
 - **Vulnerability advisories & alerts, (US-CERT Advisories/ IAVAs), configuration assessment (NIST Checklists, CIS Benchmarks, NSA Configuration Guides, DISA STIGS), asset inventory (NIST/DHS NVD), code assessment & certification (NIST SAMATE, DoD DIACAP & eMASS)**

Common Weakness Enumeration (CWE)

- Weaknesses are characteristics of software that may lead to vulnerability
- Existence of weaknesses in software can be objectively measured through the use of various techniques and tools
- Software assurance is determined by the absence of weaknesses identified as relevant for a given context and assurance level

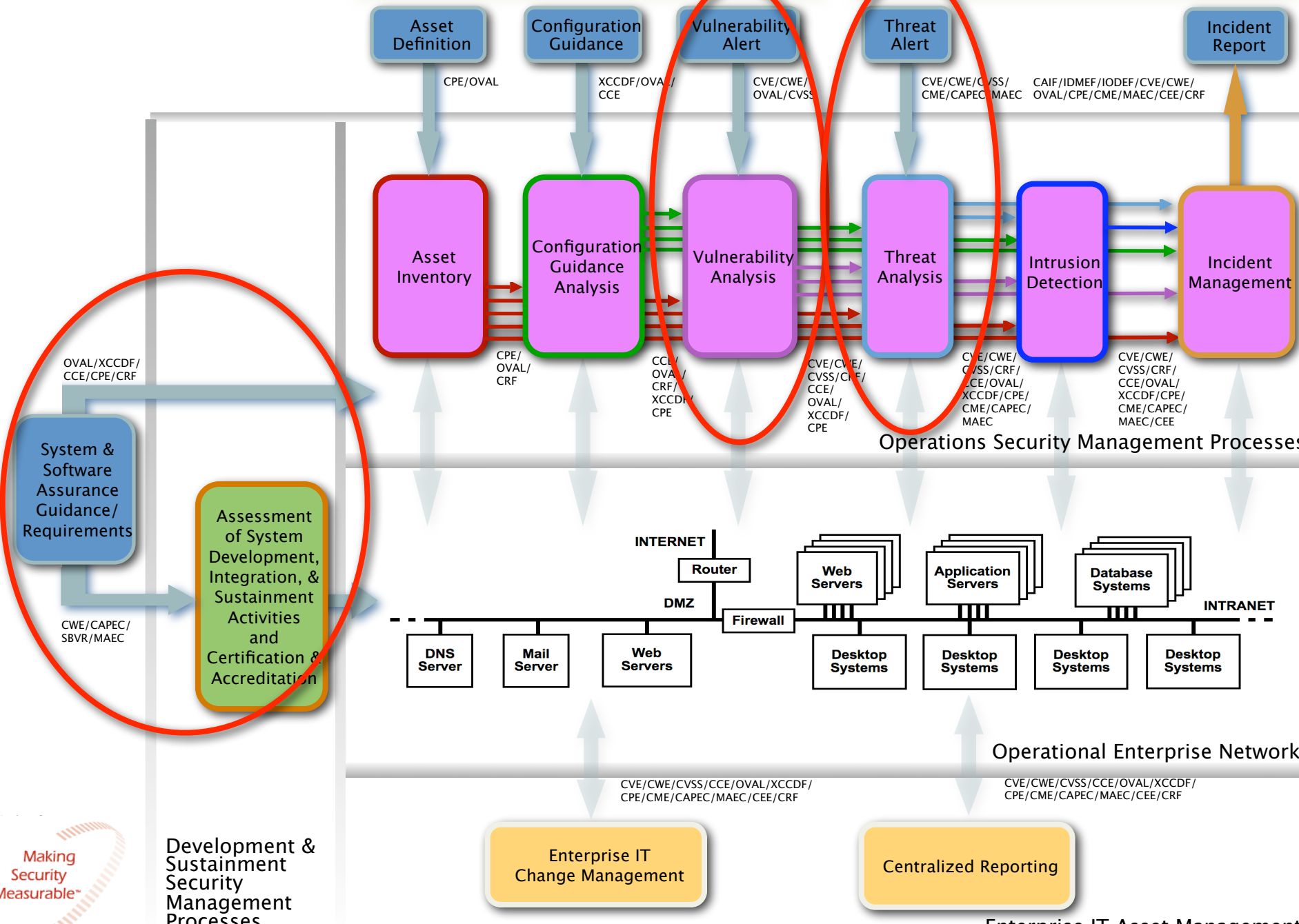
- CWE is an effort targeted at standardizing the capture and description of weaknesses and providing a useful collection to be leveraged by the community
- Community effort developed from dozens of sources
- CWE version 1.1 was released December 2008
- Already being used in education, tools, software risk assessment, policy, etc.



What is the Common Attack Pattern

- Effort targeted at:
 - Standardizing the capture and description of attack patterns
 - Collecting known attack patterns into an integrated enumeration that can be consistently and effectively leveraged by the community
 - Classifying attack patterns such that users can easily identify the subset of the entire enumeration that is appropriate for their context
- <http://capec.mitre.org>
- Sponsored by DHS
- Led by Cigital





Development & Sustainment Security Management Processes

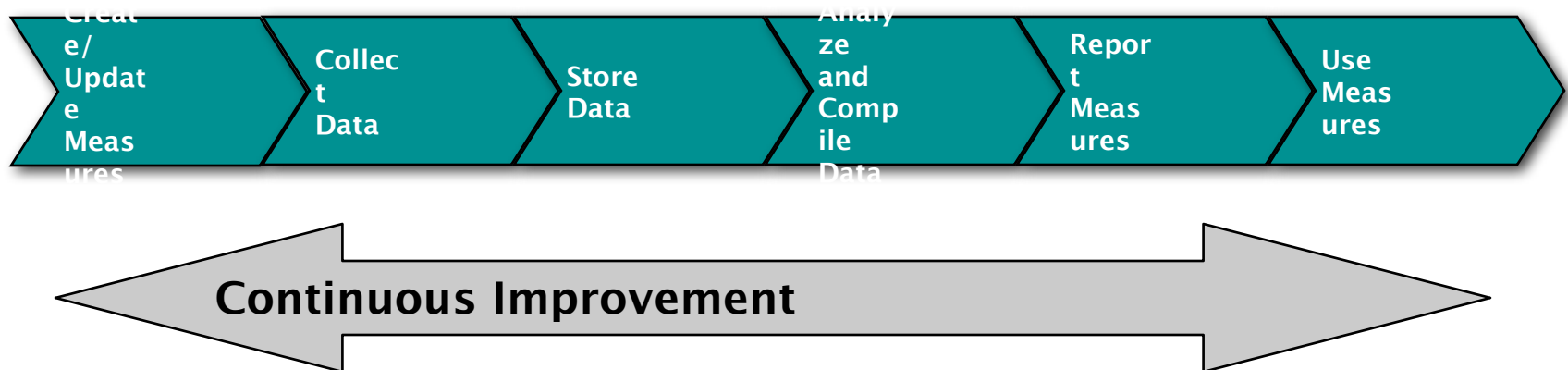
Enterprise IT Change Management

Centralized Reporting

Enterprise IT Asset Management

Practical Measurement Framework

- Harmonized with five prevailing system/software and security measurement approaches
- Provides basic measures development and implementation processes
- Provides general measures examples
- Integrates with existing measurement programs
- Incorporates Making Security Measurable products
- Provides an overarching framework for summarizing SwA measures and communicating them to stakeholders



What Is Measurable Today?

- **Enumerations of Things That We Want to Know About:**
 - Common Weakness Enumeration (CWE)
 - Common Attack Pattern Enumeration and Classification (CAPEC)
 - Common Vulnerabilities and Exposures (CVE)
 - Common Configuration Enumeration (CCE)
- **Ways of Expressing Details About Enumerated Items:**
 - Open Vulnerability and Assessment Language (OVAL)
 - XML Configuration Checklist Data Format (XCCDF)
 - Common Platform Enumeration (CPE)
 - Common Vulnerabilities Scoring System (CVSS)
 - Common Configuration Scoring System (CCSS)
 - Common Weakness Scoring System (CWSS)
- **Repositories of Content with Measurement Criteria**
 - SCAP (Secure Content Automation Protocol)

Other measurable items include quality and project management measures which are well developed and available for use