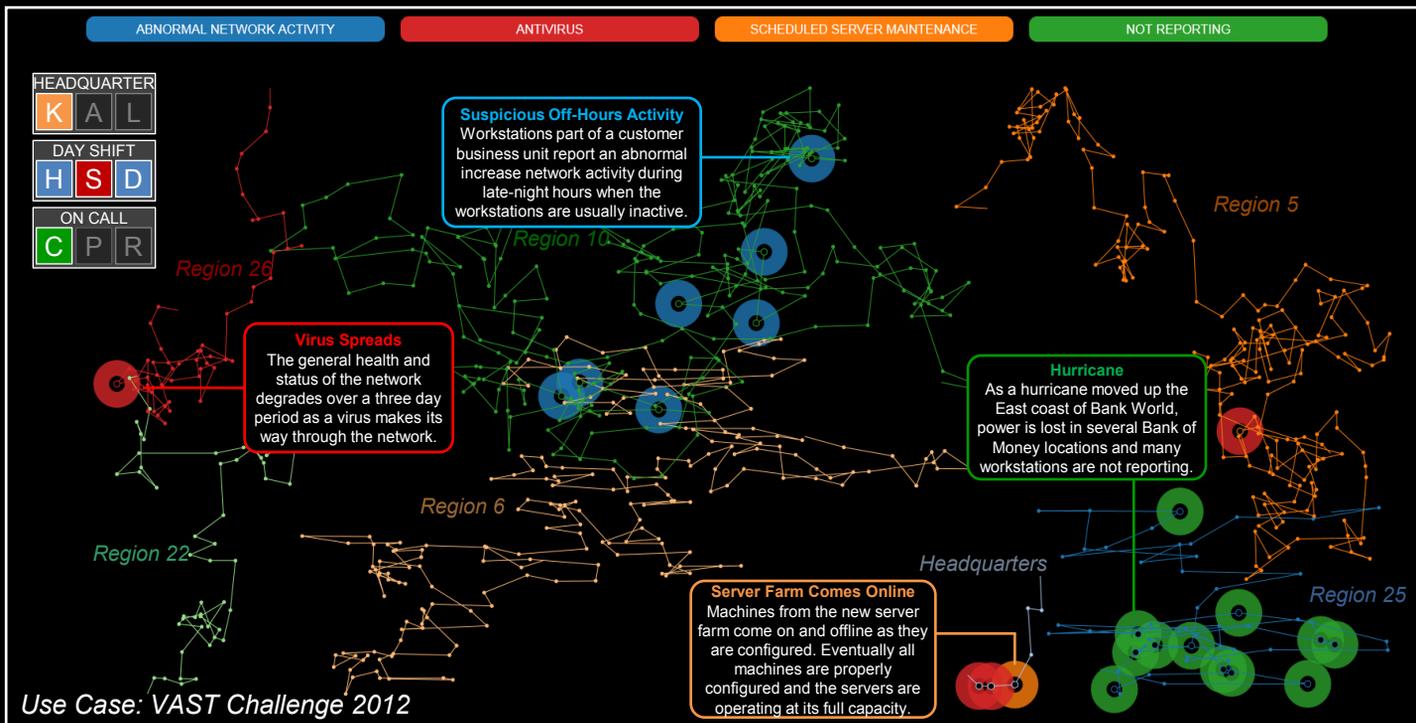# CyberSAVI

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   [2]SRA International

ABNORMAL NETWORK ACTIVITY	ANTIVIRUS	SCHEDULED SERVER MAINTENANCE	NOT REPORTING

HEADQUARTER
K A L

DAY SHIFT
H S D

ON CALL
C P R

Suspicious Off-Hours Activity
Workstations part of a customer business unit report an abnormal increase network activity during late-night hours when the workstations are usually inactive.

Virus Spreads
The general health and status of the network degrades over a three day period as a virus makes its way through the network.

Hurricane
As a hurricane moved up the East coast of Bank World, power is lost in several Bank of Money locations and many workstations are not reporting.

Server Farm Comes Online
Machines from the new server farm come on and offline as they are configured. Eventually all machines are properly configured and the servers are operating at its full capacity.

Region 26
Region 10
Region 5
Region 22
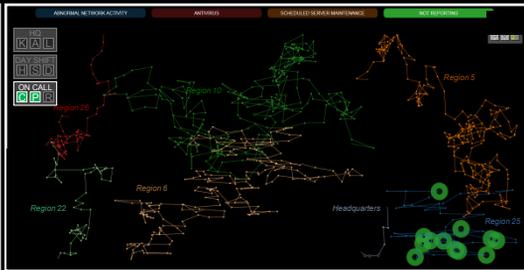Region 6
Headquarters
Region 25

Use Case: VAST Challenge 2012

Selecting Abnormal Network Activity allows you to see everywhere that type of event is occurring. Then, by selecting Hank from Day Shift, you can see which of the abnormal network activity events he is investigating.
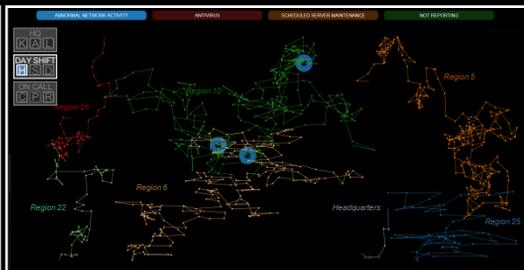
Selecting AntiVirus shows everywhere AV signatures are hitting on the network, including the Headquarters network. By selecting the Headquarters network, you can see that Kenny from Headquarters is working the Scheduled Server Maintenance — of which may be affected by the virus outbreak.

Selecting Not Reporting shows that Celeste from the On Call team is the only admin assigned the Region 25 outage due to the Hurricane and may need assistance once power is restored.