

Challenge Description

In this VAST Challenge 2013 Mini-Challenge, we are looking for innovative graphical designs to support situation awareness for large-scale computer networks.

Objective

A company called Big Enterprise has hired you to create an innovative visual design that will become the foundation for their future situation awareness display that shows the state of their entire computer network.

The computer network is global and consists of several hundred thousand computers. The network is expected to grow over time. The company wants to be able to keep track of everything important on the network in a single integrated picture.

The new situation awareness display will ultimately become a large display in the operations control room. The display will be used by members of the network operations staff. When you visit the control room to learn about the current operations, you see many computer screens, but the information being displayed is difficult to understand.

Your goal is to design the visualization for the large computer display that will provide operators with situation awareness for the Big Enterprise network.

Background: Situation Awareness

Situation awareness involves obtaining accurate knowledge about some real-world environment – in this case, a large computer network. The *situation* consists of what the pieces of the environment are and how well they are operating, communicating, and collaborating. Is everything normal? If there are deviations from normal, such as unexpected events, how serious are they? Will important components fail within the next few minutes? few hours? *Awareness* refers to the collection of knowledge people have about the real-world environment. Do they know which pieces of the environment are healthy, broken, or failing? Are they cognizant of the significance of any particular failure or trend toward failure?

Effective situation awareness of large-scale computer networks depends upon the ability to maintain a constant and clear understanding of network activity, to recognize changes, and to respond as quickly and effectively as possible. A situation awareness display does at least two things:

1. It provides an accurate portrayal of the network, such as an internal model, map, or architecture.
2. It communicates information and knowledge about the current situation in the context of the network. The information communicated must be accurate, clear, and useful, so that network operations personnel can make good decisions to ensure the network continues to run effectively.

In a situation awareness display, the health and status of the network is made visible. It displays several different types of conditions:

- Normal activity - everything is operating as expected
- Routine issues - common problems for which the solutions are well understood
- Non-routine issues - new or infrequent problems which may require a response, but the appropriate response is not established in advance.
- Crises – severe and/or multiple issues occurring simultaneously whose cause root is unclear

Big Enterprise Network Operations Center

The network operations manager is the primary person in the Big Enterprise who works with a team of network operations specialists responsible for the health, security, and performance of the entire network. She explains to you what this responsibility means by providing the following example questions routinely asked:

- Health: Are all the computers behaving as expected with the necessary patches and updates to operate normally?
- Security: Are there any attacks that might affect the Enterprise, such as an active virus, a denial of service, or theft of company secrets?
- Performance: Are there data transfer issues such as routing problems or misconfigurations that are affecting network speed?

As she gives you a tour, you learn a few things about the network itself:

- You verify that the network consists of several hundred thousand computers. The operations manager cannot give an exact number since the branch offices will connect and disconnect computers without coordinating with her.
- The network is connected to the larger Internet, and millions of computers access the company's computers daily.
- Big Enterprise has a large corporate headquarters with many computers. The headquarters also runs several data centers. Each of these data centers contains thousands of computers. These computers should appear on the network operations manager's display.

In addition to the corporate headquarters, there are offices all around the world, each of which has its own computers. These computers should also appear on the network operations manager's display.

Upper management wants your situation awareness visualization to be hosted on a large display to show the state of the entire network. The network operations manager hopes the large situation awareness display will allow her team to get the information she needs from one display instead of several that she deals with now.

She tells you the network operations center is staffed around the clock. In her role as the network operations manager, she and her team must oversee the day-to-day management of the entire corporate network. In addition to responding to routine events, they need to identify and respond to any unusual events occurring across the network. They must continually balance network health, security, and performance issues.

Her main complaints about the current situation awareness display are that the information is often unclear and complicated. The information cues are inconsistent, and important connections between events are often not obvious. She sometimes has to dig into very detailed information to understand

something that she thinks could be easily shown up front. She feels that she wastes time digging, and that there has to be a better approach.

Your Mission

Your job is to design a large-scale visualization presenting network activity in such a way that at a glance the network operations manager can effectively and accurately understand what is happening on the network.

Although you would like to ask more questions and get still more background, Big Enterprise executives have politely declined your request. They are looking for a fresh perspective on situation awareness, and do not want to bias your designs by diving into the details of their current approach. The Big Enterprise executives understand that cyber security isn't necessarily your field. They have said that it is fine if you wish to do some of your own research or talk to people you know who are more familiar with cyber security. Current solutions are inadequate, so Big Enterprise executives emphasize that creativity is key. Instead, they are looking for creative new ideas, possibly borrowed from other fields or using different technologies. They suggested that you remember the following:

- The sky is the limit: they are looking for bigger and bolder ideas than the status quo.
- The bigger the better: represent the biggest network you can.
- The bigger the network, the more stuff happens: represent the greatest amount and diversity of activity you can in the design.
- Managing complexity is essential: balance network scale and network activity with effectiveness of the visual design.