IMPROVING SOC EFFICIENCY THROUGH ANTHROPOLOGY:

A security operation center (SOC) is a workplace where security analysts work to handle the various types of tasks/events related to the security status of an organization's information technology infrastructure.

- Core Proplems
  - Low efficiency of SOC operation, lack of transparency into incident handling processes
  - Shortage of workforce and lack of systematic training for SOC analysts, made worse by the high turn-over and stressful working conditions
  - Commercially available tools not addressing operational needs
- Goals of Research
  - Make the "tribal knowledge" of SOCs explicit and shareable, by embedding researchers with SOC analysts.
  - Use fieldwork to discover workflow – fieldworkers co-build tools with SOC staff to improve its efficiency.
  - Compare recurrent patterns across multiple SOCs to separate intrinsic from incidental problems
  - A training manual for organizations that employ SOC personnel in corporate, academia, and governmental agencies.
- The Research Team Provides
  - Training for individuals in the host organization on fieldwork methods, OR Interns trained in security and anthropology to conduct fieldwork
- Collaborators Provide
  - Appropriate access for intern(s) or fieldworker(s) to SOC and SOC staff
  - Workflow and role descriptions
  - (Optional) financial support for the fieldworker
- Benefits for Collaborators
  - Third-party perspectives on SOC effectiveness
  - Tools fieldworkers build together with analysts specifically for the collaborating SOC
  - Framing and prioritization of issues to be addressed in the training manual as well as early access to learning
  - Opportunity to seek joint funding for further research

If interested, please contact soc-collaboration@arguslab.org

This research is supported by the National Science Foundation under Grant No. 1314925. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Honeywell

Kansas State
College of Engineering
Computing and Information Sciences

REDJACK