"Vendor Neutral Security Measurement & Management with Standards"

Robert A. Martin
MITRE

ITU-T Workshop on
Addressing
security challenges
on a global scale

Making Security Measurable™

6 – 7 December 2010 Geneva, Switzerland

ITU

Our Locations

- Principal locations in Bedford, Mass., and McLean, Va., with more than 60 sites worldwide

Bedford, Mass.

McLean, Va.

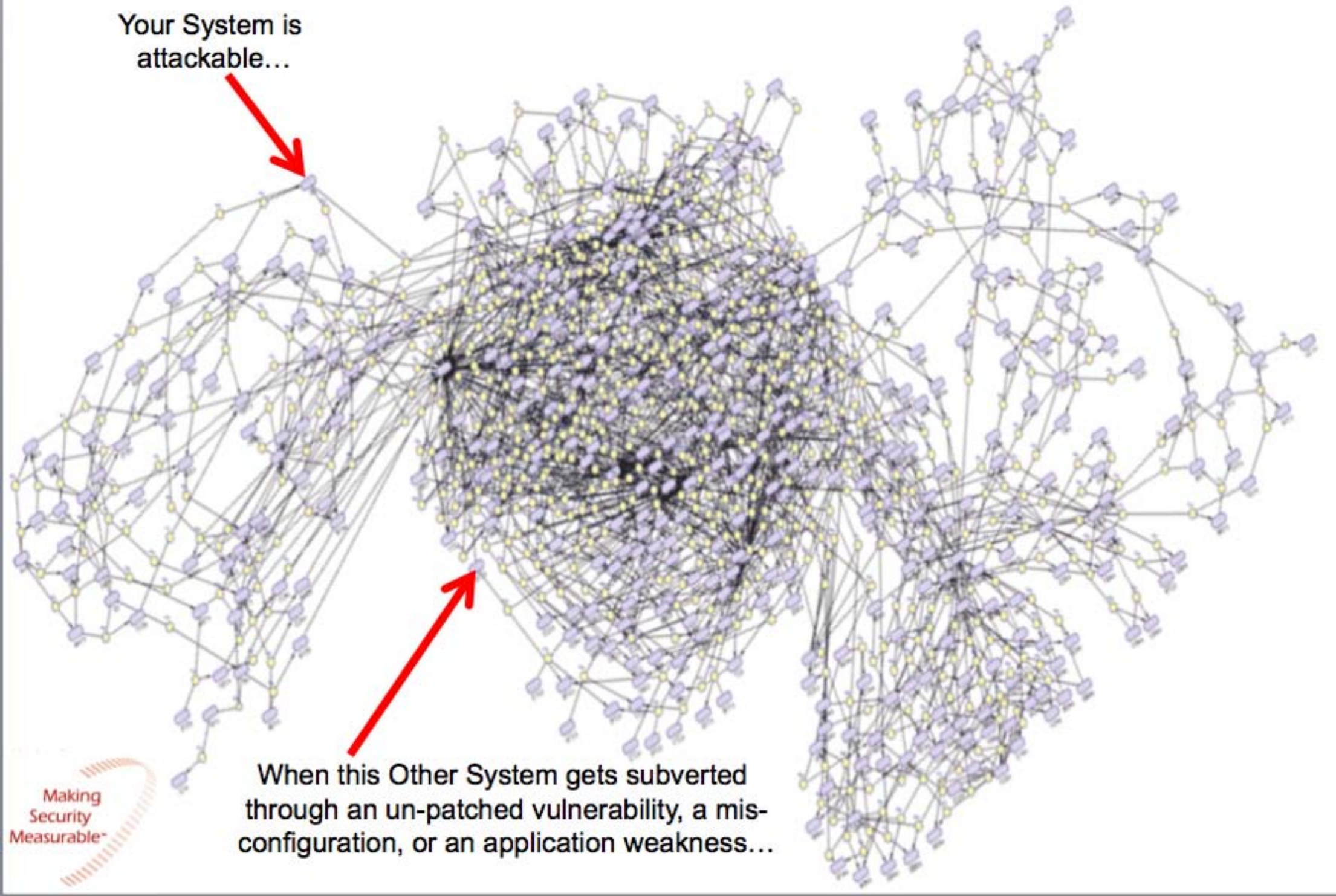
MITRE

MITRE's Workforce . . . Our Key Asset

- 7,000 employees worldwide
- Committed to public service
- Technically skilled, highly collaborative
- Work side-by-side with our sponsors

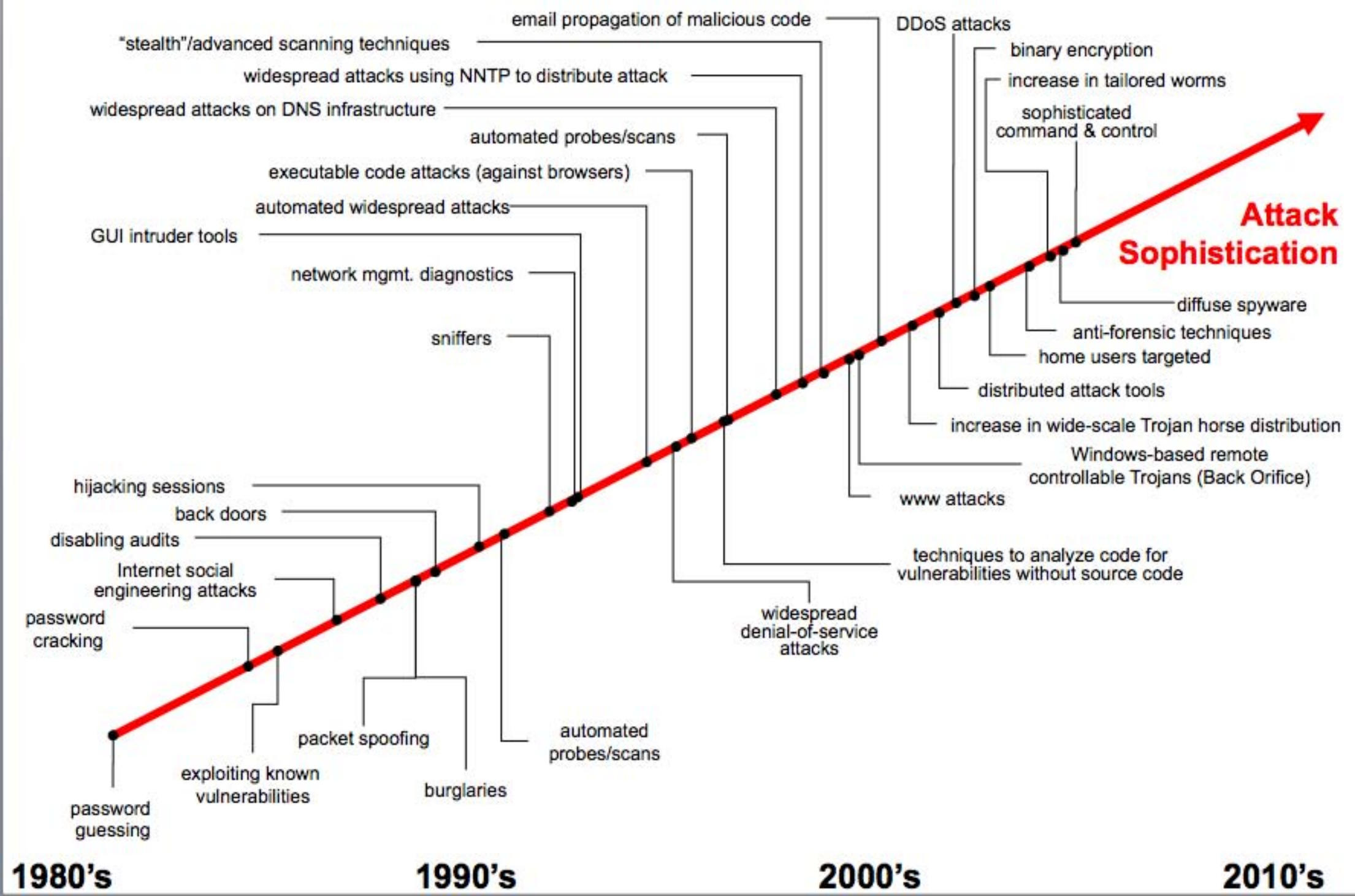
MITRE

Today Everything's Connected

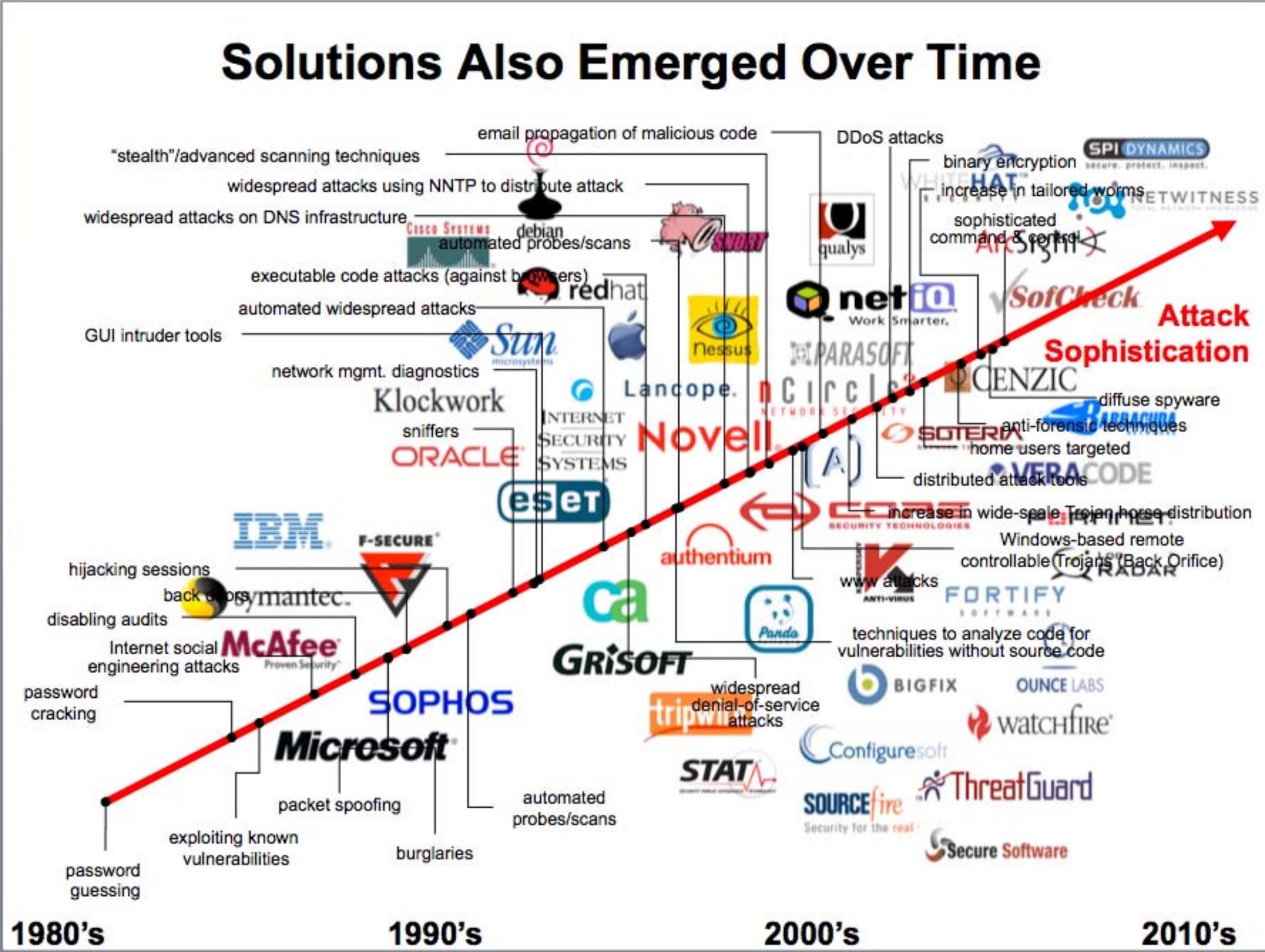


Making Security Measurable™

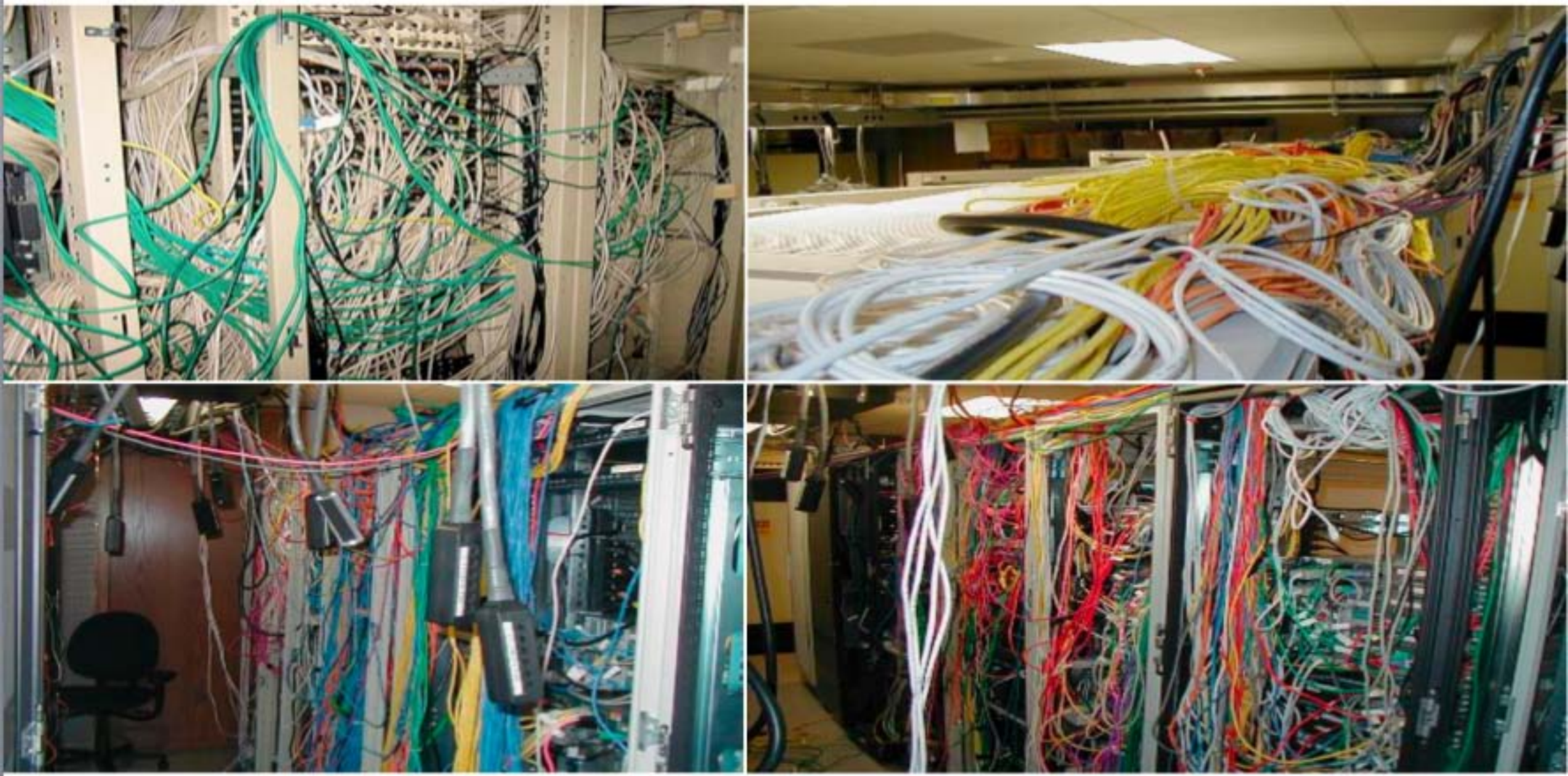
Cyber Threats Emerged Over Time



Solutions Also Emerged Over Time



Like Security - Networks Evolved



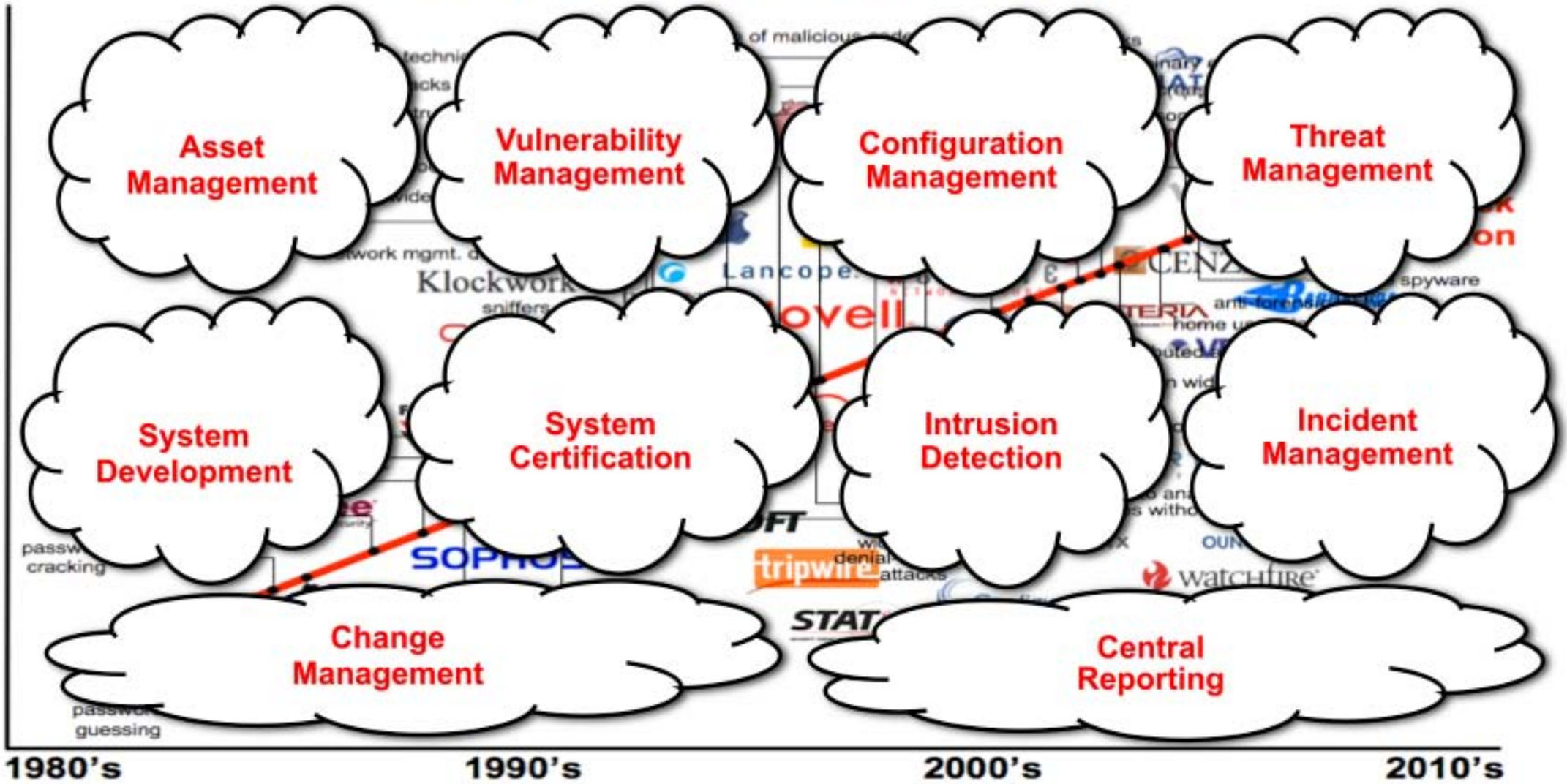
Each new solution had to integrate with the existing solutions

-->> 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:

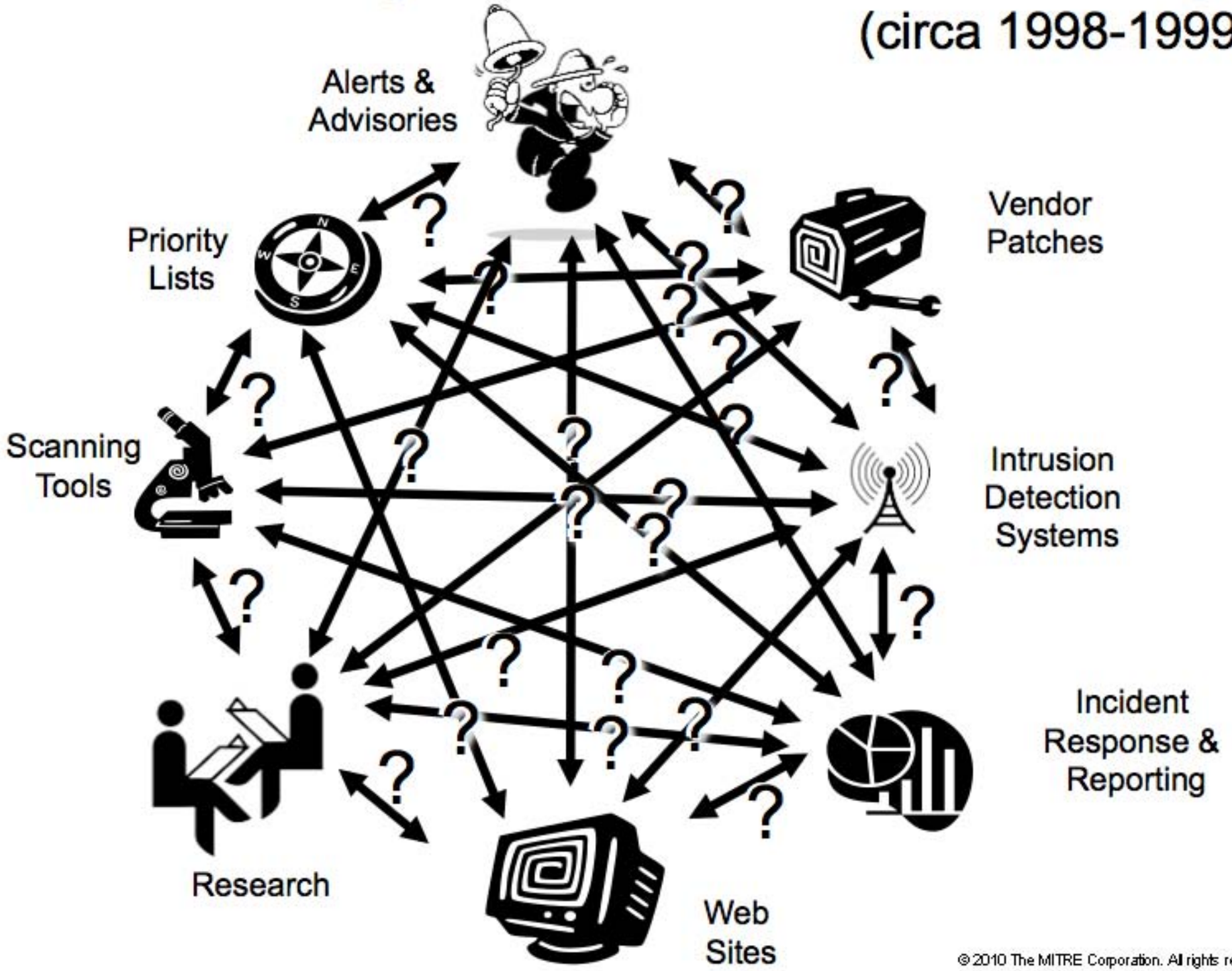
- Enumerations
  - **Catalog the fundamental entities in IA, Cyber Security, and Software Assurance**
    - **Vulnerabilities (CVE), configuration issues (CCE), software packages (CPE), attack patterns (CAPEC), weaknesses in code/design/architecture (CWE)**
- Languages/Formats
  - **Support the creation of machine-readable state assertions, assessment results, and messages**
    - **Configuration/vulnerability/patch/asset patterns (XCCDF & OVAL), results from standards-based assessments (ARF), software security patterns (SBVR), event patterns (CEE), malware patterns (MAEC), risk of a vulnerability (CVSS), config risk (CCSS), weakness risk (CWSS), information messages (CAIF & *DEF)**
- Knowledge Repositories
  - **Packages of assertions supporting a specific application**
    - **Vulnerability advisories & alerts, (US-CERT Advisories/IAVAs), configuration assessment (NIST Checklists, CIS Benchmarks, NSA Configuration Guides, DISA STIGS), asset inventory (NIST/DHS NVD), code assessment & certification (NIST SAMATE, DoD DIACAP & eMASS)**

Tools

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

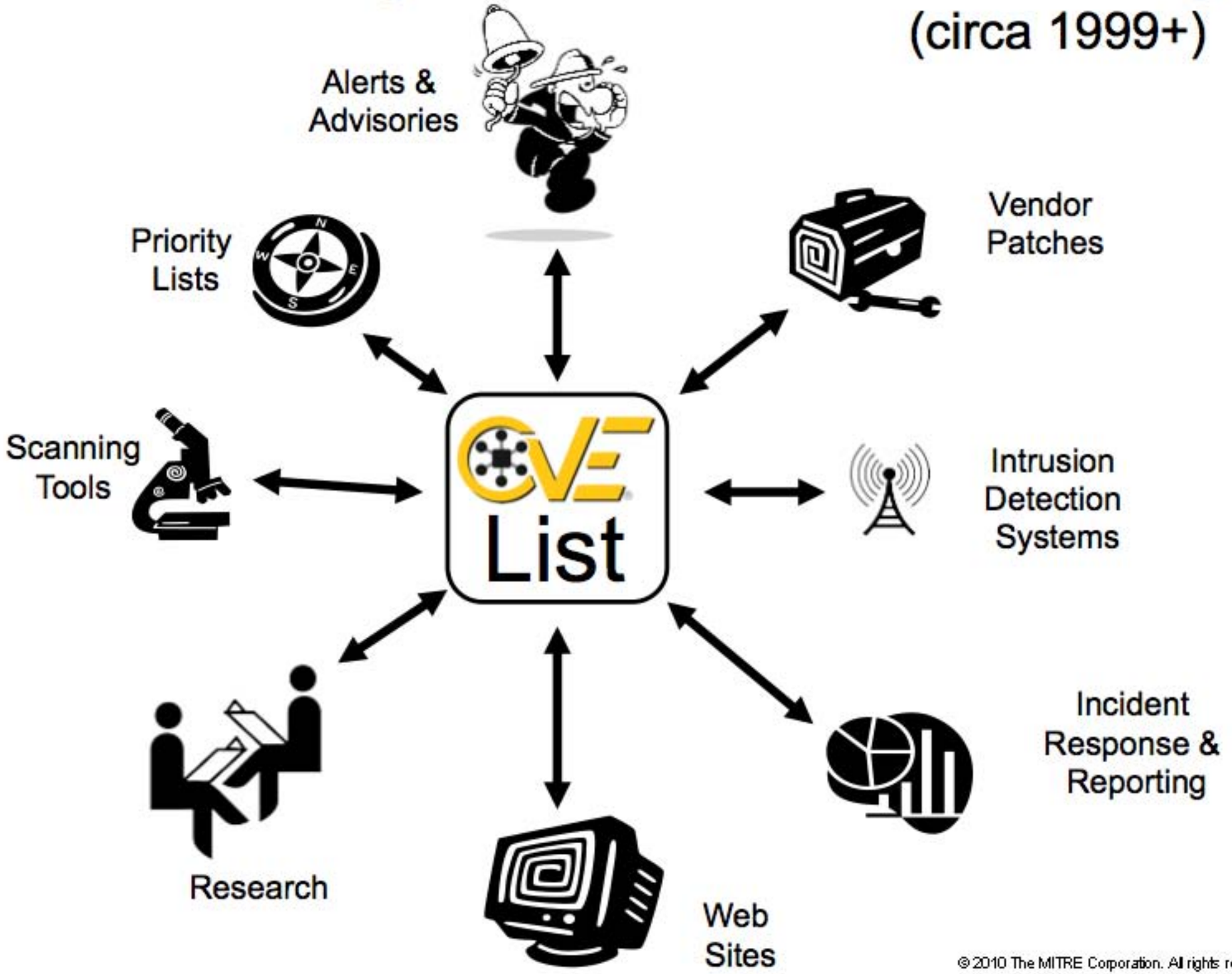
Vulnerability Information Sharing

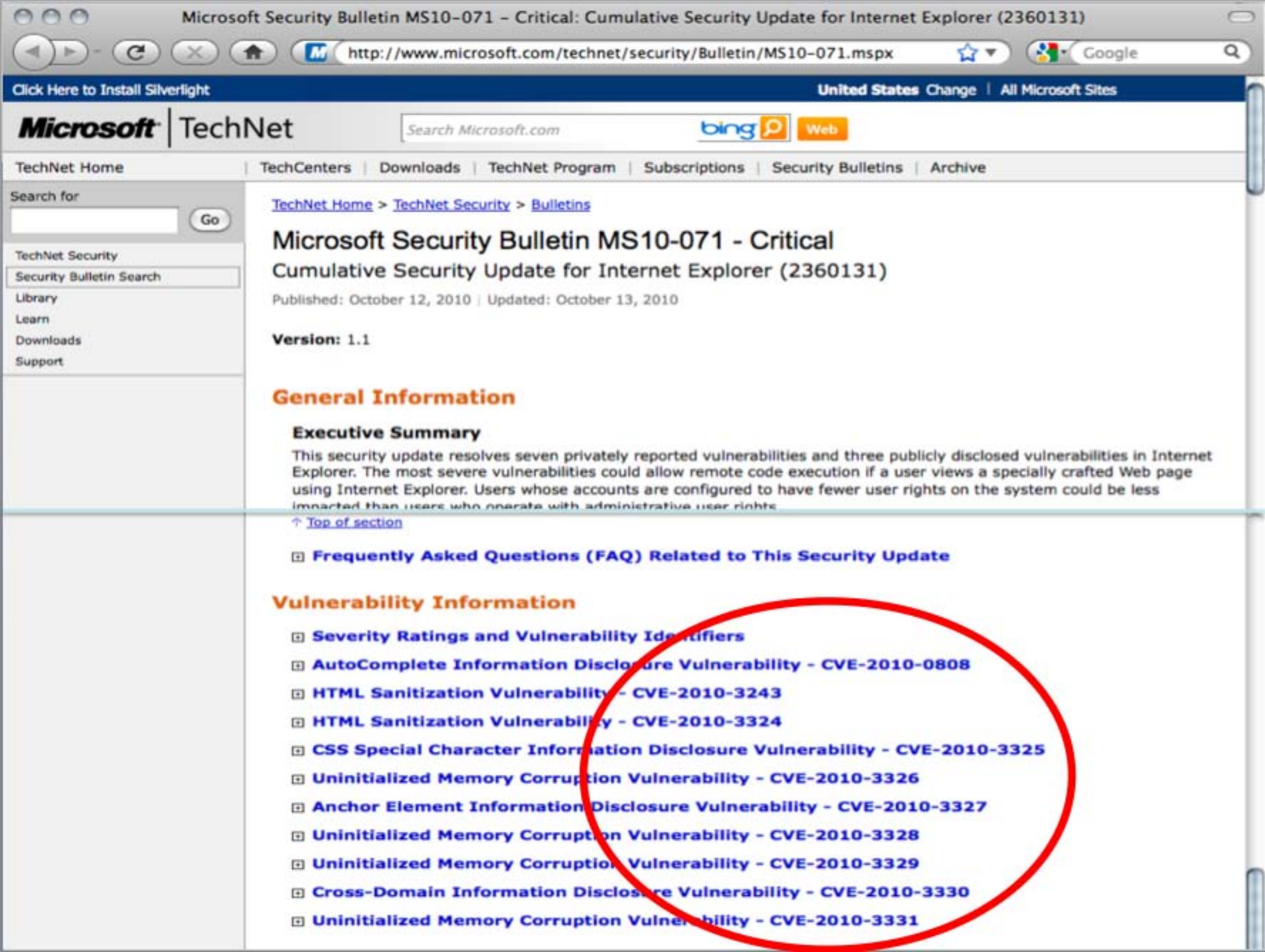
(circa 1998-1999)



Vulnerability Information Sharing

(circa 1999+)




Microsoft Security Bulletin MS10-071 – Critical: Cumulative Security Update for Internet Explorer (2360131)
http://www.microsoft.com/technet/security/Bulletin/MS10-071.mspx
Google
Click Here to Install Silverlight
United States Change | All Microsoft Sites
Microsoft TechNet
Search Microsoft.com
bing
Web
TechNet Home | TechCenters | Downloads | TechNet Program | Subscriptions | Security Bulletins | Archive
Search for
Go
TechNet Security
Security Bulletin Search
Library
Learn
Downloads
Support
TechNet Home > TechNet Security > Bulletins
Microsoft Security Bulletin MS10-071 - Critical
Cumulative Security Update for Internet Explorer (2360131)
Published: October 12, 2010 | Updated: October 13, 2010
Version: 1.1
General Information
Executive Summary
This security update resolves seven privately reported vulnerabilities and three publicly disclosed vulnerabilities in Internet Explorer. The most severe vulnerabilities could allow remote code execution if a user views a specially crafted Web page using Internet Explorer. Users whose accounts are configured to have fewer user rights on the system could be less
Top of section
Frequently Asked Questions (FAQ) Related to This Security Update
Vulnerability Information
Severity Ratings and Vulnerability Identifiers
AutoComplete Information Disclosure Vulnerability - CVE-2010-0808
HTML Sanitization Vulnerability - CVE-2010-3243
HTML Sanitization Vulnerability - CVE-2010-3324
CSS Special Character Information Disclosure Vulnerability - CVE-2010-3325
Uninitialized Memory Corruption Vulnerability - CVE-2010-3326
Anchor Element Information Disclosure Vulnerability - CVE-2010-3327
Uninitialized Memory Corruption Vulnerability - CVE-2010-3328
Uninitialized Memory Corruption Vulnerability - CVE-2010-3329
Cross-Domain Information Disclosure Vulnerability - CVE-2010-3330
Uninitialized Memory Corruption Vulnerability - CVE-2010-3331

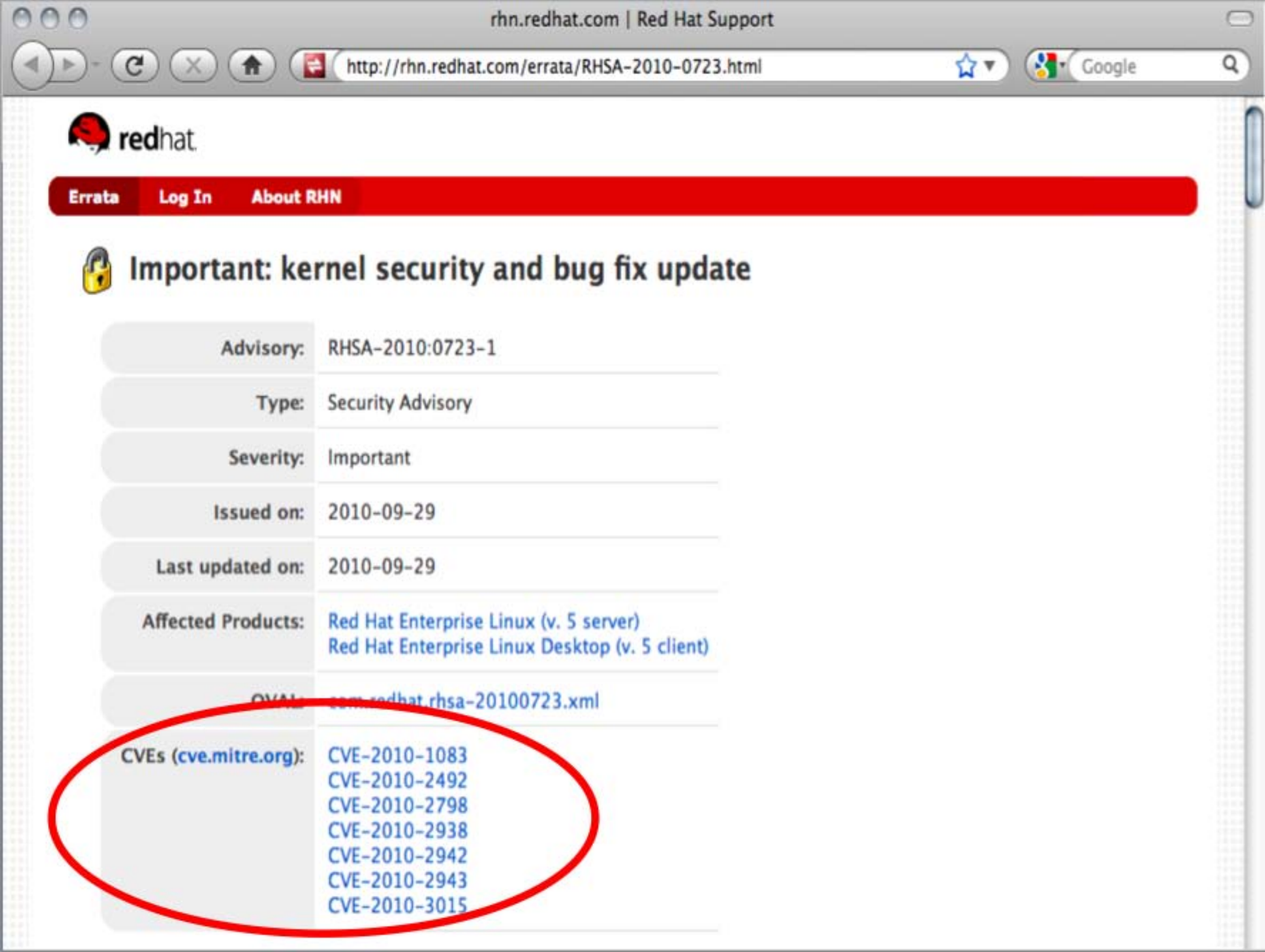
Oracle Critical Patch Update Advisory - October 2010

Description

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. It also includes non-security fixes that are required (because of interdependencies) by those security patches. Critical Patch Updates are cumulative, except as noted below, but each advisory describes only the security fixes added since the previous Critical Patch Update. Thus, prior Critical Patch Update Advisories should be reviewed for information regarding earlier accumulated security fixes. Please refer to:

Oracle Database Server Risk Matrix

CVE#	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?	CVSS VERSION 2.0 RISK (see Risk Matrix Definitions)							Last Affected Patch set (per Supported Release)	Notes
					Base Score	Access Vector	Access Complexity	Authen-tication	Confiden-tiality	Integrity	Avail-ability		
CVE-2010-2390 (Oracle Enterprise Manager Grid Control)	EM Console	HTTP	None	Yes	7.5	Network	Low	None	Partial+	Partial+	Partial+	10.1.0.5, 10.2.0.3	See Note 1
CVE-2010-2419	Java Virtual Machine	Oracle Net	Create Session	No	6.5	Network	Low	Single	Partial+	Partial+	Partial+	10.1.0.5, 10.2.0.4, 11.1.0.7, 11.2.0.1	
CVE-2010-1321	Change Data Capture	Oracle Net	Execute on DBMS_CDC_PUBLISH	No	5.5	Network	Low	Single	Partial+	Partial+	None	-	See Note 2
CVE-2010-2412	OLAP	Oracle Net	Create Session	No	5.5	Network	Low	Single	Partial+	Partial+	None	11.1.0.7	
CVE-2010-2415	Change Data Capture	Oracle Net	Execute on DBMS_CDC_PUBLISH	No	4.9	Network	Medium	Single	Partial+	Partial+	None	10.1.0.5, 10.2.0.4, 11.1.0.7, 11.2.0.1	
CVE-2010-2411	Job Queue	Oracle Net	Execute on SYS.DBMS_IJOB	No	4.6	Network	High	Single	Partial+	Partial+	Partial+	-	See Note 2
CVE-2010-2407	JDK	HTTP	None	Yes	4.3	Network	Medium	None	None	Partial	None	10.1.0.5, 10.2.0.4, 11.1.0.7	
CVE-2010-2391	Core RDBMS	Oracle Net	Create Session	No	3.6	Network	High	Single	Partial	Partial	None	10.1.0.5, 10.2.0.3	
CVE-2010-2389 (Oracle Fusion Middleware)	Perl	Oracle Net	Local Logon	No	1.0	Local	High	Single	None	Partial+	None	-	See Note 2

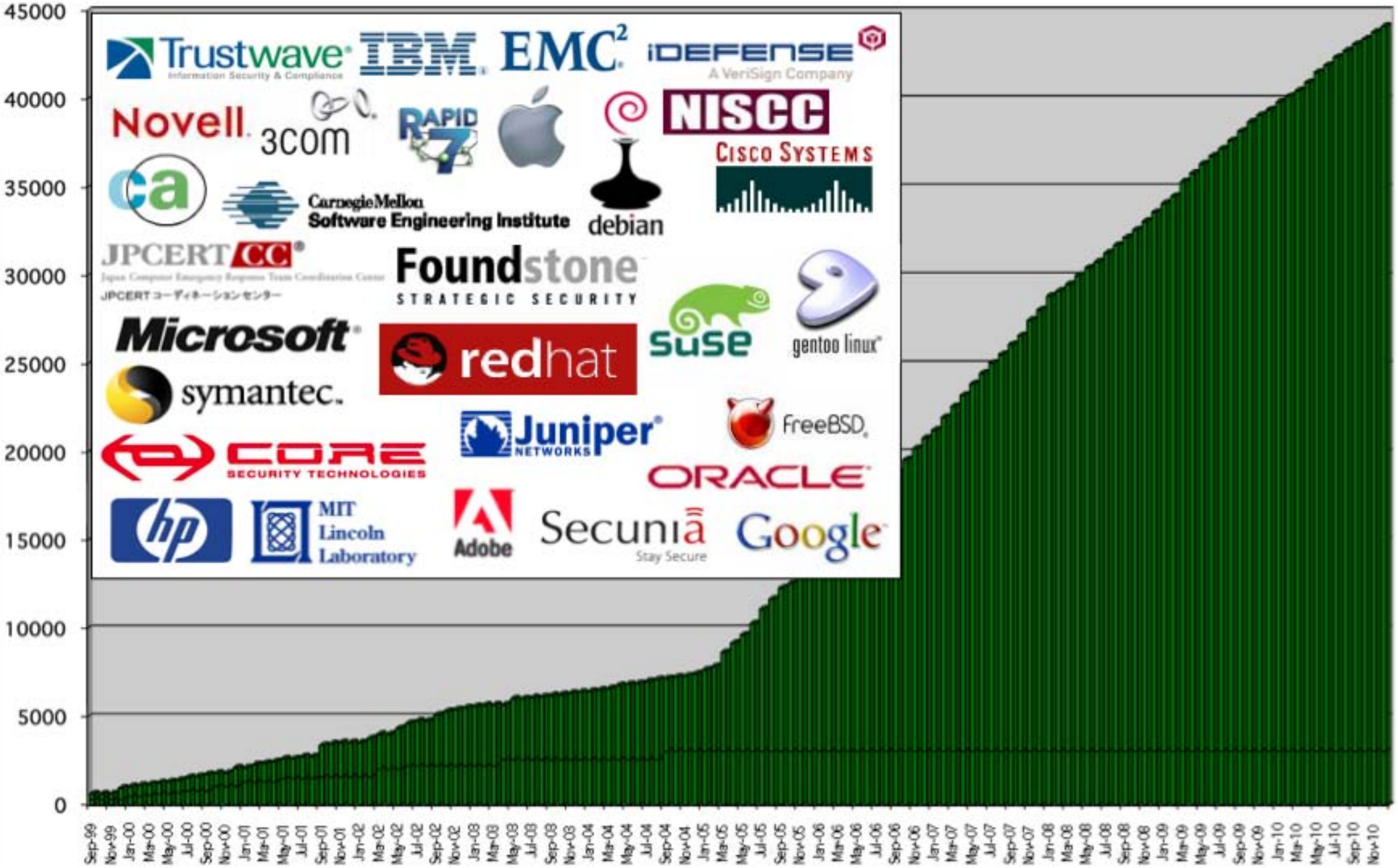

rhn.redhat.com | Red Hat Support
http://rhn.redhat.com/errata/RHSA-2010-0723.html
Google
redhat
Errata
Log In
About RHN
Important: kernel security and bug fix update
Advisory:
RHSA-2010:0723-1
Type:
Security Advisory
Severity:
Important
Issued on:
2010-09-29
Last updated on:
2010-09-29
Affected Products:
Red Hat Enterprise Linux (v. 5 server)
Red Hat Enterprise Linux Desktop (v. 5 client)
rhsa-20100723.xml
CVEs (cve.mitre.org):
CVE-2010-1083
CVE-2010-2492
CVE-2010-2798
CVE-2010-2938
CVE-2010-2942
CVE-2010-2943
CVE-2010-3015

APPLE-SA-2010-08-11-1 iOS 4.0.2 Update for iPhone and iPod touch

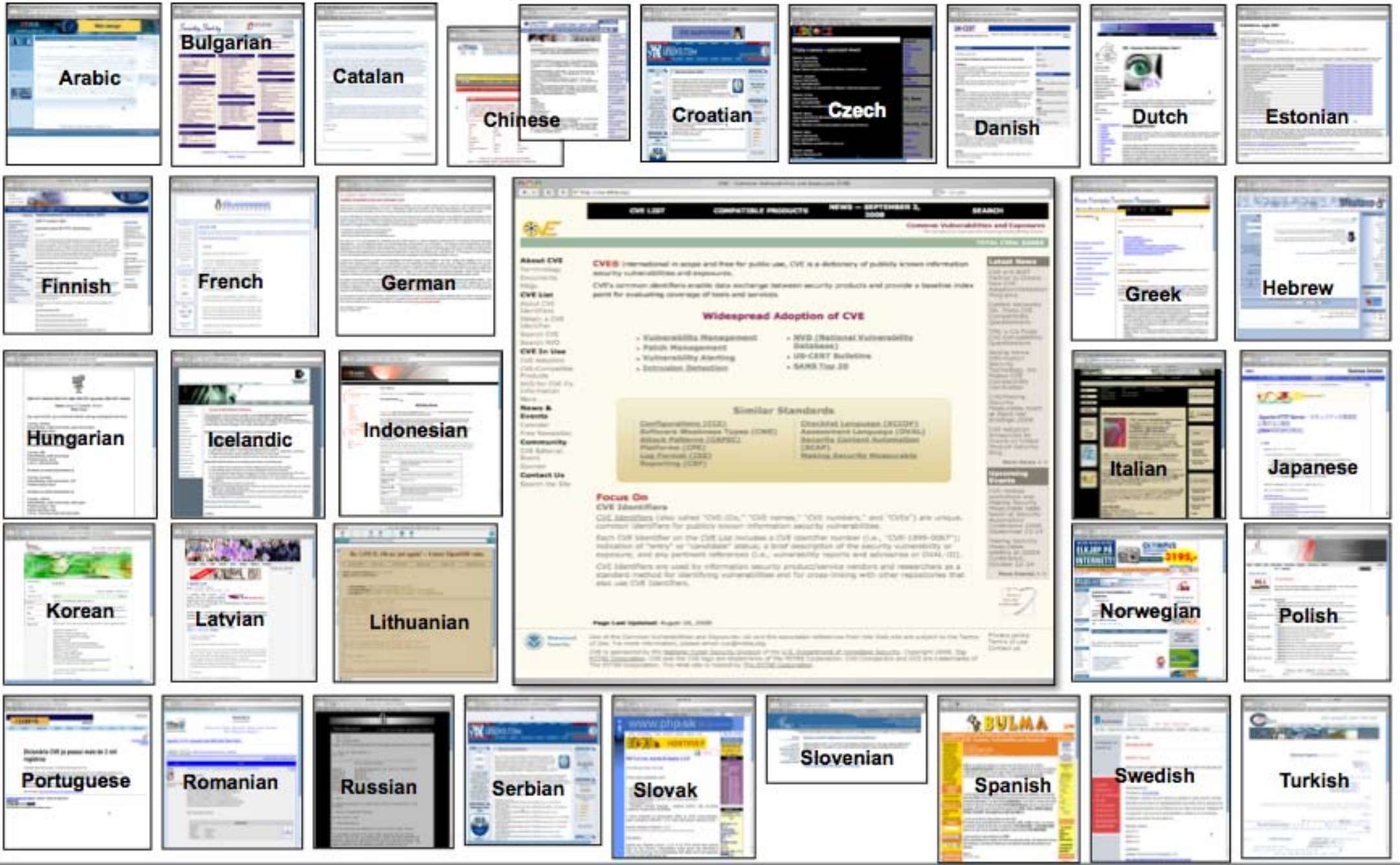
Subject: APPLE-SA-2010-08-11-1 iOS 4.0.2 Update for iPhone and iPod touch
From: Apple Product Security <email@hidden>
Date: Wed, 11 Aug 2010 12:19:43 -0700
Delivered-to: email@hidden
Delivered-to: email@hidden

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

APPLE-SA-2010-08-11-1 iOS 4.0.2 Update for iPhone and iPod touch

iOS 4.0.2 Update for iPhone and iPod touch is now available and
addresses the following:

FreeType
CVE-ID:  CVE-2010-1797
Available for:  iOS 2.0 through 4.0.1 for iPhone 3G and later,
iOS 2.1 through 4.0 for iPod touch (2nd generation) and later
Impact:  Viewing a PDF document with maliciously crafted embedded
fonts may allow arbitrary code execution
Description:  A stack buffer overflow exists in FreeType's handling
of CFF opcodes. Viewing a PDF document with maliciously crafted
```

CVE 1999 to 2010



CVE is Widely Used & Available
44,144 and climbing…



CVE Vendor/Industry Engagement

Knowledge Repositories

Vulnerability Alerts

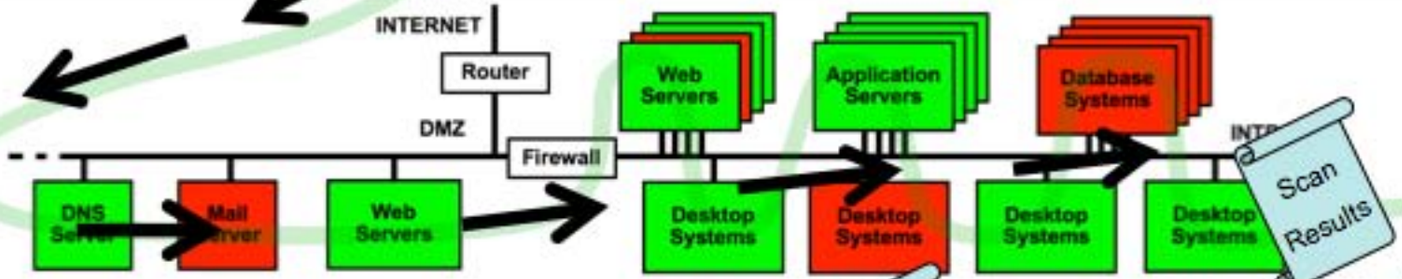
Red Hat errata

Vulnerability Analysis

Operations Security Management Processes

OVAL "Compatible" Tools

Operational Enterprise Networks



Scan Results

Scan Results

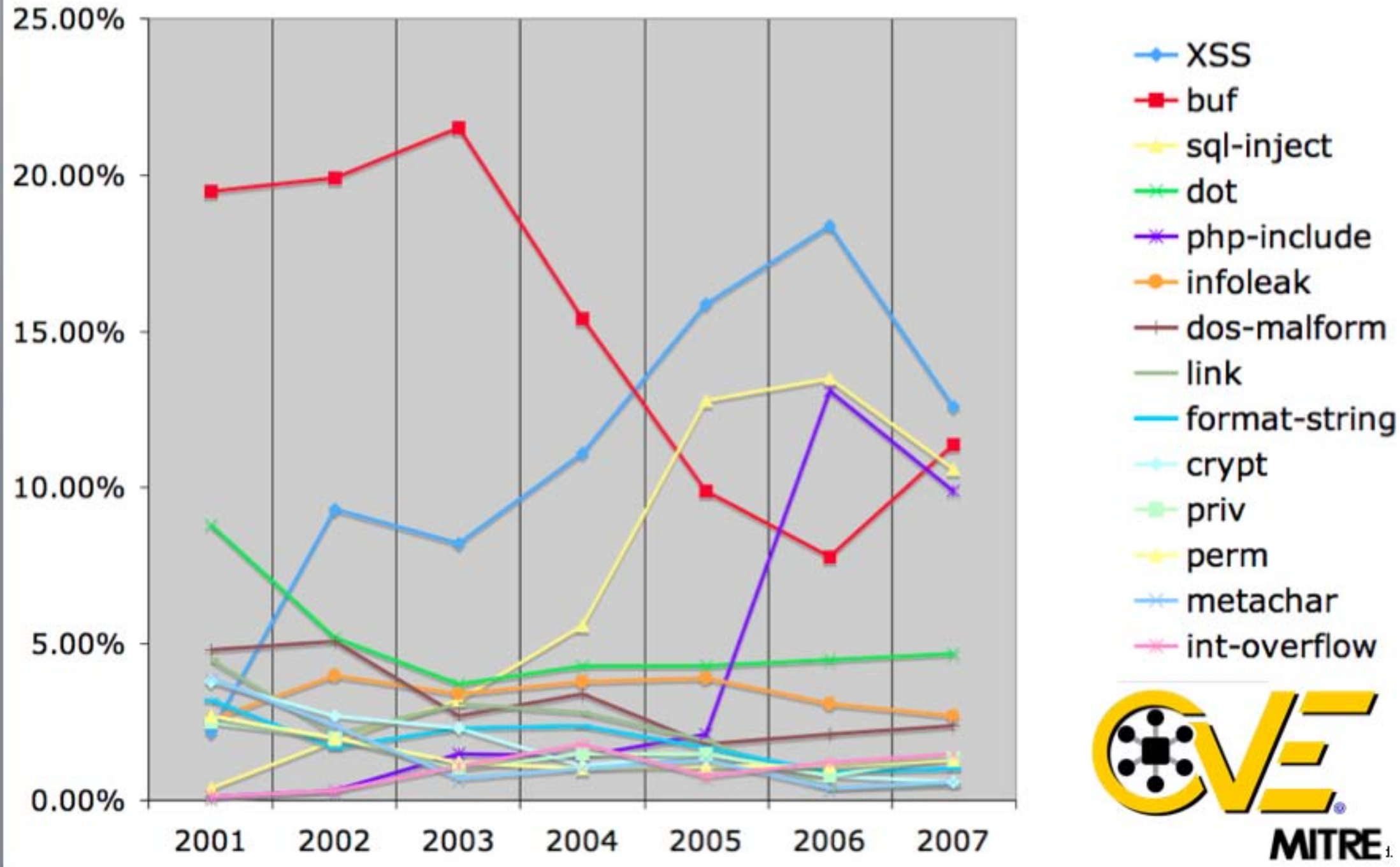
Scan Results

Enterprise IT Asset Management

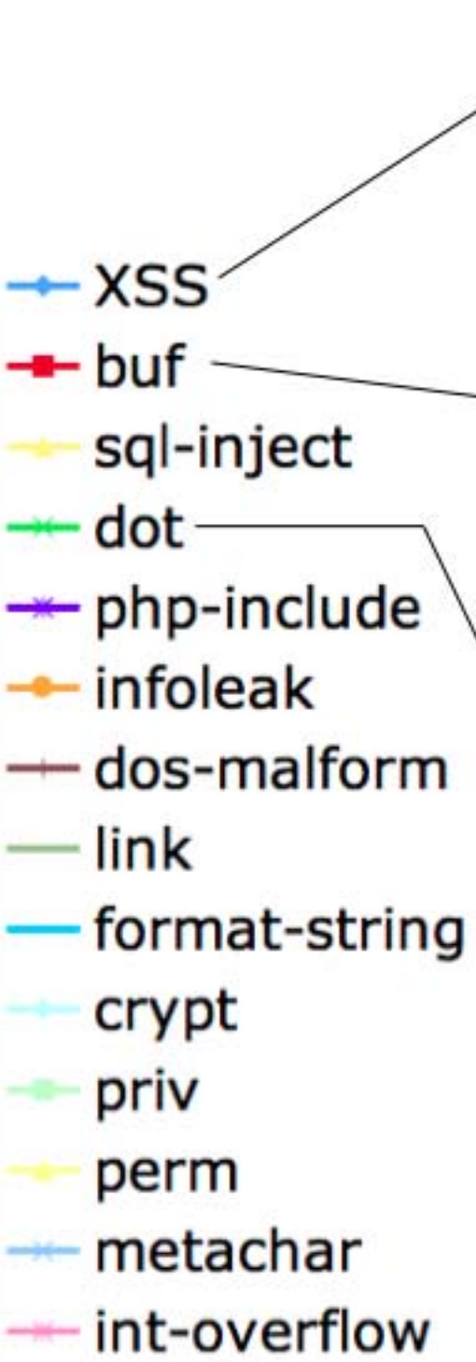
Enterprise IT Change Management

Centralized Reporting

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



Removing and Preventing the Vulnerabilities Requires More Specific Definitions…CWEs



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

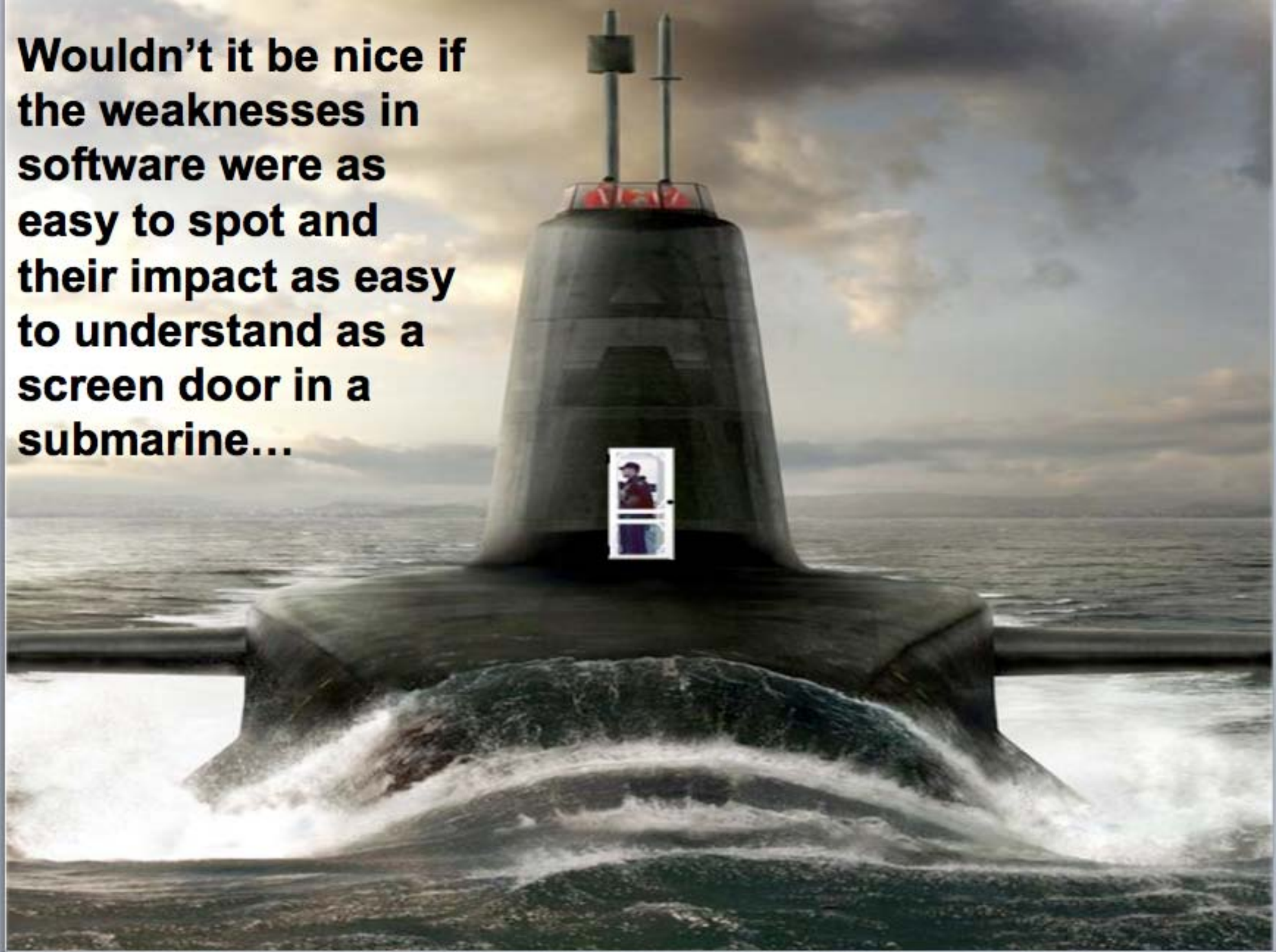
- Failure to Sanitize Script-Related HTML Tags in a Web Page (Basic XSS) (80)
- Failure to Sanitize Directives in an Error Message Web Page (81)
- Failure to Sanitize Script in Attributes of IMG Tags in a Web Page (82)
- Failure to Sanitize Script in Attributes in a Web Page (83)
- Failure to Resolve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

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

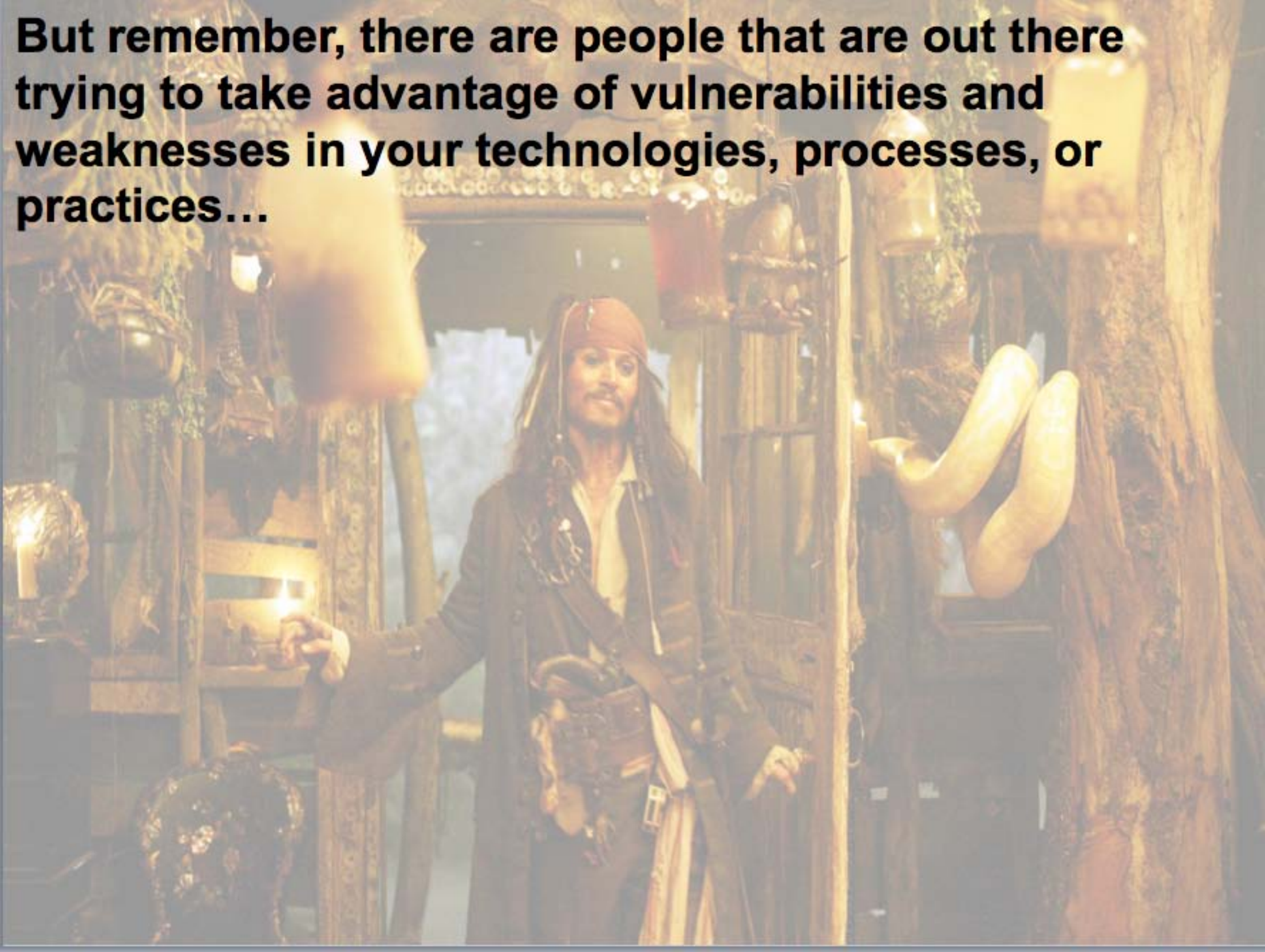
- Unbounded Transfer ('Classic Buffer Overflow') (120)
- Write-what-where Condition (123)
- Boundary Beginning Violation ('Buffer Underwrite') (124)
- Out-of-bounds Read (125)
- Wrap-around Error (128)
- Unchecked Array Indexing (129)
- Incorrect Calculation of Buffer Size (131)
- Miscalculated Null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

Path Traversal (22)

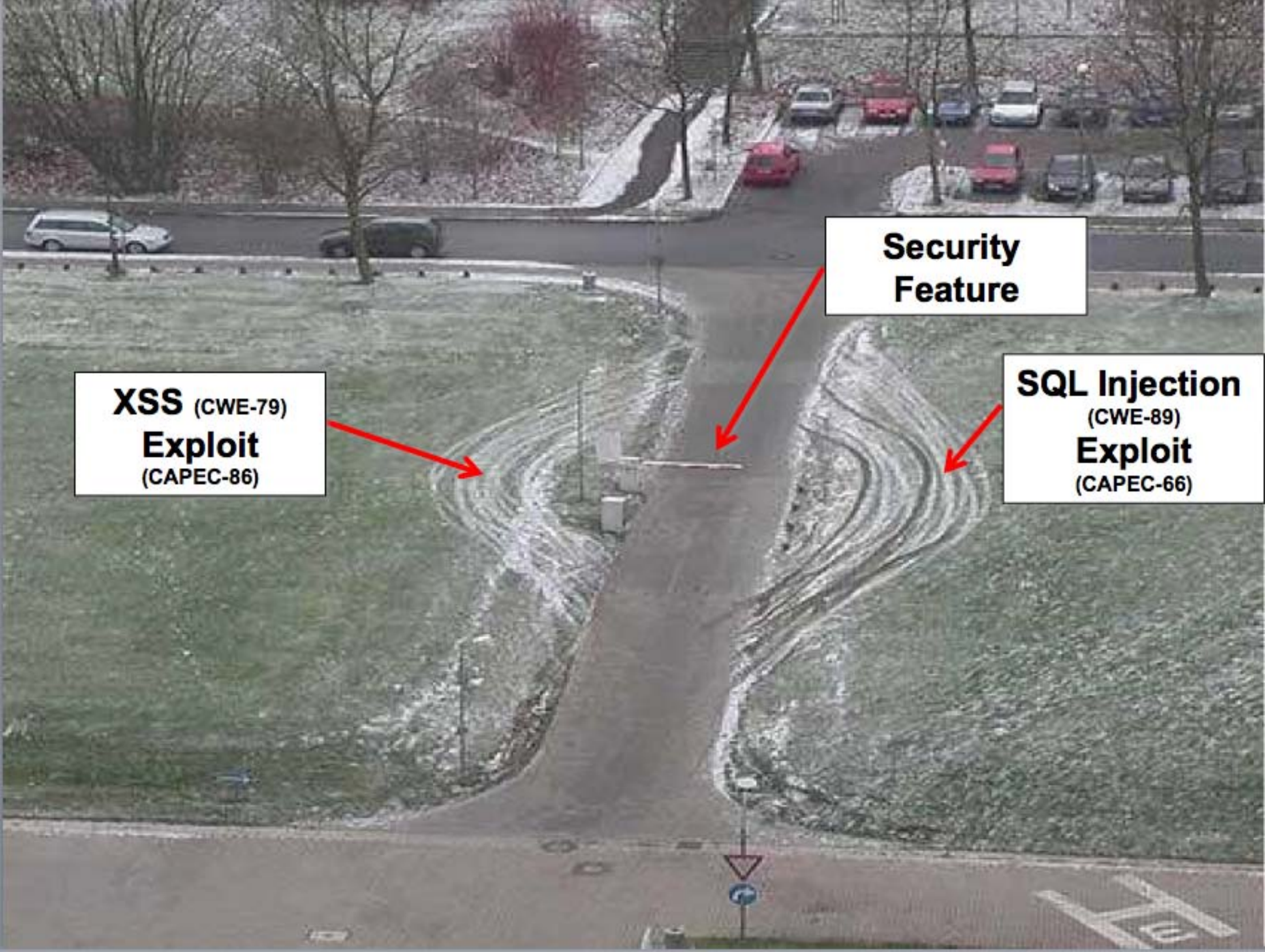
- Relative Path Traversal (23)
  - Path Traversal: '\..\filename' (29)
  - Path Traversal: '\dir\..\filename' (30)
  - Path Traversal: 'dir\..\filename' (31)
  - Path Traversal: '...' (Triple Dot) (32)
  - Path Traversal: '....' (Multiple Dot) (33)
  - Path Traversal: '..../' (34)
  - Path Traversal: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


Wouldn't it be nice if the weaknesses in software were as easy to spot and their impact as easy to understand as a screen door in a submarine…

But remember, there are people that are out there trying to take advantage of vulnerabilities and weaknesses in your technologies, processes, or practices…




…which we can respond to with defensive and offensive security capabilities.
712


Security Feature
XSS (CWE-79) Exploit (CAPEC-86)
SQL Injection (CWE-89) Exploit (CAPEC-66)

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

CWE and SANS Institute TOP 25 MOST DANGEROUS SOFTWARE ERRORS

2010 CWE/SANS Top 25 Most Dangerous Software Errors

http://cwe.mitre.org/top25/

Document version: 1.06 (pdf)

Date: September 27, 2010

Project Coordinators:

Bob Martin (MITRE)
Mason Brown (SANS)
Alan Paller (SANS)
Dennis Kirby (SANS)

Document Editor:

Steve Christey (MITRE)

Introduction

The 2010 CWE/SANS Top 25 Most Dangerous Software Errors is a list of the most widespread and critical programming errors that can lead to serious software vulnerabilities. They are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all.

The Top 25 list is a tool for education and awareness to help programmers to prevent the kinds of vulnerabilities that plague the software industry, by identifying and avoiding all-too-common mistakes that occur before software is even shipped. Software customers can use the same list to help them to ask for more secure software. Researchers in software security can use the Top 25 to

2 CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

Summary

Weakness Prevalence	High	Consequences	Data loss, Security bypass
Remediation Cost	Low	Ease of Detection	Easy
Attack Frequency	Often	Attacker Awareness	High

Discussion

These days, it seems as if software is all about the data: getting it into the database, pulling it from the database, massaging it into information, and sending it elsewhere for fun and profit. If attackers can influence the SQL that you use to communicate with your database, then suddenly all your fun and profit belongs to them. If you use SQL queries in security controls such as authentication, attackers could alter the logic of those queries to bypass security. They could modify the queries to steal, corrupt, or otherwise change your underlying data. They'll even steal data one byte at a time if they have to, and they have the patience and know-how to do so.

Technical Details | *Code Examples* | *Detection Methods* | *References*

Prevention and Mitigations

Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
For example, consider using persistence layers such as Hibernate or Enterprise Java Beans, which can provide significant protection against SQL injection if used properly.

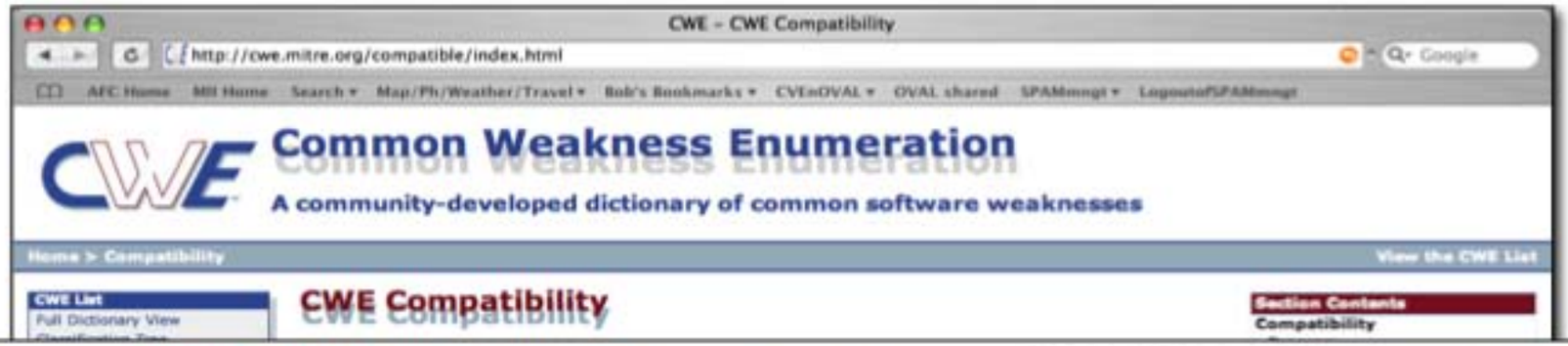
Architecture and Design
If available, use structured mechanisms that automatically enforce the separation between data and code. These mechanisms may be able to provide the relevant quoting, encoding, and validation automatically, instead of relying on the developer to provide this capability at every point where output is generated.
Process SQL queries using prepared statements, parameterized queries, or stored procedures. These features should accept parameters or variables and support strong typing. Do not dynamically construct and execute query strings within these features using "exec" or similar functionality, since you may


CAPEC - CAPEC-66: SQL Injection (Release 1.5)
http://capec.mitre.org/data/definitions/66.html
Google
CAPEC
Common Attack Pattern Enumeration and Classification
A Community Knowledge Resource for Building Secure Software
Home > CAPEC List > CAPEC-66: SQL Injection (Release 1.5)
Search by ID:
Go
CAPEC List
Full CAPEC Dictionary
Methods of Attack View
Reports
About CAPEC
Documents
Resources
Community
Related Activities
Collaboration List
News & Events
Calendar
Free Newsletter
Contact Us
Search the Site
CAPEC-66: SQL Injection
SQL Injection
Attack Pattern ID: 66 (Standard
Typical Severity: High
Status: Draft
Description
Summary
This attack exploits target so
An attacker crafts input strin
statements based on the inp
those the application intende
SQL Injection results from fa
specially crafted user-contro
validation as part of SQL que
ways not envisaged during a
design of the application, it
database execute system-re
enables an attacker to talk d
completely. Sucessful injecti
or modify data in the databa
information from a database
Attack Execution Flow
Explore
1. Survey application:
The attacker first takes an in
Attack Step Techniques
ID
Attack Step Techni
1
Spider web sites for all
Done
CAPEC - CAPEC-7: Blind SQL Injection (Release 1.5)
http://capec.mitre.org/data/definitions/7.html
Google
CAPEC
Common Attack Pattern Enumeration and Classification
A Community Knowledge Resource for Building Secure Software
Home > CAPEC List > CAPEC-7: Blind SQL Injection (Release 1.5)
Search by ID:
Go
CAPEC List
Full CAPEC Dictionary
Methods of Attack View
Reports
About CAPEC
Documents
Resources
Community
Related Activities
Collaboration List
News & Events
Calendar
Free Newsletter
Contact Us
Search the Site
CAPEC-7: Blind SQL Injection
Blind SQL Injection
Attack Pattern ID: 7 (Detailed Attack Pattern
Completeness: Complete)
Typical Severity: High
Status: Draft
Description
Summary
Blind SQL Injection results from an insufficient mitigation for SQL Injection. Although suppressing database error messages are considered best practice, the suppression alone is not sufficient to prevent SQL Injection. Blind SQL Injection is a form of SQL Injection that overcomes the lack of error messages. Without the error messages that facilitate SQL Injection, the attacker constructs input strings that probe the target through simple Boolean SQL expressions. The attacker can determine if the syntax and structure of the injection was successful based on whether the query was executed or not. Applied iteratively, the attacker determines how and where the target is vulnerable to SQL Injection.
For example, an attacker may try entering something like "username' AND 1=1; --" in an input field. If the result is the same as when the attacker entered "username" in the field, then the attacker knows that the application is vulnerable to SQL Injection. The attacker can then ask yes/no questions from the database server to extract information from it. For example, the attacker can extract table names from a database using the following types of queries:
"username' AND ascii(lower(substring((SELECT TOP 1 name FROM sysobjects WHERE xtype='U'), 1, 1))) > 108".
If the above query executes properly, then the attacker knows that the first character in a table name in the database is a letter between m and z. If it doesn't, then the attacker knows that the character must be between a and l (assuming of course that table names only contain alphabetic characters). By performing a binary search on all character positions, the attacker can determine all table names in the database. Subsequently, the attacker may execute an actual attack and send something like:
"username'; DROP TABLE trades; --
Attack Execution Flow
Explore
1. Hypothesize SQL queries in application:
Generated hypotheses regarding the SQL queries in an application. For example, the attacker may hypothesize that his input is passed directly into a query that looks like:
"SELECT * FROM orders WHERE ordernum = _____"
or
"SELECT * FROM orders WHERE ordernum IN (_____)"
Done


Google Earth
ファイル(F) 編集(E) 表示(V) ツール(T) 追加(A) ヘルプ(H)
Severity
Emergency
Critical
Warning
SQL Injection Probe Detected.
SQL Injection Detected
Image IBCAO
Image © 2010 TerraMetrics
Image USDA Farm Service Agency
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
©2010 Google

CWE Compatibility & Effectiveness Program

(launched Feb 2007)



SECURITY DATABASE
KEEP A VIGILANT EYE ON YOUR DEFENSES
KDM Analytics
VERACODE
FORTIFY SOFTWARE
armorize technologies
Secure Your Web Code
SecurityReason
Our Reason is Security
SkillBridge
coverity
Klocwork
PARASOFT
EMC²
CODENOMICON
defensics
CENZIC
GRAMMATECH
symantec
SANS
(ISC)²
CERIAS
IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
SofCheck
IBM
watchfire
checkmarx
OUNCE LABS
PRQA
Programming Research
CAST
LDRA
Software Technology
cigital
hp
SPI DYNAMICS

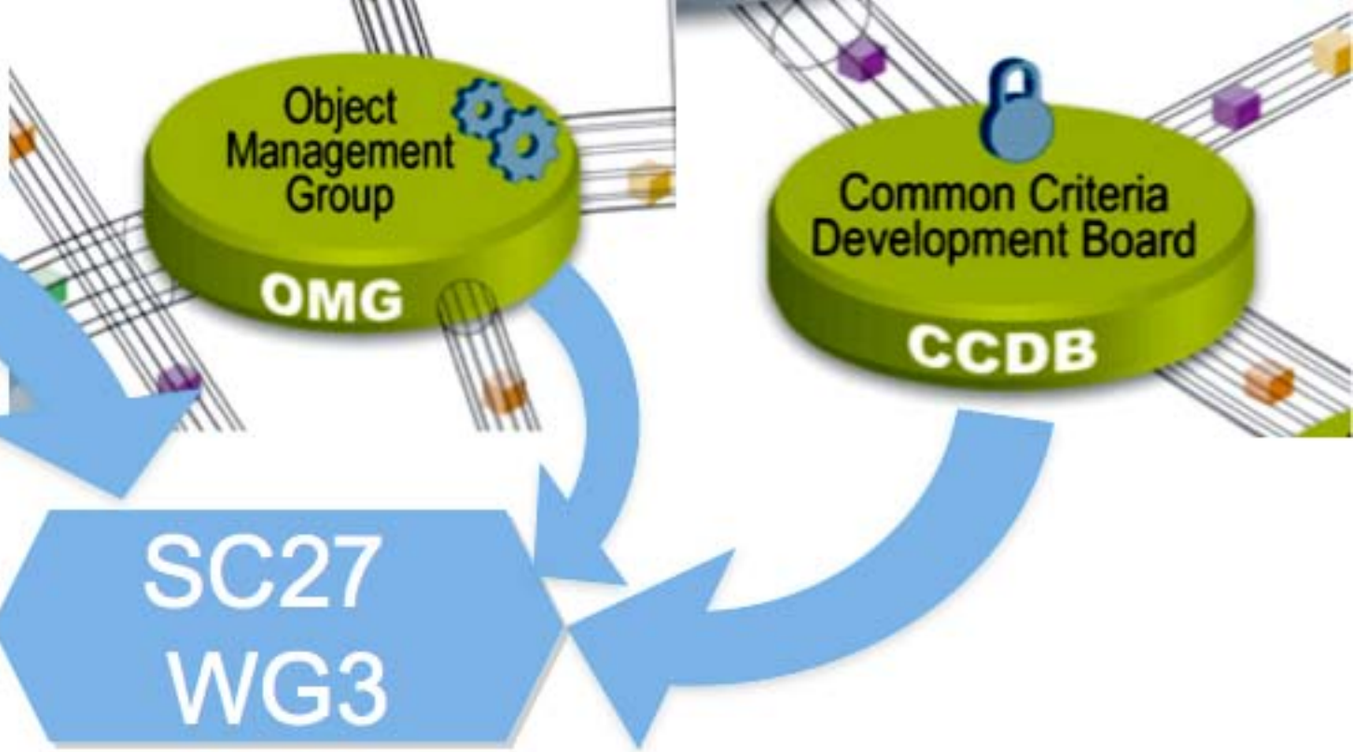
Organizations Participating

cwe.mitre.org/compatible/

All organizations participating in the CWE Compatibility and Effectiveness Program are listed below, including those with CWE-Compatible Products and Services and those with Declarations to Be CWE-Compatible.

TOTALS
Organizations Participating: 29
Products & Services: 48

Products are listed alphabetically by organization name:



SC27 WG3

ISO IEC

ISO/IEC JTC 1/SC 27 **NXXXX**

ISO/IEC JTC 1/SC 27/WG x **NXXXXX**

REPLACES: N

ISO/IEC JTC 1/SC 27

Information technology - Security techniques

Secretariat: DIN, Germany

DOC TYPE:	NB NWI Proposal for a technical report (TR)
TITLE:	National Body New Work Item Proposal on "Secure software development and evaluation under ISO/IEC 15408 and ISO/IEC 18405"
SOURCE:	INCITS/CS1, National Body of (US)
DATE:	2009-09-30
PROJECT:	15408 and 18405
STATUS:	This document is circulated for consideration at the forthcoming meeting of SC 27/WG 3 to be held in Redmond (WA, USA) on 2nd - 6th November 2009.
ACTION ID:	ACT
DUE DATE:	
DISTRIBUTION:	P-, O- and L-Members W. Fumy, SC 27 Chairman M. De Soete, SC 27 Vice-Chair E. J. Humphreys, K. Naemura, M. Bañón, M.-C. Kang, K. Rannenberg, WG-Convenors
MEDIUM:	Livelink-server
NO. OF PAGES:	xx

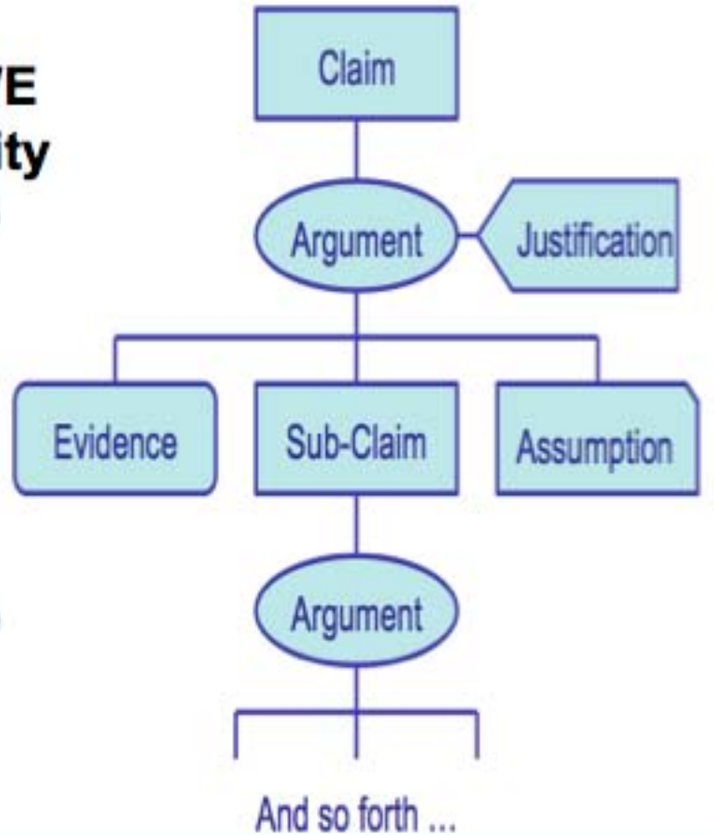
Secretariat ISO/IEC JTC 1/SC 27 –
DIN Deutsches Institut für Normung e. V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-mail: krystyna.passia@din.de
HTTP://www.jtc1sc27.din.de/en

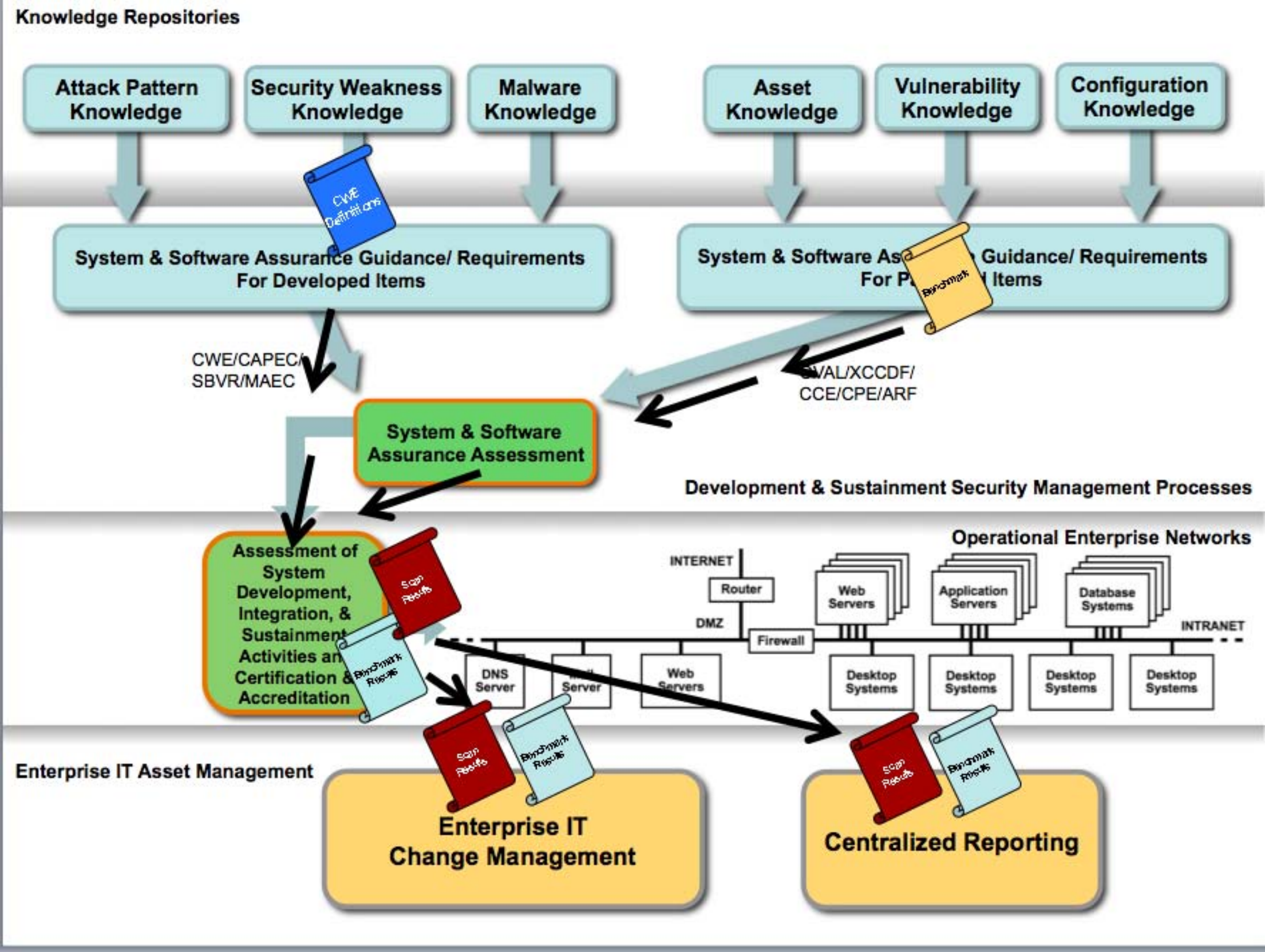
Common Criteria v4 CCDB

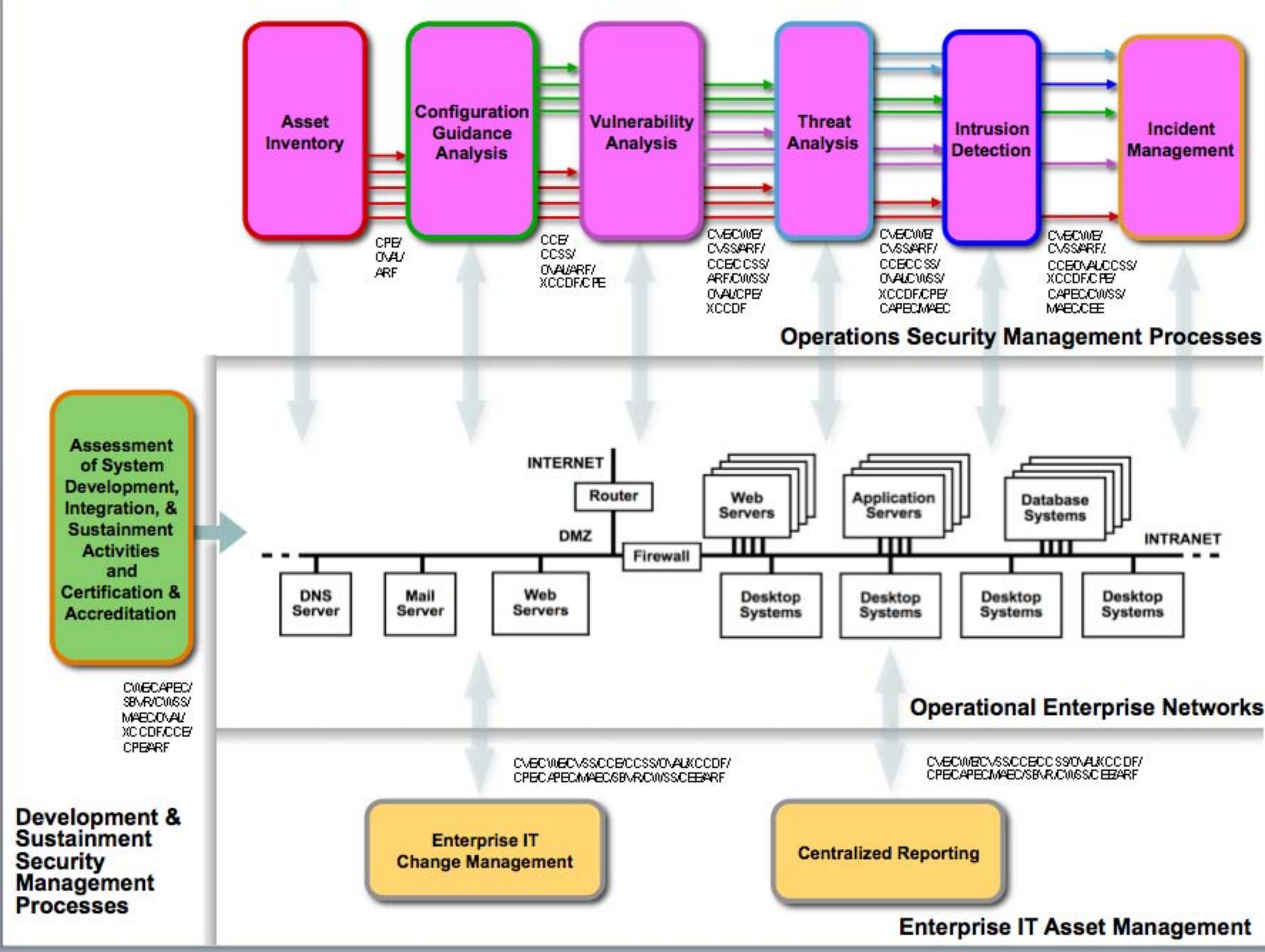
- **TOE to leverage CAPEC & CWE**
- **"Refining Software Vulnerability Analysis Under ISO/IEC 15408 and ISO/IEC 18045"**
- **Also investigating how to leverage ISO/IEC 15026 and OMG's Structured Assurance Case Metamodel**

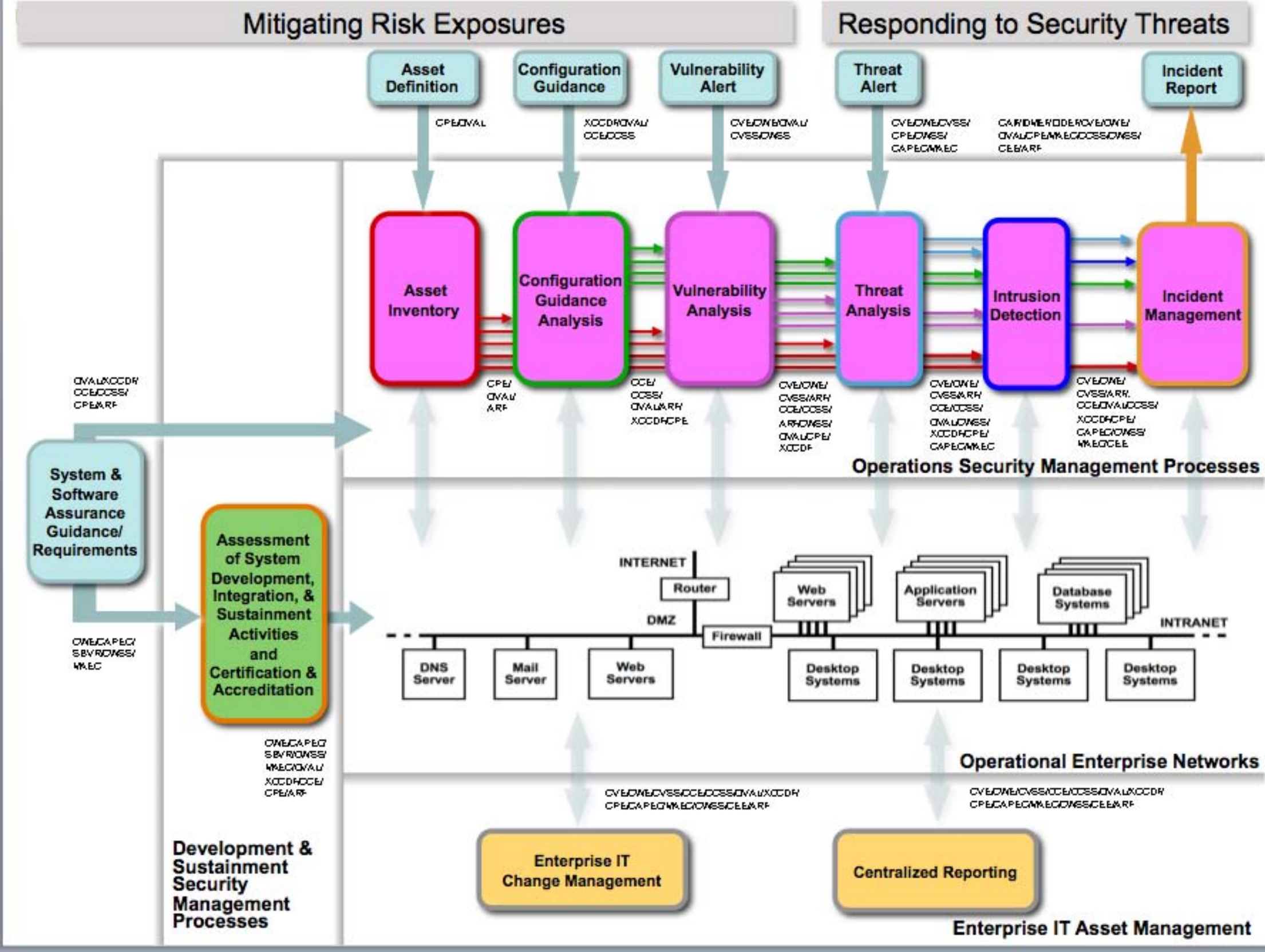
NIAP (U.S.) Evaluation Scheme

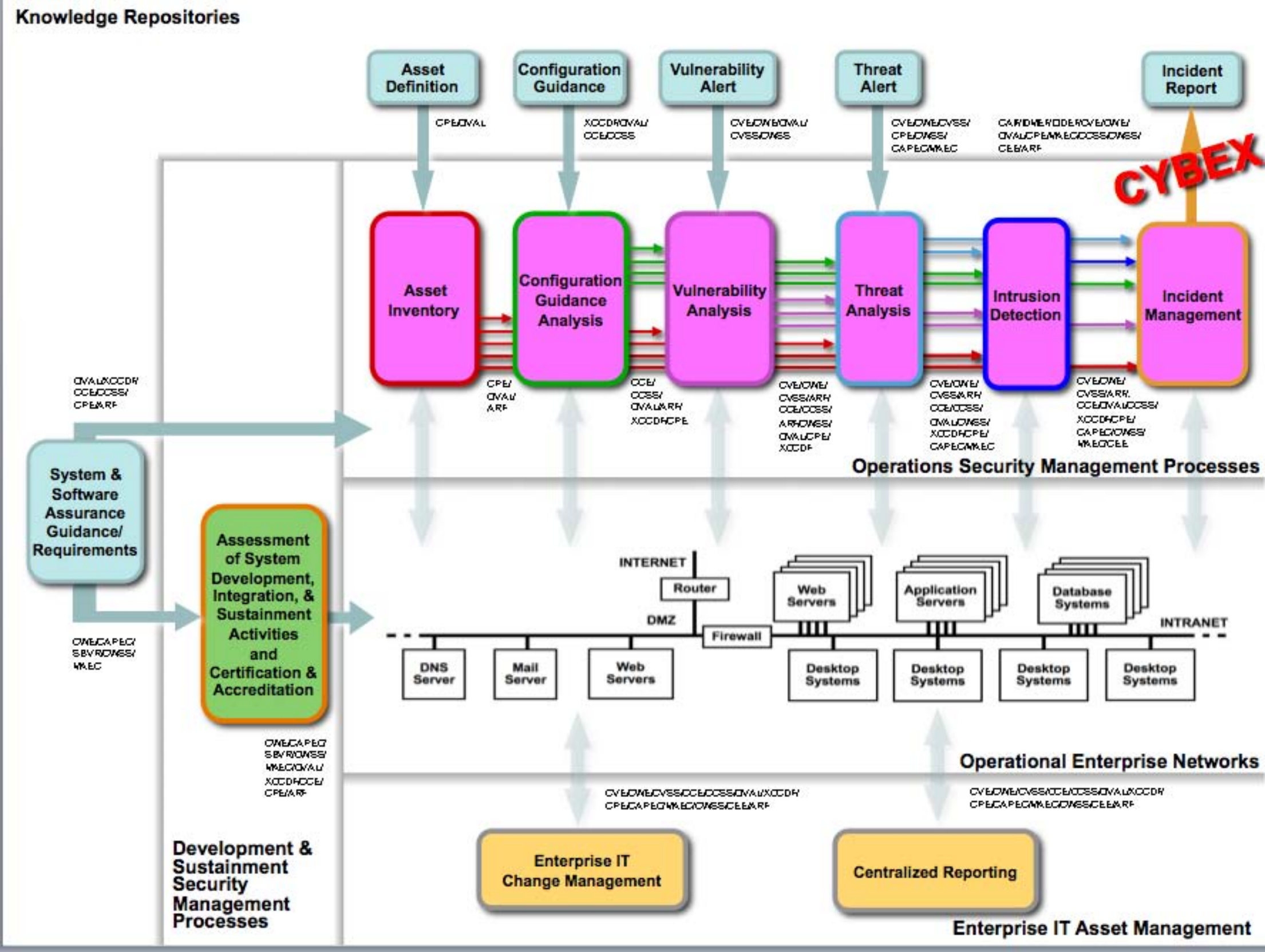
- **Above plus**
- **Also investigating how to leverage SCAP**



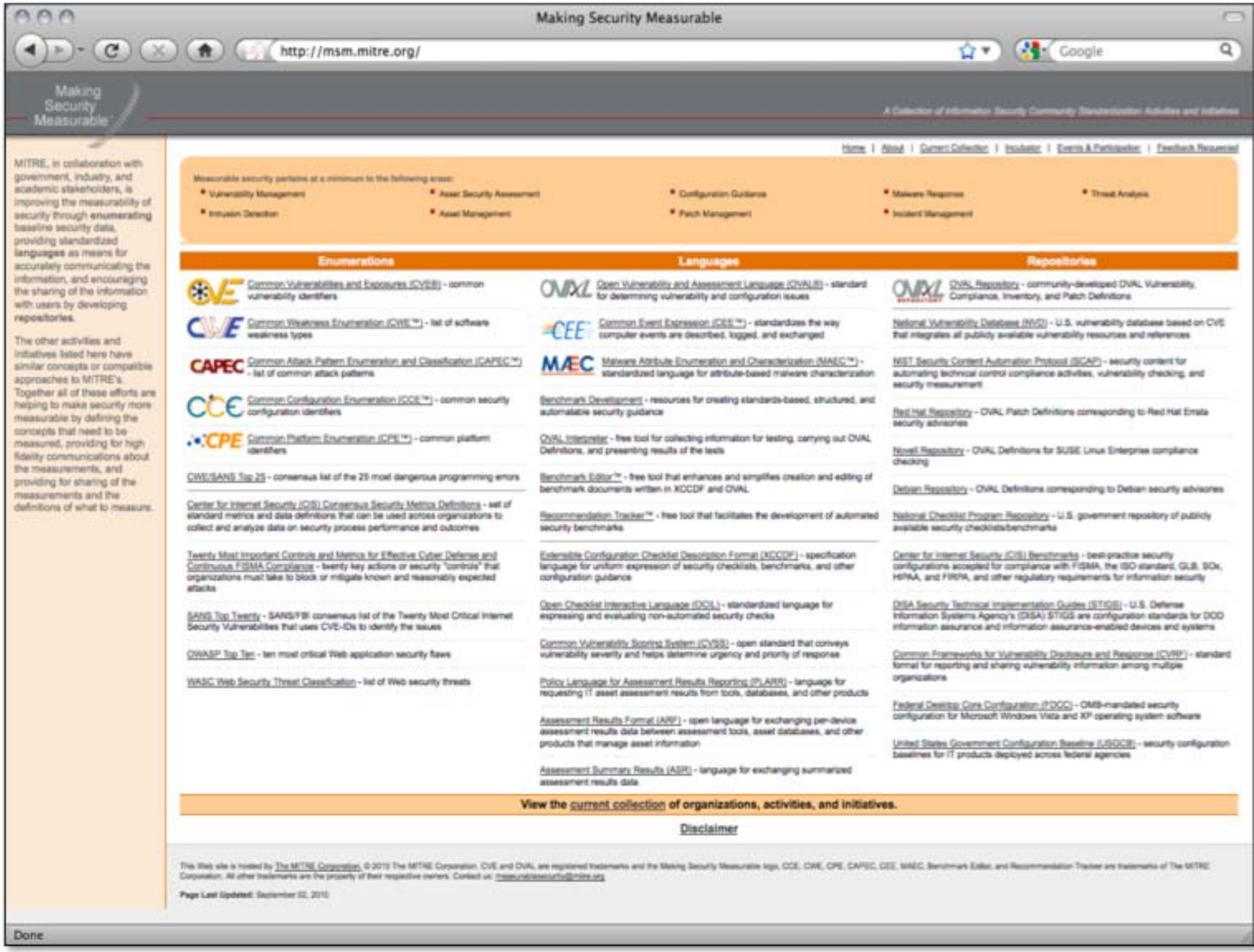

Knowledge Repositories
Attack Pattern Knowledge
Security Weakness Knowledge
Malware Knowledge
Asset Knowledge
Vulnerability Knowledge
Configuration Knowledge
CWE Definitions
System & Software Assurance Guidance/ Requirements For Developed Items
System & Software As Guidance/ Requirements For P Items
Benchmark
CWE/CAPEC/ SBVR/MAEC
VAL/XCCDF/ CCE/CPE/ARF
System & Software Assurance Assessment
Development & Sustainment Security Management Processes
Assessment of System Development, Integration, & Sustainment Activities an Certification & Accreditation
SCAP Results
Benchmark Results
Operational Enterprise Networks
INTERNET
Router
DMZ
Firewall
Web Servers
Application Servers
Database Systems
INTRANET
DNS Server
Web Server
Web Servers
Desktop Systems
Desktop Systems
Desktop Systems
Desktop Systems
Enterprise IT Asset Management
Enterprise IT Change Management
Centralized Reporting


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
CWE/CAPEC/ SBVR/CWSS/ MAEC/OVAL/ XCCDF/CCE/ CPE/ARF
INTERNET
Router
DMZ
Firewall
Web Servers
Application Servers
Database Systems
INTRANET
DNS Server
Mail Server
Web Servers
Desktop Systems
Desktop Systems
Desktop Systems
Desktop Systems
Operational Enterprise Networks
CVE/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
Development & Sustainment Security Management Processes
Enterprise IT Change Management
Centralized Reporting
Enterprise IT Asset Management


Mitigating Risk Exposures
Responding to Security Threats
Asset Definition
Configuration Guidance
Vulnerability Alert
Threat Alert
Incident Report
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
Operations Security Management Processes
System & Software Assurance Guidance/ Requirements
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
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
Operational Enterprise Networks
Development & Sustainment Security Management Processes
Enterprise IT Change Management
Centralized Reporting
Enterprise IT Asset Management


Knowledge Repositories
Asset Definition
Configuration Guidance
Vulnerability Alert
Threat Alert
Incident Report
CYBEX
Asset Inventory
Configuration Guidance Analysis
Vulnerability Analysis
Threat Analysis
Intrusion Detection
Incident Management
Operations Security Management Processes
System & Software Assurance Guidance/ Requirements
Assessment of System Development, Integration, & Sustainment Activities and Certification & Accreditation
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
Operational Enterprise Networks
Development & Sustainment Security Management Processes
Enterprise IT Change Management
Centralized Reporting
Enterprise IT Asset Management

[makingsecuritymeasurable.mitre.org]



Making Security Measurable™


Questions?
ramartin@mitre.org