CDM Generic Instance

Overview and Live Demonstration
Agenda

- General CDM Overview
- Further CDM Capability Areas and Strategic Goals
- Generic Instance – Goals
- Strategic Value
- CDM Generic Instance Build
- Lab Architecture- Phase 1 Tools and Data Flow
- Phase 1 Tools – Notable Points
- Demo
General CDM Overview

- Continuous Diagnostics and Mitigation (CDM) is a major DHS program.
  - Purpose: Provide a structured implementation of Information Security Continuous Monitoring (ISCM) per NIST 800-137.

- The CDM program has these components.
  - Multiple phases of implementation
    - Phase 1 – What is on the Network
    - Phase 2 – Who is on the Network
    - Phase 3 – What is happening on the Network
    - BOUND – How are my network boundary controls and data protection capabilities (encryption and data loss prevention)
    - Phase 4 – Ongoing Authorization Automation

- CDM implementation is managed by the DHS CDM Program Management office (PMO).
Further CDM Capability Areas and Strategic Goals

- **Bound-E and Bound-F**
  - Monitor and Manage Encryption Mechanisms Controls and Manage Network Filters and Boundary Controls

- **Phase 3 – Manage Events and Ongoing Assessments**
  - Detection of security violation events and classification of event impact
  - Ongoing Assessment is the automation of monitoring NIST Special Publication (SP) 800-53 controls that are related to CDM Phase 1, Phase 2, BOUND, and Phase 3 network and infrastructure components.

- **Phase 4 – Operate, Monitor and Improve (OMI)**
  - Ongoing Authorization uses the results of the MNGEVT ongoing assessment of NIST SP 800-53 controls for all previous phases of CDM as a set of inputs for ongoing authorization processes.

- **Changing the Paradigm**
Generic Instance – Goals

1. Build a CDM Generic Instance consistent with evolving CDM requirements
2. Apply CDM BPA Attachment N (Phase 1), N2 (Phase 2), and N..i (Phase n) technical requirements
3. Integrate and correlate data in Archer Dashboards
4. Provide stakeholders virtual and physical access to the CDM generic instance
5. COTS Vendor Outreach and Engagement
Strategic Value

- Provide Sponsor early access to configured dashboard releases
- Independent instantiation of Phase $n$
  - Phase 1 was conceived without interaction or input from CMaaS Integrators or external entities
  - Experience Phase $n$ capabilities in a controlled environment
- Ready access to fully licensed, enterprise COTS, software Sandboxed environment
  - Permits for access to software ahead of CMaaS installation and integration
- Generic Instance may be a conduit for training and/or other stakeholder engagement as determined by Sponsors (FNR, NIST)
CDM Generic Instance Build
Lab Architecture- Phase 1 Tools and Data Flow

Target Workstations and Servers

- Linux Servers
- Windows Servers
- Windows Workstations

Sensors

- ForeScout CounterACT (HWAM)
- IBM BigFix (CSM)
- IBM BigFix (SWAM)
- Tenable Nessus (VULN)

Collection and Integration

Agency Dashboard

- Archer
- SPLUNK
Phase 1 Tools – Notable Points

- **Archer**
  - Offices and Containers
    - Network objects are associated with Organizational Units; everything is in AD
  - Data Feeds
    - Archer to Splunk integration via Splunk API

- **CounterACT (HWAM)**
  - Near real time discovery
  - Policies define compliance (definitions of what is compliant) and object role definitions
  - Monitors network via Port Mirroring

- **Splunk**
  - Saved Searches return data via API calls
  - Only ingesting minimal data needed for Archer

- **BigFix (SWAM, CSM)**
  - STIGs are used to enforce FISMA controls on all endpoints and workstations
  - Used to deploy patches to correct vulnerabilities
  - Captures software inventory

- **Tenable Nessus (VULN)**
  - Scheduled vulnerability scans
  - Automatic updates from NVD
Demo
Thank You!

Questions/Comments