CERIAS
The Center for Education and Research in Information Assurance and Security

Information Alignment and Visualization for Security Operations Center Teams

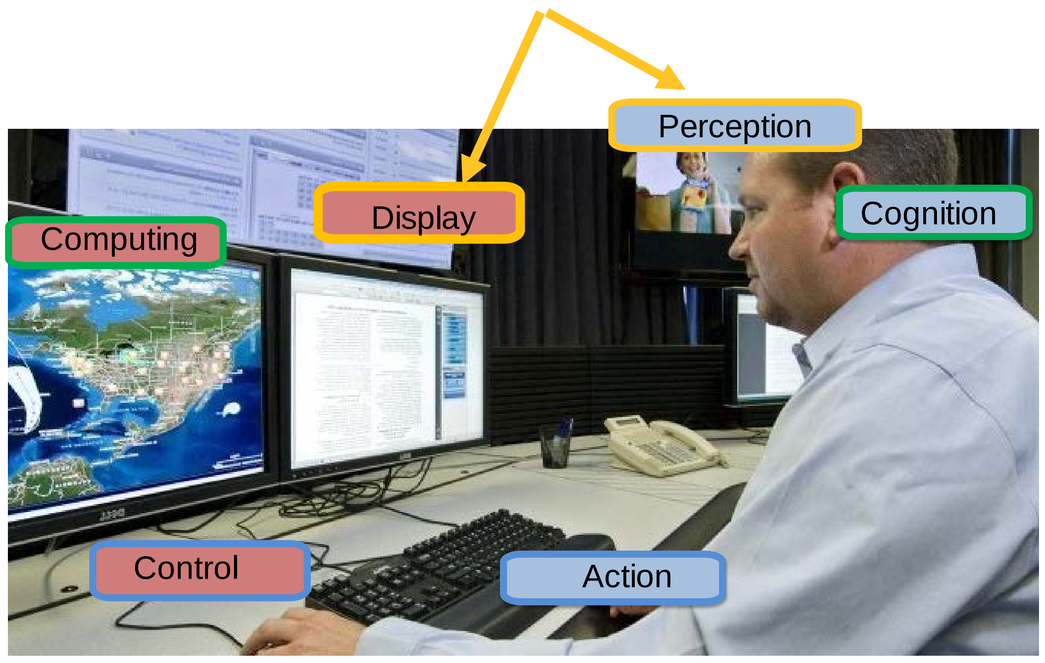
Omar M. Eldardiry, PhD Candidate; Mallorie J. Bradlau, PhD Student; Barrett S. Caldwell, PhD

ABSTRACT

The development of cyber network operations centers (NOC) has created new needs to support human sensemaking via improved information alignment and visualization. This poster focuses on information needs and gaps involving network operations centers (NOCs) and security operations centers (SOCs) analyst personnel. Our goal is to enhance analyst sensemaking and usability of tools to assist security analysts in monitoring, managing and protecting their networks from suspicious activities. This project has proceeded in several stages. Based on previous interview findings, an in depth investigation and job shadowing was conducted with different SOC teams. The findings highlighted three promising areas of improvements for NOC and SOC tools to improve network operations sensemaking, team performance, and organizational information alignment.

HUMAN-MACHINE INTERACTION

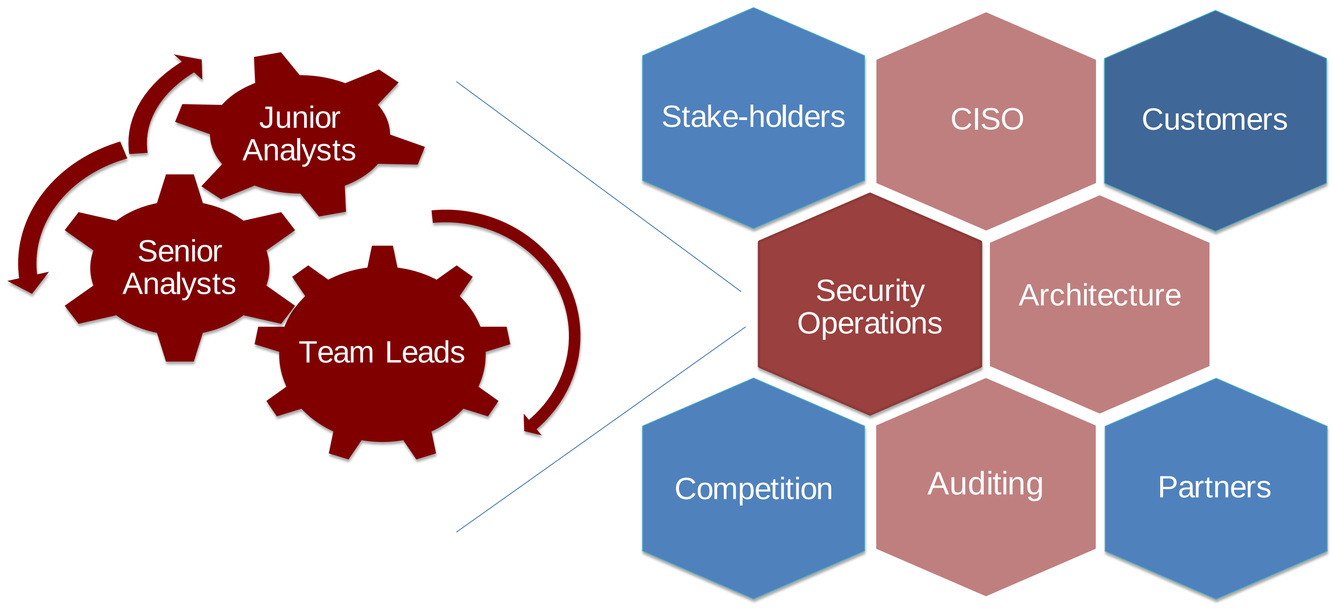
The Human-Machine Interaction Model is displayed here, with the study focus being on human perception and computer display of information in security operations



www.defenseone.com/technology/2015

SYSTEM DIAGRAM

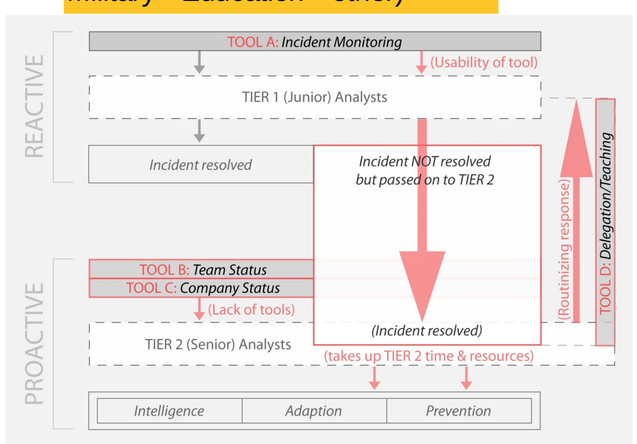
The research studies interactions between analysts within operations . Another aspect of the study considers information flow between operations and other entities both inside and outside the organization



METHODS

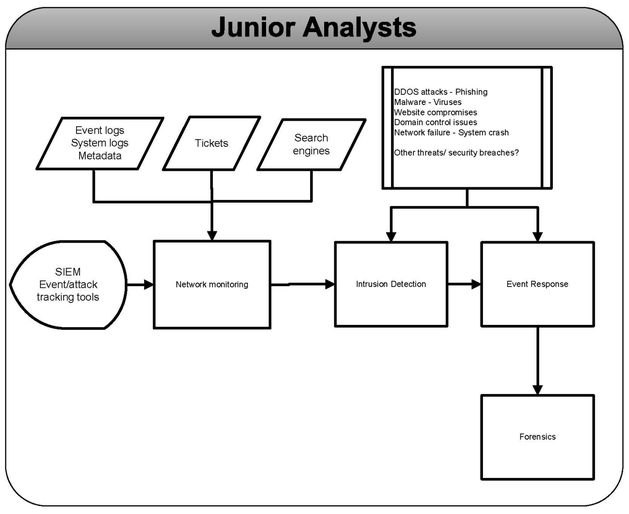
1. Project Scope

RSA Conference - Pilot Study
Network and Security Operations
Different field applications
(Manufacturing - Commercial - Military - Education - other)



2. User Research

Manufacturing SOC
In-depth Interviews
Analyst Shadowing
Goal-directed Task Analysis



3. Gaps

- Information Alignment
- Knowledge Sharing
- Team Collaboration
- Process Quantification
- Performance Measurement

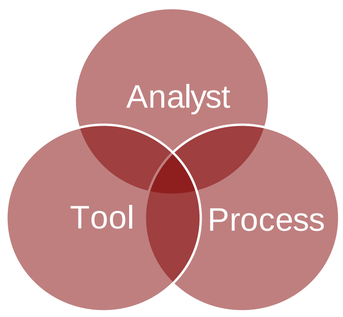
4. Future Work

Visualization Tool:
- Design Requirements
- Prototyping
- Usability Testing
- Implementation

PLANNED RESULTS

Improve understanding of information and knowledge flows between SOC team members

- Improve information visualization tools to increase understanding and reduce time to response
- Reducing on-boarding time
- Recognizing opportunities for automation and improve efficiency
- This will lead to optimizing work flow in the SOC
- Enhancing team performance and effectiveness



PURDUE INDUSTRIAL ENGINEERING
GROUPER LABORATORY
The GROUPER Lab seeks to improve how people get, use, and share information.

CERIAS
PURDUE UNIVERSITY