Information Alignment and Visualization for Cyber-Physical Network Operations Center Teams

Omar Eldardiry, PhD Student

School of Industrial Engineering

Purdue University

December 3rd 2014

PURDUE ENGINEERING Think impact.™

GROUPER LABORATORY

CERIAS®

Center for Education and Research in Information Assurance and Security

Funding

Center for **E**ducation and **R**esearch in **I**nformation **A**ssurance and **S**ecurity

www.cerias.purdue.edu

PURDUE ENGINEERING Think impact.

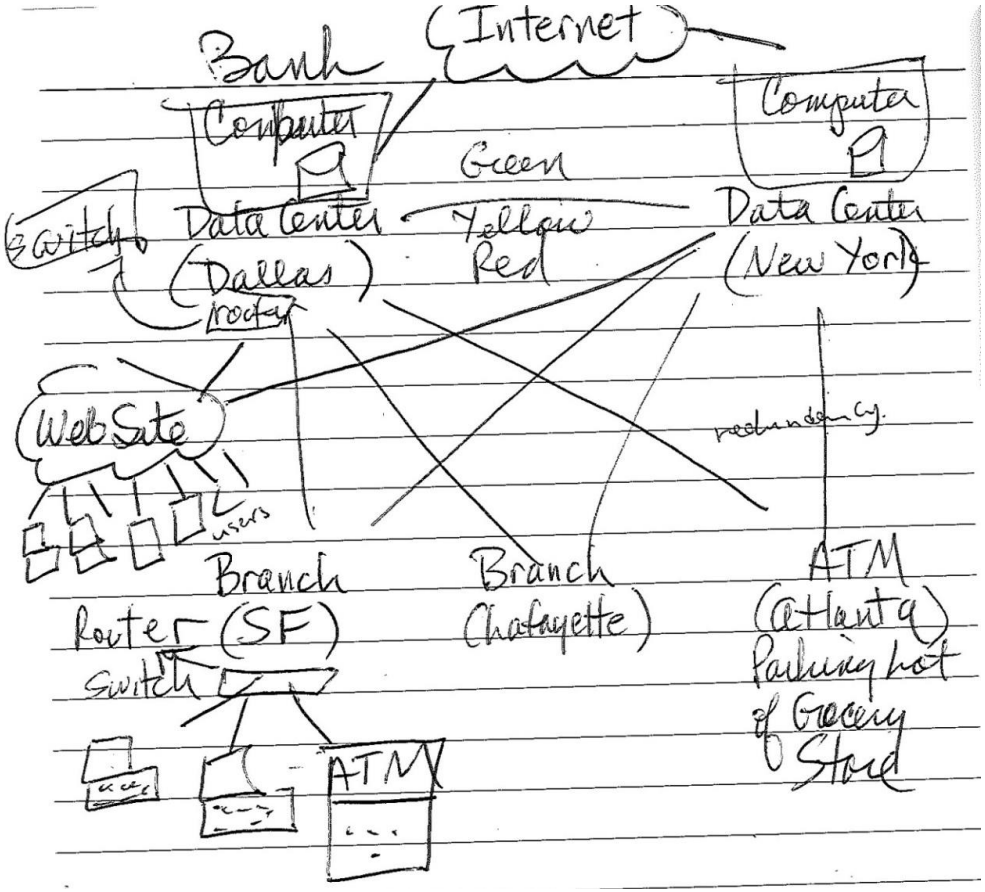
GROUPER LABORATORY

CERIAS Center for Education and Research in Information Assurance and Security

Introduction

Dedicated Teams to control and manage enterprise information systems and networks

Bank Network



PURDUE ENGINEERING Think impact.

GROUPER LABORATORY

CERIAS Center for Education and Research in Information Assurance and Security

Human Factors Engineering Problem

Situation Awareness (SA) is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future. (Endsley, 1988)

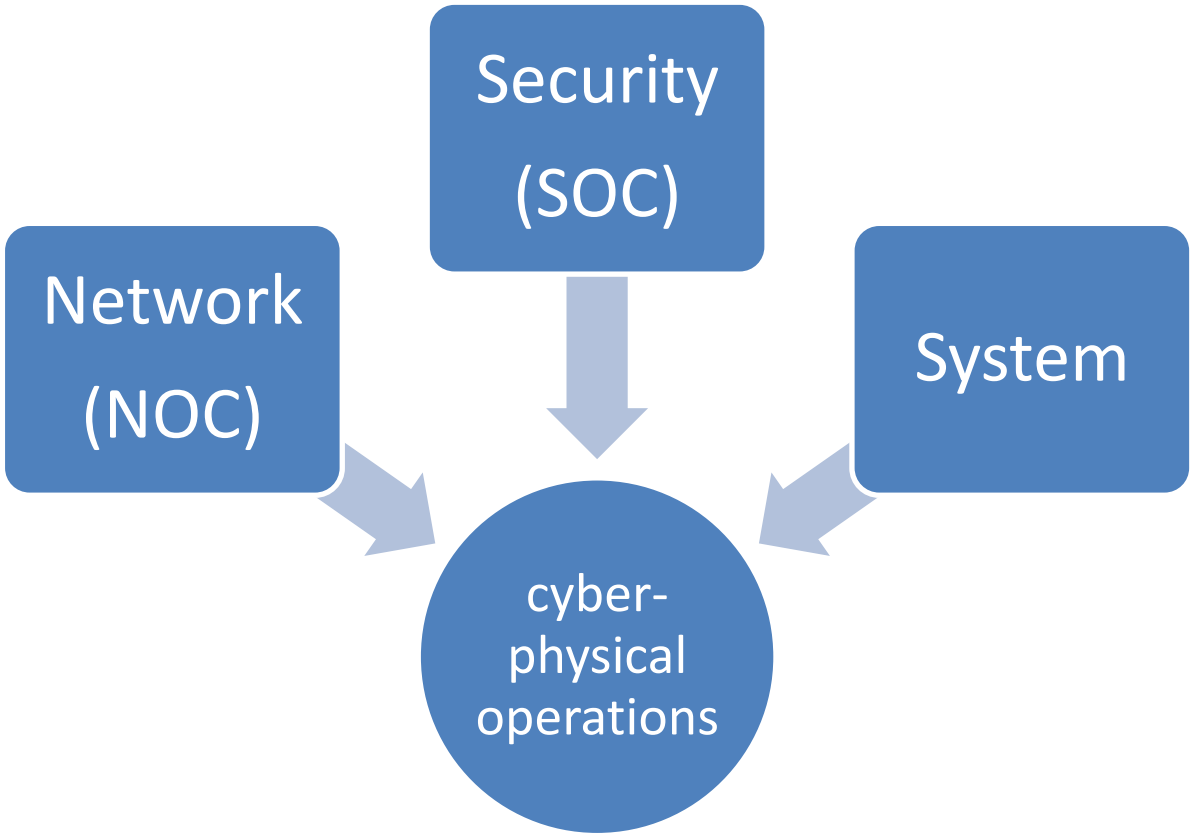
Levels of SA:

1. perception 2. comprehension
3. projection *4. resolution* (McGuinness & Foy, 2000)

Functional Requirements of SA in network Security

- information visualization (Onwubiko, 2009)

Cyber Physical Operations



Network Operation Centers (NOCs)

Network health and performance

1. Mediterranean (Jan 2008)
   Scuba Divers Fiber-Optic Cables cuts

2. United Airlines (Nov 2012)
   Computer system breakdown

PURDUE ENGINEERING Think impact.™

GROUPER LABORATORY

CERIAS Center for Education and Research in Information Assurance and Security

Security Operation Centers (SOCs)

Confidentiality, Integrity, and Availability

1. Multiple Retailer Credit Systems (2013-14)
   Target, Home Depot, Staples…

2. Yahoo Mail Accounts (Jan 2014)
   Breach of 273 million user accounts

Pilot Study

- Exploratory subjective data collection
- RSA Conference 2014
- Diversity (applications and functions)
- 10 to 30 years of IT working experience

Goal

Understand the goals, practice, challenges of analysts

Highlights

- NOC and SOC commonalities (Big data, Dynamic, Event driven, Collaboration)
- NOC and SOC integration/ separation

Case Study

Goal

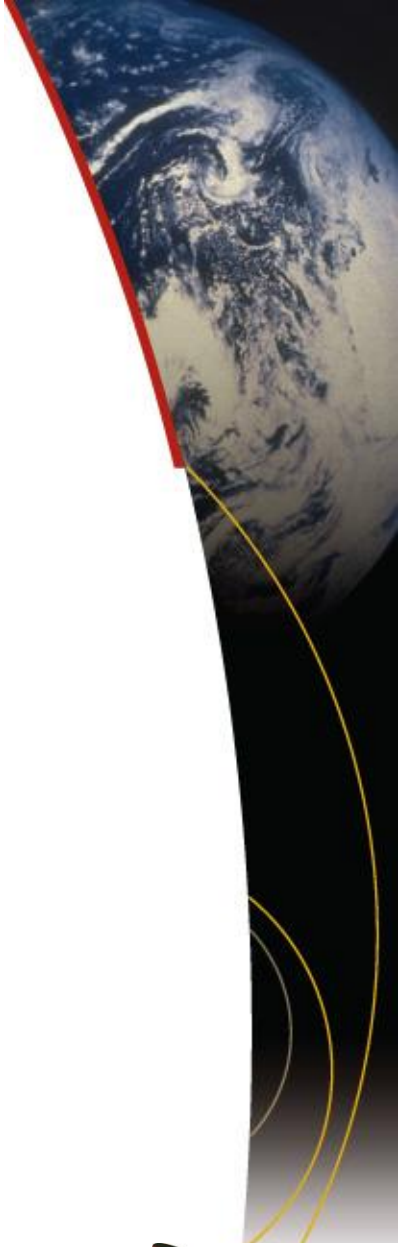
1. Analysts gaps in sense making
2. Visualization features to mitigate the gaps

Layout

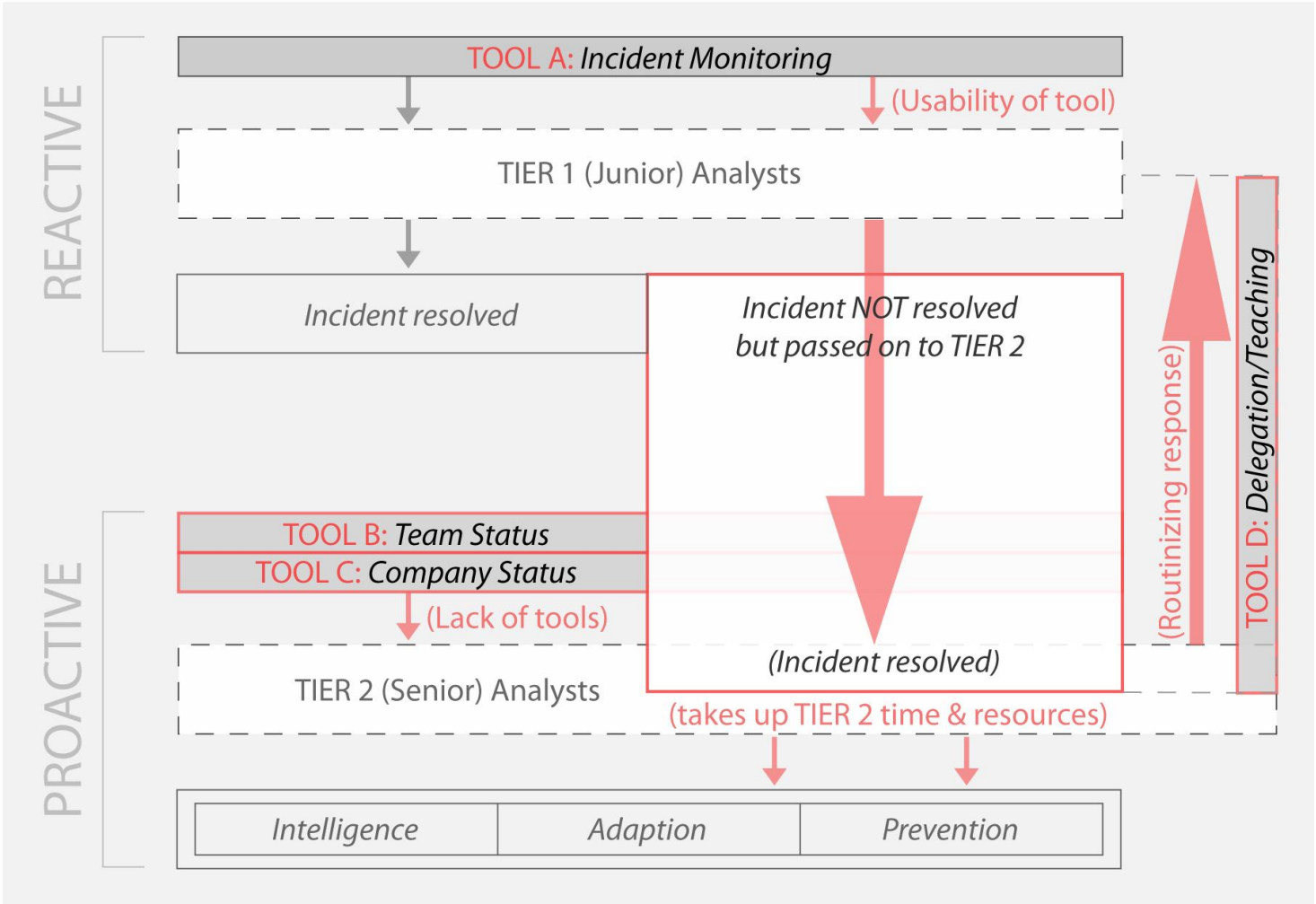
- SOC of a manufacturing enterprise
- attending team meetings
- job shadowing
- Six in depth interviews (one junior analyst, three Senior analysts , team lead, SOC manager)

Identified Gaps

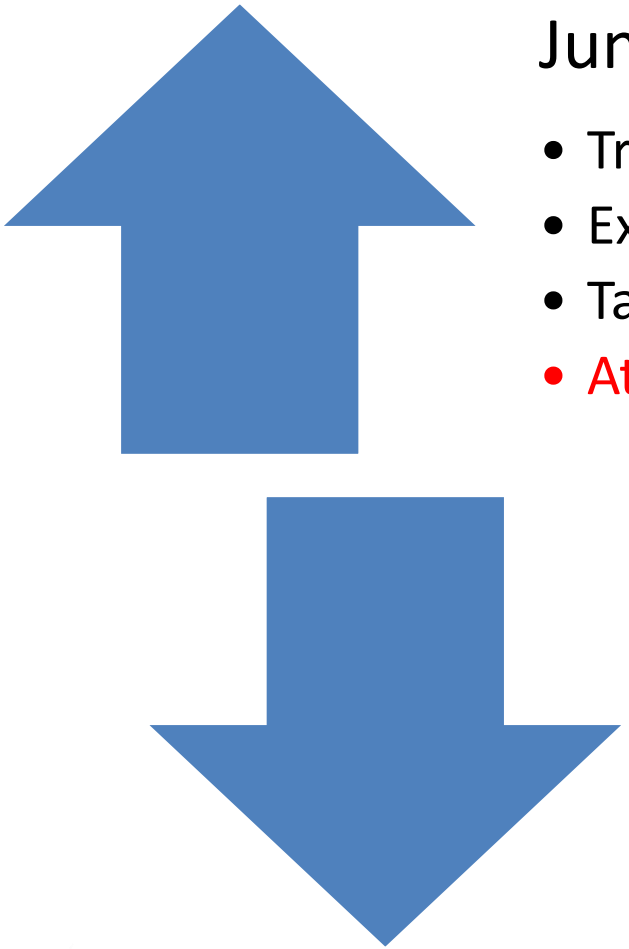
1. Information Alignment and team SA
2. Knowledge Referencing
3. Performance Management



1. Information Alignment



2. Knowledge Referencing



Junior Analysts

- Training
- Expertise Development
- Task Escalation
- Attrition

Senior Analysts

- Investigation
- Innovation
- Non-Routine Events
- Interruptions

2. Knowledge Referencing

Benefits

- Spreading expertise
- Awareness of team activity
- Integration from rare to frequent

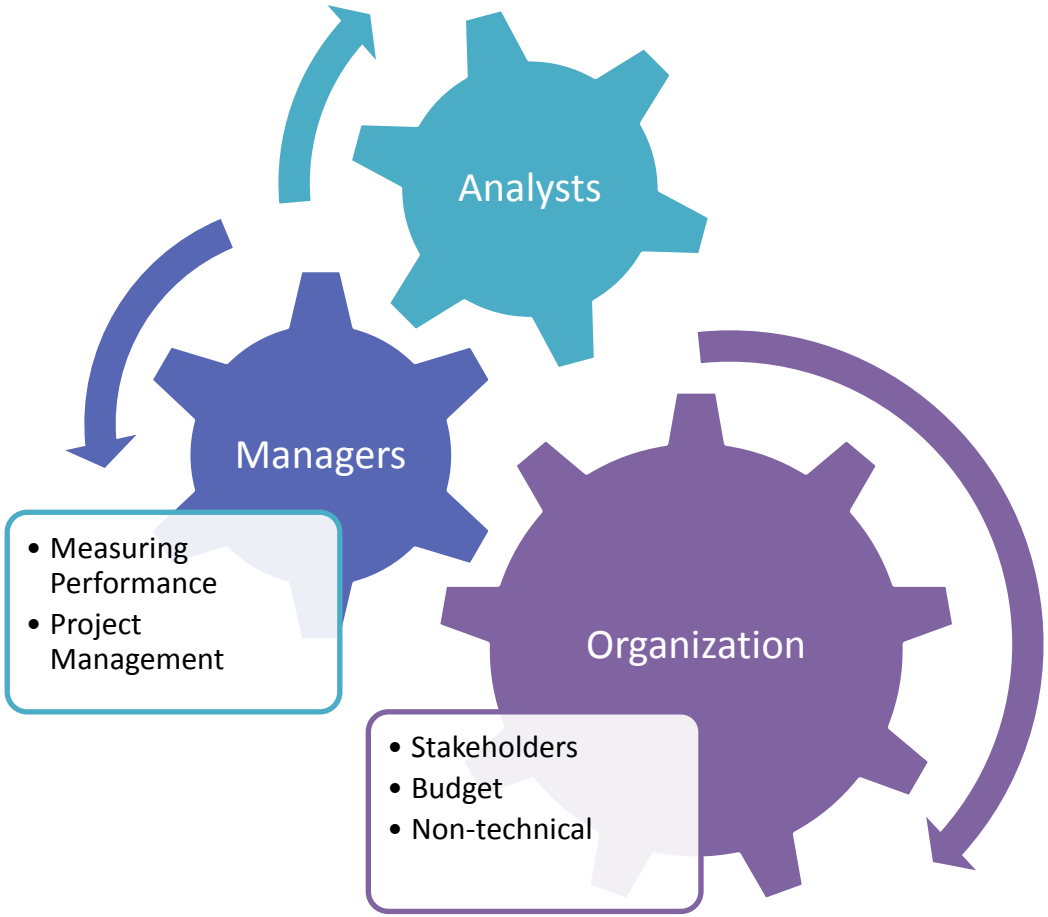
Costs

- Interruptions degrade senior analyst performance

  Interruption affects productivity and reduces the quality of final outputs (Foroughi et al., 2014)

- No time to formalize
- Lack of formulation degrade junior analyst contribution

3. Performance Management



PURDUE ENGINEERING Think impact.™

GROUPER LABORATORY

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

Projected Outputs

Tool 1: Information Alignment and Team Situation Awareness

- Added features in existing tools
- Improved team SA, responsiveness

Tool 2: Management of Team Performance

- New tools to quantify operational performance
- Improve communication with non-technical personnel

Tool 3: Operational Knowledge Referencing and System Teaching

- Delegate tasks to junior analysts – Knowledge Capture
- System automation

Outstanding Tasks

- More in depth **Case Studies** (RSA operations, IU NOC/SOC groups, Purdue ITAP)
  - Junior/ Senior Analyst
  - Goal Directed **Task Analysis** (GDTA)
  - SA requirements for NOC/SOC leads
  - Task Capture for defining and delegating routine tasks from leads to analysts
- **Prototyping** & **Usability Testing**

Our Critical Recognition

Lack of information alignment, situation awareness or team performance status in a NOC/SOC **is**, *per se*, **a SOC/NOC vulnerability**

1. tier **1** analyst performance is bounded by **usability of incident monitoring tools**

2. tier **2** analyst performance is bounded by limits in **delegating** to tier 1 and **lack of status/ context tools**

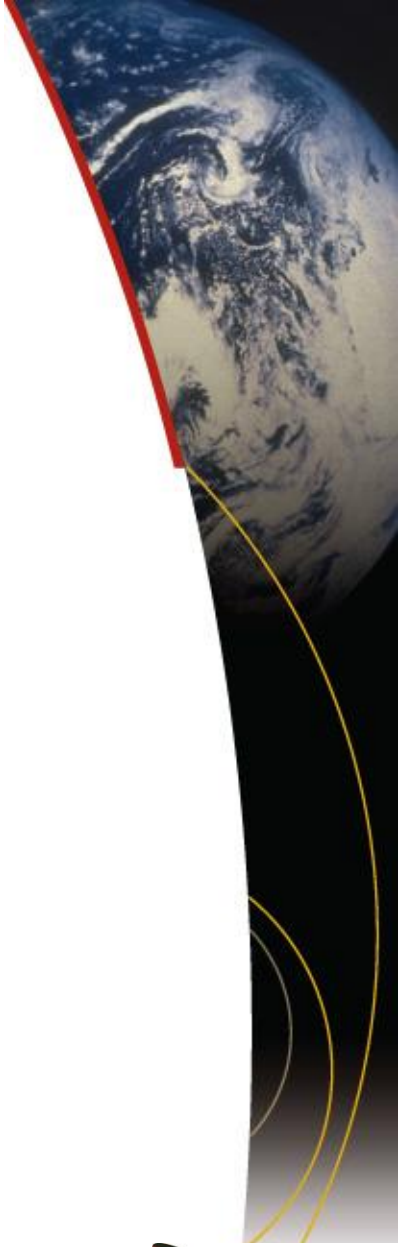
QUESTIONS?

Omar Eldardiry

- eldardiry@purdue.edu

Prof. Barrett S Caldwell

- bscaldwell@purdue.edu



PURDUE UNIVERSITY

GROUPER LABORATORY

CERIAS

Center for Education and Research in Information Assurance and Security