A Collaborative Visual Analytics System for Cyber Defense Analysis

Lindsey Thomas, Zach Courtney, Adam Vaughan, Dr. Chen Zhong, Dr. Awny Alnusair
Informatics, Indiana University Kokomo

Background
- Cyberattacks become more sophisticated.
- Many organizations have built their own Security Operations Centers (SOCs).
- SOCs rely on (1) Cyber defense technologies: Firewall, Intrusion Detection, System (IDS), etc
  (2) Human Analysts

Motivation
- Existing research aims to develop better cyber defense technologies.
- Few focus on the human side:
  (1) Cyber defense analysts are playing an extremely important role.
  (2) Their responsibilities include detecting “real signals” from the massive data set and making decisions accordingly.
  (3) Currently they are overwhelmed by the massive data set.
  (4) They usually have to collaborate to accomplish a task.
- A big need for a supporting system that facilitates analysts’ collaboration.

Our Approach

Case Study 1: Brainstorming

Case Study 2: Collaboration

Conclusion
1. Enhances time efficiency when analyzing cyber attacks.
2. Enables effective collaboration within teams.
3. Utilizes each analyst’s professional skillset.

Future Work
1. Implement a better search feature.
2. Test using actual human subjects.
3. Develop a prototype.

References