

# Cynerio Securing Hospital Medical OT Devices from Hackers and Attackers!

Date: September 2024

**Nakarin Jirakul**  
Chief of Security  
BangkokMSP







# The Results of Current Efforts

## CHANGE HEALTHCARE

- \$22M Ransom Paid
- Cascading Cost: Up to \$100M / Day / Provider
- Real Initial Costs: \$872M
- Records Exposed: ~120M (Equivalent to all 2023)

## APAC

- Australia: 22% of all data breaches are in healthcare
- Singapore: Healthcare IT Providers routinely block 3,000 malicious emails daily per location
- Singapore: Healthcare IT Providers experiences 1.7 million attempted breaches monthly per location
- Global: Average Breach Cost is \$11MM
- Global: Healthcare accounts for 70% of successful ransomware attacks annually

	\$63M
	\$102M
	\$113M
	\$150M
	\$600M
	CLOSED

**7.1 min**

**Healthcare Cyber  
Attack Frequency**

**1 in 3**

**Records Exposed  
(US)**

**35%**

**Increased Mortality  
Rates During Attack**



# What is the motivation?



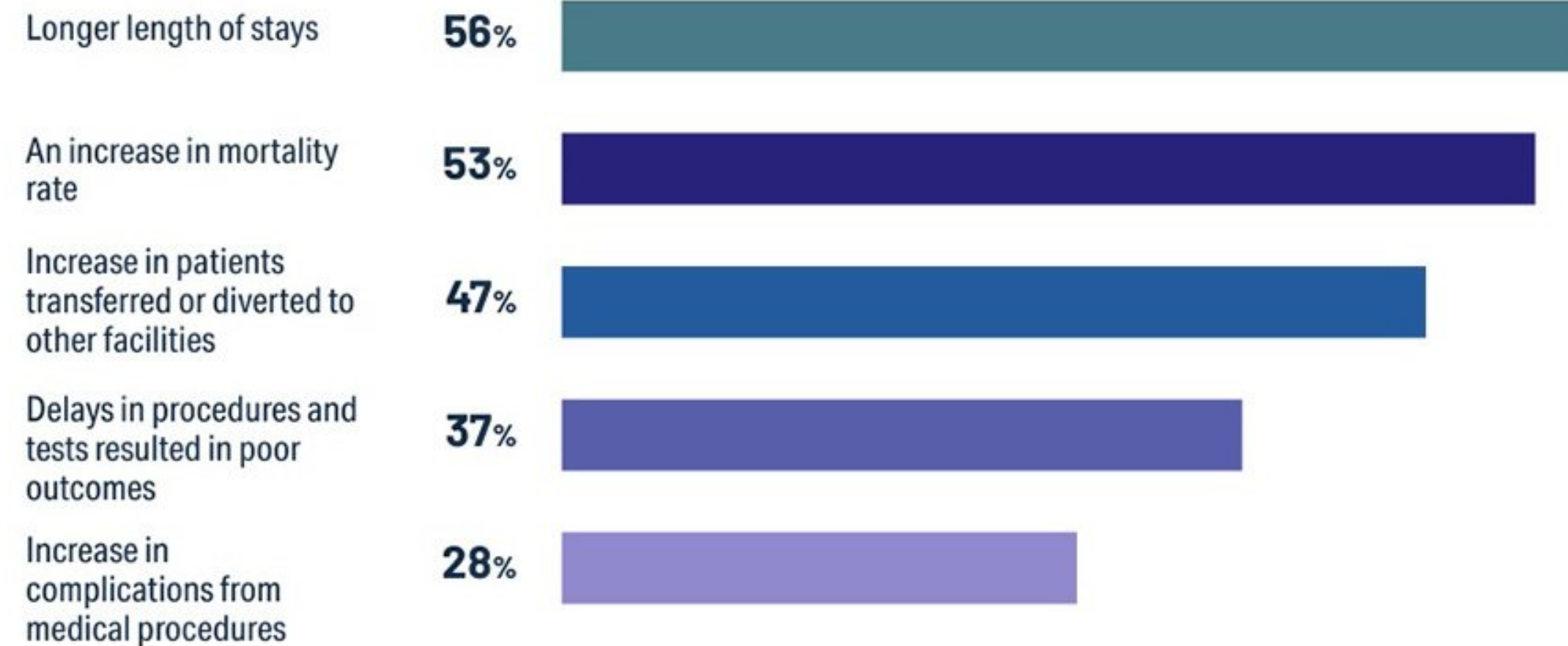
- Record Value
  - SSN: \$1
  - Credit Card: \$5
  - ePHI: \$50 - \$250
- Ransom Payments
  - 2023: \$100M
  - Change: \$22M Alone
  - 47% Pay Ransom
- Triple Extortion





# People may died

## Adverse impact of a cyberattack on patient care



### Emergency Services

- Loss of communication with other hospitals
- Diversion of ambulances

### Outpatient Services

- Delay or cancellation of elective surgeries

### Patient Portal

- Inability to view records, test results, or upcoming appointments

### Radiology

- Inability to requisition scans or imaging

### Laboratory

- Closure of COVID-19 testing sites
- Delay of processing and communicating test results

### Electronic Health Records

- Inaccessible patient record systems
- Staff required to manually record patient progress and treatment

[techtarget.com/searchsecurity/feature/Studies-show-ransomware-has-already-caused-patient-deaths](https://techtarget.com/searchsecurity/feature/Studies-show-ransomware-has-already-caused-patient-deaths)

# How they can attack us?

โรงพยาบาลถูกโจมตีได้  
อย่างไร?

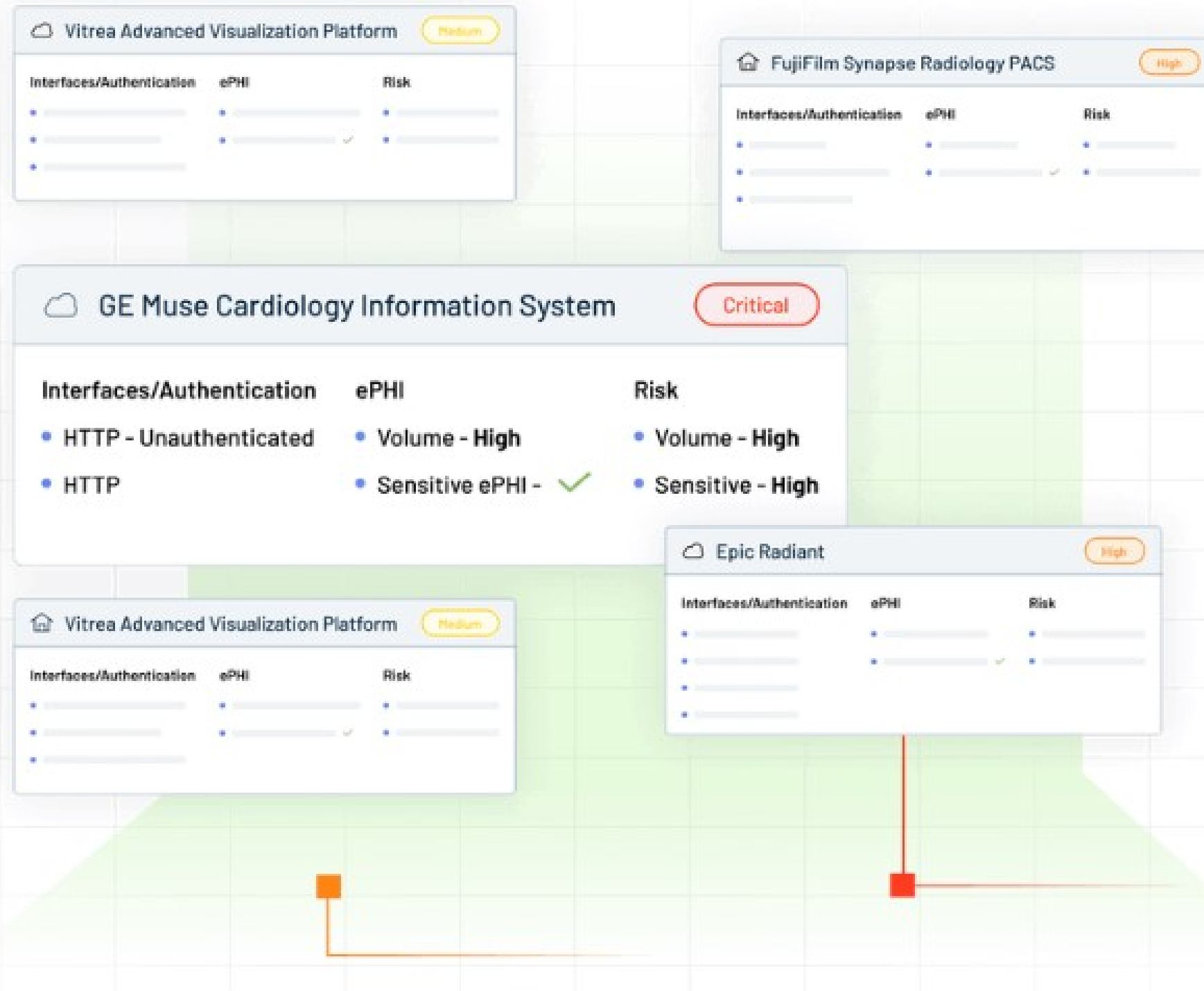
# RISK of Being Attacked



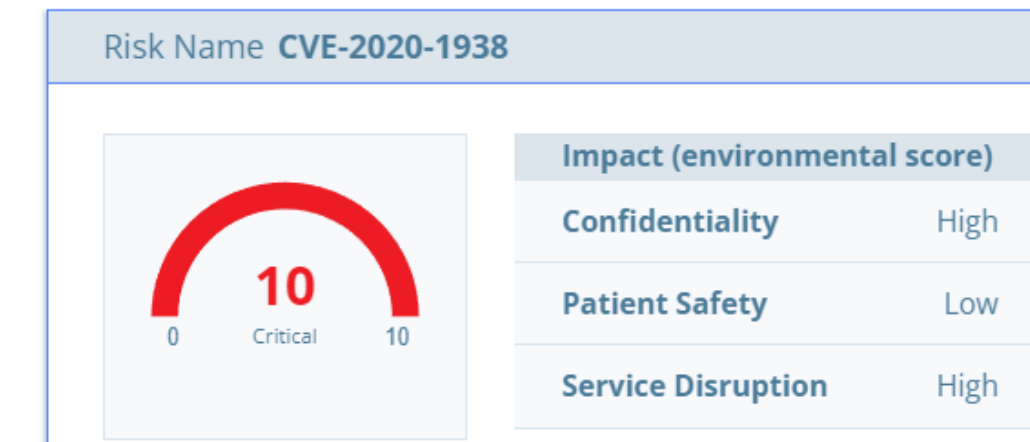
# How can Cynerio and BMSP Solve?

BMSP และ Cynerio จะช่วยแก้ไขปัญหาคือ  
อย่างไร?

# Cyber Hygiene(Legacy Device Issue)



ค้นหาช่องโหว่ของอุปกรณ์



บอกระดับความเสี่ยงและความอันตรายถึงชีวิต

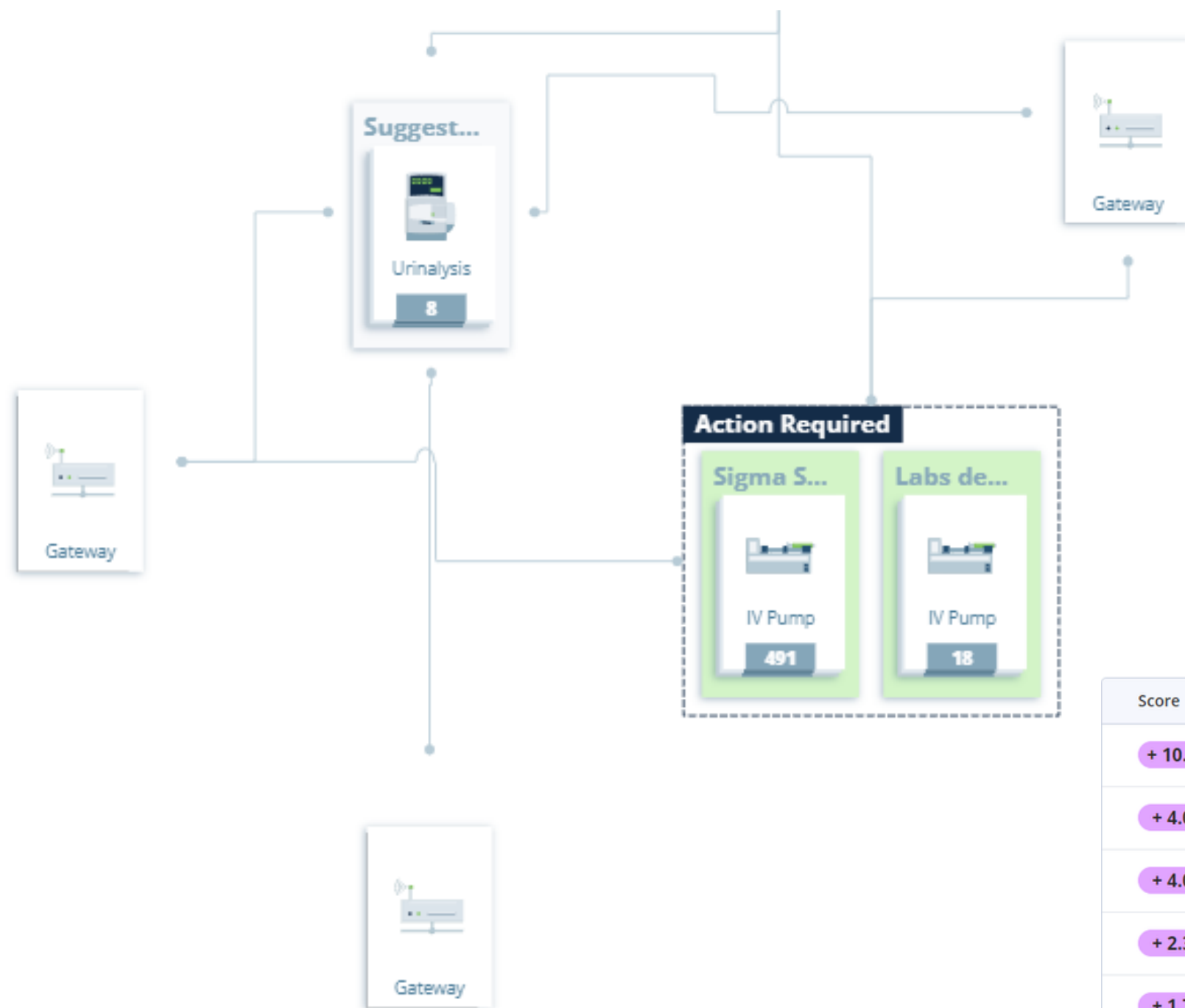
## ePHI Types

- ✓ Patient Name
- ✓ Patient ID
- ✓ Phone Number
- Geographic data
- FAX numbers
- ✓ Social security number
- ✓ Email addresses
- Medical record numbers
- Account numbers
- Health plan beneficiary numbers
- Certificate/license numbers
- Vehicle identifiers
- Web URLs
- Device identifiers
- IP addresses
- Facial photos
- Biometric identifiers
- Unique identifying numbers or code

บอกลักษณะข้อมูลส่วนบุคคลที่ใช้งานในระบบ



แนะนำว่าแต่ละอุปกรณ์มีการคุยกับภายนอกอย่างไรบ้าง



## Types

**Building Automat...**  
Trane  
18

## Services

Endpoint Protection ESET

Windows Update

OS Services Windows

Improve Your Score to 70 by Taking These Actions:

Current Score  
**48.2** → Potential Score  
**70**

Score	Mitigation Action	Device Type
+ 10.2	Apply East-West Segmentation	IV Pump
+ 4.0	Apply East-West Segmentation	IV Pump
+ 4.0	Apply North-South Segmentation	IV Pump
+ 2.3	Apply East-West Segmentation	Patient Monitor
+ 1.7	Apply Service Hardening	IV Pump



Cannot Communicate with Hacker

ระบุการสื่อสารระหว่าง อุปกรณ์

ให้คำแนะนำจะเพิ่ม Security ให้ดีขึ้นอย่างไร



## Risk Threat Intelligence



**Weaponization Difficulty**  
Easy



**Exploit Code Maturity**  
Functional Exploit Exists



**Exploited in the Wild**  
True



**Lateral Movement**  
True

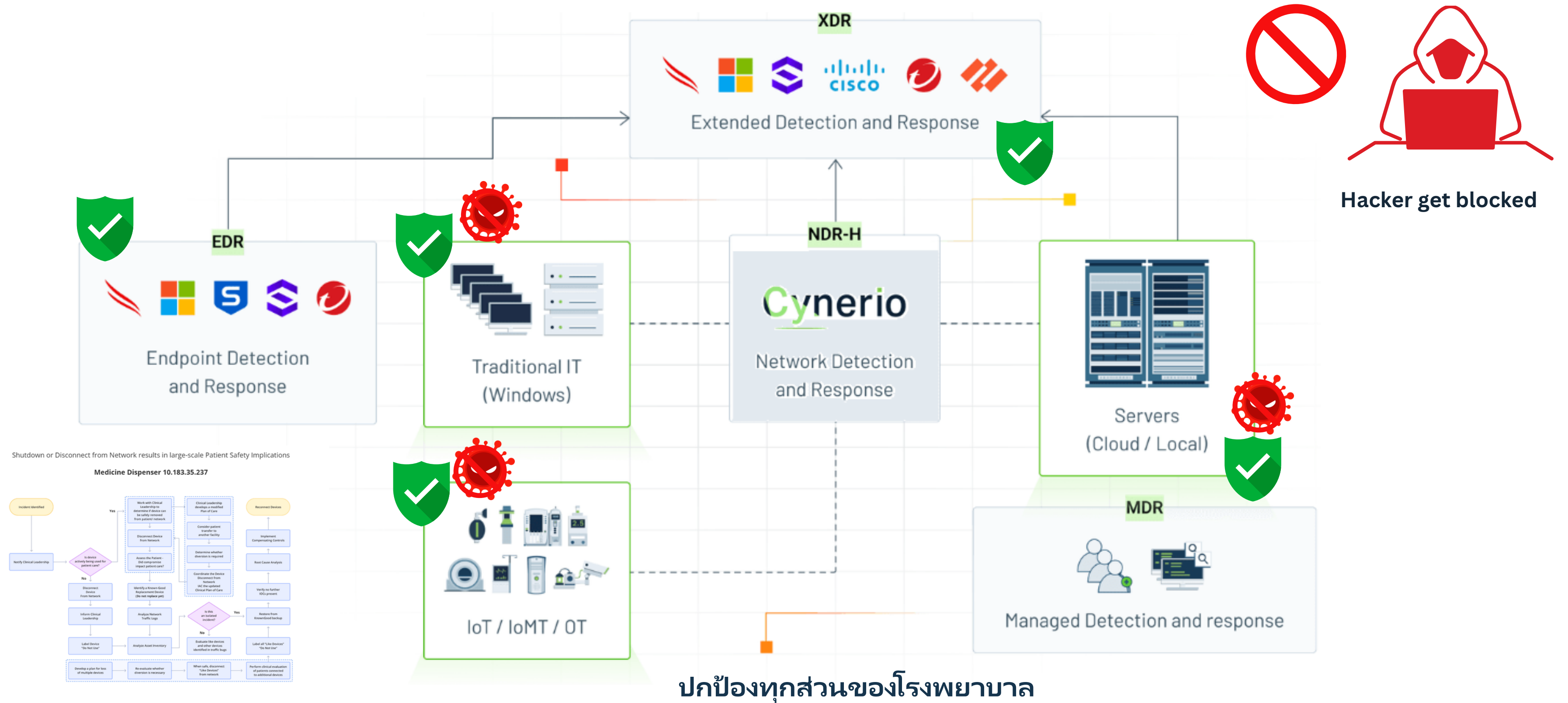


**Exploit Kits & Malware**  
Forged-PAC  
Ryuk  
Conti  
Epsilon Red  
Cuba  
[Exploit kit 1](#)


ระบบการโจมตีที่อาจจะเกิดขึ้นได้แต่ละอุปกรณ์



## Full Visibilities and Protection



**Malware - Lateral Movement**

 **QakBot Malware Spreads on Network**

C-


Reviewed by  
Cynerio Live

New

...

### Attack Description

On 2024-04-10 at 13:52 UTC, a Windows computer DESKTOP-SX3EYDP was infected with Qakbot (Qbot) malware. The Qakbot infection may have spread to another computer on the network DESKTOP-AM7UTX. The infected machine DESKTOP-SX3EYDP was also observed connecting to multiple SMTP servers, which is indicative of spambot activity.  
[Click for more info](#)

 **SOS Action**

1. Isolation - Disconnect the affected systems from the network immediately.
2. Check if other devices were affected, and try to estimate the size of the attack.
3. Identify suspicious Programs or processes running on the affected devices, and remove them. Consider using a suitable scanning software for this process.
4. Policy - Block all traffic from the malicious domain the file was pulled from (if known).

Quarantine


### Cynerio Live - Analyst Note


A CynerioLive analyst validated the detections and assessed that the machine DESKTOP-SX3EYDP is indeed infected with Qakbot, AKA Qbot. The indicators observed are consistent with Qakbot, including TLS certificates, and the external SMTP connections that indicate spam-sending activity. We have yet to see indications that DESKTOP-AM7UTX is also infected, but it is usually preferable to err on the side of caution so it should be treated as such.

### Attack Schema

First Seen - 04/10/2024 12:52:34

Last Seen - 04/11/2024 08:05:14

 7 External Addresses

 2 Targets

Hospital ABC

Attack Detection & Response Monitoring Matrix

Security Events Last 24h		Monitored Assets	
Exploitation Attempt	2	Last 24h	Total
Connection to Suspicious Domain	17	Medical	5,103 5,478
Default / Weak Password	43	IoT	735 953
Internet Browsing	52	Monitored Connections	
Scanner Activity	12	Last 24h	Total
Telnet Connection	2	Internal	6,707 150,131
RDP Connection	6	External Inbound	0 3,309
SSH Connection	1	External Outbound	19,672 944,179

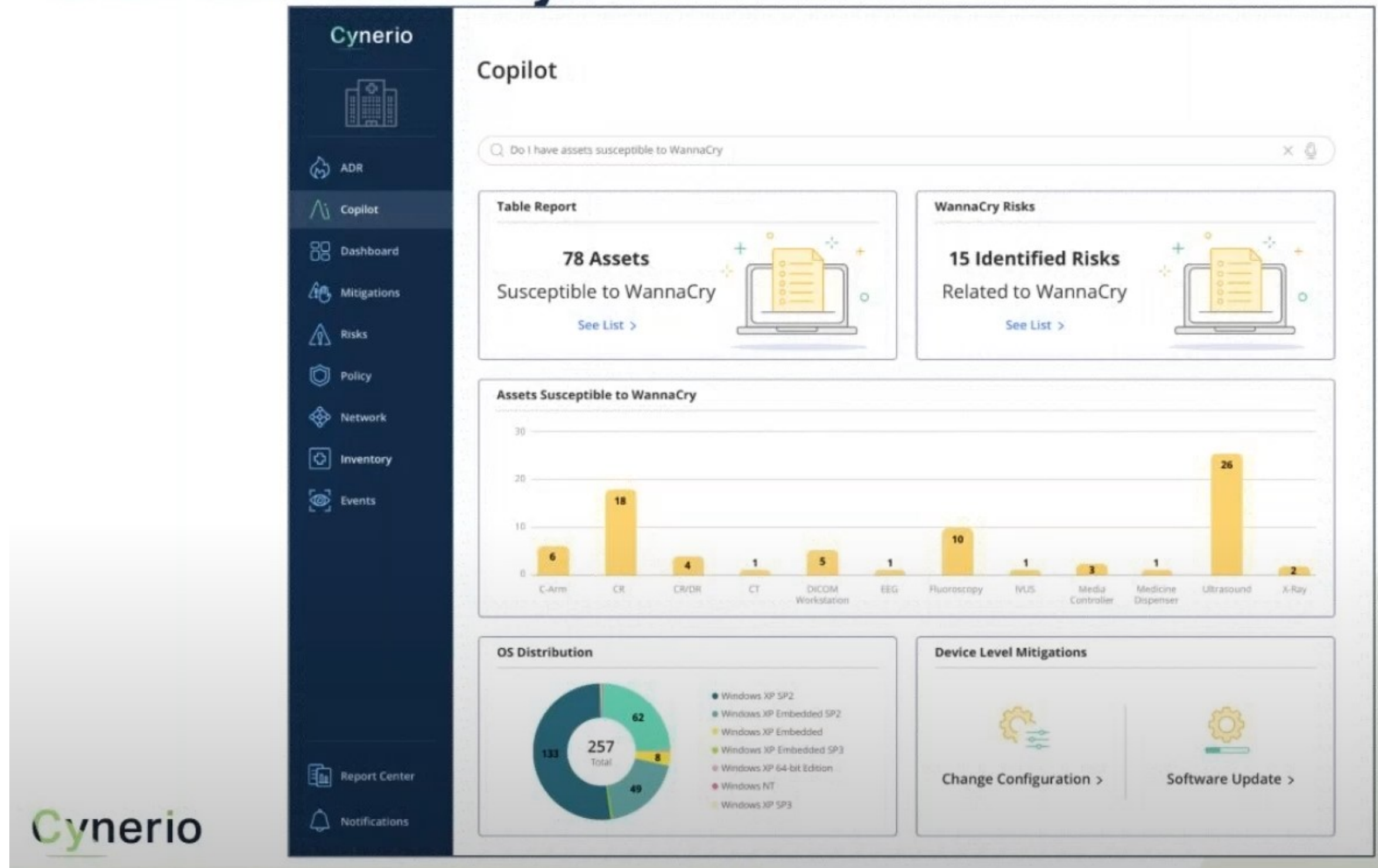
สรุปการโจมตีต่างๆที่เกิดขึ้นในช่วง 24 ชั่วโมง

ตรวจสอบการโจมตีในระบบและป้องกันอัตโนมัติ

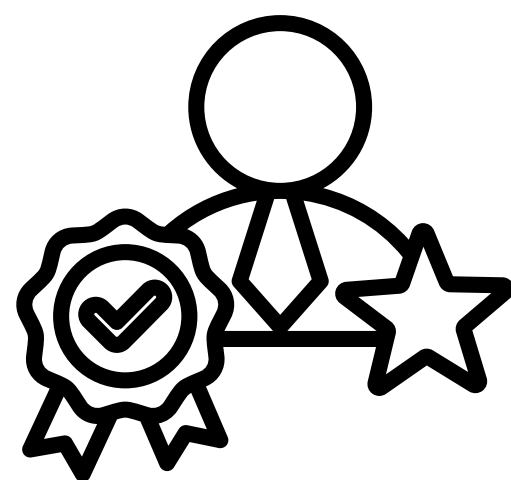
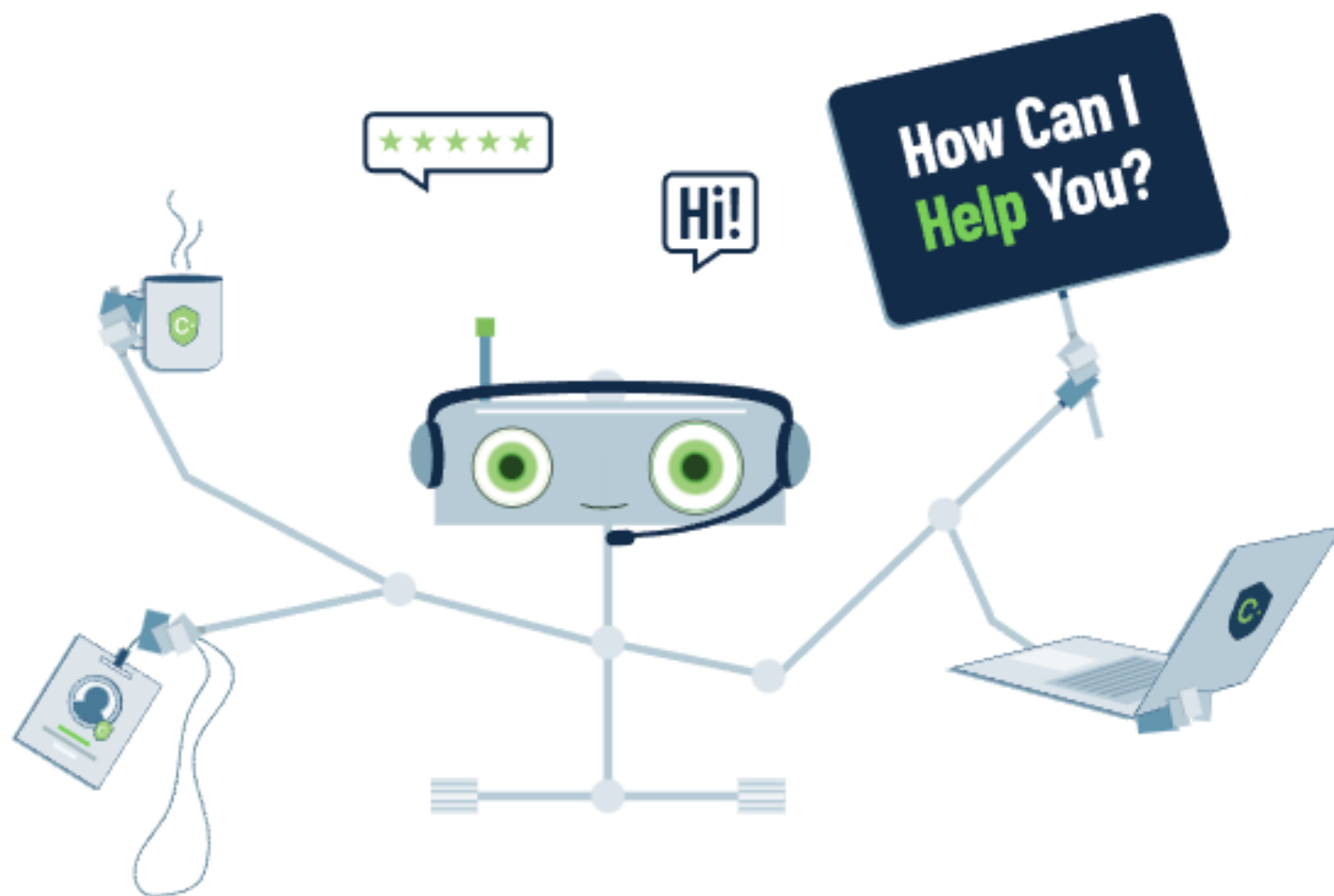


## GenAI: Advanced Analysis

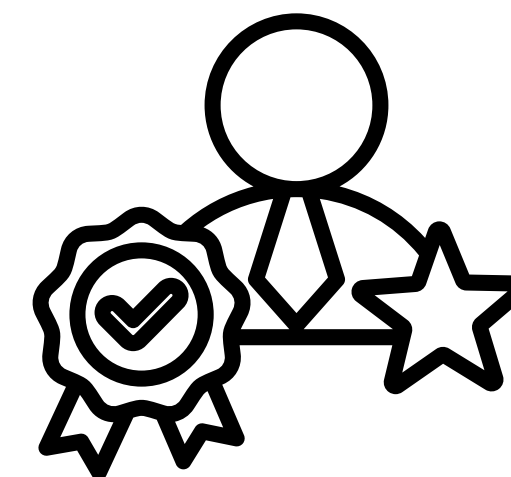
มี AI คอย Suggest และคอยสรุปโอกาสที่จะเกิดการโจมตี



มีผู้เชี่ยวชาญทั้งทางด้าน IT/OT ในการ support ลูกค้า



**Cynerio Medical Device Expert(TAM)**

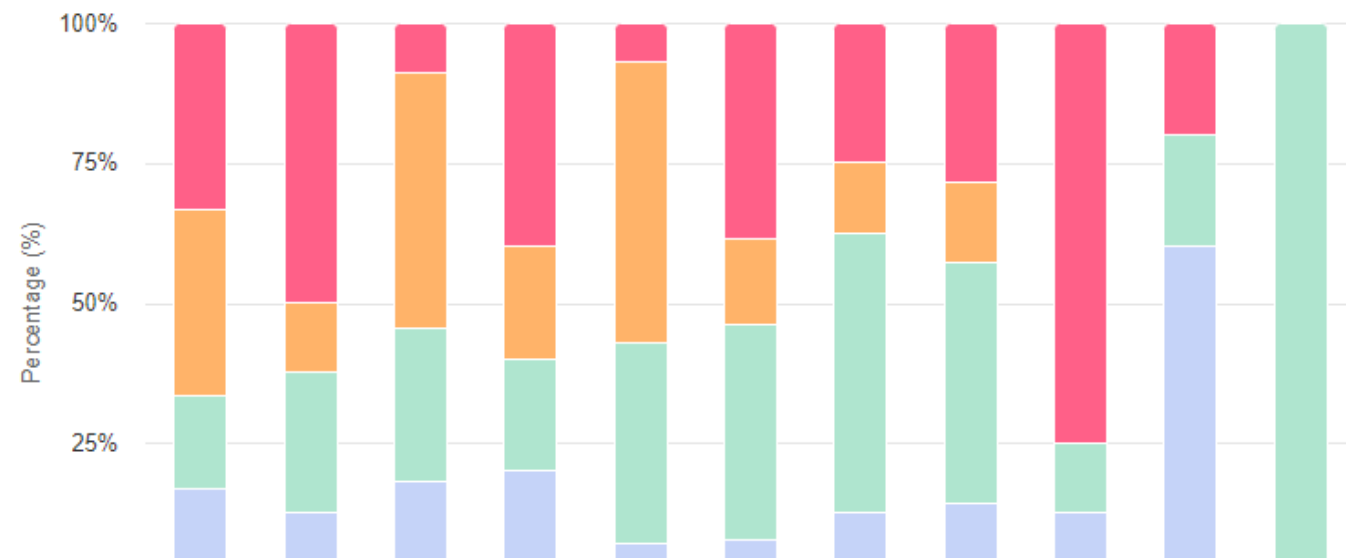


**BMSP MIoT Expert SOC 24x7**

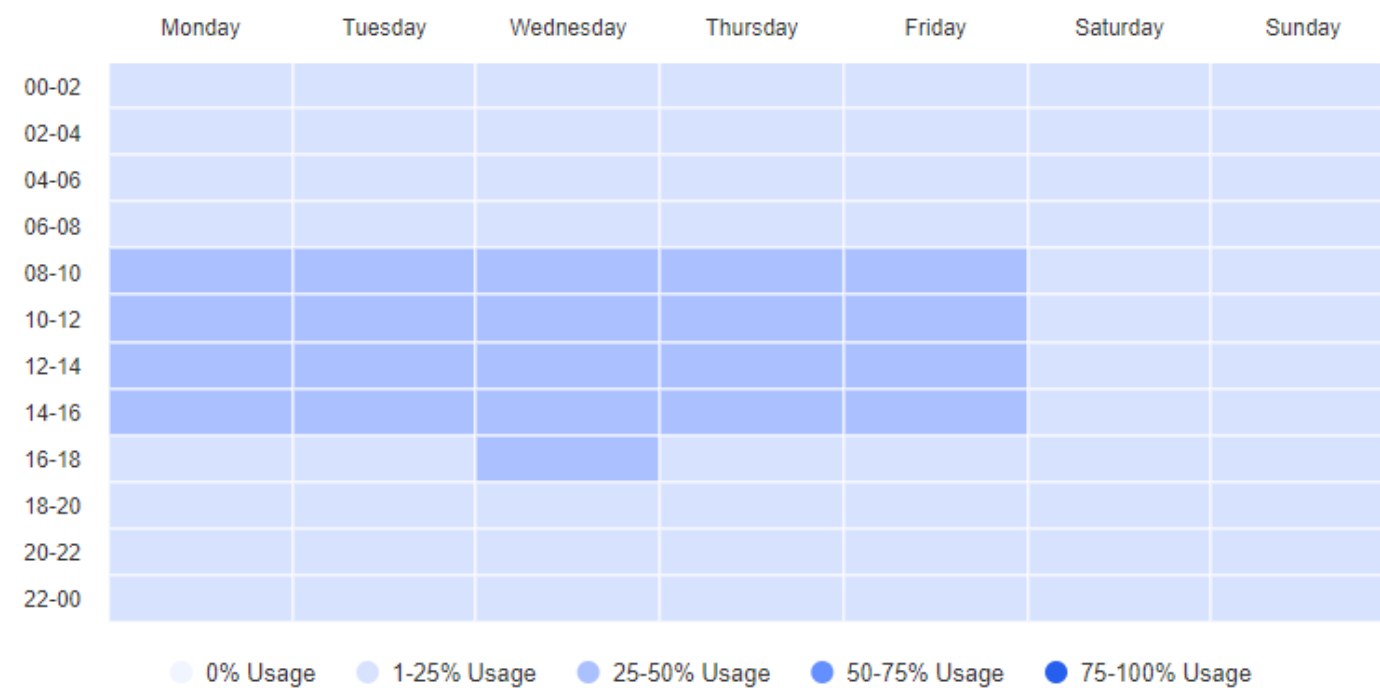


# Utilization Improvement

Site View

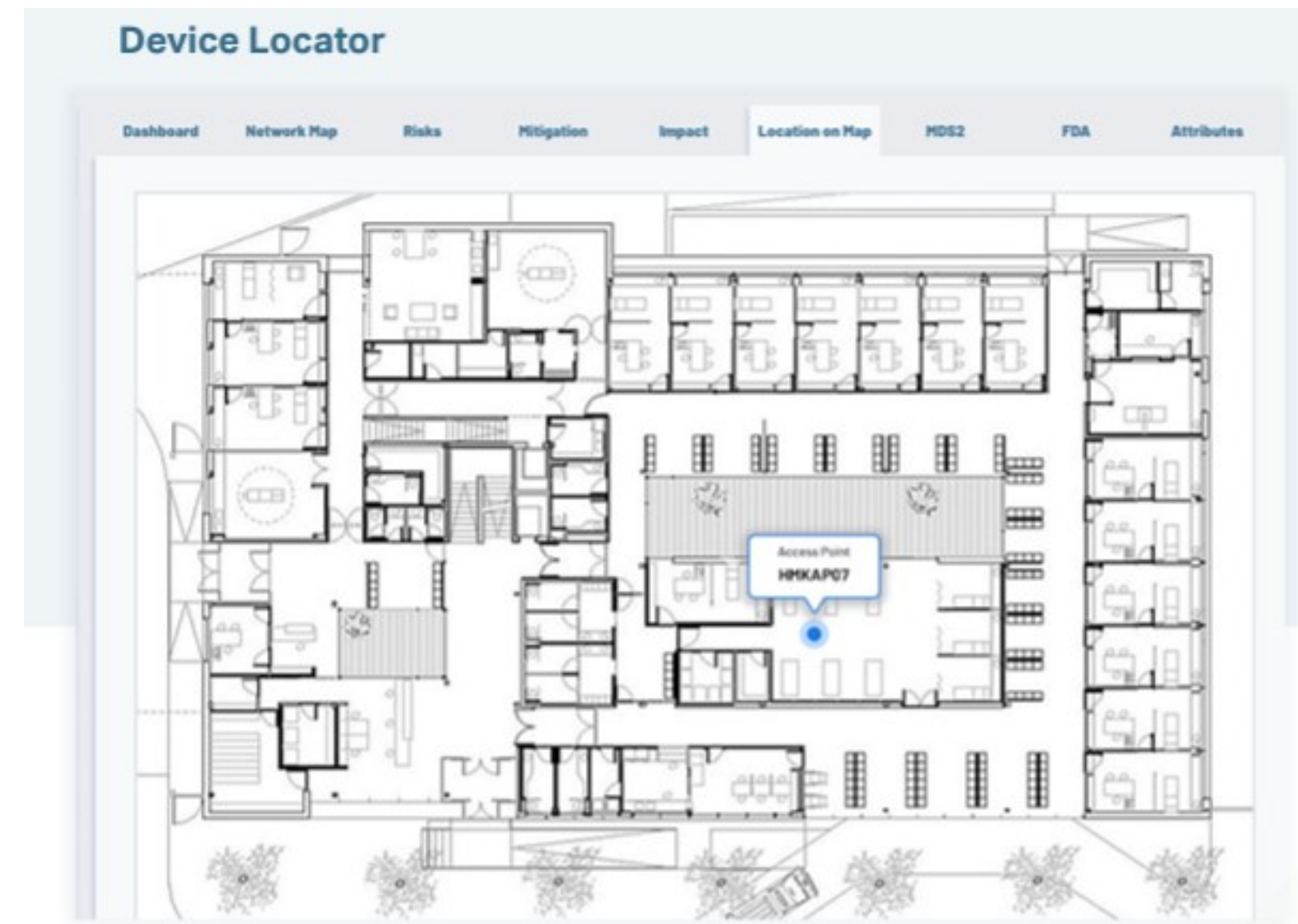


Week / Hour Usage Average



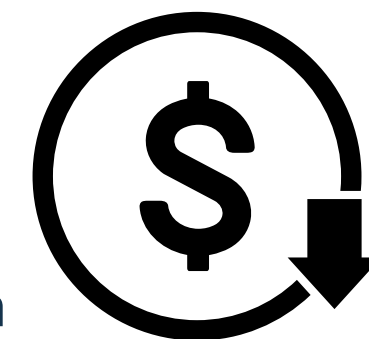
บอกปริมาณการใช้งานของอุปกรณ์

บอกตำแหน่งของอุปกรณ์



Reduce Cost

ใช้อุปกรณ์ทางการแพทย์ให้คุ้มค่าที่สุด



# Use cases





## Type of NHS Trust

Integrated acute, community, mental health and ambulance Trust

## The Challenge

The Trust lacked endpoint and server compliance and had very limited visibility and reporting of devices. It then discovered a striking gap between managed and unmanaged assets – ‘a black hole’ representing almost a third of the physical hosts on the Trust’s network.

## The Solution

The ITHealth Dashboard proves itself 'an essential tool for compliance reporting, hardware and software inventory and DSPT'. Cynerio efficiently delivers a complete, accurate inventory of all medical devices and IoT and helps effectively address associated vulnerabilities.



**Location:** Greenbrae,  
California, USA

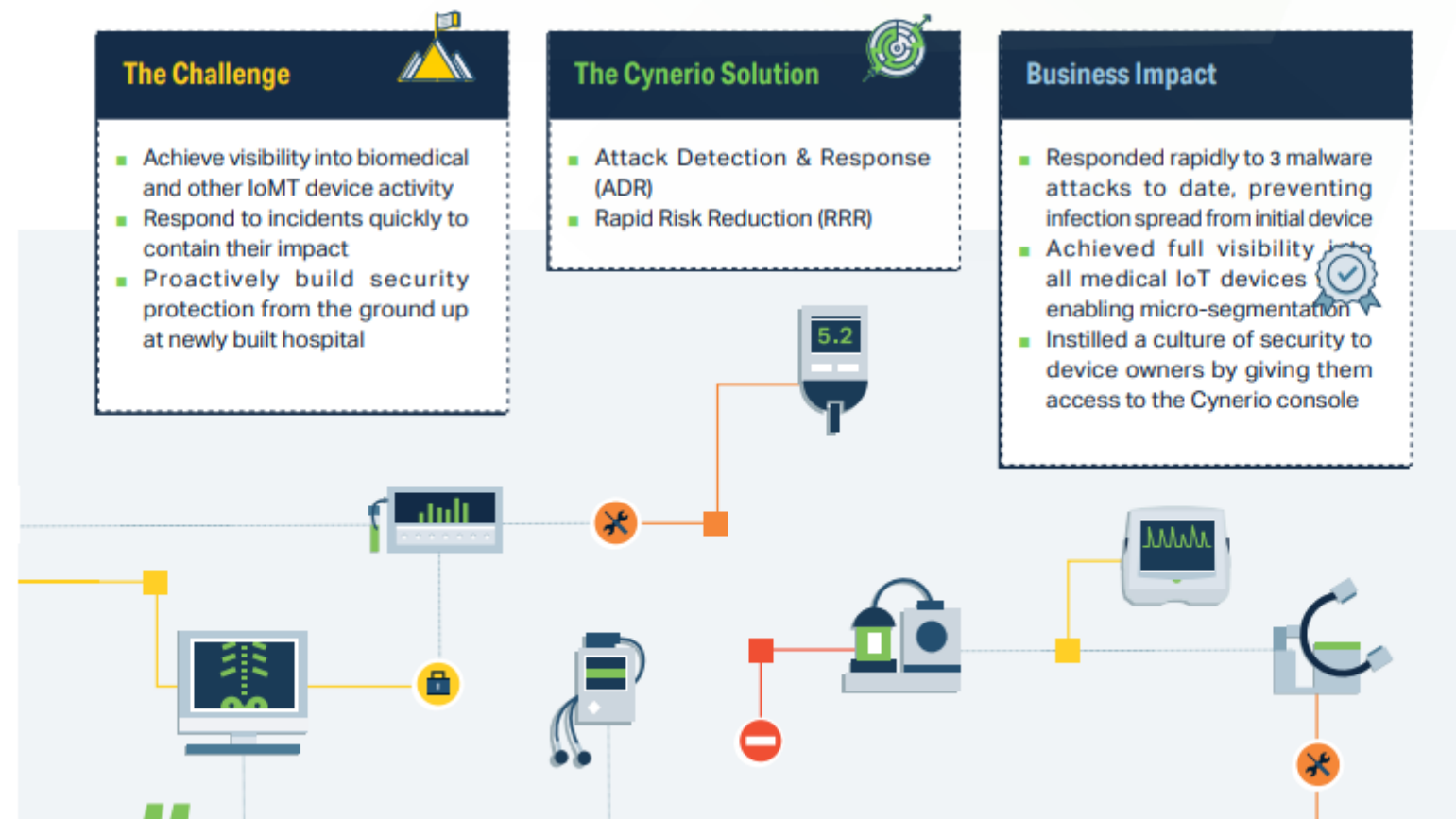
**Founded:** 1952 as Marin General Hospital

**Bed Count:** 327

**Notable:** The only full-service, acute care hospital in a county of 250,000+

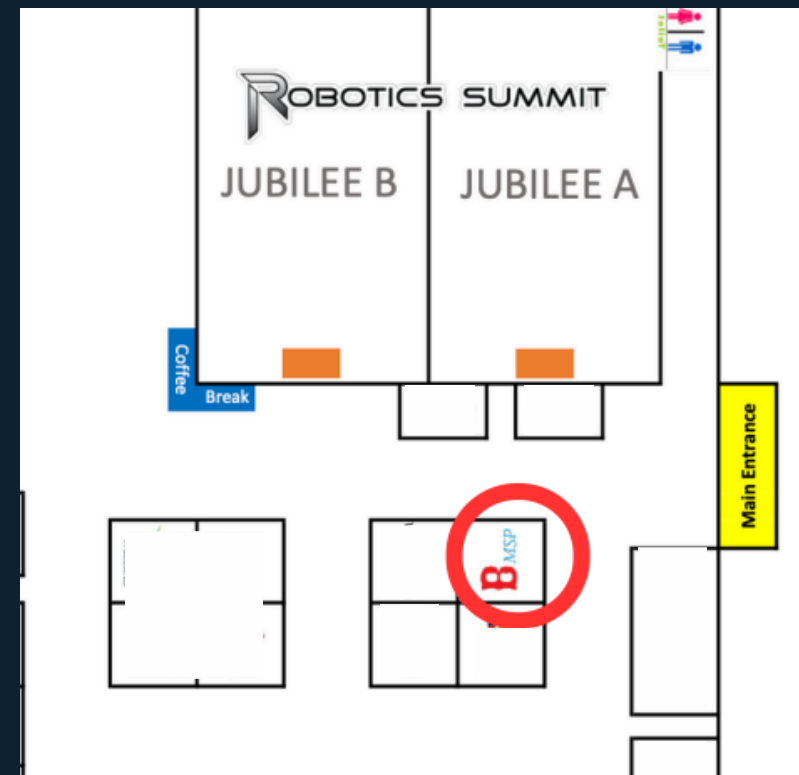
*We knew that in order to secure the devices, we needed to segment the network. And to effectively segment the network, we had to be able to see what was happening."*

– Scott Christensen, Security and Systems Engineer, MarinHealth Medical Center





Please visit our Booth  
(Near Main Entrance)



Thank You!