Bringing Anthropology into Cybersecurity

Challenge:

- Security research efforts fall short of real-world needs
- Chasm between security researchers and practitioners

Scientific Impact:

- Understanding of security operations as complex and dynamic human/technology/ management interactions
- Extracting tacit practitioner knowledge enables creation of useful analytical tools

Methods

- Four years of participation in five security operations centers (SOC)
- Anthropologists call this “participant observation”

Broader Impact:

- Research output benefits SOC operations
- Expedite technology transition

Award: CNS-1314925 PIs: Xinming Ou (USF), Michael Wesch (Kansas State), John McHugh (RedJack, LLC), Raj Rajagopalan (Honeywell)