SCAP, Security Automation, USGCB/FDCC

ISIMC

December 16, 2009

Agenda

- What is SCAP?
- SCAP Use Case Exploration
- What is security automation?
- United States Government Configuration Baseline (USGCB)/FDCC Process
- Current State of Windows 7 and Internet Explorer 8 security baseline
- Moving forward

What is SCAP?

SCAP

Languages

Means of providing instructions

- Community developed
- Machine readable XML
- Reporting
- Representing security checklists
- Detecting machine state

XCCDF security benchmark automation

OVAL Open Vulnerability and Assessment Language

Metrics

Risk scoring framework

- Community developed
- Transparent
- Metrics
  - Base
  - Temporal
  - Environmental

CVSS

Enumerations

Convention for identifying and naming

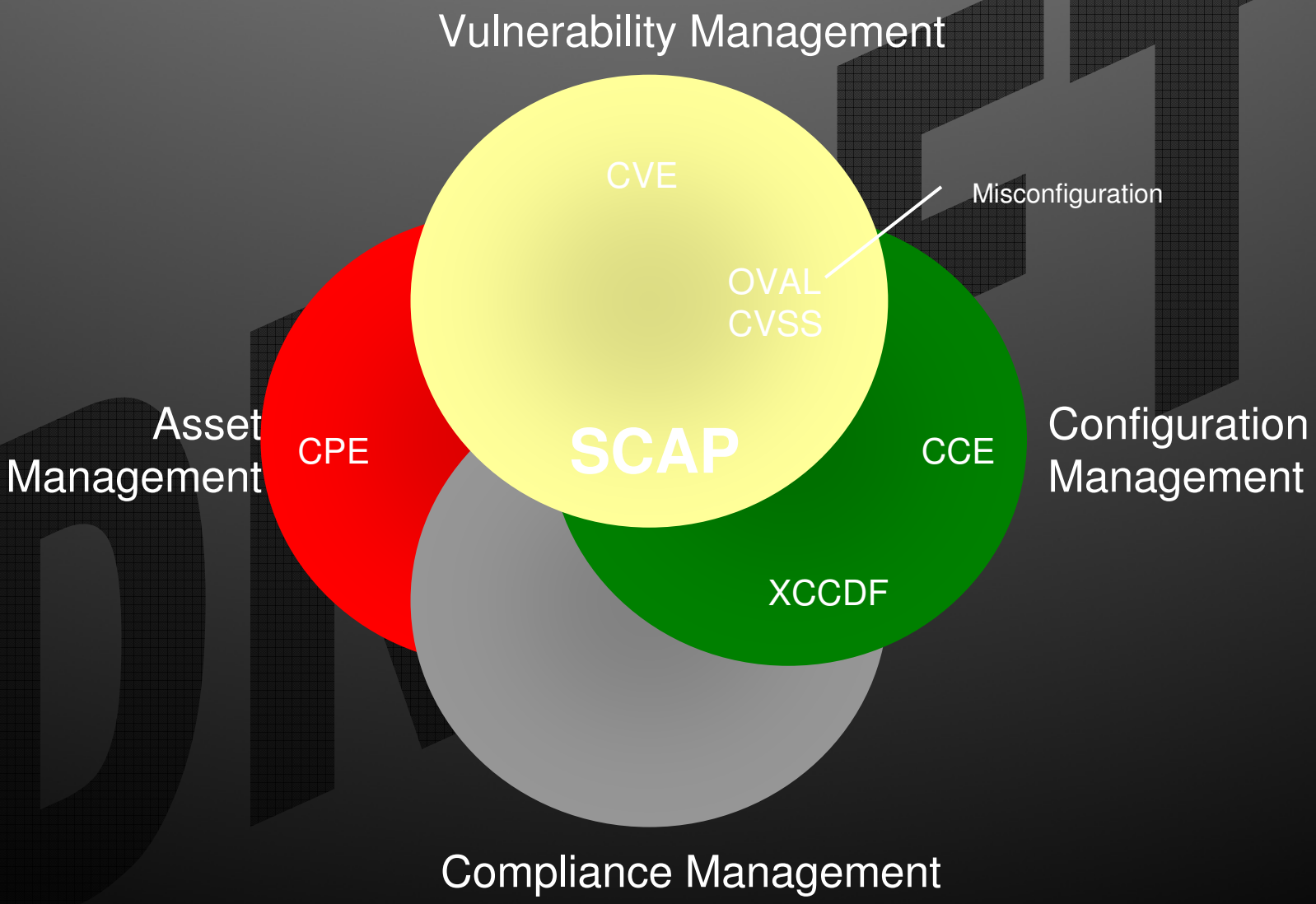
- Community developed
- Product names
- Vulnerabilities
- Configuration settings

CVE cve.mitre.org

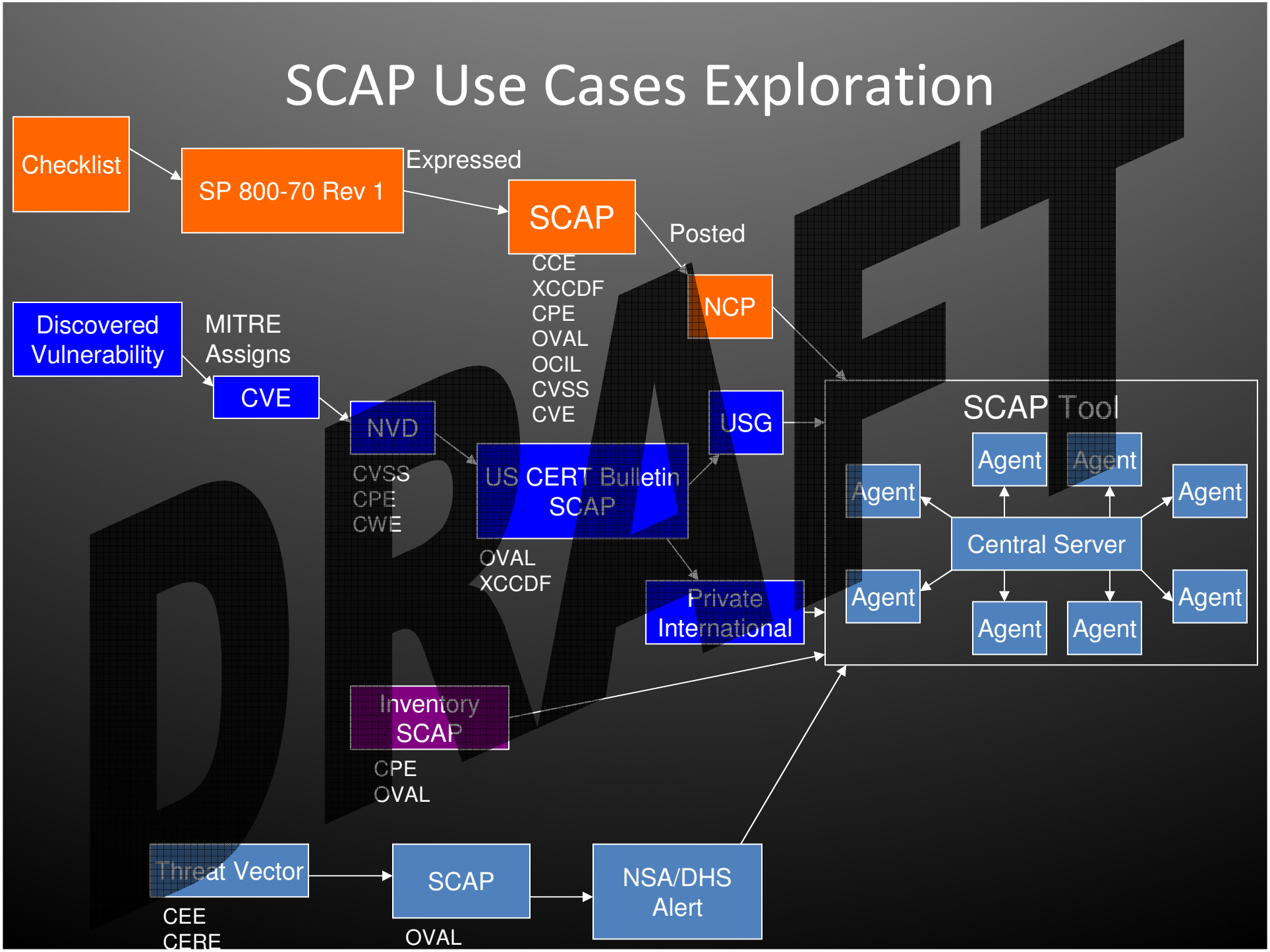
CCE

CPE common platform enumeration

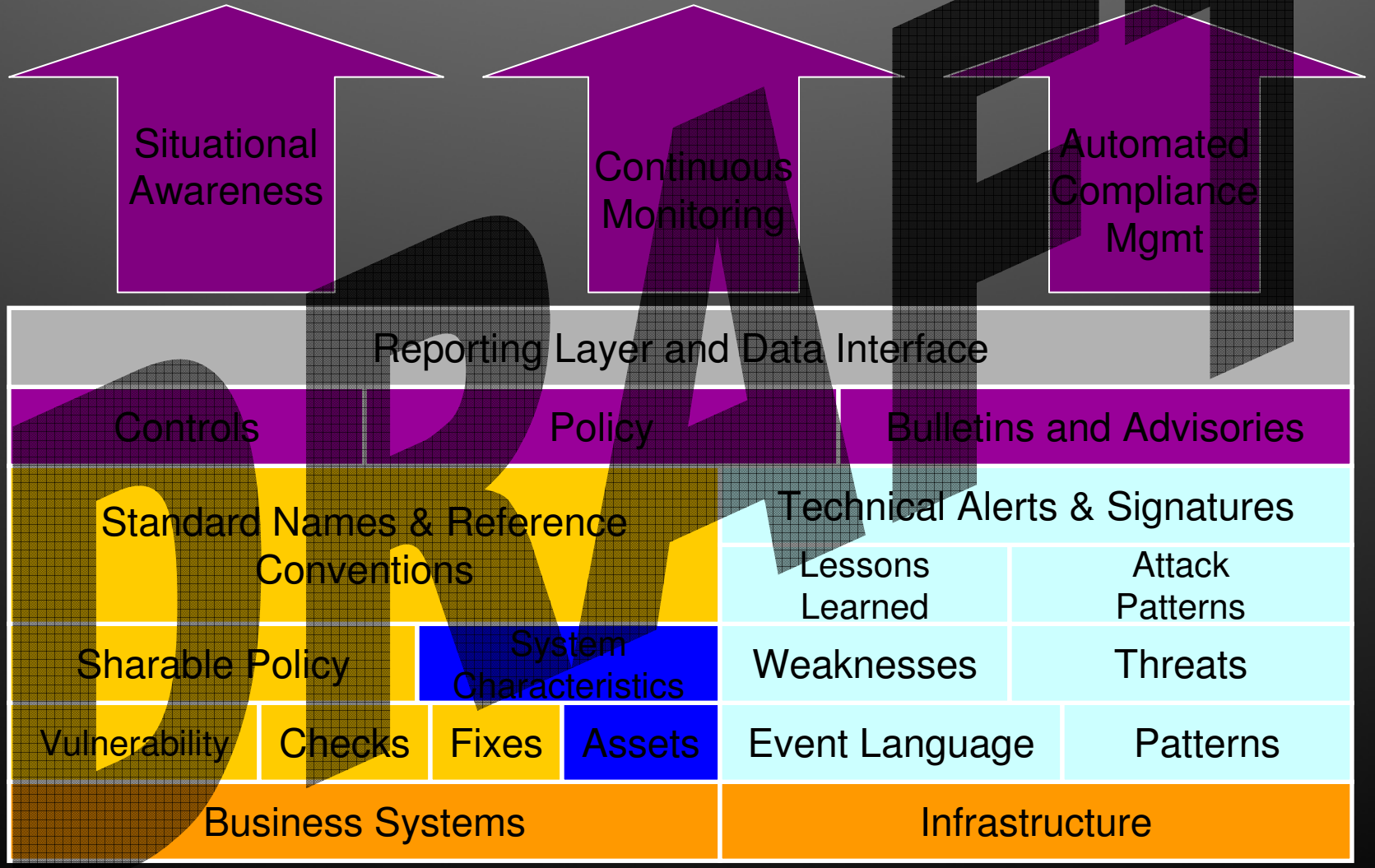
Integrating IT and IT Security Through SCAP



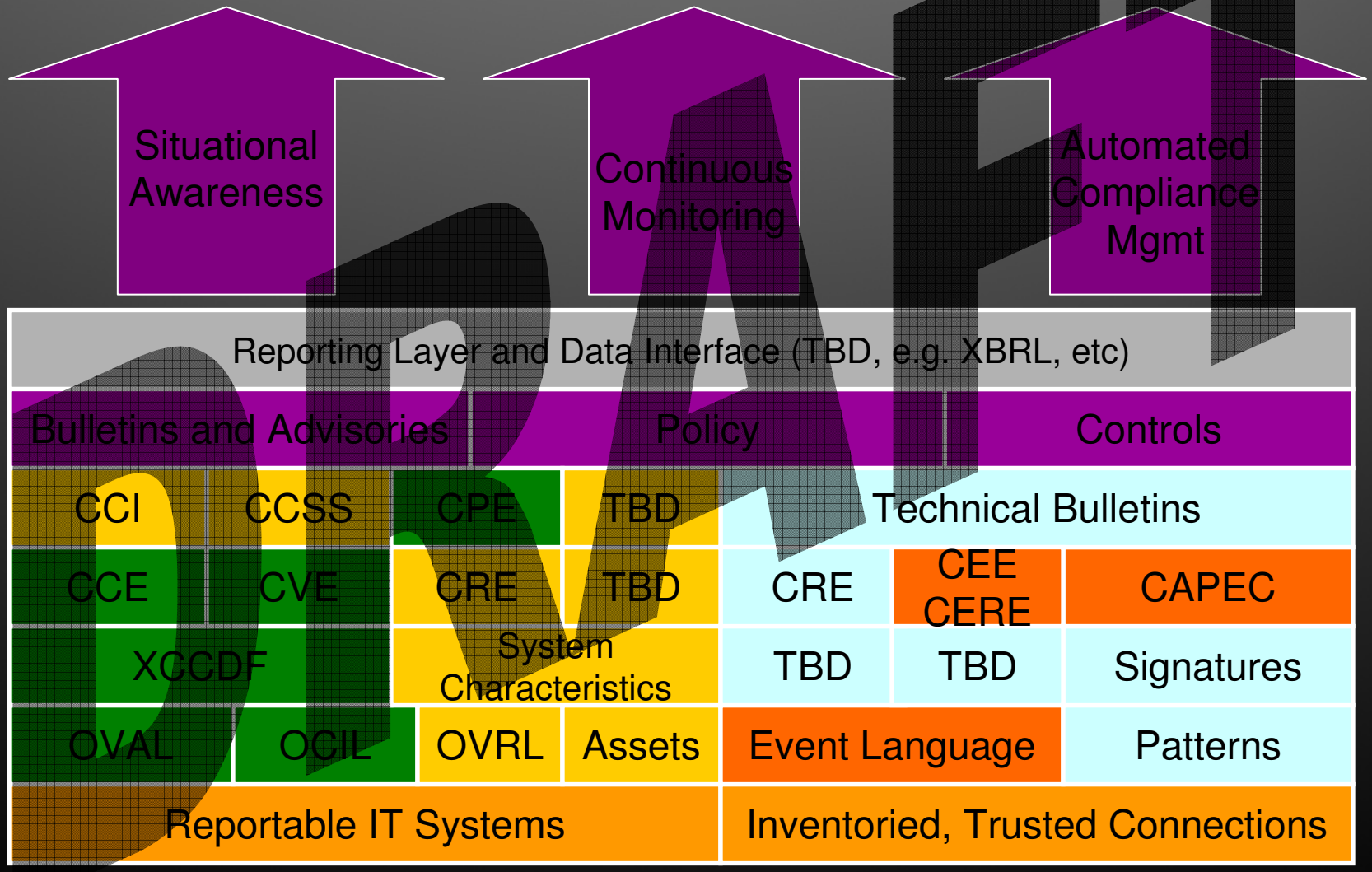
SCAP Use Cases Exploration



Notional Security Data Model



Notional Specifications-Based Security Automation

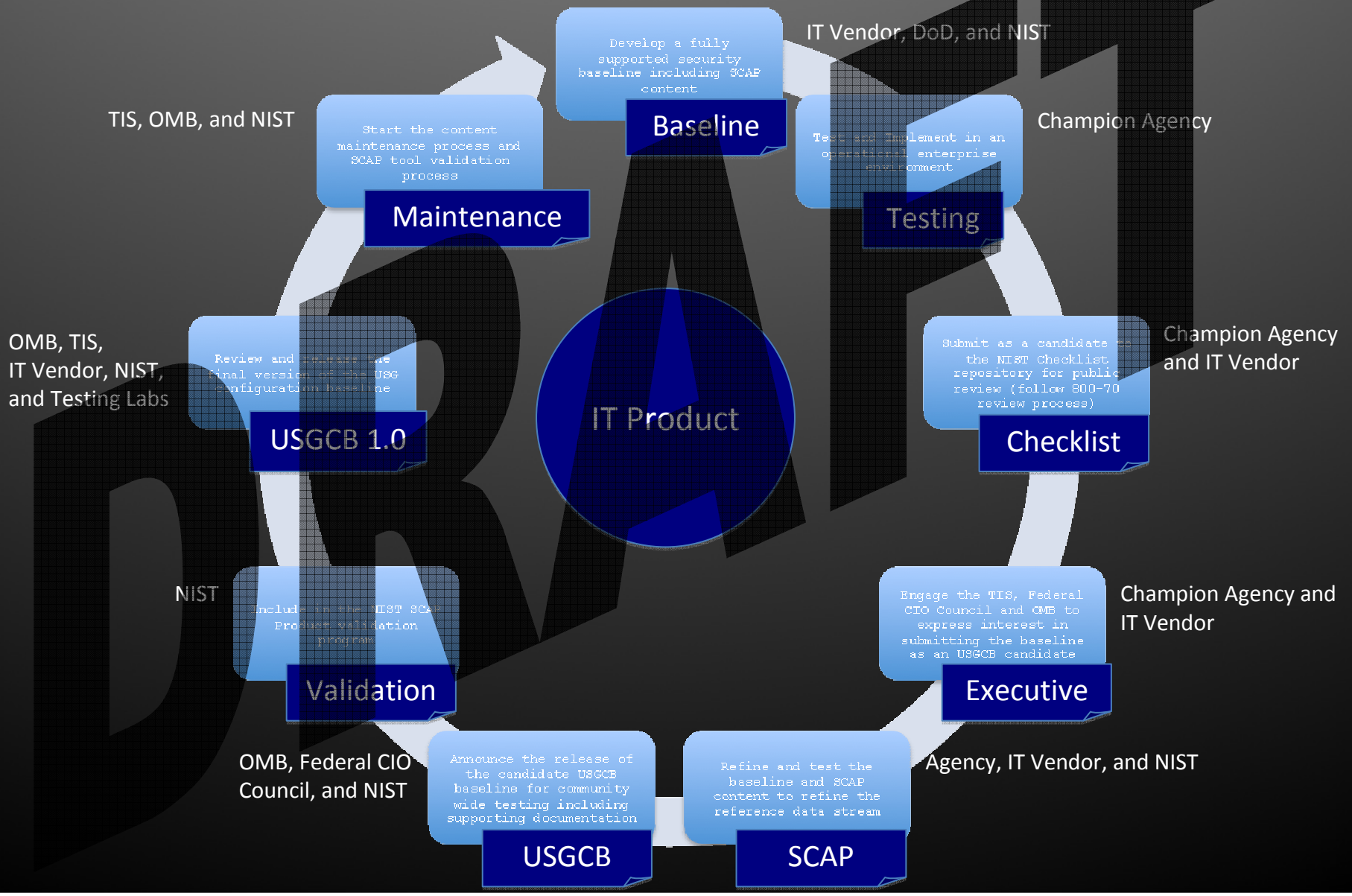


United States Government Configuration Baseline (USGCB)/FDCC

ISIMC

December 16, 2009

USGCB/FDCC Process



Current State: Windows 7 and IE 8

- Release of the Microsoft Security Guide for Windows 7 and Internet Explorer 8 (SSLF and Enterprise)
- Draft DoD security baseline for Win 7 and IE 8
- Missing SCAP supporting content
  - Microsoft is finalizing the data stream for SSLF
- No official candidate submission for the Windows 7 or IE 8 to the NIST Checklist Program
  - Microsoft is completing the submission package
- Normalizing the Win 7 and IE 8 settings with the existing FDCC recommendations for Vista, XP, and IE 7

Moving Forward

- DoD and Vendor submit the security baseline for IT products to the NIST Checklist program for public review
- Agencies can use it in the interim for testing and provide feedback
- Vendor and DoD will submit the supporting SCAP content for public review
- DoD will share the lessons learned as they deployed the vendor product with the proposed candidate USG configuration baseline
- NIST will collect the feedback from the community and complete the final recommendations
- OMB and TIC will review and approve the final recommendations
- NIST updates the SCAP validation program to the new vendor IT product

Resources

- http://scap.nist.gov
- NIST Special Publication 800-70Rev1 - http://csrc.nist.gov/publications/nistpubs/800-70-rev1/sp800-70r1.pdf
- http://fdcc.nist.gov
- NIST Special Publication 800-117 (Draft) - http://csrc.nist.gov/publications/drafts/800-117/draft-sp800-117.pdf
- NIST Special Publication 800-126 - http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf
- National Checklist Program Repository - http://web.nvd.nist.gov/view/ncp/repository