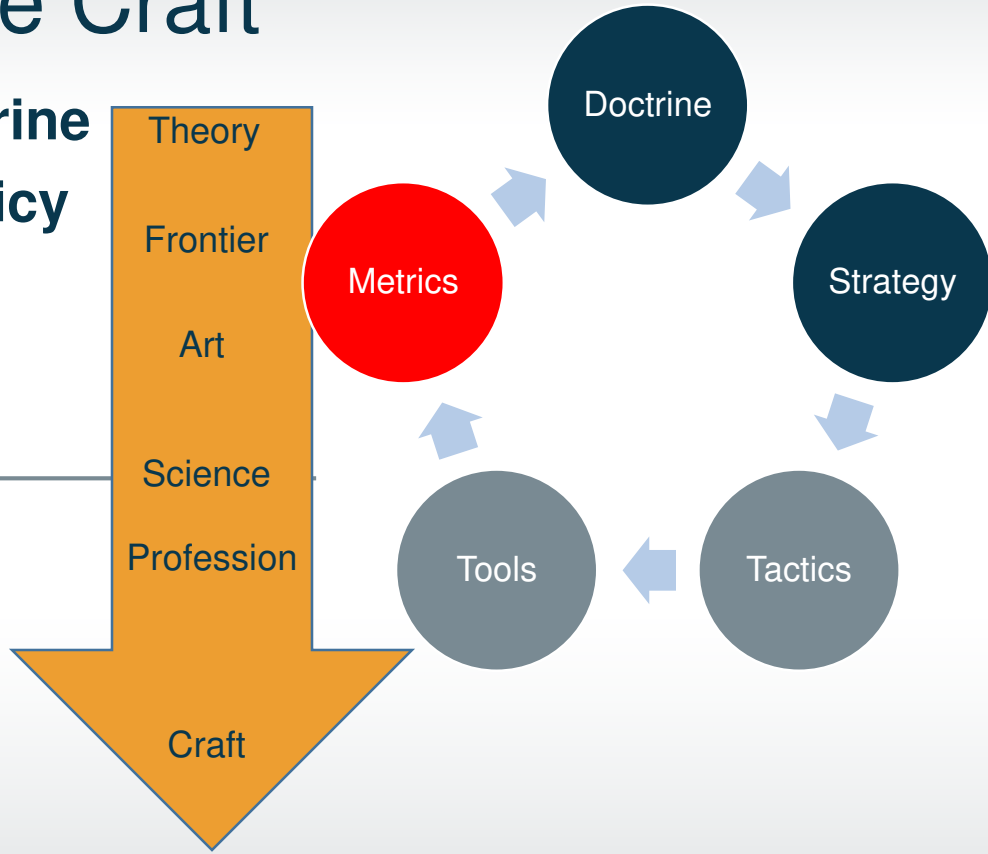
People > Machines

Charles Herring
Co-Founder, CTO

Characteristics of the Craft

- ✓**Established Concepts/Doctrine**
- ✓**Documented Strategies/Policy**
- ✓**Elite skills identified**
- ✓**Professional Development**
- ✓**Peer Review**

- Documented Tactics
- Tactical Tools
- Business Metrics
- Quality Assurance

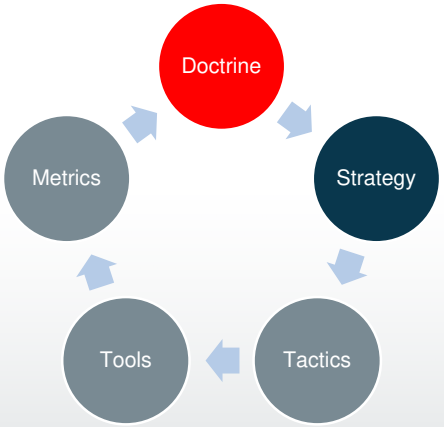


Charles Herring

- Ran IT Services for drug testing company
- Enlisted Active Duty in US Navy (1995-2005)
  - 6 years as F/A18 Avionics Technician
  - 4 years Network Security Officer at US Naval Postgraduate School
- InfoWorld Test Center for Network Security Reviews
- Solution Consultant for 7 years to DoD & State Department
- Consulting Security Architect at Lancope/Cisco 4 years
- Co-founder WitFoo & WitFuture Institute
- Master SCUBA diver

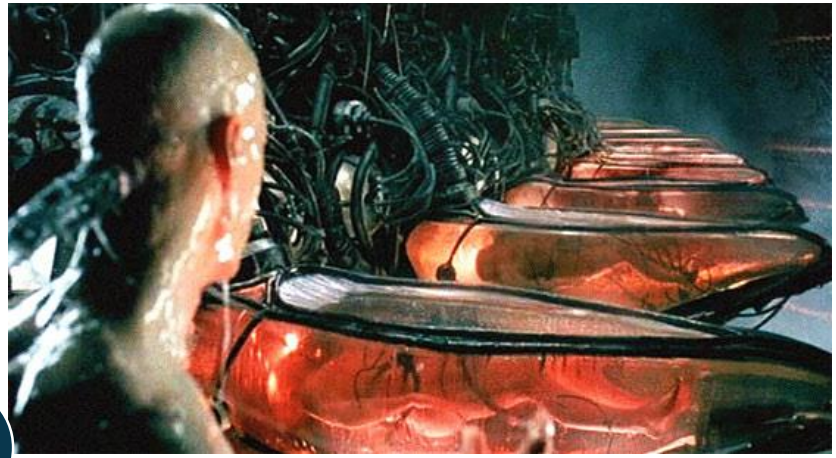
IDS is Dead; Long Live IPS

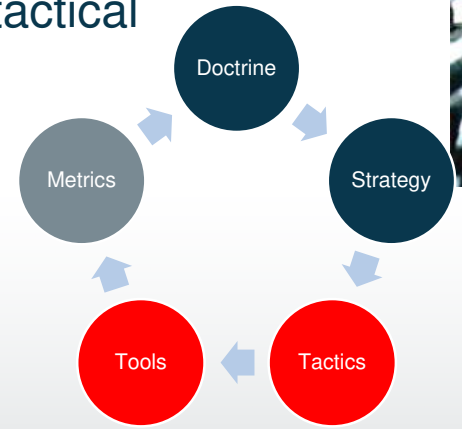
- 2002 Gartner Report
- CAPEX “Black Box” preferred over OPEX Security teams
- Delegation from Organizations to Vendors
- Incorrect Craft Fundamental: Doctrine



Machines driving Process

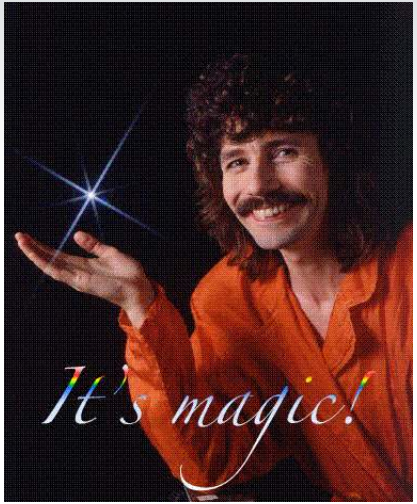
- Investigators inherited tools
- Tools pre-date process
- Tools “dictate” the work
- Incorrect Craft Fundamental:
  - Tools are not tactical

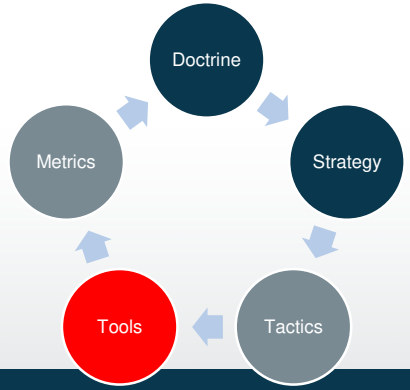




Terms

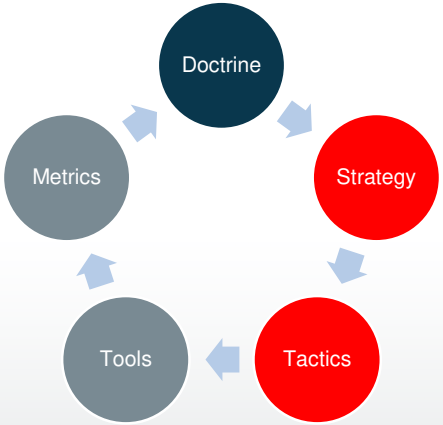
- Algorithm = Programming Function
  - Not magic
  - Quality and usefulness vary widely
- Machine Learning = Pattern Recognition
  - Young humans (toddlers & infants) can recognize faces
  - Very difficult for computers (CAPTCHA)





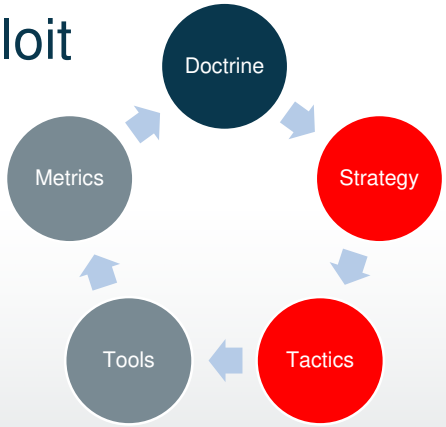
Challenges with AI

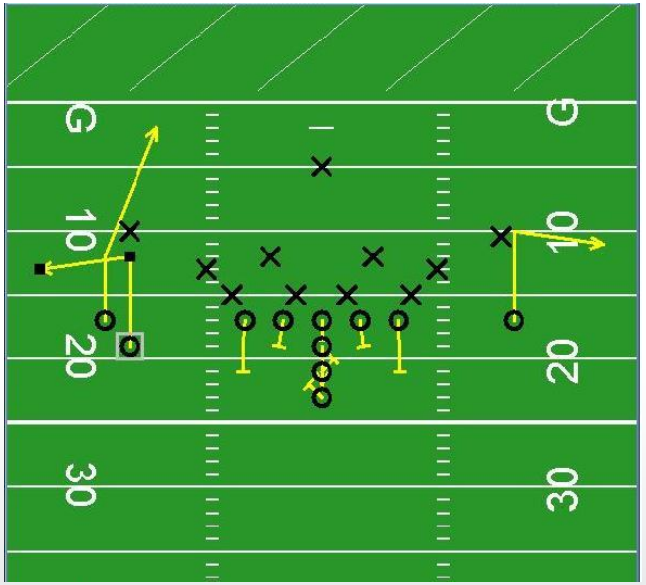
- Computers are binary; life is analog
  - Humans understand both; computers only binary
  - Humans understand the importance of range/shades
- Complexity in multi-dimensionality
  - Possible permutations
  - All facets of the human condition
  - Simple: auto bill pay; Complex: murder investigation
- Risk of calculation failure
  - Crashing cars; incorrect judicial decision



Playbook Automation Challenges

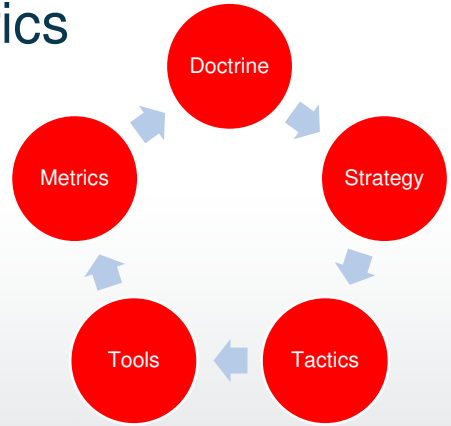
- Is only Boolean (flow chart)
- Does not account for complex cognition
- Requires every evolving playbooks
- Removes human review
- Allows for process exploit





Lessons from Law Enforcement

- Detectives, equipped by tools, investigate
- Tools are custom built from studying detectives
- Learn how to be detectives not criminals
- Systematic but flexible approach
- Success/failure metrics

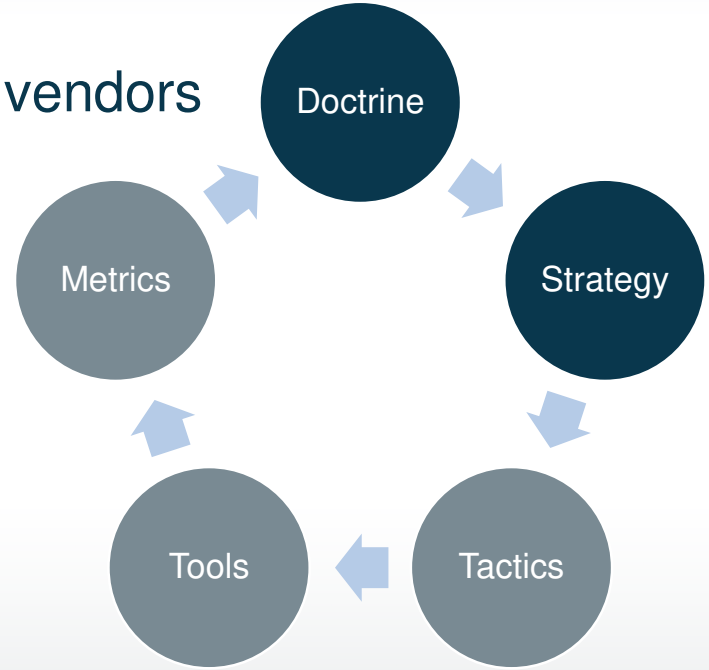


Relationship Strengths

People	Machines
• Pattern Reason • Adaptive Thinking • Cross-domain • “Gray Area” • Adaptive Query	• Pattern Recognition • Brute-force Action • Big-data processing • Human Emulation • Repetitive Query

What do we do?

- Document tactics
- Enforce tactics based requirements on vendors
- Metrics, metrics, metrics
- Perspective on feedback loop




witfoo
Security, Leveled Up.