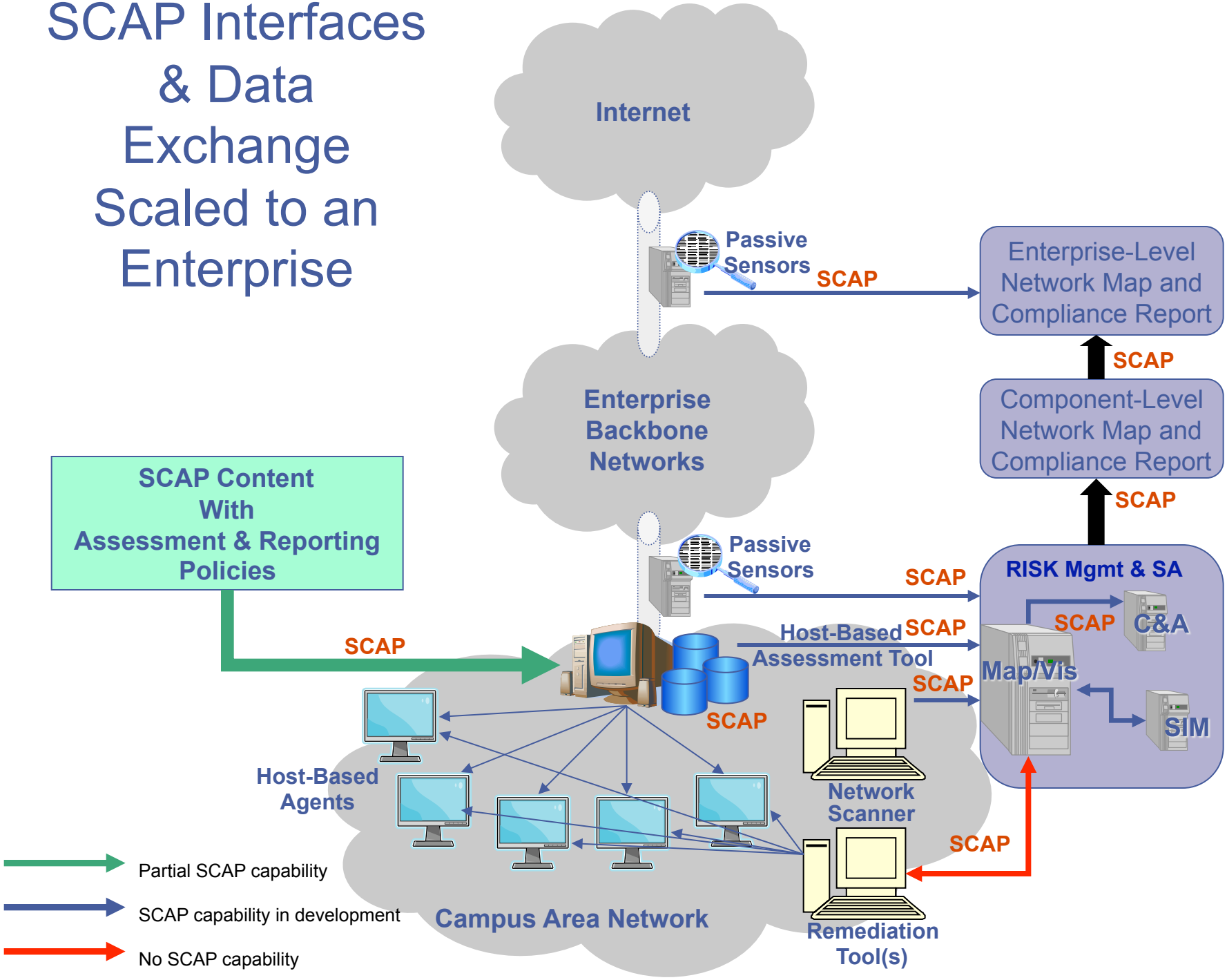
Enterprise-Level Assessment and Reporting

- The concept
- Assessment Results Format (ARF) with Summary Results
- The Policy Language for Assessment Result Reporting (PLARR)

SCAP Interfaces & Data Exchange Scaled to an Enterprise



Security Configuration Assessment & Management Scope

- Should all be reportable and described using SCAP

- Assessment Content/Defs
- Report Frequency
- Reporting Requirements
- Reporting Formats

Interoperable Assessment and Data Reporting Formats (SCAP)

Best Practice Compliance Assessment
- Commercial
- Federal
- DoD
- DoD Component

Vulnerability & Weakness Scans
- Public & DoD defined vulnerabilities
- Software & Hardware Weaknesses
- Vulnerable Configurations

Network Situational Awareness
- Logical Layout Maps
- Physical Layout Maps
- Defense-In-Depth Attack Graph

Attack Vector Analysis
- Common Exploits & Malware
- Opposing Force Attack Simulation
- Red/Blue Teaming & Assessment
- Penetration Testing

Compromise Detection
- Compromised Services
- Compromised Devices

Device Configuration

Network Configuration

Service Configuration

Architectural Robustness

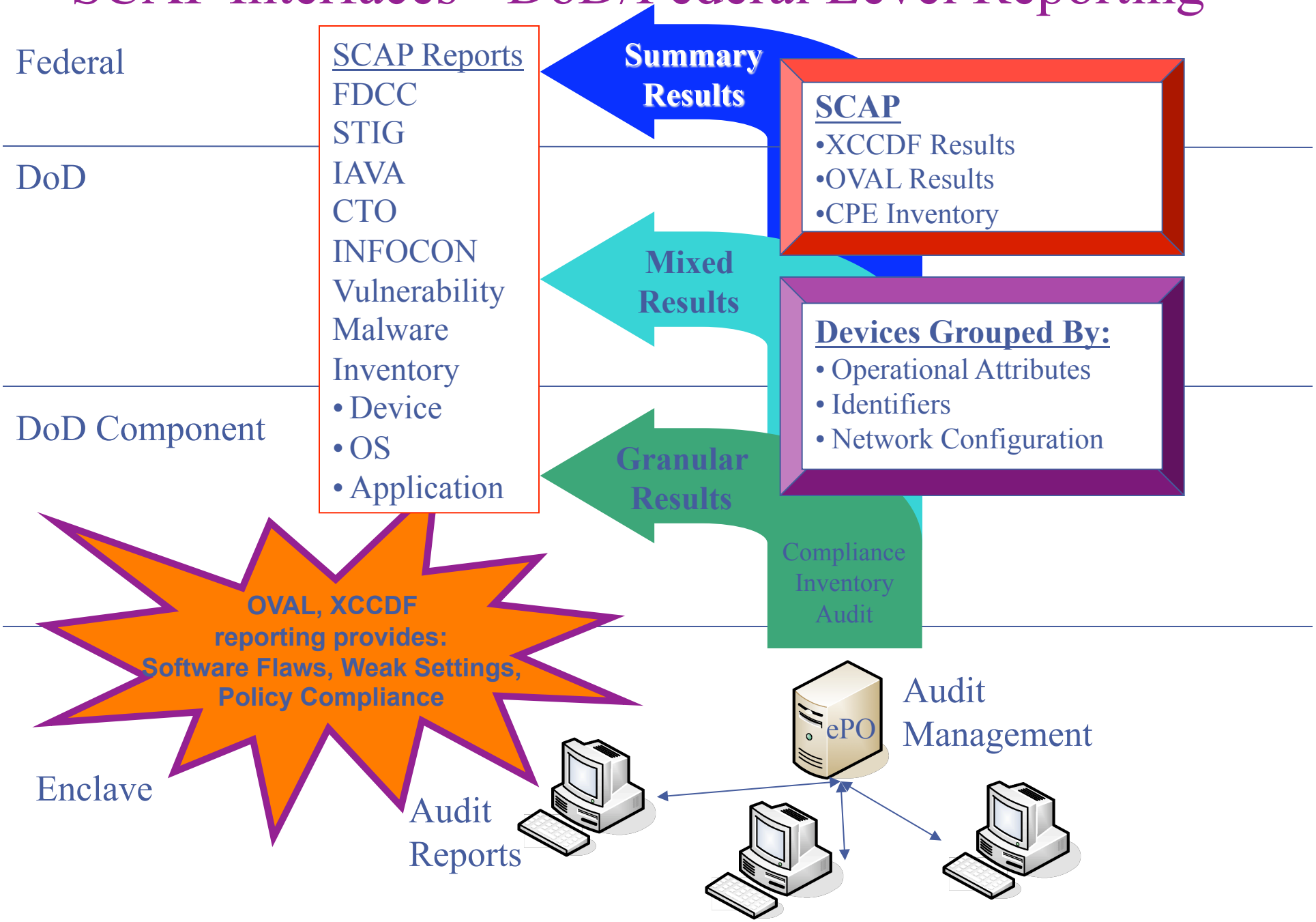
Raw Data

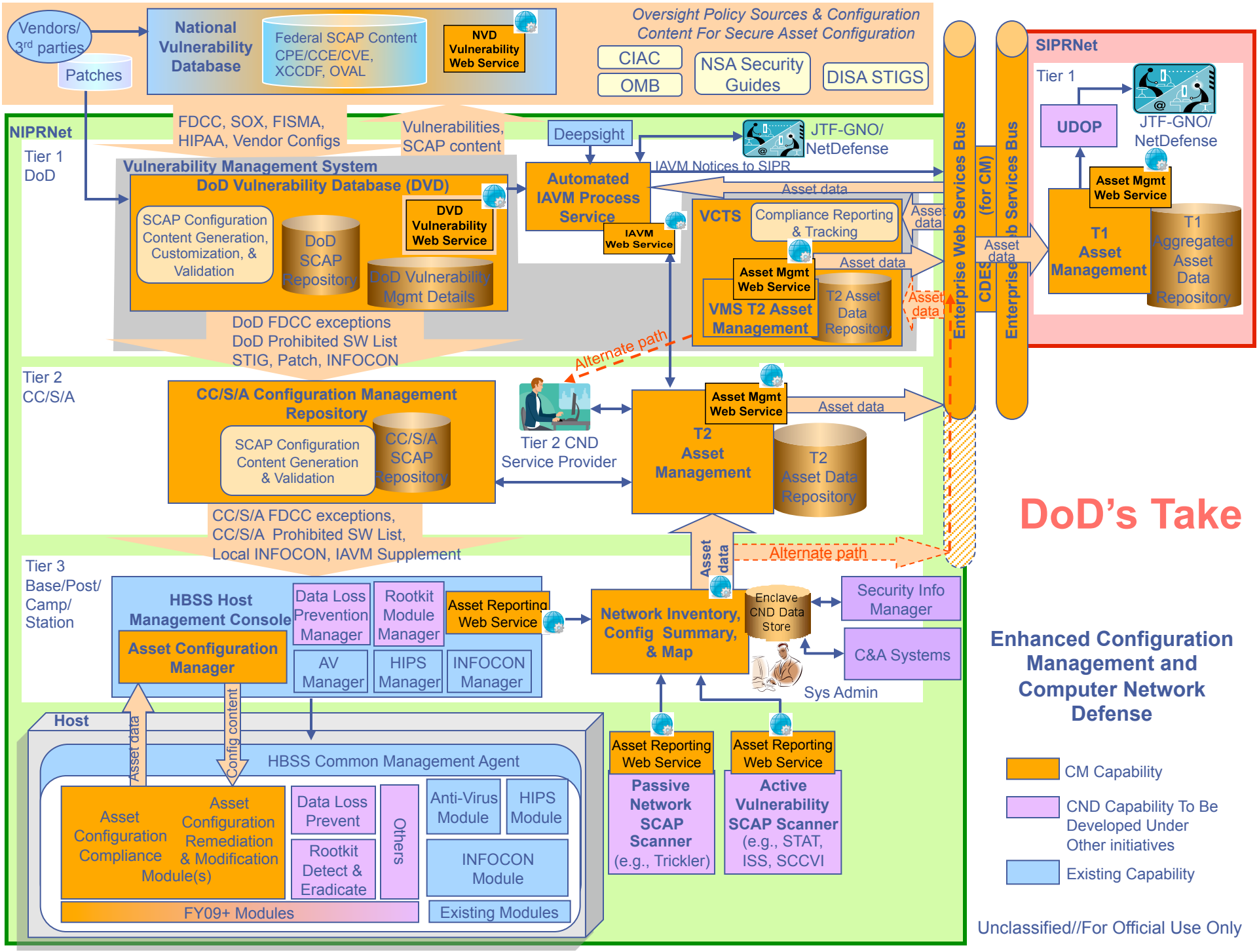
Assessment Products

Remediations, Mitigations, Courses of Action

Deliverables

SCAP Interfaces - DoD/Federal Level Reporting




Vendors/ 3rd parties
Patches
National Vulnerability Database
Federal SCAP Content CPE/CCE/CVE, XCCDF, OVAL
NVD Vulnerability Web Service
Oversight Policy Sources & Configuration Content For Secure Asset Configuration
CIAC
OMB
NSA Security Guides
DISA STIGS
NIPRNet
FDCC, SOX, FISMA, HIPAA, Vendor Configs
Vulnerabilities, SCAP content
Tier 1 DoD
Vulnerability Management System
DoD Vulnerability Database (DVD)
SCAP Configuration Content Generation, Customization, & Validation
DoD SCAP Repository
DVD Vulnerability Web Service
DoD Vulnerability Mgmt Details
Deepsight
Automated IAVM Process Service
IAVM Web Service
JTF-GNO/ NetDefense
IAVM Notices to SIPR
Asset data
VCTS
Compliance Reporting & Tracking
Asset Mgmt Web Service
VMS T2 Asset Management
T2 Asset Data Repository
DoD FDCC exceptions
DoD Prohibited SW List
STIG, Patch, INFOCON
Alternate path
Tier 2 CC/S/A
CC/S/A Configuration Management Repository
SCAP Configuration Content Generation & Validation
CC/S/A SCAP Repository
Tier 2 CND Service Provider
T2 Asset Management
T2 Asset Data Repository
CC/S/A FDCC exceptions,
CC/S/A Prohibited SW List,
Local INFOCON, IAVM Supplement
Tier 3 Base/Post/ Camp/ Station
HBSS Host Management Console
Asset Configuration Manager
Data Loss Prevention Manager
Rootkit Module Manager
Asset Reporting Web Service
AV Manager
HIPS Manager
INFOCON Manager
Network Inventory, Config Summary, & Map
Enclave CND Data Store
Security Info Manager
C&A Systems
Sys Admin
Host
HBSS Common Management Agent
Asset data
Config content
Asset Configuration Compliance
Asset Configuration Remediation & Modification Module(s)
Data Loss Prevent
Rootkit Detect & Eradicate
Others
Anti-Virus Module
HIPS Module
INFOCON Module
FY09+ Modules
Existing Modules
Asset Reporting Web Service
Passive Network SCAP Scanner (e.g., Trickler)
Asset Reporting Web Service
Active Vulnerability SCAP Scanner (e.g., STAT, ISS, SCCVI
Enterprise Web Services Bus
CDES (for CM)
Enterprise Web Services Bus
SIPRNet
Tier 1
UDOP
JTF-GNO/ NetDefense
Asset Mgmt Web Service
T1 Asset Management
T1 Aggregated Asset Data Repository
DoD's Take
Enhanced Configuration Management and Computer Network Defense
CM Capability
CND Capability To Be Developed Under Other initiatives
Existing Capability
Unclassified//For Official Use Only

Is this worth doing?

- Is anyone already doing enterprise reporting?
  - Proprietary?
  - Open? (Using SCAP potentially?)
- Is this worth standardizing the data exchanges with NIST?
  - If so, is it worth adding to the SCAP Validation program?

Assessment Results Format

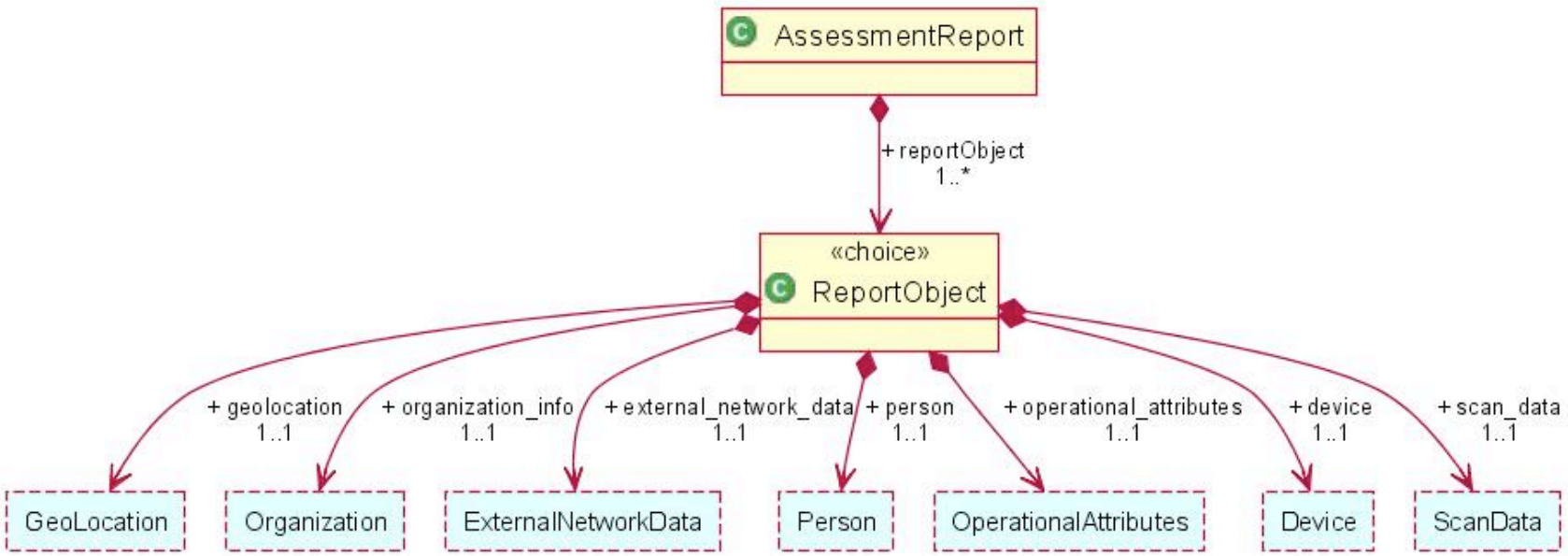
The detailed, per-device assessment results language

ARF Functionality

- Packages information any SCAP validated tool must already produce
  - OVAL Results
  - XCCDF Results
- Adds network info, CPE inventory, Ops-Attributes
  - CPE Inventory = findings reported against OS & applications
- Supports object re-use
  - References instead of building stand-alone objects
- Has built-in replication support
  - Action/Status tags
- Simplistic – Supports comprehension and CDS

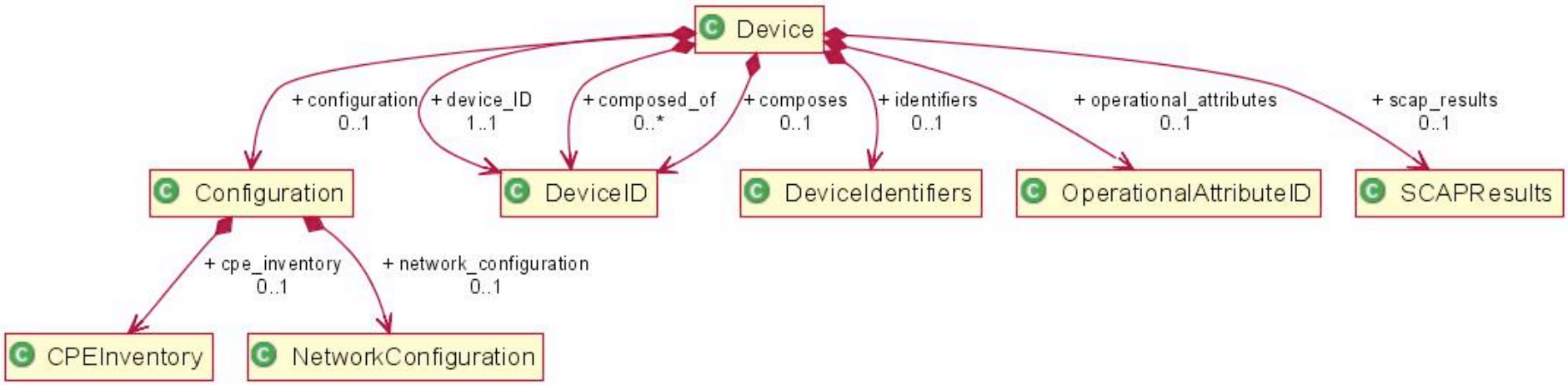
ARF Data Schema Top Level Concept

- A “report” consists of some number of “report objects” that can be paged
  - Each type of object is assigned a unique ID and can be referenced
  - Intended to support paging – 0 to many report objects/page



Device Record – The Key ARF Data Type

- The stuff from the DoD data modeling efforts
  - We're pretty sure we need
  - We're pretty sure we can get
  - No hardware inventory (disk drive, *µ*processor, memory, etc.)
    - *May re-look that before 1.0 release*

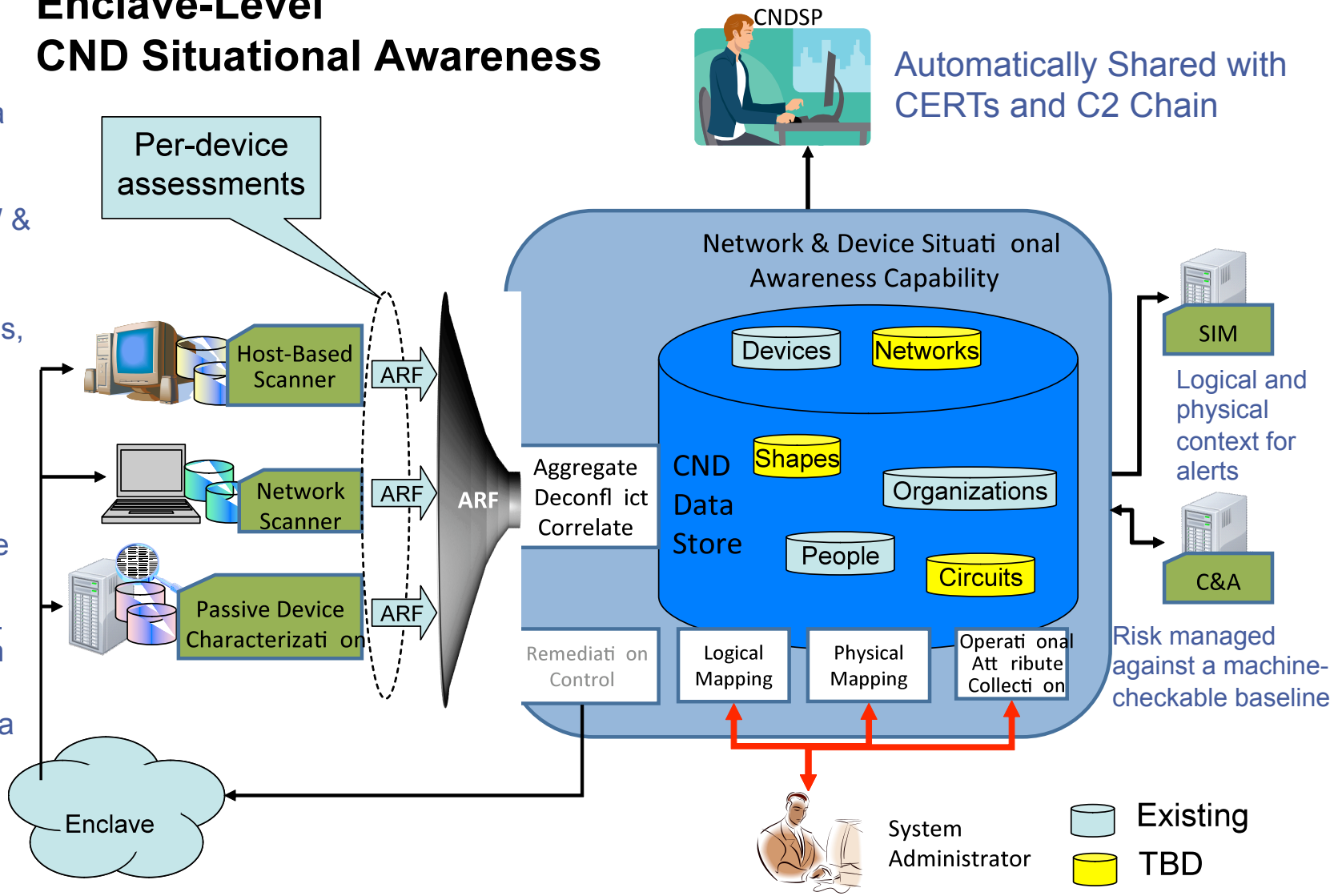


ARF Vision

Enclave-Level CND Situational Awareness

Reports - on a per-device basis of:
- Installed SW & HW
- Patches, vulnerabilities, settings
- Running services & processes
- Network infrastructure

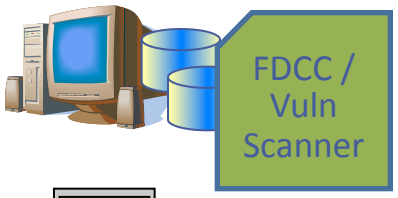
Organized by:
- Organization
- Network
- Physical area
- Building



Enclave-Level CND Situational Awareness

Asset Database?

Network & Device Situational Awareness Capability



ARF

ARF

ARF

ARF

Aggregate
Deconflict
Correlate

CND Data Store

Devices

Networks

Shapes

Organizations

People

Circuits

Remediation Control

Logical Mapping

Physical Mapping

Operational Attribute Collection

SIM

C&A

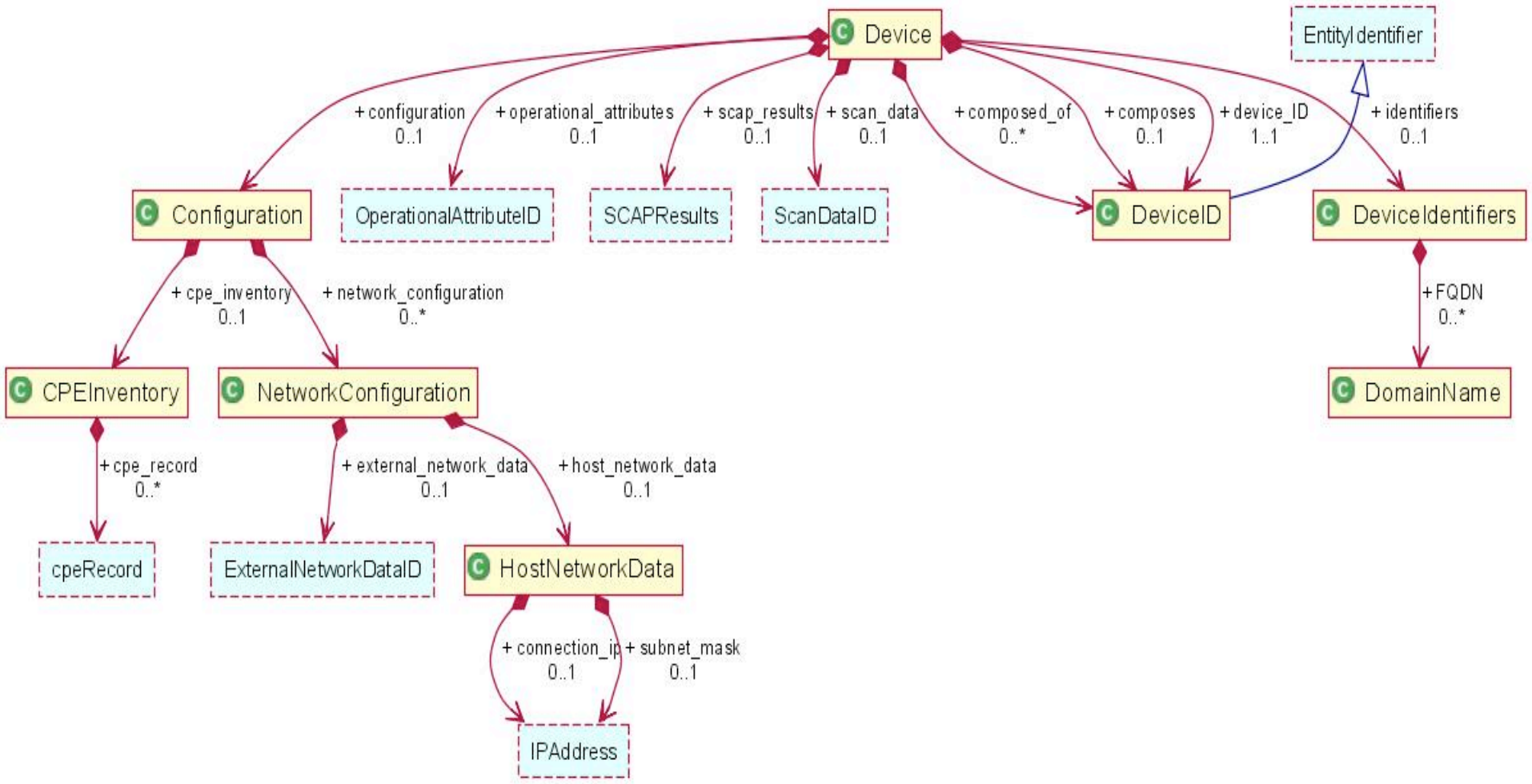
Enclave

System Administrator

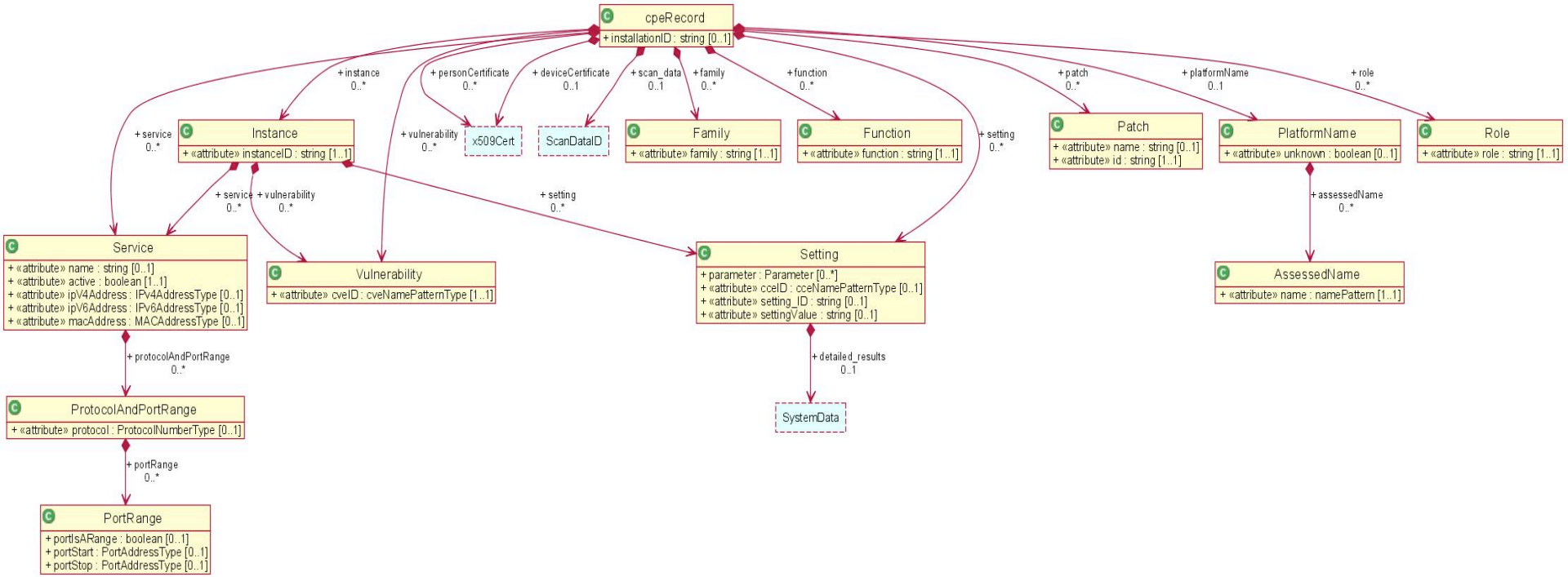
Existing

TBD

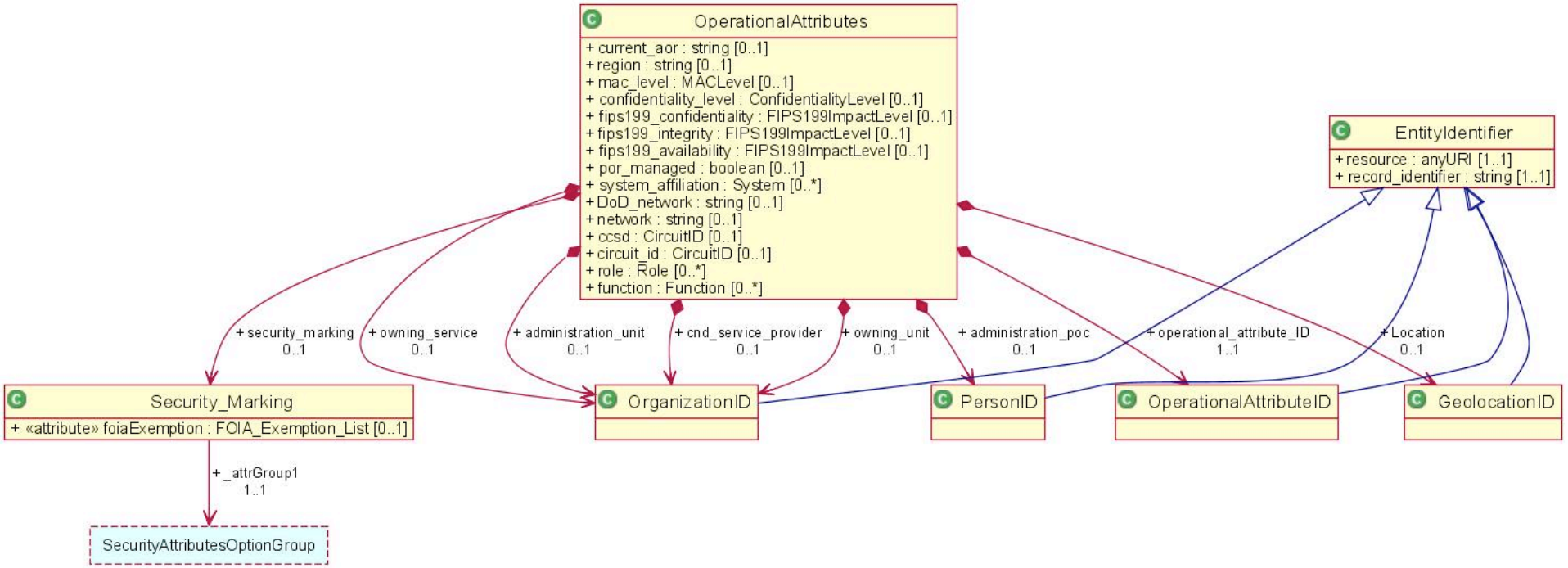
Reporting Data Elements & Relationships: The ARF Device Model



Per Software Product Data (aka cpe-record)



Operational Attributes



ARF vs. Vanilla SCAP for Assessment Reporting

- An additional XML schema
- Pros
  - Adds additional information
  - Supports products that don't use OVAL/XCCDF
  - More lightweight
- Cons
  - Another XML schema to implement

Is ARF lightweight enough?

- Specifies most fields, increasing structure and reliability
- But overspecifying means implementing things that will never be used
- What's the appropriate level?

Summary Results

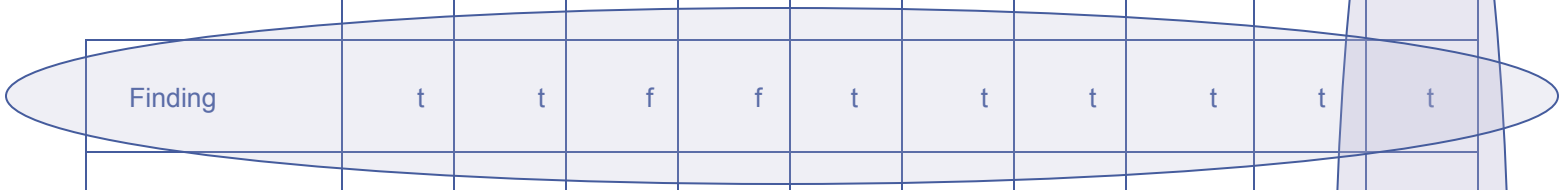
When you just want a single question answered

Summary Results Functionality

- Allows for Concise reports on single assessment checks
  - CPE platform definitions
  - CVEs
  - CCE parameters
  - OVAL Definitions
  - XCCDF Benchmarks
  - Patches
- Provides results either as Counts or Lists per finding
  - (true/false, pass/fail, not applicable, not checked, error)
  - Lists by: IP, Domain Name, Record Identifier
- Plus population data and scan data

ARF

Summary Results



Finding	t	t	f	f	t	t	t	t	t	t
Finding	t	t	f	f	t	t	t	t	t	t
Finding	t	t	f	f	t	t	t	t	t	t
Finding	t	t	f	f	t	t	t	t	t	4
Finding	t	t	f	f	t	t	t	t	t	t
Finding	t	t	f	f	t	t	t	t	t	1
Finding	t	t	f	f	t	t	t	t	t	t
Finding	t	t	f	f	t	t	t	t	t	t

Device

Device

Device

Device

Device

Device

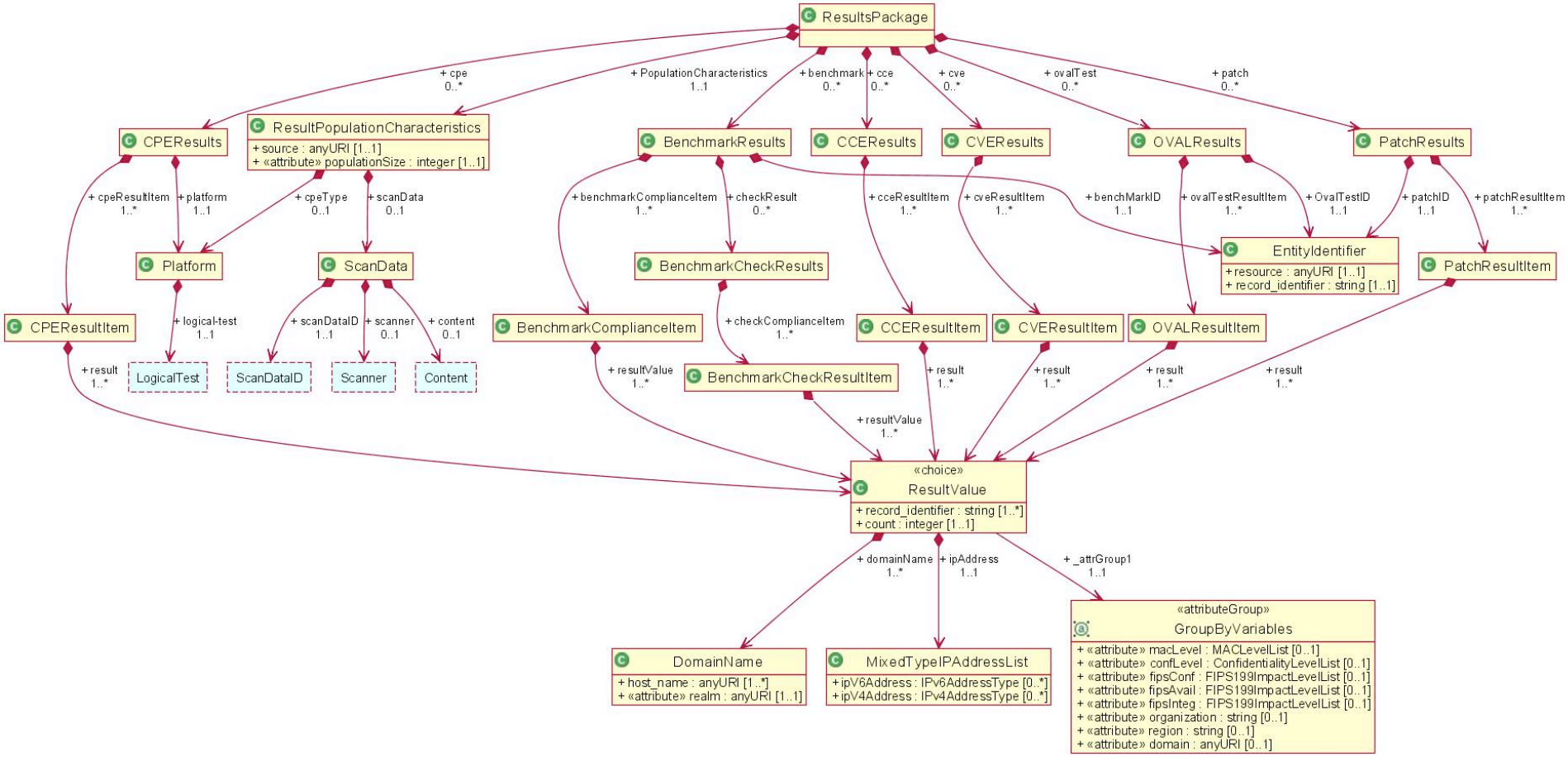
Device

Device

Device

Device

Summary Results Top Level Concept



The Assessed item is listed first, then lists or counts per possible finding value

Sample – Summary Report for WinXP with Flash

```
- <summRes:platform id="Windows XP with Flash">
  - <cpe:logical-test negate="false" operator="AND">
      <cpe:fact-ref name="cpe:/o:microsoft:windows_xp" />
      <cpe:fact-ref name="cpe:/a::flash" />
    </cpe:logical-test>
  </summRes:platform>
- <summRes:cpeResultItem cpeFinding="true">
  - <summRes:result>
      <!--  The issue that the network may have several versions of Flash isn't addressed here.  Need to add that
      to the DR tracking. Seems like we'd need to have counts for each version found on the network.   -->
      <summRes:count>16</summRes:count>
    </summRes:result>
  </summRes:cpeResultItem>
- <summRes:cpeResultItem cpeFinding="false">
  - <summRes:result>
      <summRes:count>300</summRes:count>
    </summRes:result>
  </summRes:cpeResultItem>
- <summRes:cpeResultItem cpeFinding="not applicable">
  - <summRes:result>
      <summRes:count>70</summRes:count>
    </summRes:result>
  </summRes:cpeResultItem>
- <summRes:cpeResultItem cpeFinding="not evaluated">
  - <summRes:result>
      <summRes:count>450</summRes:count>
    </summRes:result>
  </summRes:cpeResultItem>
</summRes:CPEResults>
```

Sample – Arbitrary OVAL Definition, Listed by IP, Sorted by Region

```
- <summRes:OvalTestID>
    <cndc:resource>http://www.mitre.oval.org</cndc:resource>
    <cndc:record_identifier>Definition_123</cndc:record_identifier>
  </summRes:OvalTestID>
- <summRes:ovalTestResultItem ovalFinding="true">
  - <summRes:result region="US">
    + <summRes:ipAddress>
    </summRes:result>
  - <summRes:result region="non-US">
    - <summRes:ipAddress>
        <summRes:ipV4Address>192.168.1.6</summRes:ipV4Address>
        <summRes:ipV4Address>192.168.1.7</summRes:ipV4Address>
        <summRes:ipV4Address>192.168.1.8</summRes:ipV4Address>
        <summRes:ipV4Address>192.168.1.9</summRes:ipV4Address>
        <summRes:ipV4Address>192.168.1.10</summRes:ipV4Address>
      </summRes:ipAddress>
    </summRes:result>
  </summRes:ovalTestResultItem>
- <summRes:ovalTestResultItem ovalFinding="false">
  - <summRes:result region="US">
    - <summRes:ipAddress>
        <summRes:ipV4Address>192.168.1.11</summRes:ipV4Address>
        <summRes:ipV4Address>192.168.1.12</summRes:ipV4Address>
        <summRes:ipV4Address>192.168.1.13</summRes:ipV4Address>
        <summRes:ipV4Address>192.168.1.14</summRes:ipV4Address>
        <summRes:ipV4Address>192.168.1.15</summRes:ipV4Address>
      </summRes:ipAddress>
    </summRes:result>
  - <summRes:result region="non-US">
    - <summRes:ipAddress>
        <summRes:ipV4Address>192.168.1.16</summRes:ipV4Address>
        <summRes:ipV4Address>192.168.1.17</summRes:ipV4Address>
        <summRes:ipV4Address>192.168.1.18</summRes:ipV4Address>
        <summRes:ipV4Address>192.168.1.19</summRes:ipV4Address>
        <summRes:ipV4Address>192.168.1.20</summRes:ipV4Address>
      </summRes:ipAddress>
    </summRes:result>
  </summRes:ovalTestResultItem>
</summRes:OVALResults>
```

Are Summary Results Necessary?

- Pros
  - More lightweight (bandwidth and processing)
  - Standard grammar for aggregation (less confusion)
- Cons
  - Adds complexity to the schema
  - Adds an intelligence requirement onto tools that support it (must be able to generate aggregations)
- Could validate ARF and Summary Results separately?

PLARR

- Policy Language for Assessment Results Reporting
  - Request format for assessment reports
- Use cases
  - Reporting and aggregation
    - Am I vulnerable to CVE-2008-1234? Which hosts? Which departments?
  - Security Information Managers
    - Feeds from asset managers, NOCs
    - Vulnerability/Compliance/Security status by network, organization, task, etc.
  - Compliance assessments
    - FDCC, Internal, etc
- Considered for (very) future SCAP Validation requirement

PLARR Schema

- Available at _____
- Assessment Content
  - Check content (XCCDF or OVAL)
  - (or) Enumeration content
  - Other metadata (due dates, freshness criterion, etc)
- Asset Population
  - By subnet, IP, asset ID
- Return Method

Sample PLARR – Subnet for Vulnerability

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Note: This lines up with scenario A-3 from the CND High Level Use Cases document -->
<plarr xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
 xsi:schemaLocation="http://scap.nist.gov/schema/plarr/0.1 plarr.xsd"
 xmlns="http://scap.nist.gov/schema/plarr/0.1">
  <!-- This will scan all systems in the asset population for CVE-2008-1234
   using whatever means it has, such as finding OVAL or using CPE mappings -->
  <inventory_content>
    <cpe_include>
      <cve_include>CVE-2008-1234</cve_include>
    </cpe_include>
    <!-- Only returns CPE records when CVE-2008-1234 evaluates to true -->
    <filters>
        <cve_criterion operation="equals">found</cve_criterion>
    </filters>
  </inventory_content>

  <!-- Scans any assets in the subnet 129.83.175.0 -->
  <asset_population>
    <subnet_criterion>129.83.175.0</subnet_criterion>
  </asset_population>
  <!-- Response will be posted to the given URL-->
  <post_response href="http://cyoc.mitre.org/hosts/3" />
</plarr>
```

PLARR Example – Given SCAP

```
<?xml version="1.0" encoding="UTF-8"?>
<plarr xmlns="http://scap.nist.gov/schema/plarr/0.1" xmlns:cndc="http://metadata.dod.mil/mdr/ns/
netops/net_defense/cnd-core/0.41">

  <!-- Passes XCCDF and OVAL to the assessing system -->
  <check_content>
    <reference system="http://checklists.nist.gov/xccdf/1.1" href="http://nvd.nist.gov/vulnerabilities/
xccdf/windows.xccdf.xml" />
  </check_content>

  <!-- Scans a system by asset id -->
  <asset_population>
    <id_criterion>
      <cndc:resource>http://assets.mitre.org</cndc:resource>
      <cndc:record_identifier>/assets/3</cndc:record_identifier>
    </id_criterion>
  </asset_population>

  <!-- Only wants assessment results back, in SCAP form (XCCDF+OVAL) -->
  <post_response href="http://assets.mitre.org/hosts/3" />
</plarr>
```

What's the scope?

- Request/Response transport specifications?
  - How do you actually send the PLARR and receive the response?
  - Maybe not part of the XML Schema, but part of the validation requirements.
- Error Handling
  - PLARRError response type
    - Adds complexity, but also adds detail and consistency
  - Or rely on transport (500 error)
    - Less complexity and up front cost, but more inconsistency

What's the scope? (2)

- Aggregations and Groupings
  - Is there any value to doing this?
    - Save bandwidth, processing overhead
  - Is it worth the implementation cost?
    - Complex request schema, response schema
    - Should we break it out into separate validation requirements?

Is PLARR an ARF request format?

- There are existing ARF schemas for certain fields.
  - CND Core: Asset information, common value types
  - SCAP Core: Common SCAP types
  - ARF: Assessment Results
- Should we import those namespaces?
  - Prevents miscommunications, reimplementations
  - But forces implementation of a large set all at once
- Should PLARR always return ARF?
  - Forces similar grammars
  - But forces tools to return all SCAP as ARF

Future

- ARF
  - Already submitted to NIST as an emerging spec
  - Will be posted to emerging specs list
- Summary Results
  - Will be posted to emerging specs list
- PLARR
  - Will be posted to emerging specs list

- Reply on list with comments