Reducing Healthcare Cyber Risk Using a Cooperative SOAR enabled Healthcare Community (HSOC)

Eric Eder
Sequris Group Founder & CEO

Ryan Winn
Munson Healthcare CISO & System Director

Agenda

1. The Invitation
2. MiHCC Observations
3. MiHCC Incident Response
4. Opportunity of a Shared Model
5. The Benefits of a Physical Space
6. Why SOAR Is Integral to the Service We Deliver
7. Steering Committee Leadership
8. About Munson Healthcare & Sequris Group
9. Wrap Up & Questions

sequris VENTURE BEYOND RISK

Mi | HSOC
Powered by: CYBERFORCE | Q

MUNSON HEALTHCARE

The Invitation

MiHCC
MICHIGAN HEALTHCARE
CYBERSECURITY COUNCIL INC.

- The Governor requested that critical infrastructure cybersecurity groups form
- The Michigan Healthcare Cybersecurity Council is established
    - Public/Private healthcare membership organization
    - Focused on protecting critical healthcare infrastructure, institutions, and those they serve

MiHCC Observations

- Get Together – quarterly face-to-face meetings work best
- AdHoc Collaboration – implement simple mechanisms for ongoing communication
- Focus – significant progress on a few items is better than little progress on many items
- Trust – establish it early, reinforce it often
- Experience – the source for the best knowledge share

MiHCC Incident Response

- Inability to respond to security events – a top 3 issue
- Incident Response Plans – from check the box to tried and true
- A willingness to share - willing is NOT always able
- Attempt: Broadcast when under fire. Result: After the fact
- Attempt: Automate event sharing with Soltra Edge. Result: Died on the vine.

Go Bigger!

Opportunity of a Shared Model

Elements of contract:

- Flexible vendor
- Commitment to Sector
- Data Use Agreement
- Code of Ethics
- Governance
- Intellectual Property
- Publication Rights

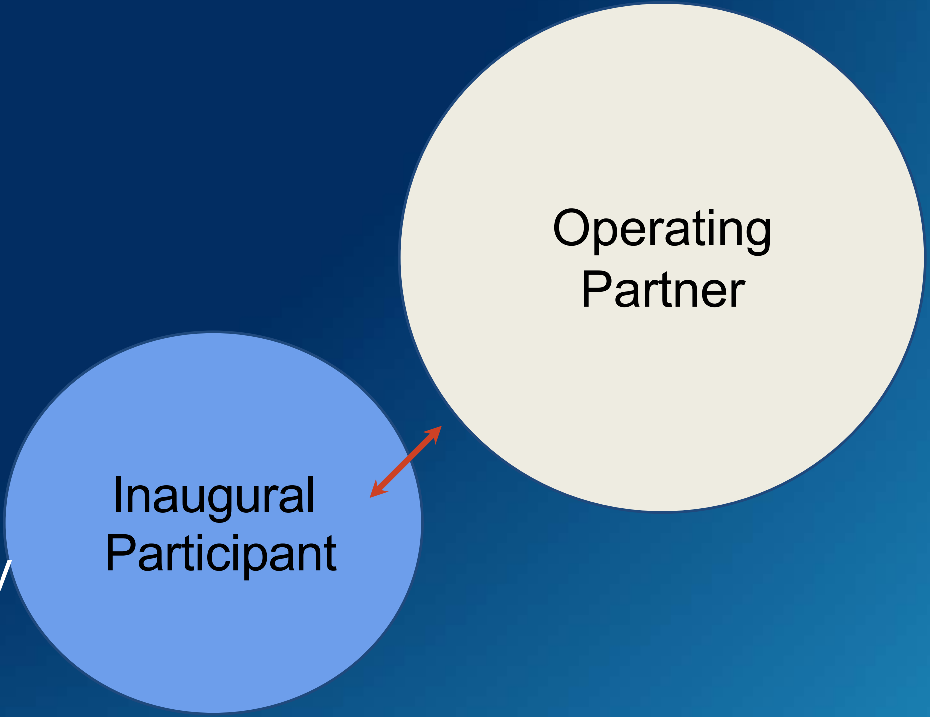
Operating Partner

Provides:

- Technology Expertise
- Flex/Surge Staffing
- Intelligence Visibility
- Sector Outreach

sequris VENTURE BEYOND RISK | HSOC Powered by: CYBERFORCE | Q | MUNSON HEALTHCARE

Opportunity of a Shared Model

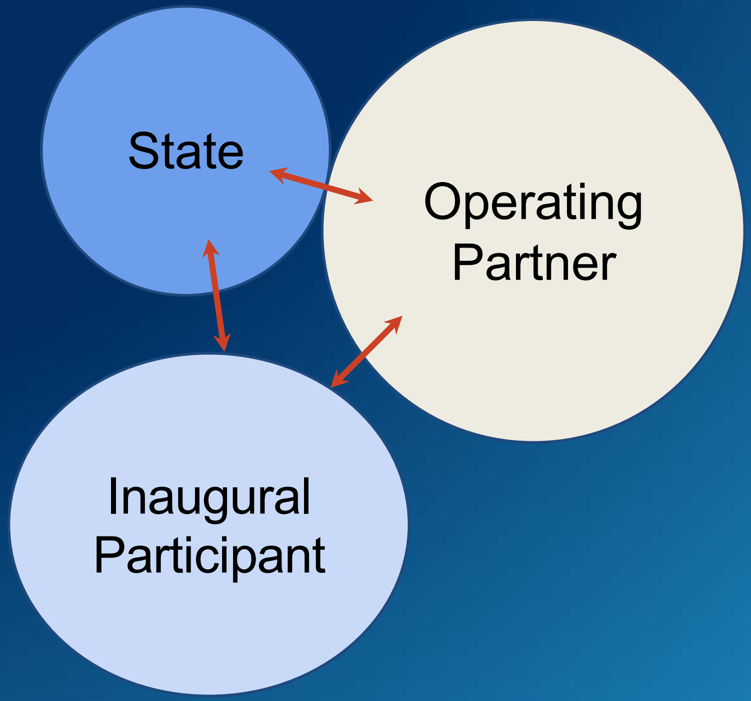


Operating Partner

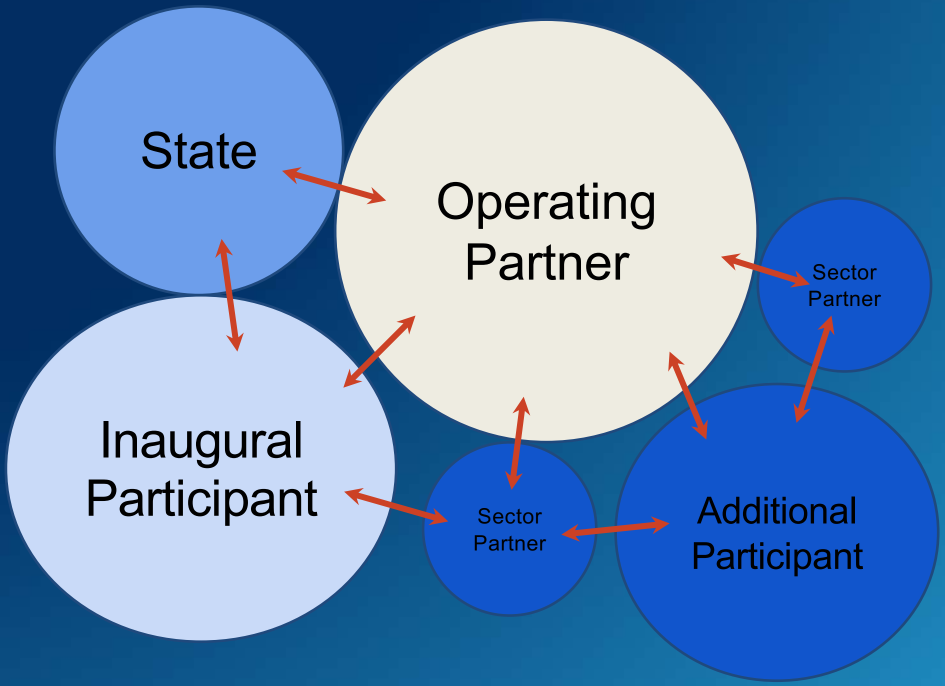
Inaugural Participant

- SOC Staff
- Technology Feeds
- Sector Coordination

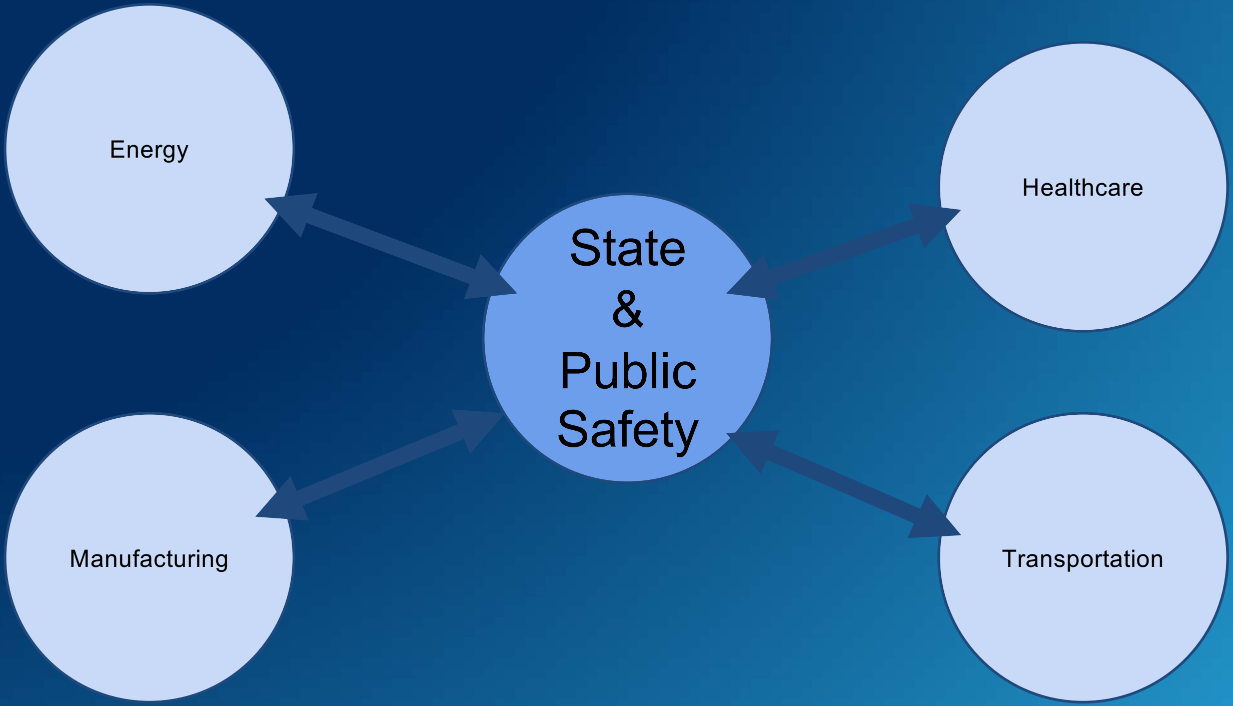
Opportunity of a Shared Model



Opportunity of a Shared Model



Opportunity of a Shared Model



sequris VENTURE BEYOND RISK | HSOC Powered by: CYBERFORCE | Q | MUNSON HEALTHCARE

Opportunity of a Shared Model

Cyberhub Model (IDA L.A. ODell)

Guiding Principles

- Lead with the “Cyber Hub” concept in order to facilitate stewardship
- Create an enterprise framework with common technical standards and processes as the default, leveraging existing models
- Optimize the use of data, information, and intelligence from existing programs (including fusion centers and ISACs), platforms, and tools in order to build and continually strengthen all operational outcomes
- Define and establish governance to promote transparency and cooperation
- Drive mission agility through communication and collaboration.

Opportunity of a Shared Model- Why Build?

- Cybersecurity is a team sport.
- Cyber crime is a team sport, and their team is ahead.
- Proactive information security requires real-time collaboration & new paths of communication.
- Development of healthcare specific information security capability.
- The opportunity to contribute to the academic process/curriculum.
- Improve patient care, research, educational effectiveness and safety through collaboration.
- Drive information security talent flow to the participating entities.

The Mi|HSOC

- Event Triage & Response
- Incident Investigation & Resolution
- Event Aggregation, Analysis, & Reporting
- Real world incident simulation and training
- Resource recruiting & retention

The Benefits of a Physical Space

- The “enclave” concept is one that all participants share a similar culture and identity.
- All entities can then have trust and reliance in the enclave.
- There is a level of value in the informal ability to work alongside cybersecurity professionals in like industries.
- Out of this thinking the CyberForce|Q Center was born.

First Responder Mutual Aid

1. The premise of active assistance
2. Common command and procedures
3. Community focused
4. Train together

SOAR Is Integral to the Service We Deliver

1. Technology Agnostic
2. Multi-Tenant while preserving collaboration
3. Meta-data orientation
4. Platform to share and obtain protection of CISA and similar acts.

SYNCURITY

sequris VENTURE BEYOND RISK

HSOC

Powered by: CYBERFORCE | Q

MUNSON HEALTHCARE

Steering Committee Leadership

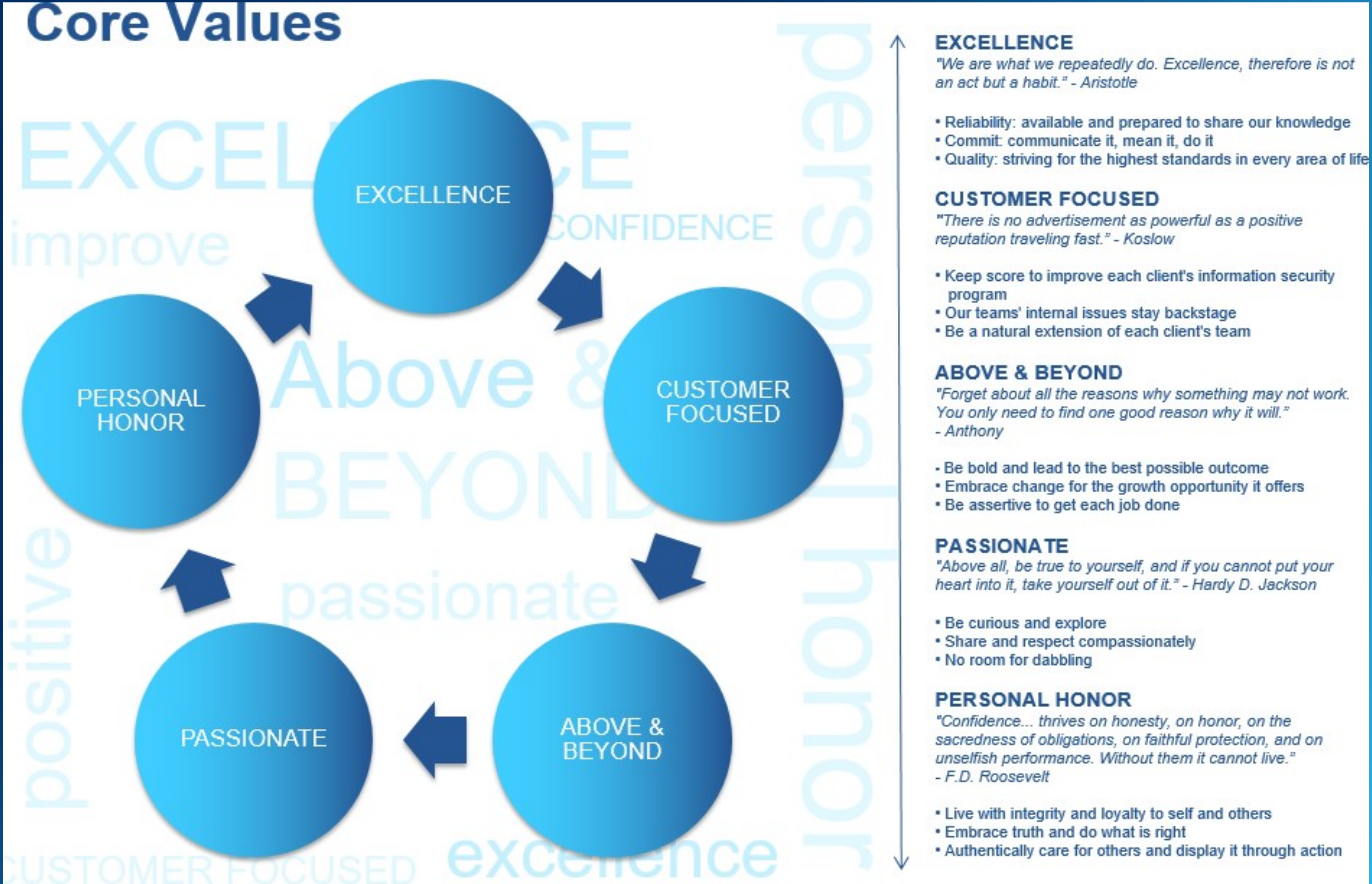
1. Common purpose and governance
2. Participants define and adhere to the rules of the game
3. Clear measurement, metrics, and accountability
4. Preservation of a higher purpose

Key Takeaways That Led to Success:

Munson Healthcare

- Munson Healthcare
  - 9 hospital system
  - 12000 users
  - 28000 network nodes
  - 2000 devices connected to patients
- Rationale for participation
  - Learn from peers
  - Protect the ecosystem
  - Demonstrate openness and trust
  - Cost effective monitoring
  - Focus on the things that a healthcare system must be great at

About Sequris Group



Core Values

EXCELLENCE

"We are what we repeatedly do. Excellence, therefore is not an act but a habit." - Aristotle

- Reliability: available and prepared to share our knowledge
- Commit: communicate it, mean it, do it
- Quality: striving for the highest standards in every area of life

CUSTOMER FOCUSED

"There is no advertisement as powerful as a positive reputation traveling fast." - Koslow

- Keep score to improve each client's information security program
- Our teams' internal issues stay backstage
- Be a natural extension of each client's team

ABOVE & BEYOND

"Forget about all the reasons why something may not work. You only need to find one good reason why it will."
- Anthony

- Be bold and lead to the best possible outcome
- Embrace change for the growth opportunity it offers
- Be assertive to get each job done

PASSIONATE

"Above all, be true to yourself, and if you cannot put your heart into it, take yourself out of it." - Hardy D. Jackson

- Be curious and explore
- Share and respect compassionately
- No room for dabbling

PERSONAL HONOR

"Confidence... thrives on honesty, on honor, on the sacredness of obligations, on faithful protection, and on unselfish performance. Without them it cannot live."
- F.D. Roosevelt

- Live with integrity and loyalty to self and others
- Embrace truth and do what is right
- Authentically care for others and display it through action

sequris VENTURE BEYOND RISK | HSOC Powered by: CYBERFORCE | Q MUNSON HEALTHCARE

Thank You!