When a Plan Comes Together: Building a SOC "A-Team"

Mark Orlando

@markaorlando

Visit sans.org/free for thousands of FREE Cybersecurity Resources

WHY ME

- 19 years in secops
- Co-founder, Bionic
- Former White House, DoE, Raytheon, MSSP, MDR
- SANS SEC450 and MGT551 Instructor
- 80s kid

@markaorlando

WHY THIS TALK

- People will make or break your security team
- Good ones are hard to find/train/keep
- Traditional ops model is not optimized to engage the best people

IF YOU HAVE A PROBLEM (SOC IS HARD)…

Lack of business alignment

Data and tools (too many, not enough)

Outdated "alert watcher" model

Sustainment mentality

@markaorlando

…AND IF NO ONE ELSE CAN HELP…

Is there really a talent shortage?

@markaorlando

MAYBE YOU CAN HIRE THE A-TEAM

Focus on:

- Build zealots, not mercenaries*
- Empowerment, purpose, and teamwork
- Ongoing coaching
- Readiness to prove yourself over and over

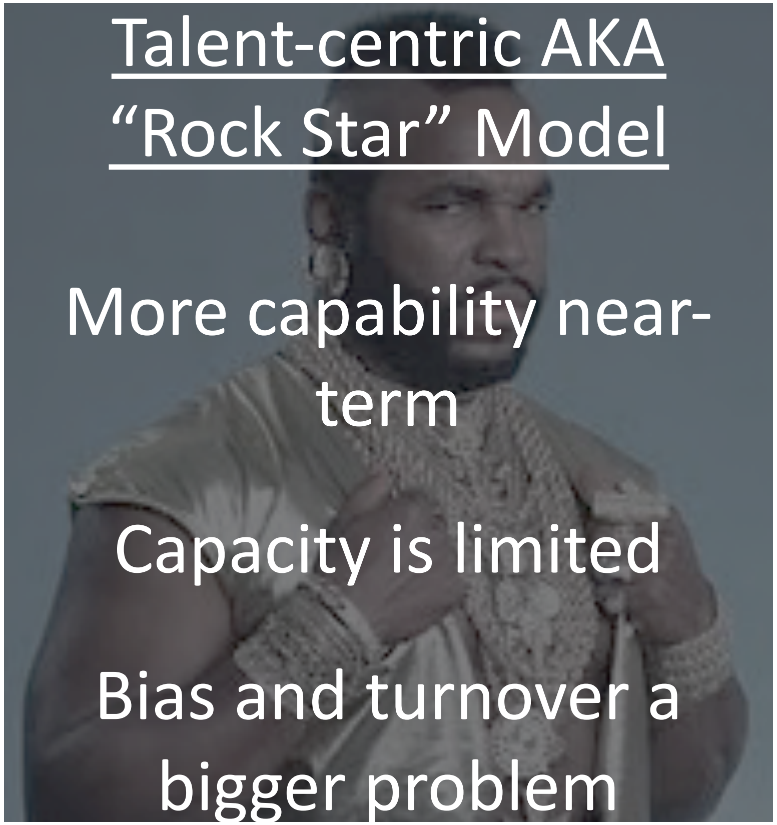
*From The Infinite Game by Simon Sinek

@markaorlando

GETTING STARTED

1. Building the A-Team
2. Experimentation and iteration
3. Ongoing management
4. Showing results (METRICS)
5. Ensuring the plan comes together

BUILDING THE TEAM

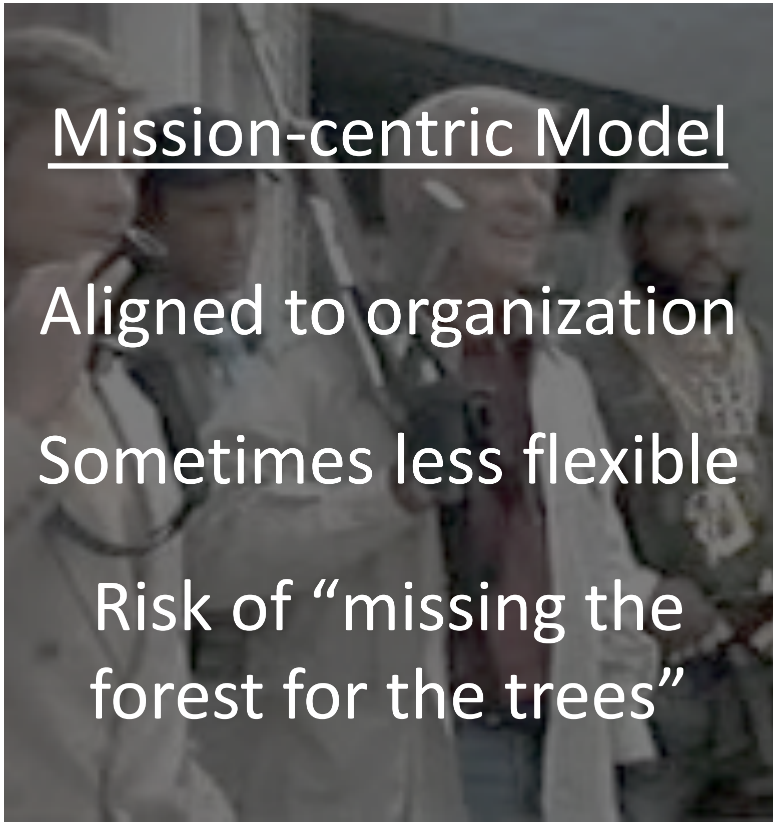


Talent-centric AKA “Rock Star” Model

More capability near-term

Capacity is limited

Bias and turnover a bigger problem



Mission-centric Model

Aligned to organization

Sometimes less flexible

Risk of “missing the forest for the trees”

@markaorlando

WHAT TO LOOK FOR

Good Signs

- Curiosity
- Motivation
- Persistence/grit
- Positive attitude
- Critical thinking
- Situational awareness
- Diverse background

Bad Signs

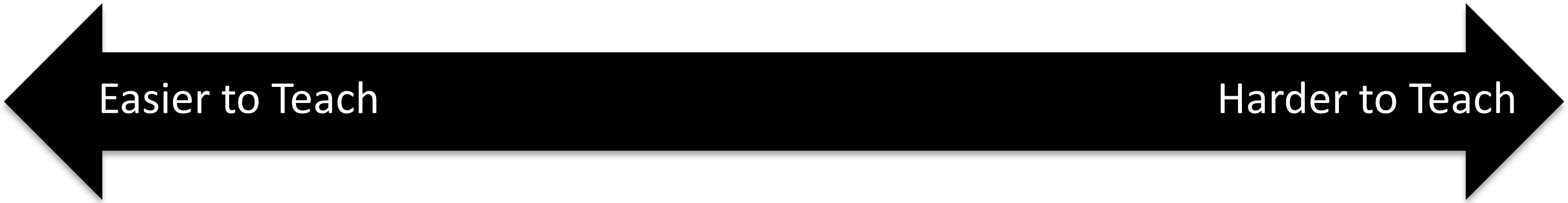
- Misrepresentation
- Ego
- Bluffing
- Disparaging former employers and teammates
- Over-reliance on credentials

BUILDING THE TEAM

- Probing for technical depth, from SANS MGT551:
  - Open-ended, situational questions
  - Questions across multiple domains that get harder
  - Allow candidate to display technical depth without undue pressure, see what happens when they don’t have the answers
- Avoid bias, questions that are easy to predict, irrelevant “puzzle” questions

@markaorlando

TRAINING



Easier to Teach

Harder to Teach

- ✓Technical analysis
- ✓Search syntax
- ✓Tool usage
- ✓SOPs
- ✓Documentation

- ✓How to think
- ✓How to communicate
- ✓Investigative theory
- ✓Business implications of cyber security

Pro-tip: Combine formal and informal, on-the-job training!

@markaorlando

TRAINING

- Continuous learning model*
  - Immediate + intermediate + transitional
- Collaborative problem solving
  - Pre-briefings for IR and hunts
  - Simulations and structured de-briefs
  - Direct, timely feedback

Pro tip: Train your own people and train them together!

MOTIVATING & RETAINING

- ✓ No competition zone
- ✓ Task shifting (hero proofing)
- ✓ Celebrate small wins
- ✓ Watch for burnout
- ✓ Keep the team happy*
  - ✓ Autonomy
  - ✓ Mastery
  - ✓ Purpose

*From <u>Drive</u> by Daniel Pink

MEASURING SUCCESS

- Show ROI
- Validate “normal” operations
- Demonstrate progress towards objectives
- Highlight areas for improvement
- In the SOC, focus is on <u>ops</u> and improvements

MEASURING SUCCESS

MISSION ACCOMPLISHED

- Enter KPIs and OKRs
- KPIs instrument your operation
- OKRs tie ops to strategy
- Constantly re-evaluate both
- Make sure you control levers that move both

METRICS THAT MATTER

- KPIs:
  - Key area + target value/threshold
  - Tells us if we're maintaining status quo
- OKRs:
  - Strategic goal + results that get us there
  - Measures advancements and initiatives
- OKRs can be used to bring KPIs into desired range
  - "Get time to respond down to x"

MEASURING PEOPLE

- Clear expectations aligned to team goals
- Feedback to inform, not penalize
- Honest, direct feedback via one-on-ones
- Set them up for their success – not

@markaorlando

CHALLENGES

“Collaboration chillers”*

1. Failure to share information
2. Failure to initiate collaboration
3. Failure to adapt
4. Poor communications practices
5. Lack of trust
6. Lack of knowledge about team member expertise
7. Interpersonal conflict

*Improving Social Maturity of Cybersecurity Incident Response Teams, DHS, GMU, et. al.

CHALLENGES

SKUE: shared knowledge of unique expertise

- Shared knowledge of “who knows what”
- Quickens IR process
- Requires:
    - knowledge tools
    - cross-training
    - after action reviews

CHALLENGES

- Inward focus
- Role-oriented bias
- Conflict and lack of trust
- Sustainment mentality
- Lack of empowerment

WHAT YOU CAN DO

- Foster interaction & social connections
- Set clear goals, roles, standards
- Exemplify communication norms
- Create a safe space for failure and learning
- Push the team out of their comfort zone*

* Just not too far, and not all the time

CASE STUDY:

4/7 Executive Branch SO

Challenges:

- Brand new SOC
- Small budget
- Team and tools pre-selected
- Highly technical customer
- Organization in flux

@markaorlando

CASE STUDY:

4/7 Executive Branch SO

Approach:

- Mission-focused team
- Focus on story telling while making measurable progress on reducing risk
- Find ways to be “smarter” than the customer to keep them engaged
- Take advantage of unique environment & opportunities to keep team engaged

@markaorlando

CASE STUDY:

MDR Service Offering

Challenges:

- Clear goals but few processes
- New, untested team
- Lack of quality checks, performance standards, team structure

CASE STUDY:

MDR Service Offering

Approach:

- Talent-focused team
- Start small and iterate
- Lots of team building
- Strong supporting functions: R&D, project management
- Build generative environment that encouraged experimentation and new ideas

WHEN A PLAN COMES TOGETHER

Talent can be found lots of different places – know how to identify and foster it

WHEN A PLAN COMES TOGETHER

Difference between an A-Team and “the other team” is how well the team works together towards common goals

OTHER RESOURCES

- SANS SEC450: Blue Team Fundamentals
- SANS MGT 551: Building & Leading SOCs
- Five Ways to Cut Costs in Your SOC: https://www.sans.org/webcasts/ways-cut-costs-soc-113275
- Blueprint Security Podcast: https://www.sans.org/blueprint-podcast
- Bionic Cyber blog: https://www.bioniccyber.com/blog
- Many more free resources: https://www.sans.org/free

HOMEWORK

1. Schedule one-on-ones
2. Ask everyone on your team discuss the SOC charter and what exactly they are protecting
3. Look for ways to remove barriers to communications and teamwork
4. Conduct a pre-briefing
5. **POP QUIZ**: Is your team talent-centric or mission-centric?

LET’S KEEP IN TOUCH

mark@bioniccyber.com

@markaorlando