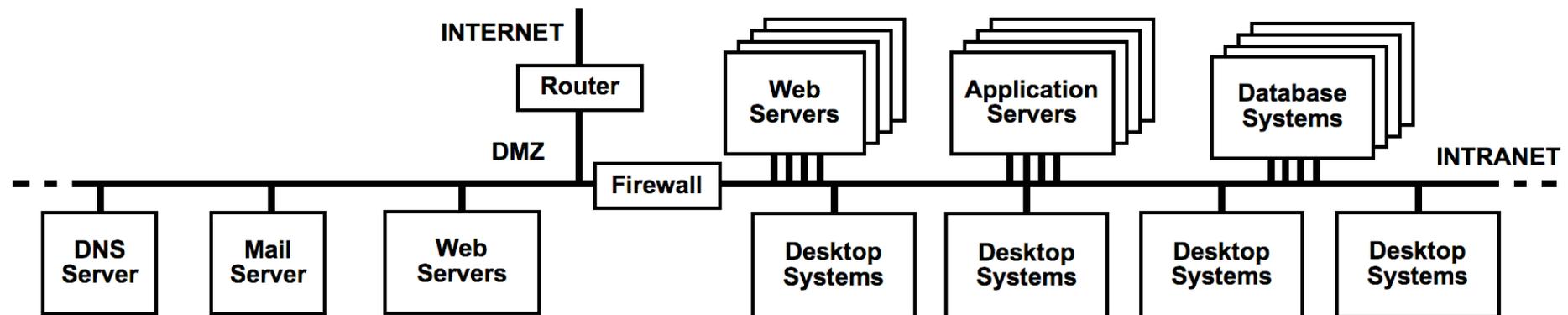


Cyber/Assurance Ecosystem

Automation Activities for Securing the Enterprise

Robert A. Martin
30 September 2010

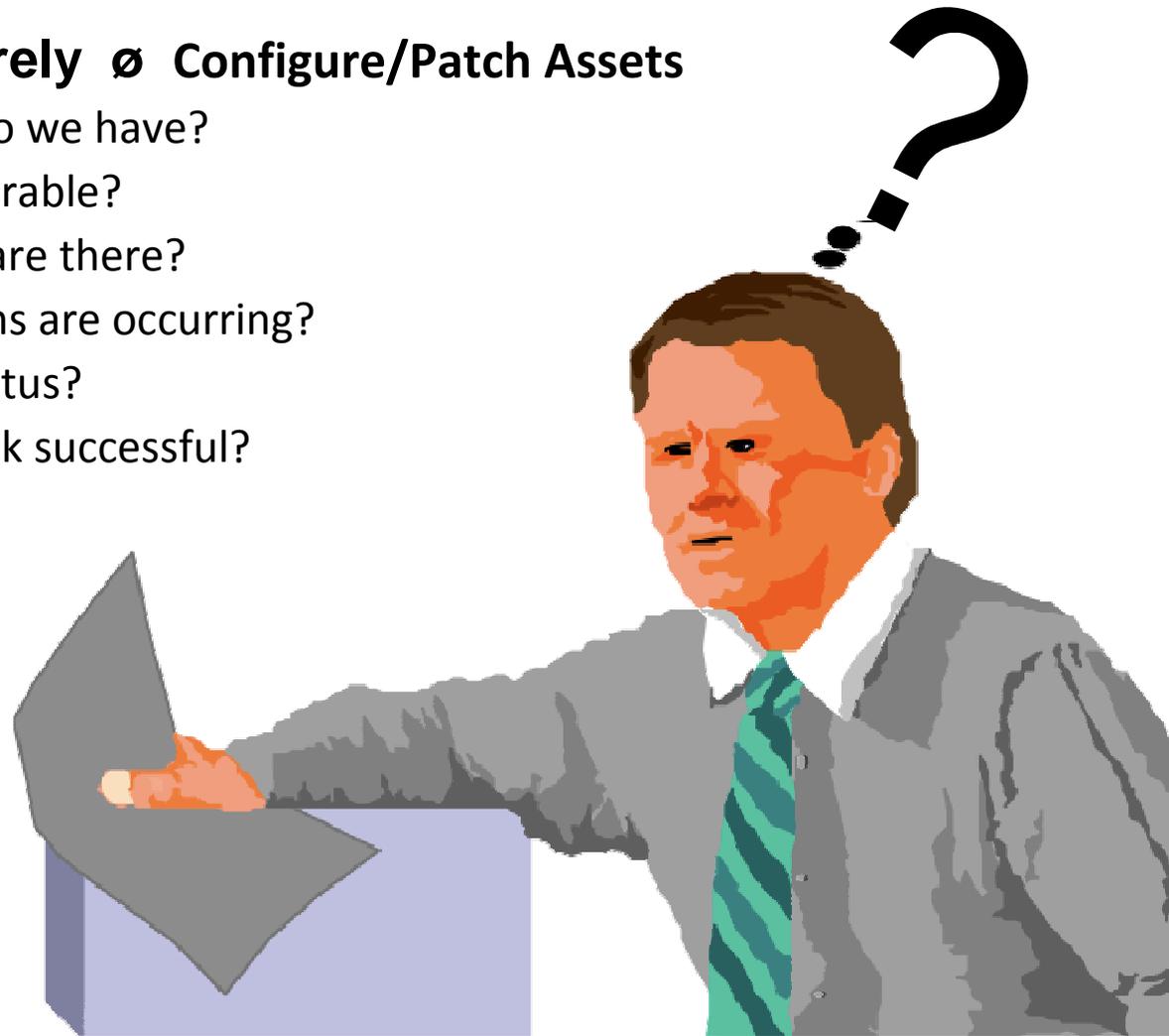
A Notional Enterprise Information Technology Infrastructure



Securing the Enterprise...

■ Operate Securely ∅ Configure/Patch Assets

- What assets do we have?
- Are they vulnerable?
- What threats are there?
- What intrusions are occurring?
- What's our status?
- Was that attack successful?
- •
- •
- •



Cognitive and Cyber Speed Activities & Info (SCAP)

- **CVE identifiers require analysts to investigate/correlate...**
 - Which enables tools to correlate at cyber speed...
- **OVAL definitions require analysts to define criteria...**
 - Which enables checking systems for user defined content at cyber speed...
- **CVSS scores require analysts to assign vector values...**
 - Which enables identifying severity and following a priori guidance on risk tolerance at cyber speed...
- **CPE names require vendors/analysts to assign names...**
 - Which allows correlating platform information at cyber speed...
- **CCE identifiers require analysts/vendors to identify controls...**
 - Which allows correlating settings with desired settings at cyber speed...
- **XCCDF requires analysts to craft policy statements...**
 - Which allows multiple tools to follow and report against user defined content at cyber speed...
- **OCIL requires analysts to craft questionnaires...**
 - Which allows multiple tools to ask and report against user defined content at cyber speed...

SCAP's Automation Requires:

- Consistent input from Cognitive activities feeding SCAP
- Structured input & output to and from those Cognitive activities
- Universal definition of concepts across SCAP elements

Cognitive Speed



Content/Guidance Writing



Enumeration Assignment

Cyber Speed



Cognitive Speed



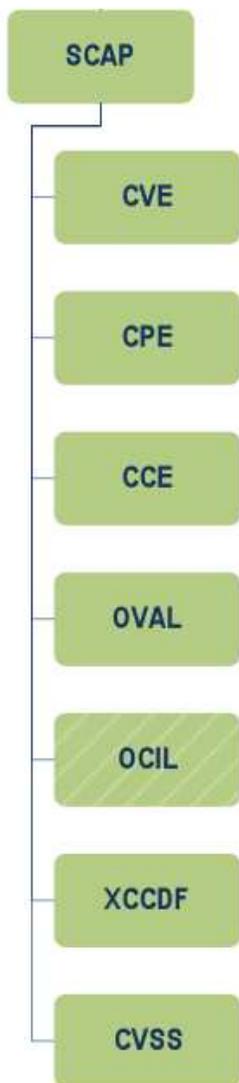
Enterprise Security Management

Cognitive Speed Activities & Info



Cyber Speed Activities & Info





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 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)**

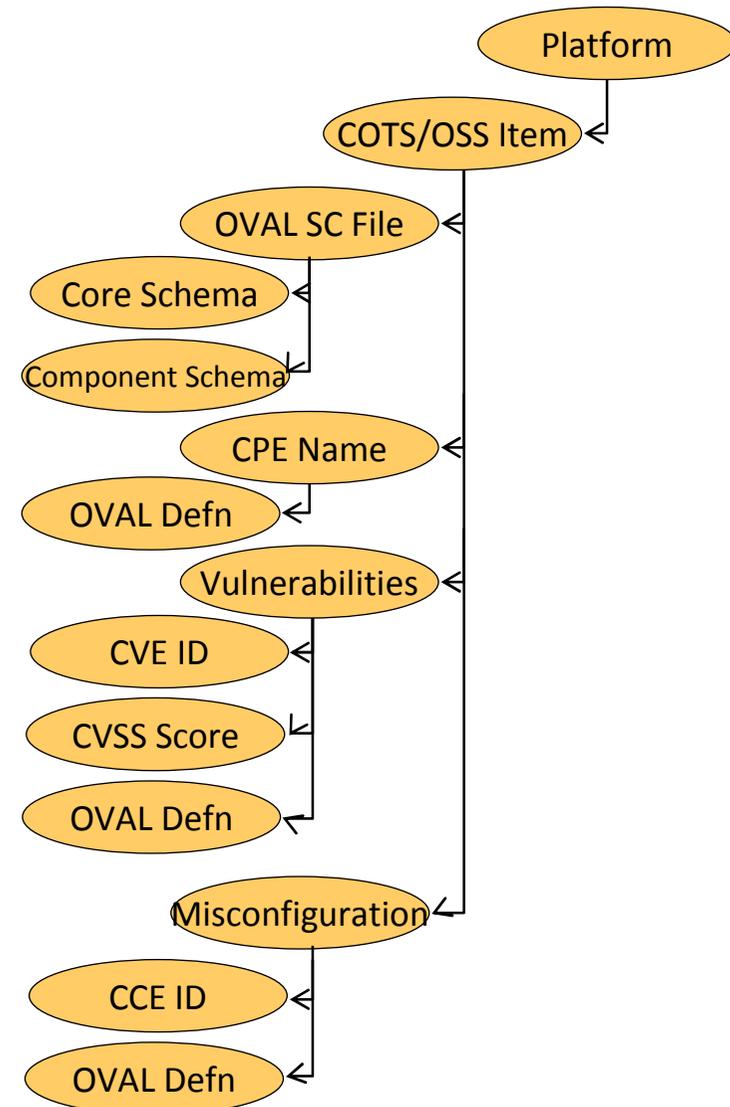
Recommendations of the National Institute
of Standards and Technology

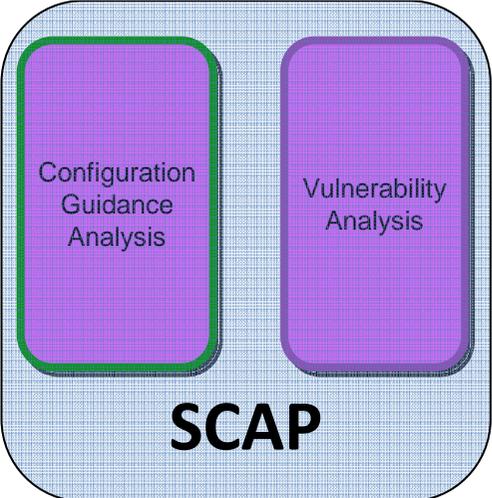
Stephen Quinn
David Waltermire
Christopher Johnson
Karen Scarfone
John Banghart

SCAP and the model beneath it...

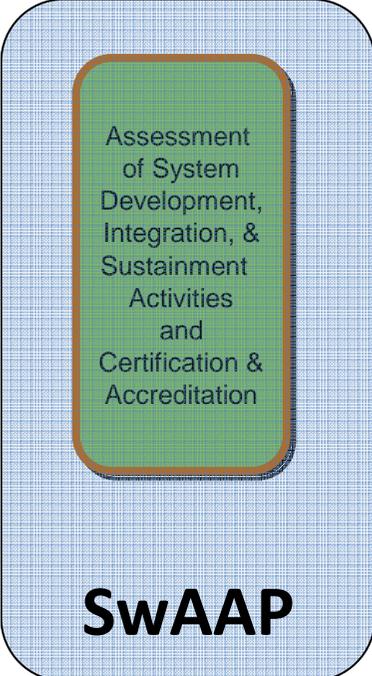
■ A platform:

- Commercial or Open Source Software
 - OVAL Systems Characteristics File
 - Core Schema
 - Component Schema
 - CPE names
 - Vulnerabilities
 - CVE identifiers
 - CVSS scores
 - OVAL definitions
 - Misconfigurations
 - CCE identifiers
 - OVAL definitions





Operations Security Management Processes



Development &
Sustainment
Security
Management
Processes

Software Assurance Automation Protocol (SwAAP)

CWE

CAPEC

MAEC

CWSS

OMG SAEM

OMG ARG

SAFES

"Food Label"

OMG SMM

ISO 15026

OMG KDM

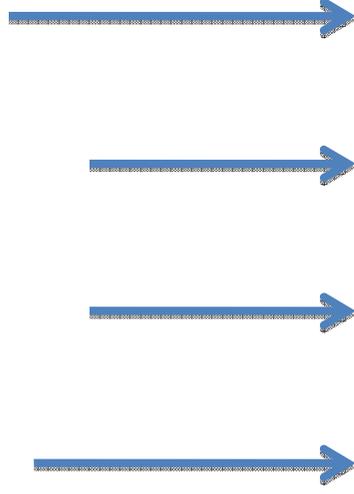
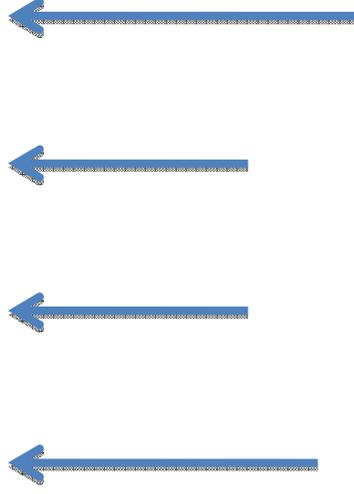
OMG ASTM

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

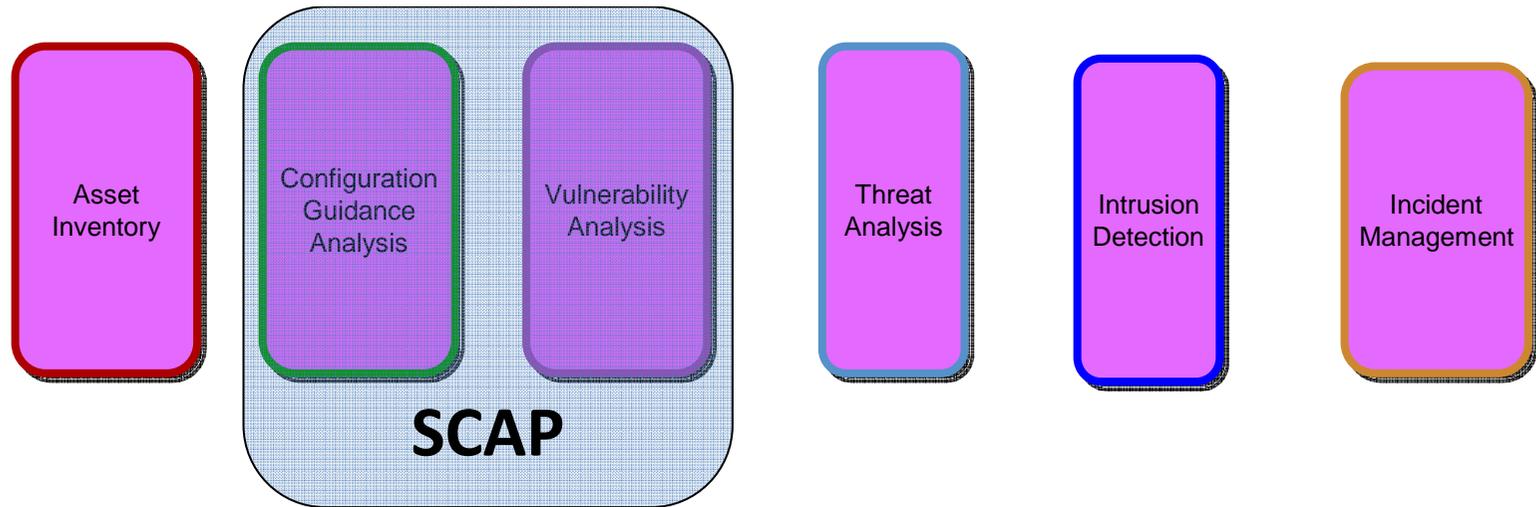
- Common Weakness Enumeration (CWE)
- Common Attack Pattern Enumeration & Classification (CAPEC)
- Malware Attribute Enumeration & Characterization (MAEC)
- Common Weakness Scoring System (CWSS)
- OMG Software Assurance Evidence Metamodel (OMG SAEM)
- OMG Argumentation Metamodel (OMG ARG)
- OMG Structured Assurance Case Metamodel (OMG SACM)
- Software Assurance Findings Expression Schema (SAFES)
- NIST SAMATE's "Software 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?

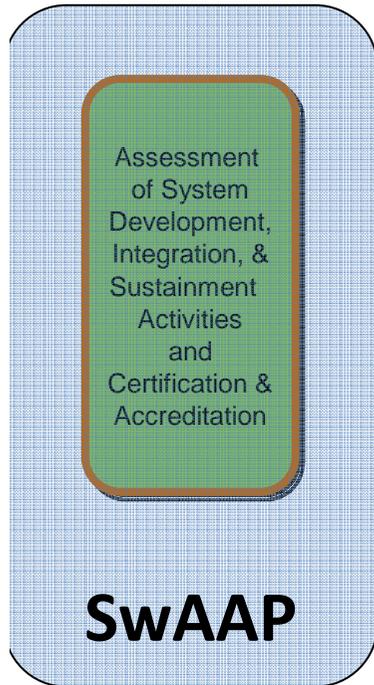
Cognitive Speed Activities & Info



Cyber Speed Activities & Info



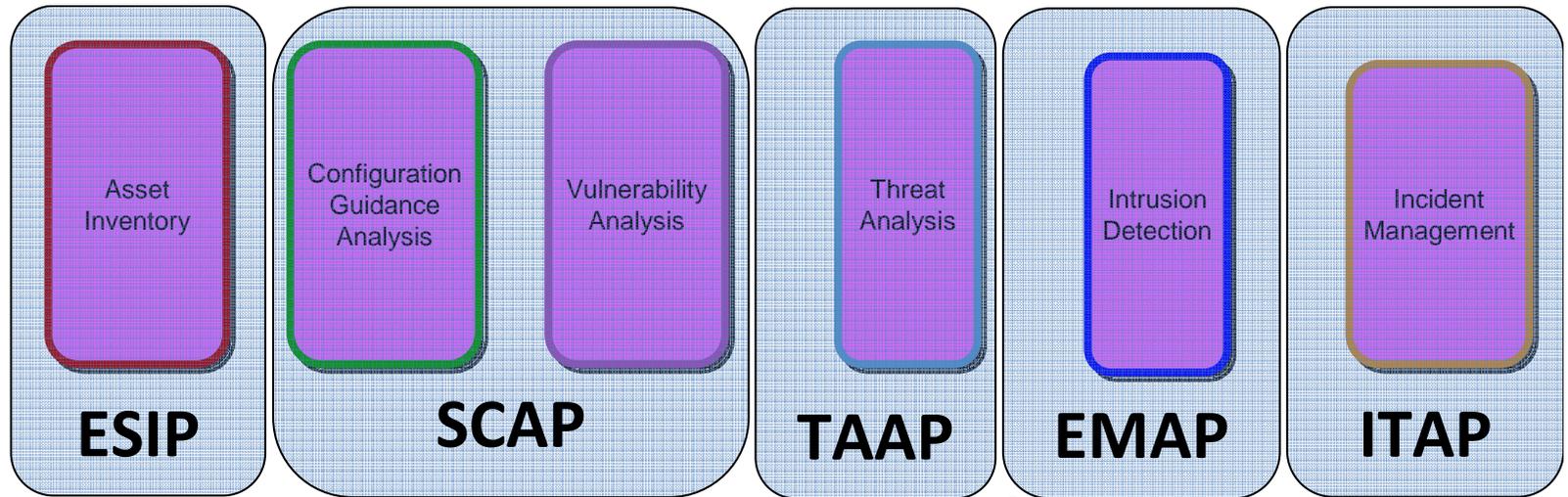
Operations Security Management Processes



Development & Sustainment Security Management Processes



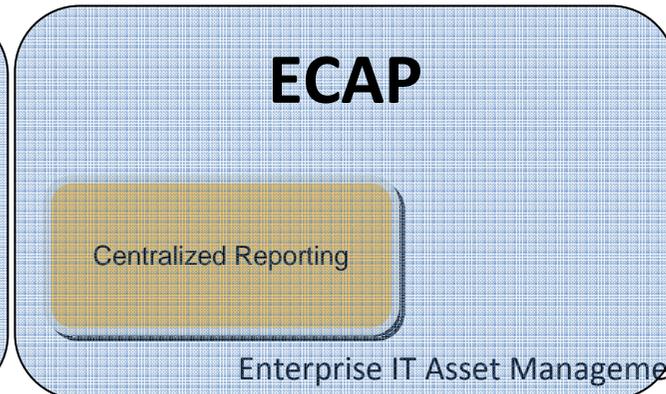
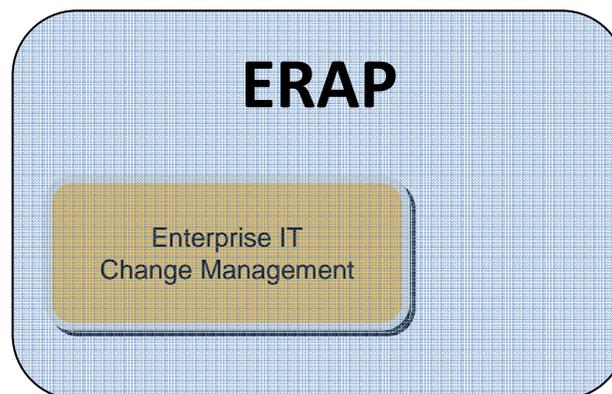
Enterprise IT Asset Management



Operations Security Management Processes



Development & Sustainment Security Management Processes



Enterprise IT Asset Management

“Other” Automation Protocols (“O”AP)



■ Event Management Automation Protocol (EMAP)

- For reporting of security events. Common Event Expression (CEE), Malware Attribute Enumeration & Characterization (MAEC), and Common Attack Pattern Enumeration & Classification (CAPEC).

■ Enterprise Remediation Automation Protocol (ERAP)

- For automated remediation of mis-configuration & missing patches. Common Remediation Enumeration (CRE), Extended Remediation Information (ERI), Open Vulnerability and Assessment Language (OVAL), Common Platform Enumeration (CPE), and Common Configuration Enumeration (CCE).

■ Enterprise Compliance Automation Protocol (ECAP)

- For reporting configuration compliance. Asset Reporting Format (ARF), Open Checklist Reporting Language (OCRL), etc.

■ Enterprise System Information Protocol (ESIP)

- For reporting of asset inventory information. Common Platform Enumeration (CPE), etc.

“Other” Automation Protocols (“O”AP)



■ Incident Tracking and Assessment Protocol (ITAP)

- For tracking, reporting, managing and sharing incident information. Open Vulnerability and Assessment Language (OVAL), Common Platform Enumeration (CPE), Common Configuration Enumeration (CCE), Common Vulnerabilities and Exposures (CVE), Common Vulnerability Scoring System (CVSS), Malware Attribute Enumeration & Characterization (MAEC), Common Attack Pattern Enumeration & Classification (CAPEC), Common Weakness Enumeration (CWE), Common Event Expression (CEE), Incident Object Description Exchange Format (IODEF), National Information Exchange Model (NIEM), and Cybersecurity Information Exchange Format (CYBEX).

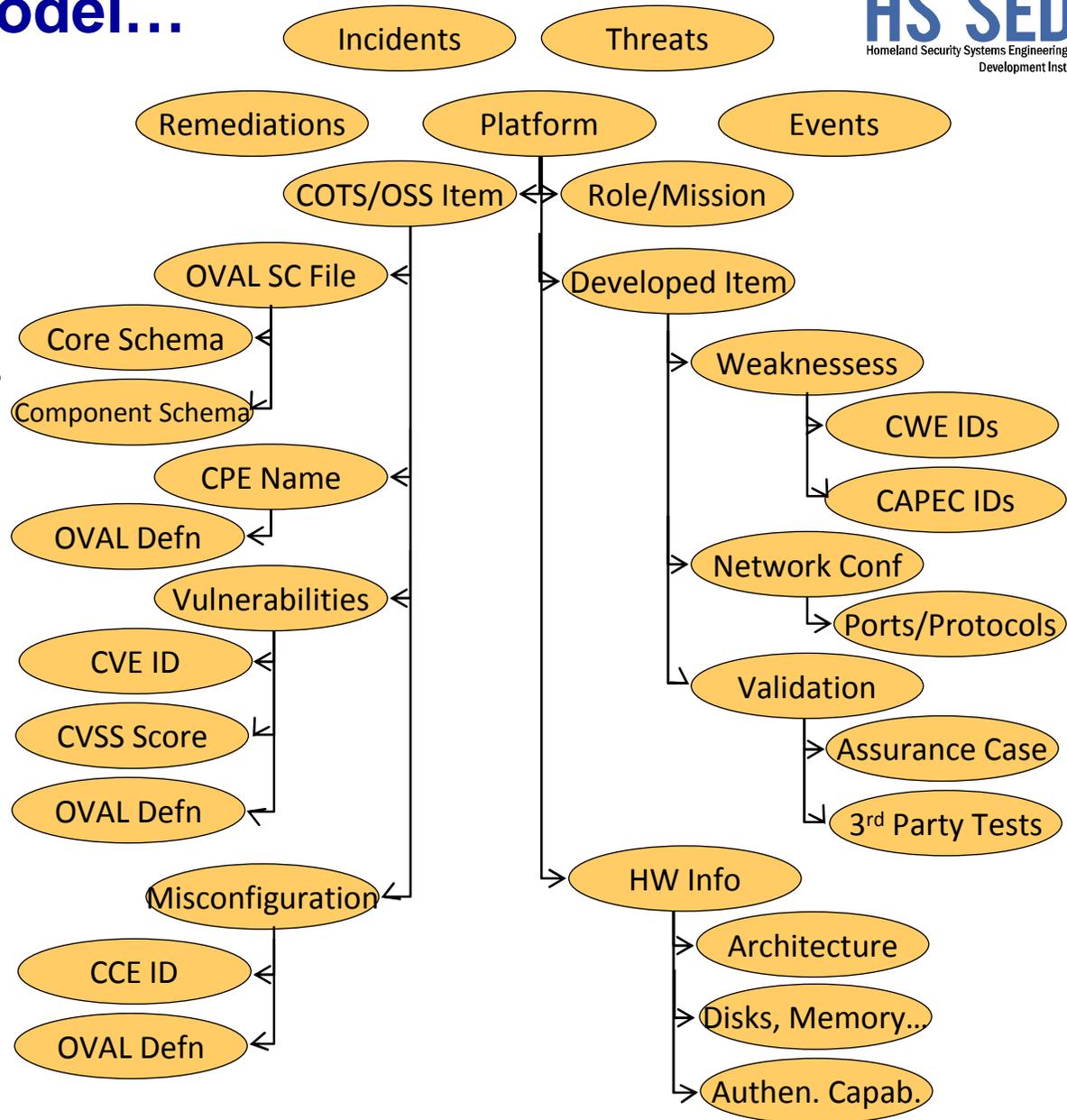
■ Threat Analysis Automation Protocol (TAAP)

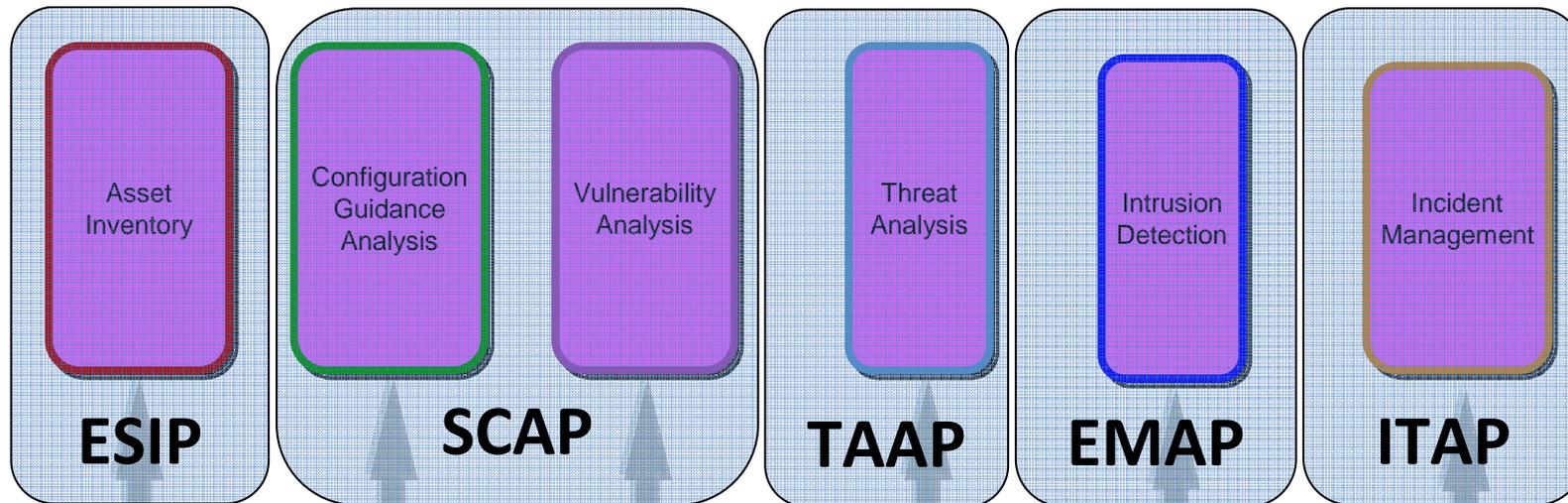
- For reporting and sharing structured threat information. Malware Attribute Enumeration & Characterization (MAEC), Common Attack Pattern Enumeration & Classification (CAPEC), Common Platform Enumeration (CPE), Common Weakness Enumeration (CWE), Open Vulnerability and Assessment Language (OVAL), Common Configuration Enumeration (CCE), and Common Vulnerabilities and Exposures (CVE).

Other things to model...

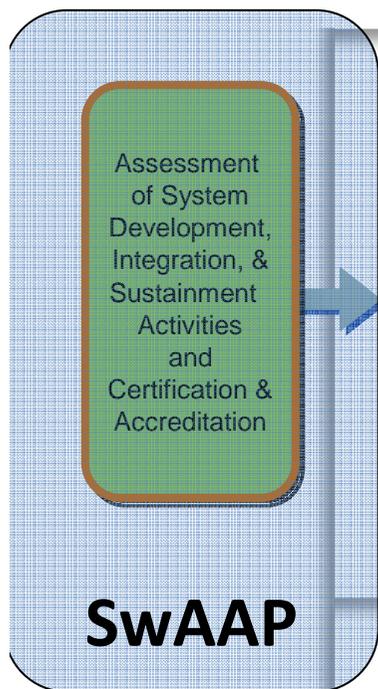
■ A platform:

- Role/Mission
- Hardware Information
 - Architecture
 - Disks, Memory, Comms, Input Devices
 - Authentication Capabilities
- Organically Developed Software
 - Weaknesses Evaluated For
 - CWE IDs
 - CAPEC IDs
 - Validation Methods
 - Structured Assurance Case
 - 3rd Party Testing
- Network Configuration Information
 - Ports/Protocols Settings



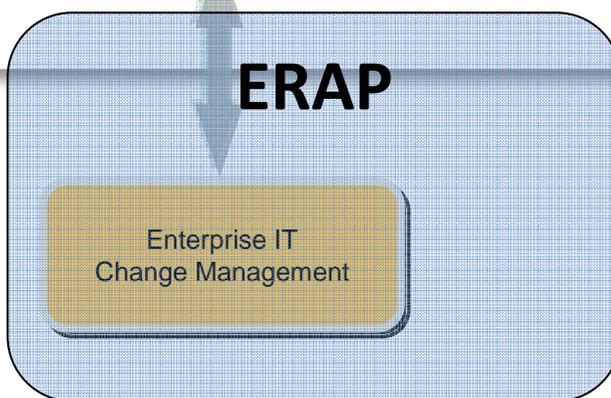
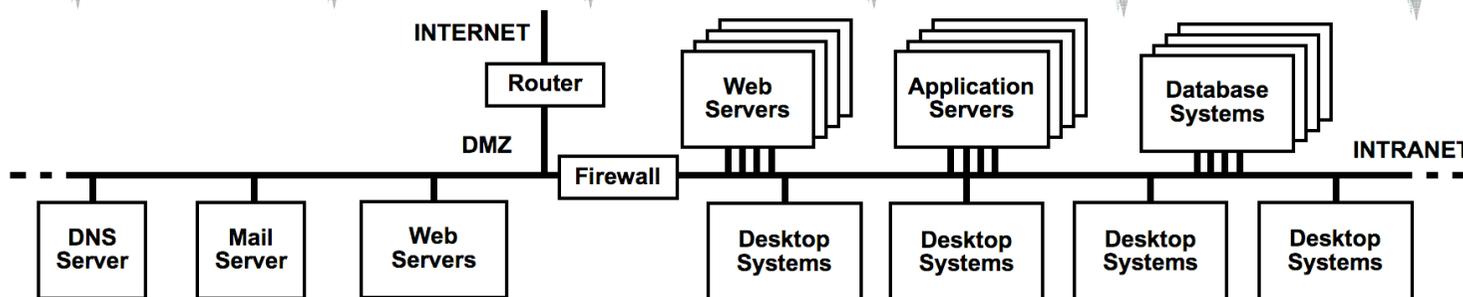


Operations Security Management Processes

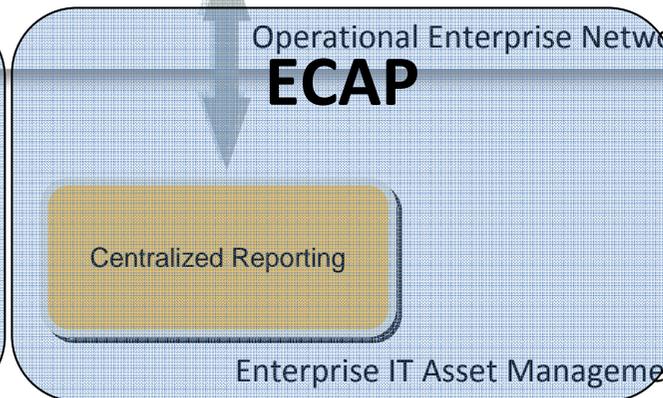


SwAAP

Development & Sustainment Security Management Processes



ERAP

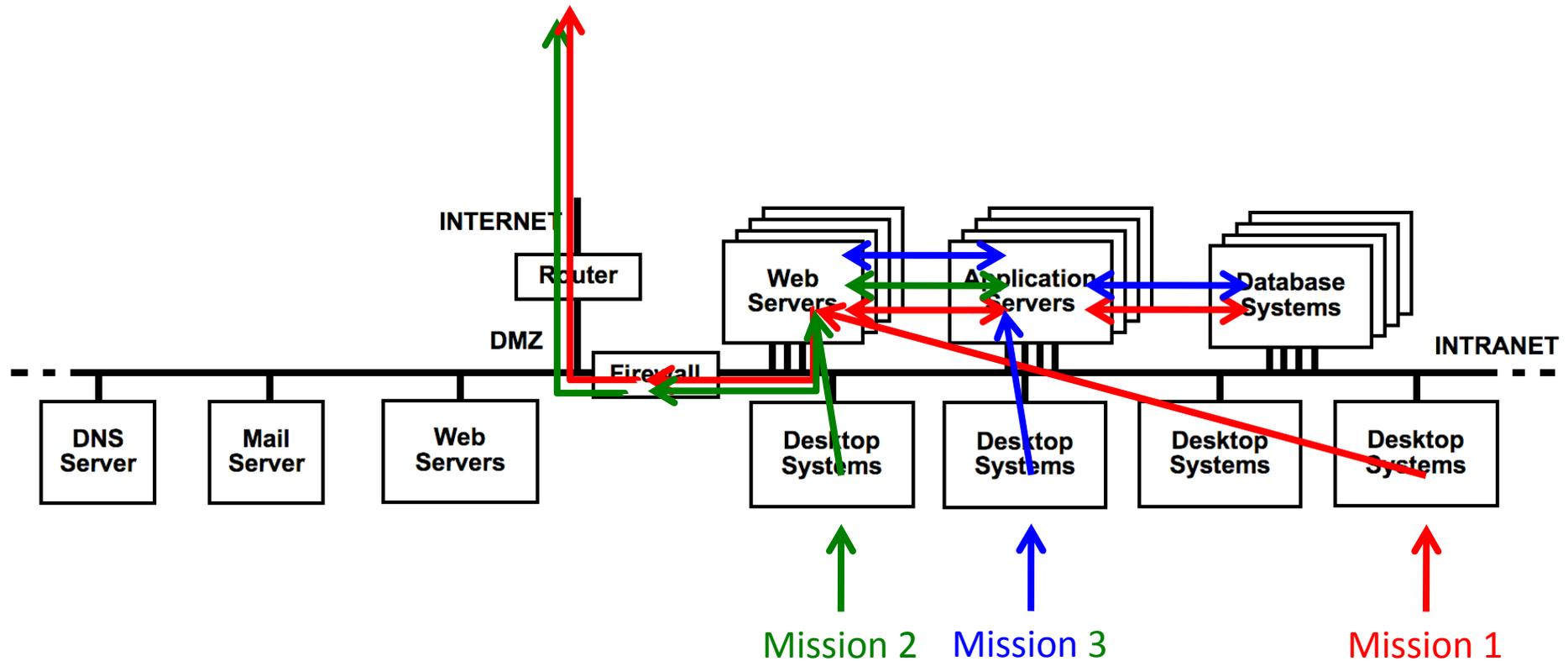


Operational Enterprise Networks

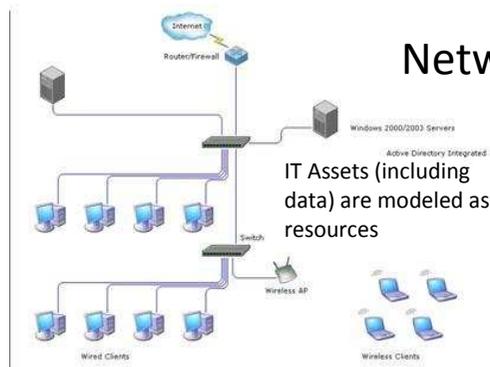
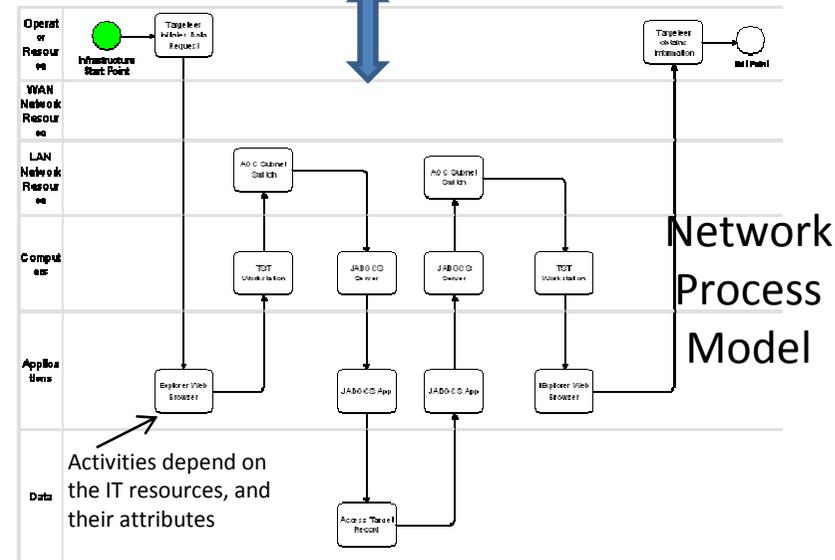
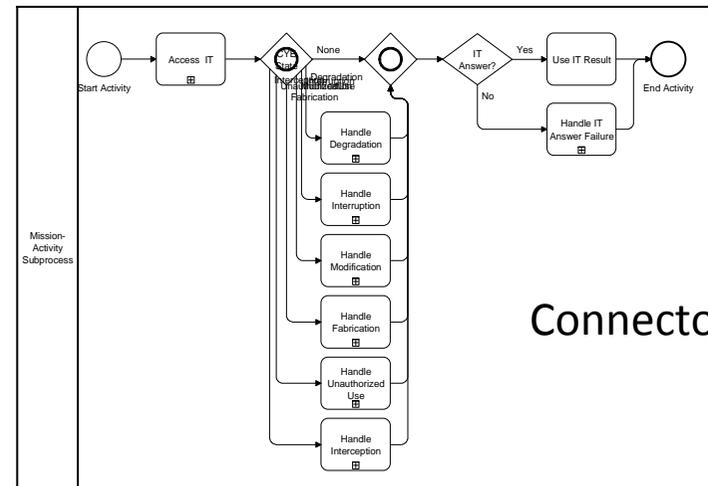
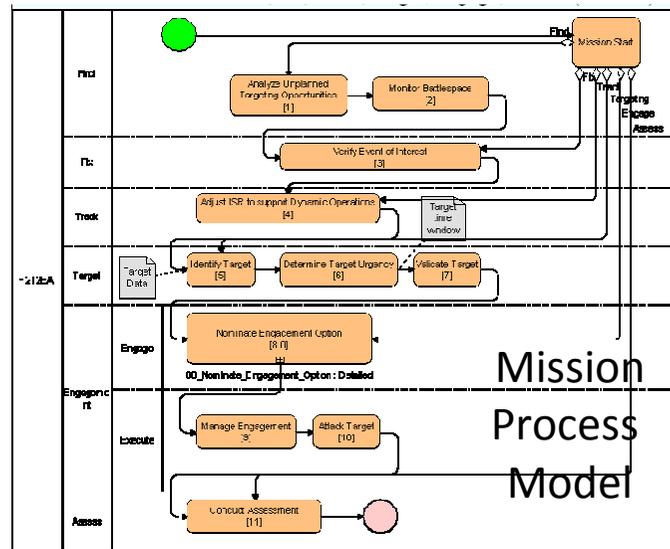
ECAP

Enterprise IT Asset Management

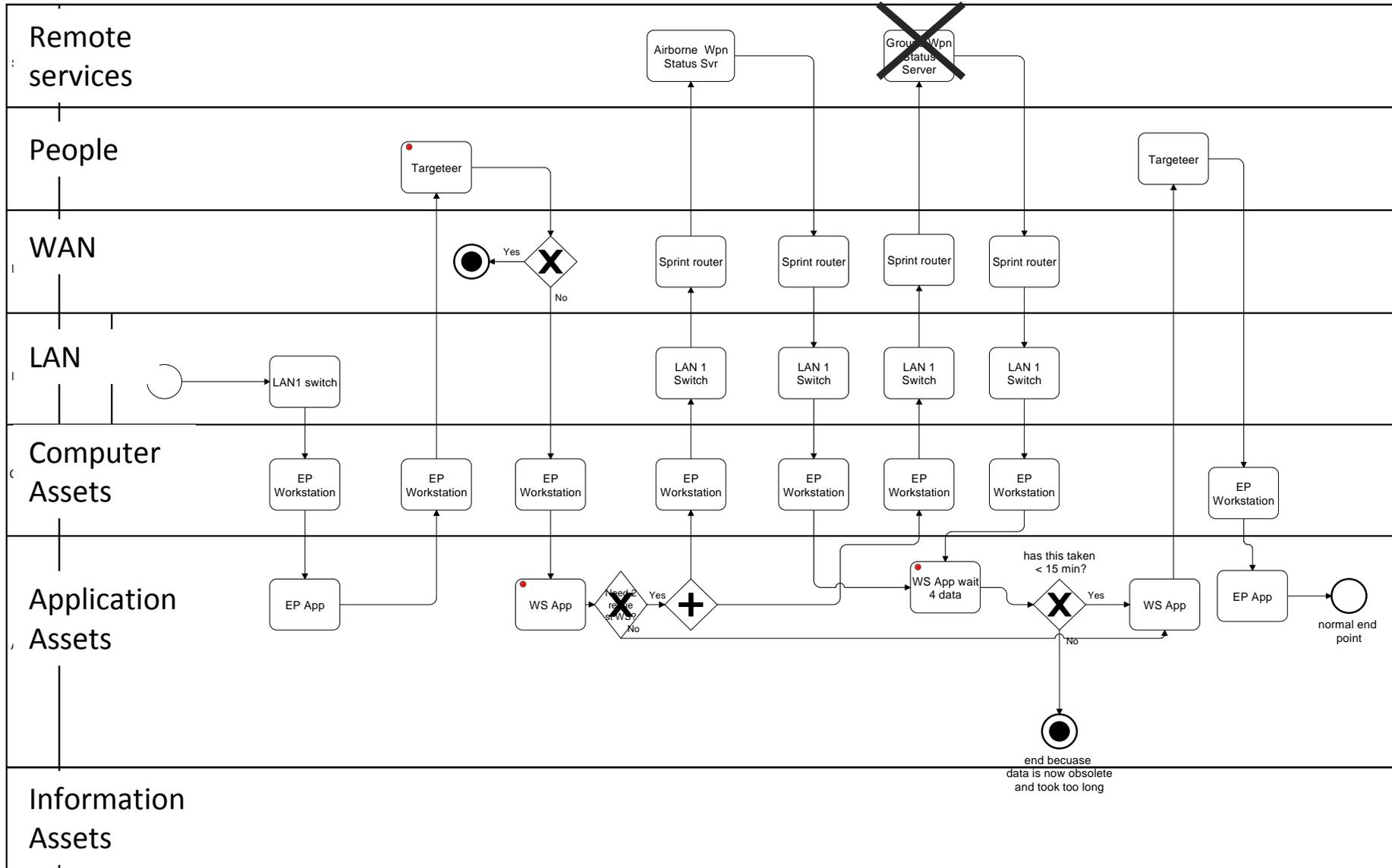
Enterprise Information Technology Infrastructures Are There to Support Missions and Enterprise Capabilities



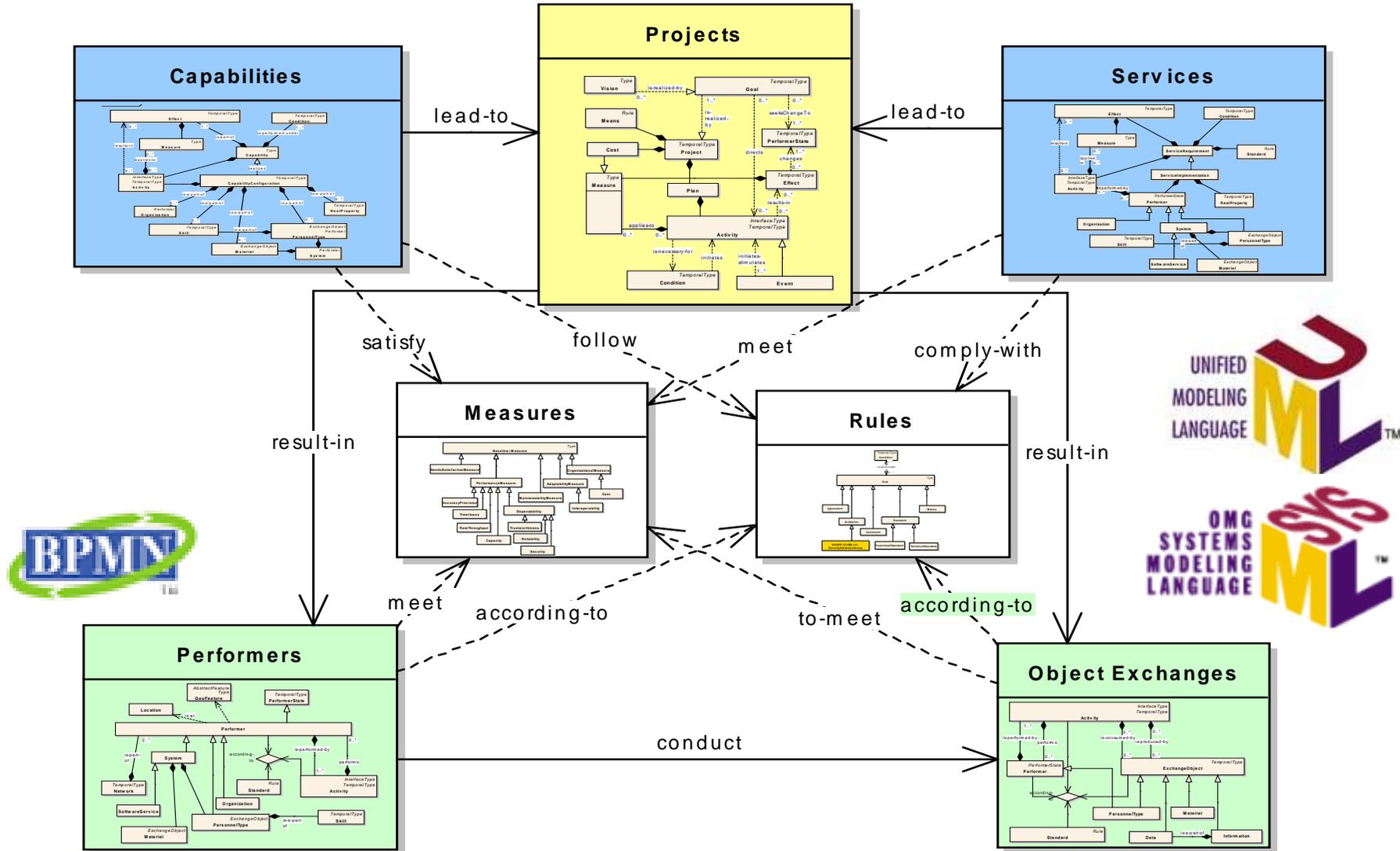
Mission Modeling: using BPMN (Business Process Modeling Notation) to represent missions and their cyber dependencies



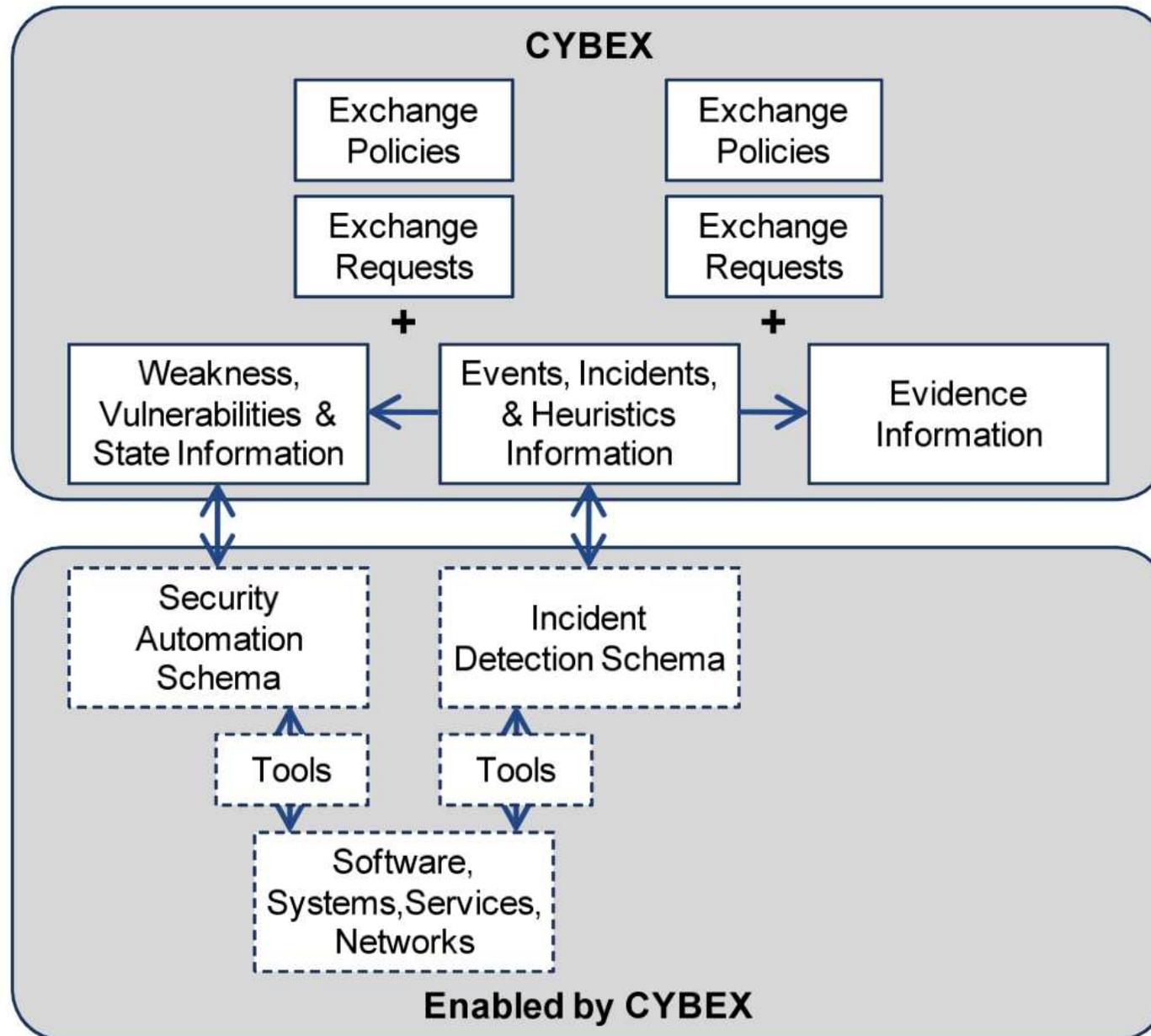
Example Incident: Remote failure interrupts access to a systems status sources



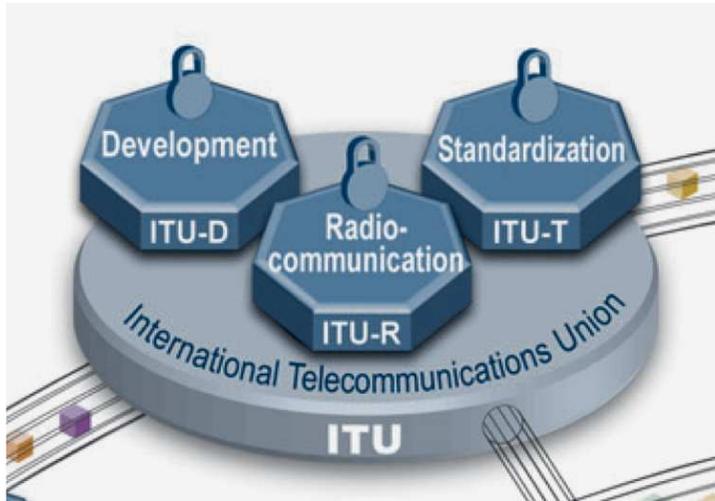
DoDAF Version 2.0 Metamodel



ITU-T CYBersecurity EXchange Framework (CYBEX)



ITU-T Study Group 17 Question 4 – Cyber Security Cyber Security Exchange Framework (CYBEX)



Creating x.series standards to capture the correct and supported USE of the enumerated concepts and languages – effort stewardship and definition stays with originating organizations

<u>Identifier</u>	<u>Title</u>	<u>Current Text</u>
X.cybief	Cybersecurity Information Exchange Framework	TD406
X.cybief.1	Guidelines for Administering the OID arc for cybersecurity information exchange	TD406
X.cce	Common Configuration Enumeration	TD406
X.cee	Common Event Expression	TD406
X.chirp	Cybersecurity Heuristics and Information Request Protocol	TD406
X.cpe	Common Platform Enumeration	TD406
X.crf	Common Result Format	TD406
X.cve	Common Vulnerabilities and Exposures	TD405
X.cvss	Common vulnerability scoring system	TD412
X.cwe	Common Weakness Enumeration	TD406
X.cwss	Common Weakness Scoring System	TD406
X.dexf	Digital evidence exchange file format	C97
X.dpi	Deep Packet Inspection Exchange Format	TD406
X.gridf	SmartGrid Incident Exchange Format	TD406
X.oval	Open Vulnerability and Assessment Language	TD406
X.pfoc	Phishing, Fraud, and Other Crimeware Exchange Format	TD406
X.scap	Security Content Automation Protocol	TD406
X.teef	Cyber attack tracing event exchange format	C135, C129
X.xccdf	eXensible Configuration Checklist Description Format	TD406
X.cybief-[namespace],	Cybersecurity Information Exchange Namespace	C148
X.cybief-discovery	Cybersecurity Information Exchange Discovery	C145
X.capec	Common Attack Pattern Enumeration and Classification	TD406
X.iodef	Incident Object Description Exchange Format	TD406

X.CVE

- **X.CVE is a literal copy of CVE Compatibility Requirements from the CVE Web Site**
 - Changes to CVE Compatibility Requirements will be reflected as updates to X.CVE
 - The CVE Editorial Board retains control of CVE
- **X.CVE will put CVE in a more “recognized” standards body versus “The MITRE Corporation” without taking control of the content or the requirements on CVE usage from the CVE Editorial Board**



Questions Can Be Addressed To:

ramartin@mitre.org