

Clinical Cyber Hygiene

The recent spike in connected devices, rising healthcare cybersecurity threats, and new vulnerabilities discovered weekly gives a hospital's CISO many reasons to be concerned. The CISO is well aware of the security weaknesses of medical and IoT devices, but the security team is fairly small and barely has the capacity to handle all the alerts generated by their security software and put out occasional fires. The CISO would much rather work systematically and have a clear overview of clinical network risks but the team lacks the data, method and actionable insights to support such a process.

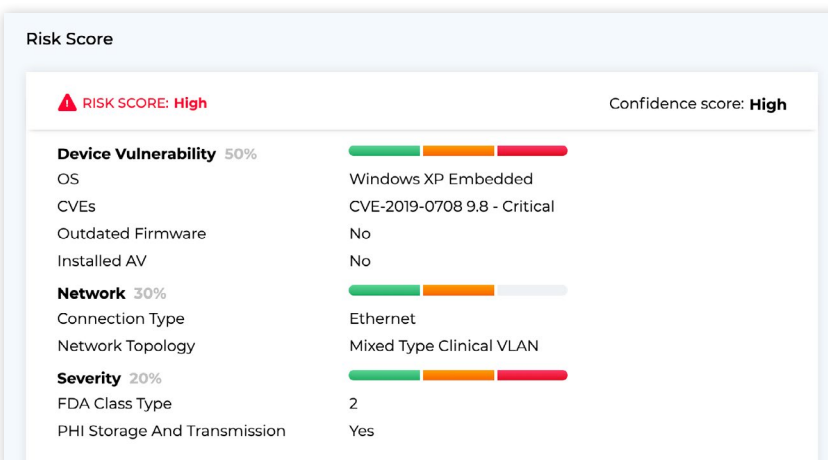
- 1. Data - The connected devices are poorly identified.** The hospital's security solution cannot identify the configuration of IoT and medical devices, such as their manufacturer, model, operating system, serial number, and hardware and app versions. Some devices are completely unidentified beyond IP and MAC addresses, while others may be classified as medical but their technical specifications, location, or responsible person or department remain unknown. With such limited information, it is difficult for the CISO and his team to assess the risk posed by a device and drive action.
- 2. Method - There is no existing, widely-accepted model for assessing medical device risk.** Their limited visibility and the risks involved in actively scanning medical devices for vulnerabilities make it hard to determine the risk posed by each device. And even if they had all data on their devices, there is no standard method to aggregate, weigh, and prioritize the unique factors affecting the probability (such as OS, app updates, CVEs) and severity (such as processing PHI) of compromising a given device.
- 3. Action - Current remediation and mitigation actions are sporadic and likely miss more critical points.** Absent of a coherent risk assessment and prioritization, the team cannot form a comprehensive plan to remediate, mitigate and contain identified risk within the organization and in collaboration with manufacturers. They end up working mostly ad-hoc and often failing to address risks posed by medical and IoT devices.

Introducing Medigate's security platform to the network gives the CISO and his team the data, method and actionable insights required to manage risk on their clinical network. It starts with granular visibility of all connected devices and comprehensive risk score calculations for each device, which are then aggregated into reports illuminating the distribution of risk both internally across departments and externally among device manufacturers.


- We fingerprint all medical devices in the network.** Medigate uses Deep Packet Inspection (DPI) on passively-collected network traffic to discover 100% of devices in the clinical network and obtain granular identifications for each device including manufacturer, model, OS, hardware and app versions and location. Our DPI techniques are based on a deep understanding of the communication protocols and workflows of medical devices, and our discovery facilitates a comprehensive assessment of the device's risk.

| | IP | MAC | MANUFACTURER | TYPE | MODEL | OS | VLAN | LAST SEEN | STATUS | RISK SCORE |
|--|---------------------|-------------------|--------------|------------------------------|------------------------|---------------------------|------|--------------------|---------|------------|
| | 10.140.26.75 | 74:FE:48:3A:2E:AA | BD | Medication Dispensing System | Pyxis Medstation 4000 | Windows 7 | 103 | 8/4/2019 9:59 AM | Offline | High |
| | 10.140.26.76 | 74:FE:48:3F:04:0B | BD | Medication Dispensing System | Pyxis Medstation 4000 | Windows 7 | 103 | 8/28/2019 6:17 AM | Offline | High |
| | 10.140.26.77 | A4:4E:31:96:FA:2F | STRONA | Anesthesia Cart | DeviceConX Fanless PC | Windows 10/Server 2016... | 103 | 8/28/2019 11:05 AM | Online | Medium |
| | 10.140.26.77 / 2203 | A4:4E:31:96:FA:2F | | Anesthesia Monitor | Datex-Ohmeda S5 | Datalight ROM-DOS | 103 | 8/28/2019 11:33 AM | Online | Low |
| | 10.140.26.77 / 2204 | A4:4E:31:96:FA:2F | | Anesthesia Machine | Datex-Ohmeda Aisys CS2 | Nucleus | 103 | 8/19/2019 9:09 AM | Offline | Low |
| | 10.140.26.78 | 10:62:E5:27:62:1F | STRONA | Anesthesia Cart | DeviceConX Fanless PC | Windows 10/Server 2016... | 103 | 8/28/2019 11:41 AM | Online | Medium |
| | 10.140.26.78 / 802 | 10:62:E5:27:62:1F | | Anesthesia Monitor | Datex-Ohmeda S5 | Datalight ROM-DOS | 103 | 8/28/2019 5:34 AM | Offline | Low |

- We give each device a multifactorial risk score.** The score incorporates the probability of a compromise and its severity for each device, based on AAMI's Risk Management Technical Information Report along with risk assessment processes and standards prescribed by the FDA, ECRI, ISO and NIST. Fusing these standards with our cybersecurity expertise and clinical domain knowledge, we have developed a simple yet comprehensive procedure considering inherent device properties, network connectivity, CVEs, among other factors to assign a level of risk for each device that is fully reflected to the user. We also integrate with vulnerability management platforms to import precise CVE information based on each device's technical attributes.



Medical Device Information



iE33

Philips




#ID: HHARKLU

Add a Description

No MDS* Forms Available

| | |
|---------------------------------------|--------------------------------|
| IP 10.106.12.136 | MAC 00:D0:C9:6F:9C:EA |
| MANUFACTURER Philips | TYPE Ultrasound |
| MODEL iE33 | OS Windows XP Embedded |
| APP VERSION 6.3.7.745 | SERIAL NUMBER 343725509 |
| AE TITLE USPH005410 | PROTOCOLS DICOM |
| VLAN 102 | VLAN NAME Radiology Network |
| VLAN DESCRIPTION Radiology Network | CONNECTION TYPE Ethernet |

Integrations

| Product | System | Status | Active Since | Info. |
|--|--------------------------|----------|--------------|-------|
|  IoT Controller | Firewall | Inactive | N/A | N/A |
|  ISE | NAC | Inactive | N/A | N/A |
|  InsightVM | Vulnerability Management | Inactive | N/A | N/A |

Risk Score

RISK SCORE: High

Confidence score: High

Device Vulnerability 50%

OS

CVEs

Outdated Firmware

Installed AV

Network 30%

Connection Type

Network Topology

Severity 20%

FDA Class Type

PHI Storage And Transmission

Windows XP Embedded

CVE-2019-0708 9.8 - Critical

No

No

Ethernet

Mixed Type Clinical VLAN

2

Yes

3. We aggregate the individual risk scores into insightful, actionable reports. Medigate provides customizable reports that clearly outline the distribution of risk both internally (across departments) and externally (by device manufacturer). The Medigate platform also integrates with vulnerability management platforms and feeds its detailed identification into their scanning and reporting procedures.


MEDIGATE

01/13

TOP HIGH RISK MEDICAL DEVICES

Medical device information **2 out of 37** detected high risk medical devices

#1



iE33

Philips

RISK SCORE: High

| | | | |
|-------------------------------|----------------------------------|--------------------------------|---------------------------|
| IP 10.128.75.47 | MAC 00:0b:28:05:80:8b | MANUFACTURER Philips | TYPE Ultrasound |
| MODEL iE33 | FIRST SEEN 12/20/2018 9:06 PM | LAST SEEN 1/7/2019 10:52 PM | |
| OS Windows XP Embedded SP3 | CLASS TYPE 2 | CONNECTION Direct | ACCESS METHOD Wireless |
| CVE CVE-2017-0716 | SEVERITY High | No high risk alert | |

| | HOSPITAL NAME | LOCATION | TOTAL MEDICAL DEVICES | HIGH RISK MEDICAL DEVICES | TOTAL IOT DEVICES |
|----------|---------------------|----------------|-----------------------|---------------------------|-------------------|
| MEDIGATE | Belmont Hospital | Livingston, NY | 1377 | 136 | 2429 |
| MEDIGATE | Nantucket Hospital | Nassau, NY | 2447 | 229 | 2460 |
| MEDIGATE | Somerville Hospital | Ontario, NY | 485 | 55 | 2412 |
| MEDIGATE | Newton Hospital | Queens, NY | 3193 | 303 | 2471 |

Medigate's data and insights immediately enhance the CISO's toolbox. The team now understands which devices pose risks and who is responsible for them. It also methodically initiates remediate and mitigate prioritize risks as well as adds a new security perspective to connected devices procurement.

- 1. Control risk across the enterprise.** With Medigate the CISO sees all existing devices in the clinical network, their location, and the person or department in charge of their maintenance. The granular per-device risk scores aggregated into customizable summaries helps identifying departments, manufacturers, and device types that pose high risk.
- 2. Drive security improvements.** The risk assessment drives remediation processes in collaboration with manufacturers for prioritized devices. Medigate also tailors suggested mitigation activities such as device-based network segmentation and policy enforcement via an existing NAC or firewall which are automatically implemented via Medigate's integrations with leading vendors.
- 3. Affect medical and IoT device procurement.** Knowing which devices pose greater risk, the CISO can now introduce a security criterion to the procurement procedure and ensure that safer de-vices are being bought and connected to the clinical network.

The CISO and his team no longer face a clinical network with limited visibility, secured by a general-purpose solution, lacking a systematic way to assess and manage the risk posed by connected devices. With Medigate, they can discover all connected devices, assign them a comprehensive risk score, and generate risk assessment reports and actionable remediation and mitigation insights. All in one place.