Michigan Healthcare Security Operations Center

Presented by:

Jack Kufahl – Michigan Medicine

Eric Eder –CyberForce|Q

October 2019

Copyright CyberForceQ, LLC All rights reserved.

HSOC

CYBERFORCE

Mission & Purpose

- Establish a platform for cybersecurity sharing and collaboration
- Enact healthcare sector-specific capability to detect/identify threats
- Align with Federal and State critical infrastructure protection
  - Cybersecurity Information Sharing Act (CISA-2015)
- Create a scalable solution for participants of varied sizes

Beaumont HEALTH

MHA Michigan Health & Hospital Association

CYBERFORCE

MICHIGAN MEDICINE
UNIVERSITY OF MICHIGAN

MUNSON HEALTHCARE

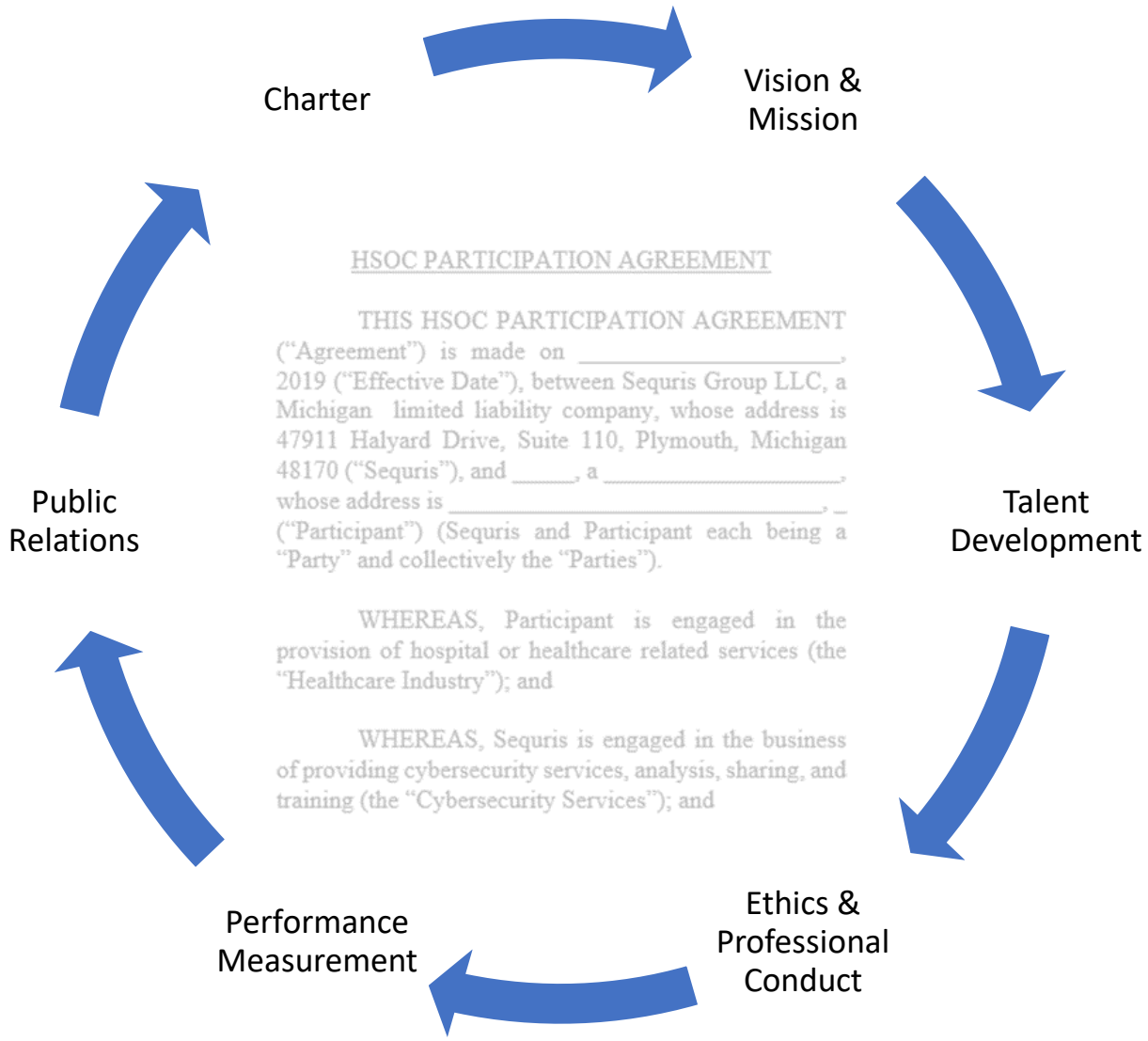
Foundation Inaugural Participants & Steering Committee

FOUNDATION

January 2018	Structure Formation
July 2018	Finalized Inaugural Participants
September 2018	Grand Opening • Offline Que • Online Que
December 2018	Simulation Training
April 2019	Participation Agreement • Provides for Participation Sharing • Authorizes CISCP Participation
June 2019	Capability made available to the entire healthcare sector Focus on scale for rural and other small healthcare providers

LESSON #1

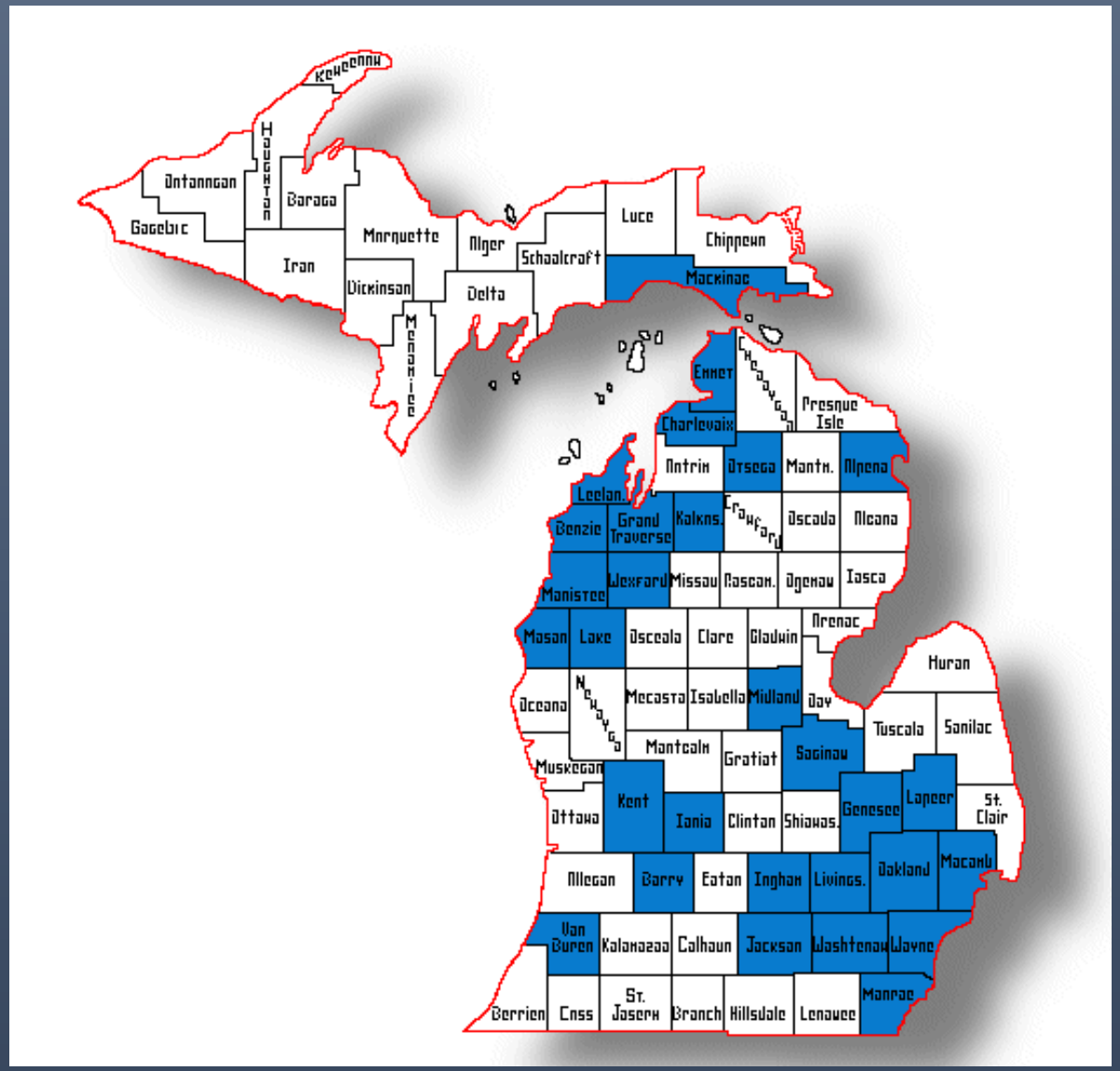
- Establish a steering committee based on:
  - Sector representation
  - Directives for the good of the whole
  - Transparency



Foundation Governance & Participation Agreement

LESSON #2

- Mutual Aid:
  - Multiple participants, One force for good
  - Common structure
  - Train together

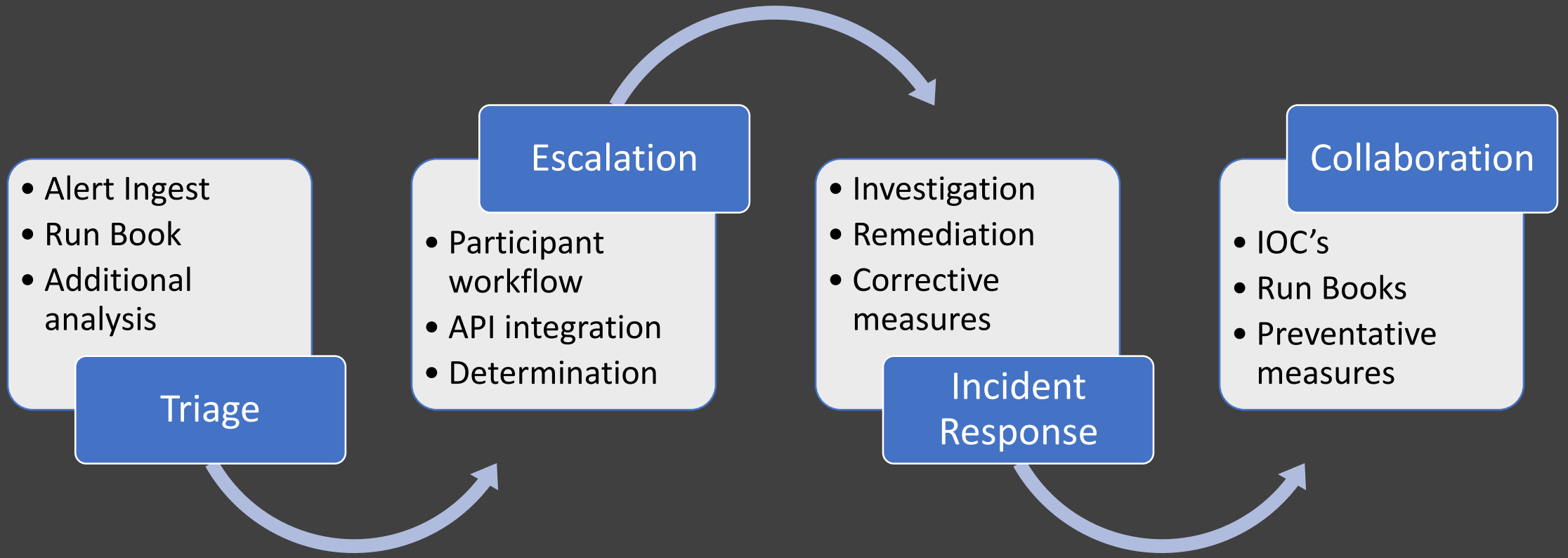


Current Outreach

Staffing

- Partcipants embed staff on the Mi|HSOC team
- Mi|HSOC team is integrated with each participant's ops team
- Operating partner provides consistent staffing and 24x7x365 coverage

Daily Operations



Operating Cadence

Strategic Cadence

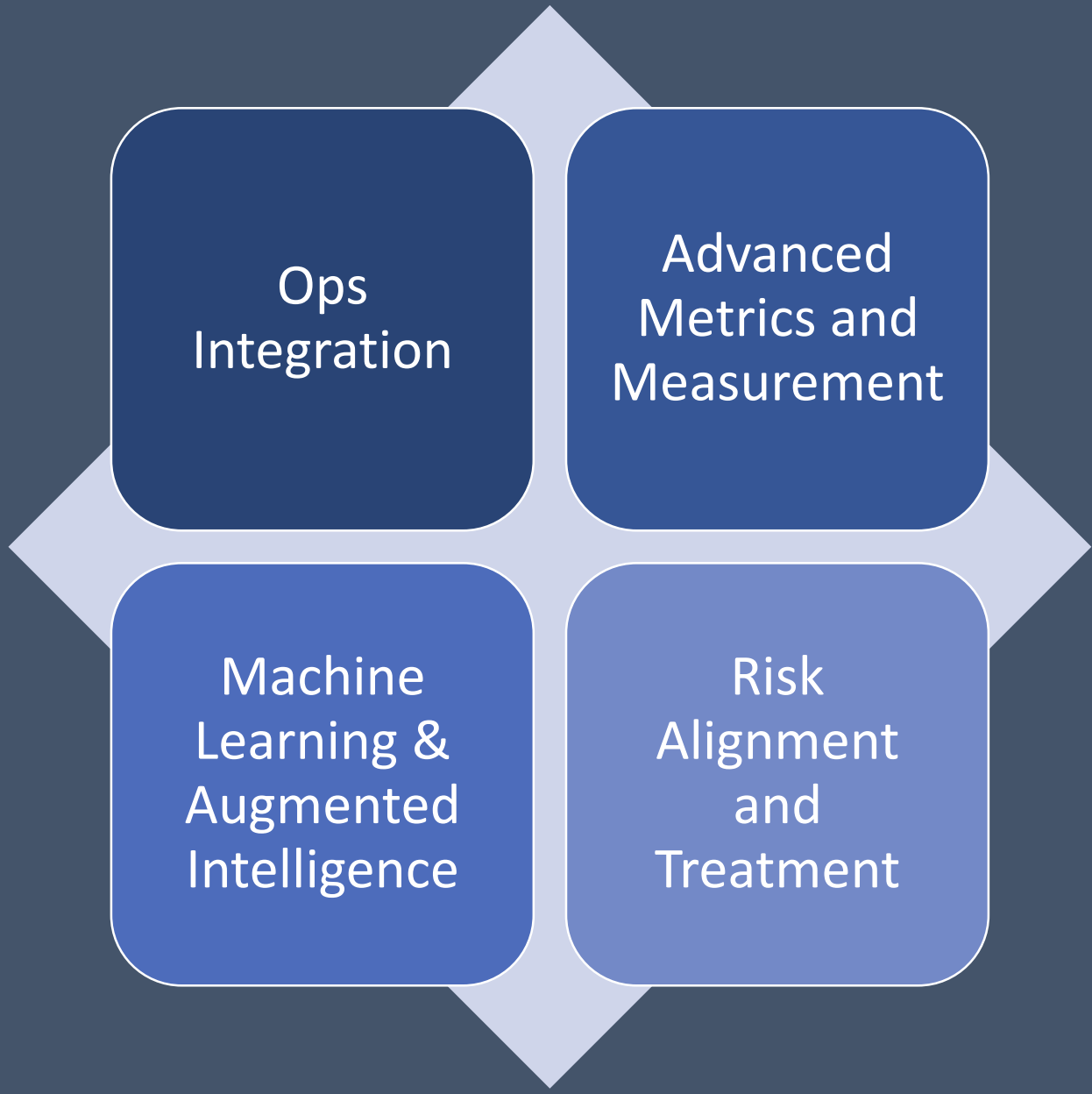
LESSON #3

- Objective Measurement:
  - Determined by steering committee
  - Aligned to inform NIST CSF controls (healthcare-specific implementation)
  - Automated

Standardized Measurement

Standardized Foundation	Flexible and Adaptive for each participant
NIST CSF Controls	Additional controls (HIPAA, PCI, etc).
Mi|HSOC performance measures	Participant performance measures
Service Level Agreements	Participant operations optimization
Automated metrics tracking	Security technology stack
Comparative analytics	Run books and Use cases

Next Steps


Ops Integration
Advanced Metrics and Measurement
Machine Learning & Augmented Intelligence
Risk Alignment and Treatment

Ops Integration

External-to-Internal Perspective

- Third party threat feeds
- Sec Ops
- Net Ops
- Sys Ops
- Dev Ops
- Health Informatics

Machine learning integration

Ticket and event flow APIs

Automated data enrichment

Automated remediation actions

Advanced Metrics and Measurement

- Expand beyond MiHSOC services
- Automated metrics integration
- Technology efficiency and effectiveness

Machine Learning

- Automated baseline and trending
- Data set time series profiling
- Asset inventory imperative
- Align with health informatics
- Machine Learning & Augmented Intelligence

Risk Alignment & Treatment

- Identify participant risk tolerance
- Risk informed inventory and data sets
- Risk prioritized run books
- Risk aligned collaboration and treatment

Thank you

Jack Kufahl – Michigan Medicine
Eric Eder – CyberForce|Q

Mi|HSOC
47911 Halyard Drive
Plymouth, Michigan 48170
www.mihsoc.com