



Continuous Monitoring Capability

16 March 2011



CM: Not an Option



- **Presidential Awareness**

“A critical aspect for agency officials of managing risk to information from the operation and use of information systems involves the continuous monitoring of the security controls employed within or inherited by the system.” - Vivek Kundra, Federal CIO, Testimony on Federal Information Security, March 24, 2010

- **Legislation**

“The Secretary of Defense shall direct the Chief Information Officer of the Department of Defense to ... to achieve, to the extent practicable, the following: (2)The automation of continuous monitoring of the effectiveness of the information security policies, procedures, and practices within the information infrastructure of the Department of Defense, and the compliance of that infrastructure with such policies, procedures, and practices.” - S. 3454, National Defense Authorization Act for FY 2011

- **Public Pressure on OMB WRT Perceived FISMA Shortcomings**

“Continuous monitoring enables government agencies to respond quickly and effectively to common and new attack vectors... The original FISMA did just the opposite – it slowed down every process and took key resources away from projects that would allow agencies to act and react more quickly. ” - Alan Paller, Director of Research, The SANS Institute, Testimony on Federal Information Security, March 24, 2010



NDAA

H. R. 6523—198

Subtitle D—Cyber Warfare, Cyber Security, and Related Matters



SEC. 931. CONTINUOUS MONITORING OF DEPARTMENT OF DEFENSE INFORMATION SYSTEMS FOR CYBERSECURITY.

(a) **IN GENERAL.**—The Secretary of Defense shall direct the Chief Information Officer of the Department of Defense to work, in coordination with the Chief Information Officers of the military departments and the Defense Agencies and with senior cybersecurity and information assurance officials within the Department of Defense and otherwise within the Federal Government, to achieve, to the extent practicable, the following:

(1) The continuous prioritization of the policies, principles, standards, and guidelines developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) based upon the evolving threat of information security incidents with respect to national security systems, the vulnerability of such systems to such incidents, and the consequences of information security incidents involving such systems.

(2) The automation of continuous monitoring of the effectiveness of the information security policies, procedures, and practices within the information infrastructure of the Department of Defense, and the compliance of that infrastructure with such policies, procedures, and practices, including automation of—

(A) management, operational, and technical controls of every information system identified in the inventory required under section 3505(c) of title 44, United States Code; and

(B) management, operational, and technical controls relied on for evaluations under section 3545 of title 44, United States Code.

(b) **DEFINITIONS.**—In this section:

(1) The term “information security incident” means an occurrence that—

(A) actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information such system processes, stores, or transmits; or

(B) constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies with respect to an information system.

(2) The term “information infrastructure” means the underlying framework, equipment, and software that an information system and related assets rely on to process, transmit, receive, or store information electronically.

(3) The term “national security system” has the meaning given that term in section 3542(b)(2) of title 44, United States Code.



CM/RS in DoD



- OSD/CIO - Lead DOD strategy and implementation
- DIAP - Develop and publish:
 - Continuous Monitoring Capability & Risk Scoring (CM/RS) Plan (Current version 0.7.2)
 - Communication Strategy – consistent message on future
 - Misconception – CM/RS is the same for all
 - Truth- CM/RS is based on the “eye” (requirements) of the Consumer
 - Working Group Charter
 - Align authorities
 - Assign roles and responsibilities (CM/RS CCB staffed)
 - Formalize requirements and maturity level concepts
- Emphasize DOD requirements
 - Develop DoD interface for DHS CyberScope
 - “Automate the automatable”
 - Align to Federal reporting requirements



CM/RS in DoD



- Align consumers
 - USCYBERCOM, CC/S/A/FA & SEs, CNDSPs, Mission Assurance, etc.
 - Define enterprise capability/requirement once – reuse imperative
- Funding Options: *Map currently deployed systems to the strategy (efficiencies, gaps, capabilities, redundancies)*
 - Review existing DOD/DISA programs for CM/RS applicability
 - Review planned DOD/DISA funding for CM/RS applicability
 - Identify efficiencies for reprioritization of funding from existing non-automated or duplicated solutions
- Strategy development
 - CC/S/A/FA & SE engagements
 - Quarterly symposiums (proposed)
 - Identify, record, assess, and resolve issues
 - Map out “RISK” scoring objectives

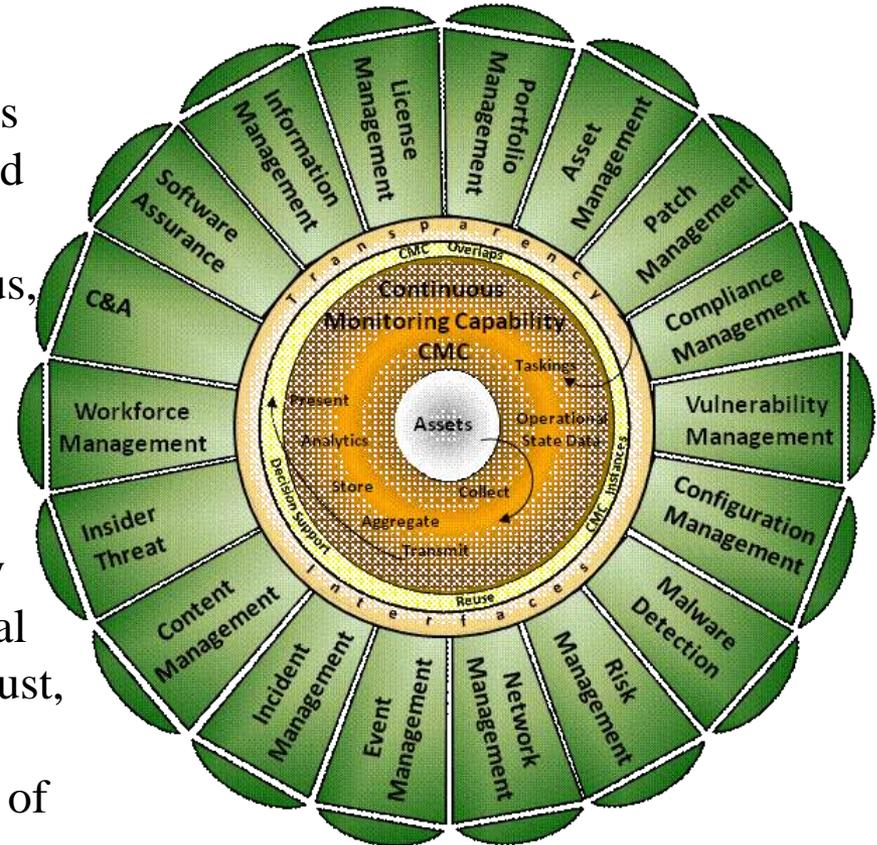


CM/RS in DoD



Definition:

- The term continuous monitoring for DoD is the capability to execute the assessment and management of organization business and operational domains to determine status, risk, and readiness postures that will enhance (expedite) leadership decision-making and authorized response.
- CMC can be seen as the capability to unify existing disparate capabilities of operational management and control to build out a robust, automated and integrated solution for expedited decision processes of all aspects of future computer network operations.
- Executed through a Maturity Level Concept



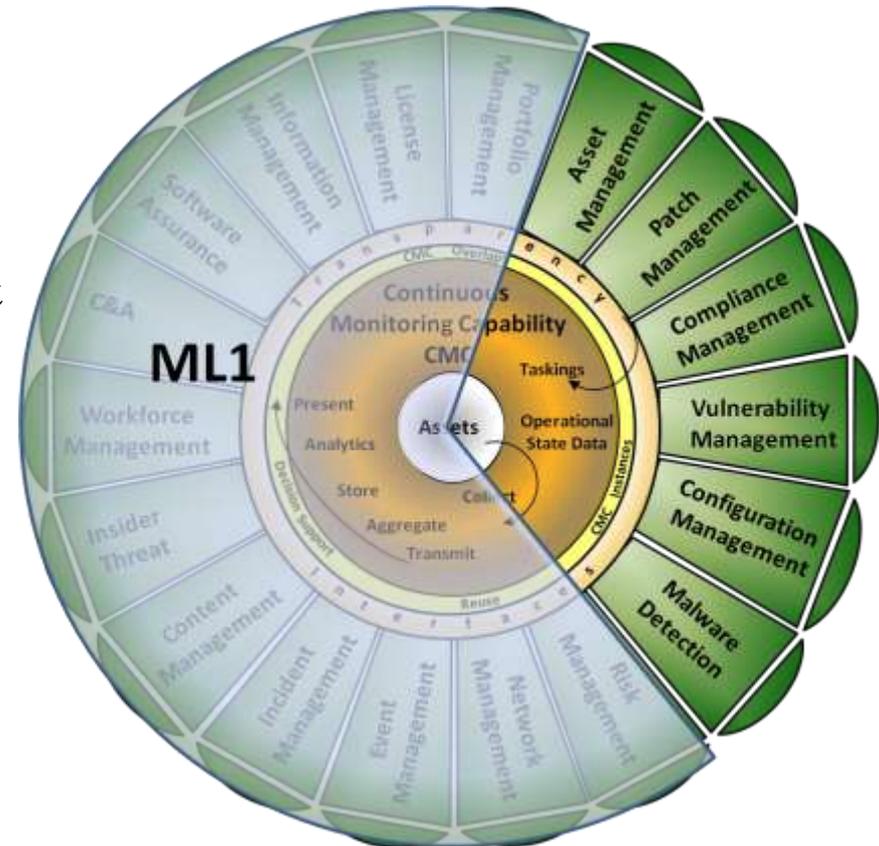


ML1 in CMC



Authoritative Repositories

- Requires the creation and management of an authoritative asset-state repository
- Owned and/or managed by the CC/S/A/FA & SEs:
 - Phase 1: Desktops (Windows OS platform)
 - Phase 2: Servers (Windows OS platform)
 - Phase 3: Mobile Devices (Laptops, PDAs, etc.)
 - Phase 4: Network Devices (Routers, Switches, Firewalls, etc.)
 - Phase 5: Desktops & Servers (non-Windows OS platform)
 - Phase 6: Program(s) of Record (POR)





ML2 in CMC

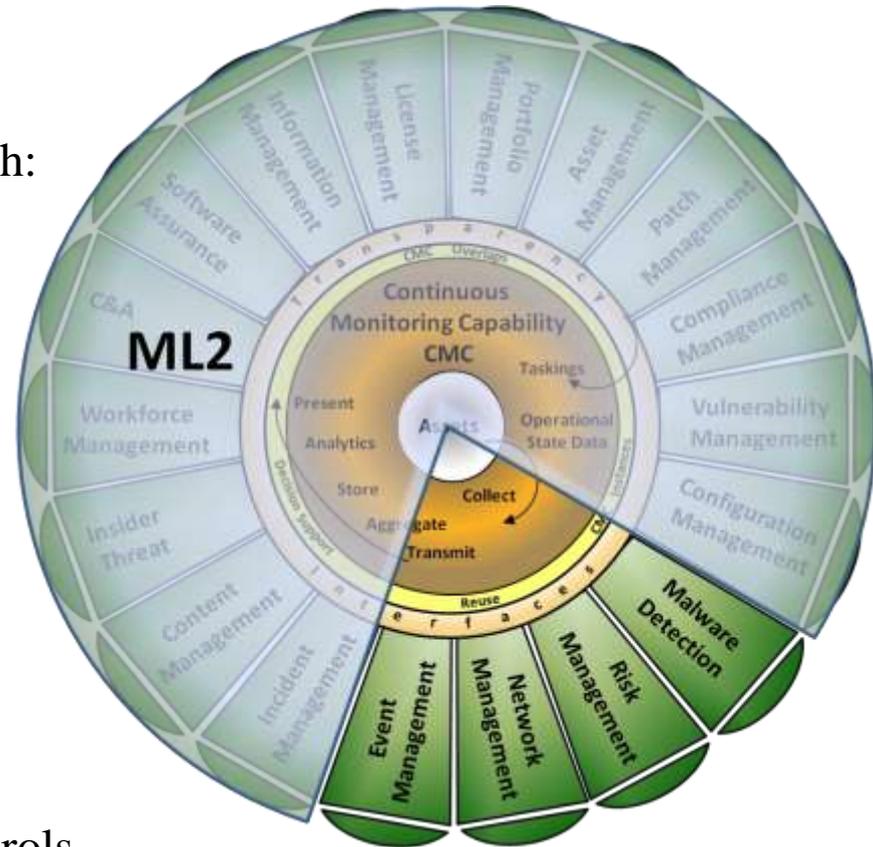


Risk Posture Capabilities

Focuses on Desktop/Network inventories through:

- Analysis Tools
- Risk Scoring enabled applications/software
- Compliance Assessment
- Security Standard
- Security Control Metrics Integration
- Enforcement of configuration/compliance
- Integrated Services
- Intentionally assumed position on all enterprise risk implementations.

Community NETOPS standards and capabilities created to manage, assess, or measure these controls in a consistent, appropriate, or automated manner





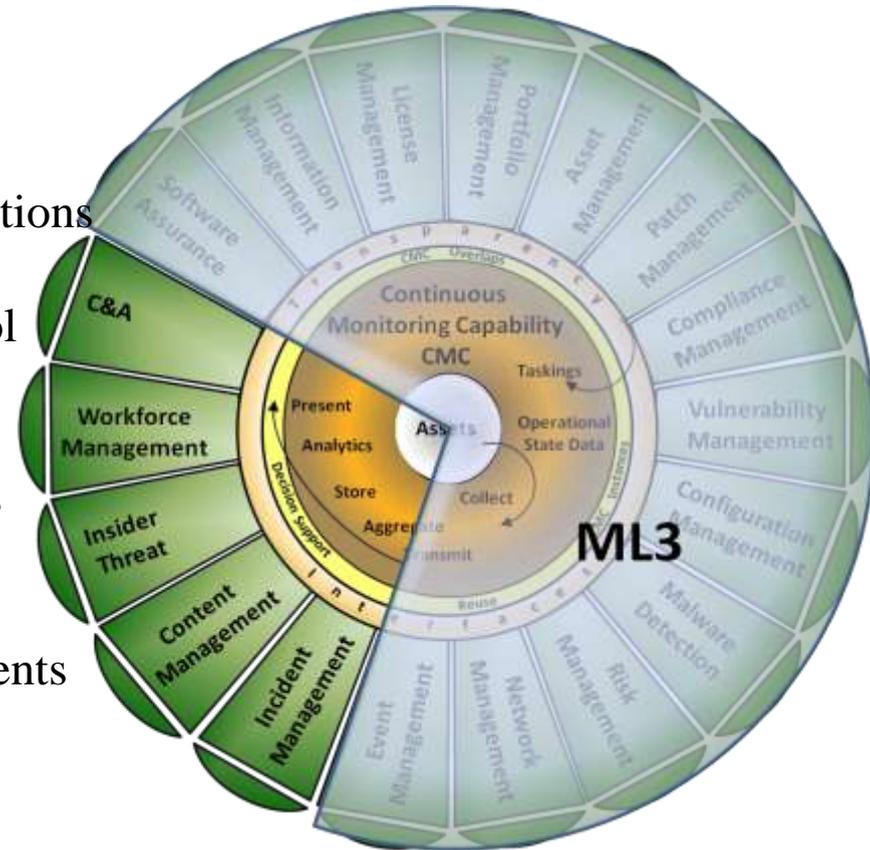
ML3 in CMC



Gain efficiencies in security posture focus

Focuses include:

- Audit Monitoring to detect vulnerable conditions and/or their exploitability
- Privileged and Non-privileged access control processes
- Security Services (i.e. CNDSP services)
- Security Tool configurations and validations
- Enhanced C&A (i.e. eMass) integration.
- Automated configuration, auditing, operational, workforce, & business assessments
- Security Status Policy Guidance
- Red/Blue Team Integration
- Identify controls that are ineffective
- Identifies services and mechanisms to identify, share, transfer, and mitigate risk.





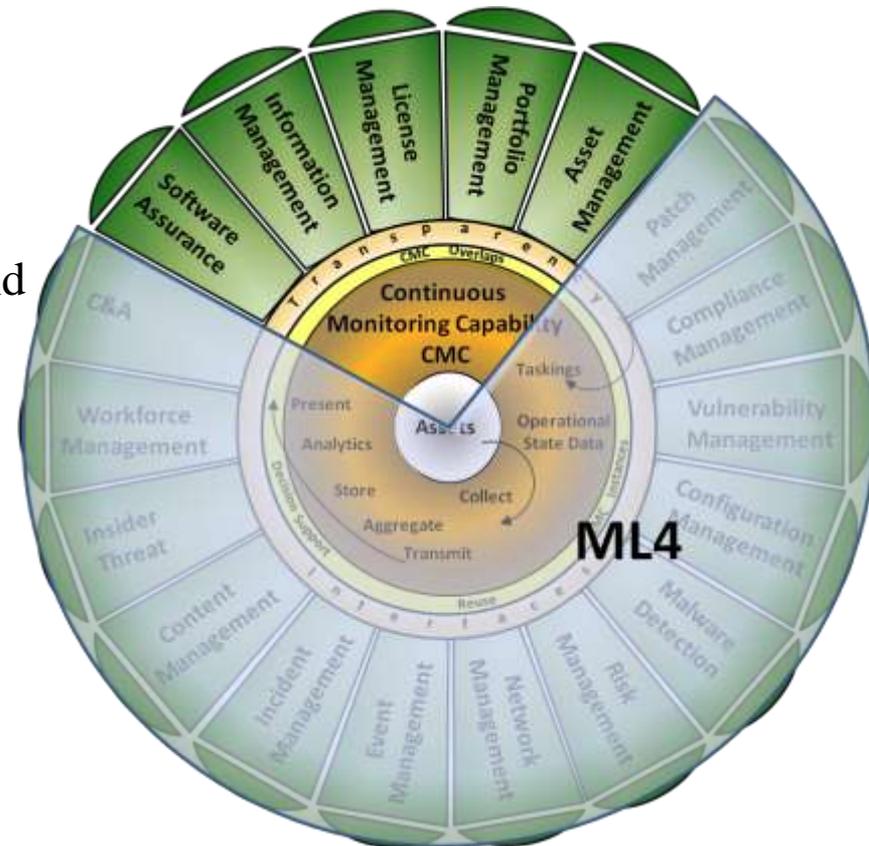
ML4 in CMC



Enterprise integration and support

Focuses include:

- Threat Vector Integration
- Dynamic RS Execution real-time, on demand
- Compliance Automation.
 - Every host
 - Every deficiency
- Adaptive Assessments.
- Positive Management.
- Redundancies Eliminated.
- Infrastructure Devices.
- Capability Driven Processes
- Managed risk with Mission Assurance Operational focus.
- Automated Querying Language.
- Integrated assessment and remediation managers





Q's & P's



Kevin M. Dulany CISSP, CISM, CISA, CAP, PMP
DoD-CIO, DIAP
Comm: 703-602-9994 DSN:332-9994
Kevin.Dulany@osd.mil

Greg Weaver CISSP/GCIH
DoD-CIO, DIAP (IBM)
Comm: 703-602-9965 DSN:332-9965
greg.weaver.ctr@osd.mil