# Leveraging Advanced IoMT Security Tools for Comprehensive Lifecycle Management

# Overview/Agenda

1. Introduction
2. Managing the Device Lifecycle: use cases & real-world examples
3. Key considerations for risk mitigation and our complimentary guide to IoMT security
4. Q&A

# Your Presenter Today

**Mike McDermott**
VP of Sales
Asimily

verathon

servicenow

connectiv
an accruent company

ePreop™

# The Full Lifecycle of Device Security Management

Keeping all devices secure requires end-to-end coverage

## INVENTORY AND VISIBILITY

- DEVICE DETAIL AND CATEGORIZATION
- DEVICE TRAFFIC/ NEIGHBOR MAPPING
- DEVICE USAGE TRACKING / IoMT IMAGING SCAN DETAILS
- RECALLS

## VULNERABILITY PRIORITIZATION

- VULNERABILITY DETECTION AND PRIORITIZATION
- ATTACK VECTOR ANALYSIS
- RISK SIMULATION

## RISK MITIGATION

- IoT PATCHING
- TARGETED ATTACK PREVENTION
- NETWORK SEGMENTATION AND MICROSEGMENTATION

## THREAT AND RESPONSE

- POLICY MANAGEMENT
- ANOMALY AND THREAT DETECTION
- PACKET CAPTURE

## GOVERNANCE, RISK, AND COMPLIANCE

- PRE-PURCHASE RISK ANALYSIS (PROSECURE)
- DEVICE HARDENING
- CONFIGURATION CONTROL

# Three Pillars to Lifecycle Management

## End Users

Clinical Efficacy

Easy to Use

## Financial

Capital & Operational Costs

Reimbursements

Expected lifespan

## Support and Maintenance

Easy to PM & CM

Is it supported by the manufacturer

Cybersecurity

All Stakeholders Need to have Best Data to Make the Best Decisions for the HDO

# Reduce IoMT Risks Using a Team Approach:
## Combining People, Process, and Technology

**Engaging all stakeholders with a team approach to reduce risks:**

- HTM/Biomed
- Cybersecurity
- Network Engineering & Infrastructure
- Cybersecurity GRC
- HTM/Biomed Supply Chain
- OEMs/MDMs

**PROACTIVE RISK MANAGEMENT** | **BLENDED EXPERTISE** | **ACTIONABLE RISK MITIGATION**

# How to Protect IoMT at an HDO?

Integrating governance, visibility, and vulnerability management for overall improved risk posture

| | ESTABLISH GOVERNANCE | ENHANCE IOMT VISIBILITY | MANAGE IOMT VULNERABILITIES |
|---|---|---|---|
| OBJECTIVE | **Standardize IoMT governance, aligned with industry leading security practices and frameworks** | **Implement outcome-based strategy to monitor IoMT providing continuous assessment of risks and threats** | **Develop a structured approach to identify, prioritize, and remediate vulnerabilities, aligning with broader organizational risk management efforts** |
| KEY ENABLERS | • IoMT Governance Model<br>• RACI Matrix for IoMT roles and responsibilities<br>• Process Flows integrated with other Hoag processes | • Reference Architecture for IoMT Discovery<br>• IoMT platform implementation for visibility<br>• Continuous monitoring of risks and threats | • Vulnerability Rationalization<br>• Prioritization of remediation efforts based on operational impact and implementation viability |
| COLLECTIVE OUTCOME | • Cyber Governance, Risk and Compliance | • Asset Management<br>• Security Monitoring<br>• Network Security | • Targeted remediation via device reconfiguration<br>• Patch management<br>• Network controls implementation |

# Hoag: Committed to Providing World-Class Healthcare in Orange County


Hoag is a hospital system that provides comprehensive care to over 32,000 inpatients and 568,000 outpatients across Orange County, California, every year. The organization is committed to ensuring that no one needs to leave Orange County to receive world-class, personalized, accessible health care.

**3**
Hospitals

**606**
Beds

**4,200+**
Connected Devices

**8k+**
Employees

Hoag's healthcare technology management (HTM) team consists of 25 full-time employees. The team is made up of Biomedical Equipment Technicians, Clinical Engineers, Imaging Service Engineers and support staff, led by Bob Meninno, Principal of Biomedical Engineering & Operations.

# Case Study: 3 Hospitals, 700+ Bed Health System, 4300+ Connected Medical Devices

>43K CVEs remediated and >820 anomalies mitigated in 8 months

## POC

**Findings:**

- ORS 79/100 (Industry Average: 30)
- Excellent Inv. & Classification
- 3 Edges Deployed for POC

**POC Conclusion:**
Incumbent solution wasn't reducing risk

MAY 2024

## Deployment

**Goals:**

- Create a Proactive Process for Risk Reduction
- Meet industry-standard ORS through strategic risk reduction
- Uplevel & train the entire HTM to manage device security program to meet compliance goals

**Methods:**

- 11 Edges Deployed
- Risk Reduction Services to meet aggressive timeline goals

AUG 2024

## Product Transformed Risk Reduction

- Gained immediate insights into exploitable vulnerabilities
- Clinically validated steps for remediation
- Instant insight into anomalous behaviors in real-time

*Implemented concurrently*
AUG 2024 – JAN 2025

## Services Upleveled process & strategy

**Operational**

- Implemented a process for patch validation
- Robust device secure configuration standard development and monitoring
- Pre-procurement risk assessments enabled quick purchase decisions

**Strategic**

- Created and trained IoMT cybersecurity governance committee
- Drove vendor discussions to obtain and review security white papers for product lines in HDO
- Advise on onsite remediation efforts to scale team
- Drove ACL Implementation with HDO network & cyber teams using SNOW

APR 2025

## Current State

- 50-point reduction in ORS
- Mitigated over 43,339 high-risk CVEs
- 820 devices with anomalies mitigated

## Right Sizing Mammography

HDO decided to not replace old equipment and reduced under utilized services for Mammography

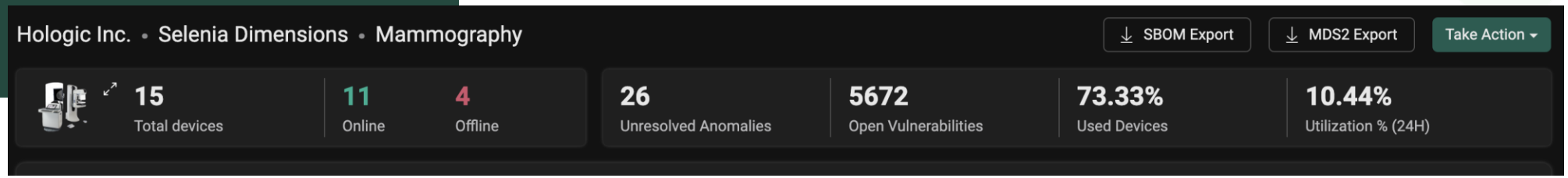
# Organizational Savings
## Right Sizing Mammography

**HDO was faced with a challenge:**

- Opex & Cap Ex shortage
- Staffing issues,
- Outdated equipment, and high risk

HDO was looking to reduce overall costs and the HTM leader & Clincal Staff were able to use data to help leadership justify a reduction in overall Mammography services.

**Saving $2m+** in capital costs
**Savings $3m** in operating costs



**CT Software Upgrade not Justified:**

A small hospital saved **$70,000**


# Software Upgrade Cost Savings Example

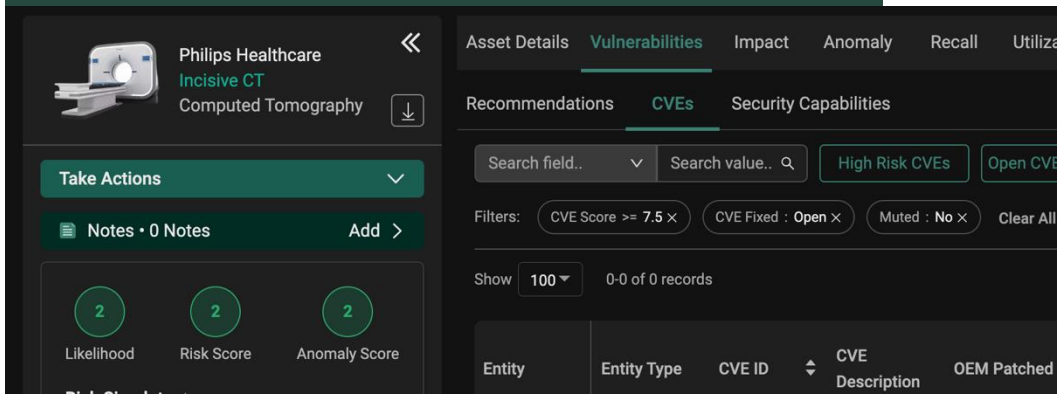
- Vendor charges for software upgrade to patch and improve security from XP to 7
- HDO uses risk modeling and identifies that upgrading software increases the security risk!

## Example: Phillips Brilliance CT (Big Bore)

| Operating Version | Max Risk | Hardened Device |
|---|---|---|
| Windows XP | 9 | 4 |
| Windows 7 | 9 | 5 |

**HDO cancels the purchase order for 2 replacement CT systems:**

HDO saved **$2M+** by foregoing replacement



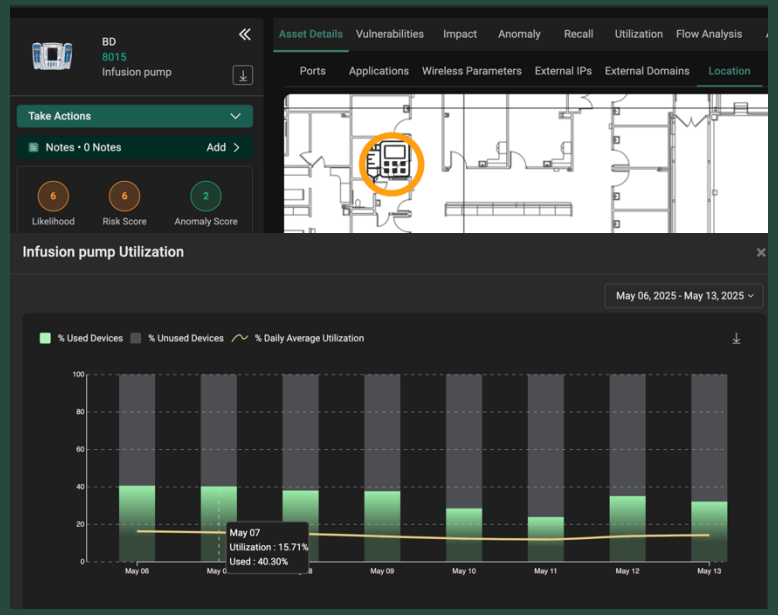

# Vulnerability Management & High-Risk Device Hardening

**HDO was planning to replace two CTs because they had outdated operating systems and were viewed as too 'risky.'**

- Opex & Cap ExThe CTs were still clinically acceptable by the providers.
- The biomedical department could still service and repair them as needed.

**Some devices were identified as high risk but leveraging advanced IoMT security tools, they were able to use the security recommendations to lower the risk to an acceptable level.**

HDO saves **$1M+** by improving utilization and effectively allocating existing devices




# Multi Hospital Health System:
## Fleet Management Improved Utilization and Efficient Distribution of Assets

**HDO was in the process of approving a $1M+ PO for additional infusion pumps.**

- When they reviewed the utilization data.
- They found that they only had a 30% utilization rate over a 3-month time period.
- When they reconciled the inventory using advance IoMT security tools, with the inventory in their CMMS (computerized maintenance management system), they found that 15% of their infusion pump inventory were sitting in closets unused.

**They canceled the PO, effectively distributed the pumps, and effectively reallocated the capital.**

# Key Questions to Consider for Risk Mitigation in IoMT

01 What type of a team will you build to solve this problem?

02 How do you remediate vulnerabilities and malicious behaviors?

03 How do you justify hiring clinical engineers for cyber work?

04 How many hours per week are you allocating to work on IoMT?

# Thank You!

Q&A