



Providing Cybersecurity Inventory, Compliance Tracking, and C2 in a Heterogeneous Tool Environment

Joseph L. Wolfkiel

Secure Configuration Management Lead Engineer

May 2018



Disclaimer

The information provided in this briefing is for general information purposes only. It does not constitute a commitment on behalf of the United States Government to provide any of the capabilities, systems or equipment presented and in no way obligates the United States Government to enter into any future agreements with regard to the same. The information presented may not be disseminated without the express consent of the United States Government.



- **Objective and Problem Statement**
- **Defining Terms**
- **Building an Enterprise Inventory and Compliance Baseline**
- **Today's Homogeneous C2 and Reporting Environment**
- **Conducting Enterprise Cyber C2 in Today's Environment**
- **Heterogeneous Environment of the Future**
- **Comparative Challenges**
- **Stuff We Think We Can Do**
- **Stuff We Still Have to Figure Out**



Objective and Problem Statement

- **Objective:** To help attendees understand the challenges in conducting Cyber Command and Control (C2) and reporting in the evolving DoD and commercial cyberspace environment
- **Problem Statement:**
 - The DoD has been moving to a common cybersecurity toolset for 10+ years
 - **Starting with Host-Based Security System (HBSS) in 2004-2005**
 - HBSS included management agent & Host Intrusion Prevention System (HIPS)
 - Moved to single AV product integrated with HBSS
 - Added enterprise
 - Compliance checking
 - “Device Control Module”
 - Application whitelisting
 - Software inventory
 - **Common vulnerability and STIG scanner acquired as Assured Compliance Assessment Solution (ACAS)**
 - Current plans go to per-component best of breed products
 - US Cyber Command and the Joint Forces Headquarters, DoD Information Network (JFHQ DoDIN) need to provide **enterprise** defense



Defining Terms

- **Cybersecurity:** Prevention of damage to, protection of, and restoration computers and networks, to ensure availability, integrity, authentication, confidentiality, and nonrepudiation (DoDI8500.01, 14 Mar 14)
- **Inventory:** A complete list of items such as property, goods in stock...(bing.com)
- **Compliance:** The state or fact of according with or meeting standards (bing.com)
- **Command and Control (C2):** Exercise of authority and direction of assigned forces (U.S. Army FM 3-0)
- **Heterogeneous:** composed of parts of different kinds... (Dictionary.com)



Building an Enterprise Inventory and Compliance Baseline

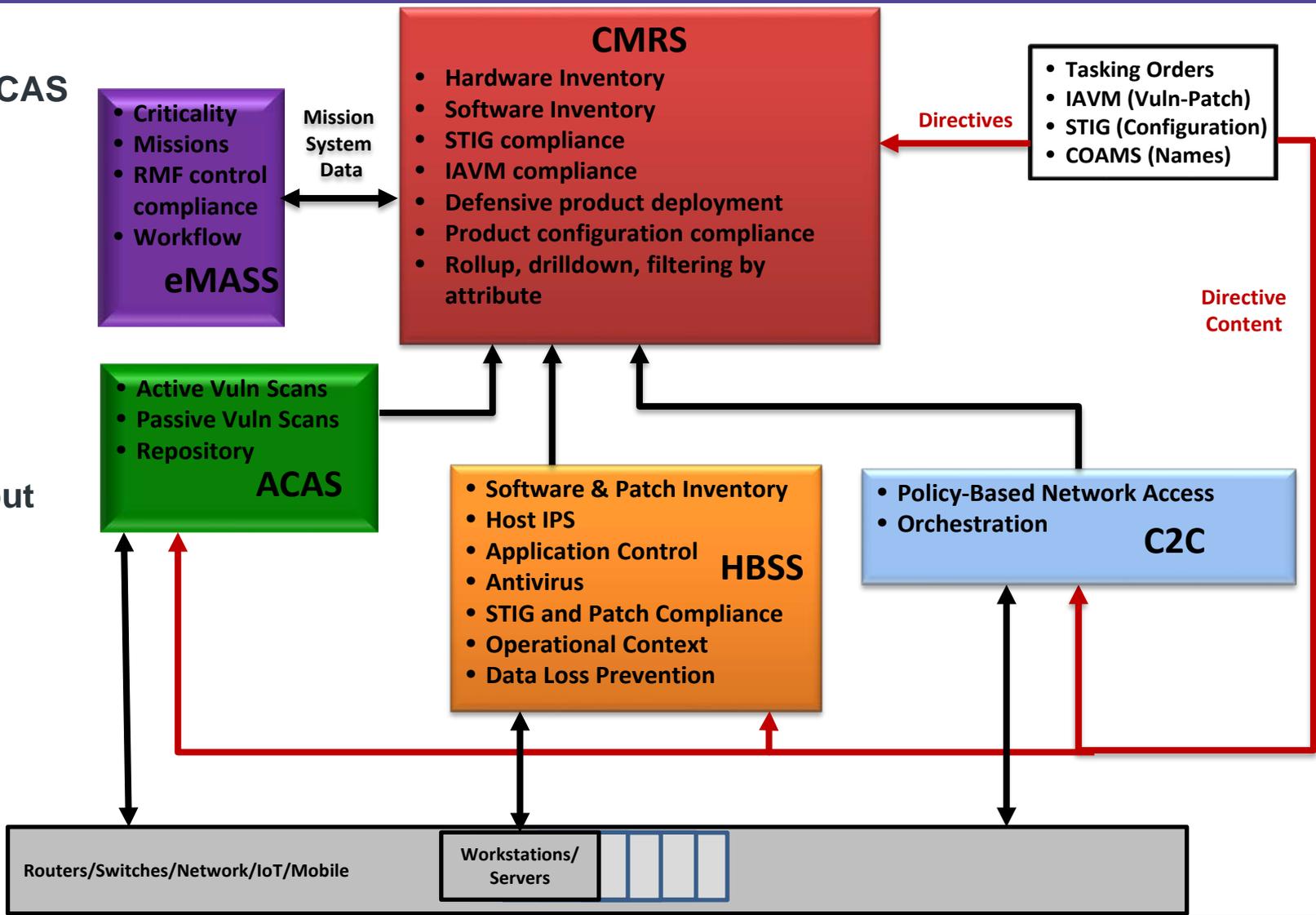
Cumulative process, following NIST 8011 and CIS basic security control concepts

- Hardware Asset Management (HWAM) - Asset ID and inventory, operational context
- Software Asset Management (SWAM) - Software inventory & install/execution control
- Vulnerability Management (VUL) - Vulnerability awareness and patch priority
- Security Configuration Management (CONF) - Security Technical Implementation Guidance (STIG) & Individual Configuration Directives
- Anti-Malware - Host Intrusion Prevention System and Antivirus
- Insider Threat Mitigations - Data Loss Prevention (DLP), user behavior analytics, and knowledge management (KM)



Today's Homogeneous C2 and Reporting Environment - Multiple Tools, But Only One Per Capability

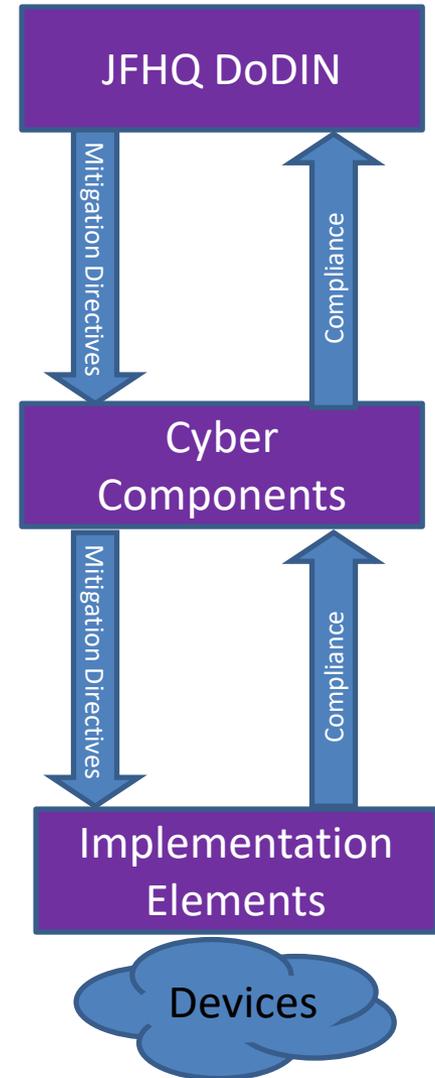
- HBSS and ACAS are Primary Sensors
- Plans to add C2C Sensor
- All data reported to CMRS or input to eMASS





Conducting Enterprise Cyber C2 in Today's Environment

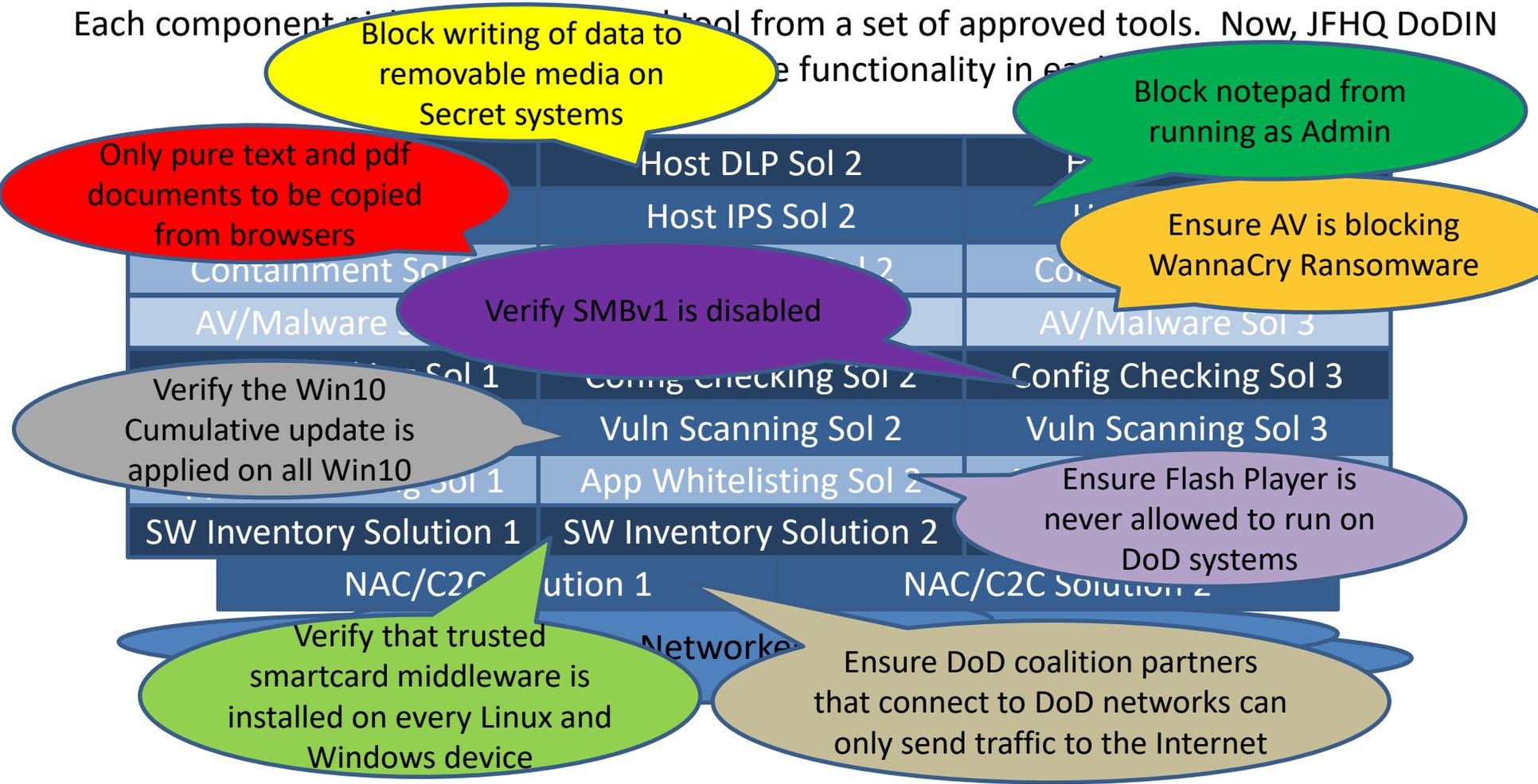
- **Which Devices are Permitted on the Network**
 - Unsupported products
 - TBD Enterprise C2C policy
- **Application of Patches**
 - The IAVM process
- **Scanning and Reporting of Vulnerabilities**
 - ACAS Tasking Orders and the IAVM process
- **Directing Secure Configurations**
 - STIG process
- **Directing Malware Mitigations**
 - Custom Host Intrusion Prevention System Signatures
 - Minimum AV signature ages and scan frequency





Heterogeneous Environment of the Future: Best of Breed Tools for All of Today's Capabilities Then Some

Each component must be replaced with a tool from a set of approved tools. Now, JFHQ DoDIN





Comparative Challenges

Homogeneous

- Implement enterprise protective or defensive measures
- Automatically collect directive compliance data
 - Broken out by device count, location, organization, and/or accreditation boundary
- Event analysis to determine how frequently measures are being invoked

Heterogeneous

- Implement enterprise protective or defensive measures in a *tool-agnostic way*
- Automatically collect compliance data
 - Broken out by device count, location, organization, and/or accreditation boundary *and correlate the compliance indicators between different tools*
- Analyze event data to determine how frequently measures are being invoked *when different events are being produced per tool for the same incident*

Future: Factor in all protective and defensive capabilities to determine, per attack vector, if a device population is protected from a threat or class of threats



Stuff We Think We Can Do – Asset Identification/Correlation

Home Inventory Policy

All Hosts Online/Offline Show only unassigned

Host	Host IP	Segment	MAC Address	Comment	Display Name
JOESNET/UNIQUEHOSTN...	214.38.224.248	FMD2 Wireless Disanet...	d4ded8850e21		Wolfkiel, Joseph L CIV DI...
JOESNET/UNIQUEHOSTN...	192.168.1.8	FMD ACQ Level 4 Users	6854fdd1fa03		Wolfkiel, Joseph L CIV DI...

Customize Properties

Custom 1: 255.255.255.0
 Subnet Mask: 255.255.255.0
 Time Zone: Eastern Standard Time
 System Tree Sorting: Enabled
 Product Version (Agent): 5.0.S.658
 Language (Agent): English (United States)
 Hotfix/Patch Version (Agent):
 Product Version (Product Coverage Reports): Not available

System Properties Products Threat Events Host Inventory McAfee Agent Virtualization Rogue System Detection DLP User Sessions

Agent GUID: 4F1444D6-A544-11E6-0612-000000000000
 Communication Type: HTTPS
 CPU Serial Number: N/A
 CPU Speed (Mhz): 2,592
 CPU Type: Intel(R) Core(TM) i5-3320M CPU @ 2.60GHz
 Custom 1:
 Custom 2:
 Custom 3:
 Custom 4:
 Default Language: English (United States)
 Description:
 DNS Name: UNIQUEHOSTNAME.JOESNET.home.org
 Domain Name: JOESNET
 Excluded Tags:
 Free Disk Space: 130.35 GB
 Free Memory: 4,156.70 MB
 Free System Drive Space: 133480 MB
 Installed Products: Asset Baseline Monitor 3.5.1, Benchmark Editor Multi-platform Scan Engine 6.3.0.194, Data Loss Prevention 10.0.350.12, McAfee Agent 5.0.S.658, Assessment 6.3.0.194, Policy Auditor Agent 6.3.0.194, ACCM 3.2.0.18, VirusScan Enterprise 8.8.0.1804
 IP Address: 214.36.72.90
 IPX Address: N/A
 Is 64 Bit OS: Yes
 Is Laptop: Yes
 Last Communication: 3/29/18 3:41:49 PM
 Last Sequence Error:
 LDAP Location:
 MAC Address: 68:54:fdd1:fa:03

Same Device? How do you tell? IP, MAC, Hostname, Serial Number, BIOS GUID, Software GUID?

joseph.l.wolfkiel.civ@... Delete

LAST UPDATED: 05:32 PM

Asset Details

Name: 192.168.1.8
 IPv4 Address: 192.168.1.8
 MAC Address: 68:54:fd:d1:fa:03
 Source: NW Scanner Scan
 First Seen: March 2 at 8:18 PM
 Last Seen: March 23 at 7:04 PM

Tags

owning unit: Global:Gov:US:DoD
 owning unit: Global:Gov:US:DoD

Device Details

Publisher: joespublisher.joesnet.org
 Device ID: 4937952
 Hostnames: [HBSS] UNIQUEHOSTNAME.JOESNET
 MACs: [HBSS] 68:54:fd:d1:fa:03
 IPv4: 192.168.1.8
 Operating System: o:windows_10:10.0__14393:

Last Published: 3/27/2018
 Owing Org: Global:Gov:_United States:DOD:DISA
 Admin Org: Global:Gov:_United States:DOD
 Location: Global:UNITE:MLD
 IPv6:
 PORs: Global: JOESPERSONALACCREDIT

Device's Tagged Value(s)

BIOSGUID: 4C4C4544-004E-4410-804E-C7C04F469534
 CPU Speed: 2592MHz
 CPU Type: Intel(R) Core(TM) i5-3320M CPU @ 2.60GHz
 McAfee ePO Agent GUID: 4F1444D6-A544-11E6-2592-000000000000
 McAfee ePO Managed: True
 MotherBoard Serial Number: JOESSERIALNUM
 userName: joseph.wolfkiel



Stuff We Think We Can Do – Asset Operational Context/Characterization

1 Create and Maintain an Enterprise Standardized List of Names to be Used

Hierarchies

Click to expand hierarchies, right click to assign name. To create a new name you must start by adding it to the default hierarchy in the tree

No Value Selected

No Value Selected

Name Maintainers

- Owner
 - global
 - Commercial
 - Government
 - Australia
 - United Kingdom
 - United States
 - Department of Defense
 - Defense Acquisition University
 - Defense Advanced Research Projects Agency
 - Defense Commissary Agency
 - Defense Contract Audit Agency
 - Defense Contract Management Agency
 - Defense Finance and Accounting Service
 - Defense Health Agency
 - Defense Human Resources Activity
 - Defense Information Systems Agency
 - Defense Intelligence Agency
 - Defense Legal
 - Add New Name Below
 - Modify Name
 - Defense Logistics
 - Delete Name and Children
 - Defense Media
 - Merge Name and Children
 - Defense Micro
 - Excel Import
 - Defense POW/MIA
 - Accounting Agency
 - Defense Security Cooperation Agency
 - Defense Security Service
 - Defense Technical Information Center
 - Defense Technology Security Administration
 - Defense Threat Reduction Agency
 - Department of Defense Education Activity
 - Department of Defense Inspector General
 - Department of Defense Test Resource Management Center
 - Missile Defense Agency
 - National Defense University
 - National Geospatial Intelligence Agency
 - National Guard Bureau
 - National Reconnaissance Office
 - National Security Agency
 - Office of Economic Adjustment
 - Office of the Secretary of Defense
 - Pentagon Force Protection Agency
 - The Joint Staff
 - U.S. Africa Command
 - U.S. Central Command

3 Leverage the Interoperability to Generate Enterprise Situational Awareness

Asset Tag Editor - Operational Attributes for "JOESTEST08J"

Title	Name	Required	Value	Actions
<input type="checkbox"/>	Geolocation	Y	Global:UNITE:MLD [Search for Geolocation]	
<input type="checkbox"/>	CND Service Provider	Y	Global:Gov:USCYBERCOM [Search for CND Service Provider]	
<input type="checkbox"/>	Owning CC/IA/FA	N	Global:DISA [Search for Owning CC/IA/FA]	Delete
<input type="checkbox"/>	Owning Unit	Y	Global:Gov:_United States:DOD:DISA [Search for Owning Unit]	
<input type="checkbox"/>	Operational Accreditation	N	Global:DISA-ID:DSIMS-CA&B ID 8421 [dsims]	Delete

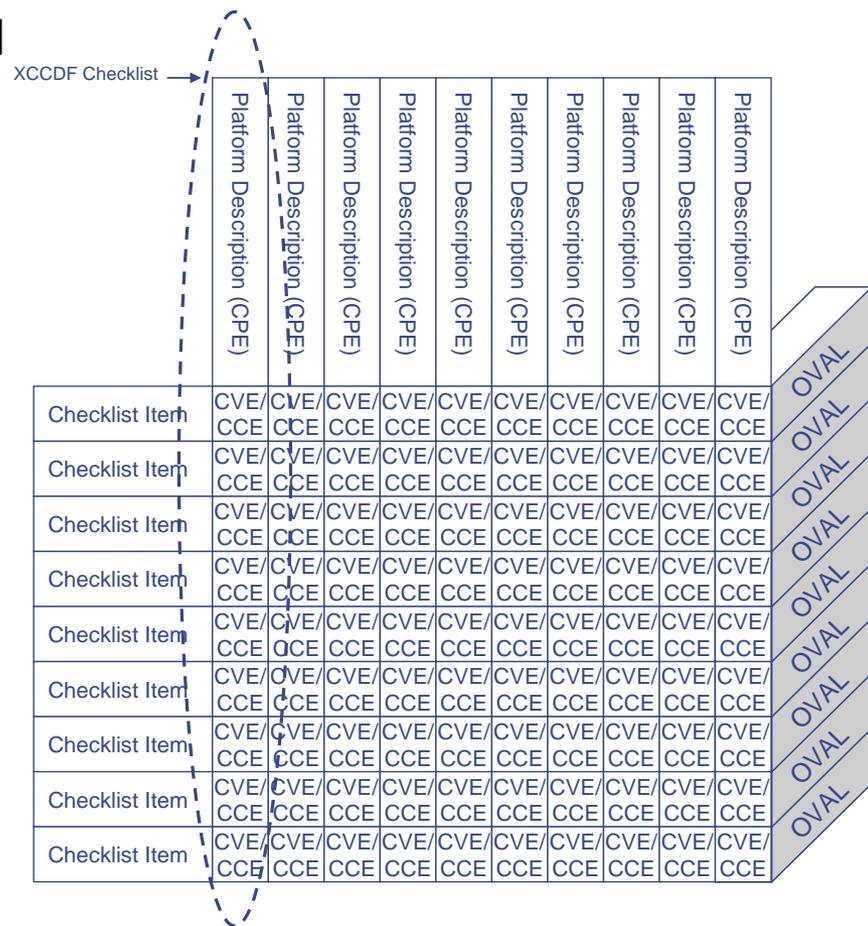
2 Use Standardized Names to Describe Elements of Operational Context:
Who owns it? Where is it? What accreditation boundary does it belong to?



Stuff We Think We Can Do – Patch and Vulnerability Management, Config Compliance

• How? Leverage the NIST Security Content Automation Protocol

- OVAL – Language to check for settings and software in a given Operating System
- XCCDF – Checklist automation (STIG)
- CVE – Standardized IDs for vulnerabilities
- CCE – Standardized IDs for settings
- CPE – Standardized names for hardware and software





Stuff We Still Have to Figure Out

- **Standard policies and compliance reporting for:**
 - Antivirus
 - Data loss prevention
 - Host IPS
 - Application whitelisting
 - Containment
 - Other TBD

- **Way Ahead: Try to leverage SCAP concepts**
 - Minimum compliance set per required function
 - Compliance measures in “benchmarks” per tool and/or capability set
 - Resolve compliance assessments to pass/fail



Questions?

rate us

take the **3-question** survey
available on the AFCEA 365 app

visit us

DISA Booth # **443**

follow us



Facebook/**USDISA**



Twitter/**USDISA**

www.disa.mil



DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

 www.disa.mil  /USDISA  @USDISA