Bringing Anthropology into Cybersecurity

Xinming Ou (University of South Florida), Michael Wesch (Kansas State University), John McHugh (RedJack), and Raj Rajagopalan (Honeywell)

CNS-1314925, TWC SBE TTP: Medium: Bringing Anthropology into Cybersecurity, $715,845, Sept 1, 2013 – Aug 31, 2017

Problem

- The researcher-practitioner chasm
- Undocumented operational security knowledge
- Lack of holistic perspective on operational culture

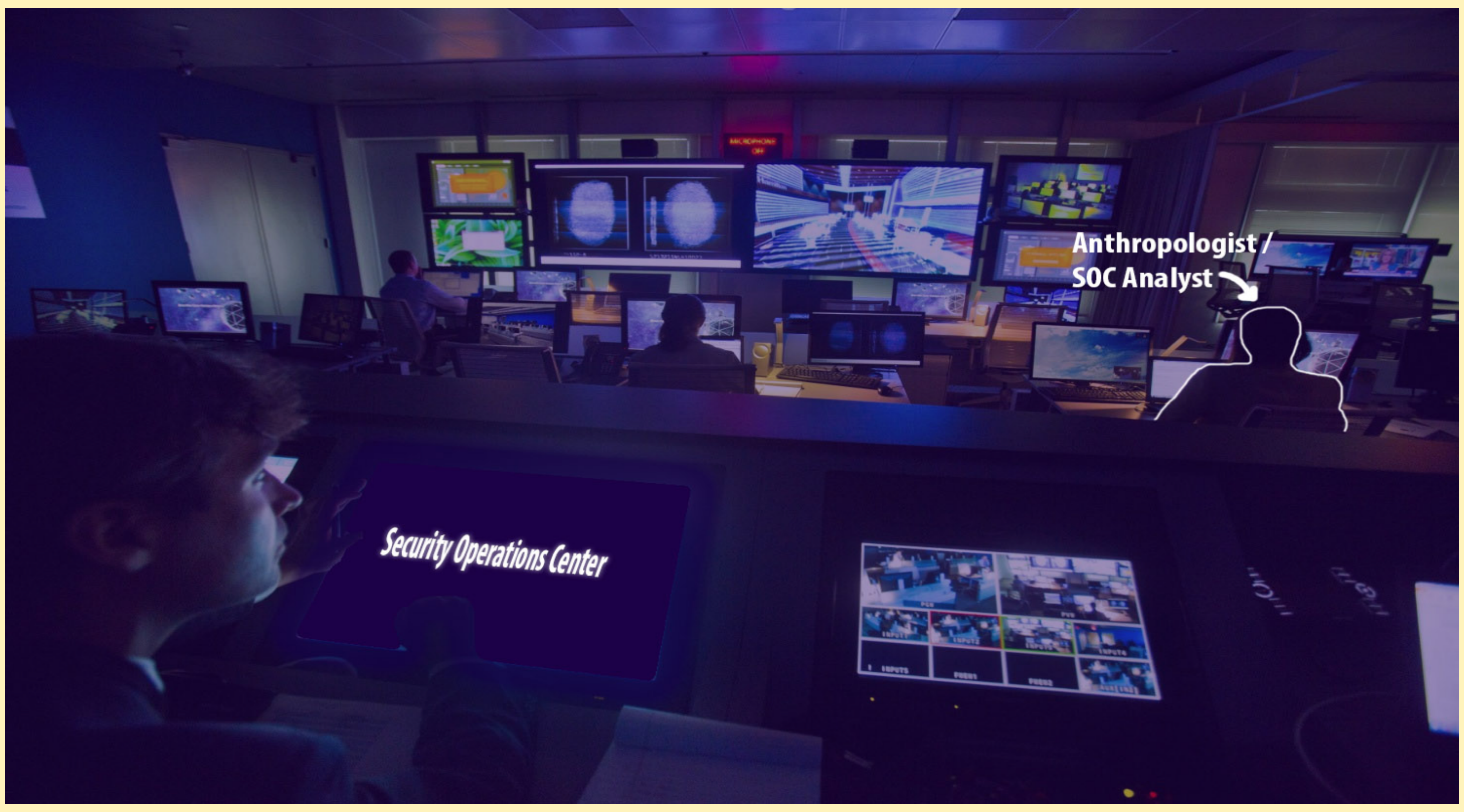
All these lead to inefficient tech transfer of security research

Methodology

- Embedded student in Security Operation Centers (SOCs)
- Played the role of observer (researcher) and the observed (analyst)
- Anthropologists call this *"participant observation"*
- Qualitative analysis of field notes
  - *Grounded theory & template analysis*

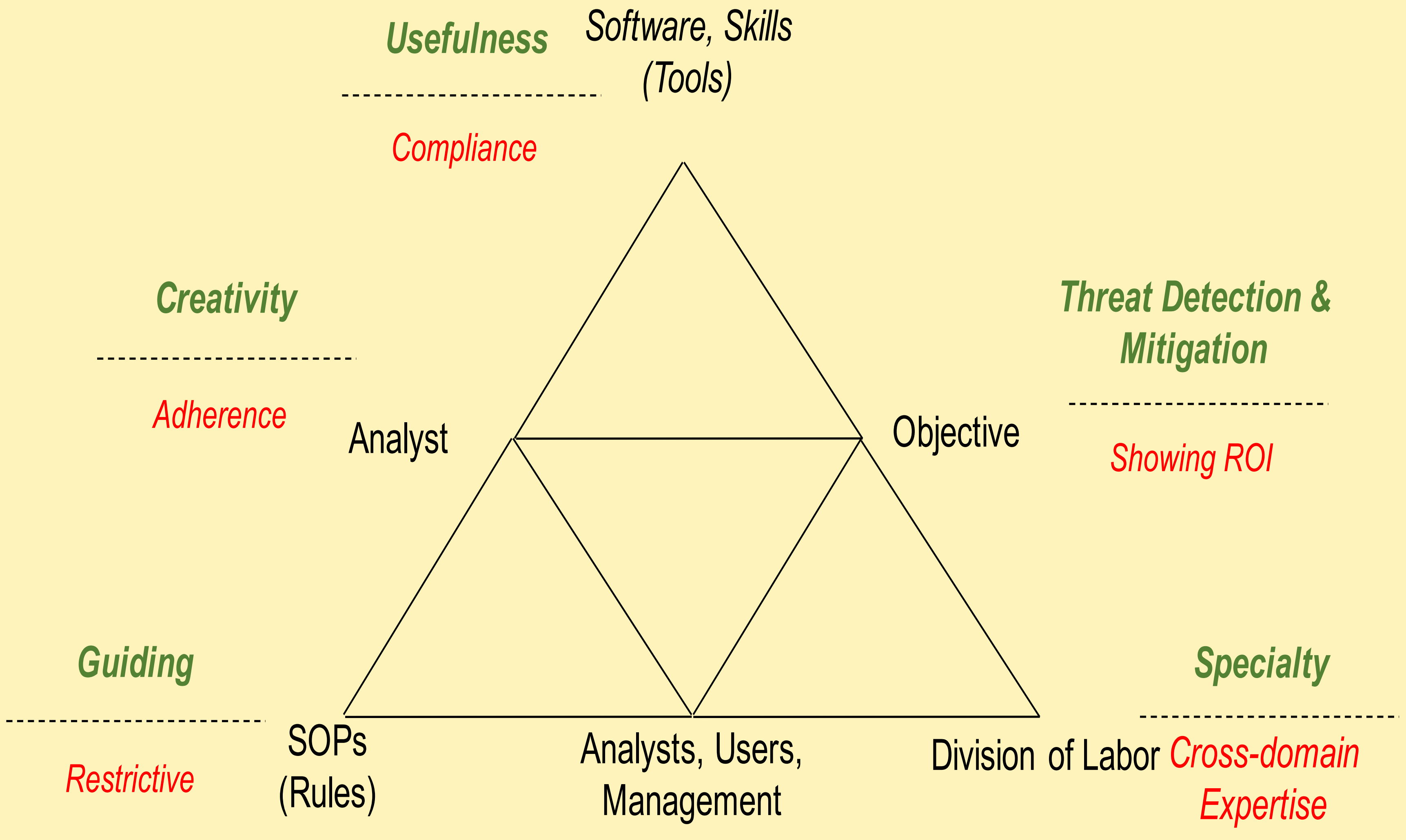
Our Efforts

- Four years of fieldwork
- Two academic and three corporate SOCs
- Multiple roles
  - Level-1&2 analyst, incident response, and software developer



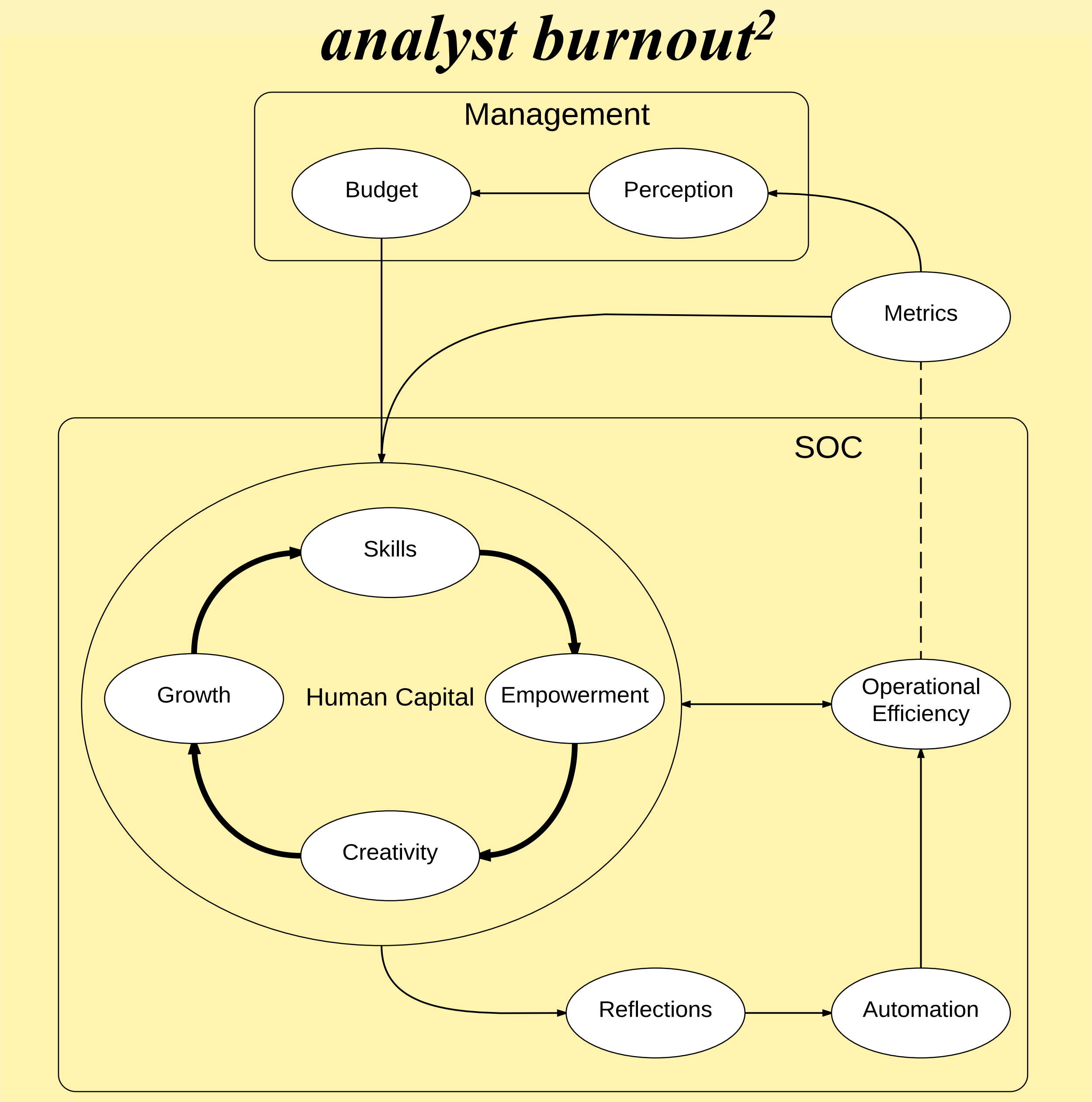
Findings

A SOC is a system of contradictions[1]



But contradictions can be sources of innovations!

Human capital mismanagement leads to analyst burnout[2]



But proper metrics and incentives can change that!

1. Turning Contradictions into innovations or: How we learned to stop whining and improve security operations. *Twelfth Symposium on Usable Privacy and Security (SOUPS'16).*
2. A human capital model for mitigating security analyst burnout. *Eleventh Symposium on Usable Privacy and Security (SOUPS'15).*
3. A tale of three security operation centers. *CCS Workshop on Security Information Workers'14.*
4. An anthropological approach to studying CSIRTs. IEEE Security & Privacy Special Issue on CSIRTs'14.
5. Designing forensic analysis techniques using anthropology. *New Security Paradigms Workshop (NSPHD track)'13.*

Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia