2023-2024 Educational Webinar Series

Cybersecurity Passive Systems – Lessons learned from an HDO Perspective

October 12, 2023

Keith Whitby, MBA

Mayo Clinic

ACCE gratefully acknowledges the sponsorship of the 2023-2024 Educational Webinar series by

About the Moderator

Eric Aring, MBA

Asset Administrator
Mayo Clinic

Eric has worked for Mayo Clinic for 4years as the Asset Administrator for HTM Medical Systems Support Virtual Care, supporting Video Telemedicine, XR technologies, and Robotics enterprise wide at Mayo Clinic. During his time at Mayo Clinic he has spent extensive time working on collaborative workflow with Information Technology, Clinical stakeholders and implementation coordinators towards the goal of scaling Telemedicine to meet the demands of the practice.

Previously working at Stanford Children's Hospital as a Clinical Systems Engineer, and UCSF as an HTM technician.

Logistics

- All attendees have their microphones muted during the presentation.
- Questions to the panelists must be submitted via the "Q&A" feature in Zoom at any time. They will be addressed at the Q&A portion.
- If there is any urgent issue, please use the "chat" feature to communicate with the host/moderator.
- Please remember to complete the webinar evaluation after attending. A link will be provided at the end.

About the Speaker

Keith Whitby, MBA

MAYO CLINIC

Keith has worked at Mayo Clinic for 24 years in several different support and leadership roles. He is currently the Division Chair of Healthcare Technology Management. Keith has also had several other positions in HTM, starting as a Unit Manager pf the X-Ray equipment service group, Section Head for Enterprise Lab, Research, and Ophthalmology Service, and most recently as the Division Chair for HTM.

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 HIoT technology.

Session Description

Discover insights into Cybersecurity Passive Monitoring Systems from an HDO and ISO perspectives. Join this session to learn how to maximize the benefit of these cybersecurity solutions and get tips on how to leverage them in enhancing your medical device security risk management and vulnerability management programs. Gain information about best practices and hear what additional benefits these solutions may offer.

Disclosure

- The focus of the presentation is on managing vulnerabilities and 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.

What We Will Discuss Today

Vulnerability management requires a broad strategy

Vulnerabilities from active and passive scanning

- Passive scanning tool for IoMT, IoT, and OT
- Active scanning tool for traditional IT

Application details from manufacturer

- SBOMS

Real-time Application-level Vulnerability

- Real-time tool for visibility into installed application, versions and dates to correlate and get accurate vulnerability impact

Mayo HTM Medical Equipment and IOT Security Program

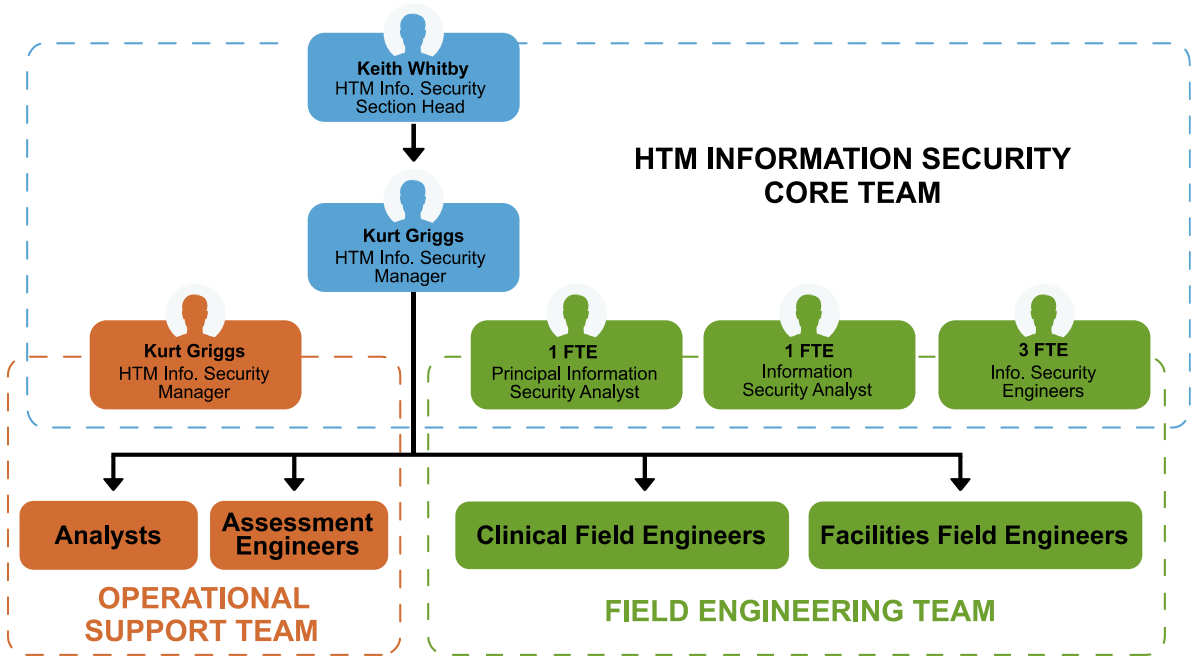
People

Process

Technology

ordr nuvolo

Mayo Clinic: People



- **Operationalize Vulnerability Management for Medical Equipment and Systems**
  - Structured
  - Standardized approach
  - Economies of Scale
- **Also….Facilities Operations and IoMT**
- **Accountability through the entire technology lifecycle**
  - Visibility
  - Monitoring
  - Action
  - Disposition
- **Guiding Principle:**
  - Ensure that equipment is functional and optimized to meet organizational needs:
    - Patient safety
    - Business continuity
    - Regulatory requirements
    - Cybersecurity requirements

Mayo Clinic: Process Vulnerability Management Operations

Type-1

- Critical or high-risk vulnerability that affects the Operating Systems used by medical device manufacturers.
- Also known as zero-day vulnerability
- Can result in the device being compromised with a ransomware attack, Remote Control Execution (RCE), unauthorized access to patient data, and other security and safety issues if exploited.
- Tends to affect multiple industries (including government)

Type-2

- A critical or high-risk vulnerability affecting specific product(s) from a medical device manufacturer.
- An example of such vulnerability may include, lack of encryption, use of default passwords, etc.
- If exploited, has the potential to compromise the device, grant unauthorized access, and cause other security and patient safety issues.

Type-3

- A critical/high/moderate vulnerability found in the component(s) or third-party software on a medical device.
- Examples includes TCP/IP libraries, Adobe Acrobat, etc.
- Exposure if exploited-can alter the device operations, allow remote control execution (RCE), grant unauthorized access, allow data exfiltration, misdiagnosis resulting in a patient safety issue, etc.

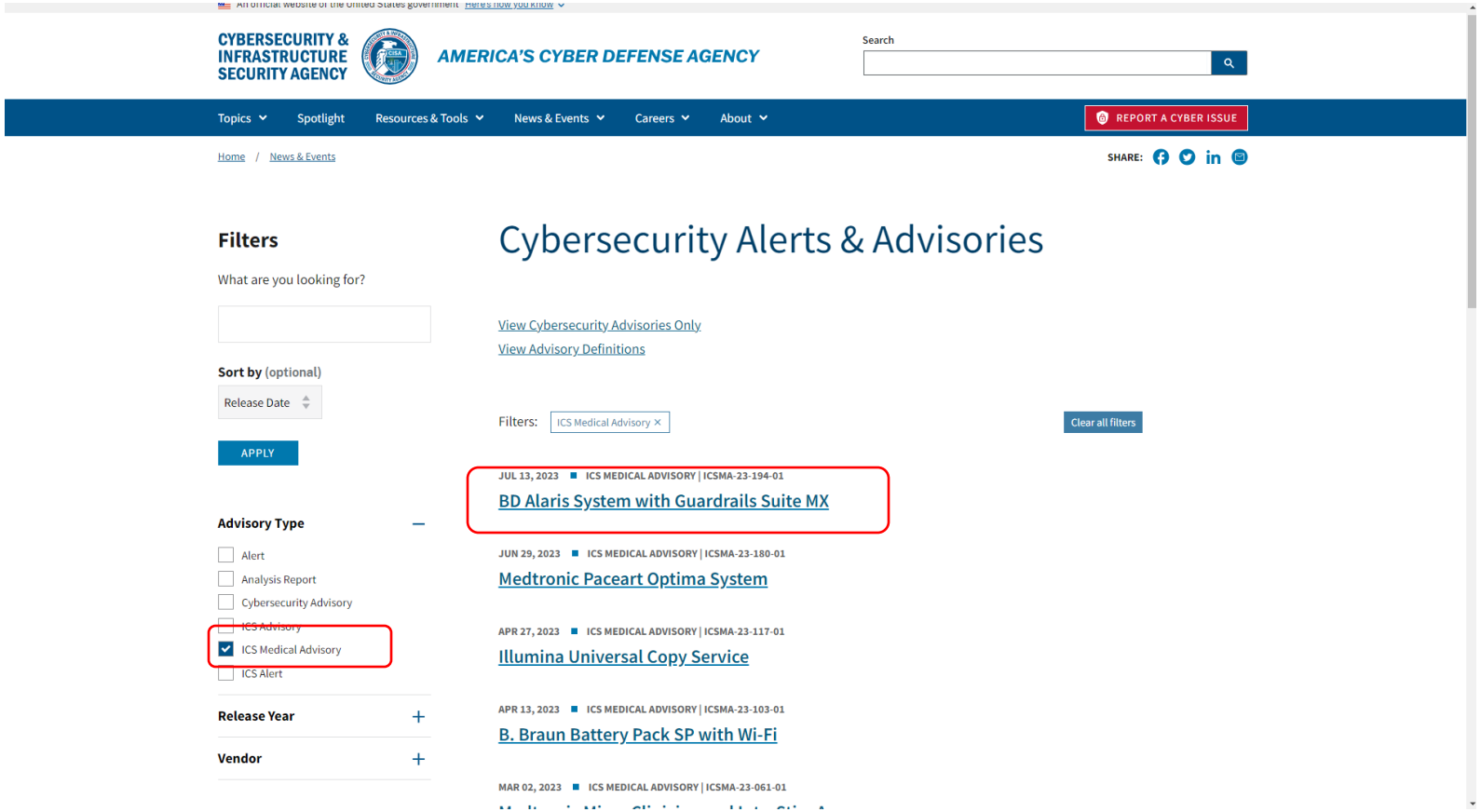
HTM Vulnerability Management Program				
Daily and Weekly Threat Monitoring - Industry Monitoring (Triage)				
ServiceNow Ticket and OIS Alerts Notification				
Type-1 Vulnerability Remediation activities for Operating Systems. (E.g. WannaCry, BlueKeep, DejaBlue, Urgent11, etc.)	**Type-2** Vulnerability Remediation Efforts for Vendor Specific Products. (E.g. GE, Philips, Carestream, Medtronic, etc.)	**Type-3** Vulnerability Remediation Efforts for Components on Medical Device. (E.g. Ripple20, Amnesia33, Ryuk, etc.)	Suspicious Activities, Investigation and Response. (E.g. strange activity on a specific device, etc.)	HTM Patch Management
Threat & Vulnerability Assessment				
Vulnerability Management Analysis & Report				
Nuvolo + Ordr+ Script + Dashboard Report	Dashboard Report + Nuvolo + Ordr	Dashboard Report + Nuvolo + Ordr	Email + Nuvolo + Ordr	Nuvolo + Ordr
Involves Vendor Inquiry Process	Vendor Information	Top 50 Vendor Process	Incident Communication Process	Patch Management Process

Type 1 Vulnerability – Operating Systems

- Windows
- Linux
- Real Time Operating System (RTOS)
- Proprietary OS

Type 2 Vulnerability- Vendor Specific

- CISA Vulnerability Advisories and Alerts



Type 3 Vulnerability- IoT and Components Vulnerabilities

AMNESIA:33

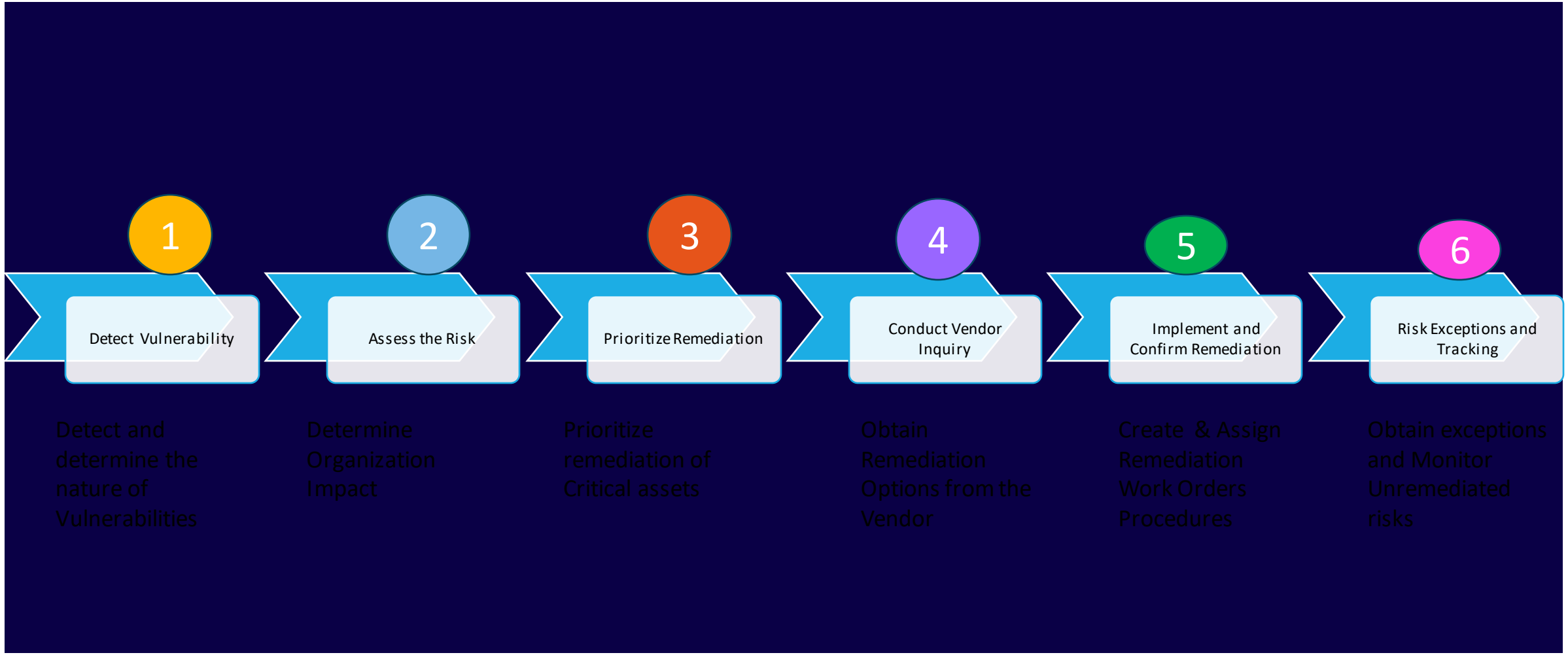
Critical TCP/IP Stack Vulnerabilities Affect Multiple Healthcare IoT Products

- Difficult to track
- Reliant on Vendor Disclosures
- Leverage SBOM
- Affecting mostly IoT Devices

ordr

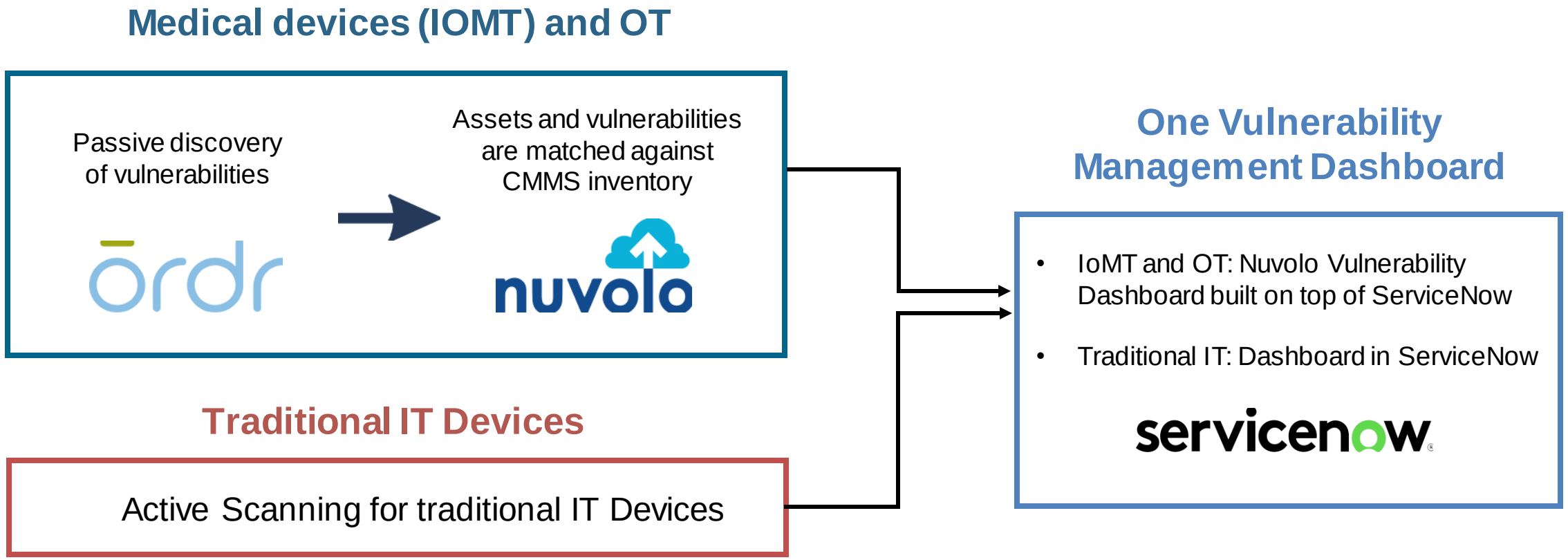
Ordr + Software Inventory Collector

Vulnerability Management Process



Mayo Clinic Best Practices: Technology

Passive Scanning for IoMT Feeds Into Centralized Dashboard



Zero Day Response: Log4J Vulnerability

- Log4J: Ubiquitous, Java-based logging tool
- Log4J vulnerability discovered in November 2021, including several remote code execution flaws
- CISA believes Log4J likely present in more than 2800 commercial products, and hundreds of millions of IT systems
- Challenge
  - *Was asset running Log4J?*
  - *Need to understand specific application and activity level (device is communicating to Log server)*
  - *Needed details at an asset level*

FDA, Omnibus and Patch Act Introduces Requirement for SBOMs

SBOM Facts

16 components in software package

# of Components Verified	**13**
Software Grade	**F***
Total Issues	
Unexpected Software Behaviors	**5**
Tampers with user/account privileges	3
Tampers with Internet download warnings	2
Active Threats Detected	**3***
High risk	2
Medium risk	1
Digital Signature Issues	**1**
Ineffective Mitigations	**0**
Sensitive Data Included	**0**

*Major supply chain risks detected. Consider this software package unsafe to install and run.

- SBOM = Software Bill of Material
- An SBOM is an inventory of all the components, libraries, and dependencies supporting a device or application, analogous to a packaged food product ingredient list.
- Current Formats are CycloneDX, SPDX, and SWID.
- Benefits for HDOs:
- Enables HTM and cybersecurity teams to identify if they are vulnerable
  - *Act more quickly in response to threats against their networks and environments.*

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

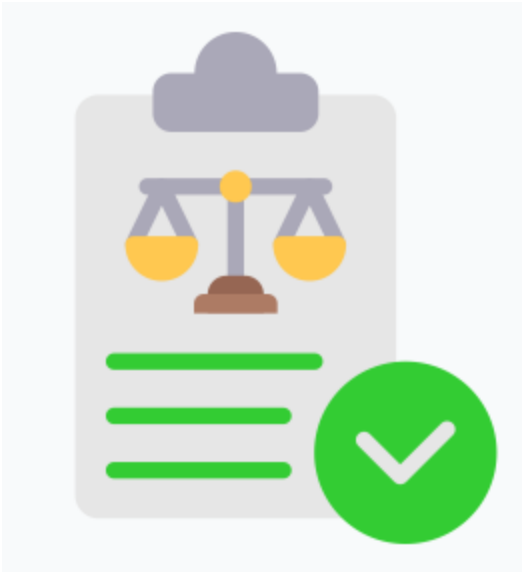
SBOM Limitations

- Point in time
- Limited capacity to ingest this in inventory in a useful way
  - *Some formats use PDF*
- Dependent on manufacturer to update when software is updated for every manufacturer/model
  - *As a developer, challenging to determine what is actually running and active in the field*
- Automation/integration needed via manufacturer sharing with HDO in future

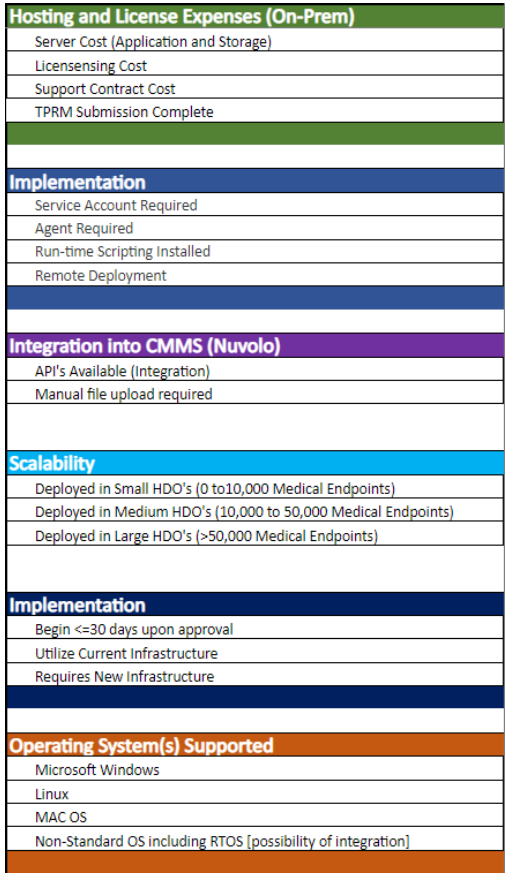
Mayo Clinic: Need Proactive Complement To SBOMs

Why do we feel empowered to be proactive?

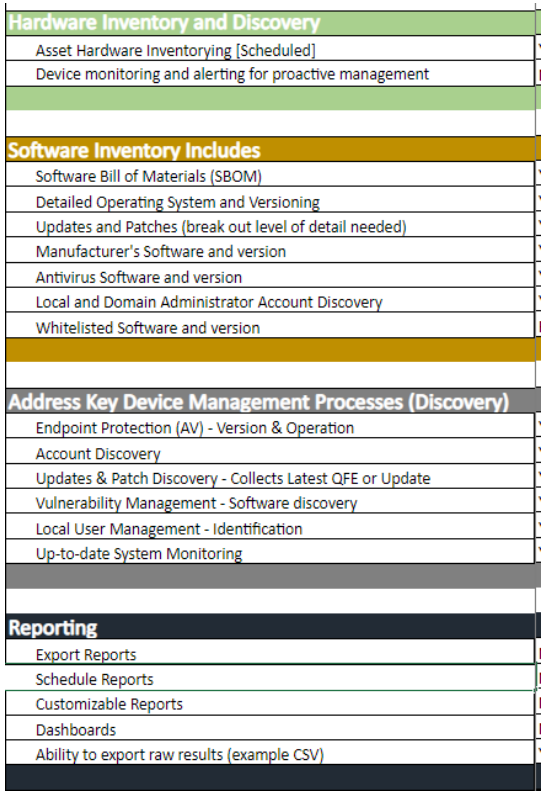
- Lack of the appropriate level of detail relating to assets
- Regulatory concerns
- Slow responsiveness from vendors
- High risk devices within environment
- Light-weight tool, using inherent technology
- Not an agent
- Real-time empirical data
- Strong contractual language in place with vendor partners (Information Security Agreement, Business Associate Agreement, Master Service Contracts)



Mayo Assessment of Tools



Hosting and License Expenses (On-Prem)
Server Cost (Application and Storage)
Licensensing Cost
Support Contract Cost
TPRM Submission Complete
Implementation
Service Account Required
Agent Required
Run-time Scripting Installed
Remote Deployment
Integration into CMMS (Nuvolo)
API's Available (Integration)
Manual file upload required
Scalability
Deployed in Small HDO's (0 to10,000 Medical Endpoints)
Deployed in Medium HDO's (10,000 to 50,000 Medical Endpoints)
Deployed in Large HDO's (>50,000 Medical Endpoints)
Implementation
Begin <=30 days upon approval
Utilize Current Infrastructure
Requires New Infrastructure
Operating System(s) Supported
Microsoft Windows
Linux
MAC OS
Non-Standard OS including RTOS [possibility of integration]



Hardware Inventory and Discovery
Asset Hardware Inventorying [Scheduled]
Device monitoring and alerting for proactive management
Software Inventory Includes
Software Bill of Materials (SBOM)
Detailed Operating System and Versioning
Updates and Patches (break out level of detail needed)
Manufacturer's Software and version
Antivirus Software and version
Local and Domain Administrator Account Discovery
Whitelisted Software and version
Address Key Device Management Processes (Discovery)
Endpoint Protection (AV) - Version & Operation
Account Discovery
Updates & Patch Discovery - Collects Latest QFE or Update
Vulnerability Management - Software discovery
Local User Management - Identification
Up-to-date System Monitoring
Reporting
Export Reports
Schedule Reports
Customizable Reports
Dashboards
Ability to export raw results (example CSV)

- Completed and analysis of several different tools in 2022
- Evaluated many different factors:
  - Technical feasibility
  - Coverage
  - Cost
  - Deployment effort
- Tested
- Collaborated with Ordr to define the output and tune the script
- Developing a “landing zone” for the data

Ordr Software Inventory Collector

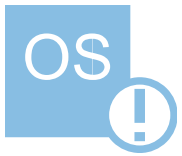
Lightweight script automatically collects granular context for all devices

- Any operating system (Win/Mac/Linux)
- Any location (on prem/remote/cloud)
- Physical or virtual
- Managed or unmanaged
- Online or offline

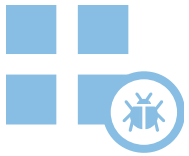
Device Context

- OS Patches/Updates
- 3rd Party Software Installed
- Anti-Virus Software Status
- Disk encryption
- BIOS password status

Comprehensive view of devices and vulnerabilities



Unpatched Operating Systems



Vulnerable Applications

Outdated/ Disabled AV

Mayo Clinic Best Practices:
SBOM Alternative for Device Context/Vulnerabilities

ōrdr

Software Inventory Collector

Plan: Enterprise wide installation starting with 1000+ devices during initial implementation phase

- *Integration with CMMS*
- *Single pane of glass – rich, real-time, empirical data including applications running on the device.*
- *Match against vulnerability management solutions*
- *Empirical risk scoring*
- *Internal whitepaper to educate*

Mayo Clinic Best Practices: Operationalizing Ordr Software Inventory Collector

Install Ordr Software Inventory Collector on:


Any new onboarded equipment


During patch management


During vulnerability management


During break fix

Benefits:

- ✓ Identify software applications on medical devices and facilities/IoT/OT equipment in real-time
- ✓ Ability to understand risk posture
- ✓ Ability to orchestrate and automate work
- ✓ Integrates with other existing cybersecurity and networking tools

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Summary

- Vulnerability management requires a broad strategy.
- Traditional vulnerability tools don’t work for IoMT, IoT, OT.

1. *Need a passive scanning tool like Ordr for IoMT, IoT, OT.*
2. *SBOMs being mandated but have limitations*
3. *Use Ordr Software Inventory Collector to complement SBOMs with understanding of applications and software levels in real-time*
4. *Send all data into centralized dashboard for enterprise-wide visibility and prioritization of vulnerabilities and risk management*

Questions & Discussions

Enter your questions to the Q&A window

Thank You

Please complete the online evaluation form at

https://www.surveymonkey.com/r/2023-2024_2

or scan the QR code

2024 ACCE ADVOCACY AWARD

CALL FOR NOMINATIONS

THE AWARD CATEGORIES ARE:

DEADLINE: December 10, 2023

Awards will be presented at ACCE awards reception during 2024 AAMI eXchange, Phoenix, AZ

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING