WHEN A PLAN COMES TOGETHER: BUILDING A SOC A-TEAM

By Mark Orlando

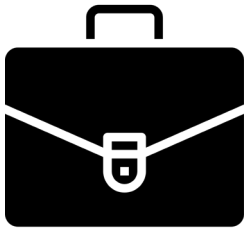
ABOUT ME

- 17 years in secops
- Public & private sector
- 80s kid
- @markaorlando

ABOUT THIS TALK

- Foundation of a security team is **people**
- Good ones are hard to find/train/keep
- Time to hack the traditional SOC model

IF YOU HAVE A PROBLEM (SOC IS HARD)…



Lack of business alignment

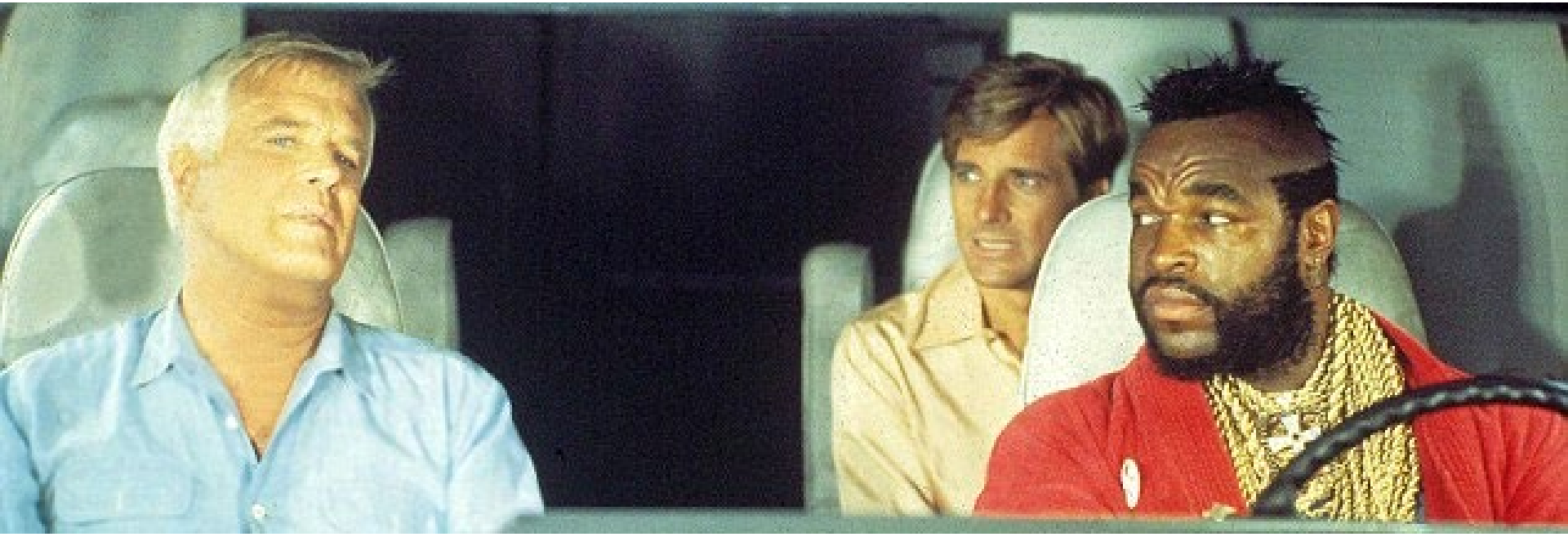
Data and tools (too many, not enough)

Outdated “alert watcher” model

Sustainment mentality

…AND IF NO ONE ELSE CAN HELP

Is there really a talent shortage?



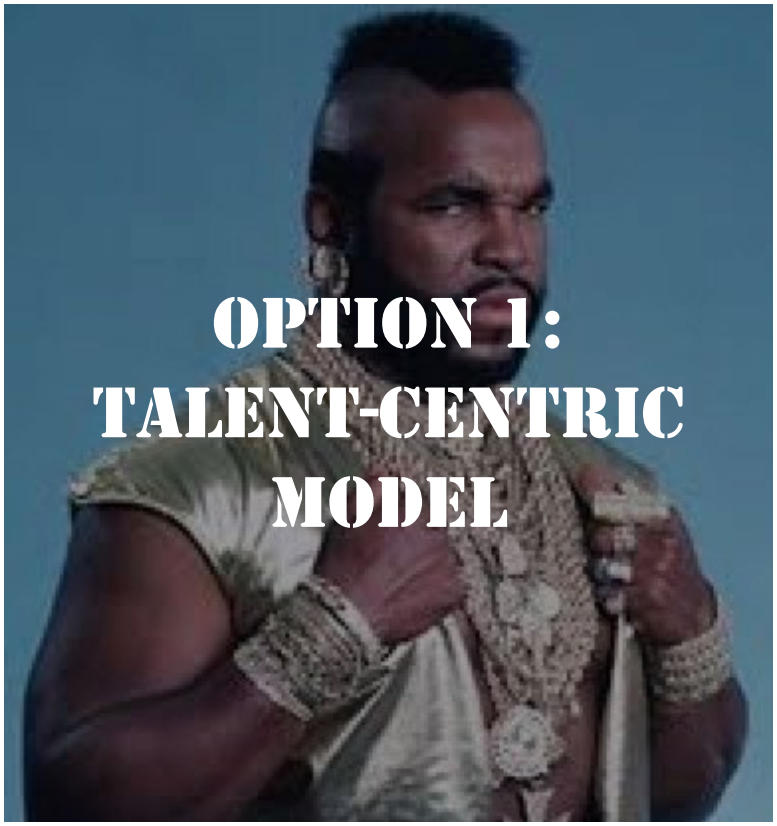
MAYBE YOU CAN HIRE THE A-TEAM

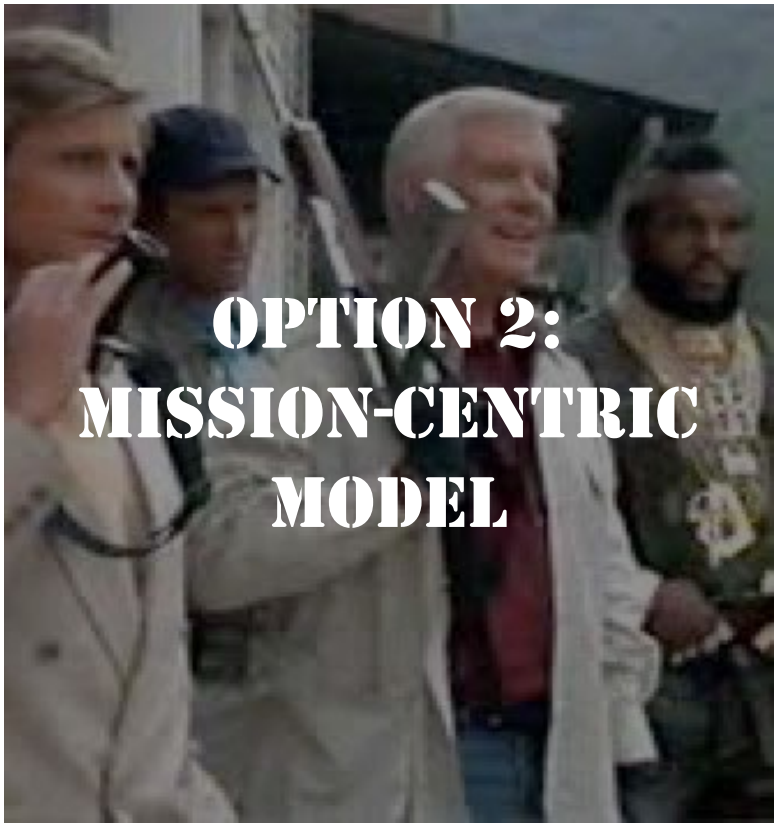
- How do you create value?
- Direction, purpose, and teamwork
- Competent coaching
- Readiness to prove yourself

GETTING STARTED

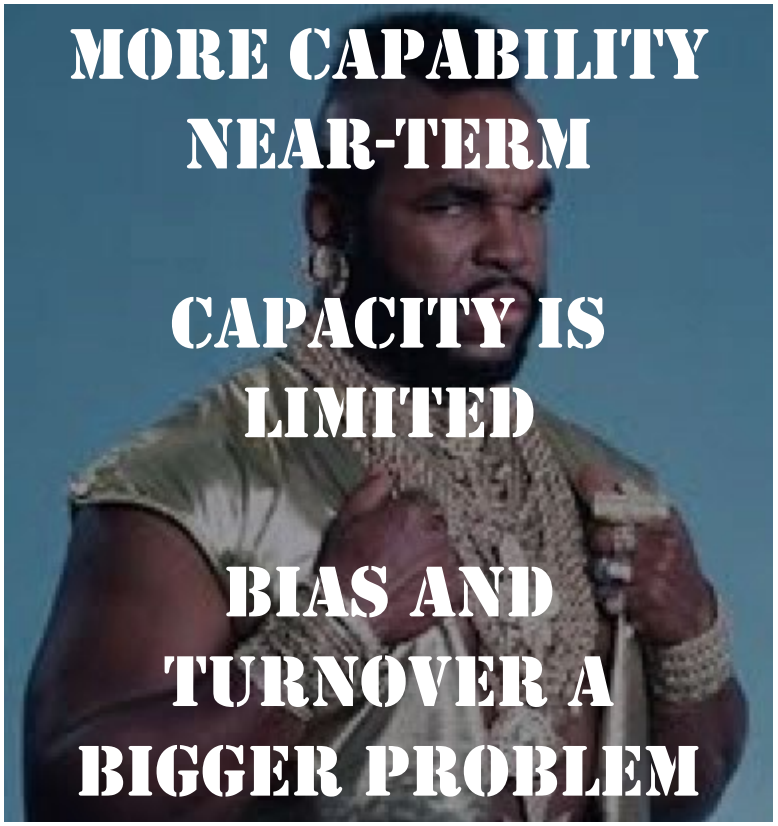
1. Study the business/mission
2. Experiment and iterate
3. “Servant” leadership
4. Show results (METRICS)
5. Always have a plan

BUILDING THE TEAM





BUILDING THE TEAM



BUILDING THE TEAM

Attract

- ✓ Aptitude
- ✓ Attitude
- ✓ Desire
- ✓ Diversity

Avoid

- ✓ Over-reliance on experience or creds
- ✓ Egos
- ✓ Misrepresentation

@markaorlando

BUILDING THE TEAM

- Talented junior staff
  - Requires long-term **investment**
  - Longer lead time*
  - Identifying aptitude is harder than tech skill

- Try:
  - Plan pay adjustment in out years
  - Build in time for training, mentorship, and research
  - Long-term career development

*YMMV

BUILDING THE TEAM

- Talented senior staff
  - Higher cost*
  - Less flexibility*
  - Hyper specialization*

- Try:
  - Look elsewhere in the org
  - Find “fishing holes”
  - Watch out for bias

*YMMV

BUILDING THE TEAM

- Ask about:
  - Influences
  - Ways of working/being managed
  - Failures

- Look for:
  - Participation – clubs, events, projects
  - Well-informed opinions
  - **Referrals**
  - Technical evaluations

TRAINING

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

- ✓ How to think
- ✓ How to communicate
- ✓ Investigative theory
- ✓ Business implications of cybersecurity

Start with your mission/business, threat model, envi

MOTIVATING & RETAINING

- ✓ No competition zone
- ✓ Task shifting (hero proofing)
- ✓ Celebrate small wins
- ✓ Promote collaboration & creativity
- ✓ Align to core values – Speed? Accuracy? Quality? Quantity? Ingenuity?

@markaorlando

Measuring Success: KPIs and OKRs

- KPIs instrument your operation
- OKRs tie ops to strategy
- Constantly re-evaluate both
- How will training and mentorship drive improvement in these?

Measuring Success: KPIs and OKRs

- Sample KPIs:
  - Coverage/visibility
  - Control
- Sample OKRs:
  - Reduce successful social engineering attacks
  - Reduce identification and response time

MEASURING PEOPLE

- Inform, learn and mature – not penalize
- Avoid solely quantitative measures
- Prepare them for future success
- Prepare them to handle change

MEASURING PEOPLE

- Great resources:
  - Analyst "baseball card" by Chris Crowley: https://www.first.org/resources/papers/conf2019/Public SOC-Metrics-for-FIRST-v07-002-.pdf - productivity, quality, growth
  - Read blog post by Chris Sanders on Infosec Careers and Tours of Duty: https://chrissanders.org/2019/07/infosec-tour-of-duty/

MEASURING PEOPLE

Analyst Baseball Card	
Christopher Crowley	Name
Chris	Preferred first name
TwoGuns	Callsign
2015-11-17	Join Date
NSM Analyst - Senior	Current Role
1 year, 1 month	Time in Role
38	Alerts Triaged in last 30 days
91.40%	Percent True Positive Rate
82.70%	Response rate percent for customer escalation
19	Escalated cases handled in last 30 days
1:34	Mean time to close case
7	Number analytics created currently in production
28	Number detection modified currently in production
423	Total lines committed to SOC code repository in last 90 days
91.40%	Success rate of queries against SIEM in last 30 days
0:09	Median run time per query
0.23	Mean lexical structure similarity in queries run in last 30 days

@markaorlando

WHEN A PLAN COMES TOGETHER

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

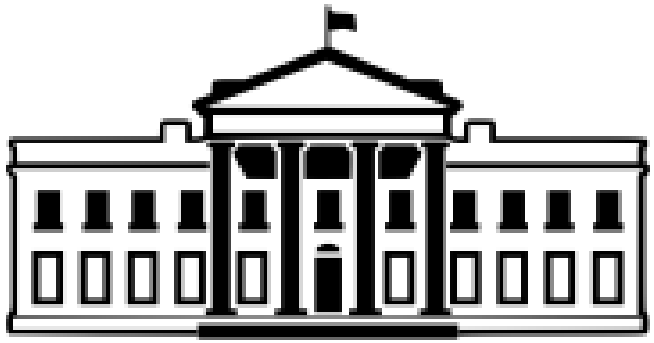
WHEN A PLAN COMES TOGETHER

Difference between an A-Team and "the other team" is cohesion and measurable results*

CASE STUDY:
24/7 EXECUTIVE BRANCH SOC

Challenges:

- Small budget
- Customer just wants things to work



Case Study: 24/7 Executive Branch SOC

- Tell stories that interest customer
  - State-sponsored activity
  - Targeted VIPs
- A-Team = intel focus to tell the story, engineering to save them from themselves
- You must be "smarter" than your customer to keep them engaged

CASE STUDY: BUILD AN MDR

Challenges:

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

CASE STUDY: BUILD AN MDR

- Find good fishing holes, start small
- Strong supporting functions: R&D, project management
- A-Team = utility players, good communicators, strong support team, generative environment

OTHER RESOURCES

- SANS SEC450: Blue Team Fundamentals
- SOC Summit Presentation Archive: https://www.sans.org/cyber-security-summit/archives/cyber-defense
- MITRE's "10 Strategies…": https://www.mitre.org/sites/default/files/publications/pr-13-1028-mitre-10-strategies-cyber-ops-center.pdf

HOMEWORK

- How are you protecting/enabling business value?
- What are your core values and how does your team personify them?
- Analyst baseball cards


THANK YOU