



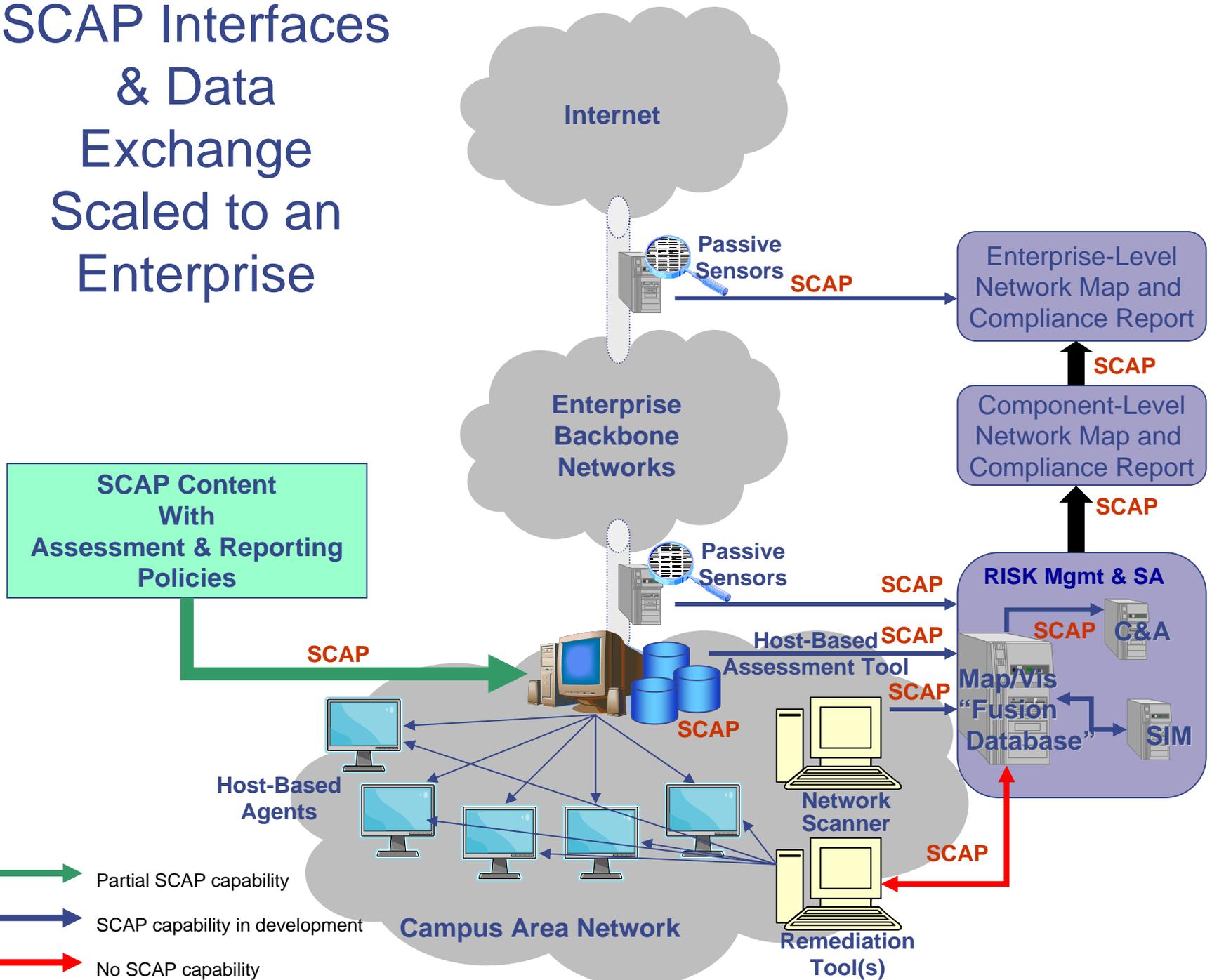
ARF, ARCAT, and Summary Results

Lt Col Joseph L. Wolfkiel

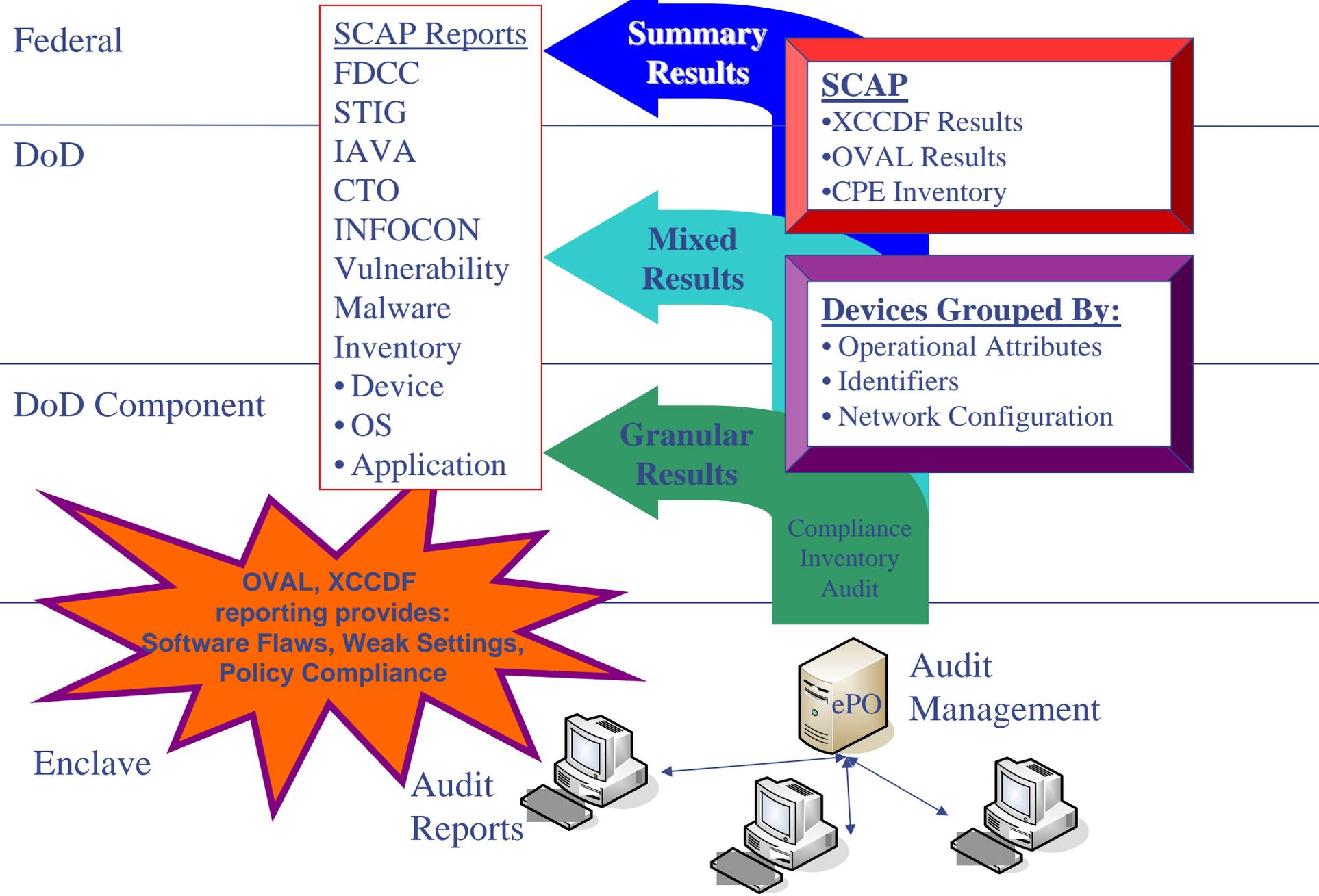
Enterprise-Level Assessment and Reporting

- The Concept
- Assessment Results Format (ARF)
- Assessment Summary Results (ASR)
- The Assessment Results Consumer and Analysis Tool (ARCAT)

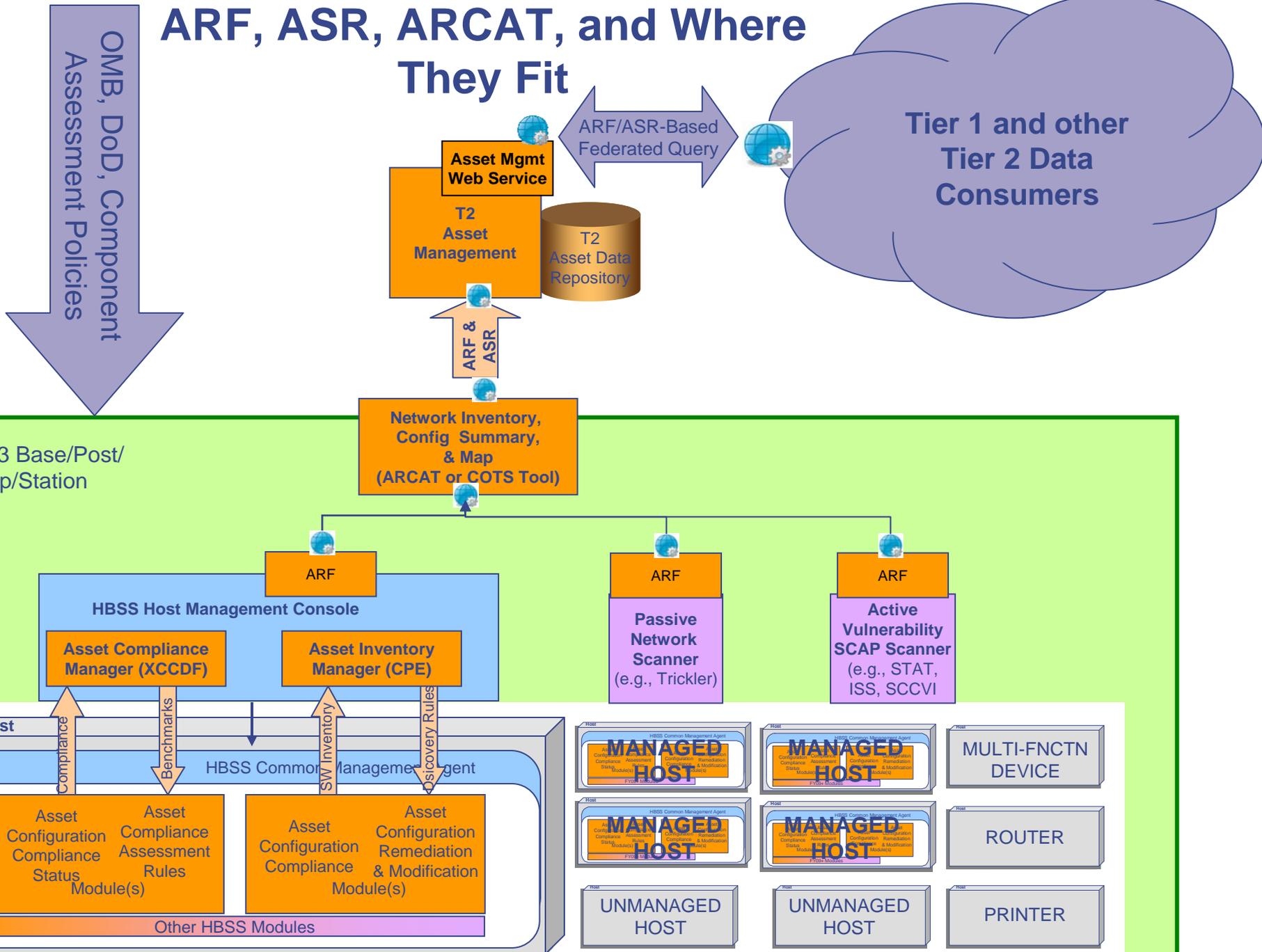
SCAP Interfaces & Data Exchange Scaled to an Enterprise



SCAP Interfaces - DoD/Federal Level Reporting



ARF, ASR, ARCAT, and Where They Fit



Assessment Results Format

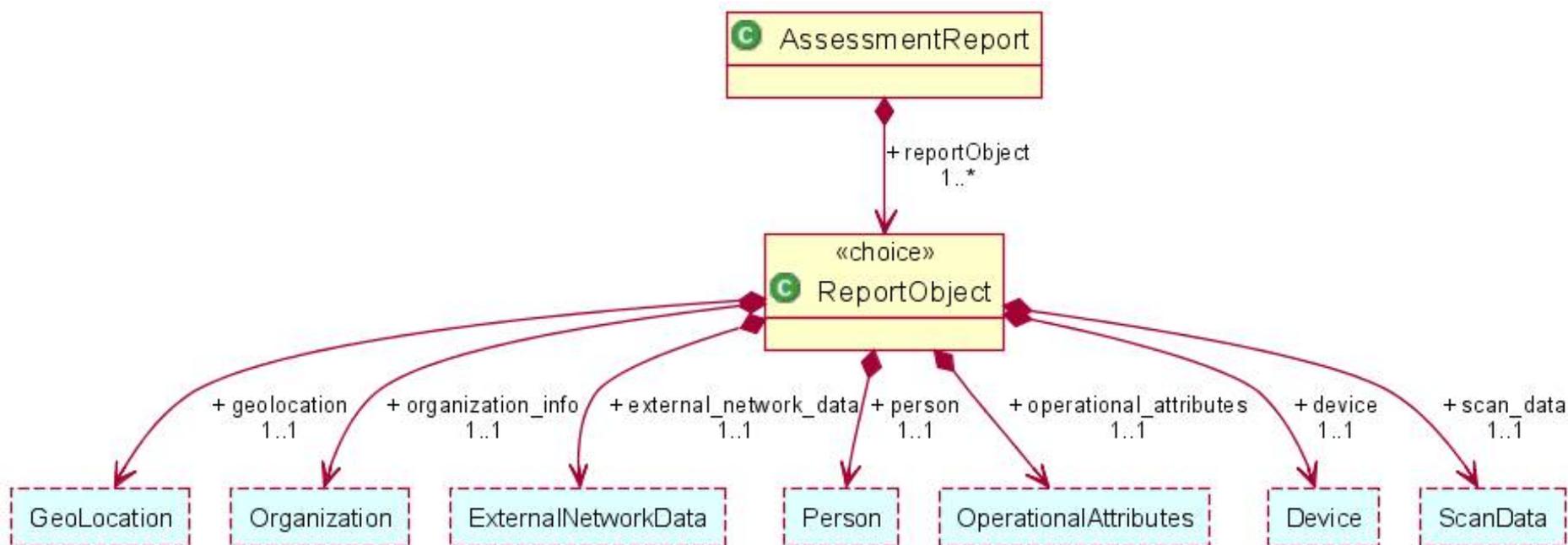
The detailed, per-device assessment results
language

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 Cross-Domain Solution (CDS)

ARF Data Schema Top Level Concept

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



ARF Vision

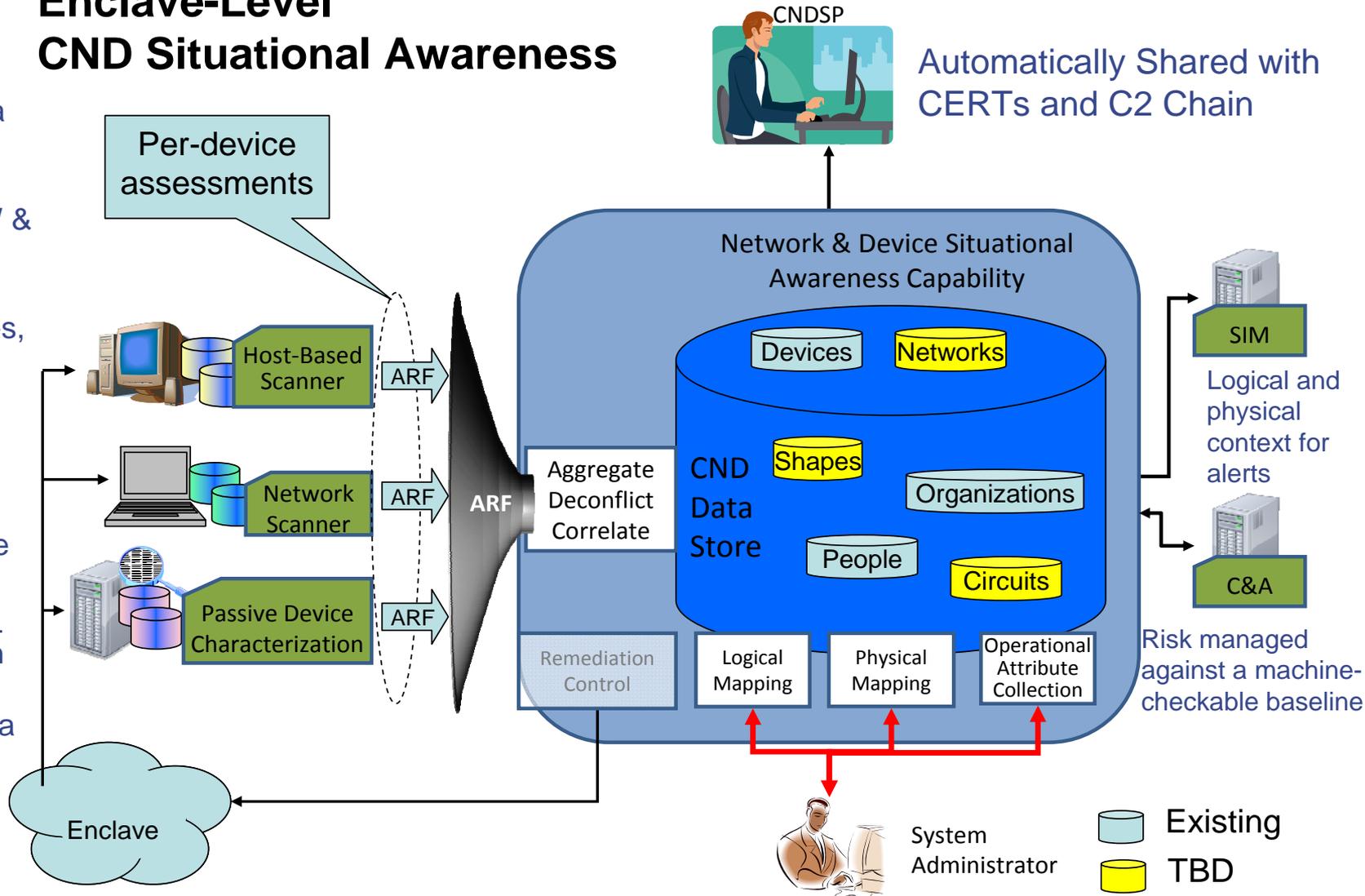
Enclave-Level CND Situational Awareness

Reports - on a per-device basis of:

- Installed SW & HW
- Patches, vulnerabilities, settings
- Running services & processes
- Network infrastructure

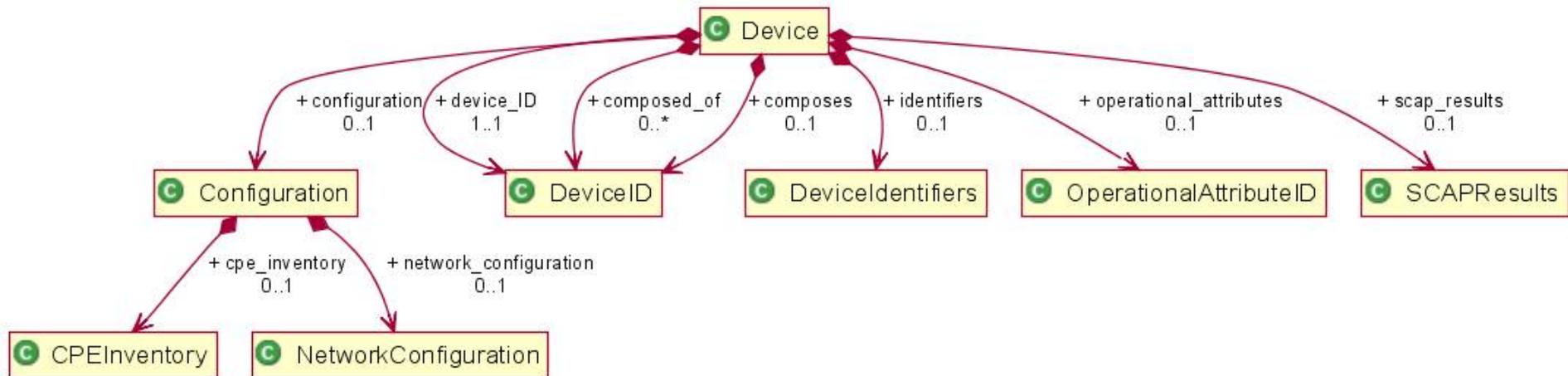
Organized by:

- Organization
- Network
- Physical area
- Building

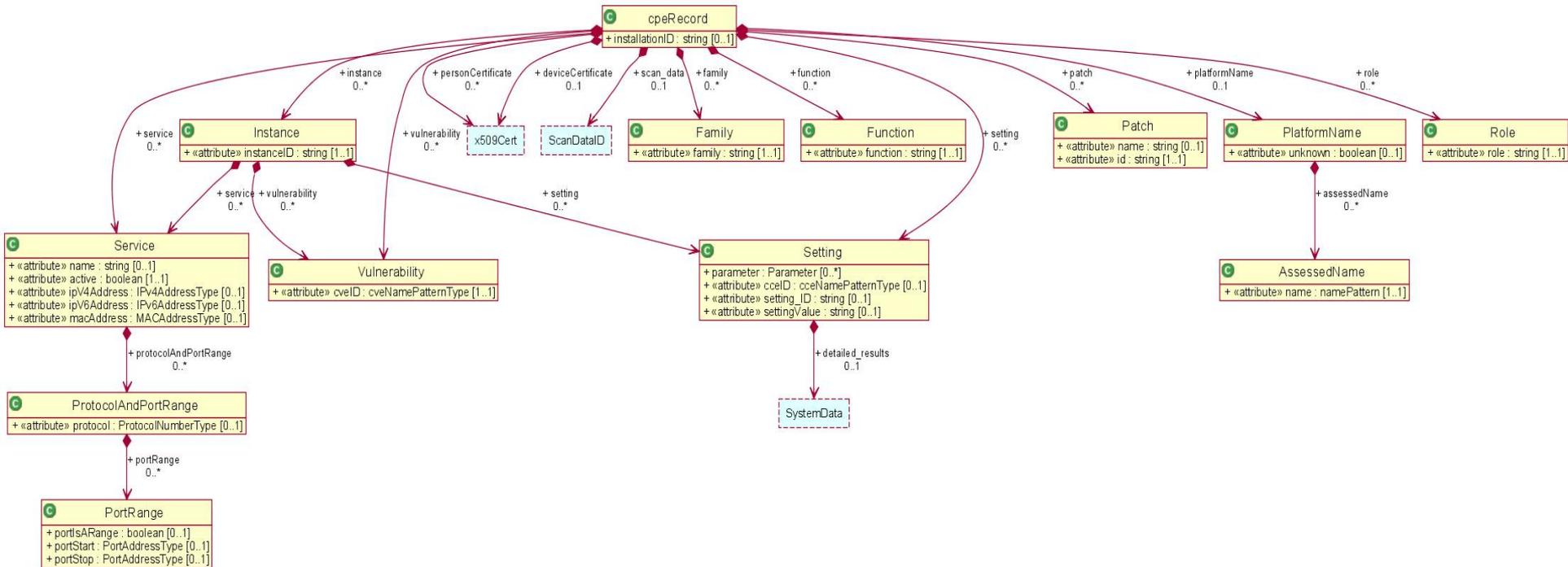


Device Record – The Key ARF Data Type

- 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*



Per Software Product Data (aka cpe-record)



Summary Results

When you just want a single question
answered

Summary Results Functionality

- Allows for Concise reports on single assessment checks
 - CPE platform definitions – For a CPE mask, how many devices have a matching CPE?
 - CVEs – Which devices have/don't have CVEs?
 - CCE parameters – How many/which devices have each parameter value?
 - OVAL Definitions - How many/which devices resolve to true or false for each OVAL def?
 - XCCDF Benchmarks
 - Average benchmark score, max score, min score, pass/fail
 - How many/which devices pass or fail each rule
 - Patches - How many/which devices have resolved to true or false for each patch?
- Provides results either as Counts and (optionally) Lists per finding
 - (true/false, pass/fail, not applicable, not checked, error)
 - Lists can include: IP, Domain Name, Record Identifier
- Plus population data and scan data

Sample – CPE Summary Report for cpe:/a:adobe:flash

```
<?xml version="1.0" encoding="UTF-8" ?>
<summRes:ResultsPackage xmlns:cia-enum="http://scap.nist.gov/schema/cia_enums/0.1"
  xmlns:cndc="http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41"
  xmlns:cpe="http://cpe.mitre.org/language/2.0" xmlns:p="http://scap.nist.gov/schema/cve/0.1"
  xmlns:scan_data="http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41"
  xmlns:summRes="http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41 summary_res.xsd
  http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41 cnd-core.xsd
  http://scap.nist.gov/schema/cia_enums/0.1 cia_enumerations.xsd http://cpe.mitre.org/language/2.0 cpe-language_2.0.xsd
  http://scap.nist.gov/schema/cve/0.1 cve_0.1.xsd http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41
  scan_data.xsd">
- <summRes:PopulationCharacteristics populationSize="250">
  <summRes:resource>http://cpeDb.dod.mil</summRes:resource>
</summRes:PopulationCharacteristics>
- <summRes:cpe>
  <!-- First line "platform" defines the CPE mask that is the basis of the CPE results report -->
  <summRes:platform>cpe:/a:adobe:flash</summRes:platform>
- <!--
  Each CPE Result item record gives a count and may provide a list of products that match the
  "platform" defined above. Also count/list of devices that don't have any products
  that match the platform mask.
  -->
- <summRes:cpeResultItem cpeFinding="true" platformName="cpe:/a:adobe:flash:1.02">
  <summRes:result count="50" />
</summRes:cpeResultItem>
- <summRes:cpeResultItem cpeFinding="true" platformName="cpe:/a:adobe:flash:1.05">
  <summRes:result count="50" />
</summRes:cpeResultItem>
- <summRes:cpeResultItem cpeFinding="true" platformName="cpe:/a:adobe:flash:1.20">
  <summRes:result count="100" />
</summRes:cpeResultItem>
- <summRes:cpeResultItem cpeFinding="false" platformName="cpe:/a:adobe:flash">
  <summRes:result count="50" />
</summRes:cpeResultItem>
</summRes:cpe>
</summRes:ResultsPackage>
```

Sample – Arbitrary XCCDF Benchmark with 1 Rule, Listed by IP Address, Ungrouped

```
<?xml version="1.0" encoding="UTF-8" ?>
<summRes:ResultsPackage xmlns:cia_enum="http://scap.nist.gov/schema/cia_enums/0.1" xmlns:cndc="http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41" xmlns:cpe="http://cpe.mitre.org/language/2.0" xmlns:cve="http://scap.nist.gov/schema/cve/0.1"
xmlns:scan_data="http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41"
xmlns:summRes="http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://metadata.dod.mil/mdr/ns/netops/net_defense/summary_res/0.41 summary_res.xsd
http://metadata.dod.mil/mdr/ns/netops/net_defense/cnd-core/0.41 cnd-core.xsd http://scap.nist.gov/schema/cia_enums/0.1 cia_enumerations.xsd
http://cpe.mitre.org/language/2.0 cpe-language_2.0.xsd http://scap.nist.gov/schema/cve/0.1 cve_0.1.xsd
http://metadata.dod.mil/mdr/ns/netops/shared_data/scan_data/0.41 scan_data.xsd">
- <summRes:PopulationCharacteristics populationSize="500000">
  <summRes:resource>DoDIAVMReportingdB</summRes:resource>
</summRes:PopulationCharacteristics>
- <summRes:benchmark profile="Gold">
- <summRes:benchMarkID>
  <cndc:resource>vms.dod.mil</cndc:resource>
  <cndc:record_identifier>winXPSTIGv2.53</cndc:record_identifier>
</summRes:benchMarkID>
<summRes:benchmarkStats aveScore="62.0" minScore="2.0" maxScore="93.0" minPassScore="62.3" scoreType="flat" />
<!-- Compliance lists and counts at the overall benchmark level -->
- <summRes:benchmarkComplianceItem benchmarkResultStatus="pass">
- <summRes:result count="375231">
  <summRes:deviceRecord record_identifier="asset1" ipv4Address="192.168.2.3" />
</summRes:result>
</summRes:benchmarkComplianceItem>
<!-- Compliance lists and counts at the individual rule level -->
- <summRes:ruleResult ruleID="rule1">
  <summRes:ident>CCE-20075-7</summRes:ident>
- <summRes:ruleComplianceItem ruleResult="pass">
- <summRes:result count="3">
  <summRes:deviceRecord record_identifier="asset1" ipv4Address="192.168.3.5" />
  <summRes:deviceRecord record_identifier="asset2" ipv4Address="192.168.3.7" />
  <summRes:deviceRecord record_identifier="asset3" ipv4Address="192.168.3.11" />
</summRes:result>
</summRes:ruleComplianceItem>
- <summRes:ruleComplianceItem ruleResult="fail">
- <summRes:result count="3">
  <summRes:deviceRecord record_identifier="asset4" ipv4Address="192.168.3.12" />
  <summRes:deviceRecord record_identifier="asset5" ipv4Address="192.168.3.13" />
  <summRes:deviceRecord record_identifier="asset6" ipv4Address="192.168.3.14" />
</summRes:result>
</summRes:ruleComplianceItem>
</summRes:ruleResult>
</summRes:benchmark>
</summRes:ResultsPackage>
```

ARCAT

When you have a bunch of ARFs and want to look at and evaluate them

Assessment Results Consumer & Analysis Tool (ARCAT)

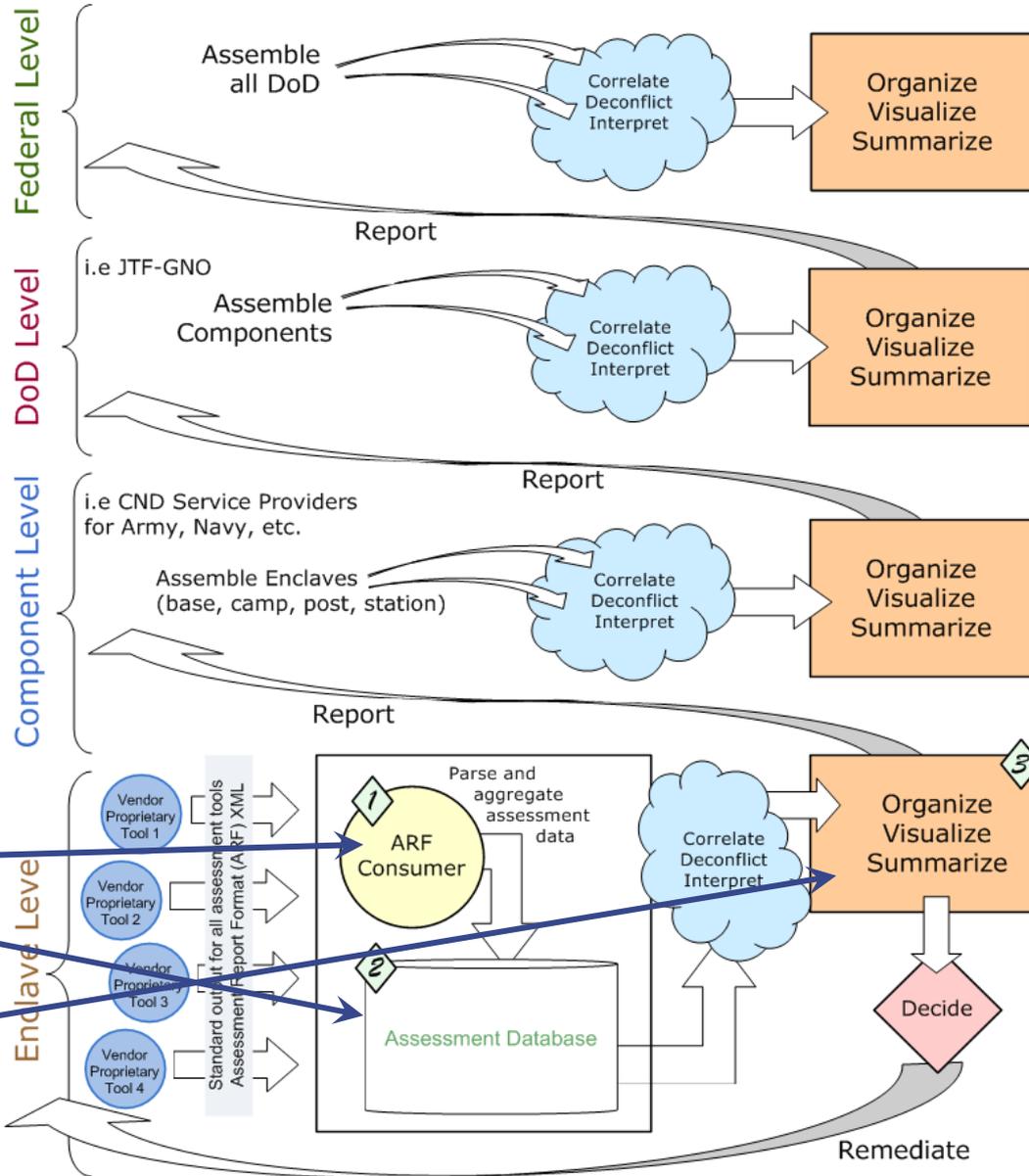
Status

- ARCAT development began in June 09
 - Reference implementation of standard for device data reporting -
- Assessment Results Format (ARF)
 - ARCAT is a generic ARF consumer (i.e. not a sensor, a sensor output data collection capability)
 - Used for reporting compliance with FDCC, STIG, IAVA, and CTO
 - Used for collecting inventories of devices and installed applications/OS
 - May serve as basis for multi-sensor network assessment data fusion capability
 - Source code to be made available within DoD and can be shared across US Government

Vision

DoD Network Configuration Management Process Vision

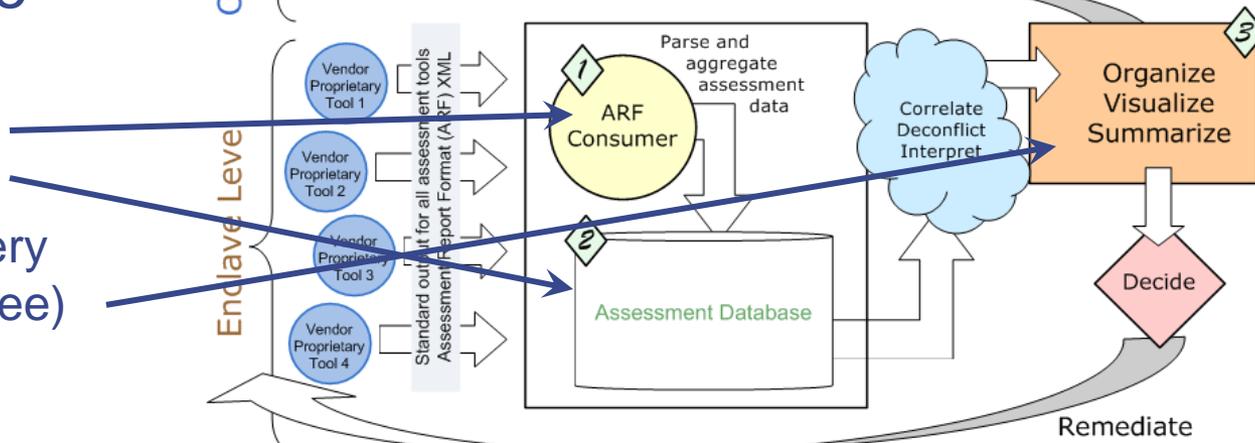
Assess - Report - - - Consume & Aggregate - - - Correlate - Organize/Visualize



Assess - Report - - - Consume & Aggregate - - - Correlate - Organize/Visualize

ARCAT Spiral One

- 1) Consumer
- 2) Repository
- 3) GUI (to a very limited degree)



CND R&T Reference Implementation of the Assessment Results Consumer & Analysis Tool

Manage Your Attributes

Name	Location	CNDSP	Owning Service	Owning Unit	Admin Unit and POC	
Cool Group	Airport Square	Pentagon J6	Navy	Navy HQ J6		
AOR:	Reg:	DoD NW:	NW:	CCSD:	Circuit:	
Class: CTS-BALK	MAC: 1	Confidentiality: Classified	FIPS 199 Confidentiality: H Integrity: H Availability: H			
Not POR Managed	System Affiliations:		Functions:			
Roles:						
Joe's Group	Chik fil A	USAF	USAF	USAF	POC: Wolfkiel, J	
AOR: AFRICOM	Reg: West Africa	DoD NW: NIPRNET	NW: Internet	CCSD:	Circuit:	
Class: U	MAC: 2	Confidentiality: Classified	FIPS 199 Confidentiality: L Integrity: L Availability: L			
Not POR Managed	System Affiliations:		Functions: Lab Network			
Roles: Testing						
Management	FANX3	Navy HQ J6	Navy	Monterey NPS	Monterey NPS	
AOR: Pacific	Reg:	DoD NW: SIPRNET	NW:	CCSD: IJSNDF	Circuit:	
Class: U	MAC: 3	Confidentiality: Sensitive	FIPS 199 Confidentiality: H Integrity: L Availability: M			
POR Managed	System Affiliations: CNDSP Pacific		Functions:			
Roles:						
R and D	Five Guys	Monterey NPS	Army	Army		
AOR:	Reg:	DoD NW:	NW:	CCSD:	Circuit:	
Class: NS-S	MAC:	Confidentiality:	FIPS 199 Confidentiality: Integrity: H Availability:			
POR Managed	System Affiliations:		Functions:			
Roles:						
UNCLAS Email	FANX3	Navy	Pentagon J6	Navy	Navy	
AOR: CONUS	Reg: Mid Atlantic	DoD NW: NIPRNET	NW: COMCAST	CCSD: AXNKL	Circuit: Fiber	
Class: C	MAC: 2	Confidentiality: Public	FIPS 199 Confidentiality: L Integrity: L Availability: L			
Not POR Managed	System Affiliations:		Functions: Email Support			
Roles: System Admin						

Total Operational Attributes: 5

Provides ability to associate devices with operational/environmental information
 – e.g. Where is it, who owns it, who defends it, what network is it on, how important is it, etc.. (see example – above)

CND R&T Reference Implementation of the Assessment Results Consumer & Analysis Tool

Device List

Group Role Function Status 1 2 3 4 5 6 7

Op Att	Group	Host Name	IP Address	MAC Address	Role	Function	Status
R and D		mirage.acme.corp.net	10.1.3.126	A0:EE:05:1D:43:42			true
R and D		mbddev.acme.corp.net	10.1.3.129	01:44:6B:36:B3:8C			true
R and D		ksrealtimedev.acme.corp.net	10.1.3.137	11:33:2A:17:47:23			true
R and D		precision.acme.corp.net	10.1.3.139	11:2D:34:58:69:00			true
R and D		weblogic10	10.1.3.150	00:1D:3A:55:75:96			true
R and D		temporaryspare.acme.corp.net	10.1.3.151	10:10:A0:1A:C8:ED			true
R and D		viggen.acme.corp.net	10.1.3.154	11:23:2A:6D:23:BC			true
R and D		gunner.acme.corp.net	10.1.3.155	01:1C:29:16:1D:3A			true
R and D		tomahawk.acme.corp.net	10.1.3.156				true
R and D		acme-desktop-4	10.1.3.158	37:2D:09:EA:7A:0A			true
R and D		martinsville.acme.corp.net	10.1.3.198	00:26:CD:A7:E7:D7			true
R and D			10.1.3.247	00:1B:C9:2A:25:3F			true
R and D		docmanager.acme.corp.net	10.1.3.248	00:1D:56:28:BD:E2			true
R and D		redmine.acme.corp.net	10.1.3.250	00:0D:2A:3C:A7:08			true
R and D		svn.acme.corp.net	10.1.3.252	00:1D:3A:79:AA:CD			true
R and D		corporate-nas.acme.corp.net	10.1.3.254	01:1E:B3:10:6D:86			true
R and D		jones-pc.acme.corp.net	10.1.4.100				true
R and D		ARCAT01	10.1.4.50	00:00:00:00:00:00	role0	function0	true
			0:0:0:0:0:0:0	00:00:00:00:00:00			
			0:0:0:0:0:0:0	00:00:00:00:00:00			
UNCLAS Email		WHITELIST-DB	64.124.158.104	00:1A:4B:34:DD:C2			true

Shows device information collected from all sensors and any environmental information associated – supports “clickable” drill down for any device

CND R&T Reference Implementation of the Assessment Results Consumer & Analysis Tool

Device Detail

general	network	software	test results	oval results	scan data
Resource:	hbss-dev.dev.boozallenet.com	Record ID:	8B8DFE6A-1230-47C7-8184-1D02CD22D9DF		
Domain:	HBSS	Host Name:	HBSS6		
GUID:		OS:			
IP Address:	64.124.158.213	MAC Address:	00:0C:29:2E:14:5E		
Composes:		Composed Of:			
Op Att Group:	UNCLAS Email	TPM:			
Role:		Function:			
Status Attributes					
Timestamp:	01 Oct 2009 11:30:58A	Status:	true	Confidence:	1.00
Source:		Version:			
Check Ref:		Check Source:			
Tagged Values					
CPUSpeed:	2388MHz	CPUType:	Intel(R) Xeon(TM) CPU 2.40GHz		
McAfee ePO Agent GUID:	8B8DFE6A-1230-47C7-8184-1D02CD22D9DF	OSBuildNum:	3790		
McAfee ePO Managed:	True	OStype:	Windows 2003		
OSServicePackVer:	Service Pack 2				
OSVersion:	5.2				

Shows device detail that can be packaged in standard ARF device inventory or compliance fields.

CND R&T Reference Implementation of the Assessment Results Consumer & Analysis Tool

Device Detail

general

network

software

test results

oval results

scan data

Home

Review

list

search

summary

results

Manage

attributes

locations

orgs

people

Installation ID:

CPE: **Unknown**

CVEs: **CVE-2003-9161**

Settings: **No Settings**

Services:

Name
unknown

Active
Yes

IP Address

MAC Address

Protocol [Ports]

**TCP[22,80,427,443,902,5989]|UDP
[0,427]**

Roles: **No Roles**

Functions: **No Functions**

Families: **No Families**

Patches: **No Patches**

Status Attributes

Timestamp: **01 Oct 2009 11:31:06A**

Status: **true**

Confidence: **1.00**

Source:

Version:

Check Ref:

Check Source:

Tagged Values

No tagged values

Combines installed software descriptions, plus any vulnerabilities, settings, patches, services, and open ports/protocols associated.

CND R&T Reference Implementation of the Assessment Results Consumer & Analysis Tool

Device Detail

general	network	software	test results	oval results	scan data
Test:	Windows-Server-2003-DC-deviations	Start:	End: 14 Sep 2009 10:05:42A		
System:	Secutor Magnus	Ver:	2.0.4	ID:	
Benchmark:	SCAP-Win2003-DC-XCCDF-Beta-v3.xml	Profile:	Domain-Controller-Enterprise-Moderate		
Identity:		Authenticated:	True	Privileged:	True
Score	System	Maximum			
67.6000000000					
Rule	Ident	Result	Severity	Timestamp	
AccountLockoutDuration	CCE-Winv2.0-235[http://cce.mitre.org]	fail		09:42:18A	
AccountLockoutReset	CCE-Winv2.0-234[http://cce.mitre.org]	fail		09:42:18A	
AccountLockoutThreshold	CCE-Winv2.0-236[http://cce.mitre.org]	fail		09:42:18A	
AdministratorsGroupObjectCr...	CCE-Winv2.0-421[http://cce.mitre.org]	fail		09:42:17A	
AlerterService	CCE-Winv2.0-270[http://cce.mitre.org]	pass		09:42:17A	
AllowICMPRedirectsDisabled	CCE-Winv2.0-352[http://cce.mitre.org]	fail		09:42:17A	
AllowLogOnLocally-Administr...	CCE-Winv2.0-215[http://cce.mitre.org]	fail		09:42:17A	
AllowLogOnThroughTerminalSe...	CCE-Winv2.0-229[http://cce.mitre.org]	fail		09:42:17A	
AllowServerOperatorsToSched...	CCE-Winv2.0-384[http://cce.mitre.org]	fail		09:42:18A	
AllowUndockWithoutLogin	CCE-Winv2.0-424[http://cce.mitre.org]	fail		09:42:18A	
AlwaysDigitallyEncryptSecur...	CCE-Winv2.0-414[http://cce.mitre.org]	pass		09:42:18A	
AnonymousEnumerationOfAccounts	CCE-Winv2.0-333[http://cce.mitre.org]	pass		09:42:17A	
AnonymousEnumerationOfAccou...	CCE-Winv2.0-332[http://cce.mitre.org]	fail		09:42:17A	
AnonymousUsersPermissions	CCE-Winv2.0-432[http://cce.mitre.org]	pass		09:42:17A	
arp.exePermissions	CCE-Winv2.0-60[http://cce.mitre.org]	fail		09:42:18A	

Shows compliance with any XCCDF checklist – e.g. FDCC, STIG, IAVM, CTO

CND R&T Reference Implementation of the Assessment Results Consumer & Analysis Tool

Search Your Collection

Search for:

CPE or CVE or IP Address

or IP Address Range: from to

Filter by:

Owning Unit Admin POC Location

Home

Review

list

search

summary

results

Manage

attributes

locations

orgs

people

Supports search for common data elements reported in ARF.

CND R&T Reference Implementation of the Assessment Results Consumer & Analysis Tool

Test Results

- Home
- Review
- list
- search
- summary
- results**
- Manage
- attributes
- locations
- orgs
- people

Test Result/Benchmark	Profile/Scoring System	Scores	Average	Best	Worst	
id27 http://www.oxygenxml.com/	idref0 http://www.oxygenxml.com/	6	0.00	0.00	0.00	▼
Windows-Server-2003-DC-deviations SCAP-Win2003-DC-XCCDF-Beta-v3.xml	Domain-Controller-Enterprise-Moderate	7	74.09	88.00	54.00	▲
HostName	IP	MAC	Owning Unit	Admin POC		
1) W2K3SERVER	192.168.3.139					
2) HBSS6	64.124.158.213	00:0C:29:2E:14:5E	Navy	Johnson, Jon		
3) HBSS1	64.124.158.188	00:0C:29:E6:0C:E8	Navy	Johnson, Jon		
4) HBSS4	64.124.158.215	00:50:56:AC:71:50	Navy	Johnson, Jon		
5) HBSS-DOMAIN	64.124.158.210	00:50:56:AC:7C:C5	Navy	Johnson, Jon		
6) HBSS2	64.124.158.211	00:50:56:AC:32:04	Navy	Johnson, Jon		
7) HBSS9	64.124.158.219	00:0C:29:DB:33:42	Navy	Johnson, Jon		
Rule	Devices	Pass	Fail	Error	Unknown	Other
1) AccountLockoutDuration	7	3	3	0	0	1
2) AccountLockoutReset	7	3	3	1	0	0
3) AccountLockoutThreshold	7	4	2	1	0	0
4) AdministratorsGroupObjectCreator...	7	3	4	0	0	0
5) AlerterService	7	6	1	0	0	0
6) AllowICMPRedirectsDisabled	7	4	3	0	0	0
7) AllowLogOnLocally-Administrators...	7	3	4	0	0	0
8) AllowLogOnThroughTerminalService...	7	2	4	0	0	0
9) AllowServerOperatorsToScheduleTasks	7	1	6	0	0	0
10) AllowUndockWithoutLogin	7	3	4	0	0	0
11) AlwaysDinitallyEncryptSecureChan	7	1	5	1	0	0

Provides summarized roll-up for decision maker-level situational awareness.

Why ARCAT?

- Serves as reference implementation to ensure ARF provided by tools is valid
- Acts as development platform to do proof-of-concept for vendor discussions
- Allows for testing of bandwidth, processing, and implementation of new reporting capabilities
- Serves as surrogate network sensor central collection point pending commercial availability

When?

- Spiral 1 of ARCAT is complete and can be accessed by DoD personnel on DKO at the CND Architecture Web Site
- Has been distributed internal to DoD as development platform/sample implementation
 - DISA VMS
 - Navy NRL
 - Others
- Can share with other organizations, but...
 - Not ready for deployment as finished product
 - Not locked down in “STIG’d” mode
 - No promises on scalability or stability
 - Will request memo documenting limited liability/terms of use

POC

- Lt Col Joe Wolfkiel
e-mail: jlwolfkiel@nsa.gov
phone: 410-854-5401