



## IoT Cyber Security: Foundational Security for IoT

**Lyndon Brown**

Chief Strategy Officer

Pondurance

1



PONDURANCE

## Addressing Your IoT Security with MDR

---

Lyndon Brown  
Chief Strategy Officer



2



Today's Speaker

Lyndon Brown

Chief Strategy Officer

©2021 Pondurance Inc. All rights reserved.



3



**63% of healthcare security managers** have experienced one or more security incidents related to unmanaged and IoT devices.

- Healthcare IT Security

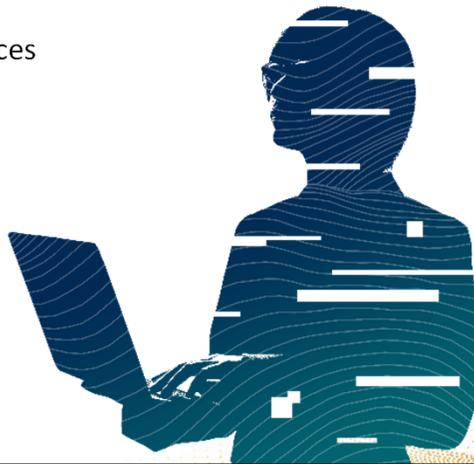


4

# IoT Was Not Designed With Security in Mind

Cyber adversaries view hospital IoT devices as low-hanging fruit:

- Weak passwords
- Unprotected network services
- Overall lack of hardening



5

# Questions to Ask When Looking at Securing IoT Devices

- Where does IoT exist in your health care systems?
- Who owns security of IoT at your health care organization?
- What is the relationship between IT and IoT protection?
- Are you implementing detection and response best practices?
- Do you need to bring in a partner?



6

# Different Service Offerings

What is the difference between SIEM, MSSP, and MDR?



**SIEM**



**MSSP**



**MDR**



7

7

# Customer Pain Points



Shortage of  
cybersecurity talent



Security professionals that are  
expensive to hire and hard to retain



Security technology is expensive  
and hard to maintain



Difficulty managing multiple tools  
and investigating all alerts



Technology alone can't deter motivated  
attackers



New compliance and  
regulation requirements



Undocumented processes in event  
of an attack or breach



Lack of visibility  
across the enterprise



Inability to quickly remediate or reduce  
attacker dwell time

©2021 Pondurance Inc. All rights reserved.



8

8

## Poll Question: What is your top pain point as it relates to protecting IOT and IT devices?

- Shortage of cybersecurity talent
- Security professionals that are expensive to hire and hard to retain
- Security technology is expensive and hard to maintain
- Difficulty managing multiple tools and investigating all alerts
- Technology alone can't deter motivated attackers
- New compliance and regulation requirements
- Undocumented processes in event of an attack or breach
- Lack of visibility across the enterprise
- Inability to quickly remediate or reduce attacker dwell time



9

9

## Components of MDR



PEOPLE	PROCESS	TECH
24/7	Technology Management	Detection and Response Platform
Expert Human Intelligence	Detection	Log Analysis
Security Analysts	Response	Network Analysis
Threat Hunters	Threat Intelligence	Endpoint Detection and Response
Incident Responders	Vulnerability Management	Forensics

©2021 Pondurance Inc. All rights reserved.



10

10

# Evaluating MDR Vendors

-  Technology Stack
-  Fits With Your Policies
-  Monitor On-Premises and Cloud Assets
-  Custom Reports Including Compliance
-  Real-Time Alerts Backed by Human Intelligence
-  Incident Response and Remediation
-  Experience with Your Industry

©2021 Pondurance Inc. All rights reserved.



11

11

# Advanced Managed Detection and Response Platform



## 360 DEGREE VISIBILITY

Fully managed best-in-class Extended Detection and Response (XDR) across:

- **Network** Traffic Analysis (NTA) sensors
- **Endpoint** Detection and Response (EDR)
- **Logs** via SIEM as a Service platform
- **Cloud** Infrastructure, including AWS, GCP, Azure

## PURPOSE-BUILT PLATFORM

- Integrates with your existing security investments
- Provides dynamic detection powered by real-time threat intelligence, AI and smart tuning
- Tailored to your security policies
- Ability to provide high-fidelity monitoring on most critical assets

## 24X7 EXPERTISE & ADVISORY

- US-based Security Operations Centers (SOCs)
- Closed-loop incident response
- Proactive threat hunting
- Managed investigations
- Actionable recommendations and strategic insights



12

12



## Dedicated Experience in Health Fields

- Health care and insurance providers.
- Behavioral health.
- Research facilities, labs, and diagnostics.
- Health-related retail and e-commerce.
- Medical manufacturing.
- Technology-enabled personal devices.
- State and local governments and agencies.

40%  
Customers in  
Health-Related  
Fields

99%  
Customer  
Retention

70%  
Customer  
Referrals and  
Expansion



13

13

## Customer Spotlight



### Challenge

Full-service health care network with

- 20 facilities,
- 1,300 staff,
- 150 active physicians. and
- 400 volunteers

hit with a publicly disclosed ransomware attack in January 2018.

Limited internal detection and response capabilities.



THEY IMMEDIATELY PROVED THEIR VALUE AND EARNED OUR TRUST DUE TO THEIR IMMENSE EXPERTISE AND GUIDANCE THROUGHOUT THE ENTIRE PROCESS  
- STEVE LONG, PRESIDENT & CEO OF HANCOCK HEALTH

### Outcome

- Quickly recovered from the incident with most systems back just 3 days later.
- Rapidly reduced organizational risk while accelerating detection and response capabilities.

### Solution

#### Immediate

- Incident Response

#### Continuous

- 24 x 7 MDR Network, Endpoint, Log
- Vulnerability Management



14

14

# Is MDR Right for You? Customer Testimonial



STEVE LONG  
PRESIDENT & CEO  
HANCOCK HEALTH



15

15



## About Pondurance

**Pondurance delivers** world-class **MDR** services to industries facing today's most pressing and dynamic cybersecurity challenges including ransomware, complex compliance requirements, and digital transformation accelerated by a distributed workforce. By combining our advanced platform with our experienced team of analysts, we continuously hunt, investigate, validate, and contain threats so your own team can focus on what matters most.

Pondurance experts include seasoned security operations analysts, digital forensics and incident response professionals, and compliance and security strategists who provide always-on services to customers seeking broader visibility, faster response and containment, and more unified risk management for their organizations.

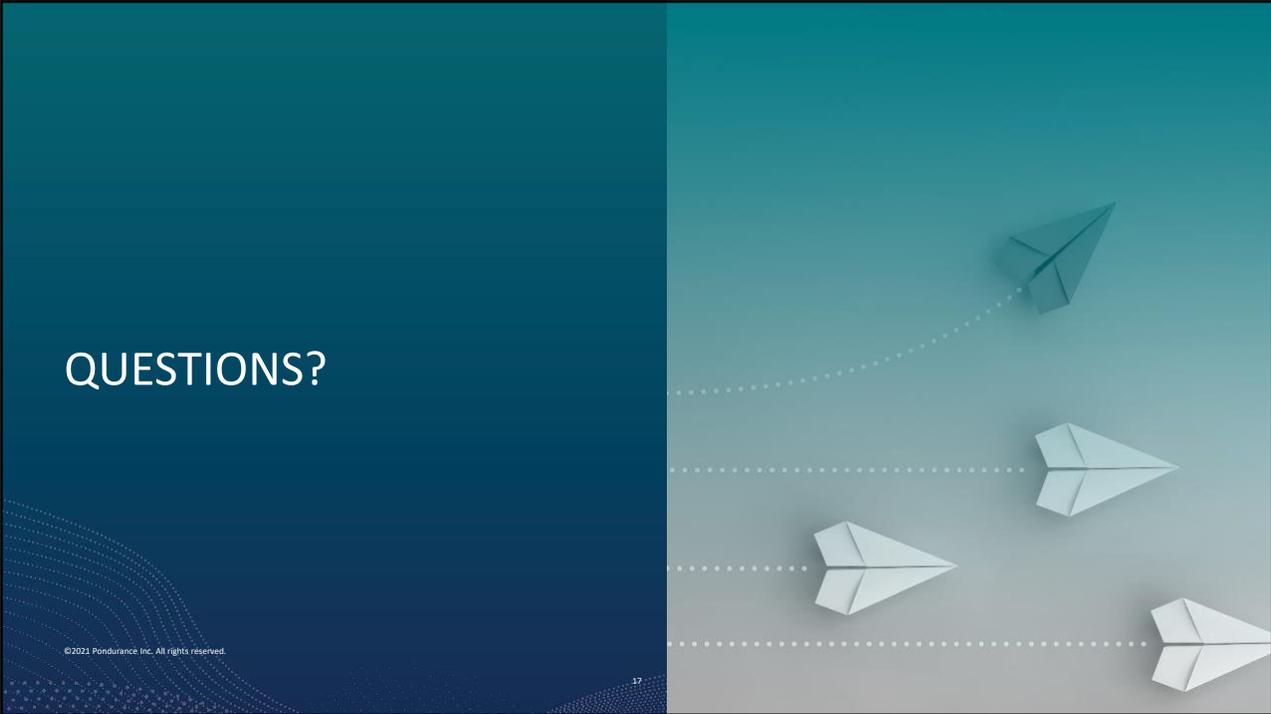
Visit [www.pondurance.com](http://www.pondurance.com) for more information.

[pondurance.com](http://pondurance.com)

500 N. Meridian St., STE. 500  
Indianapolis, IN 46204



16



17

Determination & Perseverance  
2020's Lessons and 2021's Challenges

Thank You

**Lyndon Brown**  
Chief Strategy Officer  
Pondurance  
[lyndon.brown@pondurance.com](mailto:lyndon.brown@pondurance.com)



18