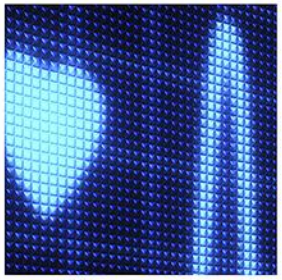
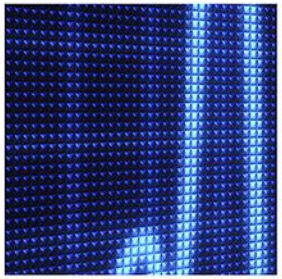
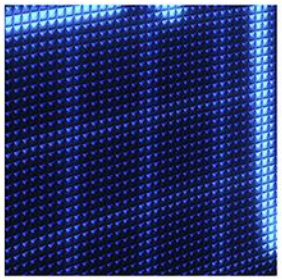






Medical Device Security in the VA: Through the Eyes of a Clinical Engineer




Presented by: Jason Newman, VISN 16 Healthcare Technology Manager

June 6, 2015

Veterans Health Administration
Healthcare Technology Management

Agenda

- Background
- Medical Device Protection Program Overview
- MDPP Security Controls
- Pre-Procurement
- Medical Device Isolation Architecture (MDIA)
- Malware Remediation
- VA HTM Toolbox

Background: What has the VA Done to Address Medical Device Security?

- VA has been involved with medical device security activities for over a decade.
- Has grown and changed over time to meet the challenge of evolving threats.

Milestones:

- 2004: MDIA Guidance
- 2010: MDIA Implemented
- 2012: Windows 7 Guidance
- 2014: ACL, VLAN, MDIA Certification
- 2015: Updated 6550

Medical Device Protection Program

Overview

- The Medical Device Protection Program (MDPP) is a comprehensive security initiative that coordinates VA efforts across multiple organizations to maintain the safe and effective operation of VA's networked medical devices.

- MDPP efforts will always support the preservation and sustainment of these three foundational principles:
  - Safety
  - Effectiveness
  - Data/System Security

Medical Device Protection Program

Stakeholders

- MDPP was created in 2009 to help VA safeguard all network connected medical devices that provide direct patient care.

- VHA Program Offices:
  - VHA Healthcare Technology Management (HTM)
  - VA OIT Field Security Service (FSS) Health Information Security Division (HISD)
  - VA OIT Service Delivery and Engineering (SDE)

MDPP Security Controls

- Pre- Procurement Assessment
- Administrative Access
  - Two-Factor Authentication
  - None-Email Accounts
- Mobile Media Scanning
- Medical Device Isolation Architecture (MDIA)
  - MDVLANs
  - Access Control List (ACL) or Firewall
  - Organizational Units
  - 802.11 wireless
- OS and AV update Server
- Incident Response to Malware Infections
- Media Sanitization

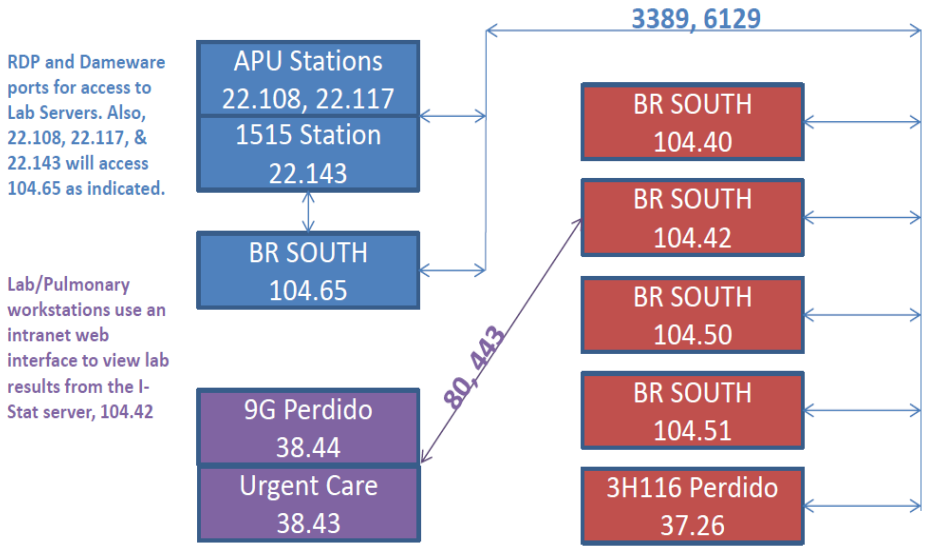
Medical System Security Controls	
Elevated Privileges	Elevated privileges for BME relate to administrative access to medical systems.
→ **BME Administrative Access to Medical Devices**	Process for BME staff to be granted administrative access to Windows O/S.
Incident Response	Expedites the cyber security incident reporting and response to compromised medical devices in order to prevent alteration of the device's function or availability.
Pre Procurement Assessment	VA Directive 6550 Pre-Procurement Assessment to evaluate the security and technical requirements for medical devices that will be connected to VA information networks.
Mobile Media	Requirement to scan all mobile media prior to attaching to a medical device and for updating local policy on visitors to incorporate the scanning requirement.
Medical Device Isolation Architecture (MDIA)	The VA network architecture solution to segregate medical devices from the VA enterprise network and provide limited, controlled access to external resources (Internet).
→ **MDIA Rule Set 2014**	A standard process for the isolating and securing networked medical devices using a protected Virtual Local Area Network (VLAN) approach.
→ **Change Management**	A standardized change management process for the addition/removal of medical devices to/from a MDIA VLAN or for the modification to the Access Control List (ACL).
→ **ACL Monitoring**	OIT Enterprise Risk Management Office (ERM) assessment of the implementation and management of the Medical Device Isolation Architecture (MDIA) as part of the sustainment of CRISP.

Pre-Procurement

- Fastest way to prevent future issues is by accessing new acquisitions
  - Pre-Procurement Assessment for Medical Devices (6550)
    - Establish technical requirements
    - Signed/Reviewed by OI&T, ISO, and HTM
  - Roadmap to Implementation
    - Patching
    - Antivirus
    - CPU configuration

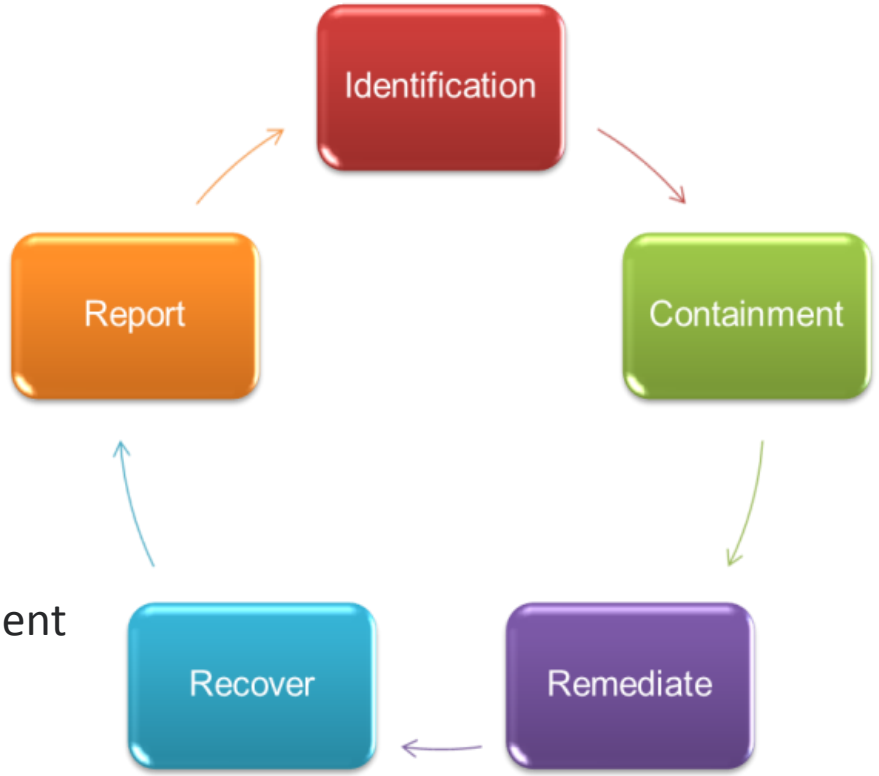
Medical Device Isolation Architecture (MDIA)

- All Medical Devices are placed behind MDIA
  - MDVLANs
    - Grouped by function (modality) and/or manufacturer
      - I.E: GE VLAN
  - ACL
    - Limit necessary traffic at the IP and Port level
    - National Rule Set
  - Firewalls
    - ASA Firewalls
  - Organizational Units
    - Medical devices using AD placed in specialized bins to prevent OI&T updates and GPOs
  - 802.11 wireless
    - FIPS 140-2 compliant



Malware Remediation

1. Identification
   - Characteristics of infection
2. Containment
   - Remove from network
   - Isolate
3. Remediate
   - Removal
   - Restoration
4. Recover
   - Brought back online
   - Insure will not lead to another incident
5. Report
   - 5 Ws
   - After Action Reports



VA HTM Toolbox

- Piloting National Inventory DB (HTM built)
  - Current inventory system not built for tracking networked medical devices
  - Allow for automated rollup by facility, VISN, and national
- Solar Winds: ACL (HTM Built)
  - Provides full copies of all ACLs by site.
    - Used for troubleshooting and development
- OS and AV Update Server (HTM Built)
  - WSUS national server
- NEWT Reports (OI&T)
  - Breakout by system showing vulnerabilities
  - OS reports
- Security Trainings
  - Onsite trainings

Questions?

Jason Newman

Email: jason.newman2@va.gov

713-301-2559