

Cyber Situational Awareness:

The Integration and Role of Visualization in Information Assurance Operations

Robert J. Bagnall

RobertB@SecureDecisions.com

(202) 302-1900

Secure

DECISIONS

A Division of Applied Visions, Inc.

Contents

- Introduction
- Results of CTA and other Studies of Analysts
- The Advantages of Visualization in Incident Handling
- Issues Impacting Visualization's Effectiveness
- A Novel Approach to Incident Handling Visualization
- Future Approaches to Incident Handling in the Visualization Space
- Conclusions & Questions

Introduction

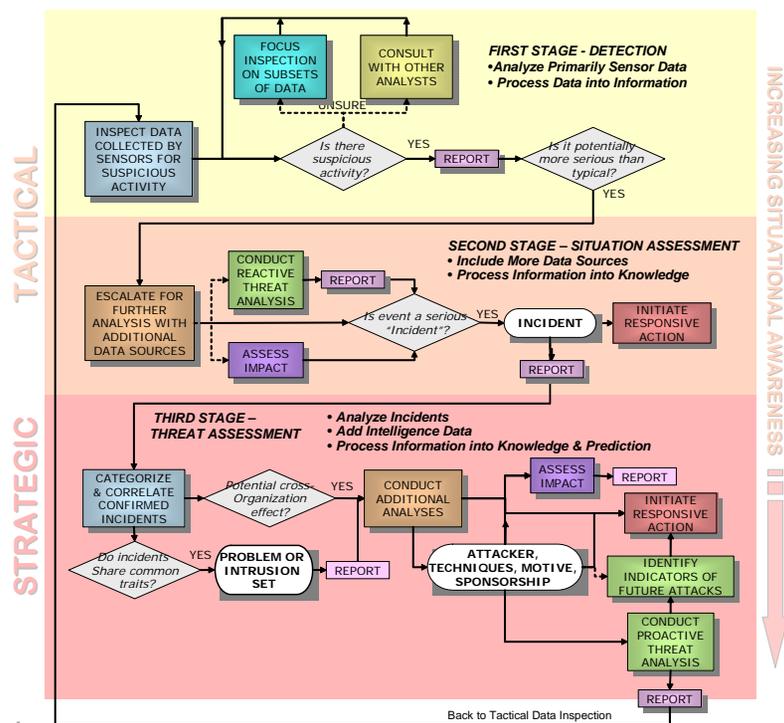
- Robert J. Bagnall
 - Senior Systems Analyst
 - 13 Years USAF Intelligence
 - 10 Years Building & Running CERTs

- Secure Decisions
 - Intelligent Visualization Company
 - Increases the Value You Derive from Security Investments
 - Improves Situational Awareness and Decision-making



Cognitive Task Analysis (CTA) Examined the Multiple Tactical & Strategic Roles of IA Analysis

- ❖ Studied 41 analysts at 6 sites (5 DoD and 1 MSSP)
- ❖ Results uncovered *how* IA analysts:
 - Detect suspicious activity amidst millions of data points
 - Mentally correlate seemingly disparate incidents across enclaves
- ❖ CTA identified specific cognitive challenges and obstacles that can be addressed through improved technology & policy



Products of project

- Model of 3-stage IA analytic process
- Clarification of IA analysis roles based on what analysts do, not on job titles
- Comprehensive resource for future training, metrics, and research
- Scenarios for framing R&D
- Recommendations - technical & policy
- Analyst-driven design of new visualization suite

Other Cognitive Research

❖ A Survey and Comparison of Human Monitoring of Complex Networks (Su, Yurcik - 2005)

- Surveyed comparisons of 4 major infrastructures (water, electric, air traffic control, and nuclear)
- Found variations in level of cognitive difficulty based upon infrastructure type
- Operators severely filter the information they are receiving based upon their stress level in order to minimize cognitive load
- Working memory in operators is susceptible to interference from competing processes
- Uncovered the following common challenges:
 - Analysts experience data overload
 - Analysts have difficulty filtering data
 - Difficulty querying the network for information
 - Operators respond to network management tasks along a continuum between proactive and reactive

Other Cognitive Research

❖ Information Handling in Dynamic Decision Making Environments (Wong, Blandford - 2004)

- Examined high-stress decision making in emergency medical dispatch environment
- Collected data in 24x7 environment, divided into call-takers and dispatcher cells, receiving more than 3500 calls per day
- Found a significant increase in dispatch times when a specific workload threshold is crossed
- Linked insufficient resources as one cause of the spike in dispatch time during high-stress call workloads
- Uncovered incompatible information forms as a significant factor in dispatch time inefficiency
- Excessive reliance on working memory to compare details during high-stress dispatch workloads; information grouping difficult to achieve during times when duplicate issue call-ins occurred

The Advantages of Visualization in Incident Handling

- ❖ Based upon the CTA and other cognitive analyses, it can be concluded that visualization offers / would offer the following specific advantages within the Incident Handling space:
 - Information aggregation to prevent duplicate event handling
 - Visual indication of progress within plans, intentions, operations, and execution
 - Visual cues of existing and queued workload
 - Easy and efficient reprioritization and reorganization of workload
 - Visual connection of related information and indicators
 - Annotation of electronic records provides quick visual cues and reminders without having to “drill into” data
 - Global information summaries and rapid viewing of global information
 - Rapid and descriptive explanatory information on displays for instant situational awareness at a high level
 - One of 4 core components to effective human monitoring of complex networks

Issues Impacting Visualization's Effectiveness

- ❖ As a “last-mile” tool in the Incident Handling process, the effectiveness of visualization is impacted by several key factors:
 - Data quality
 - Data accuracy
 - Data coverage
 - Ease-of-use
 - User-centric customization
 - Lack of / inefficient reporting capability
 - Dislocation from network & network security resources
 - Information collaboration capability
 - Analyst-driven data organization

A Novel Approach to Incident Handling Visualization

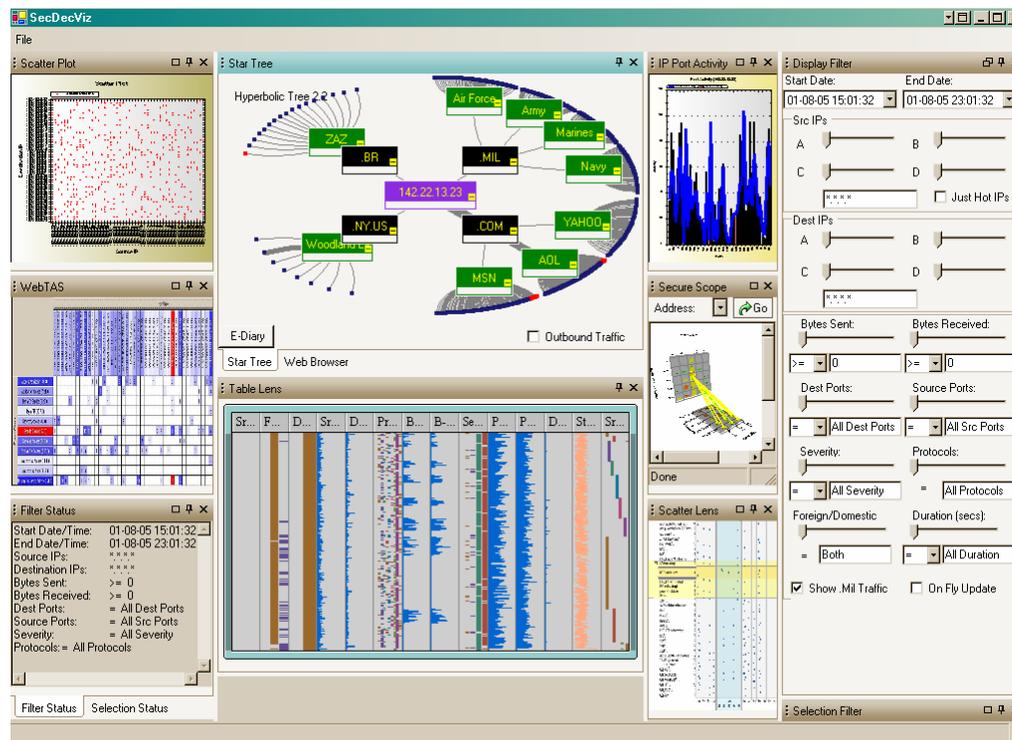
VIAssist Tool Suite: Designed to Support IA Analyst Cognition

- ❖ Innovative combination of an agnostic, novel UI framework with multiple commercial IA tools
 - Supports cognitive skills of IA analyst
 - Detection of relationships in activity within and across organizations
 - Maintenance of many separate mental models of suspected attackers
 - Evaluation of alternative hypotheses
 - Mitigates cognitive challenges to effective analysis
 - Seeing patterns in massive datasets
 - Communicating what is “normal” for an enclave
 - Keeping track of where they are in an analysis & how they got there

VIAssist Tool Suite: Designed to Support IA Analyst Cognition

Features of VIAssist Tool Suite

- Dual displays for global awareness and local event analysis
- Different visualization techniques for different stages of IA analysis
- Novel UI shows effect of filtering and highlighting simultaneously in all visualizations; supports multiple hypotheses and data correlation



Future Approaches to Visually-Supported Incident Handling

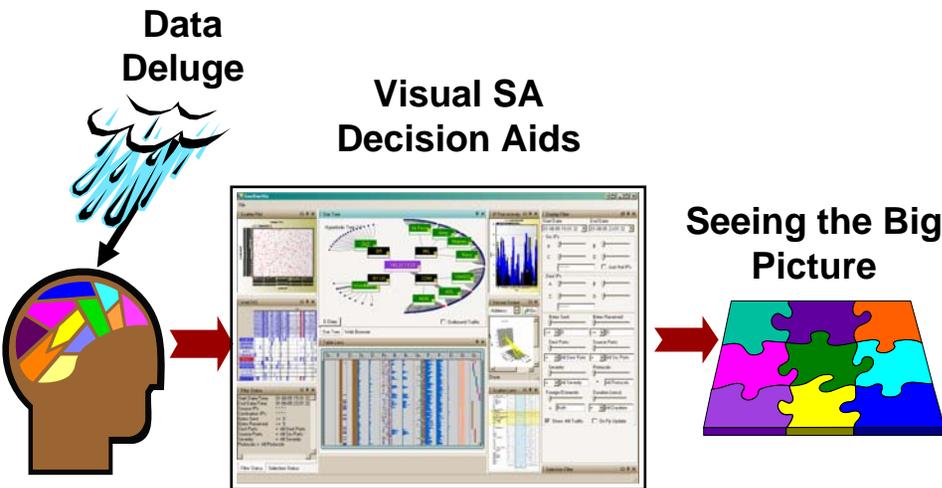
- Incident Handling “Wizard”
- Real-time Data Flow Modeling Display
- Behavior-based Learned Alerting
- Predictable Data Source Collection

Conclusions

- Incident Handlers and operations deal with numerous performance inhibitors during operations
- Human factors impact the success, accuracy, consistency, and efficiency of the tasks required within complex environment monitoring
- Workload, environment makeup, operational inhibitors, and stress factors adversely impact the success of the IH process
- Visual tools and solutions can positively impact the above conditions and issues
- Visualization is only as good as the data it is fed

Questions?

Cyber Situational Awareness System (CSAS): Visualizations for IA Analysis (VIA)



Goals

- Refine the cognitive analysis of IA analysts through in-depth CTAs at NSA
- Develop a prototype of the VIA system
- Install and evaluate system at an operational site conducting IA analysis, e.g. JTF-GNO/J2
- Install and evaluate VIA system at IC's test lab at MITRE
- Demonstrate the VIA prototype at CWID 06

Novel Ideas

- User interface tools to support the workflow of IA analysts
- Presentation of the same dataset in multiple visualizations
- Simultaneous filtering & highlighting of coordinated views
- In-depth application of formal methodology of Cognitive Task Analysis (CTA) of IA within the IC

Milestones

- FY05
- Q4 Commence prototype an integrated suite of visualizations for IA (VIA)
 - Q4 Develop ConOps for use of VIA in JTF-GNO/J2
- FY06
- Q1 Commence NSA IA CTA data collection
 - Q2 Install & demo VIA at JTF-GNO/J2
 - Q2 Report on NSA IA CTA results
 - Q3 Report on VIA evaluation at JTF-GNO/J2
 - Q3 Demonstrate VIA at CWID
 - Q4 Install & demo VIA at MITRE lab
 - Q4 Final report