ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

IoMT Risk Remediation: How Context-rich Assessments Rationalize Response Effectiveness

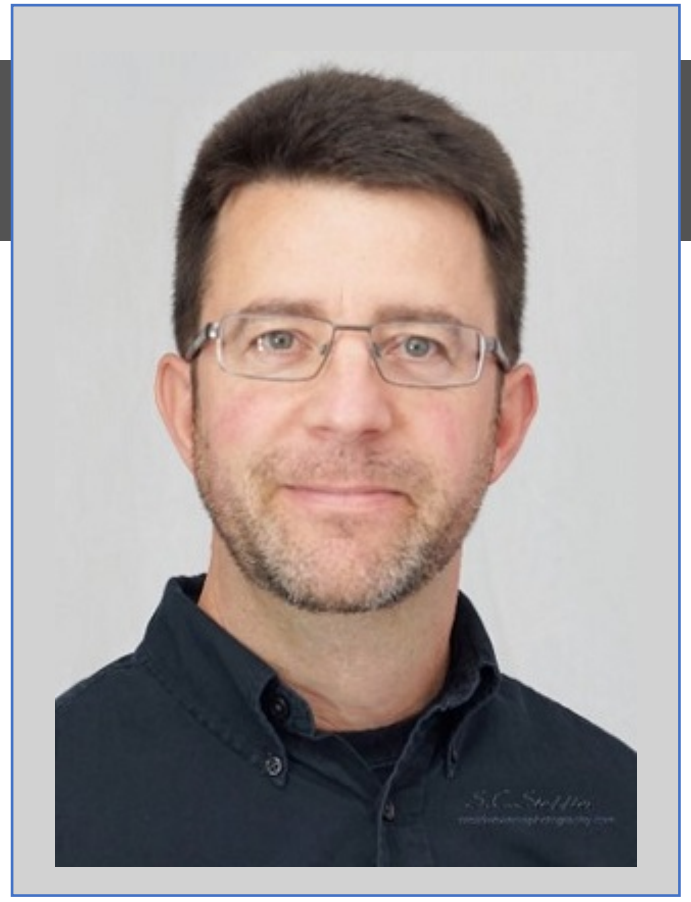
Drew Ganther - Presenter
Regional Director of Sales – WEST
Medigate

Matt Dimino - Presenter
Connected Asset Program Manager
First Health Advisory

July 22, 2021

ACCE gratefully acknowledges the sponsorship of this webinar by

About the moderator



Martin Poulin, P.Eng., FCMBES| Director, Biomedical Engineering

Director of Biomedical Engineering for Island Health, Victoria, BC, on the west coast of Canada.

22+ years management

5 years in the medical device development industry in Vancouver.

Master of Engineering in Clinical Engineering from UBC

Past President of CMBES

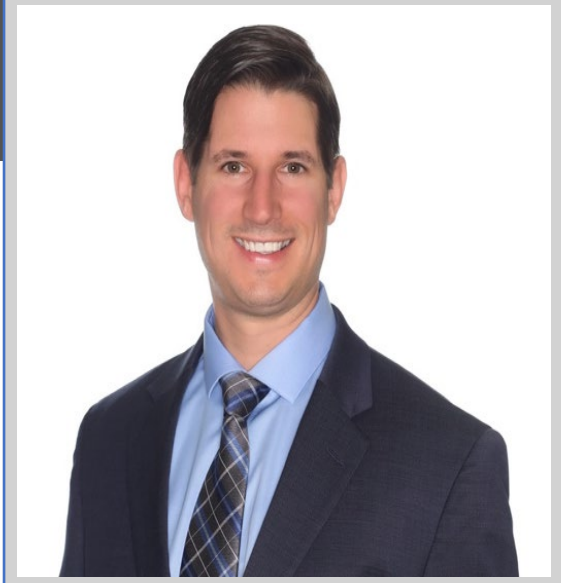
About the speaker

Drew Ganther, Regional Director at Medigate

Drew Ganther is Regional Director at Medigate. Before joining Medigate as the first sales leader in the western US, Drew spent 7 years with an IT systems reseller and professional services organization where he helped create a cyber security consulting practice (later acquired by Insight). Drew's career started in IT training after he moved from Virginia Beach, VA to San Diego, CA with his Bachelors Degree from James Madison University in Harrisonburg, VA.

About the speaker

Matt Dimino, Connected Asset Program Manager at First Health Advisory



Matt comes to First Health as a Connected Asset Program Manager. He brings a wide range of technical, security, academic and HTM knowledge to this team. Matt has over 15 years' experience in various roles from associate faculty teaching Infosec, IT, HTM courses, and HTM leadership roles, many of those years as a practitioner in medical device security. Through his career he has developed multiple security programs, integrated complex architectures, performed security consulting, as well as developed risk assessment methodologies coupled with hands on device hardening experience. A major focus for Matt is to expand on IoMT risk management strategies and prepare First's customers and partners for the future of IoMT.

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 Drew and Matt 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.

Session Description

IoMT risk is constant and ever evolving as the threat landscape changes and our ecosystem of disparate systems continues to grow and intertwine. IoMT systems have numerous dependencies and factors that create not only inherent risk, but aggregated and cascading risk which can have significant impacts on how and what IoMT risks to remediate. The process behind risk remediation is to characterize the systems and contextualize the risks to understand what they mean to the organization faced with them before trying to remediate them. Today, to properly remediate IoMT risks, healthcare organizations must understand the environment of the risks and learn how to prioritize by evaluating and ranking risks that are most credible.

Medigate's Drew Ganther and Matt Dimino from First Health Advisory will host a conversation about the IoMT risk identification and remediation. Webinar attendees will be treated to an open, candid discussion.

IoMT Risk

Your Challenge

- CVE's / CISA notifications, industry alerts, and IoMT passive scanning tools are revealing more vulnerabilities, increasing risk, and it's unclear how to manage and prioritize.
- Organizations are struggling to not only understand IoMT risk but also how to prioritize vulnerabilities for remediation, as there are many factors to consider, including the threat of the vulnerability, the exposure, and the potential remediation option.

Common Obstacles

- Patches are often seen as an answer to vulnerabilities, but these are rarely an applicable solution as many IoMT systems cannot be patched.
- Many don't understand that vulnerabilties for IoMT devices exist beyond CVE's and CVSS scores.
- Organizations are unaware of the risk implications and lack insight to remediation options.

Approach

- Design and implement a risk management program that identifies, prioritizes, and remediates vulnerabilities, anomalies and risk.
- Understand what needs to be considered when implementing remediation options, including patches, configuration changes, and defense-in-depth controls.
- Build a strategy from a framework that includes a risk management lifecycle approach that allows you to identify risk, assess risk, apply risk response and mitigation efforts and risk monitoring.

Vulnerability management  Patch Management

ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

IoMT Risk is a Business Risk

- The business risk associated with the use, ownership, operation, involvement, influence and adoption of IoMT within an enterprise.
- We are failing to grasp the security risks of our IoMT assets.
  - Risk is constant and ever evolving as the threat landscape changes and our ecosystem of disparate systems grows.
  - IoMT has dependencies and factors that create not only inherent risk but aggregated and cascading risk.
  - Understand the environment of the risks and learn how to prioritize by evaluating and ranking risks that are most credible.
- Process behind risk remediation is to characterize the systems and contextualize the risks to understand what they mean to the organization.

What is Risk?

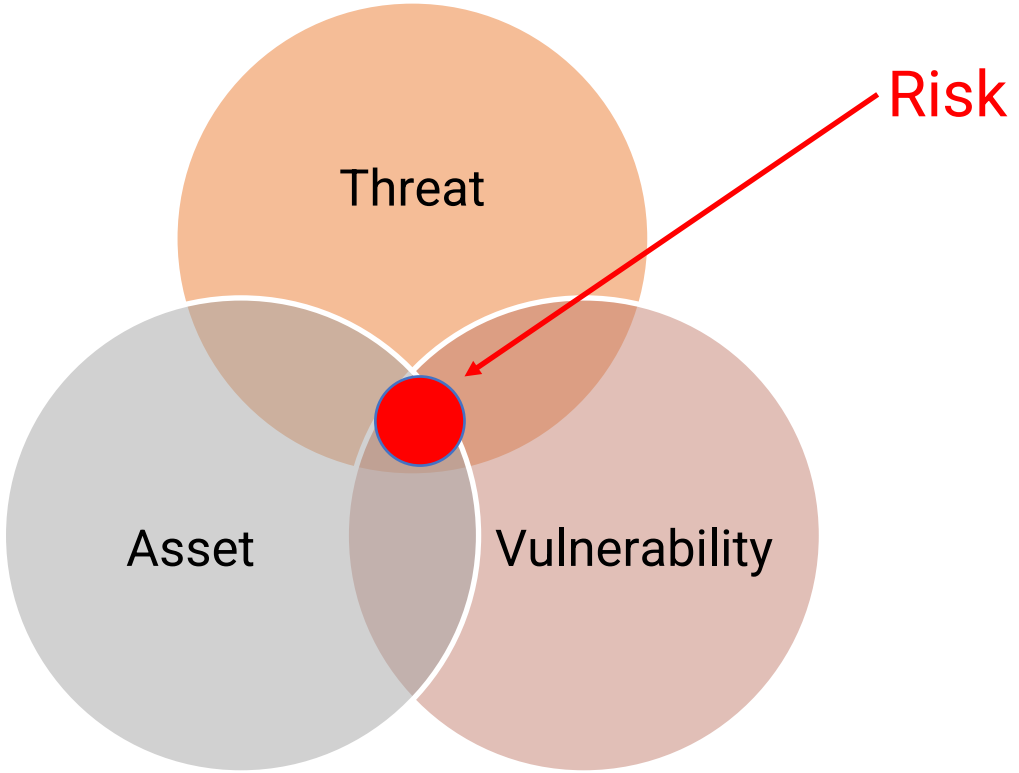
- **Risk** is a combination of the probability of an event and its consequences.
- The probability of an event is the likelihood that a given threat will exploit an exposed vulnerability.
- If there are no consequences or impact, there is considered to be no **risk.**
- Conversely, the greater the consequences or impact, the greater the risk.

- **Exposure**, the extent to which a vulnerability is exposed, to a threat factors into the risk equation.
- Exposure is also known as the attack surface.
- Exposure is affected by the extent and effectiveness of controls and where a particular device is within the network.

What is a Vulnerability?

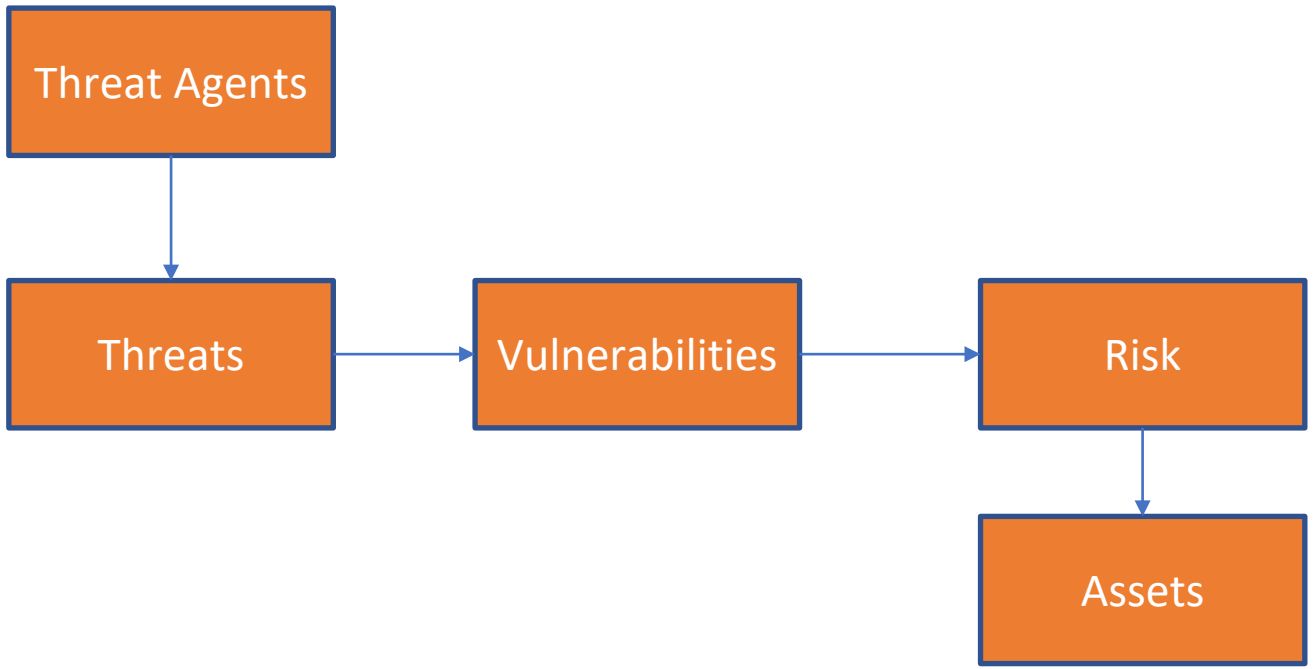
Any kind of exploitable weak spot in your defense that threatens your organization:

- Unpatched Software
- Misconfiguration
- Weak Credentials
- Phishing
- Trust Relationships
- Compromised Credentials
- Malicious Insider
- Missing Encryption
- Zero-days and Unknown Methods



Elements of IoMT Risk

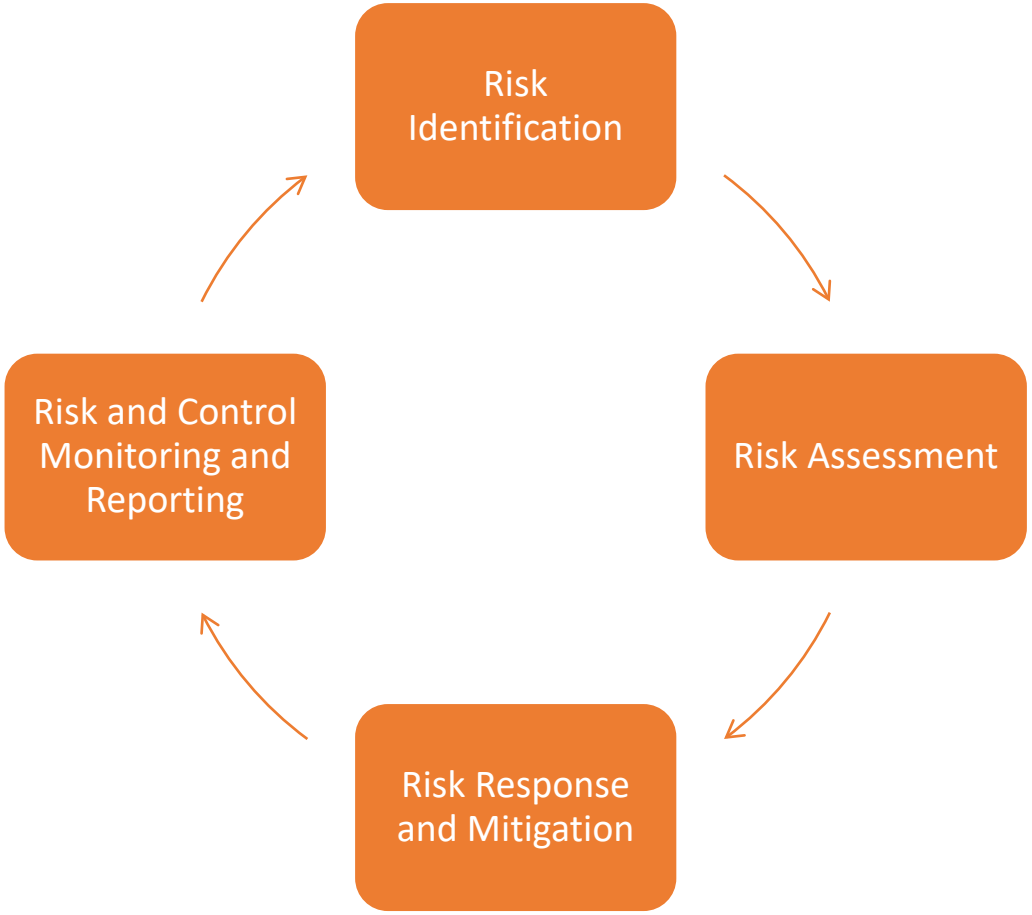
- Consequences associated with specific assets
- A threat to those assets, requiring both intent (motivation) and capability
- Vulnerability specific to the threat




THREATS
CONTROL
ASSETS
FOOD COURT
BOUTIQUE
EXPLOIT
VULNERABILITY
ATTACK
ASSETS
Jewels

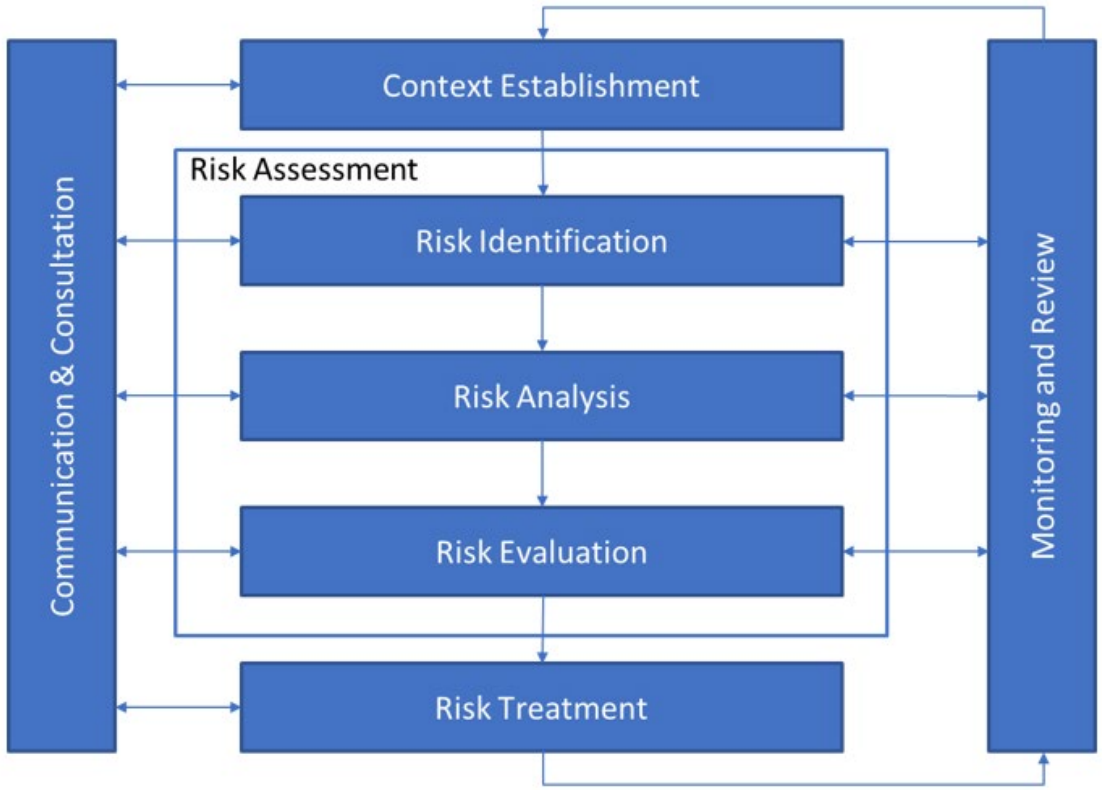
The Risk Management Approach

- Develop a Risk Management Strategy
  - Define scope and charter
  - Define risk appetite
- Begin by identifying risk
- Frame and analyze risk
- Evaluate Risk

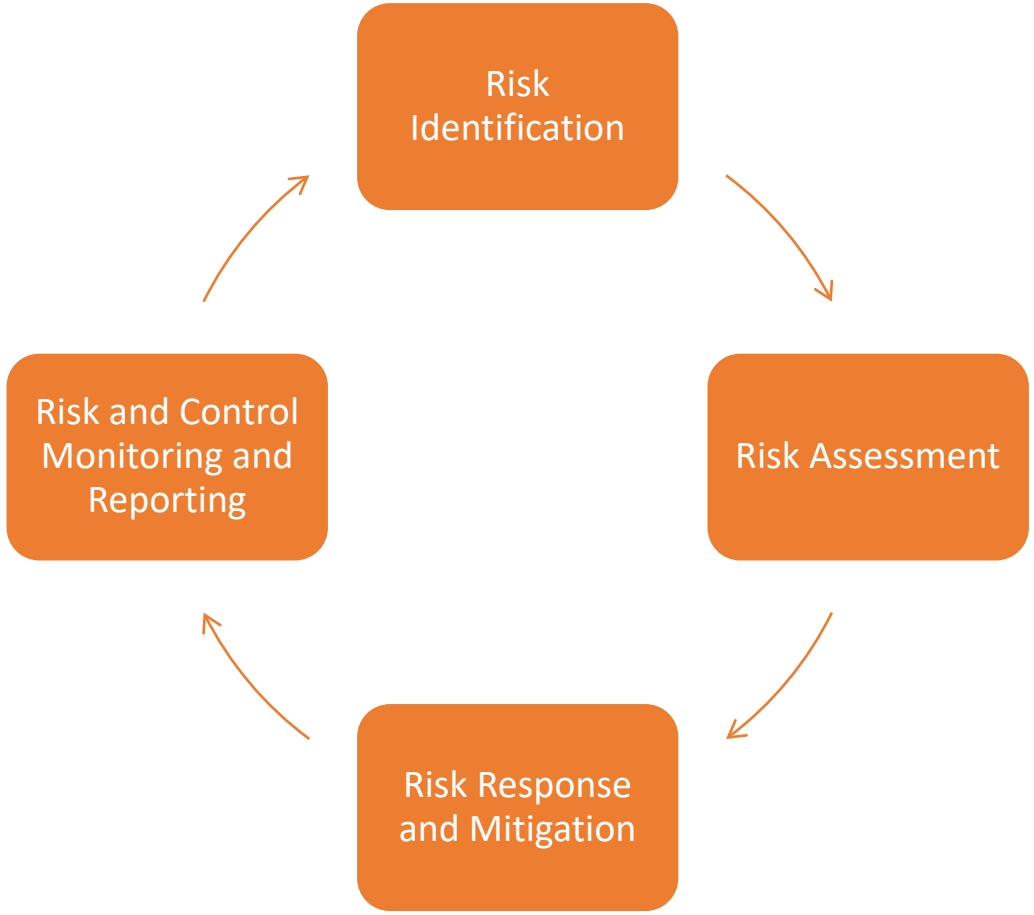


Risk Management Lifecycle

The Risk Management Approach



Risk Management Process

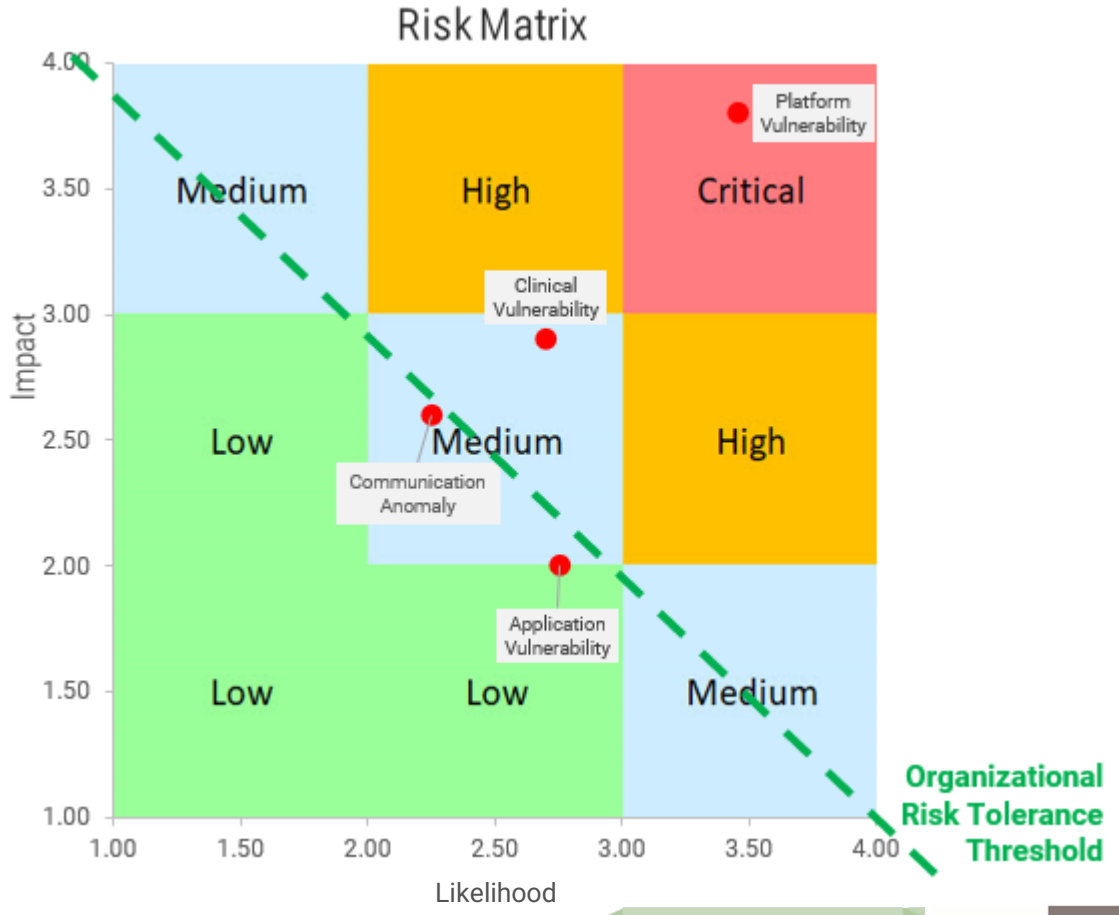


Risk Management Lifecycle

Assessing Risk

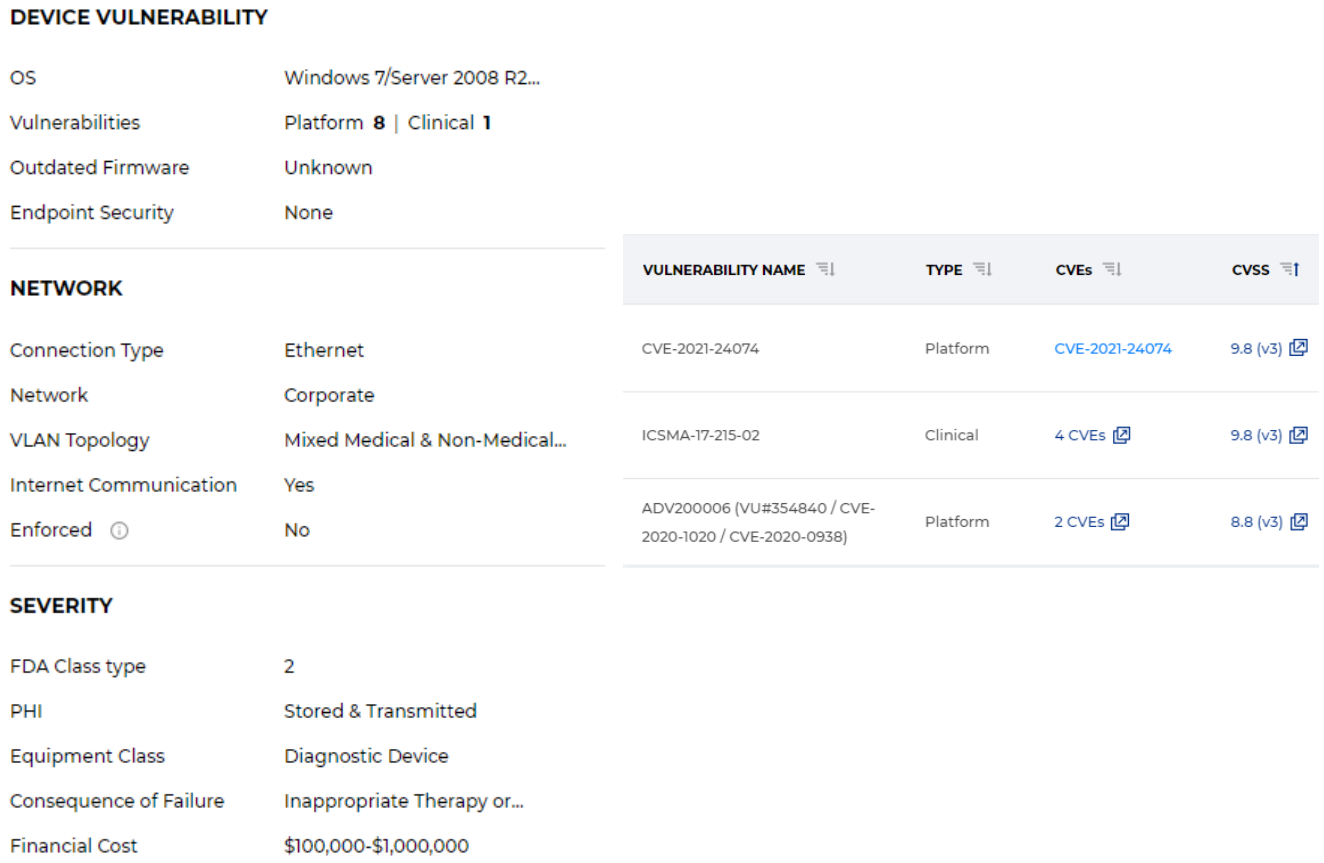
- A comprehensive risk assessment includes:
  - System Characterization
  - Threat Identification
  - Vulnerability Identification
  - Control Analysis
  - Likelihood Determination
  - Impact Analysis
  - Risk Determination
  - Control Recommendations
  - Results Documentation
- Define asset criticality and sensitivity
- Creation of a fully connected asset inventory

A risk matrix is useful in calculating a risk rating for vulnerabilities.



Contextualizing Risk

- Creating a risk profile:
  - Data (Impact)
  - Patient (Impact)
  - Business (Impact)
  - Active Vulnerabilities (likelihood)
  - Security Capabilities (likelihood)
  - Technical/Administrative / Physical controls (likelihood)
- Develop scoring metrics / Risk Ranking



DEVICE VULNERABILITY

OS	Windows 7/Server 2008 R2...
Vulnerabilities	Platform **8** | Clinical **1**
Outdated Firmware	Unknown
Endpoint Security	None

NETWORK

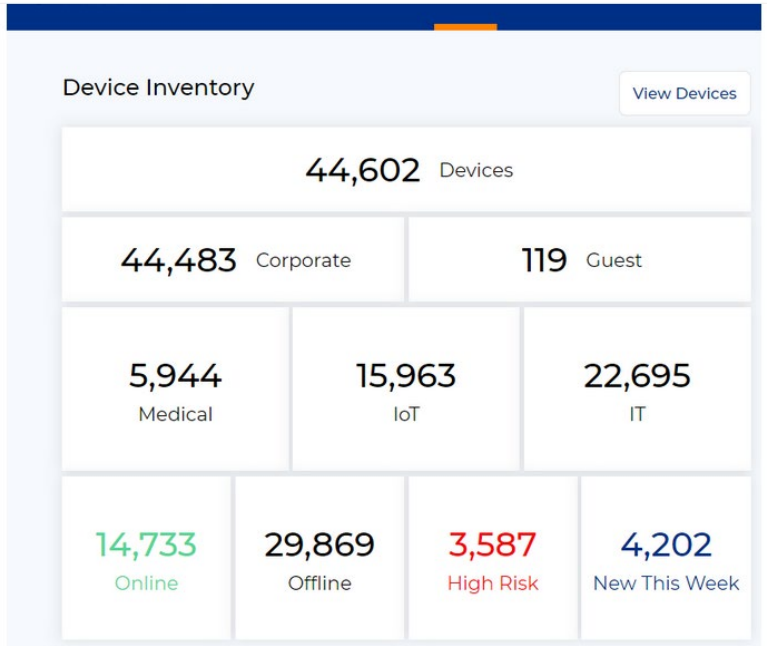
Connection Type	Ethernet
Network	Corporate
VLAN Topology	Mixed Medical & Non-Medical...
Internet Communication	Yes
Enforced	No

SEVERITY

FDA Class type	2
PHI	Stored & Transmitted
Equipment Class	Diagnostic Device
Consequence of Failure	Inappropriate Therapy or...
Financial Cost	$100,000-$1,000,000

VULNERABILITY NAME	TYPE	CVEs	CVSS
CVE-2021-24074	Platform	CVE-2021-24074	9.8 (v3)
ICSMA-17-215-02	Clinical	4 CVEs	9.8 (v3)
ADV200006 (VU#354840 / CVE-2020-1020 / CVE-2020-0938)	Platform	2 CVEs	8.8 (v3)

Assessing Risk - System Characterization - Threat ID

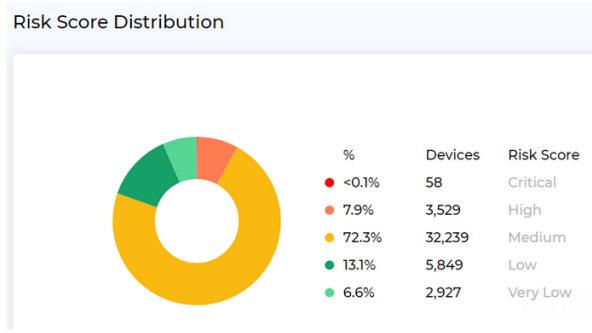


Medication Dispensing System	162
Clinical Video Camera	128
Mobile Printer	117
UPS	113
Imaging Workstation	103
Server	101
Blood Gas Analyzer	94
Time Clock	66
Patient Intake	66
Medical Device Integrator	59
Building Automation Device	59
Access Control	50
Defibrillator	43
Pharmacy Management	43
Smartwatch	40
Serial-to-Ethernet	40
EEG	40
Ultrasound	38
Room Monitor	35
Glucose Meter	34
ECG	34
Video Encoder	30
Video Conference	30
Telemedicine	30
Room Display	26
Imaging Device	24

2.3.1. Security / Vulnerabilities / Top 10 Clinical Vulnerabilities

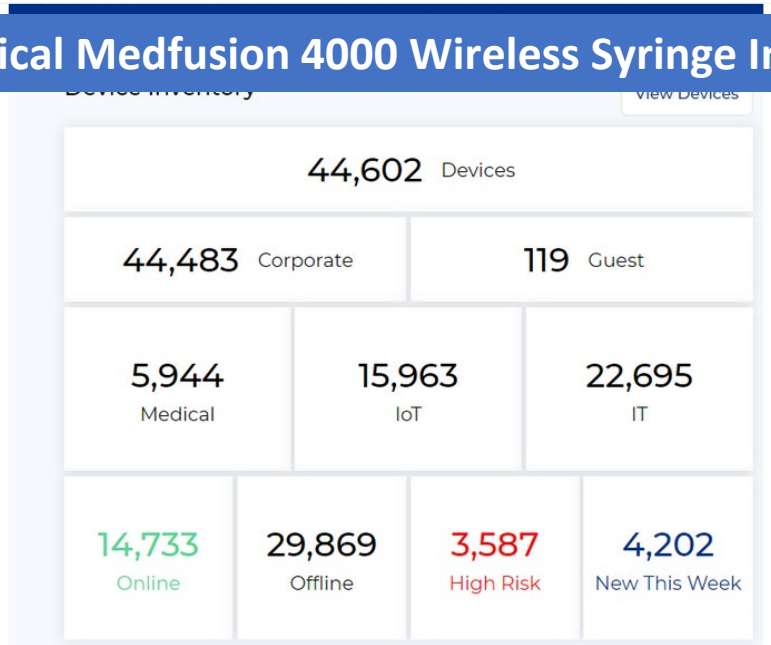
Vulnerability Name	Affected Models	Affected Devices
ICSMA-17-250-02A	1	799
ICSMA-20-317-01	2	577
ICSMA-17-017-02A	1	575
ICSMA-18-128-01	4	38
ICSMA-19-248-01	1	36
ICSMA-20-049-02	6	19
ICSMA-20-343-01	3	5
ICSMA-20-177-01	3	5
ICSMA-20-170-01	1	2
ICSMA-18-226-01	2	2

H / M / L Risk Score Distribution:

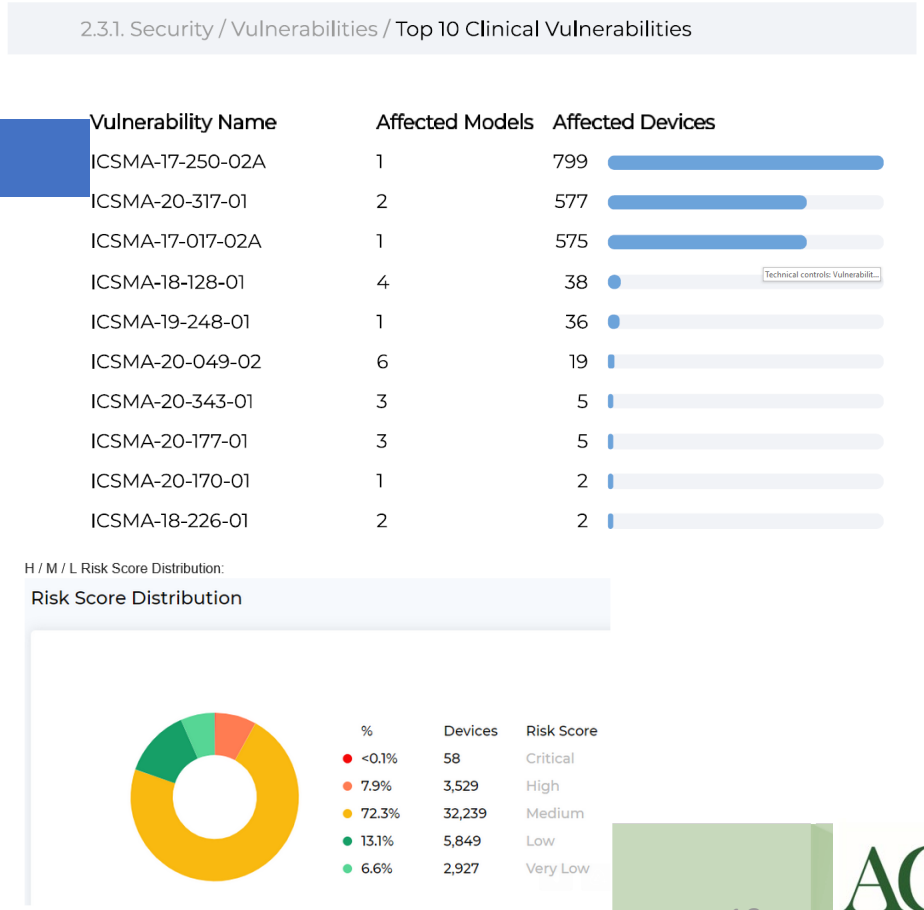


Assessing Risk - Vulnerability Identification

Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump >

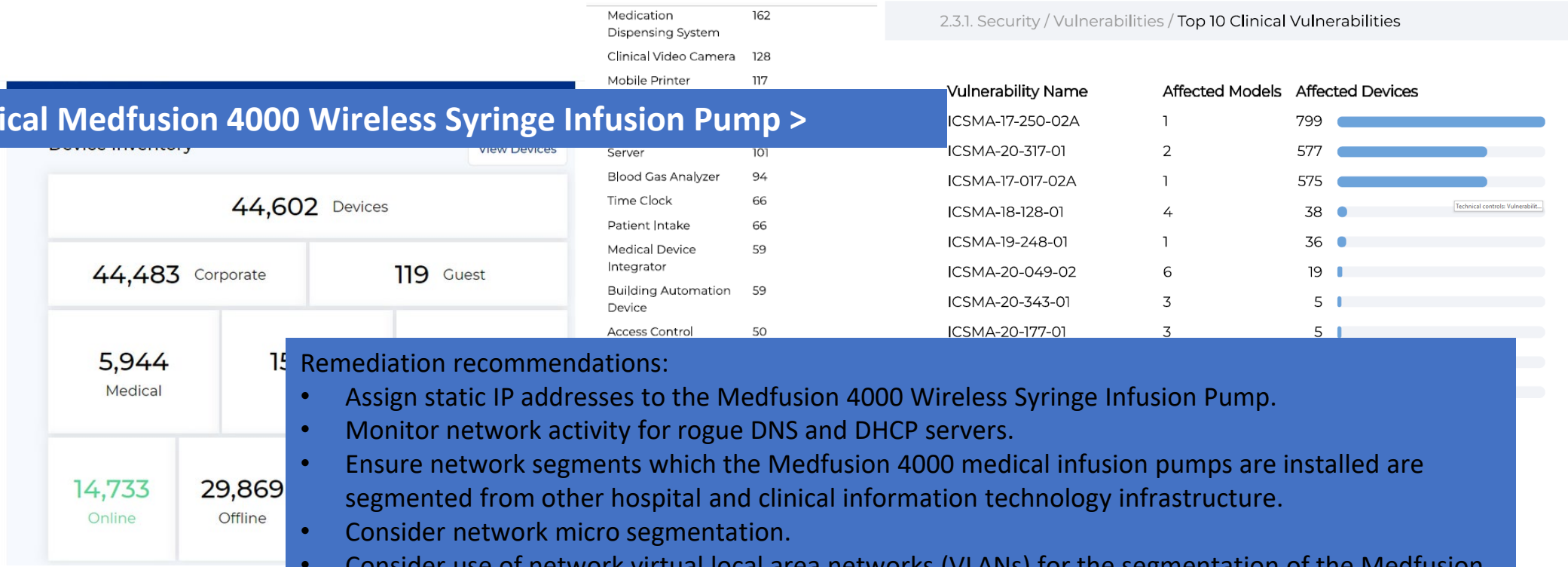


Medication Dispensing System	162
Clinical Video Camera	128
Mobile Printer	117
Server	101
Blood Gas Analyzer	94
Time Clock	66
Patient Intake	66
Medical Device Integrator	59
Building Automation Device	59
Access Control	50
Defibrillator	43
Pharmacy Management	43
Smartwatch	40
Serial-to-Ethernet	40
EEG	40
Ultrasound	38
Room Monitor	35
Glucose Meter	34
ECG	34
Video Encoder	30
Video Conference	30
Telemedicine	30
Room Display	26
Imaging Device	24



Assessing Risk - Control Analysis

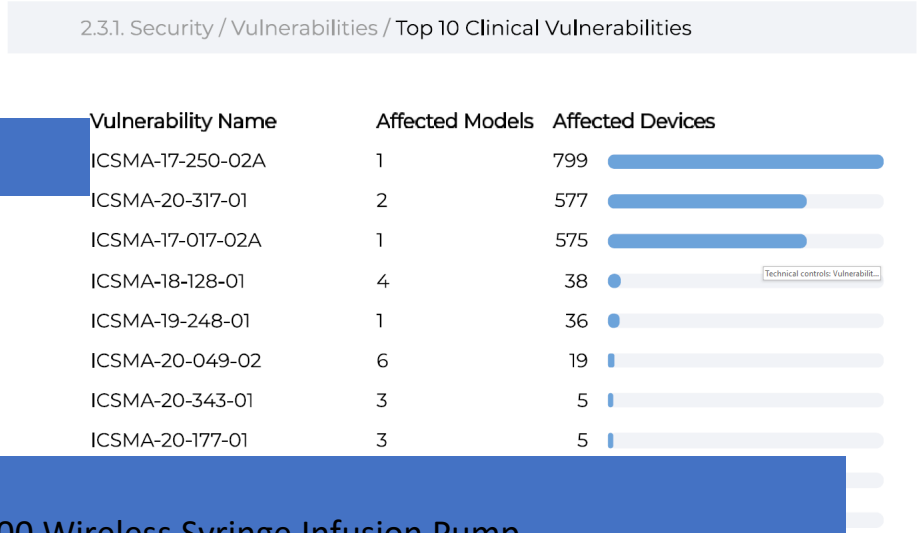
Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump >

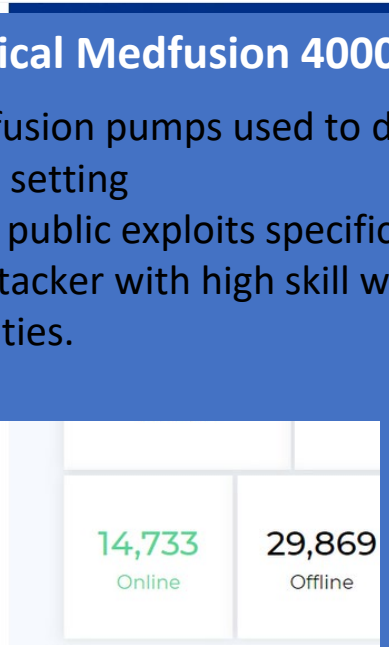


Remediation recommendations:

- Assign static IP addresses to the Medfusion 4000 Wireless Syringe Infusion Pump.
- Monitor network activity for rogue DNS and DHCP servers.
- Ensure network segments which the Medfusion 4000 medical infusion pumps are installed are segmented from other hospital and clinical information technology infrastructure.
- Consider network micro segmentation.
- Consider use of network virtual local area networks (VLANs) for the segmentation of the Medfusion 4000 medical infusion pumps.
- Apply proper password hygiene standards across systems (i.e., use uppercase, lowercase, special characters, and a minimum character length of eight).
- Do not re-use passwords.

Assessing Risk - Likelihood Determination





Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump >

- Syringe infusion pumps used to deliver small doses of medication in acute care setting
- No known public exploits specifically target these vulnerabilities
- Only an attacker with high skill would be able to exploit these vulnerabilities.

Remediation recommendations:

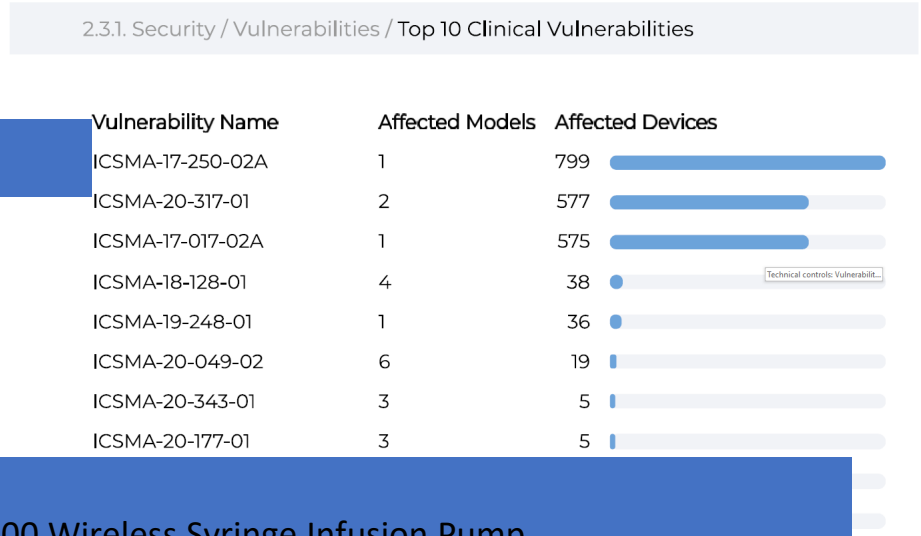
- Assign static IP addresses to the Medfusion 4000 Wireless Syringe Infusion Pump.
- Monitor network activity for rogue DNS and DHCP servers.
- Ensure network segments which the Medfusion 4000 medical infusion pumps are installed are segmented from other hospital and clinical information technology infrastructure.
- Consider network micro segmentation.
- Consider use of network virtual local area networks (VLANs) for the segmentation of the Medfusion 4000 medical infusion pumps.
- Apply proper password hygiene standards across systems (i.e., use uppercase, lowercase, special characters, and a minimum character length of eight).
- Do not re-use passwords.

Assessing Risk - Risk Determination

Risk Level	Total Score (Impact + Likelihood)	Category Description
Low	0-7	Medical devices with no active technical vulnerabilities, a low impact on patient care, little to no ePHI storage or transmission, and little to no organizational impact if disabled. Likely an acceptable risk level without additional review.
Moderate	8-13	Medical devices with no active technical vulnerabilities but may have non-technical vulnerabilities and few or no technical security controls currently implemented. These devices have a lower impact on patient care, data, and the overall business operations of the organization.
High	14-18	Medical devices that likely have at least one active technical vulnerability requiring remediation activities or extremely robust compensating controls to be implemented - causing a very high likelihood of threat occurrence. These devices usually have non-technical vulnerabilities, do not have any technical security controls currently implemented, will impact care delivery if affected, and store and/or transmit large amounts of ePHI. It is not suggested to proceed at this risk level.
Critical	19-21	Medical devices with more than one active technical vulnerability requiring specific remediation activities to mitigate, such as, security updates or system upgrades which causes a very high likelihood of threat occurrence. These devices also directly impact patient care and pose a risk to patient safety if affected, store and/or transmit large amounts of ePHI, and have a high level of asset utilization causing a higher level of impact to the organization if disabled.

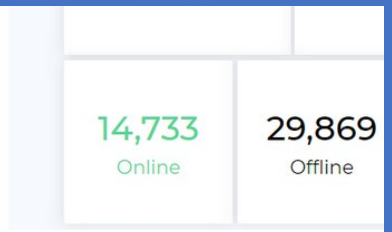
ACCE
AMERICAN COLLEGE OF CLINICAL ENGINEERING

Assessing Risk - Control Recommendation



Smiths Medical Medfusion 4000 Wireless Syringe Infusion Pump >

- Syringe infusion pumps used to deliver small doses of medication in acute care setting
- No known public exploits specifically target these vulnerabilities
- Only an attacker with high skill would be able to exploit these vulnerabilities.



Remediation recommendations:

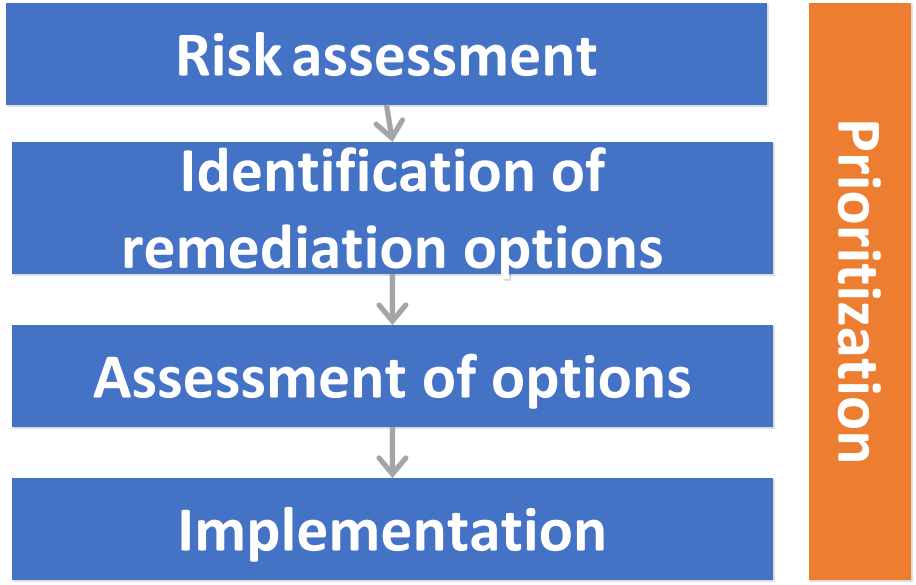
- Assign static IP addresses to the Medfusion 4000 Wireless Syringe Infusion Pump.
- Monitor network activity for rogue DNS and DHCP servers.
- Ensure network segments which the Medfusion 4000 medical infusion pumps are installed are segmented from other hospital and clinical information technology infrastructure.
- Consider network micro segmentation.
- Consider use of network virtual local area networks (VLANs) for the segmentation of the Medfusion 4000 medical infusion pumps.
- **Apply proper password hygiene standards across systems (i.e., use uppercase, lowercase, special characters, and a minimum character length of eight).**
- **Do not re-use passwords.**

Prioritizing Remediation Response

- Triage vulnerabilities, filter out the noise
- Evaluate vulnerabilties for urgency (verified exploit, CVSS base of 7+, lateral movement)
- Determine business criticality
- Use patient safety factors to help determine urgency
- Review current security posture
  - What does your network look like? (Flat, ACL's, VLANS,)
  - Defense-in-depth controls

Prioritize Remediation Based on Risk

- Identify remediation options
  - Patch or update
  - Configuration change
  - Compensating controls
  - Accept the risk
- Assess the options and identify how to implement
  - Task force
  - Operationally (PM's & CM's)
- Implement or select another option



Remediation Response Effectiveness

- Based on a Risk Management Strategy
  - List of controls
  - Risk appetite
- Create a risk register / risk treatment plan
- Input assessment and response activities into CMMS as work orders
- Properly code and track work orders and progress
  - Establish a baseline
- Heavily consider IoMT passive scanning solution and CMMS integration

HTM/CE Risk Treatment Plan Summary: July 1st, 2021				
Rank	**HTM Risk Treatment Plan Description**	**%**	**Estimated Completion Date**	**Notes**
10	Address CVE-2020-1350 – Patch	50%	*8/14/2021*	48 Devices initially affected, Current: 24
7	Non-medical device in medical device VLANS	28%	*6/1/2022*	Risk Management Program Related
6	Medical devices communicating externally with unsecure protocols	85%	*8/1/2021*	Risk Management Program Related
7	Address medical device inventory deficiencies	94%	*8/1/2021*	Initial: 462, Current: 97
3	Change of default passwords on infusion pumps	100%	12/1/2020	Complete
2	Determine enterprise and IoMT risk appetite	100%	1/1/2021	Complete
3	Medical device security strategy, and executive engagement and ownership	100%	3/1/2021	Complete
4	Address medical device alert workflows	100%	3/1/2021	Complete
4	Ad hoc threat intelligence and profiling	100%	4/1/2021	Complete
3	Instances of unmanaged privileged access	100%	4/1/2021	Complete
5	Limited protective technologies deployment	100%	5/1/2021	Complete
3	Med devices at clinics not centrally managed.	100%	6/1/2021	Complete

Metrics, KPI's, and CSF's

- Without metrics, you lack the visibility to manage or improve your processes.
- KPIs are the specific metrics that help you track performance. KPIs tell the story of "how are we doing?"
- CSFs are the specific KPIs that track the activities that are necessary to accomplish for the organization to be successful.

Business Goal	Critical Success Factor	Key Performance Indicator	Metric to track
Minimize overall risk exposure	Reduction of overall risk due to vulnerabilities	Decrease in the number of vulnerabilities	The number of vulnerabilities year after year.
Appropriate allocation of resources	Proper prioritization of mitigation activities	Decrease of critical and high vulnerabilities	The number of critical and high vulnerabilities.
Consistent & measurable remediation of threats to the organization	Minimize risk when vulnerabilities are detected	Remediate vulnerabilities more quickly	The average time between the identification to remediation.

Questions

Thank You

Please complete the online evaluation at

https://www.surveymonkey.com/r/ACCE_07-22-21

Or scan the QR code: