FIRST HEALTH ADVISORY

ADVANCING SECURE AND EFFICIENT HEALTHCARE

Implementing a Medical Device Security Program:

Aligning with System Strengths

About the speakers

Matt Dimino

Chief Security Officer of Clinical and OT Security for First Health Advisory

Matt is the Chief Security Officer of Clinical and OT Security for First Health Advisory, a professional services firm specializing in medical device and IT cybersecurity. Matt’s unique HTM/Biomed, security, and leadership experience bring unparalleled depth to First Health. Matt has over 17 years of experience in various HTM roles from senior technical to leadership roles and 6 of those years as a practitioner in medical device security. Throughout his career, he has developed multiple security programs, integrated complex architectures, performed security consulting, and developed risk assessment methodologies.

About the speakers

Jim Caporali

Corporate Director, Biomedical Equipment Services

Jim has 35-year background in Clinical Engineering/Healthcare Technology Management. Throughout his career he has always dealt with security concerns regarding medical devices. The initiation of the medical device security program at a Pennsylvania hospital System was the first opportunity for detailed involvement in the implementation of a program jointly designed around requirements of Cybersecurity, Information Services and Clinical Engineering. Jim's role included project scoping, securing funding, gaining executive support, and acting as the project manager for implementation.

Overview

- **Pennsylvania Hospital System:**
  - **Health system consists of six medical centers, various institutes and centers of excellence, and multiple practices sites serving patients and communities across 29 counties of Pennsylvania.**
  - **Faced with the challenge of remediating cybersecurity audit findings and reconciliation of 30K+ unknown IP addresses.**
  - **Medical device security practices were heavily scrutinized, and the audit findings shed light on a security gap in the organization.**
  - **The Clinical Engineering department was accountable for the remediation of the audit findings. They had limited internal resources and no visibility into what devices were connected to the network and the security posture of these devices.**
  - **Risk Management practices were ad-hoc, undocumented, and Clinical Engineering had no internal policies or procedures to address cyber risk.**
  - **Vulnerabilities were reactively addressed, internal communication**

The Challenges

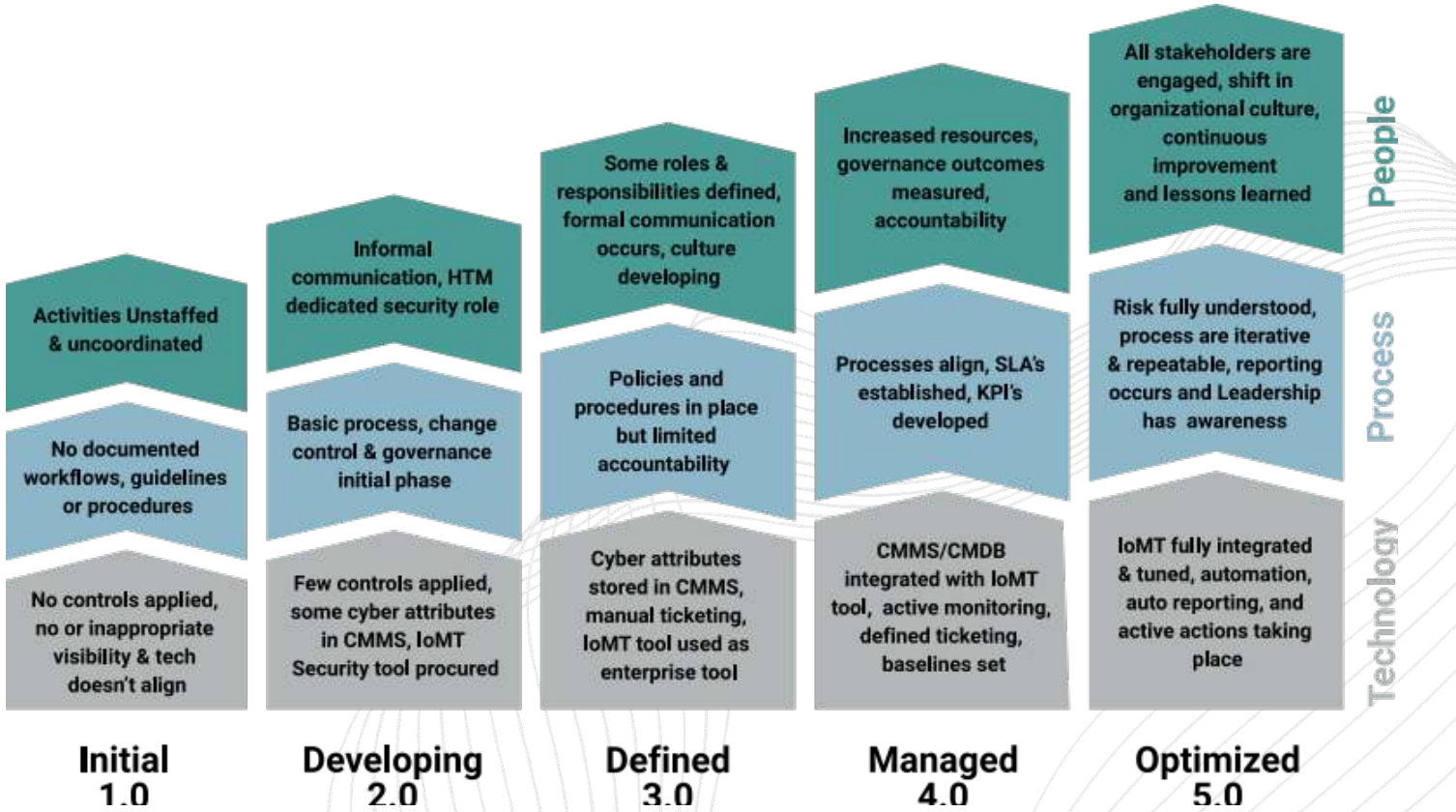
1) No network discovery tools to identify and profile IoMT/OT
   - What tools are needed?
   - How long will it take to deploy and optimize?
2) Insufficient governance and oversight to address IoMT cyber risk
   - Who should be involved?
   - What will their role be?
3) Addressing IoMT vulnerabilities and how to prioritize remediation
   - Likelihood x Impact
   - Exploitability
4) Operationalizing IoMT cybersecurity
   - Who will manage the tool?
   - What does the day-to-day look like?

Vision, Mission & Strategy

- What are we trying to achieve?
- What resources do you have available?
- What are the short-term and long-term milestones?
- How will we align resources?
- Budget & forecasted needs?
- Where do the people, process, and technology fit?

Tactics & Strategies

- Break everything down into measurable pieces (phases) with clear milestones
- Prioritize phases and track the LoE
- Understand and define maturity
- It’s OK to after a quick win but do not chase all easy targets, we will quickly become inefficient
- A complete solution includes people, processes, and technology
- Documented processes are a



Solution to Challenge #1

1) No discovery tools to identify and profile IoMT/OT & reconcile unknown IP Address

- Align IoMT security platforms with health system strengths
  - Developed criteria specific to the organization's needs
  - Evaluated and mapped technology stack:
    - Nuvolo (CMMS)
    - Rapid 7 (VM)
    - Cisco ISE (NAC)
    - ServiceNow (ITSM)
    - Splunk (SIEM)
  - Appropriate staffing with clearly defined roles
- Develop a project plan for deployment and value realization
  - Intake – Define success criteria
  - Network architecture discovery
  - Hardware install
  - Integrations
  - Data validation & optimization
  - Training

Solution to Challenge #2

2) Insufficient governance, sponsorship, and oversight to address IoMT cyber risk

- First Health and internal stakeholders created formal governance via a Charter
  - Quarterly meetings with leadership
  - Reported Risk(s)
- A steering committee was formed –the most critical part of system alignment
  - Address tactical and operational objectives
  - Configured and identified reporting & SLAs
  - Align business units on processes and objectives

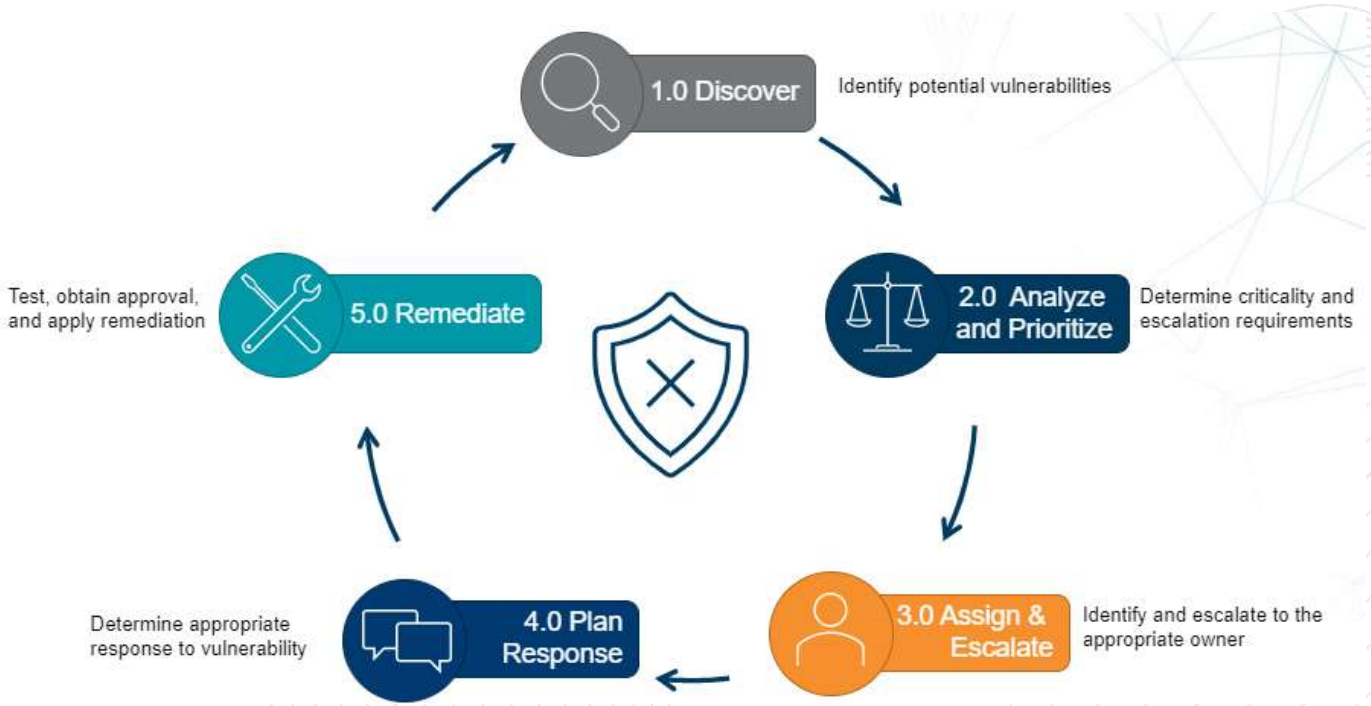
Solution to Challenge #3

FIRST HEALTH ADVISORY

3) Limited understanding of IoMT vulnerabilities, impact, and how to prioritize remediation

First Health helped create a vulnerability management program:

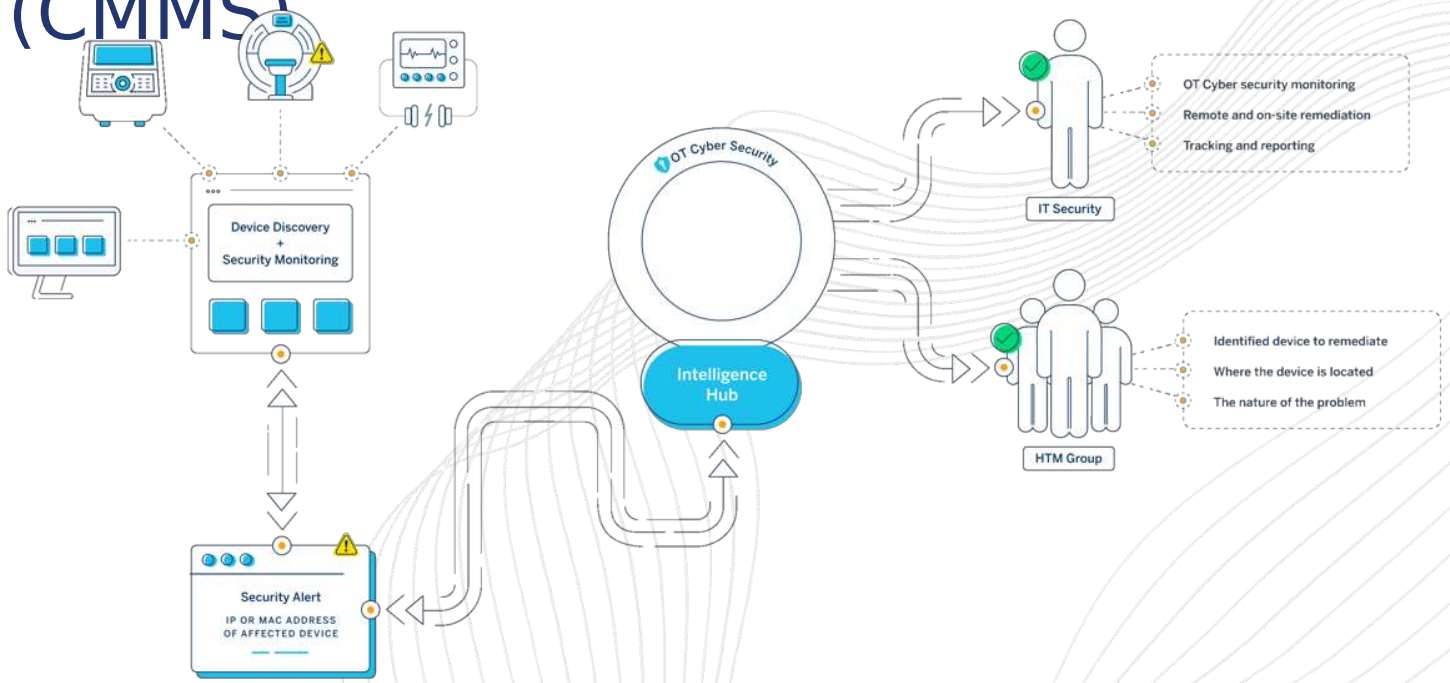
- Discovery
- Analysis and prioritizat
- Assign and escalate
- Plan response
- Remediate



Solution to Challenge #4

4) Operationalizing IoMT cybersecurity

- First Health helped develop policies, processes, and work instructions
- Integrated the IoMT tool and Computerized Maintenance Management System (CMMS)



Lessons Learned

- Evaluate workflows
  - If it’s not documented, it doesn’t exist
  - If it’s documented but not followed, what’s the point?
- Align priorities with IS/Cyber/GRC
  - Be firm on what is realistic and what is not – i.e. patching
  - Define and agree on the exception process
- Support business objectives
  - Optimize current investments in people, processes, and technology before procuring
- Visibility is not security
- Data is one of the most critical elements for decision making

Lessons Learned

- Educate and train throughout the project, not at the end
- Have a solid project plan with stakeholder signoff and accountability
- Develop a RACI as you build out your program
- Follow a framework
- Understanding the risk landscape
  - Define criticality and sensitivity of your assets
- Understand what controls and compensating controls are available
  - Scalability, cost savings, efficiency
- Only pay for you need and what aligns with your strategy

Questions?