Training Methodologies for Continuous Diagnostics and Mitigation (CDM)

Eric Goldstein
Federal Network Resilience
Department of Homeland Security
March 19 2014

Homeland Security

Topics

- Why CDM?
- What is CDM?
- Purpose of CDM training
- CDM training approaches
- CDM training outcomes
- The need for collaboration
- Q&A

Homeland Security

Why CDM?

- A significant number of the most frequent cybersecurity compromises are enabled by easily fixed vulnerabilities and weaknesses.
- These can often be prevented by searching for, finding, fixing, and reporting on vulnerabilities and weaknesses in near-real-time
- CDM introduces a standardized, scalable, measurably effective approach to Information Security Continuous Monitoring

Homeland Security

What is CDM?

- CDM provides sensors, integration services, and dashboards
- Automatically identifies and prioritizes cybersecurity problems based upon greatest risk.
- Resources can in turn be allocated toward fixing the most important problems first and reducing the attack fabric for cybersecurity compromises

Homeland Security

What is CDM?

- CDM consists of three phases:
  - Phase 1 (managing devices):
    - Hardware Asset Management, Software Asset Management, Vulnerability Management, and Configuration Settings Management.
  - Phase 2 (managing users and networks):
    - Access Control Management, Security-Related Behavior Management, Credentials and Authentication Management, Privileges, and Boundary Protection (network, physical, and virtual).
  - Phase 3 (managing events):
    - Planning for Events and Responding to Events

Homeland Security

What is CDM?

- DHS is authorized to implement the CDM program under FY13 and 14 Congressional appropriations
- OMB M-14-03 further establishes CDM as a:

  "consistent, government-wide set of information security continuous monitoring (ISCM) tools to enhance the Federal government's ability to identify and respond, in real-time or near real-time, to the risk of emerging cyber threats."

Homeland Security

Purpose of CDM training

- Enable cybersecurity personnel to effectively manage, design, implement and evaluate CDM in a standardized fashion across the federal government and among state, local, tribal, and territorial governments.

Homeland Security

Purpose of CDM training

- CDM training will encourage common approaches to implementation across diverse organizations.
- In this context, CDM training will promote knowledge and skills required for the integration, operation, and management of CDM process and tools to help measurably reduce cybersecurity risk.

Homeland Security

CDM training approaches

- DHS is implementing training across a variety of platforms to reach a broad scope of audiences:
  - Instructor-led training
  - Self-study materials
  - Online videos, presentations, and webinars
  - eLearning courses

- The intent of multi-platform delivery is to maximize participation, promote flexible learning, and facilitate the accomplishment of specific learning objectives.

Homeland Security

Initial CDM Training Content

- Program Overview
- Phase 1 Capabilities
  - Hardware Asset Management
  - Software Asset Management
  - Vulnerability Management
  - Configuration Settings Management
- Implementation Considerations
- Dashboard
- Risk Scoring
- Maturity Metrics
- Human Factors
- Ongoing Assessment

Homeland Security

CDM training approaches

- CDM training is designed to align with and map to :
  - NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*
  - NIST SP 800-37, *Guide for Applying the Risk Management Framework*
  - NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*
  - NIST SP 800-16, *Information Technology Security Training Requirements*
  - DHS CyberSkills Management Support Initiative (CMSI)
  - National Initiative for Cybersecurity Education (NICE)

Homeland Security

CDM training outcomes

- CDM training is designed to accomplish several outcomes:
  - Students use CDM concepts and operations after concluding training, based on post-assessments and evaluations, to best adapt CDM to their agency's needs.
  - Students are more effective in implementing and operating their department/agency CDM solution after concluding training
  - Students find CDM training and course materials to be easily accessible and with high practical application before, during, and after training
  - CDM training is integrated into department/agency cybersecurity curricula

Homeland Security

The need for collaboration

- CDM training will be most effectively accomplished through the ongoing input of students, practitioners, and other partners
- DHS is exploring the development of innovative training approaches, such as Adaptive Learning and Role-Based Training
- DHS will work with FISSEA membership to gather input on the effectiveness of CDM training and support integration of CDM concepts into department/agency curriculum

Homeland Security

Q&A

Presenter information:

Eric Goldstein

eric.goldstein@hq.dhs.gov

202.510.4956

Homeland Security

Homeland
Security

Homeland
Security