CyberSAVI: A Cyber Situation Awareness Visual Interface for Mission-Level Network Situation Awareness

Celeste Lyn Paul[1], Randall Rohrer[1*], Patrick Sponaugle[2], Jenna Huston[1], Bohdan Nebesh[1]

[1]Department of Defense
{clpaul, jlhusto, banebes}@tycho.ncsc.mil
*rohrer@acm.org

[2]SRA International
patrick_sponaugle@sra.com

ABSTRACT

This poster abstract presents CyberSAVI, a Situation Awareness Visual Interface that provides mission management level situation awareness of the health and status of a network and the people assigned to investigate irregular network events. CyberSAVI focuses on supporting the interaction and coordination between people to provide situation awareness of suspected, known, and on-going network events. The coordinating poster demonstrates how CyberSAVI accomplishes these goals through the description of a realistic network security use case.

Categories and Subject Descriptors

C.2.3 [**Computer-Communication Networks**]: Network Operations – *network management, network monitoring*.

General Terms

Design, Human Factors, Management, Security.

Keywords

Cyber security, situation awareness, visualization.

1. INTRODUCTION

Computer network situation awareness challenges are not limited to identifying a suspicious point on a screen in a sea of large amounts of network data. Resources, such as people, must also be managed to effectively support the mission of monitoring the health and status of a network. Situation awareness at this mission management level must support the ongoing, evolving awareness of multiple detections by many analysts, help them work efficiently and in concert, and have the right amount of information available to make critical decisions and deploy resources as necessary [2, 3, 4].

A visualization that provides information on who is doing what and where can quickly become a valuable tool in the management and security of a large computer network. Through CyberSAVI, we provide network situation awareness through awareness of people's actions on the network.

VizSec'13, October 14, 2013, Atlanta, Georgia, USA.

2. CYBERSAVI

CyberSAVI is a situation awareness visual interface that provides mission-level information about the current health and status of the network and the people assigned to investigate the network events. As people on a network team identify and respond to events information about these events become visible in the visualization display. Members of the network team can see where events are happening on the network, know who is working on these events, and be able to assess the impact of events on their own responsibilities.

CyberSAVI is meant to provide mission-level awareness for managers and decision makers rather than support detailed analysis. The visualization supports situation awareness through the display of people's tasks on the network instead of activity on the network. Instead of using network-based sensor data and analytics to populate the visualization, it is driven by the artifacts of people's work. For example, when a network analyst claims an IDS alert to investigate the analyst and his event activity is indicated on the related part of the network.

This abstract describes the CyberSAVI visualization concept. The corresponding poster provides an example use case of how CyberSAVI supports mission-level situation awareness of human resources engaged in network events. Future work includes testing the visualization design concept with larger networks and more complex event scenarios as well as a pilot study in a collaborative network situation awareness environment.

2.1 Design Process

The CyberSAVI design process followed a top-down, "design first" approach that focused on the creation and design of a visual concept before integrating visualization, analytics, and data (as opposed to the more common "data first" approach used in visualization design). We chose this process as a way to encourage new creative ideas in a highly technical space. The visual design concept was created to solve a story-like scenario that described a typical day in the life of a network operations center manager and was based on the IEEE VAST Challenge 2013 Mini-Challenge 2 scenario using data from the VAST Challenge 2012 Mini-Challenge 1 [1].

2.2 Visualization

The CyberSAVI visualization supports situation awareness through the display of three types of information objects: an abstracted network, network events, and teams of people.

The visualization of the network is abstracted into set of single lines with nodes, rather than the traditional node-link graph to represents a network map with logical or geographic context.

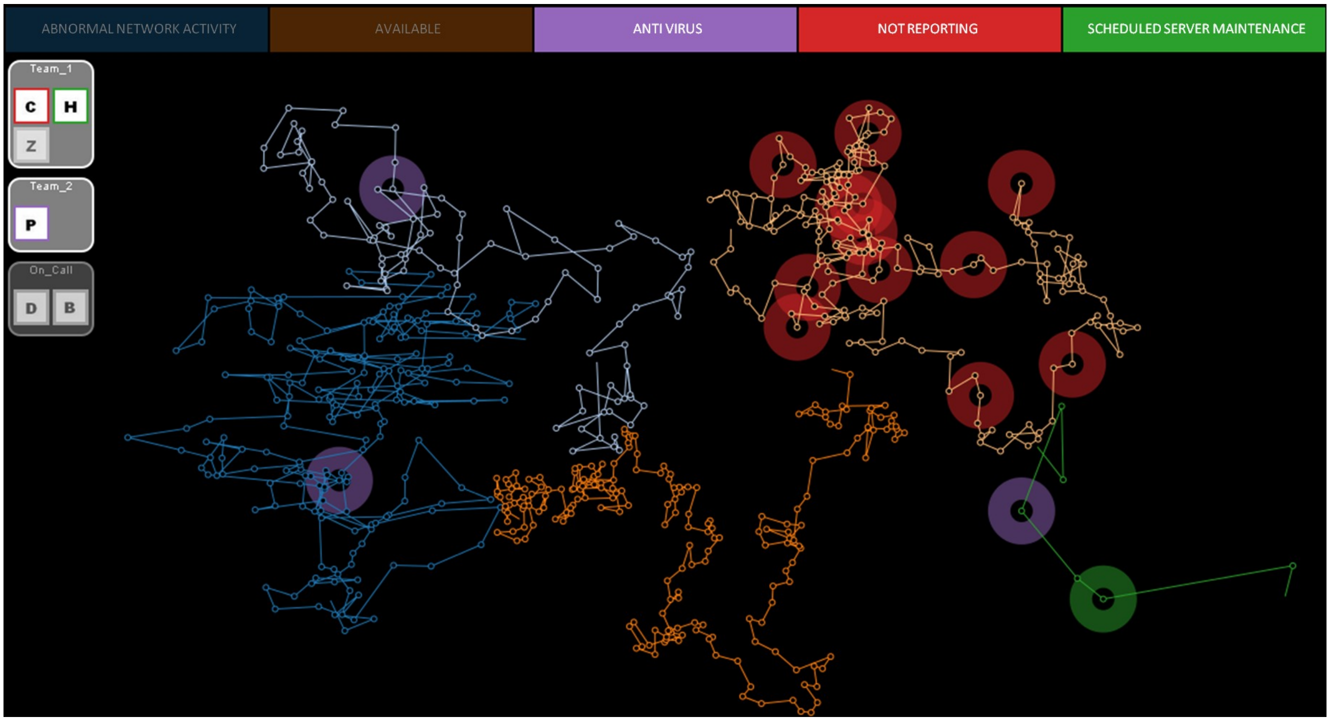

Figure 1. CyberSAVI showing network activity from the VAST Challenge 2012 MC1 dataset

- **Lines** represent a network, sub-network, or other grouping of significance.
- **Nodes** represent a single computer, a cluster or sub-network of computers, or network hardware such as a firewall.
- **Connections** between the nodes on the line are implied—what is important is that all the nodes on the line belong together in some way.

The abstracted network view helps simplify what could be a very complicated network for a large number of computers. This abstraction is a way for dealing with the big data problem often associated with visualizing large networks.

Human resources are displayed as teams of people who are working or are available for tasks related to network security.

- **Teams** are groups of people organized by location, expertise, and/or management hierarchy.
- **People** are those who are engaged in or are available to conduct activities to contribute to the security of the network.

Displaying the status of human resources helps managers coordinate, prioritize, and assign resources as well as supports collaboration within and across teams during more difficult tasks.

Network security events are displayed as events across the top as well as in context as indicators on the network nodes.

- **Event labels** are the categories of events routinely identified on the network.
- **Event nodes** represent a network node that has an event or events attached to it.

An event is shown on a node by a circle indicator. If a single event occurs on multiple nodes on multiple networks, all of the relevant nodes will display an indicator. In the case that multiple events are linked to the same node, the event indicator displays all event colors.

2.3 Interaction

All visual objects can be selected with coordinating highlights:

- **Network**: all of the network nodes, events, and people related to the selected network are highlighted.
- **Network Node**: all of the events and people related to the selected network node are highlighted.
- **Event**: all network nodes and people related to the selected event are highlighted.
- **Person**: all of the network nodes and events related to the selected person are highlighted.
- **Team**: all of the network nodes and events related to people within the selected team are highlighted.

This coordinated selection and highlighting interaction allows users to create a specific visual context to aid in decision making.

3. ACKNOWLEDGEMENTS

The CyberSAVI visual design concept was created by Gong Szeto Design Office for the Department of Defense.

4. REFERENCES

[1] IEEE VAST Challenge. http://vacommunity.org/VAST+Challenge .

[2] Erbacher, R.F. Visualization Design for Immediate High-Level Situational Assessment. ACM VizSec 2012, 17-24.

[3] Grimaila, M.R., Mills, R.F., Forston, L.W. Improving the Cyber Incident Mission Impact Assessment (CIMIA) Process. ACM CSIIRW 2008.

[4] Paul, C. and Whitley, K. A Taxonomy of Cyber Awareness Question for the User-Centered Design of Cyber Situation Awareness. HCII 2013, HAS, 145-154