A new way of thinking…. Driven by intelligence
...the ability to gain victory by changing and adapting according to the opponent is called genius.

Sun Tzu – The Art of War
- Merge 3 teams into 1
- Create organizational direction & strategy
- Build world-class SOC
- Talent assessment
- Training curriculum
- Measure effectiveness

It's kind of fun to do the impossible.

Walt Disney
Old v. Different

TWO CHOICES
- Operations focused
- Reactive
- Remediation driven
- Network Defense
- Technology
- Design based on Mitre, Kill Chain, personal experience, and talent
- Can’t secure EVERYTHING!
- Change in thinking of entire SOC personnel
- Setting the foundation for intelligence automation
THE RESULT

Cyber Intelligence & Internal Threat
- Intel Collection, Analysis and Distribution
- Threat Assessments
- Internal Threat & Case Support

Threat Prevention
- Border Protection
- Sensor Tuning
- Policy Management

Threat Detection
- L1 - Call center (24x7x365)
- L2 – J&J Employees

Cyber Incident Management
- IR Coordination
- Forensic Artifact handling and analysis
Man v. Machine
Vulnerability focused
Threat focused
Training to think like criminals (Profile & Hunt)
Actions based on intelligence – Crowdsourcing
Stop operating within the BOX – Talk to the business

WHERE TO BEGIN?
In ancient times skillful warriors first made themselves invincible, and then watched for vulnerability in their opponents.

Sun Tzu
- Built one brick at a time
- Smaller is more nimble and able to understand the business
- Technology is Security’s problem
- Not always about money
Stop just reacting
Focus on industry and the specific threats aimed at your industry
Read industry specific intelligence sources
Keep your house clean!!!
  - Storage
  - Access control (least privilege)
  - Vulnerability Management

TIPS FOR ALL SIZE SOC’S
Press on. Obstacles are seldom the same size tomorrow as they are today.

Robert H. Schuller