HOW TO BUILD A SUCCESSFUL VULNERABILITY MANAGEMENT PROGRAM FOR MEDICAL DEVICES

Sarah Kennedy
Robert Sloan
WHO WE ARE

- Sarah
  - B.S. in Telecommunications Systems Management
  - M.S. in Information Security
  - CISSP
  - Leader of selection and implementation of new vulnerability assessment tool

- Robert
  - At HCA for 15 years
  - Diverse background in technology and information security
  - Key team member in implementation and use of Qualys
• Our Implementation
• Authorization
• Process for Safe Assessment
• Reporting and Accountability
CURRENT IMPLEMENTATION

- 200 Scanning Appliances
- Appliance assignment based on physical location of divisions
- Rescan environment within 24 hours – Occurs twice a week
- Discover new assets (scan every IP in subscription) weekly
- Data from scans sync to Splunk and to an internally created tool for review
- On the 12\textsuperscript{th} of each month, we snapshot the data and each division gets a high level report of the expectations vs actual results
GOALS FOR NEW VULNERABILITY ASSESSMENT PROCESS

- Capable of more frequent scan time
- Faster publishing of new vulnerabilities
  - ASAP for headline vulnerabilities
- Continued scanning of troublesome devices
- Improved customer service
SUPPORT TO DO WHAT WE DO

• Authorized and responsible for scanning everything on our network
  • Including medical and non-traditional devices
• High level of support from upper management
• Bonus: Strong relationships with Vendor Management Team
YOU CAN’T SCAN THIS DEVICE!

- Impacts to devices present as:
  - Service locks up
  - Reboot necessary
  - System locks up entirely
  - Major delays in processing jobs
  - Resources are heavily impacted
- Usually occurs in devices that are misconfigured, outdated, or just not built by the vendor properly
• Having an impact and an excuse ≠ exclusion from scanning
• If a system was impacted from a vulnerability scan, it’s vulnerable to a Denial of Service Attack
Among the more specific actions when it comes to pushing for greater medical device cybersecurity, the FDA says it is thinking about requiring firms to:

- Make their devices capable of being updated and patched
- Provide both to the FDA and medical device customers and users with a “Software Bill of Materials,” which will include details about the software running on the device so that users can “better manage their networked assets and be aware of which devices in their inventory or use may be subject to vulnerabilities.”
STEP 1: DID WE CAUSE THE IMPACT?

• Investigation process for systems that don’t like being assessed
  • Use dates, times, logs, etc. for impact and cause
  • Schedule controlled scan and monitor for impact
  • Use Qualys data for what possibly went unresponsive
QID FOR UNRESPONSIVE SERVICES

- **38229** - Service Stopped Responding
  - Example: On port 23/TCP 3 consecutive connection attempts failed after a total number of 3 successful connections.

- **86476** - Web Server Stopped Responding / **86718** - Exhaustive Web Testing Skipped
  - Example: The web server stopped responding to 4 consecutive HTTP requests 2 minutes ago.

- **42432** – Possible Scan Interference
  - Example: Service name: Unknown - Possible Scan Interference on TCP port 443.
PAUSE: WHAT IF THEY STILL SAY “NO”
STEP 2: ARE THERE ANY MORE OF THESE DEVICES OUT THERE?

• Get inventory of the systems
  OR
• Fingerprint the host based on:
  • Open Ports
  • DNS name string
  • OS
  • SSL Header
  • …
• Unauthenticated:
  • QID 12230 – Default Web Page
  • QID 86002 – SSL Certificate – Information

• Authenticated:
  • QID 90065 – Windows Services List
  • QID 105231 – Administrator Group Members Enumerated
STEP 3: NO MORE IMPACT DURING A SCAN

Target
Hosts with all of these tags were included in the scan.
- Unknown
Hosts with any of these tags were excluded in the scan.
- Long Scan Time  - Special Case Exclusi...

Special Case: No Port 21

Special Case: No Port ...

Special Case: APC Net...

Special Case: i.LON

Special Case: No Port 22

Special Case: No Port 23

Special Case: No Port ...

Special Case: Digi OS

Special Case: No Port ...

Special Case: DryStar ...
OPTION PROFILES AND TAG OVERLOAD

- Asset Group; includes any known static IPs:
  - Special Case: No Port ______
- Logic Fingerprint Tag; to cover any additional:
  - Special Case: ___OS/Device Type___
TEMPORARY EXCLUSION OVERLOAD
AFTER ROOT CAUSE ANALYSIS

- Only assess systems in a safe manner
- Balance of security vs usability
- Builds relationships with system administrators
- Document every step in detail for accountability
REPORTING AND ACCOUNTABILITY

- Can’t handle standard port traffic = vulnerable to DOS
- Language for purchase contract focuses on maintaining secure system
- Depersonalize the result data
- Focus on: We all have the same goal
From Sys Admin
Anger and Frustration
Understanding and Explanation of Process
Additional Helpful Information
Willingness to Test Quickly
Satisfaction With Solution and No More Impact

Response from Us
Scheduling Test Time
Valid Test and Solution
SUMMARY OF PROCESS

1. Get complaint that system went down OR we proactively investigate systems that are likely having issues

2. Add the systems into a temporary exclusion from scanning using groups while we continue to investigate

3. Use the QIDs for service interruption as a starting point for ports to exclude from being scanned on the systems (and other factors like logs and time/date correlation between impact and us scanning)

4. Test under controlled conditions when system is stable to verify impact from default settings

5. If impact is confirmed as causation, test for impact in the modified scan (ports removed)

6. If no impact with the scan modifications, we move the tagged systems to only be scanned with these modifications – Therefore we met the goal of continuing to assess a device that has issues

7. When possible or needed, we then turn this information over to a vendor and encourage remediation of the system having an impact from being assessed
QUESTIONS?