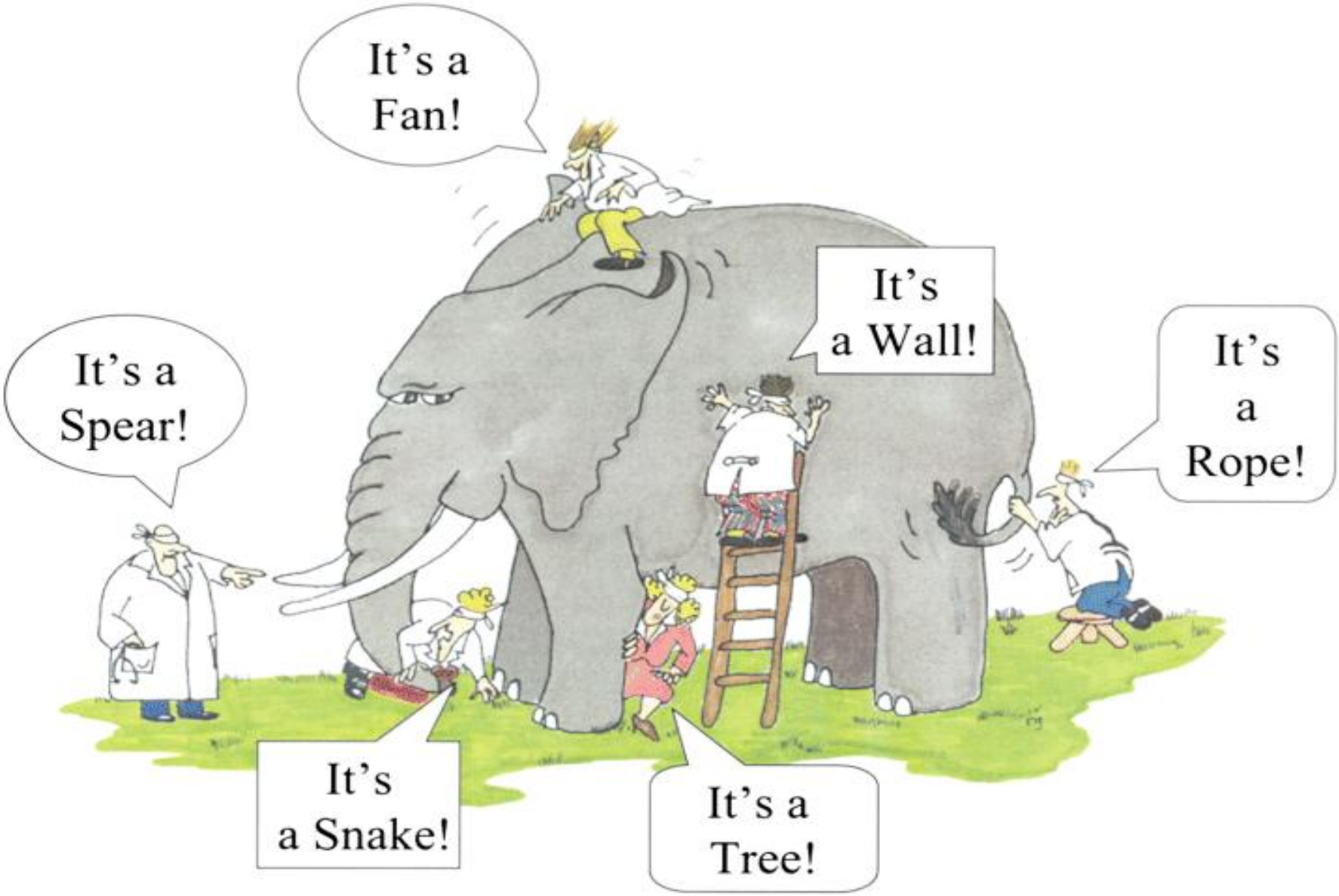

McAfee
An Intel Company
Continuous Monitoring
History and Directions
Kent Landfield, McAfee
SCAP Developer Days 2012
SAFE NEVER SLEEPS™

Continuous Monitoring – What is it?



Description applied to Cybersecurity for use with Technical Reference Architectures

McAfee
An Intel Company

Continuous Monitoring Defined

"Continuous Monitoring is a risk management approach to cybersecurity that maintains an accurate picture of an organization's security risk posture, provides visibility into assets, and leverages use of automated data feeds to quantify risk, ensure effectiveness of security controls, and implement prioritized remedies."

-NIST

DHS – Continuous Monitoring

- Build capability using existing data feeds and tools
  - Component based approach
  - Based on a standardized reference architecture
  - Focused on security controls in NIST SP 800-53/CAG
  - Solutions from multiple vendors can be combined together to create a CM solution
- Phase in additional capabilities in a logical manner
- Converges with capabilities found in FISMA
- Auto Feed Metrics Requirements
  - Asset Management (CPE)
  - Configuration Management (CCE)
  - Vulnerability Management (CVE)

DHS Continuous Monitoring Evolution

- Expanded scope of auto feed metrics
- Boundary Defense
- Audit Log Analysis
- Application Security
- Privileges
- Access
- Dormant Accounts
- Ports, Protocols, and Services
- Data Leakage Protection
- Others

Derived Capabilities of a CM Program

- Maintains an accurate picture of an organization’s security risk posture
- Provides visibility into assets
- Leverages automated data feeds
- Allows for Quantification of risk
- Ensures continued effectiveness of security controls
- Informs automated or human-assisted implementation of remediation
- Enables prioritization of remedies
- Empowers employees at multiple levels within the organization

Important CM solution goals

McAfee
An Intel Company

- Component based approach
  - Based on a standardized reference architecture
  - Solutions from multiple vendors can be combined together to create a CM solution
- Standard-based for interoperability and scoring consistency
  - Languages
    - Using the same machine-readable expressions for checking and remediating machine state (e.g., FDCC / USGCB policy)
  - Metrics
    - Using the same equations for risk calculations
  - Nomenclatures
    - Using the same names for vulnerabilities, assets, configuration issues, and remediation options.
- Mathematically rigorous scoring approach
  - Motivational scoring is important
  - True risk calculations are also needed


McAfee
An Intel Company
History of the CM Effort
SAFE NEVER SLEEPS™

History

- Starting in 2002, FISMA required annual information security program reporting from federal agencies
- Cost since 2002 launch of FISMA reporting: **$40B+**
  - Only 32% of agencies received “good” or “excellent” FISMA grades in FY 2008
- White House directive to save costs: ***CyberScope***
  - All Federal agencies are mandated to use CyberScope for FISMA reporting by November 15, 2010
  - As implemented, frustrating for agencies
  - http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-15.pdf
- White House directive to shift to reporting FISMA related metrics through CyberScope on a monthly, not yearly basis
  - http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-33.pdf
- **BUT**:
  - CyberScope only a “baby step” to solve CM reporting requirement
  - Long term goal: smarter networks in which Ops can have greater risk visibility

A. Continuous Monitoring and Remediation

In FY 2011 the shift from the once-a-year FISMA reporting process to a monthly reporting of key metrics through Cyberscope will allow security practitioners to have more information than ever before to assist the protection of agency information and information systems. In the years to come, this reporting will require minimal human interaction and allow immediate remediation of many vulnerabilities.

While automation efforts such as the Security Content Automation Protocol (SCAP) and continuous monitoring are not magic solutions, they do offer enterprises of all sizes the ability to enhance one's security posture at lower costs. This work has begun to pave the way for new and robust capabilities that agencies can easily adopt in the future. Applying the continuous monitoring and remediation approach must be coupled with an increased engagement across government and industry to better cooperate to address information security.

Strengthening Security Management through CyberStat Model

To increase this cooperation, in January 2011, DHS launched CyberStat. Using the TechStatmodel, DHS cybersecurity experts will now meet with agencies regularly to ensure accountability and to help agencies develop focused actions plans to improve their information security posture. CyberStat is grounded in the data provided by CyberScope, among other key data sources about agencies' information security. The development of clear and consistent metrics for CyberScope has increased the ability of DHS to hold agencies accountable for outcomes. As DHS works with agencies to improve data quality, CyberStat and CyberScope will allow DHS to assist agencies in quickly addressing problems that pose risks.

History of the USG CM Reference Model

- September 2010
  - DHS Federal Network Security (FNS) Branch releases ***"Continuous Asset Evaluation, Situational Awareness, and Risk Scoring Reference Architecture Report (CAESARS)"***
- February 2011
  - ***[IR 7756] NIST Interagency Report 7756 - CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture (Draft)***
- March 2011
  - NIST held a ***" CONTINUOUS MONITORING ARCHITECTURE WORKSHOP"*** – Initial straw man presented but too high level and vendors asked for more specifics
- September 2011
  - ***[SP 800-137] NIST Special Publication (SP) 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations***
- December 2011
  - ***[IR 7799] NIST Interagency Report (IR) 7799 – Continuous Monitoring Reference Model Workflow, Subsystem, and Interface Specifications (Draft)***
- January 2012
  - ***[IR 7800] NIST Interagency Report 7800 - Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration, and Vulnerability Management Domains (Draft)***

Current Logistical Problems Facing CM

- Large installed base of security point products
- Lack of security automation standards to enable plug and play
- Lack of means to provide automated reach down and reporting to support federated network hierarchies
- The Continuous Monitoring Reference Architecture is more notional than reality
- Must achieve some successes today while the interface and extended security automation data model specifications are developed
  - iPost model for reporting various gather metrics


McAfee
An Intel Company
CyberScope & CAESARS FE
SAFE NEVER SLEEPS™

Differences Between CyberScope and CAESARS

McAfee
An Intel Company

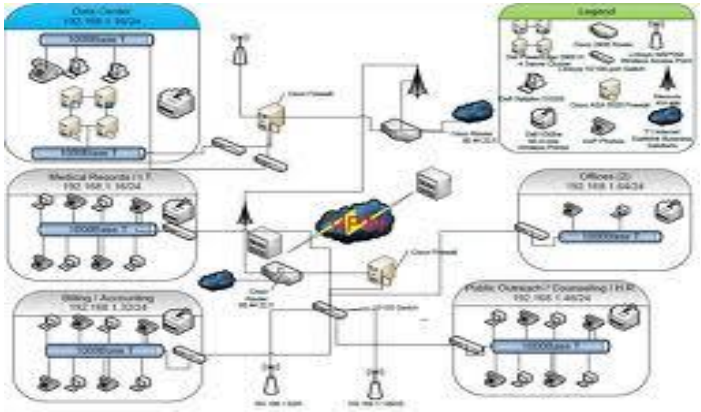
CyberScope

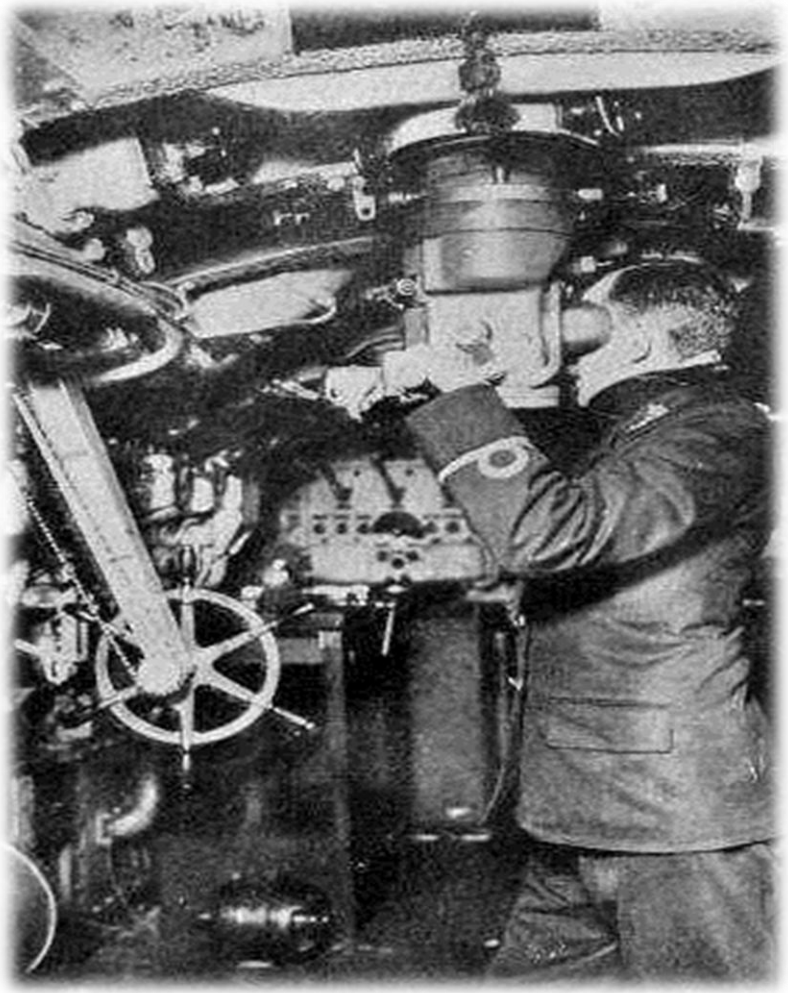
- Reporting at a very high level
- Currently file based transmission of results
- Hope to be automated at some point in the future
- Agencies manually transmit the collected information to the CyberScope POC
- More FISMA and CIO focused

CAESARS FE

- A "target-state reference architecture" that *scales* for *large* government enterprise networks
- *Not* an output - a *vision* for longer term, better risk visibility
- Goal: Full plug and play network environment that can facilitate better visualization and network event awareness
- More operations focused

CyberScope





CyberScope requests

- Asset Inventory using SCAP Common Platform Enumerations (“CPE”) to report on total systems by CPEs.

- Configuration Data that uses checklists written using SCAP Extensible Configuration Checklist Description Format (“XCCDF”) to report on systems security SCAP Common Configuration Enumerations (“CCE”). Each CCE associated within a specific XCCDF benchmark are evaluated and reported within the submission.

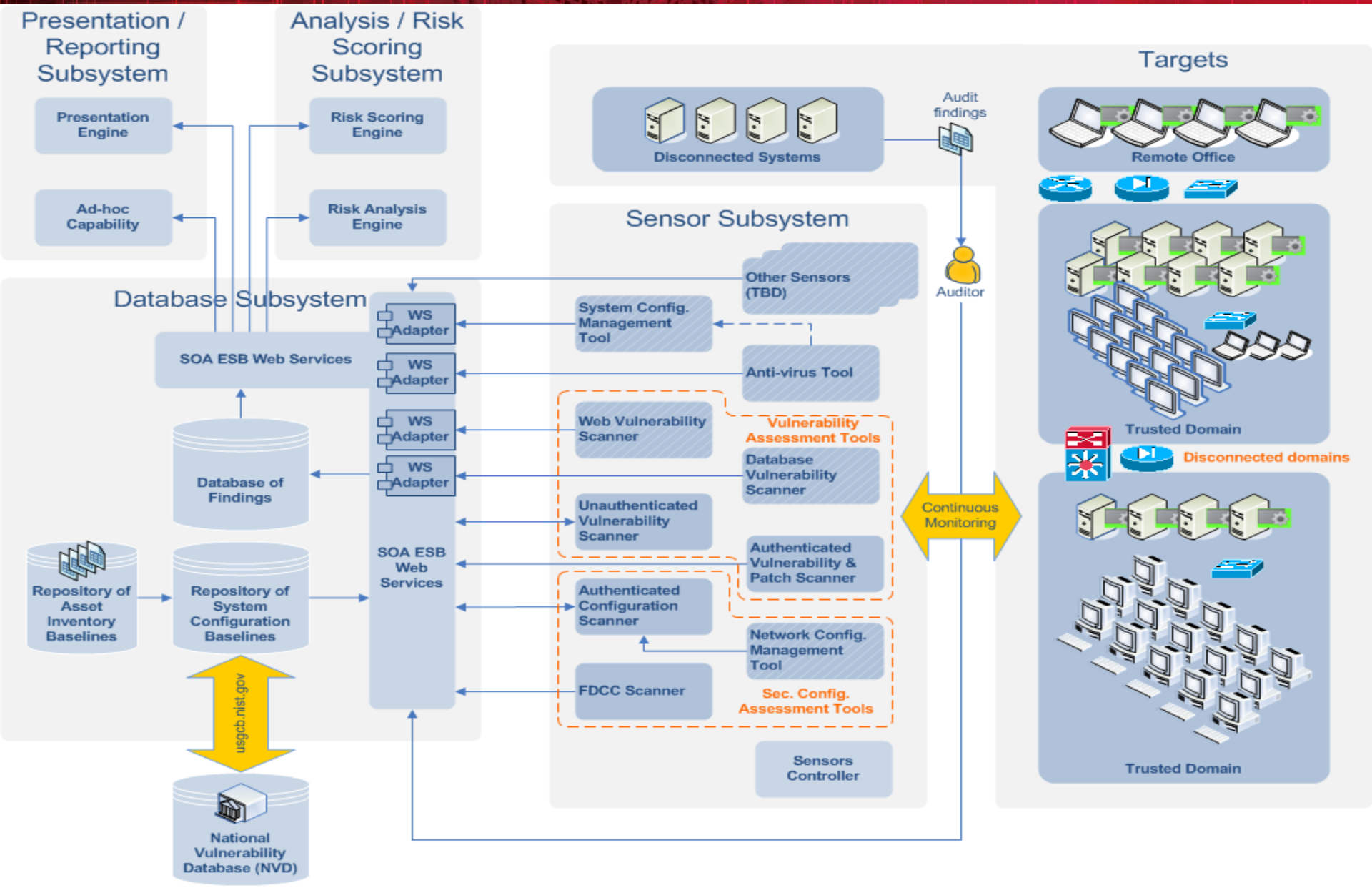
- Common Vulnerability Enumerations (CVEs) to report on CVEs within a specific environment and an aggregate value of systems affected by the specific CVE.

CAESARS

Continuous **A**sset **E**valuation, **S**ituational **A**wareness, and **R**isk **S**coring Reference Architecture

Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS)

McAfee
An Intel Company

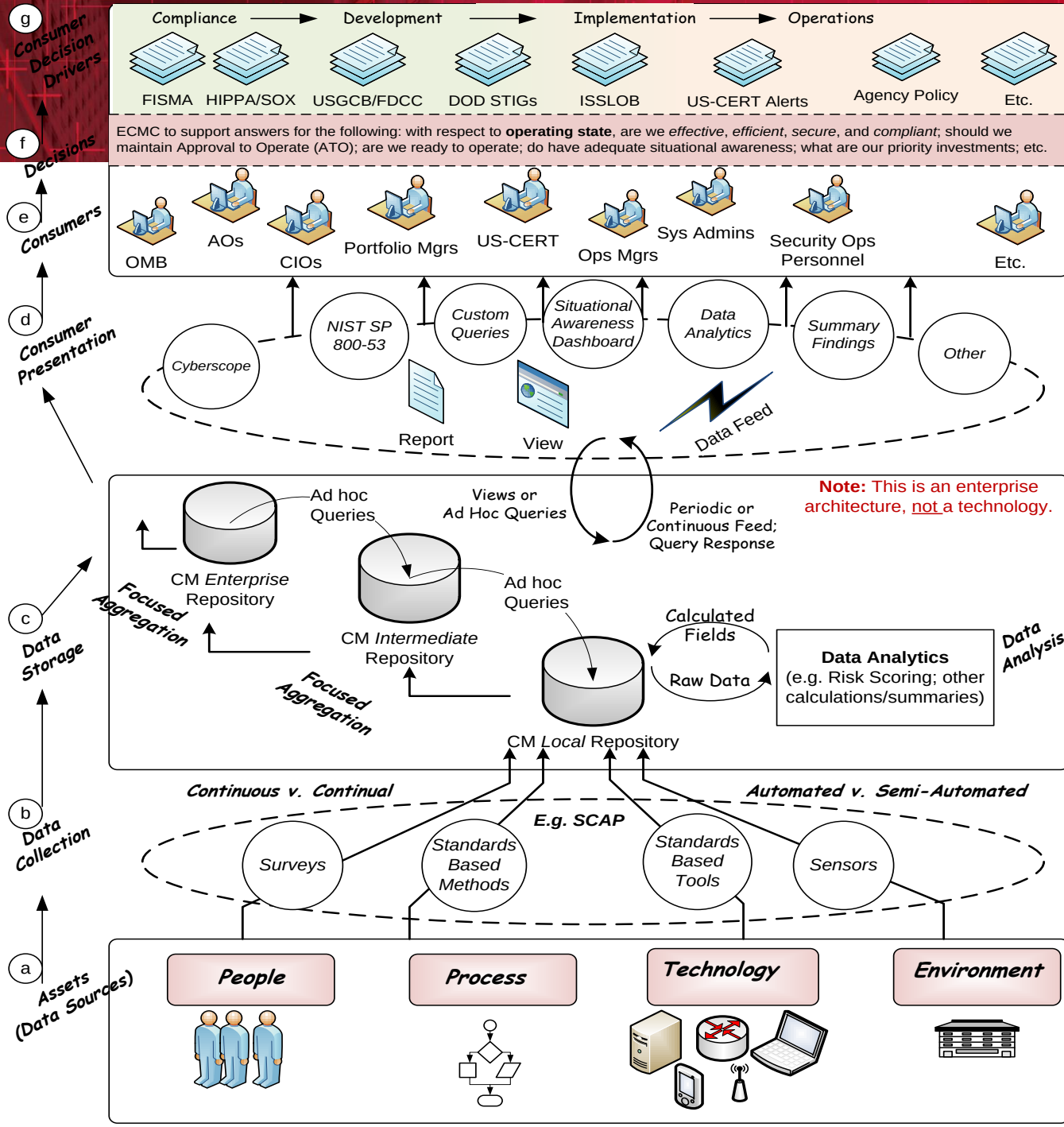


CM Enterprise Architecture

- **This shows an enterprise architecture view, not a technology focus view**

Source: NIST IR 7756

Note: Diagram derived from NSA work (original diagram credit: Keith Willett, MITRE)

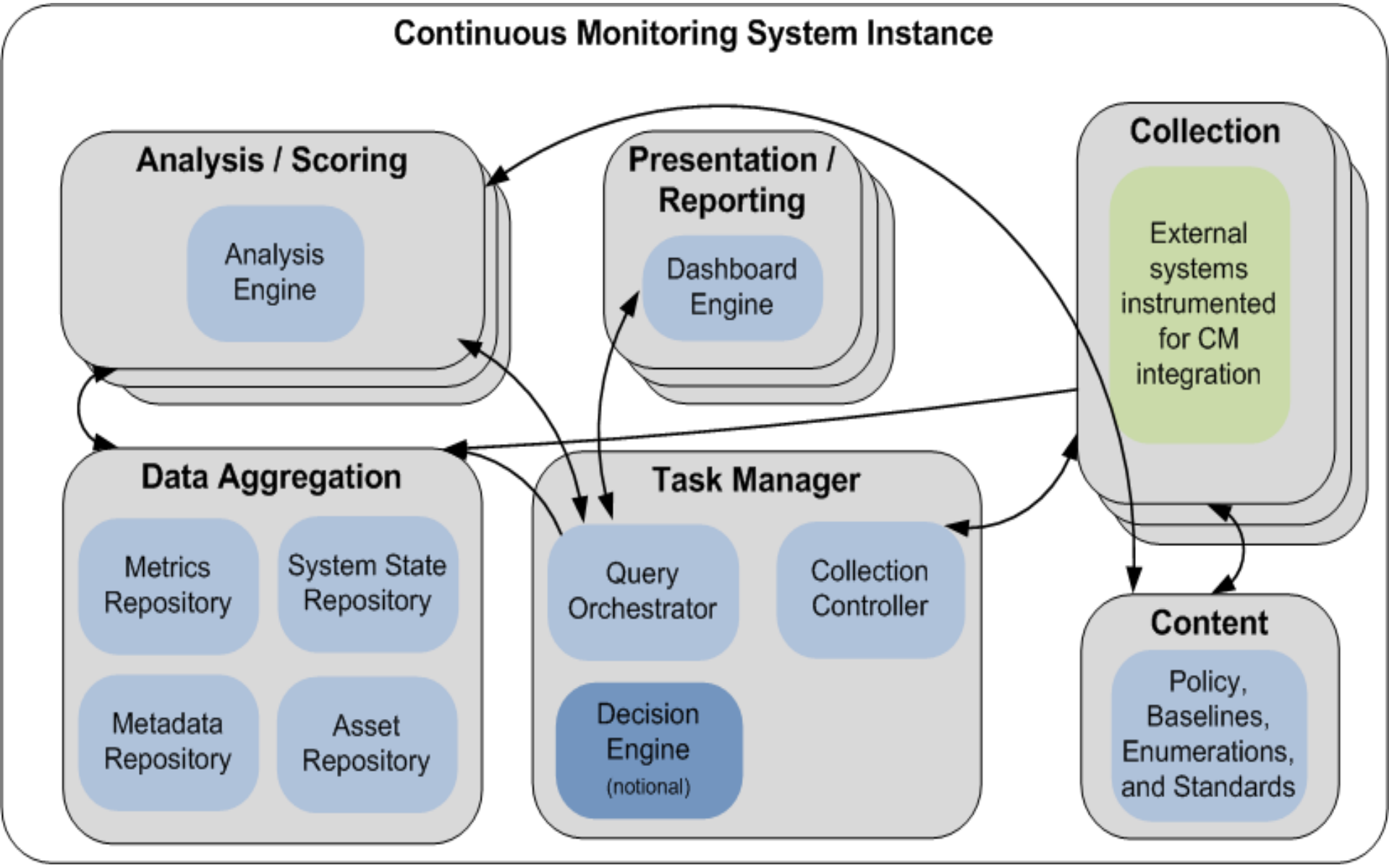


CAESARS FE and the Continuous Monitoring

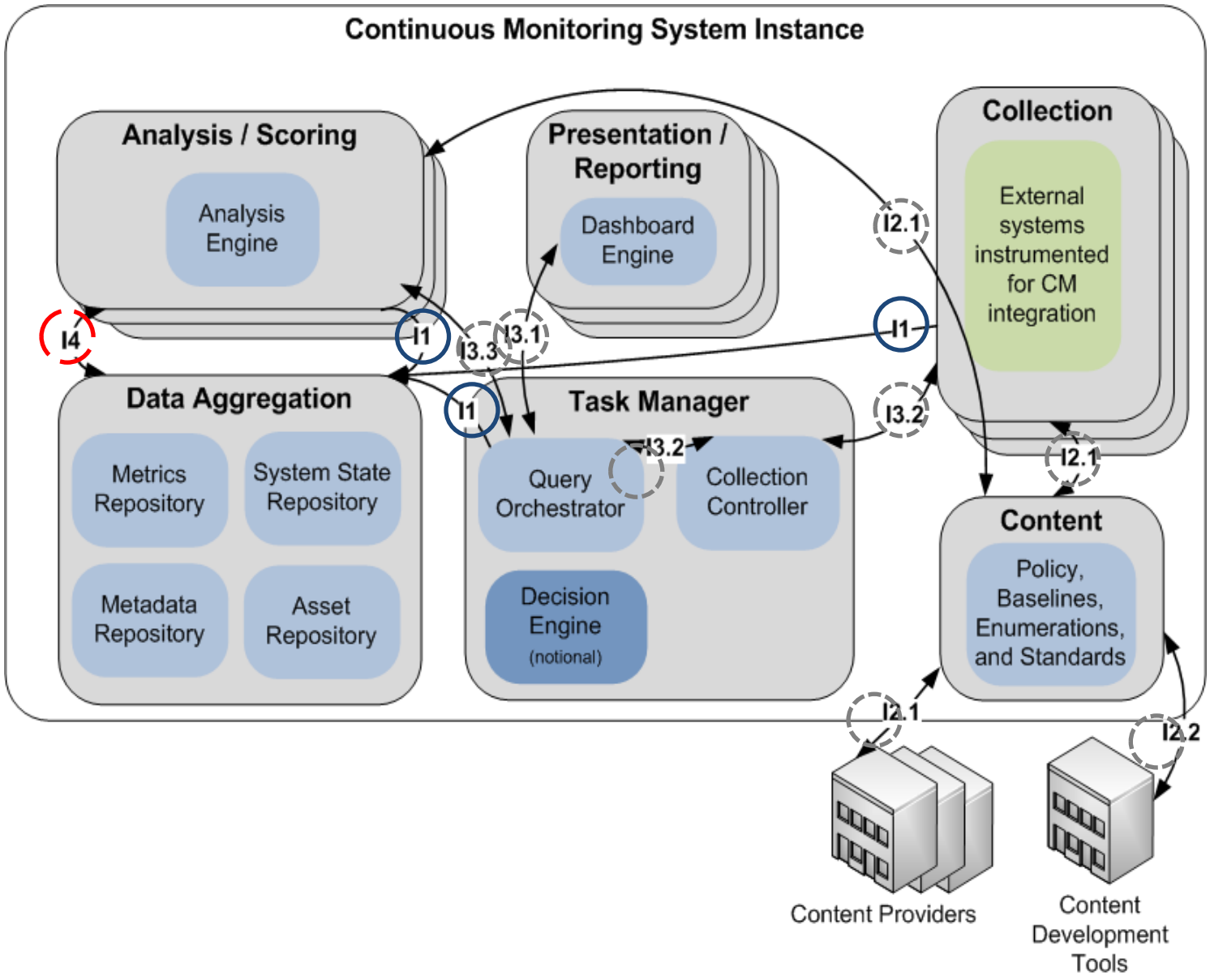
- CAESARS Framework Extension
  - Corrected issues in DHS CAESARS specification
  - http://csrc.nist.gov/publications/PubsDrafts.html
  - NIST-IR-7756

- Desire is to have a ‘plug and play’ environment for security products
- Best of Breed procurement capabilities
- Provide support for operations
- Ability to Abstract Gathered Data for Decision Makers
- Drill down when needed
- Automated Roll up for Data Calls
- New Standards needed (connection protocols and data models)
- Procurement wording to include support for this architecture
- Focusing on Situational Awareness Capabilities

CM Instance Model
(Organizations may have multiple CM instances)



CM Instance Model Proposed Interfaces



Interface Specifications:

- Existing/ Standardized
- Current focus/ Parameterized
- Future Focus/ Proprietary


McAfee
An Intel Company
Continuous Monitoring: Phase 1
Risk Scoring and iPost
SAFE NEVER SLEEPS™

iPost

- Custom application that continuously monitors and reports risk on the IT infrastructure at US Department of State
- The risk scoring program uses data integrated into iPost from various monitoring tools to produce a holistic view of vulnerabilities
- Each host and user is scored in multiple categories using the NVD CVSS scoring system
- Scores are aggregated across categories to give a risk score for the host, site, region or enterprise
- Small and large sites are compared via normalized scores
- Letter grades are applied based on normalized scores
- Exception capabilities are provided for dealing with anomaly situations

iPost background

- NIST, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, Special Publication 800-37 (Gaithersburg, Md.: February 2010).
- Although iPost does not provide a complete view of information security risks, it helps to prioritize vulnerability mitigation efforts
- iPost Risk Scoring Program only addresses Windows host computers
- iPost's Risk Scoring Program Address several but not all NIST SP 800-53, rev. 3 IA controls

Scoring Components of State's Risk Scoring

Scoring Component	What is Scored	Source
1. Vulnerability	Vulnerabilities detected on a host	Scanning Tool
2. Patch	Incompletely installed or uninstalled patches required by a host	SMS
3. Security Compliance	Failures of host to use required security settings	Scanning Tool
4. Anti-Virus	Out-of-date anti-virus signature file	SMS
5. Standard operating environment compliance	Incomplete/invalid installations of any product in the Standard Operating Environment suite, of which there are 19 products	SMS
6. AD users	User account password ages exceeding 60-day threshold (scores each user account, not each host)	AD
7. AD computers	Computer account password ages exceeding 30-day threshold	AD
8. SMS reporting	SMS client agent on host is not reporting all expected information and and the incomplete reporting is due to specific types of errors	SMS
9. Vulnerability reporting	Hosts that miss two consecutive vulnerability scans	Scanning tool
Security compliance reporting	Hosts that miss two consecutive security compliance scans	Scanning tool

iPost Scoring Guidelines

McAfee
An Intel Company

Component	Risk Score	Avg / Host	% of Score	How Component is Calculated
VUL - Vulnerability	947.0	3.0	10.9 %	From .1 for the lowest risk vulnerability to 10 for the highest risk vulnerability
PAT - Patch	603.0	1.9	6.9 %	From 3 for each missing "Low" patch to 10 for each missing "Critical" patch
SCM - Security Compliance	6,181.2	19.5	71.2 %	From .9 for each failed Application Log check to .43 for each failed Group Membership check
AVR - Anti-Virus	0.0	0.0	0.0 %	6 per day for each signature file older than 6 days
SOE - SOE Compliance	115.0	0.4	1.3 %	5 for each missing or incorrect version of an SOE component
ADC - AD Computers	26.0	0.1	0.3 %	1 per day for each day the AD computer password age exceeds 35 days
ADU - AD Users	222.0	0.7	2.6 %	1 per day for each account that does not require a smart-card and whose password age > 60, plus 5 additional if the password never expires
SMS - SMS Reporting	230.0	0.7	2.6 %	100 + 10 per day for each host not reporting completely to SMS
VUR - Vulnerability Reporting	84.0	0.3	1.0 %	After a host has no scans for 15 consecutive days, 5 + 1 per 7 additional days
SCR - Security Compliance Reporting	279.0	0.9	3.2 %	After a host has no scans for 30 consecutive days, 5 + 1 per 15 additional days
Total Risk Score	**8,687.1**	**27.4**	**100.0 %**	

For additional information on Risk Scoring, assistance with remediations, or to report suspected false positives, contact the IT Service Center to open a "Risk Score" ticket.

iPost Component Scoring Methodology

Scoring	How the Score is calculated for a host
1. Vulnerability	Sum of vulnerability scores of all detected vulnerabilities. Scores for individual vulnerabilities range from 0.01 and .1 for the lowest-risk vulnerability to 10 for the highest risk vulnerability.
2. Patch	Sum of patch scores of all incompletely installed patches. Each patch is assigned a score based on its risk level: low = 3, medium = 6, high = 9, and critical = 10.
3. Security Compliance	Sum of all scores of all failed security compliance checks. According to one screen, the scores can range from .43 to .9 for each instance of security noncompliance. (settable)
4. Anti-Virus	After a grace period of 6 days, a score of 6 per day is assigned to a host with an old antivirus signature file
5. Standard operating environment compliance	Score of 5 assigned for each missing or unapproved version of a standard application.
6. AD users	Score of 1 assigned for each day an account that does not require a smart-card, and are not disabled or expired, and whose password age exceeds 60 days. Accounts that have no date in AD for the last password reset are assigned a fixed score of 200. If the password is set to never expire, an additional score of 5 is assigned.
7. AD computers	Score of 1 assigned for each day password age exceeds 35 days. (settable)
8. SMS reporting	One hundred plus 10 for each day since last day agent correctly reported. Before scoring begins, there is a grace period that varies from 5 to 30 days, depending on the error conditions detected.
9. Vulnerability reporting	Vulnerability reporting After a host has not been scanned in 15 consecutive days, a score of 5 is assigned, then increased at the rate of 1 for each additional 7 days. (settable)
Security compliance reporting	After a host has not been scanned for 30 consecutive days, a score of 5 is assigned, then increased at the rate of 1 for each additional 15 days. (settable)

Resource Links Available to Users in iPost

Resource	Description
Patch Management Web Site	Facilitates the management, installation and monitoring or Window operating system patches
SMS post admin tool	Allows and SMS Administrator to accomplish tasks required to administer an SMS system
IT Change Control Board baseline	Includes a list of approved hardware and software that can be used on department systems that has been approved by the IT Change Control Board, which manages and approves changes to the department's IT infrastructure
Site Risk Scoring Toolkit	Provides online reference documents that iPost users can utilize for evaluating the site risk data and scores located in iPost
IT Asset Baseline	Maintains the department's IT asset inventory
Diplomatic Security configuration guides	Documents the required configuration settings that should be in place for various operating systems
IT Service Center	Provides technical support for department users on IT-related issues

CAG ID	Consensus Audit Guidelines
1	Inventory of authorized and unauthorized hardware
2	Inventory of authorized and unauthorized software
3	Secure configurations for HW and SW, if available
4	Secure configurations for network devices such as firewalls and routers
5	Boundary Defense
6	Maintenance/Analysis of complete security audit logs
7	Application software security
8	Controlled use of Administrative Privileges
9	Controlled access based on need to know
10	Continuous vulnerability testing and remediation
11	Dormant account monitoring and control
12	Anti-malware defenses
13	Limitation and control of ports, protocols and services
14	Wireless device control
15	Data leakage protection


McAfee
An Intel Company
Continuous Monitoring: Phase 2
Bringing Definition to the CM Technical Reference Architecture
SAFE NEVER SLEEPS™

Continuous Monitoring Interface Standards

- Need to develop the plug and play connections standards for the Query Management, Collection Controller, etc.
- Need to create data models to support queries and tasks
- Needless to say there is a great deal of work here that will not happen quickly
- Vendors need to participate and contribute where it makes sense

Resources

- **OMB M-10-15**, *FY2010 Reporting Instructions for the Federal Information Security Management Act (FISMA) and Agency Privacy Management*
  - http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-15.pdf
- DHS specifies **CAESARS** September 2010:
  - http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf
- NIST CM policy guidance in **NIST Special Publication 800-137** - DR*AFT Information Security Continuous Monitoring for Federal Information Systems and Organizations:*
  - draft-SP-800-137-IPD.pdf
- NIST-issued **CAESARS Framework Extension (FE)**:
  - http://csrc.nist.gov/publications/drafts/nistir-7756/Draft-nistir-7756_feb2011.pdf
- Continuous Monitoring Architecture Workshop 2011 Presentations:
  - http://scap.nist.gov/events/2011/cm_workshop/presentations/index.html
- Security Automation Developer Days Winter 2011 Presentations:
  - http://scap.nist.gov/events/2011/saddsp/presentations/index.html