



Defense Information Systems Agency

A Combat Support Agency

DoD Secure Configuration Management (SCM) Operational Use Cases

**DISA PEO-MA
Computer Network Defense Enclave Security
26 September 2010**



This brief contains references to U.S. Government military capabilities that may not be authorized for release to foreign governments. Mention of these capabilities in no way implies that the U.S. Government will release or consider release of them, or of any additional associated classified or unclassified information pertaining to them. This brief may also contain references to U.S. Government future plans and projected system capabilities. Mention of these plans or capabilities in no way guarantees that the U.S. Government will follow these plans or that any of the associated system capabilities will be available or releasable to foreign governments.



Agenda

- **SCM BLUF**
- **SCM Goals**
- **SCM Lifecycle**
- **SCM Portfolio**
- **Lifecycle Capabilities**
- **Example use case (HBSS – VMS – eMASS Integration)**
- **Backup Slides**



Bottom Line Up Front

- **DISA PEO-MA stands committed to provide IA solutions through adaptive, automated, and multitier mechanisms, together, Enclave & Host Security (EHS) and Secure Configuration Management (SCM) will provide an unprecedented enclave level of compliance checking, situational awareness and improved security protections for the war fighter**
- **SCM is a lifecycle methodology providing the integration and optimization of enterprise IA applications and tools to provide an automated and comprehensive process for risk management and valued mitigation.**
 - **SCM delivers capabilities to enable dynamic continuous monitoring, enterprise risk measurement and awareness**
- **Simply put SCM is:**
 - **Configuring assets securely in the first place**
 - **Maintaining secure configuration**
 - **Providing continuous situational awareness to the right people**



Current SCM Capabilities

- **Disconnected, autonomous tools**
- **Manual scans**
- **Manual reporting**
- **Manual re-entry**
- **Time consuming**
- **No enterprise view of risk**

Labor Intensive processes do not achieve effective end-to-end risk management



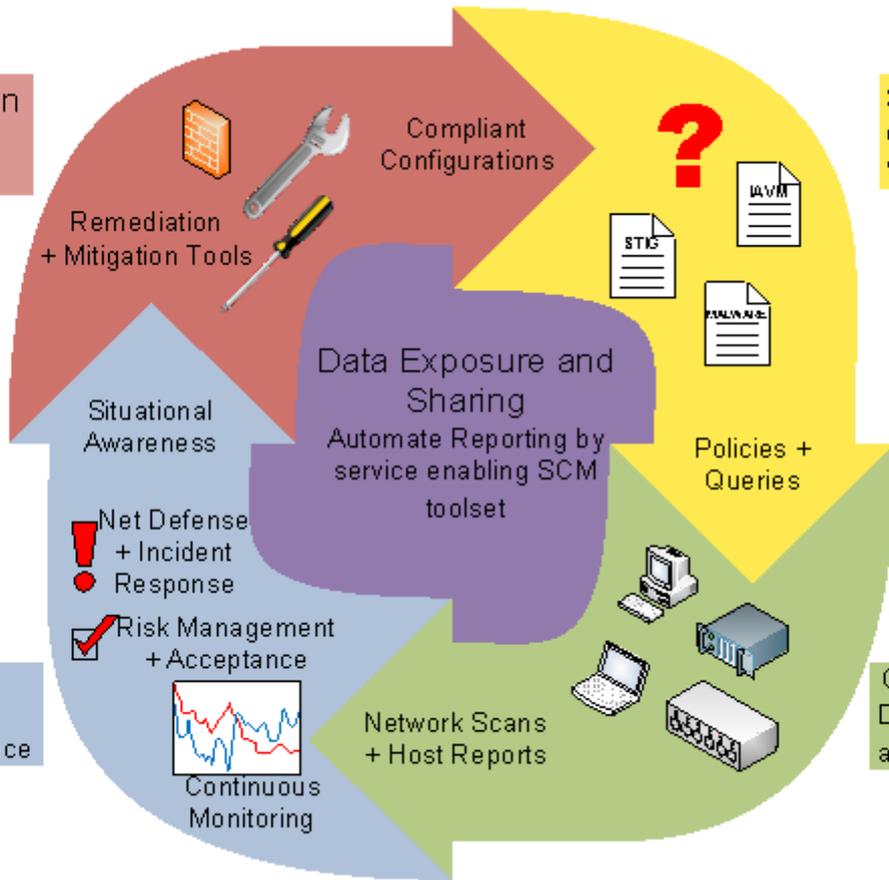
Secure Configuration Management (SCM) Goals

- Leverage **all available capability** from **existing enterprise tools**
- **Listen** to the network operators and defenders for **requirements**
- **Reduce operator burden** (Machine to Machine...)
- Deliver **actionable results** to improve DoD security readiness/awareness (e.g., Risk Scoring)
- Provide **continuous** and on demand **situational awareness** to all levels (e.g., Continuous Monitoring)
- Utilize **Net-Centric services** and **data standards** (e.g., SCAP, CND Data Standards, NCES JUM)

Influence and change DoD culture, capability, and conduct to maintain secure, operational, and mission-ready systems

SCM Lifecycle

Configuration Risk Mitigation
Allow for the remediation of non-secure configurations



Security Content Management
Create and distribute content for vulnerability and configuration tools

Security State Analysis
Assess risk by correlating asset attributes and compliance evidence

Configuration Discovery and Detection
Discover and audit assets with standardized, automated tools



- Security Content Management

- Automatable STIG Publication (Operational)
- Antivirus/Antispyware (Operational)
- IAVM System (FY11Q2)
- Digital Policy Management Solution (DPMS) (Planning)



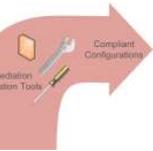
- Configuration Discovery and Detection

- Host Based Security System (HBSS) – RSD, PA, OAM (Operational)
- Assured Compliance Assessment Solution (ACAS) (FY11)
- Secure Configuration Compliance Validation Initiative (SCCVI) (Operational)
- Enterprise Network Mapping and Leak Detection Solution (ENMLDS) (Piloting)
- Asset Configuration Compliance Module (ACCM) (FY11)



- Security State Analysis

- Vulnerability Management System (VMS) (Operational)
- Enterprise Mission Assurance Support Service (eMASS) (Operational)
- Continuous Monitoring and Risk Scoring (CMRS) (Piloting)



- Configuration Risk Mitigation

- Patch Management, WSUS (Operational)
- Remediation Manager (FY11-12)



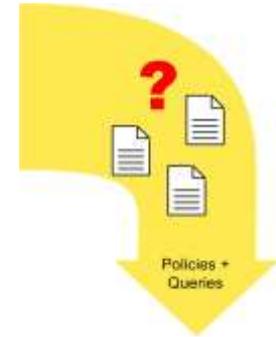
- SCM Data Exposure and Sharing

- Asset Publishing Service (APS) (Operational)



Security Content Management

- **STIG**
 - CCE, CVE, CCSS, CVSS, OVAL, OCIL
- **IAVM**
 - CVE, CVSS, OVAL, OCIL
- **AV/AS Updates**
- **Patches**
- **HIPS signatures**





Configuration Discovery and Detection

- **HBSS ePO**
 - ePO Agent
 - Asset IDs
 - **HBSS Policy Auditor (PA)**
 - Agent-based assessment for CCE/CVE Compliance
 - **HBSS Operational Attribute Module (OAM) [GOTS]**
 - Host ID, FQDN, IP, MAC, Subnet, Mission Assurance Category, Confidentiality, Owing Org, Administering Org, Location, System Affiliation, AOR, Region, Network, Unit
 - **HBSS Asset Configuration Compliance Module (ACCM) [GOTS]**
 - Installed Application Inventory
- **Asset Compliance Assessment Solution (ACAS)**
 - Network-based vulnerability scanner
- **Enterprise Network Mapping and Leak Detection Solution (ENMLDS)**
 - Network discovery/crawl (logical assets relationships)

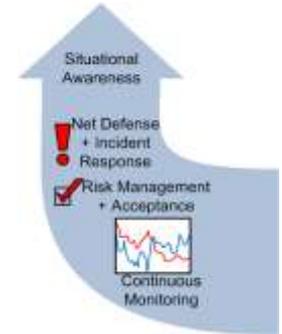




Security State Analysis

- VMS [GOTS]
- eMASS [GOTS]
- CMRS (Pilot PRSM/ARCAT) [GOTS]
- IAVM System [GOTS]

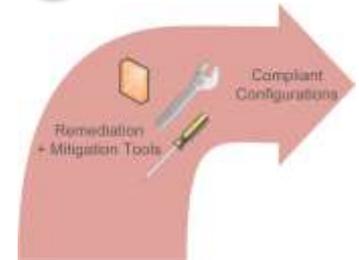
- Inputs
 - CVSS
 - CCSS
 - NSA Threat Scoring
 - NVD Feeds





Configuration Risk Mitigation

- **CMRS (future) [GOTS]**
 - Prioritize Fixes
- **WSUS**
- **Global Content Distribution Service (GCDS) Patch Server**





Data Exposure and Sharing

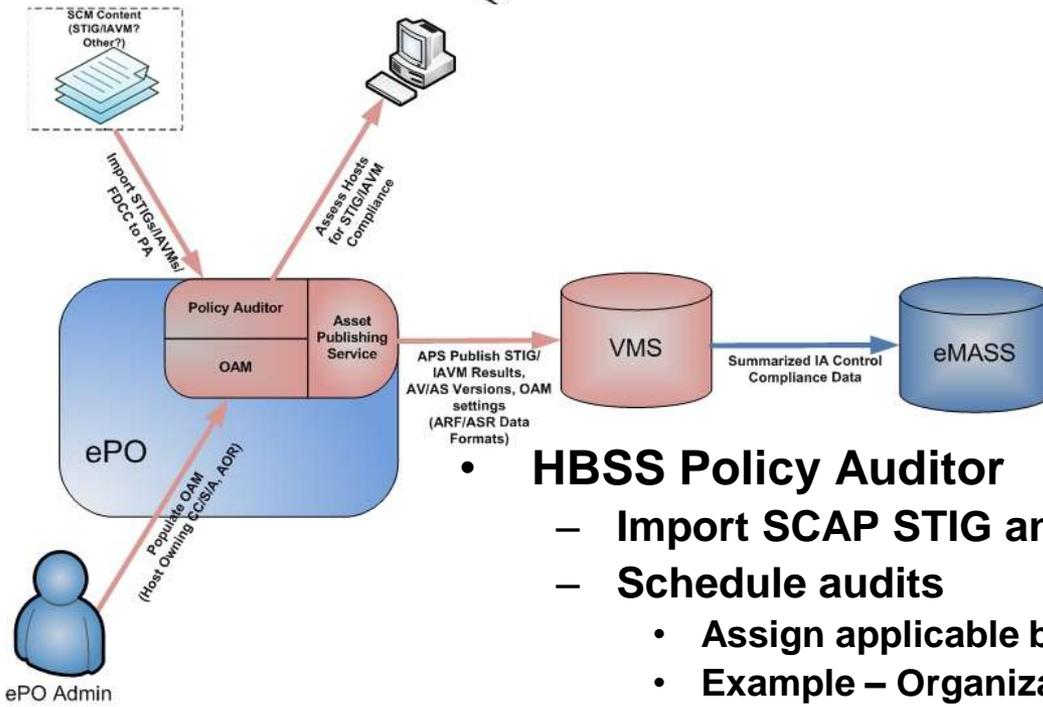
- **HBSS APS (Asset Publishing Service) [GOTS]**
 - Publish HBSS Events, ePO Assets, PA Results
- **PEO-MA Reference JUM Client [GOTS]**
 - Subscribe, Consume, Publish
- **JUM (NCES Joint User Messaging BUS)**
 - WS-Notification - Standard
- **Data Standards**
 - ARF
 - ASR
 - XCCDF





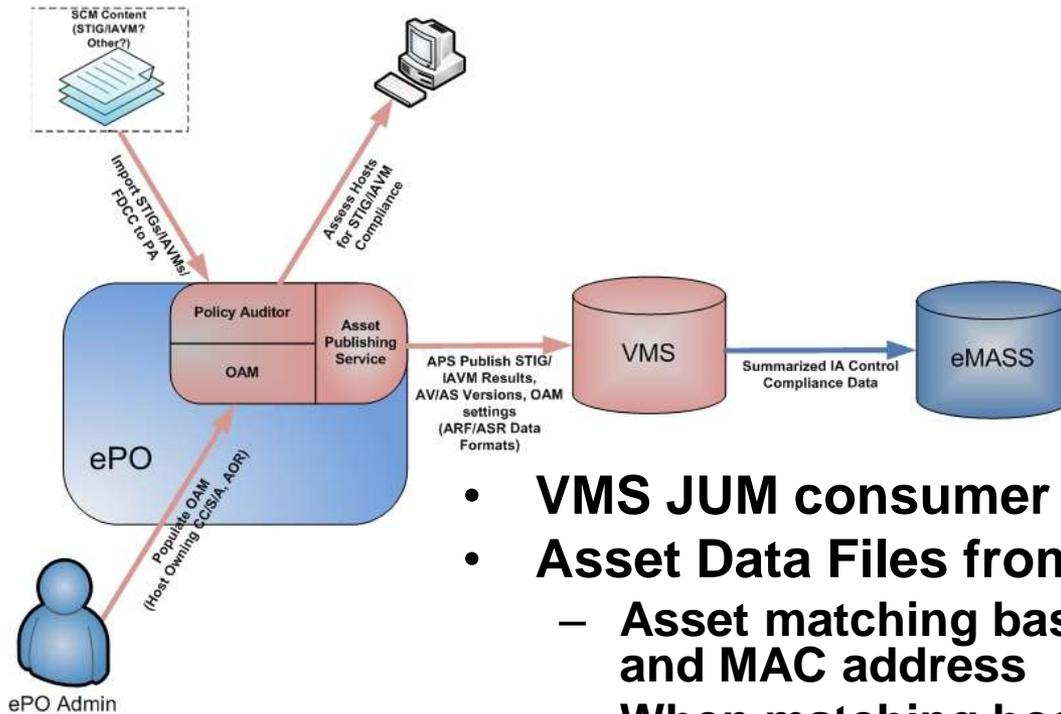
Example Use Case: Use HBSS to update vulnerability status in VMS and support accreditation decisions in eMASS using machine to machine integration with VMS

HBSS Host Audit Overview



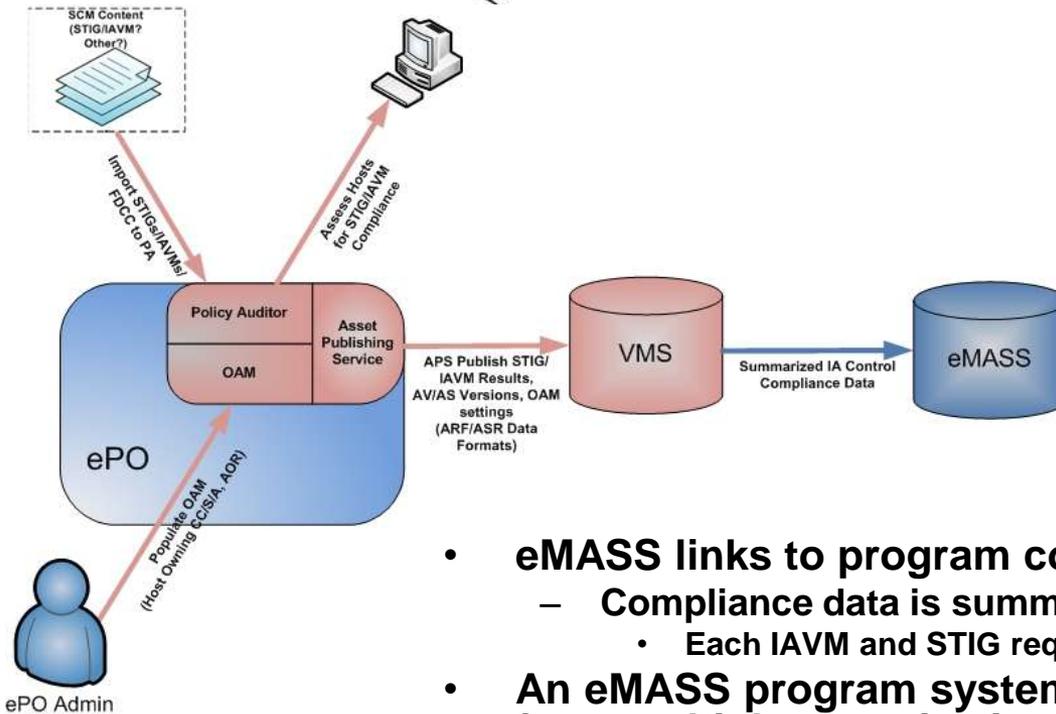
- **HBSS Policy Auditor**
 - Import SCAP STIG and IAVM benchmarks
 - Schedule audits
 - Assign applicable benchmarks to ePO-managed hosts
 - Example – Organization Group of XP Workstations is assigned IAVM benchmarks and XP STIG
- **HBSS Asset Publishing Service (APS)**
 - Configure APS to publish asset events, asset data, and assessment summary results
 - Configure number of assets to include in each data file
 - Configure for publication time and publication frequency

VMS Overview



- **VMS JUM consumer runs every 15 minutes**
- **Asset Data Files from HBSS APS process**
 - Asset matching based on Host name, IP Address, and MAC address
 - When matching host found, ePO agent GUID is added to VMS asset record
- **Assessment Summary Results**
 - Each matching GUID and SCAP benchmark rule id is searched for in VMS and updated when a match is found

eMASS Overview



- **eMASS links to program compliance data in VMS**
 - Compliance data is summarized using IA Control
 - Each IAVM and STIG requirement maps to an IA Control
- **An eMASS program system can be linked to program data from multiple organizations or locations in VMS**
 - Example, HBSS POR in eMASS can be linked to eMASS baseline or eMASS baseline and multiple deployed instances of eMASS if assets in VMS are defined as HBSS system assets
- **eMASS and VMS links require the eMASS user to have an account in VMS with appropriate permissions to target program systems**
- **eMASS VMS data can be refreshed by anyone with permissions in eMASS at any time**



Example Assessment Summary Data from HBSS

XP STIG Results

```

<ns7:resource>STIG.DOD.MIL</ns7:resource>
<ns7:record_identifier>Windows_XP</ns7:record_identifier>
</ns30:benchmarkID>
- <ns30:ruleResult ruleID="SV-3376r8_rule">
- <ns30:ruleComplianceItem ruleResult="pass">
  - <ns30:result count="10">
    <ns30:deviceRecord record_identifier="D51A5587-E97C-40F6-9D5D-F2A164923C2E" />
    <ns30:deviceRecord record_identifier="6E057995-367D-4E84-B4BA-356561140D71" />
    <ns30:deviceRecord record_identifier="E8E7CABB-B25C-4249-B100-6E68312DCD95" />
    <ns30:deviceRecord record_identifier="250D4E74-7525-4E81-BDD7-D035D2D7F3D4" />
    <ns30:deviceRecord record_identifier="FAF354A0-4937-44A1-BF58-7E14FDA70BE0" />
    <ns30:deviceRecord record_identifier="2B29E565-3659-4342-A127-3485B060FB58" />
    <ns30:deviceRecord record_identifier="40A7D85D-6310-40A6-921D-E95DE811A5C2" />
    <ns30:deviceRecord record_identifier="0B074EB4-D288-4E1E-A30F-B41004A426E5" />
    <ns30:deviceRecord record_identifier="A3AEF908-9EBA-49CC-9BE7-C2DB90E688C0" />
    <ns30:deviceRecord record_identifier="F70140D5-BCBE-485E-8D6B-3593D0D109A9" />
  </ns30:result>
</ns30:ruleComplianceItem>
</ns30:ruleResult>
- <ns30:ruleResult ruleID="SV-14839r4_rule">
- <ns30:ruleComplianceItem ruleResult="pass">
  - <ns30:result count="10">
    <ns30:deviceRecord record_identifier="D51A5587-E97C-40F6-9D5D-F2A164923C2E" />
    <ns30:deviceRecord record_identifier="6E057995-367D-4E84-B4BA-356561140D71" />
    <ns30:deviceRecord record_identifier="E8E7CABB-B25C-4249-B100-6E68312DCD95" />
    <ns30:deviceRecord record_identifier="250D4E74-7525-4E81-BDD7-D035D2D7F3D4" />
    <ns30:deviceRecord record_identifier="FAF354A0-4937-44A1-BF58-7E14FDA70BE0" />
    <ns30:deviceRecord record_identifier="2B29E565-3659-4342-A127-3485B060FB58" />
    <ns30:deviceRecord record_identifier="40A7D85D-6310-40A6-921D-E95DE811A5C2" />
    <ns30:deviceRecord record_identifier="0B074EB4-D288-4E1E-A30F-B41004A426E5" />
    <ns30:deviceRecord record_identifier="A3AEF908-9EBA-49CC-9BE7-C2DB90E688C0" />
  </ns30:result>
  </ns30:ruleComplianceItem>
</ns30:ruleResult>

```

STIG Requirement

Pass/Fail Status

Hosts with that compliance status

IAVM Results

```

<ns7:resource>IAVM.DOD.MIL</ns7:resource>
<ns7:record_identifier>IAVM_2010</ns7:record_identifier>
</ns30:benchmarkID>
- <ns30:ruleResult ruleID="IAVM2010B0020">
- <ns30:ruleComplianceItem ruleResult="pass">
  - <ns30:result count="10">
    <ns30:deviceRecord record_identifier="F70140D5-BCBE-485E-8D6B-3593D0D109A9" />
    <ns30:deviceRecord record_identifier="250D4E74-7525-4E81-BDD7-D035D2D7F3D4" />
    <ns30:deviceRecord record_identifier="A3AEF908-9EBA-49CC-9BE7-C2DB90E688C0" />
    <ns30:deviceRecord record_identifier="2B29E565-3659-4342-A127-3485B060FB58" />
    <ns30:deviceRecord record_identifier="40A7D85D-6310-40A6-921D-E95DE811A5C2" />
    <ns30:deviceRecord record_identifier="D51A5587-E97C-40F6-9D5D-F2A164923C2E" />
    <ns30:deviceRecord record_identifier="0B074EB4-D288-4E1E-A30F-B41004A426E5" />
    <ns30:deviceRecord record_identifier="FAF354A0-4937-44A1-BF58-7E14FDA70BE0" />
    <ns30:deviceRecord record_identifier="6E057995-367D-4E84-B4BA-356561140D71" />
    <ns30:deviceRecord record_identifier="E8E7CABB-B25C-4249-B100-6E68312DCD95" />
  </ns30:result>
</ns30:ruleComplianceItem>
</ns30:ruleResult>
- <ns30:ruleResult ruleID="IAVM2010B0005">
- <ns30:ruleComplianceItem ruleResult="pass">
  - <ns30:result count="10">
    <ns30:deviceRecord record_identifier="F70140D5-BCBE-485E-8D6B-3593D0D109A9" />
    <ns30:deviceRecord record_identifier="250D4E74-7525-4E81-BDD7-D035D2D7F3D4" />
    <ns30:deviceRecord record_identifier="A3AEF908-9EBA-49CC-9BE7-C2DB90E688C0" />
    <ns30:deviceRecord record_identifier="2B29E565-3659-4342-A127-3485B060FB58" />
    <ns30:deviceRecord record_identifier="40A7D85D-6310-40A6-921D-E95DE811A5C2" />
    <ns30:deviceRecord record_identifier="D51A5587-E97C-40F6-9D5D-F2A164923C2E" />
    <ns30:deviceRecord record_identifier="0B074EB4-D288-4E1E-A30F-B41004A426E5" />
    <ns30:deviceRecord record_identifier="FAF354A0-4937-44A1-BF58-7E14FDA70BE0" />
  </ns30:result>
  </ns30:ruleComplianceItem>
</ns30:ruleResult>

```

Hosts with that compliance status

IAVM ID



VMS XP Asset Finding Counts Before/After

New VMS XP Asset (Before HBSS Data Import)

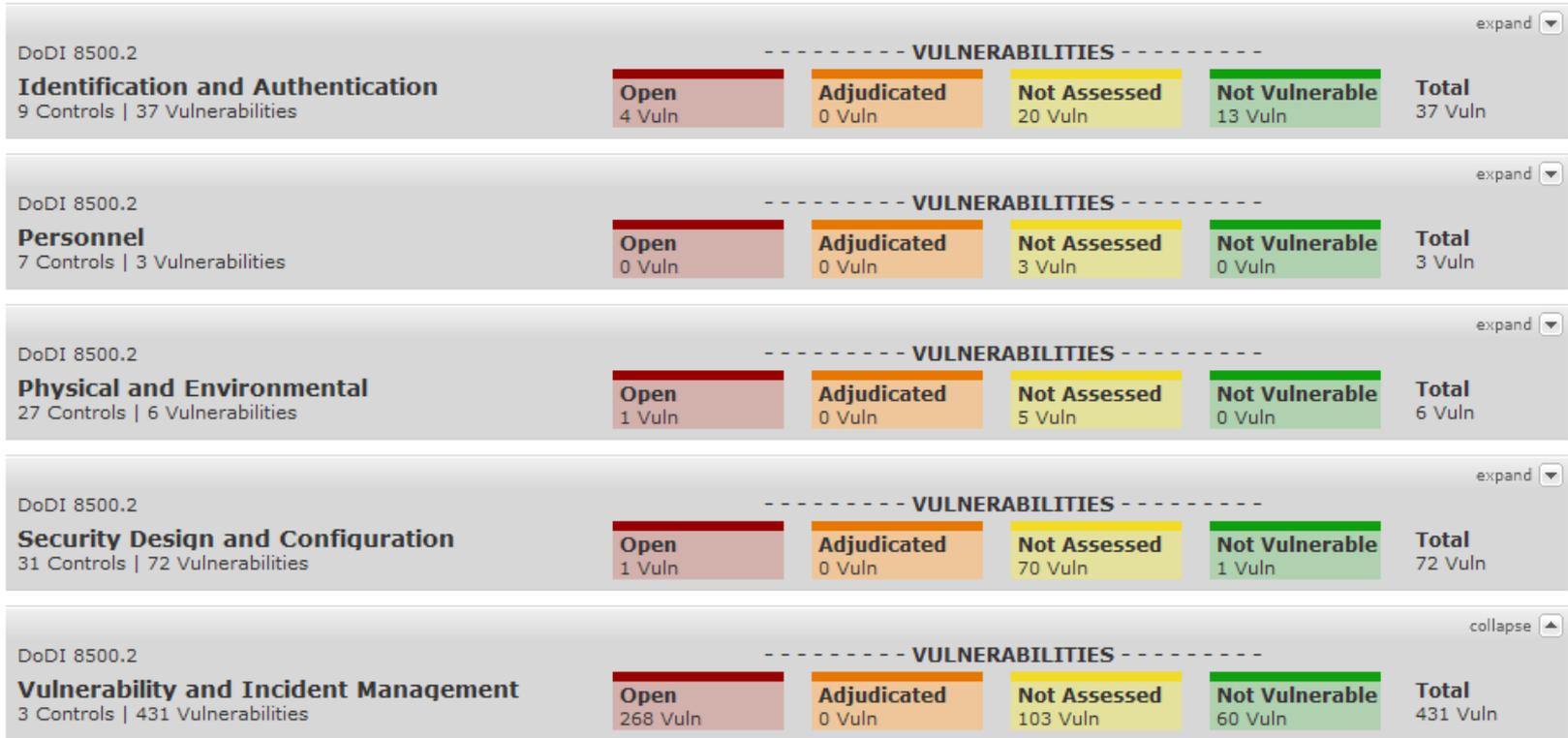
by Location	Severity	Total	Total Open	NU	WDA	ARQ	MS	ADA	ARA	ARJ	NR	MR	D	MA	DRA	F	NF
Desktop Application - General	Category I	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Category II	5	0	0	0	0	0	0	0	0	5	0	0	0	0	0	0
	Category III	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Category IV	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Total	5	0	0	0	0	0	0	0	0	5	0	0	0	0	0	0
Windows XP	Category I	250	178	10	0	168	0	0	0	0	72	0	0	0	0	0	0
	Category II	387	149	17	0	132	0	0	0	0	238	0	0	0	0	0	0
	Category III	76	0	0	0	0	0	0	0	0	76	0	0	0	0	0	0
	Category IV	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Total	713	327	27	0	300	0	0	0	0	386	0	0	0	0	0	0

Same VMS XP Asset (After HBSS Data Import)

by Location	Severity	Total	Total Open	NU	WDA	ARQ	MS	ADA	ARA	ARJ	NR	MR	D	MA	DRA	F	NF
Desktop Application - General	Category I	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Category II	5	0	0	0	0	0	0	0	0	5	0	0	0	0	0	0
	Category III	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Category IV	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Total	5	0	0	0	0	0	0	0	0	5	0	0	0	0	0	0
Windows XP	Category I	250	167	10	0	157	0	0	0	0	62	0	0	0	0	12	9
	Category II	387	127	15	0	112	0	0	0	0	177	0	0	0	0	46	37
	Category III	76	14	0	0	14	0	0	0	0	41	0	0	0	0	0	21
	Category IV	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	Total	713	308	25	0	283	0	0	0	0	280	0	0	0	0	58	67



Example eMASS “Vulnerability Data” Dashboard



Control Acronym	VMS Organization	Control Status	Highest Severity Category	Open	Adjudicated	Not Assessed	Not Vulnerable	Total
VIIR-1	SCM Test SCM Test	NCUO		0	0	0	0	0
VIIR-2	SCM Test SCM Test			0	0	0	0	0
VIVM-1	SCM Test SCM Test	NCUO	I	268	0	103	60	431



BACKUP SLIDES



Automating STIGs and Content Distribution



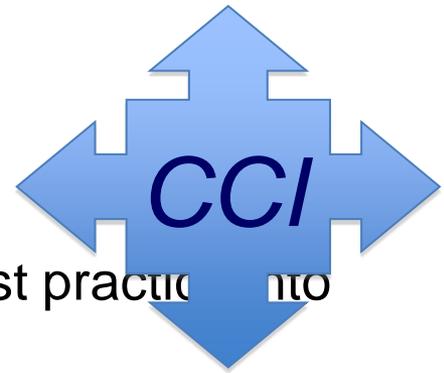
Transformation Efforts

- **Combination of STIG and Checklist into a STIG that looks like a Checklist but has the authority of the STIG**
- **Publication of DoD Content (STIGs) in eXtensible Configuration Checklist Description Format (XCCDF)**
 - XCCDF is an XML definition of a checklist
 - One of the NIST SCAP (protocols)
- **Mapping STIGs to new DoD Control Set**
- **Breakdown of DoD Control Set into measurable CCIs**
- **Publication of automated “benchmarks” for use in SCAP tool (i.e., HBSS Policy Auditor)**



XCCDF

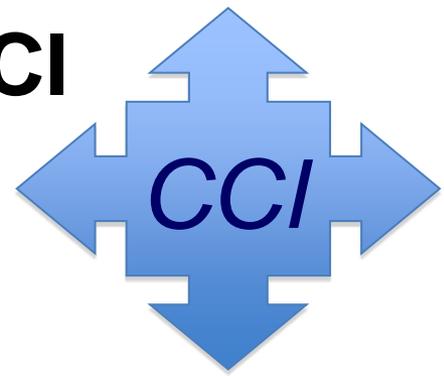
- **XCCDF**
 - Standardized look for STIGs
 - Customer requests for export of requirements
 - Easier for customers to extract data for import into another database
 - Benchmark used by SCAP capable tools
 - OVAL required for true automation of check
- **Status**
 - **Non-Automated**
 - **zOS, Network Infrastructure STIGs, Windows Desktop Application STIGs, ISA Server 2006, as updates are finalized**
 - **Automated**
 - **Windows XP, Vista, 2003, 2008**
 - **IE8 – Aug**
 - **Win7 – as soon as issues resolved**
 - As new STIGs are released – if vulnerability structure supports the level of granularity



A Control Correlation Identifier (CCI) is:

- A decomposition of an IA Control or an IA industry best practice into single, actionable statements
- A foundational element of an IA policy or standard, written with a neutral position on an IA practice so as not to imply the specifics of the requirement
- Not specific to a product or a Common Platform Enumeration (CPE).

DISA Requirement Guides & CCI



DoD Policy Document
NIST SP 800-53v3

Control Correlation Identifier (CCI)

Security Requirements Guide

Applications

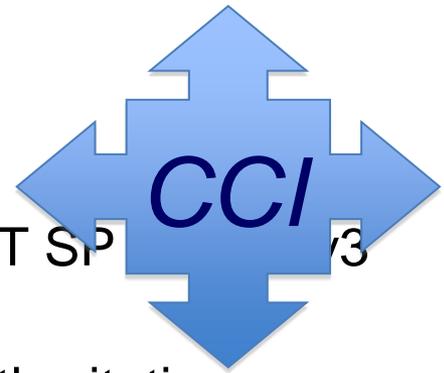
Operating Systems

Network Infrastructure Devices

Organizational Policy



CCI Way Ahead



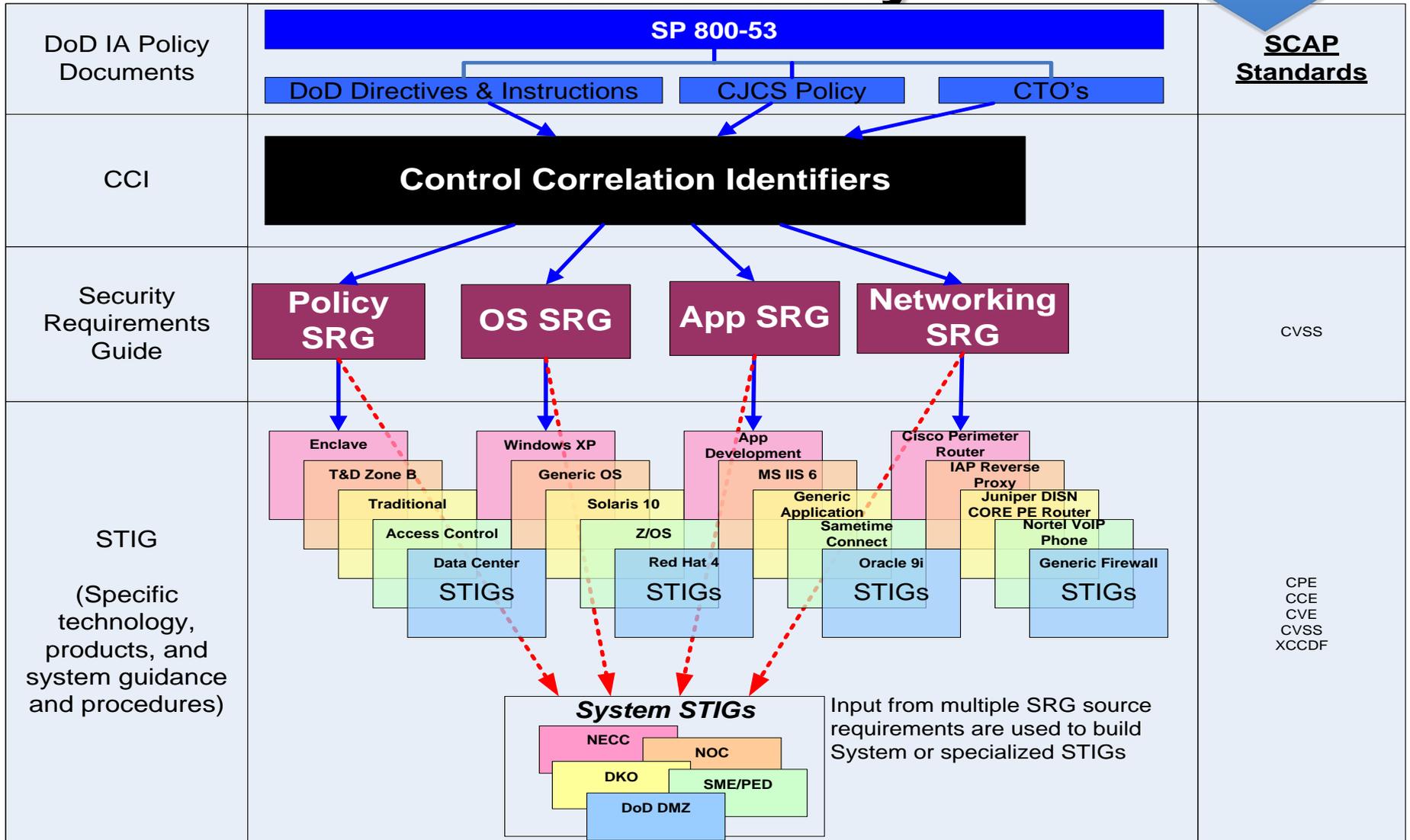
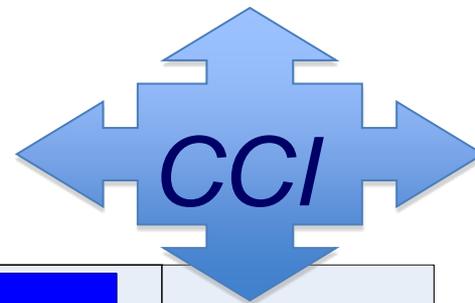
- DISA FSO established the initial CCI List based on NIST SP 800-53 and validated against 800-53a.
- DISA FSO is working with source policy owners and authoritative sources to validate
- “TIM” the list
- Additions to the CCI List can be submitted to DISA FSO for inclusion to the CCI List. Submissions should be sent to cci@disa.mil.



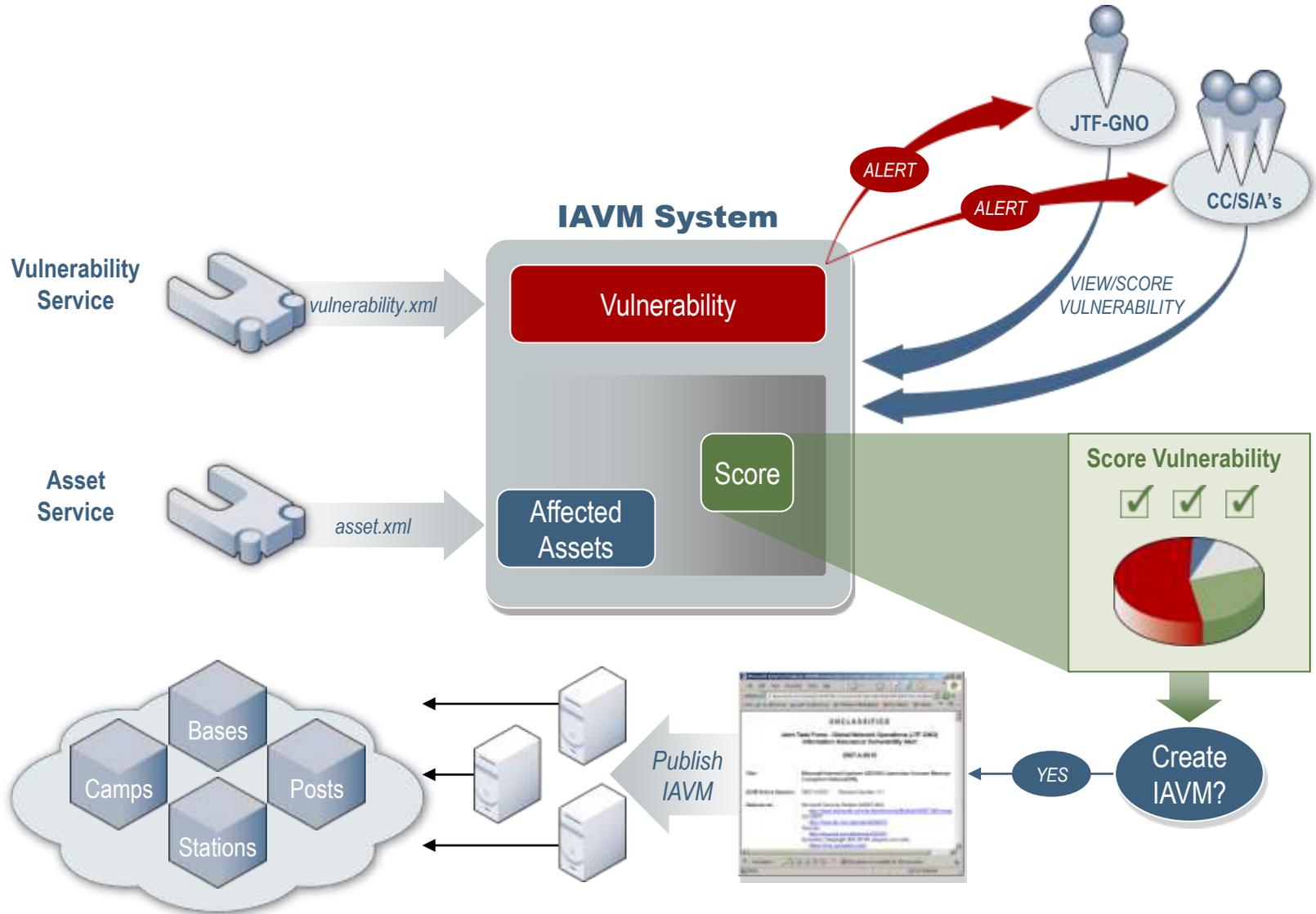
Security Requirements Guide (SRG)

- **Grouping of CCIs**
- **Similar to what a STIG is today**
- **Prose discussion of requirements**
- **No check or fix information**
- **Operating System, Application, Network, Policy**
- **Will be expressed in XCCDF**

Future STIG Traceability



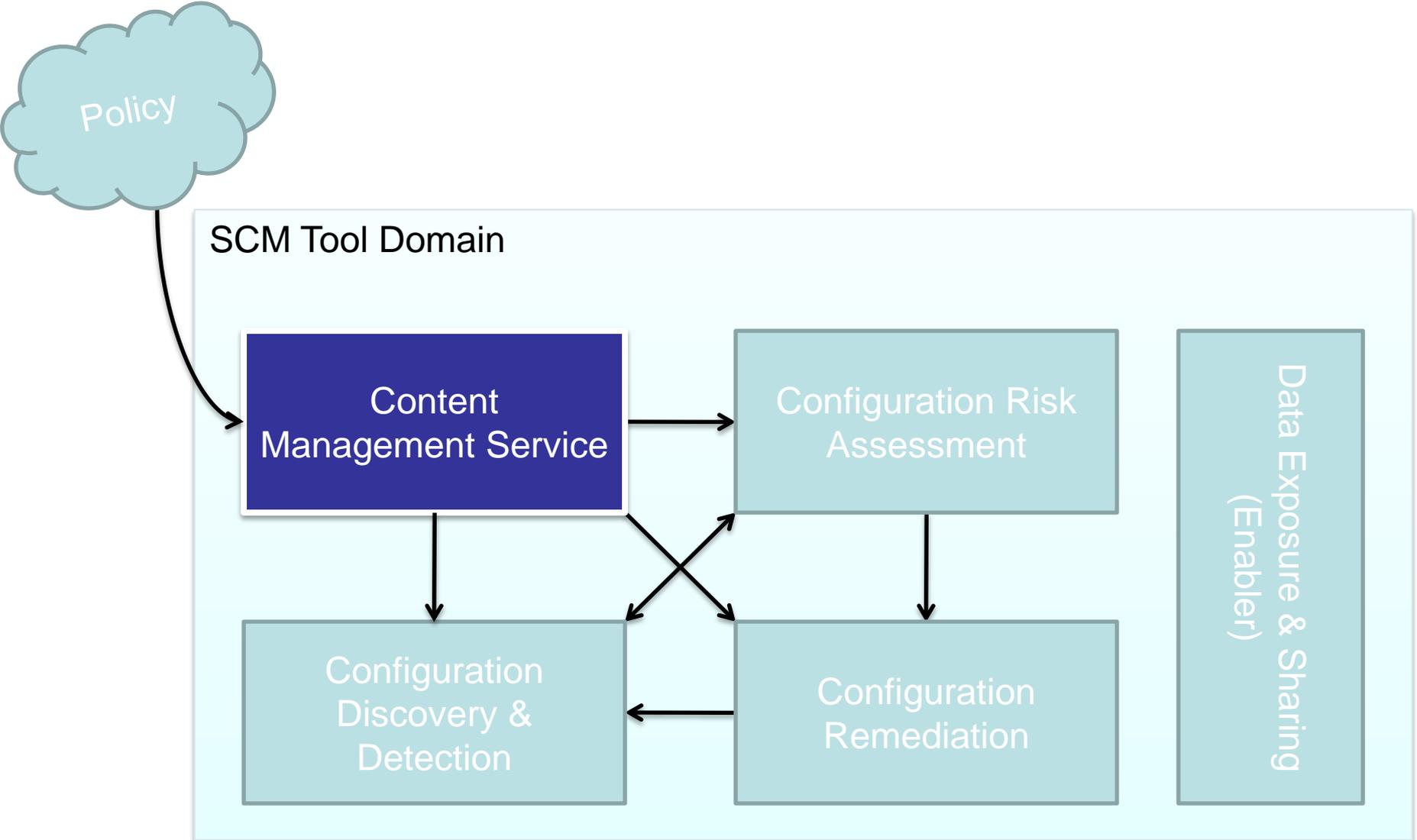
IAVM Service Data Flow





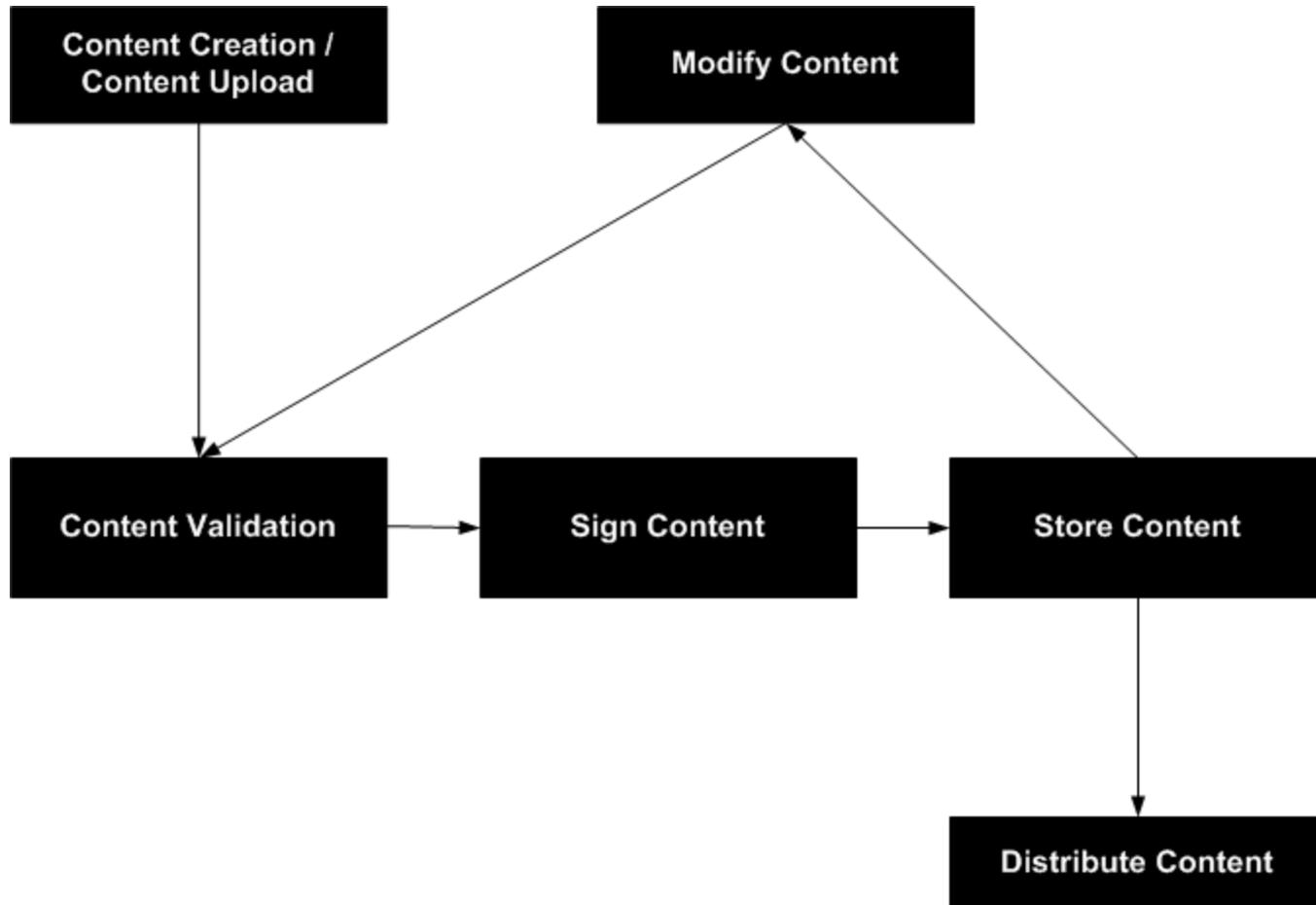
What is Digital Policy Management?

- **Author validated Machine-readable Content**
 - Store content allowing it to be query-able based on SCAP fields, creator/signer, and other values
 - Modify/Copy already created content
 - Allow content-sharing where possible
- **Content Distribute Capability (Machine-to-Machine (M2M), Versioning)**
 - Maintain pedigree while service enabling distribution
- **Collaboration**
 - Reap benefits of enterprise IA workforce to develop, tune, and expand content coverage and usability

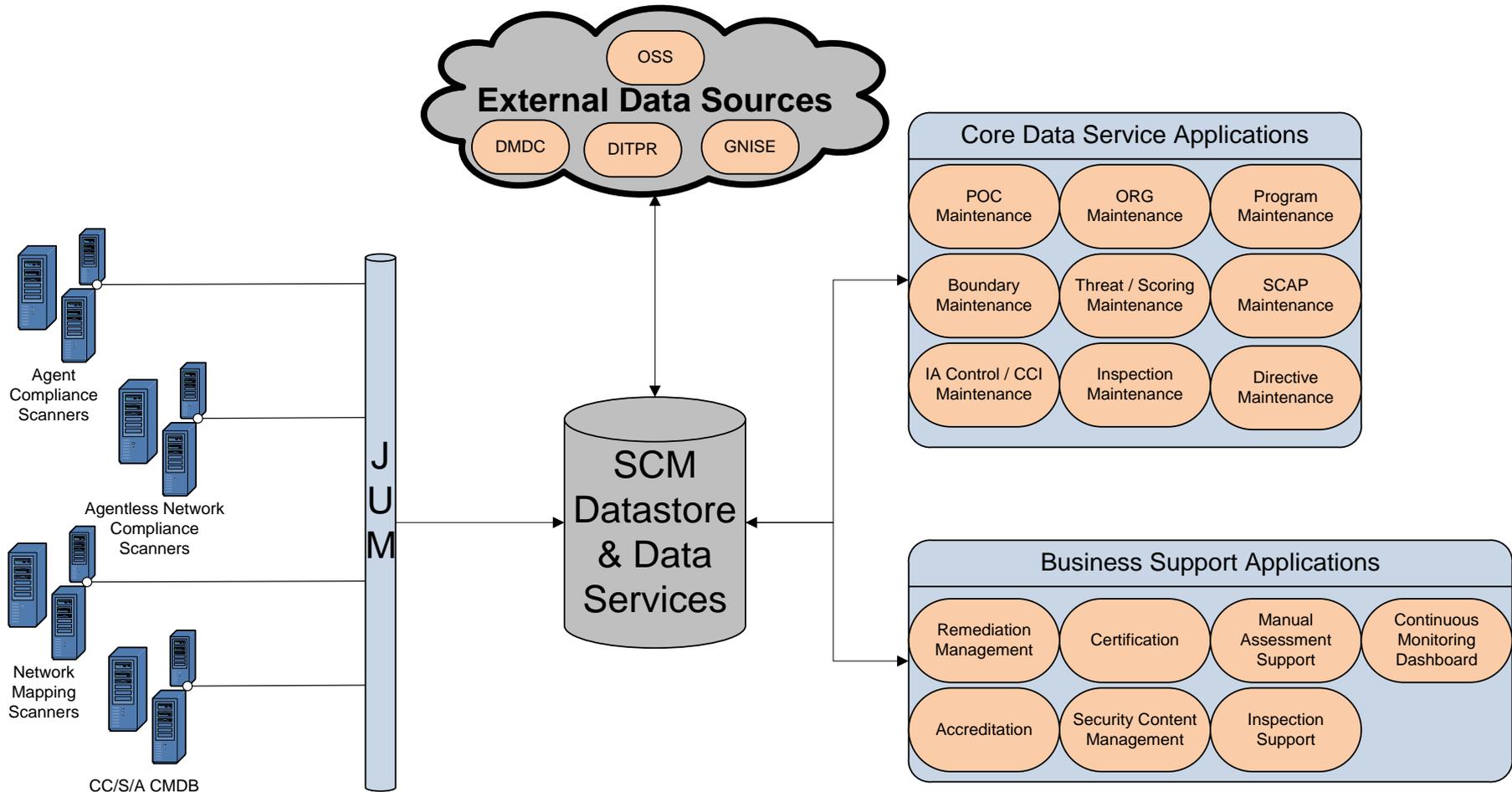




Digital Policy Management Workflow



Conceptual SCM Data Store



Service enable a data centric risk management process



Notional XCCDF Rule Score

SCAP Benchmark Rules					
		Ident	CCI	Agent Scanner Risk Score	Network Scanner Risk Score
STIG	Rule 1	CCE-1	CCI-1	7	10
STIG	Rule 2	CCE-2	CCI-2	4	5
STIG	Rule 3	CCE-3	CCI-3	6	9
IAVM	Rule 4	CVE-1	CCI-4	9	10
IAVM	Rule 5	CVE-2	CCI-4	7	8
IAVM	Rule 6	CVE-3	CCI-4	6	9
CTO	Rule 7	CTO-x.1	CCI-5	9	10
CTO	Rule 8	CTO-x.2	CCI-6	7	8
CTO	Rule 9	CTO-x.3	CCI-6	6	9



SCM HOST Data

HBSS Asset & OAM

Host 1		Host 2	
HOST ID	GUID1	HOST ID	GUID2
FQDN	h1.scm.dom	FQDN	h2.scm.dom
MAC	aa.bb.cc.dd.ee.ff	MAC	bb.cc.dd.ee.ff.aa
IP Address	10.1.1.1	IP Address	10.1.1.2
IP Subnet	255.0.0.0	IP Subnet	255.0.0.0
MAC Level	1	MAC Level	2
Confidentiality	Sensitive	Confidentiality	Public
Owning Org	DISA PEO-MA IA5	Owning Org	DISA PEO-MA IA5
Administering Org	DISA CSD OKC	Administering Org	DISA CSD OKC
CC/S/A	DISA	CC/S/A	DISA
AOR	USNORTHCOM	AOR	USNORTHCOM
System Affiliation	POR1	System Affiliation	POR1
Network	NIPRNet	Network	NIPRNet
CCSD	12abc	CCSD	12abc
OS Type	Windows XP	OS Type	Windows XP
OS Version	5.1	OS Version	5.1
OS Service Pack	Service Pack 3	OS Service Pack	Service Pack 3
OS Build Number	2600	OS Build Number	2600
OS Platform	Professional	OS Platform	Professional
ePO Managed	Yes	ePO Managed	Yes
	Intel(R) Pentium(R)		Intel(R) Pentium(R)
CPU Type	D CPU 3.00GHz	CPU Type	D CPU 3.00GHz
CPU Speed	2990MHz	CPU Speed	2990MHz

ENMLDS

Device	Peers
Host 1	10.1.1.2
<i>10.1.1.1</i>	10.1.1.100
Host 2	10.1.1.1
<i>10.1.1.2</i>	10.1.1.100
Switch	10.1.1.1
<i>10.1.1.100</i>	10.1.1.2
	10.1.1.200
Firewall	
<i>10.1.1.200</i>	10.1.1.100
<i>172.16.1.2</i>	172.16.1.1
PE Router	
<i>172.16.1.1</i>	172.16.1.2
<i>192.168.2.2</i>	192.168.2.1



Score Sample

Rules	Hosts	Internal Result	Internal Risk	External Result	External Risk	Total Raw Score	MAC/Conf Weighted Score
Rule 1	Host 1	F	50	NF	0	50	75
	Host 2	NF	0	NF	0	0	0
Rule 2	Host 1	F	17	F	101	118	177
	Host 2	NF	0	NF	0	0	0
Rule 3	Host 1	NF	0	NF	0	0	0
	Host 2	NF	0	NF	0	0	0
Rule 4	Host 1	F	82	NF	0	82	123
	Host 2	F	82	NF	0	82	82
Rule 5	Host 1	F	50	F	65	115	172.5
	Host 2	NF	0	NF	0	0	0
Rule 6	Host 1	NF	0	NF	0	0	0
	Host 2	F	37	F	82	119	119
Rule 7	Host 1	F	82	NF	0	82	123
	Host 2	NF	0	NF	0	0	0
Rule 8	Host 1	NF	0	NF	0	0	0
	Host 2	F	50	F	65	115	115
Rule 9	Host 1	F	37	NF	82	119	178.5
	Host 2	F	37	F	82	119	119

	MAC 1	MAC 2	MAC 3
Classified	3	1.8	1.2
Sensitive	1.5	1.3	1.1
Public	1.2	1	0.8

Host 1 Weighted Score = 848.5

Host 2 Weighted Score = 435

Mission Assurance Category and Confidentiality Score Weighting



Remediation Prioritization

Prioritize Fix Plan by Host Risk (Current Approach Fix CAT 1 each host)

Fix Order	Host/Rule	Risk Score	Stacked Risk Score
0	Host 1 - Rule 9	179	1284
1	Host 1 - Rule 2	177	1105.5
2	Host 1 - Rule 5	173	928.5
3	Host 1 - Rule 4	123	756
4	Host 1 - Rule 7	123	633
5	Host 2 - Rule 6	119	510
6	Host 2 - Rule 9	119	391
7	Host 2 - Rule 8	115	272
8	Host 2 - Rule 4	82	157
9	Host 1 - Rule 1	75	75
10	Host 1 - Rule 3	0	0

Prioritize Fix Plan by Rule Risk (Optimize Effort to Increase ROI)

Fix Order	Rule	Rule Risk	Stacked Risk Score
1	9	297.5	1284
2	4	205	986.5
3	2	177	781.5
4	5	172.5	604.5
5	7	123	432
6	6	119	309
7	8	115	190
8	1	75	75
9	3	0	0

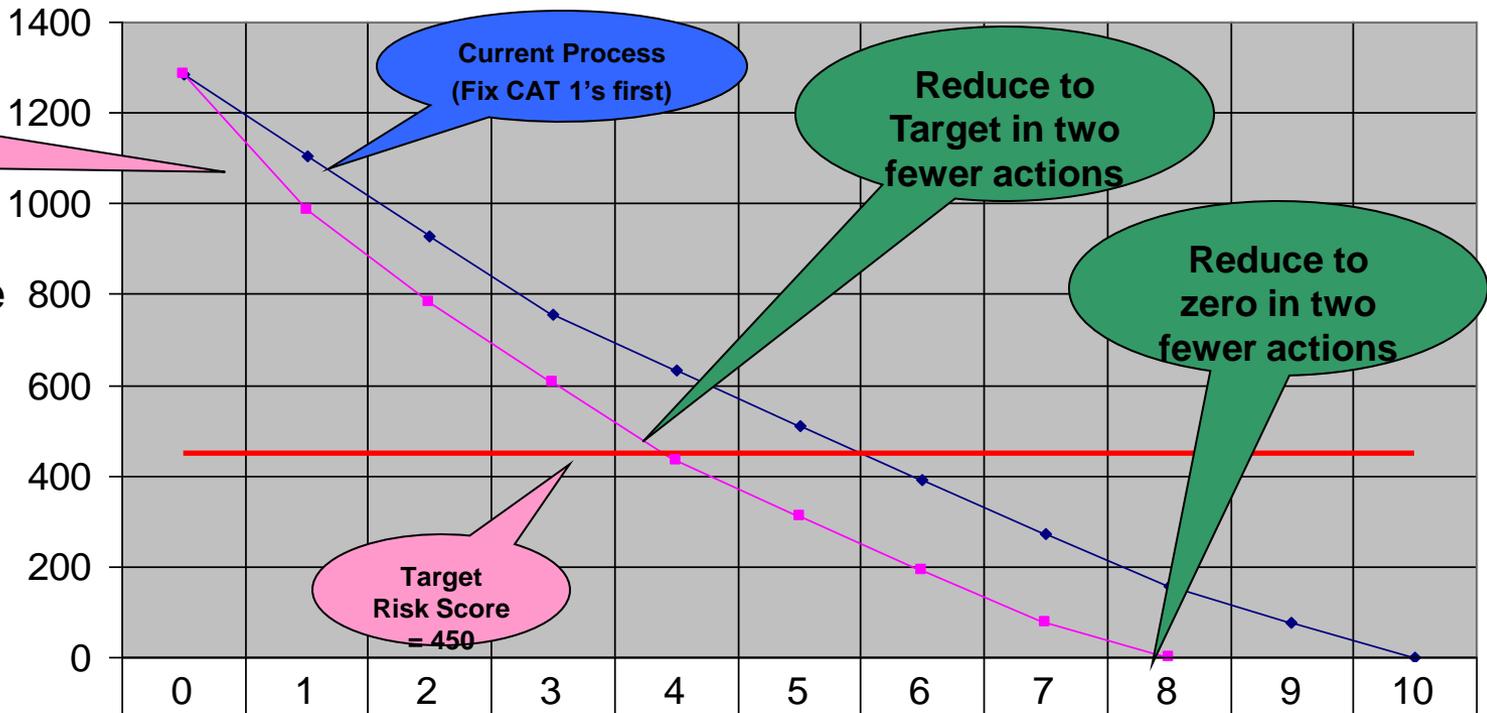
**Optimize fix actions
based on risk saturation**



Remediation Prioritization

Remediation Burn Down Rule Risk vs Host Risk

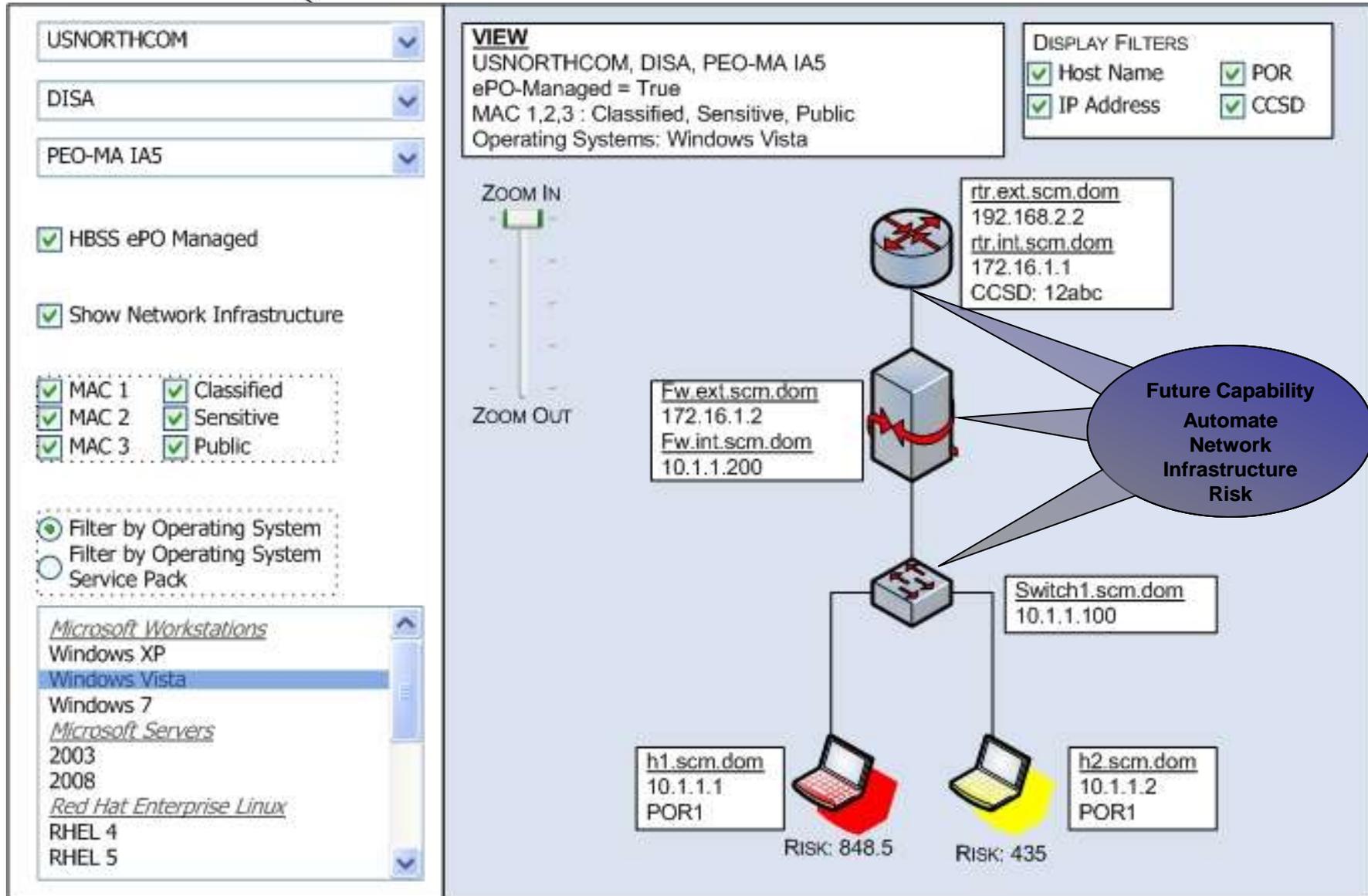
- ◆ Burn down by Host
- ◆ Burn Down by Rule Risk



◆ Burn down by Host	1284	1106	928.5	756	633	510	391	272	157	75	0
◆ Burn Down by Rule Risk	1284	986.5	781.5	604.5	432	309	190	75	0		
— Target Risk Score	450	450	450	450	450	450	450	450	450	450	450

Remediation Action #

Notional Risk Map





Terminology

- **ARF – Asset Report Format**
- **ASR – Assessment Results Format**
- **CCE – Common Configuration Enumeration**
 - SCAP configuration ID
- **CCI – Control Correlation ID**
 - Maps Requirements to IA Controls/Policy
- **CCSS – Common Configuration Scoring System**
- **CPE – Common Platform Enumeration**
 - SCAP OS/App/HW ID
- **CVE – Common Vulnerability and Exposure**
 - SCAP vulnerability ID
- **CVSS – Common Vulnerability Scoring System**
- **OCIL – Open Checklist Interactive Language**
- **OVAL – Open Vulnerability Assessment Language**
- **XCCDF – Extensible Configuration Checklist Data Format**
 - Benchmarks – STIGs, IAVMs, CTOs, etc...