CERIAS

The Center for Education and Research in Information Assurance and Security

Enhancing Analyst Situation Awareness and Event Response in Cyber Network Operations Centers

Omar M. Eldardiry, PhD Student; Barrett S. Caldwell, PhD

ABSTRACT

The development of cyber network operations centers (NOC) has created new needs to support human sense-making and situation awareness in a cyber network common operating picture (CNCOP).

The goal of this research is to identify critical features that support expert analysts in event detection, identification, and response to cyber events (emergency scenarios, hardware break-downs or other sources of degraded perform-ance), and to improve information visualization to support recognition and response to cyber- and cyber-physical network events.

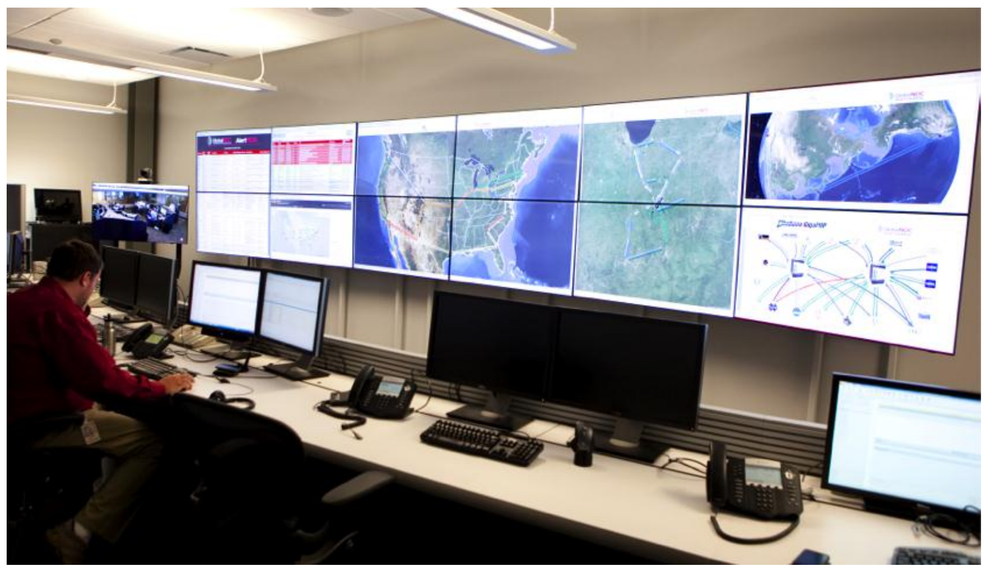
The results of this research project will be used to improve operational capability and analyst situation awareness in NOC environments and provide design guidance to improve analyst event monitoring and response in other cyber-physical infrastructure operations centers.

RESEARCH QUESTION

A great source of “Big Data” is the logs and alerts generated within an enterprise and kept for compliance or incident response reasons. How can security-relevant events best be displayed and visualized to highlight abnormalities and help analysts focus their time and efforts on those events most critical to the enterprise?

RESEARCH SIGNIFICANCE

Security Breaches	Description
Indiana University Unsecured Student Records, February 2014	Employee notices nonfunctioning security patch affecting access to 146,000 encrypted university student records
Yahoo Mail Accounts Stolen, January 2014	Yahoo mail usernames and passwords were hacked. Yahoo did not reveal how many of its 273 Million users’ data was breached. Possible bank accounts theft since many use same ID for their bank accounts
Target Data Breach, December 2013	Millions of customers’ personal information was stolen. As a result, Target profits decreased by 46%
Hardware Breakdowns	**Description**
Tornado hitting Indiana and the Midwest, November 2013	Tornado caused power outage and damage to hardware affecting the internet and mail servers at Purdue University campus
Fiber Cuts in the Mediterranean, March 2013	Scuba-Divers accidently cut cables affecting Europe connections with Africa, the Middle East and parts of Asia
United Airlines Operations Center Breakdown, November 2012	A Computer Breakdown in the central operation center affected thousands of customers due to delays in more than 250 flights.



Global Network Operations Center – Indiana University

METHODS

1. Conduct individual interviews with experts in the field and NOC analysts at different operation levels
2. Conduct Goal Directed Task Analysis to determine the Situation Awareness (SA) Requirements for the analysts.
   a. Construction of goal hierarchies drafts
   b. Refine drafts, evaluate and make corrections/ additions by analysts
   c. Analysis of hierarchies to identify information requirements
3. Develop prototypes of suggested designs and modifications to the displays
4. Test and improve the proposed prototypes and measure the analysts’ SA and evaluate potential improvements

PURDUE INDUSTRIAL ENGINEERING

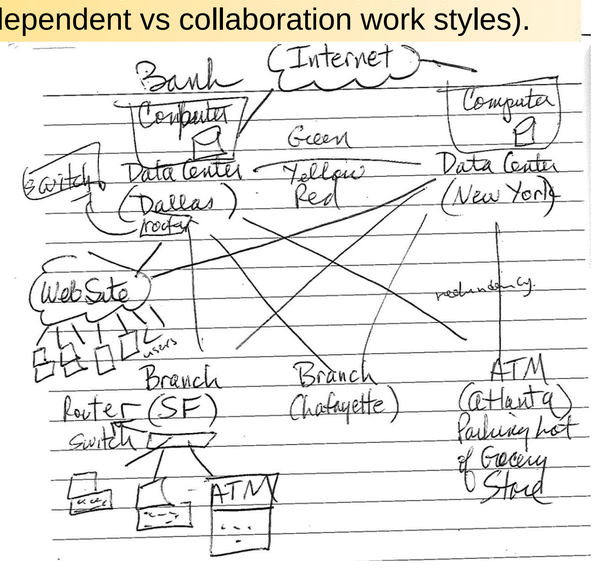
GROUPER LABORATORY

The GROUPER Lab seeks to improve how people get, use and share information.

PRELIMENARY RESULTS

Eight experts were individually interviewed during The RSA Conference (San Francisco, Feb 2014). The interviews helped determine the types of information NOC analysts need to fulfill their job requirements, the events that generate this information, the external manifestations that affect the work environment, what information analysts wish to have to minimize the effect of such interruptions, how work is divided among the analysts (e.g., physical separation, by expertise) and the work style (e.g., independent vs collaboration work styles).

The figure on the right shows a map of a bank network. It was drawn by one of the interviewees while discussing the elements of the network that should be monitored by analysts working in a bank’s NOC. The interviewee worked in the field of security for 32 years. During the interview, she emphasized the importance of visualizing the whole network as well as finer details, how analysts should understand where the critical activities happen within the network, and the wide variation of work responsibilities of analysts with different levels of expertise.



An interviewee drawing of a bank’s network map

INTENDED OUTCOMES

1. Efficient Use of Visual Displays	Minimizing information redundancy, categorizing information (potential threats, status updates, etc.) to be displayed on large wall screens or small desk screens
2. Knowledge Sharing	Integration and sharing of expertise across operation levels. Enabling senior analysts of documenting and standardizing work procedures for junior analysts
3. Recognizing Prototypical and Anomalous Situations	Determining cues of recurring incidents and cues of incidents with prime importance to facilitate tasks prioritization and goal switching

CERIAS

PURDUE UNIVERSITY