

# Continuous Diagnostics and Mitigation Civilian FY 2013 Implementation - Priority Tools Phase I

Mark Crouter

The opinions expressed in this presentation are those of the speaker and do not represent the position of The MITRE Corporation or its government sponsors.

# Tool Function Overview

- Know the Desired State
- Know the Actual State
- Know the Differences
  - Between Actual and Desired States and
  - Automatically or Manually Act On the Differences
- Group Items Found for Reporting
- Interoperate
- Scale
- Secure Data Collected

# Hardware Asset Management (HWAM)

- Desired State: Create, operate, and maintain an inventory baseline of authorized HW, including unique identifiers for hardware, who manages it, and other properties.
- Actual State: Create, operate, and maintain the actual inventory of all authorized/unauthorized and managed/unmanaged hardware in near-real time, along with information needed to assess the risk, assign responsibility to, and physically locate the hardware.
- Determine the difference between the authorized hardware inventory baseline and the actual hardware inventory. Differences include both missing and extra devices.
- Assign risk to each difference based on relevant scoring factors.
- Address the risk. Provide the information needed to:
  - Assign the hardware for management and disposition manually or automatically.
  - Remove or authorize any unauthorized hardware promptly
  - Bring missing authorized hardware back into operation promptly, record its non-operational status, or de-authorize the hardware.

# Software Asset Management (SWAM)

- Desired State: Create, operate, and maintain an authorized software inventory, unique identifiers for software, the assigned manager of the software, and other properties.
- Actual State: Create, operate, and maintain the actual inventory of authorized and unauthorized software in near-real time, along with information needed to assess the risk to and physically locate the SWCIs (incl. manager assigned).
- Determine the difference between the authorized software inventory baseline and the actual software inventory.
- Assign risk to each difference based on relevant scoring factors.
- Address the risk. Provide the information needed to:
  - Assign software for management and disposition (i.e., authorization for software to operate on, or be removed from, the network) manually or automatically.
  - Fix or disposition software when authorized software inventory baseline and actual software inventory differ.

# Configuration Management (CM)

## (Configuration Setting Management)

- Desired State : Establish authorized security configuration benchmarks, consisting of the acceptable value(s) for each relevant configurable setting for each IT asset type.
  - Establish a core federal benchmark for hardware devices and software.
- Desired State : Allow departments and agencies (D/As) to adopt the federal benchmark and/or:
  - Add, modify, and delete non-core configuration settings.
  - Assign alternate method to score risk for internal D/A use.
  - Manage a change control process that documents D/A extensions or exceptions.
- Actual State: Determine the value of the actual settings within the authorized security configuration benchmark tool.
- Report the difference between authorized security configuration baseline and actual assessment results (non-compliant settings) with relevant risk scores.
- Address the risk.
  - Prioritize reported differences using the federal and D/A scoring rules.
  - Act to change or accept the configuration setting differences.

# Vulnerability Management (VUL)

- Desired State: Eliminate known vulnerabilities and software weaknesses for which patches or other remediation are available. Reduce exposure to exploitation by removing most serious weaknesses first.
- Actual State: Discover, identify, and locate known security vulnerabilities in software.
- Actual State: Discover, identify, and locate other known software weaknesses in software applications and source code.
- Report the Difference: Support the awareness and understanding of potential exposure risks associated with software weaknesses.
- Assign Risk:
  - Assign responsibility for vulnerability risk based on asset ownership and business rules.
  - Use available standards (CVSS) and federal and D/A scoring rules to prioritize vulnerabilities.
- Address the Risk: Inform actions to accept or remediate vulnerabilities according to D/A business rules and priorities.

# Dashboard Functionality

- Provide timely information. The information needs to be timely enough to allow rapid response, but not faster than operational personnel can actually respond to the information.
- Provide targeted information. The information needs to be actionable and at the right level of detail and technical simplicity for the audience to support the specific decision(s) to be made.
- Provide prioritized information. Individual security defects must be assessed on a ratio scale such that it is meaningful to add and average risk scores to obtain meaningful risk scores for individual defects on single devices and for composite defect risk scores.

# What is a Risk Score?

- A risk score for an individual defect is a numerical representation of the relative severity or importance of the finding to the risk for the system as a whole.
- Risk scores provide a single common severity scale for defects of different types, not inherently comparable.
- Risk scores can be aggregated for:
  - All defects on a single device.
  - Defects of a particular category (SWAM, VUL, CM, etc.).
  - Defects associated with any logical grouping of defects or assets.
- Risk scores can be averaged to normalize results across large and small groupings of assets.

# Notional Dashboard Hierarchy

