ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

A Stronger Future with Legacy Technology

Building a Strategy

Ty Greenhalgh
Industry Principal, Healthcare
Medigate by Claroty
Ty.g@claroty.com

Skip Sorrels
Director, Cyber Security
Ascension Technologies

MEDIGATE by Claroty

Ascension

March 16th, 2023

ACCE gratefully acknowledges the sponsorship of this webinar by

About the Moderator

Juuso Leinonen

Principal Project Engineer
ECRI

Juuso Leinonen is a Principal Project Engineer, at the Device Evaluation group at ECRI, where he performs comparative medical device evaluations and investigates medical device related accidents. His current subject-matter expertise includes infusion technology, medical device cybersecurity, and telehealth.

Logistics

- All attendees have their microphones muted during the presentation.
- Questions to the panelists must be submitted via the “Q&A” feature (not chat) in Zoom at any time.
- If there is any urgent issue, please use the “chat” feature to communicate with the panelists.
- We will try to ask Ty, Skip and Jon to answer questions not addressed during the webinar and distribute them to participants via email or post them to ACCE website.
- Please remember to complete the webinar evaluation after attending. A link will be provided at the end.

About the speaker

Ty Greenhalgh, HCISPP
Industry Principal, Healthcare

MEDIGATE
by Claroty

Ty Greenhalgh was an early pioneer of the electronic medical record (EMR). The Henry Ford Health System awarded the "Most Innovative Technology of the Year" to Mr. Greenhalgh, in conjunction with the AHIMA, for groundbreaking work in developing one of the first EMR systems to contain automated HIM workflow, electronic signature and integration into the AHIMA FORE library in Chicago.
He was employed with 3M Health Information Systems for over 25 years. He helped introduce disruptive technologies to include Remote Transcription, Digital Dictation and Speech Recognition, Document Scanning, Computer Assisted Coding and Computer Assisted Clinical Documentation Improvement.
Ty is currently an ambassador with the HHS 405(d) Program and Task Group which was responsible for the recognized security practices referenced in the new HITECH amendment more commonly known as the *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients.*

Ty is currently the Healthcare Industry Principal with Medigate by Claroty. Claroty, a worldwide leader in cybersecurity, empowers organizations around the world to secure all their cyber-physical systems. Claroty recently purchased Medigate, the Best in KLAS healthcare solution, integrating the tools required for cybersecurity of medical devices to become the dominant leader for healthcare device cybersecurity. Ty has authored dozens of articles and is a frequent speaker for AHIMA, HCCA, HIMSS and AAMI.

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

About the speaker

Skip Sorrels
Director of Cybersecurity
Ascension Technologies

Skip Sorrels is Director of Cybersecurity for Ascension Technologies having oversight across Ascension for cyber and information security operations. He is responsible and directs the following programs: standards and policies (GRC), vulnerability management, privileged access management, threat intelligence, pen testing, medical device and operational technologies cyber security.

Previously, Skip served as Dell and then NTT's Program Executive of service delivery for Ascension as well as for AMITA Health. He is a graduate of the University of Arkansas for Medical Sciences.

Session Description

Legacy equipment in healthcare is a pervasive cybersecurity risk. The IMDRF has defined a legacy device as medical devices that cannot be reasonably protected against current cybersecurity. Legacy devices are critical to healthcare delivery, are cost prohibitive to simply replace and mitigating their risks cause confusion and contention between medical device manufacturers (MDM) and healthcare delivery organizations (HDO) when it comes to Governance, Communications, Cybersecurity Risk Management and Future Proofing.

The Healthcare Sector Coordinating Council (HSCC) has recently released *Health Industry Cybersecurity – Managing Legacy Technology Security (HIC-MaLTS)* which defines the shared responsibilities and tasks for mitigating risk for currently installed devices, and those in development. Developed over 2 years by a team of 67 experts, it provides Insights, Challenges and Recommendations for how MDMs and HDOs can develop their own strategies while increasing effective communication between themselves.

- In this session you will learn:
  - What is HIC-MaLTS?
  - Who should use it?
  - The 4 Core Pillars.
  - How to address the common legacy cyber risk management challenges?
  - What is the “Responsibility Transfer Framework”?
  - Recommendations for Patching and Lifecycle Management.

Agenda

- What is HIC-MaLTS?
- The 4 Core Pillars
- Legacy Cyber Risk Management Challenges
- Responsibility Transfer Framework
- Patching Lifecycle Management

- Questions

Claroty At-A-Glance

Empowering organizations with unmatched security for all cyber-physical systems across the XIoT

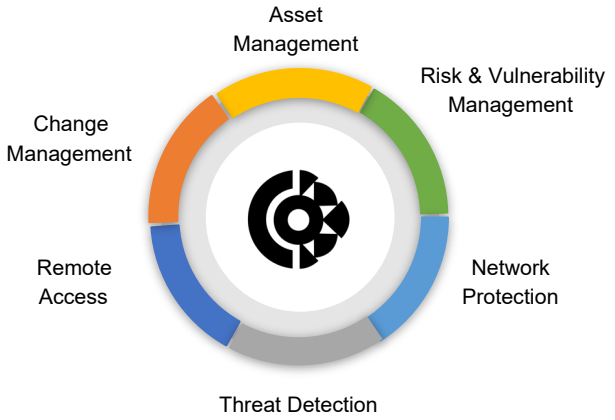
HQ: **NYC**	Founded: **2015**	Funding: **$635M (Series E)**	Healthcare Facilities: **1000+**

DEEP DOMAIN EXPERTISE

The Extended Internet of Things (XIoT)

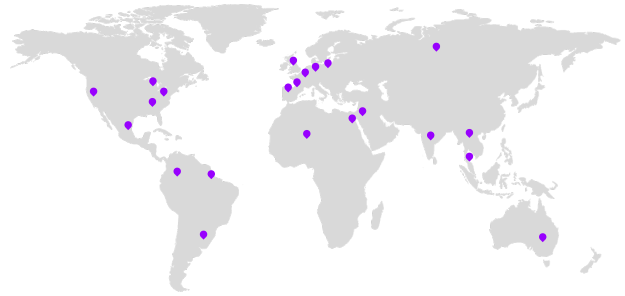
Industrial **Commercial** **Healthcare**

COMPREHENSIVE CAPABILITIES



GLOBAL ADOPTION

100s of Orgs, 1000s of Sites, 50+ Countries, 25+ Verticals



VALIDATION FROM LEADING INDUSTRY ANALYST FIRMS & OTHER TRUSTED THIRD-PARTIES

SC AWARDS · 25TH YEAR · TRUST AWARD WINNER 2022

DEVELOPMENTAL TESTING AND EVALUATION DESIGNATION · SAFETY ACT · www.safetyact.gov

FORRESTER® WAVE LEADER 2021 Industrial Control Systems (ICS) Security Solutions

BEST IN KLAS HEALTHCARE IOT SECURITY 2021 · BEST IN KLAS HEALTHCARE IOT SECURITY 2022 · BEST IN KLAS HEALTHCARE IOT SECURITY 2023

500™ Technology Fast 500 2022 NORTH AMERICA Deloitte.

2021 CYBERSECasia READERS' CHOICE AWARDS

The Medigate by Claroty Platform

This comprehensive, scalable solution is purpose-built for your entire healthcare cybersecurity journey

Vuln & Risk Management | **Network Protection** | **Threat Detection** | **Device Management** | **Lifecycle Management** | **Operational Intelligence**

Device Discovery

White-Glove Delivery Model

Simple Onboarding & Purpose-Built UX

Fully Integrated Ecosystem


Patient Monitoring


Imaging Equipment


Lab Equipment


Care Administration


Infrastructure


Web Servers


Printers


Workstations


Elevator


Smart Grid


BMS/BAS


HVAC


Physical Intrusion

Smart Devices


Signage


Mobile Devices

Internet of Medical Things (IoMT) | **Information Technology (IT)** | **Smart Buildings/Grids (BMS)** | **Internet of Things (IoT)**

Regulation and Legislation

Aligning Claroty Functionality with Basic Cyber Hygiene for Connected Medical Devices

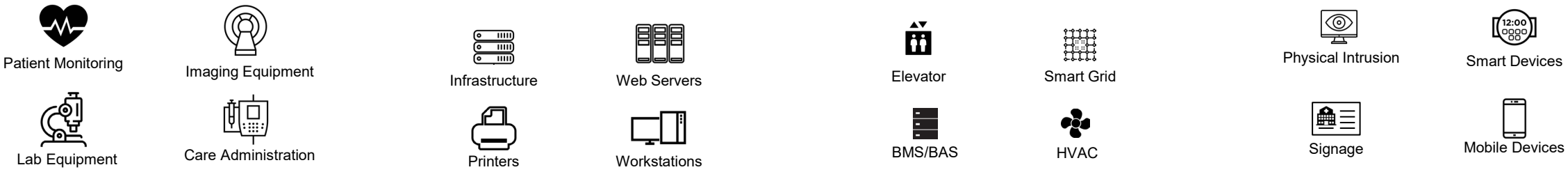
Vuln & Risk Management | **Network Protection** | **Threat Detection** | **Device Management** | **Lifecycle Management** | **Operational Intelligence**

Device Discovery

White-Glove Delivery Model

Simple Onboarding & Purpose-Built UX

Fully Integrated Ecosystem



Internet of Medical Things (IoMT) | **Information Technology (IT)** | **Smart Buildings/Grids (BMS)** | **Internet of Things (IoT)**

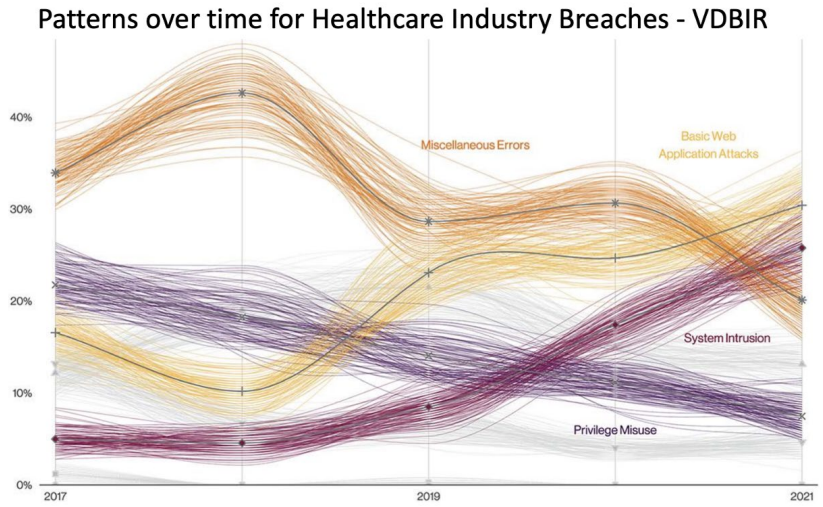
ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Regulation and Legislation

Aligning Claroty Functionality with Basic Cyber Hygiene for Connected Medical Devices

CLAROTY FUNCTIONALITY	405(d)	Warner CIPS	HIC MaLTS	FDA Post Market	Section 3305 (PATCH)
Device Discovery	9MA, 9MD	2.3, 3.1, 3.4	Visibility, Technical Investigation, MDS2, SBOM/VEX, Assessment Surge	Monitor for Identification & Detection of Vuln. & Risk over Lifecycle; Intack & Handling.	524B.(b).1
Vuln & Risk Management	9ME	2.1, 2.2, 3.4, 4.4, 5.1, 5.4, 5.5, 6.1	Disclosure, Patching Lifecycle, Updates, Risk Mgmt.	Detecting Presence and Impact of Vuln. Deploy Mitigations & Remediations	524B.(b).2, 524B.(b).2.(A), 524B.(b).2.(B)
Network Protection	9MG	2.1, 2.3, 3.4, 8.1	Connectivity & Technical Exposure Reduction	Traffic Monitoring using Deep Packet Inspection, Automated Network Segmentation/Zero Trust.	
Threat Detection	9MD	1.1, 1.2, 1.3, 1.4, 2.1, 3.4, 5.4	HDO Cybersecurity Signals	Anallyze Detect and Assess Threat Sources.	524B.(b).2.(A)
Device Management	9MA, 9MD	2.1, 2.2, 2.4, 2.5, 3.1	CMMS Unified Asset Mgmt.	Integration with CMMS for single source inventory & automated workflow	
Lifecycle Management	9LC	2.1, 2.2, 3.4, 4.5, 6.2	EOG, EOS, EOL, Technology Stages	Maintain Safety & Essential Performance: CVSS 3.0, Manufacturer CVSS	524B.(b).2
Operational Intelligence	9MB	2.1, 2.5, 3.4, 3.5, 7.4	Communications	Assess Severity of Patient Harm	524B.(b).2, 524B.(b).2.(A, 524B.(b).2.(B)

HIC-MaLTS



- Health Sector Coordinating Council (HSCC)
  - 67 Security Experts over 2 years
- Reason
  - Networks are evolving in complexity; remote monitoring, telehealth, cloud, etc.
  - Healthcare is a target rich environment containing valuable data
  - Diverse device types; diagnostic, therapeutic, wearable, implantable, SaMD, etc.
  - Off-The-Shelf components create inconsistent lifecycles
  - Need for better understanding of cyber responsibilities between HDO & MDM
  - Slow adoption of improved practices
  - Wide variation of size and capabilities of healthcare organizations

What is a Legacy Medical Device?

- Defined by the IMDRF Cyber Working Group
  - Medical devices that cannot be reasonably protected against current cybersecurity threats.
- HDO
  - Is it past manufacturer declared EOL/EOGS/EOS
  - Contains a critical software component (e.g., operating system) which is not supported
  - Components in the Software Bill of Materials (SBOM) is not supported
- MDM
  - Off-The-Shelf (OTS) software components no longer receive support
  - Hardware (e.g., PLC, CPU) no longer receive support
  - Technology firmware no longer receive support
  - Contains Known Exploitable Vulnerabilities (KEV) with limited mitigations
  - Technology does not have a mechanism to update software, firmware, etc.

Structure of the Publication

- Modular components create actionable content
- Designed for both HDO and MDM
- 114 Pages
- 4 Core Pillars
- Responsibility Transfer Framework
- Patching & Lifecycle Management
- Common Legacy Risk Management
  - Challenges & Recommendations

Core Pillar #1 - Governance

- Define goals and objectives
- Establish responsibilities
- Enable accountability
- Insure information flow & monitoring
- Supports compliance & lifecycle mgmt.

Governance – HDO Considerations

- Defining a legacy tech risk management strategy
    - Procurement requirements
    - Risk assessment and prioritization
    - Incident response and business continuity
    - Information Sharing
    - Vulnerability management
    - Asset lifecycle management
    - Disposal and data protection
- Establish a model and criteria for risk tolerance
    - Probability * Impact vs. Exploitability
- Developing a lifecycle management plan
    - Tracking inventory and managing technology
    - Implementing risk remediation practices
    - Planning technology replacement & decommissioning

Core Pillar #2 - Communications

- Diverse stakeholder groups – engage the correct team members
- MDMs communicate with HDOs
  - New product, alerts/recalls, upgrades, vulnerabilities, etc.
- HDOs communicate with MDMs
  - Cyber assessments, vulnerabilities, upgrades, incident reports, etc.
- Topics of interest
  - Coordinated Vulnerability Disclosure Programs
  - Security & supply chain documentation
  - Technology lifecycle information
  - Vulnerabilities

Core Pillar #3 – Cybersecurity Risk Management

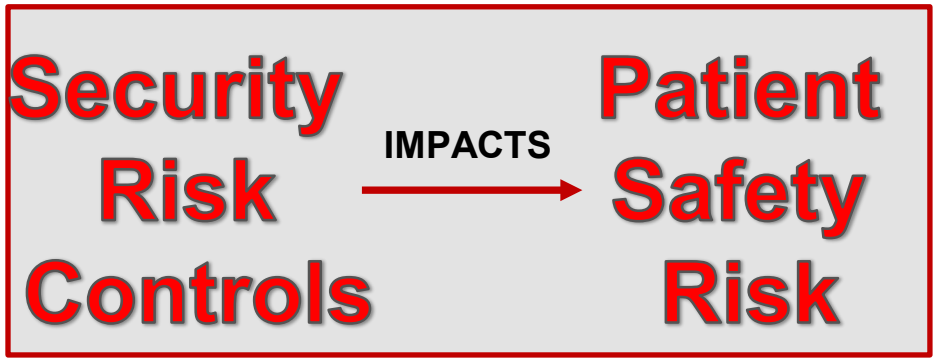
HDO Considerations

- Passive Network Monitoring (PNM)
  - Observe and analyze network traffic
  - Complement with internally collected data (SBOM, MDS^2, Manufacturer, etc.)
  - Provide asset risk information
  - Abnormal network behavior
- Stages of Risk Management throughout Technology Lifecycle
  1. Product Assessment
  2. Acquisition
  3. Implementation
  4. Support/Maintenance
  5. End of Support
  6. Decommissioning

Core Pillar #3 – Cybersecurity Risk Management

MDM Considerations

- Medical Device & Health Joint Security Plan
- HDO environments will be different than MDMs
  - Requiring contextual assessments
  - MDMs should play a role
- MDM should send EOL/EOGS/EOS to HDO



Core Pillar #3 – Cybersecurity Risk Management

Responsibility Transfer Framework

- Should the HDO continue to utilize the device or decommission?
- Risk Assessment Factors
  - Safety and Effectiveness – can the HDO handle support
  - Clinical – impact clinical care workflows & patient safety
  - Technical Examples
    - Known Exploitable Vulnerabilities
    - Mitigations
    - Remote protocols, ports or services needed?
    - Will security controls mitigate the vulnerabilities
    - Costs

EOL/EOGS/EOS Options

	Supported	Unsupported
Option #1		
Hardware	X	
Software		X
Option #2		
Hardware		X
Software	X	
Opton #3		
Hardware		X
Software		X

Core Pillar #4 - Future Proofing

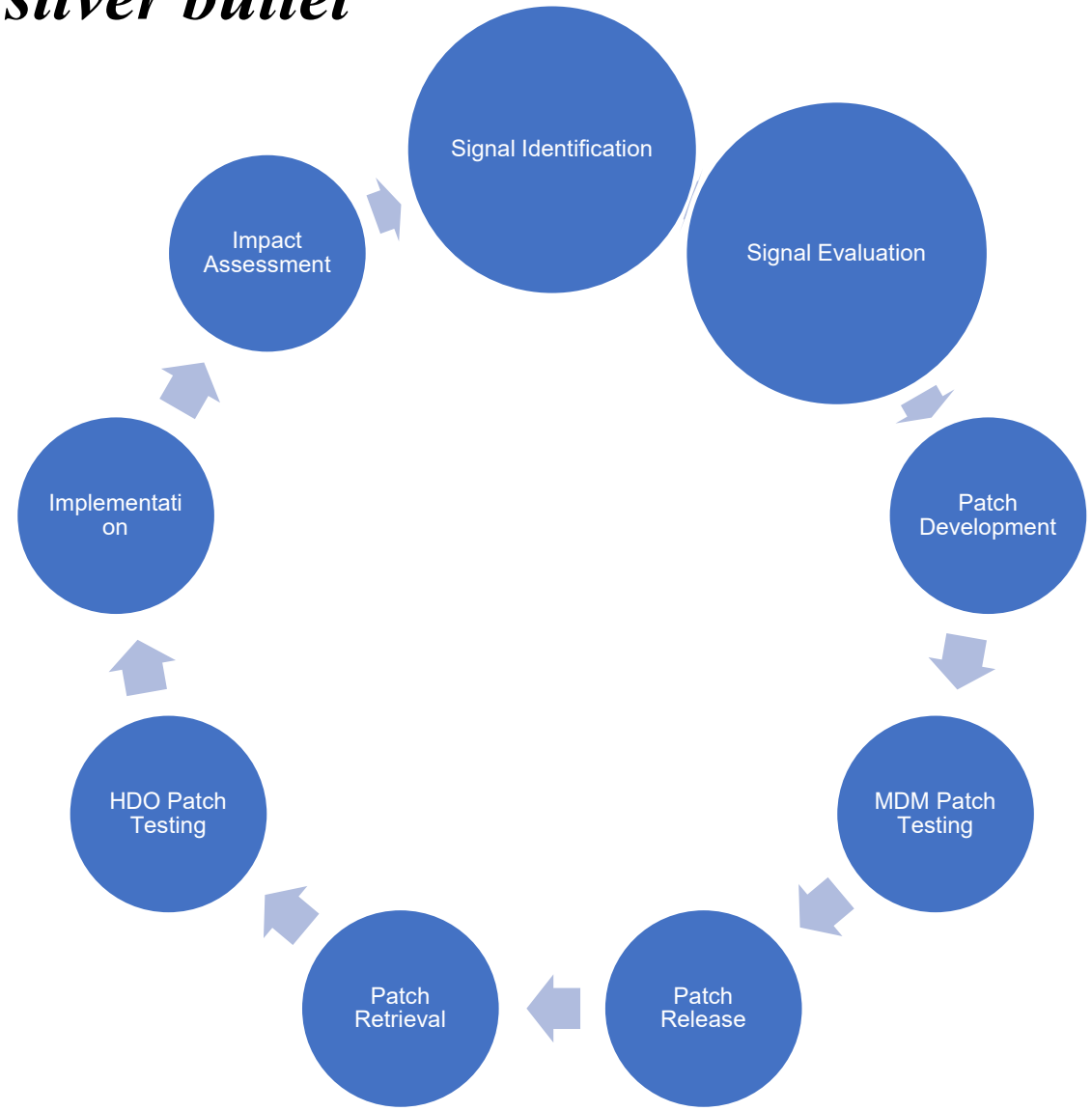
- Address Know Legacy Issues During Threat Modeling
- Secure Technology Design
  - Selecting software
  - Alignment with Executive Order 14028
- Secure Technology Deployment

Patching Management Lifecycle

Not a silver bullet

Patching Management Lifecycle

Not a silver bullet



What is a signal?

A cybersecurity signal can refer to any kind of indication or alert that suggests a potential security threat or breach within a system or network

Patching Management Lifecycle

Not a silver bullet

HDO Signals

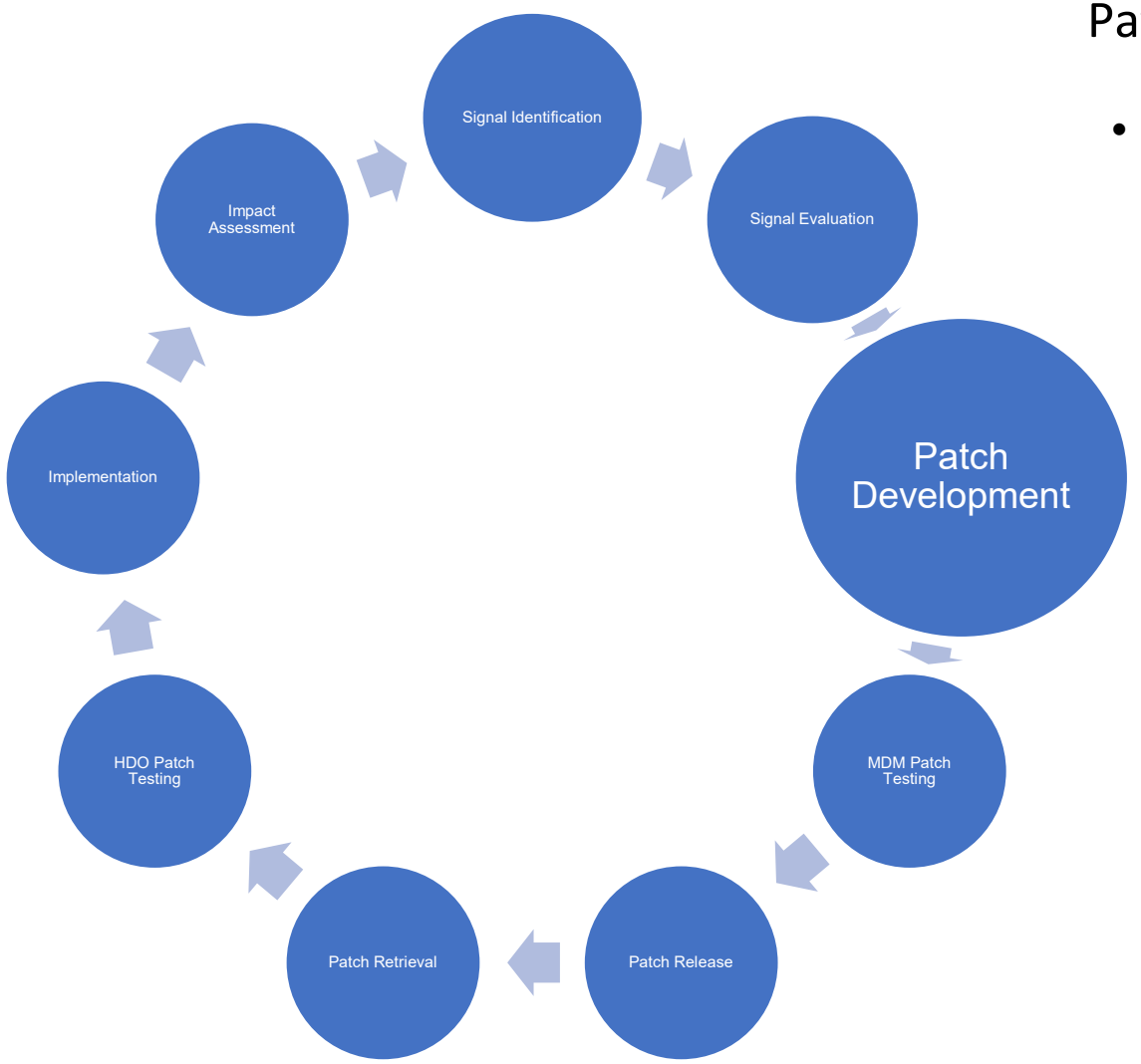
MDM Advisories
CERT Advisories
Vuln Scanning
Monitoring
Security Incidents
Researcher
Regulator
ISAC/ISAO

MDM Signals

Vuln Monitoring
Gap Analysis
Security Audit
Pen Testing
Static Code Analysis
Supplier
Regulator

Patching Management Lifecycle

Not a silver bullet



Patch Development

- Communications provided by MDM to HDO
  - Patch Details, Risks it Addresses, Links to Vuln. Com., Delivery Date, Who Installs, Install Req., Post Testing, Labeling, ……

Patching Management Lifecycle

Not a silver bullet

Patch Testing

- Module, verification, security and regression testing
- Implementation & technical assessment

Patching Management Lifecycle

Not a silver bullet

Software Bill of Materials

Omnibus Bill 2023 SEC. 3305. ENSURING CYBERSECURITY OF MEDICAL DEVICES.
IN GENERAL.—Subchapter A of chapter V of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 351 17 et seq.) is amended by adding at the end the following:

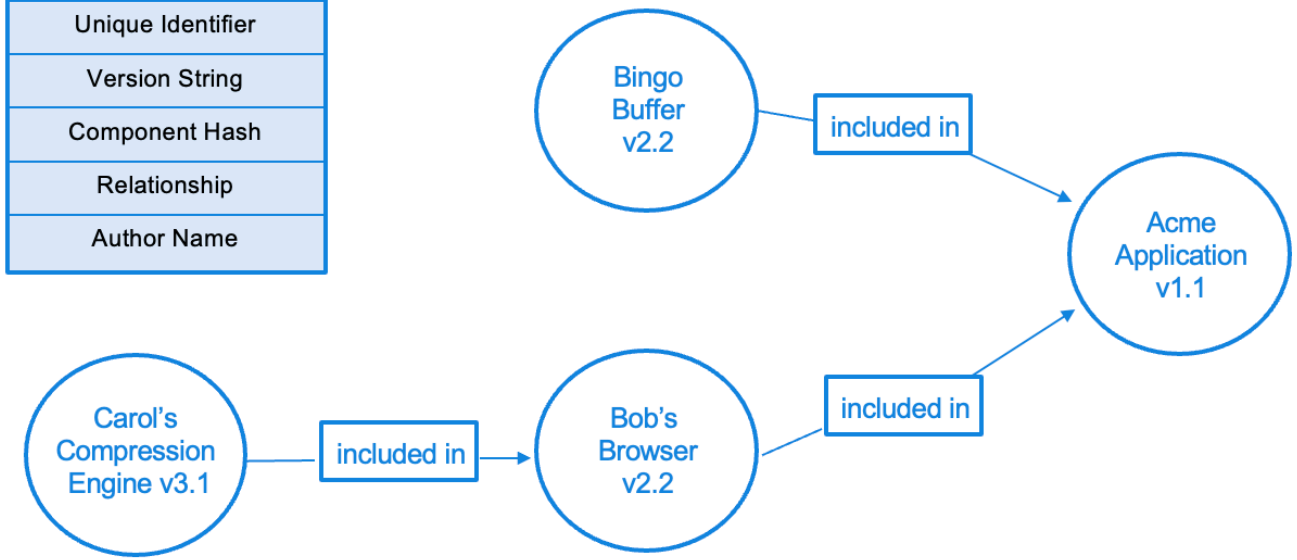
(2) design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure, and make available postmarket updates and patches to the device and related systems to address—

‘‘(A) on a reasonably justified regular cycle, known unacceptable vulnerabilities; and

‘ ‘(B) as soon as possible out of cycle, critical vulnerabilities that could cause uncontrolled risks;

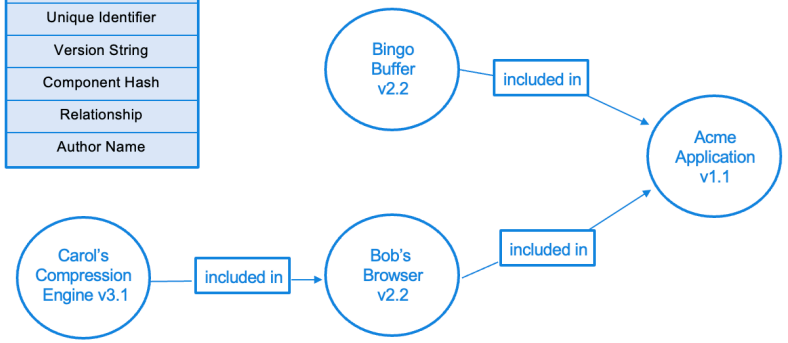
‘‘(3) provide to the Secretary a software bill of materials, including commercial, open-source, and off-the-shelf software components;

Baseline Software Component Information
Supplier Name
Component Name
Unique Identifier
Version String
Component Hash
Relationship
Author Name



Software Bill of Materials

Baseline Software Component Information
Supplier Name
Component Name
Unique Identifier
Version String
Component Hash
Relationship
Author Name



HDO

- Request from MDM SBOM information in machine readable format
- Leverage passive monitoring tools
- Import and analyze to identify released vulnerabilities (NVD or ISC-CERT)
- Do technologies in the inventory contain software components affected

MDM

- Develop maintain and provide SBOMs to HDOs over life of device
- For EOS, provide customers with Final/Last SBOOM

Additional Topics in HIC-MaLTS

Third Party Servicers

Connectivity

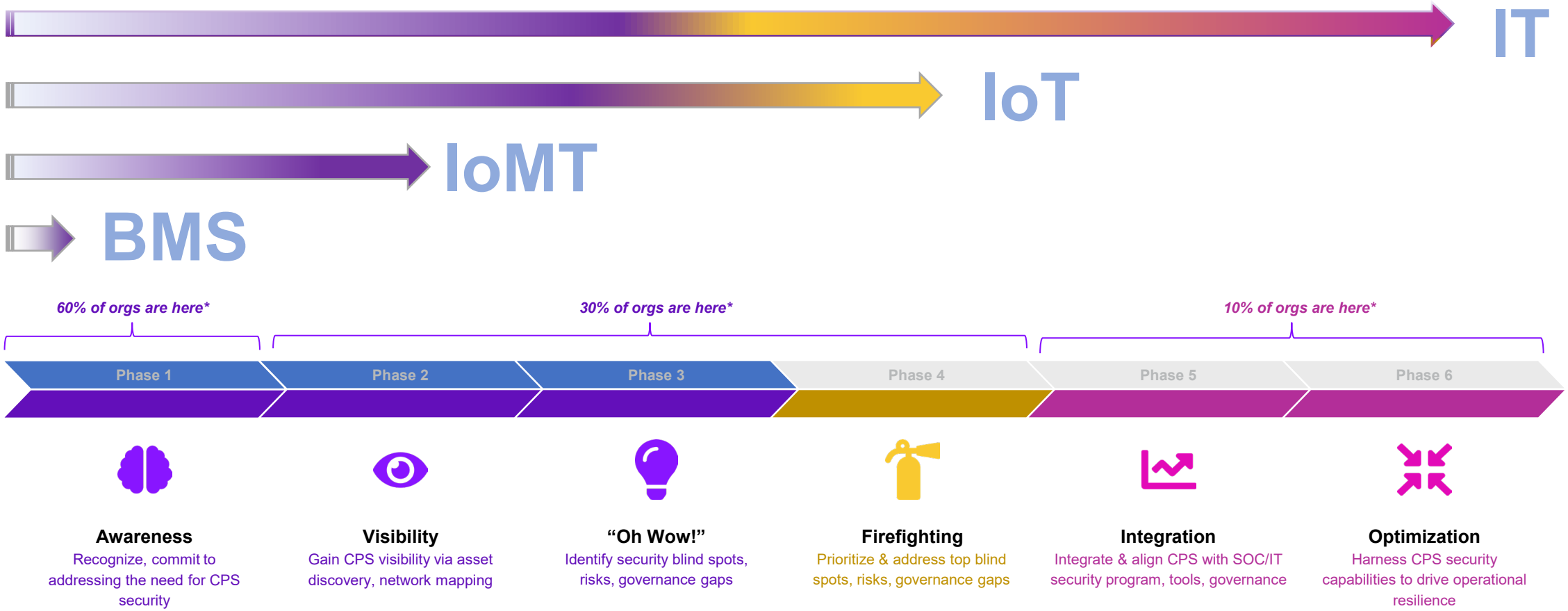
3rd Party Components

End-of-Life/Service

Inventory/Asset Management

The Cyber-Physical Systems (CPS) Security Journey

Gartner's 6-phase approach to achieving CPS Security Maturity



Gartner®

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Resources

- Health Sector Coordinating Council (HSCC)
- HIC-MaLTS
- Joint Security Plan – Cyber Risk Mgmt. for MDMs
- Senator Warner – Cybersecurity Is Patient Safety (CIPS)
- White House Cybersecurity Strategy
- 405(d) Healthcare Industry Cybersecurity Practices (HICP)
- NIST CSF Healthcare Implementation Guide

Thank You

Please complete the online evaluation/attendance form at https://www.surveymonkey.com/r/03_-16-23

Skip Sorrels

Ty Greenhalgh – ty.g@claroty.com