black hat EUROPE 2021
november 10-11, 2021
BRIEFINGS

Building Better CSIRTs Using Behavioral Psychology

Mark Orlando and Dr. Daniel Shore

All About Us (intro to ego-centrism)

- Studying Cybersecurity Teamwork since 2012
- PhD in Workplace Psychology
- Co-founder & Chief Research Officer, LETS
- Trained government teams in US, Sweden, & Netherlands

- 20 years in security operations
- Co-founder & CEO, Bionic Cyber
- Former White House, DoE, Raytheon, MSSP, MDR
- SANS Instructor, SEC450 and Co-author, MGT551

The Problems We're Solving

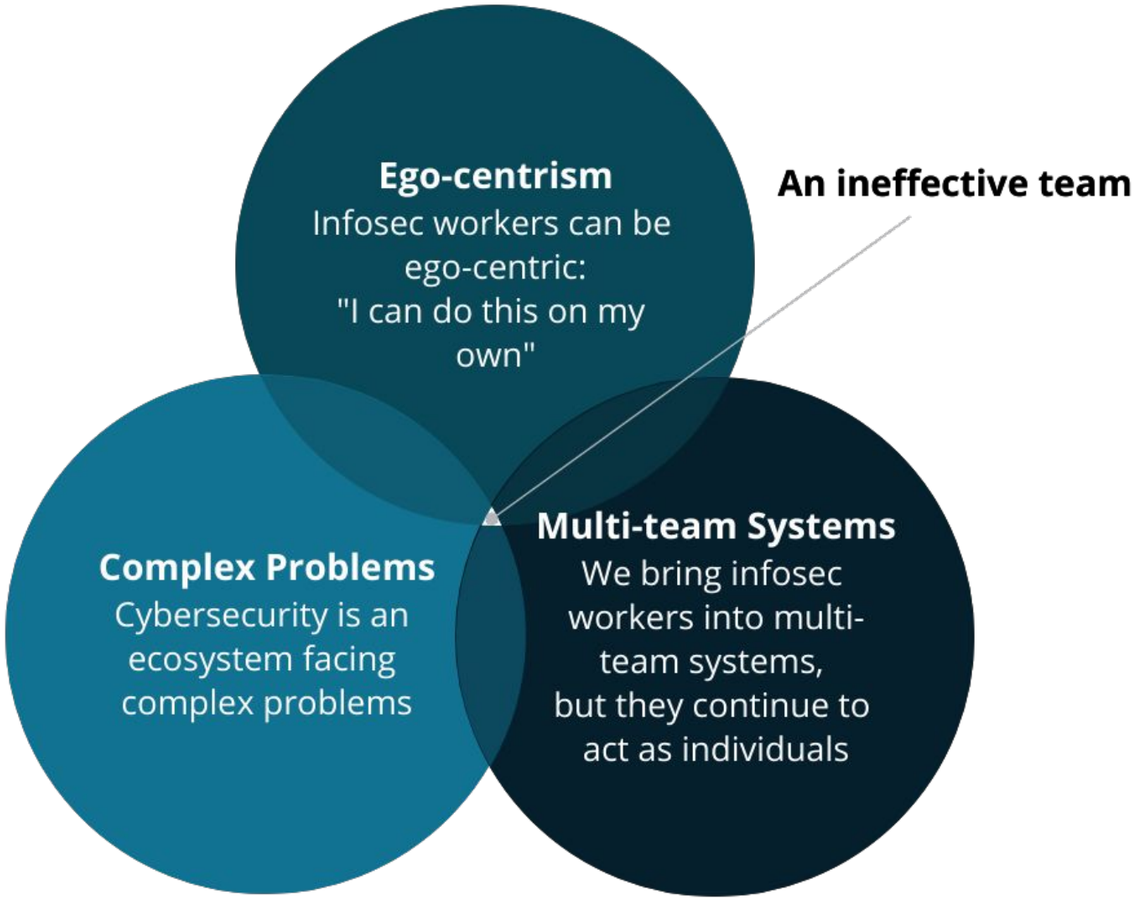
A **The Superhero Problem**
Most teams are over-reliant on a few key people to repeatedly save the day.

B **The Teamwork Problem**
Security operations training is heavily focused on technical capabilities.

C **The Firefighting Problem**
We constantly need to adapt during crises without structure or tools

D **The Lone Wolf Problem**
We have talented analysts who are only motivated to do work on their own.

Why We're Here



The Largest Social-Behavioral Study of InfoSec Teams to Date

5 years

20+ researchers & practitioners

56,000+ research hours

52 focus groups

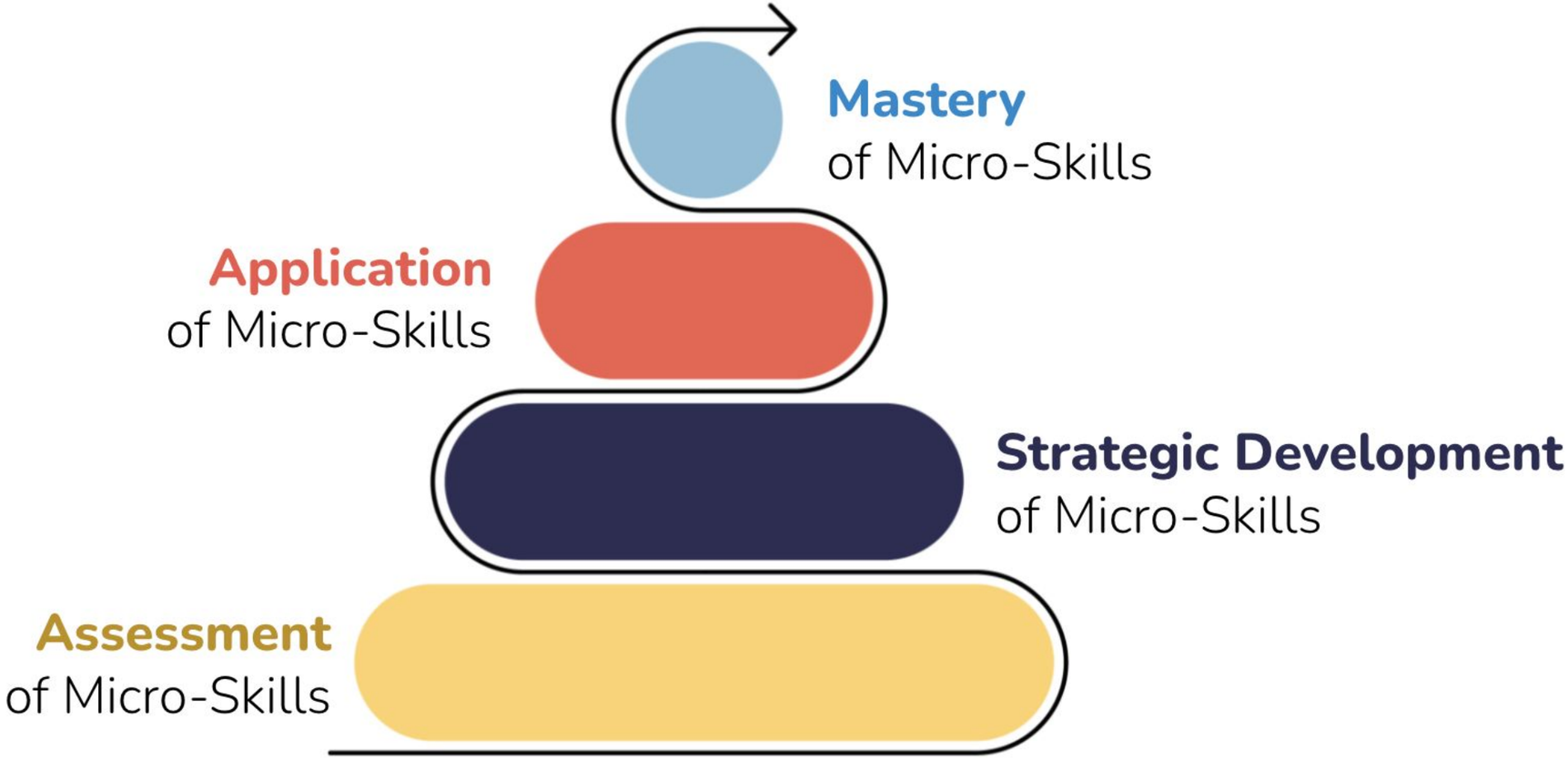
148 survey and cognitive task analysis participants

28 multi-team systems (MTSs)

17 organizations across the US & Europe

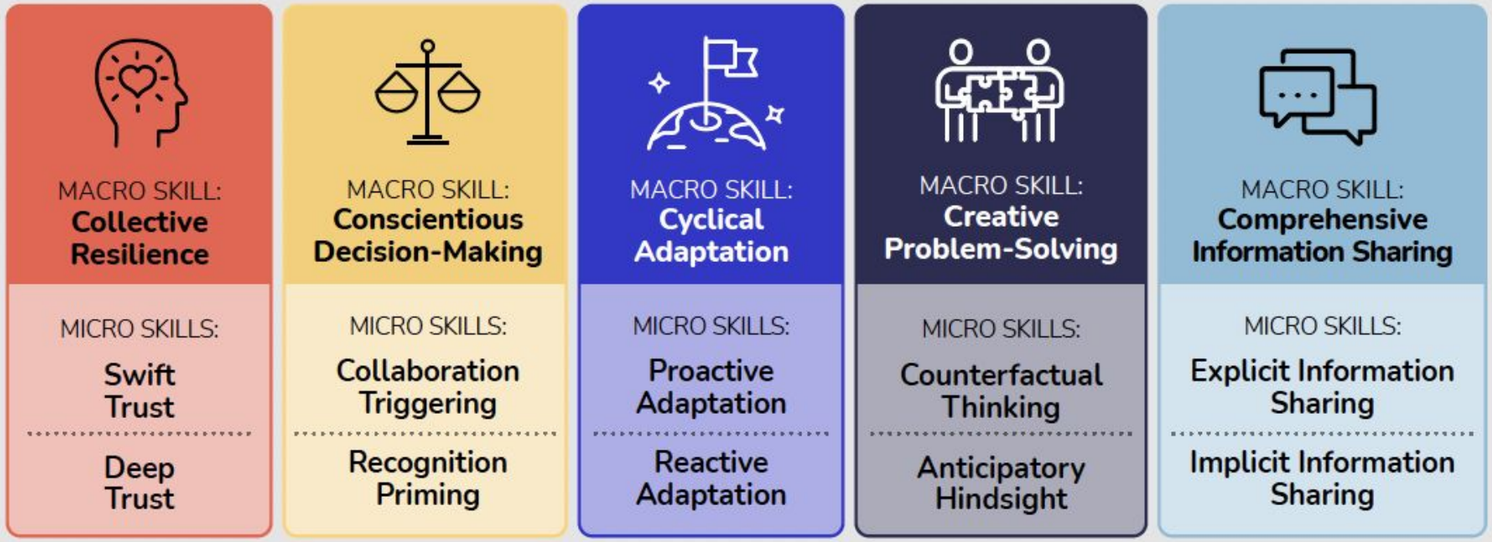
US Government | George Mason University | Dartmouth | HP Labs | Swedish Government | Dutch Government

Social Maturity Framework



The Top Priorities for Effective Cybersecurity Teamwork

5Cs: MTS Collaboration Macro- and Micro-Skills



*DHS-funded Research Team: Tetrick, L., E., Zaccaro, S. J., Dalal, R. S., Steinke, J. A., Repchick, K. M., Hargrove, A. K., **Shore, D. B.**, Winslow, C. J., Chen, T. R., Green, J. P., Bolunmez, B., Tomassetti, A. J., McCausland, T. C., Fletcher, L., Sheng, Z., Schrader, S. W., Gorab, A. K., & Niu, Q. (2016). Improving social maturity of cybersecurity incident response teams. Fairfax, VA: George Mason University.

Figure 1: 5C Model

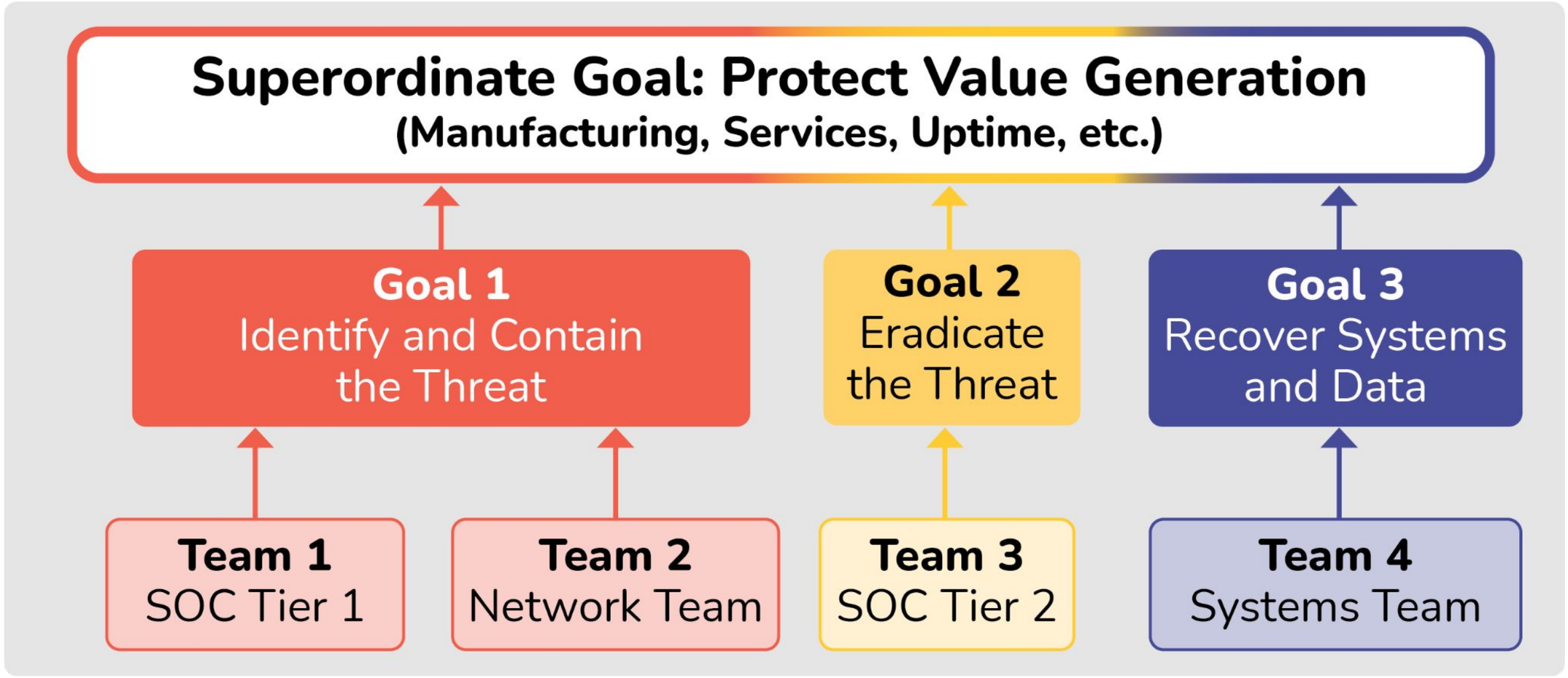
Why It Works


Celebrate
Motivation for Teamwork
Create
Psychological Safety
Cultivate
Autonomy,
Belonging, &
Competence

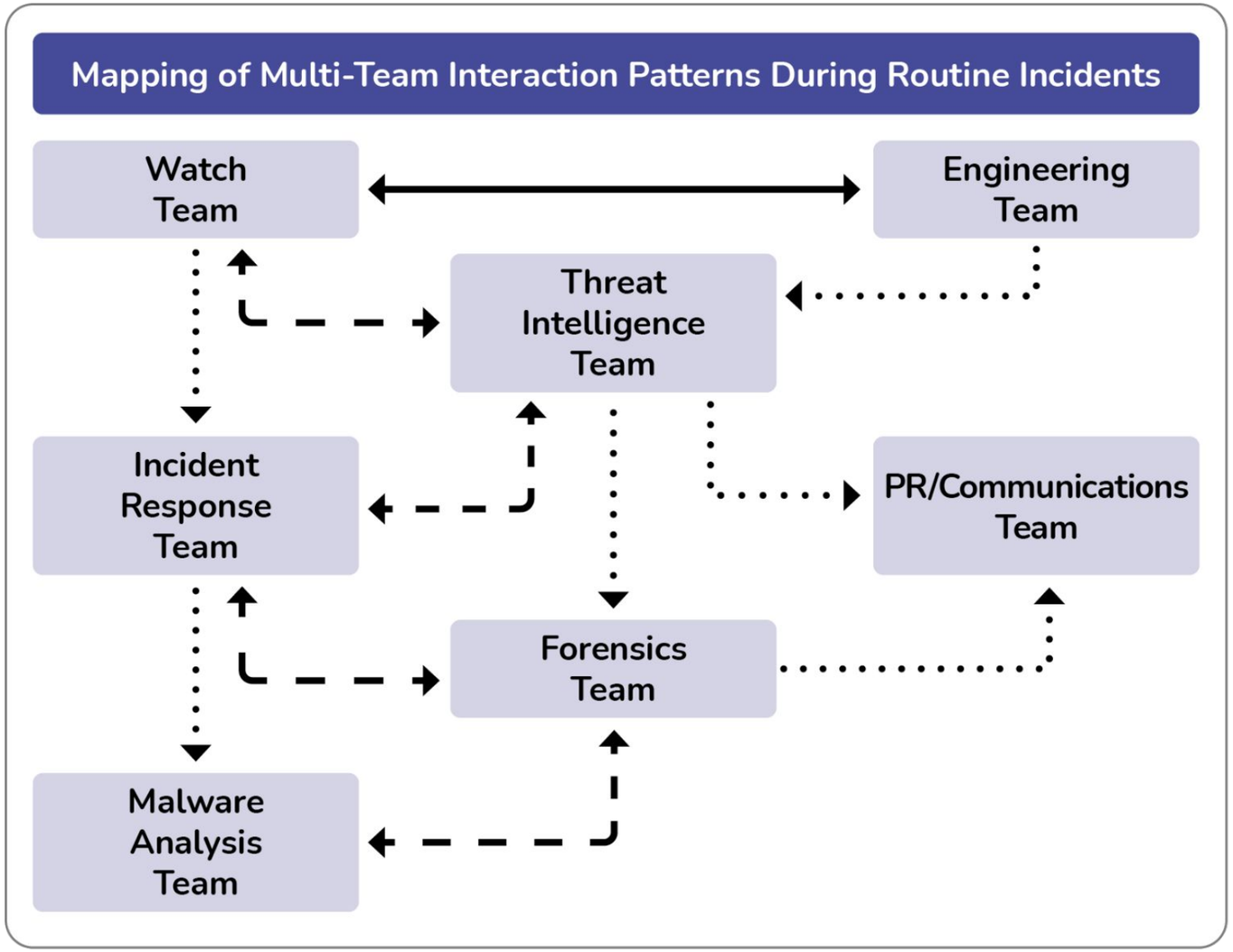
Case Study: 24/7 Executive Branch SOC

Engaging Goal Setting	Collaboration and Communication
• Balancing strategic and tactical goals: *what do we focus on?* • Be an “expert” in an expert organization • How do we know we’re getting the job done?	• Identify situations where team members should engage others • Share knowledge effectively • Measure effective collaboration as an indicator of successful identification and response

Example MTS Goal Hierarchy



Example MTS Interaction Diagram



Interaction Levels

Moderate levels of interactions

High levels of interaction

Very high levels of interaction

Note: At higher levels of incident severity, interactions between teams increase in intensity. Also, teams that do not generally interact begin to interact more frequently.

Case Study: Managed Detection and Response Service

Norms and Expectations	Knowledge Management
• Establish norms for ongoing service delivery • Closely manage time and effort per customer while ensuring positive customer experience	• Team studies and catalogs customer environments and threat model(s) • Experiential knowledge is retained in a way that whole team benefits • Knowledge is actively maintained, not stored and forgotten

Team Charter Roadmap

Step 1a:

Each team member identifies their own. . .

- Goals
- Responsibilities
- Style of Communication
- Openness to Collaboration

Step 1b:

Each team member identifies their perspective of the team's. . .

- Goals
- Responsibilities
- Style of Communication
- Openness to Collaboration

Step 2:

Team members align on expectations from Steps 1a & 1b

- Identify Similarities
- Reconcile Differences
- Reach Consensus
- Aggregate into one document

Step 3:

The team creates a plan on how to maintain their alignment from Step 2

- Accountability
- Opportunities for Feedback
- Qualitative and Quantitative Metrics
- Proactive and Reactive Adaptation

Example Team SKUE* Board

For Myself				
Information I have that I think is unique from that of other team members	Examples of situations when that unique information is most useful	Skills I have that I think are unique from that of other team members	Examples of situations when those unique skills are most useful	Major events/incidents that I have been involved with
For Each Team Member				
Information (Team Member) has that I think is unique from that of other team members	Examples of situations when that unique information is most useful	Skills (Team Member) has that I think are unique from that of other team members	Examples of situations when those unique skills are most useful	Major events/incidents they have been involved with

*Shared Knowledge of Unique Expertise

Summary and Homework

- We immediately update our software, we never update our teamwork
- Making time to invest in teamwork, not just taskwork, has long term gains
- Four tools discussed today that you can use:
  - **MTS Goal Hierarchy**
  - **MTS Interaction Diagram**
  - **Team Charter**
  - **Team SKUE Board**

Stay In Touch!

Twitter:
@markaorlando
@LETS_thinkHuman

E-mail:
mark@bioniccyber.com
daniel@letswecan.com

Web:
https://bioniccyber.com
https://letswecan.com