NINTH ANNUAL LEADERSHIP EVENT

CYBER SECURITY SUMMIT

Security solutions through collaboration.™

October 28–30, 2019 | Minneapolis Convention Center

cybersecuritysummit.org | #cybersummitmn

Securing Medical Devices

- Background & Landscape
- Understanding your Attack Surface
- Protect & Respond

Background & Landscape

- Increased focus on the impact of medical devices in technology environment
- Root cause of the problem, the devices, are still playing catch up both in secure design and configuration
- Active research in encapsulating the problem through microkernel security to “weaponized” hypervisors is not widely accepted or adopted
- Mitre has published rubic for applying CVSS to medical devices

Understanding Your Attack Surface

- Maintain accurate asset inventory and software details
- Know your MD weaknesses
- Define and understand a perimeter where points of attack that can lead exploitation of weaknesses in medical devices
- Strengthen perimeter, and validate strength

Understanding Your Attack Surface

- Reduce attack surface by:
  - Limiting protocols and ports
  - Appropriate access controls without hindering users
  - Whitelist outbound connections
  - Understand which devices can be zoned from other devices

Protect and Respond

- Segmentation / Firewall
  - Communication pathways of devices
  - Reduce risk to these devices and interrupt the attack vectors
  - Critical Med Devices on own VLAN
- Antivirus/Malware Protection
  - Defense in Depth & Basic security hygiene that gets overlooked
  - Exclusions, check reports, dats/sigs

Protect and Respond

- Get Patched – Stay Patched
  - Med Device may not be supported any longer
  - If not able to maintain other security controls- Do this first
  - Patch recommendations from scan
- Disaster Recovery / Backups
  - Devices, Medical Data, Patient Data, MRI images, etc.
  - Test, Test and Test the restore process

Checklist

- Define and defend your attack surface perimeter and determine MD vulnerabilities
- Perform Vulnerability/Penetration tests
- AV Signatures - stay up to date and check report daily
- Firewall Rules ensure no any/any rules exist
- Stay up on Patches from Medical Device companies
- DR Plan ensure you have one and it has been tested
- Perform Phishing education to staff