Mayo Clinic’s IoT Journey
From Asset Inventory to Cybersecurity
ACCE gratefully acknowledges the sponsorship of this webinar by ördr
About the Moderator

Eric C. Aring, MBA
Member, ACCE Education Committee

Eric has worked for Mayo Clinic for 2 years as the Asset Administrator for HTM systems support, previously working at Stanford Children’s Hospital as a Clinical Systems Engineer, and UCSF as an HTM technician.

During his time at Mayo Clinic, he has spent extensive time working on collaborative workflow with Information Technology, Clinical stakeholders, and implementation coordinators.
The focus of the presentation is on securing Healthcare IoT (HIoT) within Healthcare Organizations and should not be construed as an endorsement of any product.

Mayo Clinic has a financial interest in Ordr Inc.
Keith has worked at Mayo Clinic for 23 years in several different support and leadership roles. He is currently the Section Head of Healthcare Technology Management Cybersecurity and Business Operations. Keith has also had several other positions in HTM, starting as a Unit Manager of the X-Ray equipment service group and most recently as the Section Head for Enterprise Lab, Research, and Ophthalmology Service. Prior to his roles in HTM, he worked in Surgical Services as a Core and Prosthesis Supervisor, and as a Surgical Process/Systems Analyst.

During his time at Mayo, Keith has had extensive experience collaborating on several multidisciplinary teams. He has demonstrated a commitment to customer service, strong leadership skills, and experience with process analysis, project management, and technical support. During his tenure in Surgical Services and HTM, he has been exposed to the depth and breadth of medical equipment in a large healthcare organization. This includes the use of, service and support on, and the operationalization of cybersecurity for a wide range of medical equipment and IoT technology.
Greg Murphy
Chief Executive Officer at Ordr Inc.

Greg joined Ordr as CEO in December 2018. Previously, he was VP Business Operations for the HPE Aruba Group, the 4,000 person networking and IoT business unit of Hewlett Packard Enterprise. In that role, Greg was responsible for leading the business integration of Aruba and HP Networking following HP’s $3 billion acquisition of Aruba Networks in 2015. Greg held multiple prior senior executive positions within Aruba, including SVP Business Operations, GM of network management software, GM of outdoor and mesh products and VP of Marketing. Greg joined Aruba in 2008 through its acquisition of AirWave Wireless, a network management software provider that Greg founded and led. Greg received his M.A. from Stanford University and his B.A. from Amherst College.
About Ordr

- Ordr is the leader in healthcare IoT security:
  - Largest market share in healthcare with customers including the top hospitals in U.S. and UK
  - KLAS Healthcare IoT Security Leader 3 years in a row
  - Representative vendor in Gartner Medical Device Security

- Customers in North America, Europe and APJ

- “Whole Hospital Approach” to security:
  - See every device and network connection
  - Know every risk, vulnerability and anomaly
  - Secure via automated proactive, reactive, retrospective policies

Ordr Proven In Top Hospitals/HC Systems

- Mayo Clinic
- Cleveland Clinic
- Fairview
- Aspirus
- Unity Point Health
- Southampton NHS Trust
- Cedars Sinai
- Nat’l Institute of Health
- Sutter Health
- Hartford Healthcare

Ordr Recognized as Market Leader

- Three-Time Healthcare IoT Security Market Leader
- Representative Vendor
Explosion of Connected Medical Devices

- 10-15 connected devices per bed including medical devices
- 20% connected medical devices are running on outdated O/S
- 50 Billion medical devices will connect to clinicians, health systems, patients, and to one another over the next decade.
- Healthcare IoT CAGR growth of 25.9% (2021-2028)
Pain Points for Technology Support Teams

- CMMS not up to date. No real-time inventory of medical devices
- 30-60 mins per person/shift locating missing and misplaced devices
- Many vulnerability disclosures. How to scan? Where to focus?
- How are devices being used? Need to schedule maintenance and support procurement decisions
Journey from Asset Inventory To Cybersecurity

2019

- ~30,000 Medical, Research, and Facilities devices
- 3 Primary hospitals

- Licensed initially by HTM
- Subsequently expanded to all devices
- Automated inventory and classification

Today

- 500,000+ Connected devices
- Enterprise-wide: 100s of facilities

- Risk and vulnerability rating for devices
- 9,000+ vulnerable Windows 7 devices (~$600M replacement cost)

- Segmentation policies based on Ordr behavioral baselines
- Integrated with Cisco ISE for policy enforcement

Visibility and Asset inventory

Risk and Vulnerability

Segmentation
Explosion of Connected Medical Devices
Mayo Clinic – At a Glance

Mission:
• To inspire hope and contribute to health and well-being by providing the best care to every patient through integrated clinical practice, education and research

Primary value:
• The needs of the patient come first
Mayo Clinic Locations

- Rochester, Minnesota
- Scottsdale and Phoenix, Arizona
- Jacksonville, Florida
HTM at Mayo Clinic

~350 HTM Staff:
~275 Biomed technicians
~30 Managers
~45 Support staff

26 Shops providing
in over 66 communities, and spanning 5 states

Over 130,000 medical devices and systems inventoried, and valued at over $2B

~60k Network Connectable medical devices/systems
~16k Facilities IoT devices/systems
Historical Cybersecurity Challenges in the Healthcare Environment

- **Security Efforts**
  - Practices Haphazard and Inefficient
  - Processes Not Automated or Operationalized
  - Risk Response Reactive

- **Equipment Security and Vendor Support**
  - Lack of Receptiveness to Scans, Patching, etc.
  - Slow to Upgrade
  - Support Deficient Through Entire Lifecycle
  - Lack Clarity and Details of Installed Software

- **Legacy Devices**
  - Large Volumes
  - Cost Prohibitive to Replace
  - Unclear Guidelines for Retirement at End of Life
Unique Nature of IoMT

- Regulatory guidelines (FDA, CAP, TJC)
  - New Federal guidance with PATCH Act
  - Zero Trust guidelines
  - OIG Report
  - 405d
- Manual, resource intensive patching process
- Lack of “IT” like deployment options
- Outdated/Unsupported Devices
- Largely unable to scan with standard tools
- Unable to load agents
The HTM Cyber Team Process Challenges

- High Knowledge but Limited Resources
- Complex Mitigating Control Requirements
- Inadequate & Insufficient Tools to Identify Assets
The HTM Cyber Team Organizational Fit

Information Technology

Health Technology Management (HTM)

HTM
Information Security

OIS
Risk & Service Mgt. and Assurance Services

Office of Information Security (OIS)
HTM Role in Cybersecurity

- Operationalize Security on Medical Equipment and Systems
  - Structured
  - Standardized approach
  - Economies of Scale

- Also....Facilities Operations and HIoT

- Accountability through the entire technology lifecycle
  - Visibility
  - Monitoring
  - Action
  - Disposition

- Guiding Principle:
  - Ensure that equipment is functional and optimized in order to meet organizational –patient safety, business continuity, regulatory, and cybersecurity requirements.
Key Operational Tools To Execute and Automate Security Operations

Robust CMMS Solution (Lifecycle Maintenance)

- Enterprise Asset Management Solution
- Flexible and robust work order and workflow engines
- Supports risk scoring and modeling
- Supports vulnerability management
- Provides device profile-based approach for mitigation efforts
- Integrates with CMDB and other Enterprise Security tools
- Provides dashboarding and metrics for asset and security management

Modern Asset Discovery and Security

- Improves quality of data for Asset inventory
- Capability to detect networked medical devices (including legacy)
- Robust medical device asset classification
- Provides insight into connected device actions
- Supports device security operations
- Integrates with other Enterprise Security tools
- Micro-Segmentation
- Behavior detection and monitoring
Execution

HTM Cybersecurity Program

- Policy & Process
- Vulnerability Management
- Tools Deployment
- Lifecycle Profile
- Training & Industry workgroups
- Patch Management
- Fleet Risk Assessment
- Vendor and Device Assessment
Visibility:
Asset Inventory, CONNECTIVITY AND FLOWS, and Device Utilization
Visibility at Mayo Clinic

- 130,000 connected devices
  - CMDB with specific attribute capture
  - ISE MAC address match

- Ordr identifying devices profiled as medical devices and facilities devices and matching with CMDB
  - Attributes – MAC address, IP address, hostname to clean and complete inventory
  - 570 medical device categories – examples: medical devices/systems, research instruments/systems
Visibility is More Than Device Attributes

**Device information**
- **MAC:** 00:18:65:65:8D:8E
- **Device description:** CT Scanner
- **Manufacturer:** Siemens Healthcare Diagnostics Manufacturing Lt
- **Model Name:** Somatom Force
- **Serial Number:** SI38913958
- **O/S Version:** BSP
- **DHCP**
- **Hostname:** somatomforce-537
- **PHI:** NO
- **Vulnerabilities:** Log4J

**Connectivity**
- **SCE Sensor:** San Jose Office
- **IP:** 10.38.138.202
- **SUBNET:** 10.38.136.0/22
- **VLAN:** VLAN0860
- **ACCESS TYPE:** Wireless
- **Location:** FOURTH FLOOR
- **Network Device:** 10.1.24.40 (Cisco-AP-117)
- **WLAN SSID:** CloudPost
- **WLAN AP:** 84:B8:02:62:16:B7
- **FIRST SEEN:** 9/25/20 7:21:49 PM
- **LAST SEEN:** 9/25/21 7:21:49 PM

**Network flows**
- Complete inventory with rich context
- Baseline activity per device and/or category (profile)
- Connectivity and behavior critical to Zero Trust and to identify anomalies
Device Utilization at Mayo

- Leveraged Covid to implement utilization features
- Benchmark tool for ventilators and infusion pumps
  - Volume/Location
  - Special integration with pump infrastructure
  - Capsule Neuron—asset labeling
  - Also used CMMS and RTLS
- Collaboration with Radiology Informatics
  - Developing DICOM reporting
Risks
and Vulnerabilities
Risks of Connected Devices in Healthcare

Healthcare organizations need a comprehensive view of medical device and HIoT risks

Medical Device Overall Risk

Incident Risk
- High Risk Protocols
- Communication Anomaly
- External Communication

Device Vulnerability
- Device Vulnerability
- OS Identification
- Endpoint Security State (MDS2)
- Software Bill of Material (SBOM)

PHI Exposure Risk
- PHI presence
- Manufacturer disclosure (MDS2)
- Behavior
- Device Portability
- Encryption at Rest/Transit

Clinical Risk
- Physical Risk
- Equipment Location
- Mission Criticality (Availability)
Vulnerability Management

- Organizations conduct extensive scanning of traditional IT equipment
- Cannot complete active scanning for most medical devices and OT technology
  - Traditional vulnerability discovery products are using passive tools to "scan"
  - Mayo partnering with Ordr
- Target is a single pane of glass view
  - All vulnerabilities
  - Every connected device in the environment
  - Aggregating vulnerability information and reporting
- Risk-based approach
  - How should organizations prioritize where to start risk mitigation?
Vulnerability Management

Medical devices and OT

Passive Medical Device Scanning tool delivering vulnerability details

Assets are matched against Nuvolo inventory

Traditional IT devices

- IoMT and OT: Nuvolo Vulnerability Dashboard built on top of ServiceNow
- Traditional IT: Dashboard in ServiceNow
Dashboard Examples

HTM Vulnerabilities 30 Day Running Average

HTM Vulnerabilities Past 6 Months by Priority

HTM Vulnerabilities Past 6 Months (Device Type)

All Open HTM Vulnerabilities (Number)

All Open HTM Vulnerabilities (Percentage)
Zero Trust Segmentation - Micro and Macro
Unsegmented Means Unregulated Behavior

- Everything is put into the same enclosure
  - Herbivores
  - Carnivores
  - Omnivores
  - Endangered species
  - Convalescing animals
Segmentation: Setting trust boundaries between all animals

Top Down Segmentation for Scale

Bottom Up Segmentation for Control
Micro Segmentation at Mayo

• Security
  • Microsoft ended general support for the Windows 7 operating system (OS) in 2020
  • January 2020 - Desktop
  • October 2020 - Embedded
  • Medical device inventory also includes other out of support OS’s

• Impact
  • Thousands of medical devices impacted

• Remediation
  • Micro-segment devices utilizing capabilities of Ordr tool
  • Successfully created segments and related policy
Visibility is More Than Device Attributes

Approach

• Approved to Microsegment Medical Devices with Windows 7 and Older OS’s
• The project team evaluated several methods to identify device segments
  • manufacturer, model, device category, sub-category, region, building, floor
• Preferred Identification method is device category and sub-category (from CMMS)
  • Based on utilization of existing category/subcategory classification in HTM management system
  • Estimated 15-20 categories (device groups)
• Leverage Ordr
  • Create custom profiles (Category/Sub)
  • Monitor flows and establish baselines
  • Generate ISE SGACL policy
Macro Segmentation – Limiting communications

Approach
- Scoped project to "close" specific business areas
- Closed = nearly zero inter-segment traffic between business area segments
- Systematic assessment to assure correct device membership
- Identified workflows that cross segment boundaries
- RemEDIATE cross segment traffic
  - Enterprise services to perform function (file transfer, e.g.)
  - Leverage ISE SGT’s to classify devices and apply policy (define permit and deny capabilities)
- Monitor changes

Segmentation Process

Communication throughout the Process

“ORDR Snapshot”

<table>
<thead>
<tr>
<th>TRAFFIC INTO Sample Segment</th>
<th>dataSetProfile</th>
<th>IN</th>
<th>Count of srcdp</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADM_NET_INT (13900)</td>
<td>16403</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>RES_WKS_MAN_TEMP</td>
<td>1947</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>ANY</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>ADM_WKS_MAN (12120)</td>
<td>ANY</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>ADM (10000)</td>
<td>445</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>17500</td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>PRC_WKS_MAN (17100)</td>
<td>445</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Unknown (0)</td>
<td>1001</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>19310 (19310)</td>
<td>445</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1947</td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td></td>
<td>13</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TRAFFIC OUT OF Sample Segment</th>
<th>dataSetProfile</th>
<th>OUT</th>
<th>Count of srcdp</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ADM_NET_INT (10150)</td>
<td>1026</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>80018</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>ADM_NET_INT (13900)</td>
<td>80</td>
<td>68</td>
<td></td>
</tr>
<tr>
<td>PRC_WKS_MAN (17100)</td>
<td>445</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Unknown (0)</td>
<td>3478</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>16386</td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>ANY</td>
<td></td>
<td>6</td>
<td></td>
</tr>
<tr>
<td><strong>Grand Total</strong></td>
<td></td>
<td>547</td>
<td></td>
</tr>
</tbody>
</table>
Traffic Analysis and Anomaly Detection at Mayo

Use Cases
• Specific Patients
• Specific vulnerability signatures
• Fleet

Proactive
• Ordr Profile/Baseline
• Integration with SOC/SIEM

Reactive
• Rules based
  • Specific flows, protocols, services
  • Custom profiles (locations, devices)
  • Custom alerting
  • Specific vulnerabilities
Anomalous Behavioral Detection and Response at Mayo

- VIP patient room = custom profile
- Behavioral baselining
- Alerting when deviation from baseline is
  - Email alert
- Future: automation of segmentation
  - Full integration on SIEM, security response based on log file analysis
  - Automated segmentation policies for devices that behave outside of baseline
Summary

- Medical devices and healthcare IoT (HIoT) pose unique security challenges
- No silver bullet – people, process, technology
- Specialized and focused teams facilitate the operationalization of organizational security efforts
- Need clear goals on what to accomplish
- Leverage tools/automation to:
  - Reduce resource overhead
  - Asset Visibility
  - Workflows
  - Dataflow visibility
  - Segmentation
  - Utilization
Questions?

Keith Whitby, Mayo Clinic
Whitby.keith@mayo.edu

Greg Murphy, Ordr
Gmurfy@ordr.net
Thank You

Please complete the online evaluation/attendance form at

https://www.surveymonkey.com/r/ACCE-Ordr_08-05-22

Or scan the QR code