

Stories of Agile Acquisition

PlugFest – Results Operationally Measured Acquisition

Eric Westreich,
PlugFest Consortium Lead
Esri Defense C2 Industry Manager



Stories

- **Paul's story (the engineer)**
- **Jeff's Story (the advocate)**
- **Chris' Story (the validator)**
- **Mike's Story (the collaborator)**

Real Solutions: West 2014 PlugFest Technology Team



Cyber



Ship
Positions



Application
Development



Real-time



Crisis
Communication



esri

Foundation Data
Geospatial Viz & Analysis
Presentation



Enterprise
Solutions



Workflow
Development



Emergency
Management



Presentation &
Modeling

PlugFest Events Summary

(Over 1200 visitors/300 Collaborators)

Challenge	Sponsor	Event
Emergency Response -Haiti	AFCEA SPAWAR	AFCEA SD C4ISR Symposium
Opposed Maritime BattleGroup Transit	AFCEA SPAWAR	AFCEA SD C4ISR Symposium
Find, Fix, Finish Adversary	AFCEA Director USMC Intelligence	AFCEA Technet Southwest
Counter Narcotics	AFCEA DEA/DoD	AFCEA Technet South
Indications and warning of Cyber Threat	AFCEA US Army Cyber Command	AFCEA Technet East
Emergency Response for Bomb at Public Event	AFCEA USNI Los Angeles Sherriff's Dept Red Cross San Diego Police USMC	West 2013

PlugFest Events Summary (Multiple Organizations)

Challenge	Sponsor	Event
Intelligent Common Operational Picture	Security Network	Security Summit
DI2E Architecture	OSD(I)/DI2E	DI2E PlugFest
Operational Cyber Logistics	AFCEA US Cyber Command	AFCEA Cyber Symposium
Army Common Map API	DI2E GMU	GMU Academic PlugFest
Basic Cyber Attack on U.S. Ports	InterAgency Board	IAB Meeting
Advanced Cyber Attack on U.S. Ports	AFCEA USNI InterAgency Board SPAWAR	West 2014
Common Map API	OSD(I)/DI2E	DI2E PlugFest
Sustained Communications	AFCEA US Army	AFCEA Technet Augusta

PlugFest Consortium
(*Transitional* Organization)

Non-profit collaboration that believes that Government, Industry, and Academia working on the same problem, at the same time, together can deliver some technical capability better, faster and cheaper.

PlugFest Consortium Action (Transitional Organization)

Investigate, Test, and Educate,
agile Verification and Validation
methods.

Facilitate and train others to
Facilitate Agile V&V Events.

Find a permanent home for these
functions.

Stories

- **Mark's Story (the educator)**

Your Story

Agile is to Development, as PlugFest is to V&V

- ✓ What can I do today deliver better stuff faster?
- ✓ What will I do today that is outside of my comfort zone?
- ✓ What will I do to help teach others?
 - Place to discover and test theories, best practices, programs (virtual, scalable PlugFest lab)
 - Place to teach (virtual classroom)
 - Place to respond (virtual center of excellence)

Quote

“I must have heard “cool” a thousand times!”

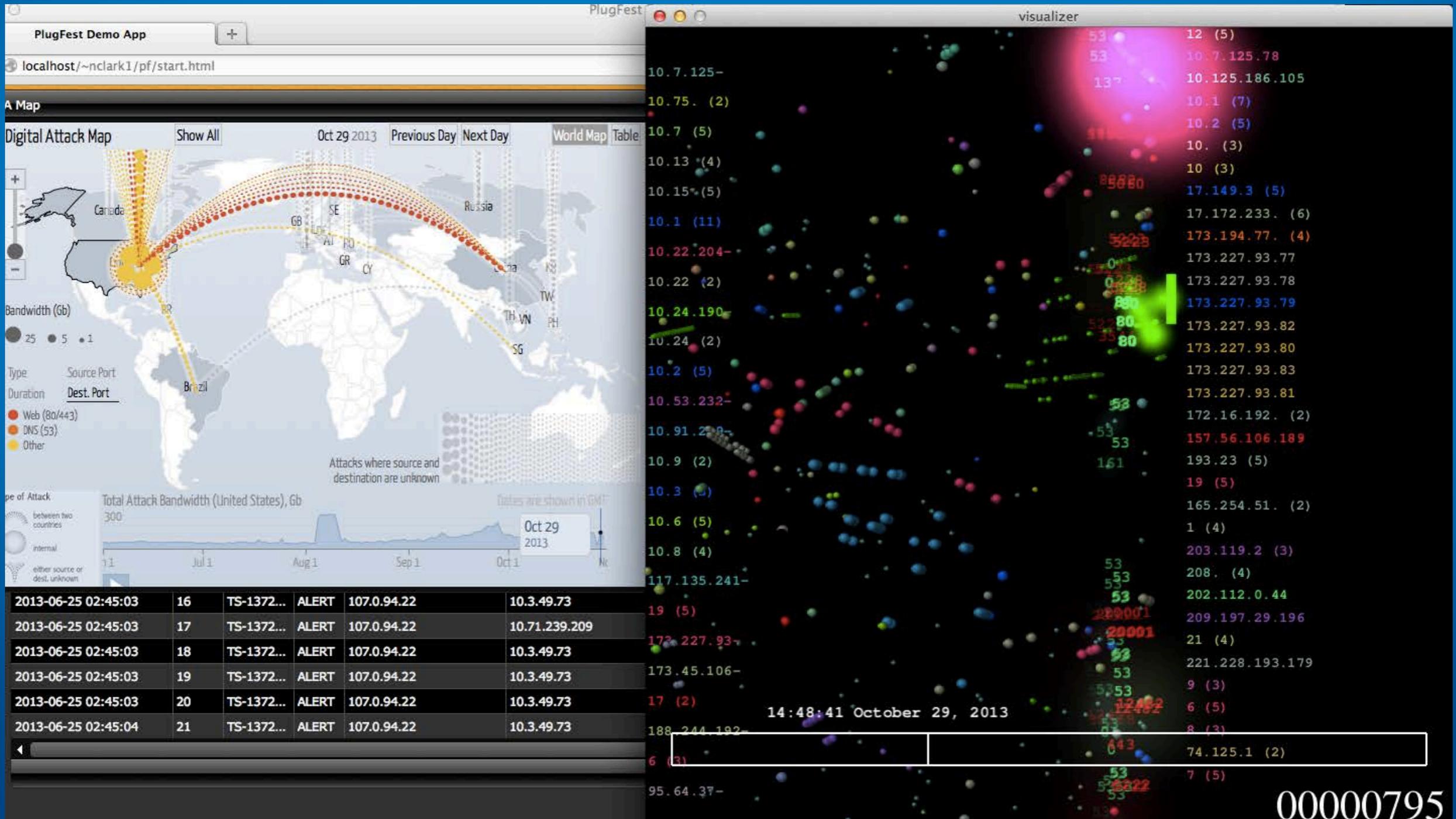


Government Provided Problem: Cyber Attack on the Ports of Los Angeles & Long Beach



Hacker Goal: **Disrupt** 40% of the containerized cargo and material that enter the U.S.

Real Cyber Data (Real Attacker, Anonymized Victim)



Every Application is part of the Common Operational Picture

The COP is shared awareness delivered

The image displays a collage of various operational software interfaces, illustrating the components of a Common Operational Picture (COP). The interfaces include:

- Top Left:** A window titled "IAB Plugfest 2013 Long Beach Scenario" showing a map with traffic signals and a list of ships (e.g., NORD OBTAINER, NAT GEO SEA L).
- Top Center:** A map showing traffic signals with a legend listing locations like AS32-SHOPPING CENTER & CARSON, A426-PACIFIC AVE & 27TH ST, etc.
- Top Right:** A window titled "Geocortex Viewer" showing a map with a yellow and blue highlighted area.
- Middle Left:** A 3D map view showing a city area with numerous "Alert!" and "Danger!" labels overlaid on the terrain.
- Middle Right:** A window titled "Ortho and Oblique Aerial View" showing a 3D aerial view of a city area.
- Bottom Left:** A window titled "VirtualAgility - DS" showing a decision model interface with a flowchart and a table of "Degraded Container Ship Operations".
- Bottom Right:** A window titled "Pictometry" showing a 3D aerial view of a city area with a table of "Export CoA" results.

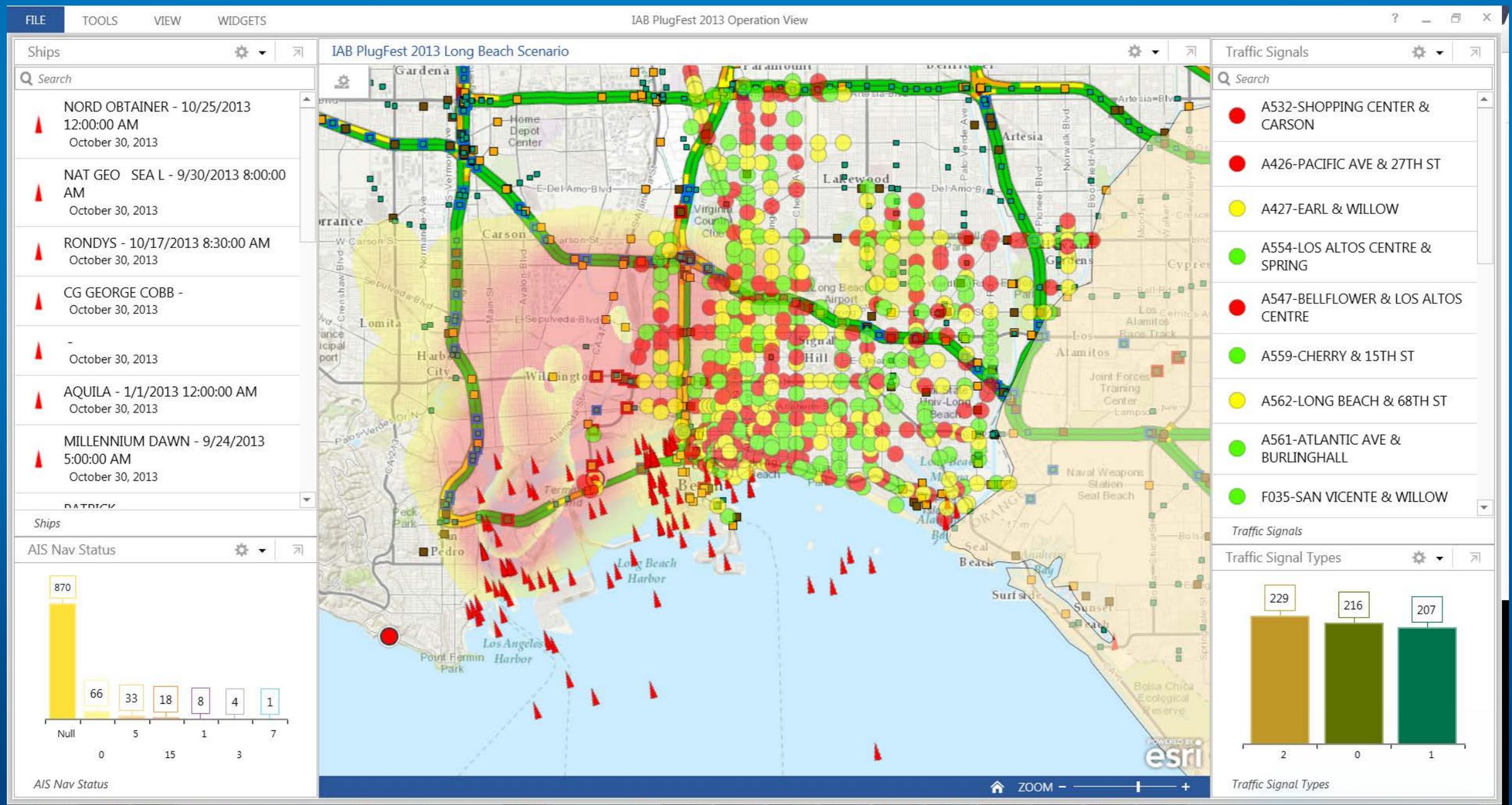
Question: What would take out loading capability at Ports of LA and Long Beach?

- Loading/Unloading Ships SCADA DoS Attack
Crude Oil, Chlorine, Xylenol spills



Question: What is the most immediate impact? Chlorine Plume

Fused, updating picture on PowerPoint, Excel, and Operations Dashboard

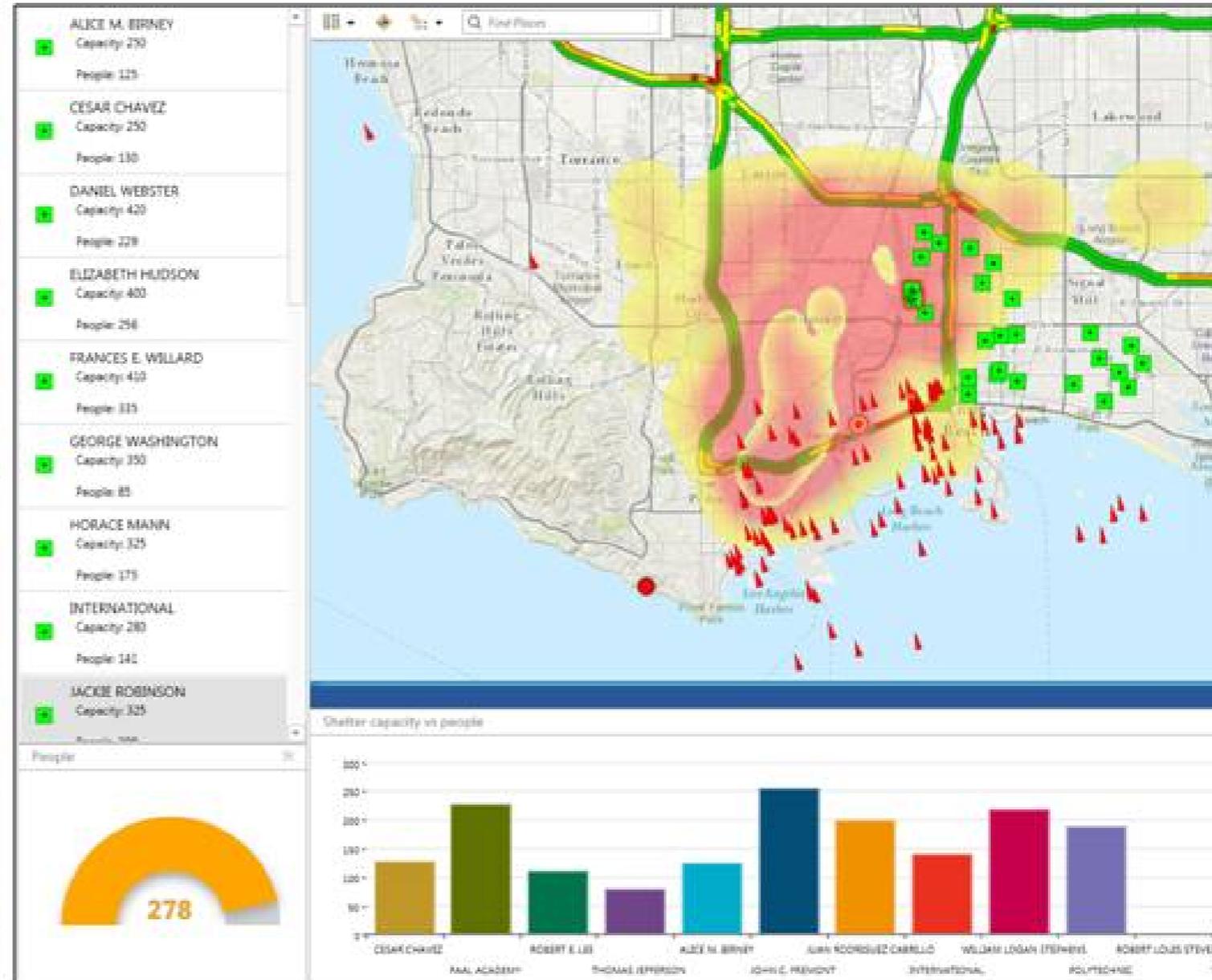
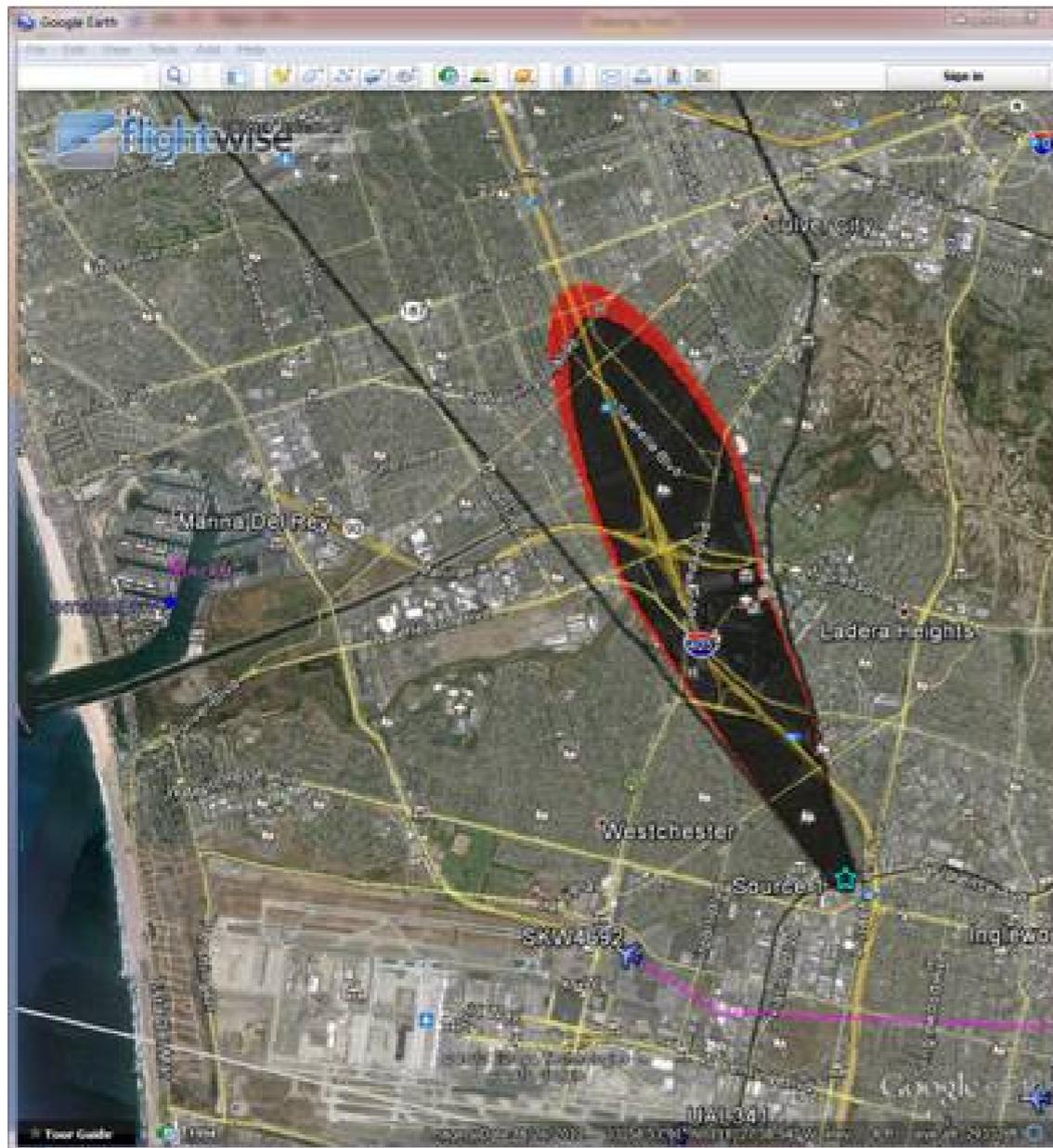


MARINE CORPS TACTICAL SYSTEMS SUPPORT ACTIVITY

Technical Excellence...Tactical Value

How to maintain Situational Awareness?

The ability to display relevant information rapidly and efficiently.

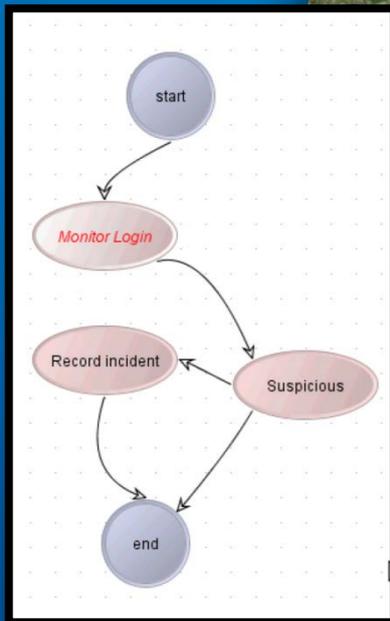


Question: How do we detect and defend sophisticated cyber-attacks against systems (including CIKR)?

Leverage Complex Event Processing to correlate data in real-time from a variety of monitoring sensors, providing alerts and automated responses



Monitor hackers via social media
Coordinate key personnel



Incidents
Tools
Darryn Graham

Activity on host
from Darryn Graham

Time: 02/03/2014 10:50:20
Visibility: No
Mobile Access: No
Incident: No Incident

Contact Information
Email Work (SMTP):
darryn.graham@softwareag.com

Latitude, Longitude: 39.53791, -76.98721

More details from Darryn Graham
Suspicious activity on host

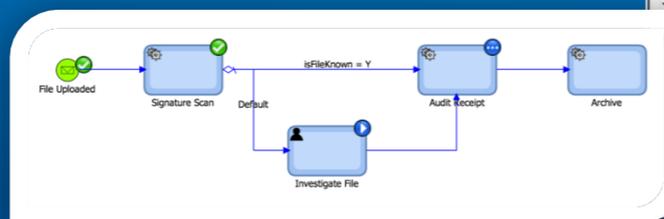
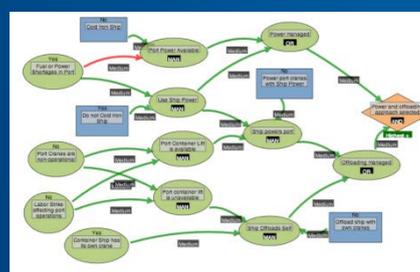
Service	metro_code	zipcode	area_code	EventID	password	country_cod	Timestamp	country_name	ip	city	region_name	username	region_code	SourceIP	longitude	latitude
ssh				ID-apamac-orelator(243)	privat3	GB	2014-02-05 13:28:15+0000	United Kingdom	185.2.138.125		root	root		185.2.138.125	-0.13	51.5
ssh				ID-apamac-orelator(243)	privat3	GB	2014-02-05 13:28:15+0000	United Kingdom	185.2.138.125		root	root		185.2.138.125	-0.13	51.5
ssh				ID-apamac-orelator(243)	privat3	GB	2014-02-05 13:28:15+0000	United Kingdom	185.2.138.125		root	root		185.2.138.125	-0.13	51.5
ssh				ID-apamac-orelator(245)	cacti	NL	2014-02-05 13:28:27+0000	Netherlands	93.174.90.30		root	root		93.174.90.30	5.75	52.5
ssh				ID-apamac-orelator(245)	cacti	NL	2014-02-05 13:28:27+0000	Netherlands	93.174.90.30		root	root		93.174.90.30	5.75	52.5

Login Attempts by Country

- United States
- Netherlands
- Moldova, Republic of
- China
- Canada
- United Kingdom
- Germany
- France
- Sweden

stateful behavioral analysis

malware file processing



response plans

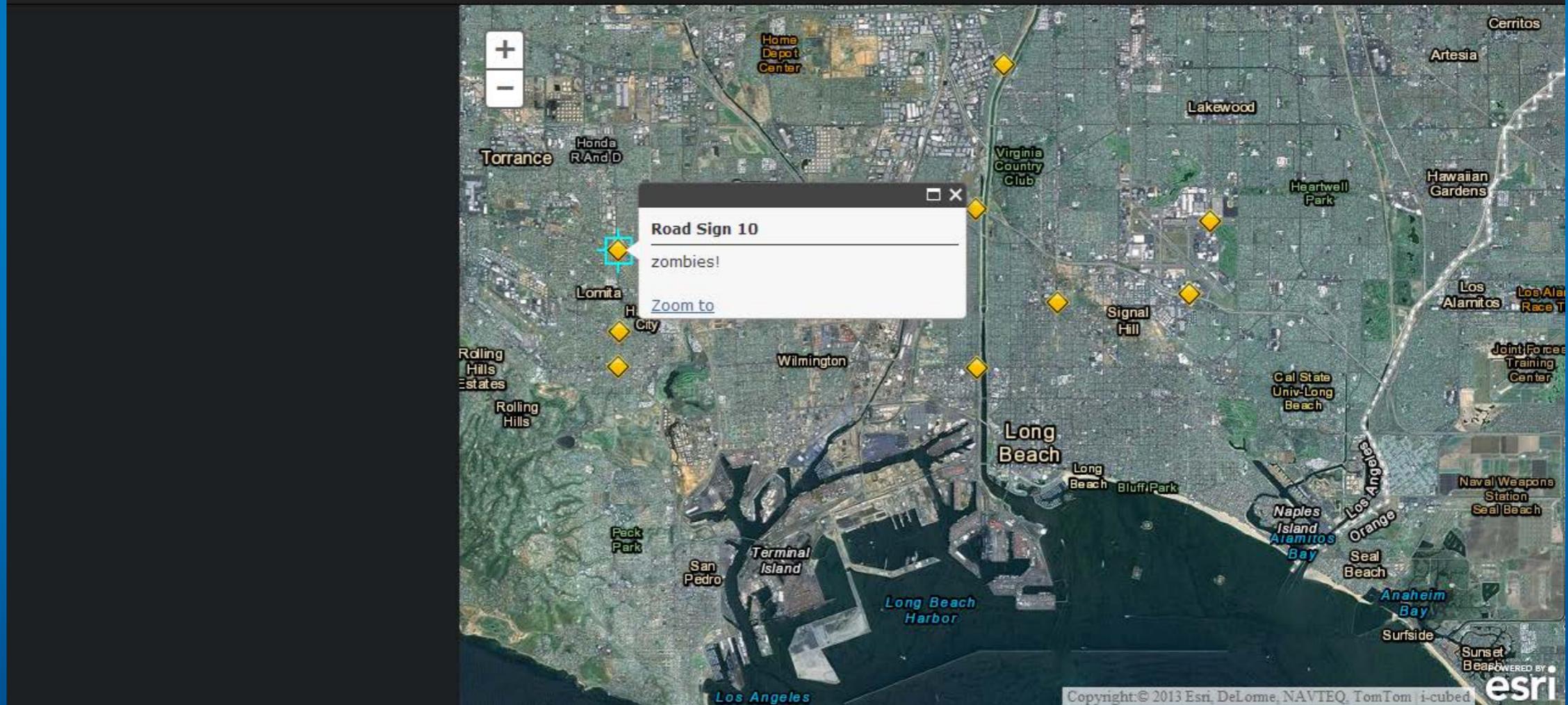


COP / dashboards

Question: How does the public know where to go to be safe?

Interactive Tactical Map

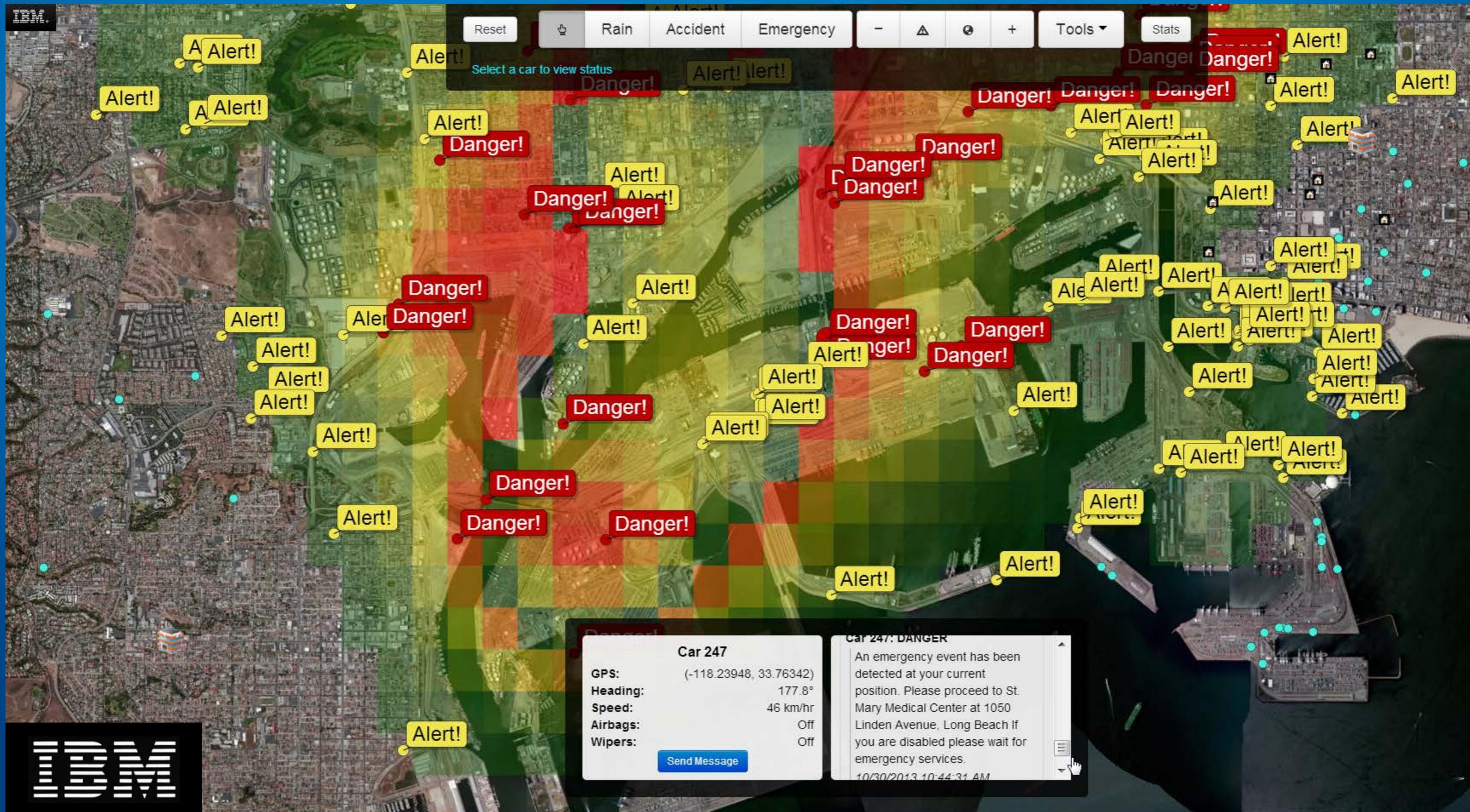
long breach



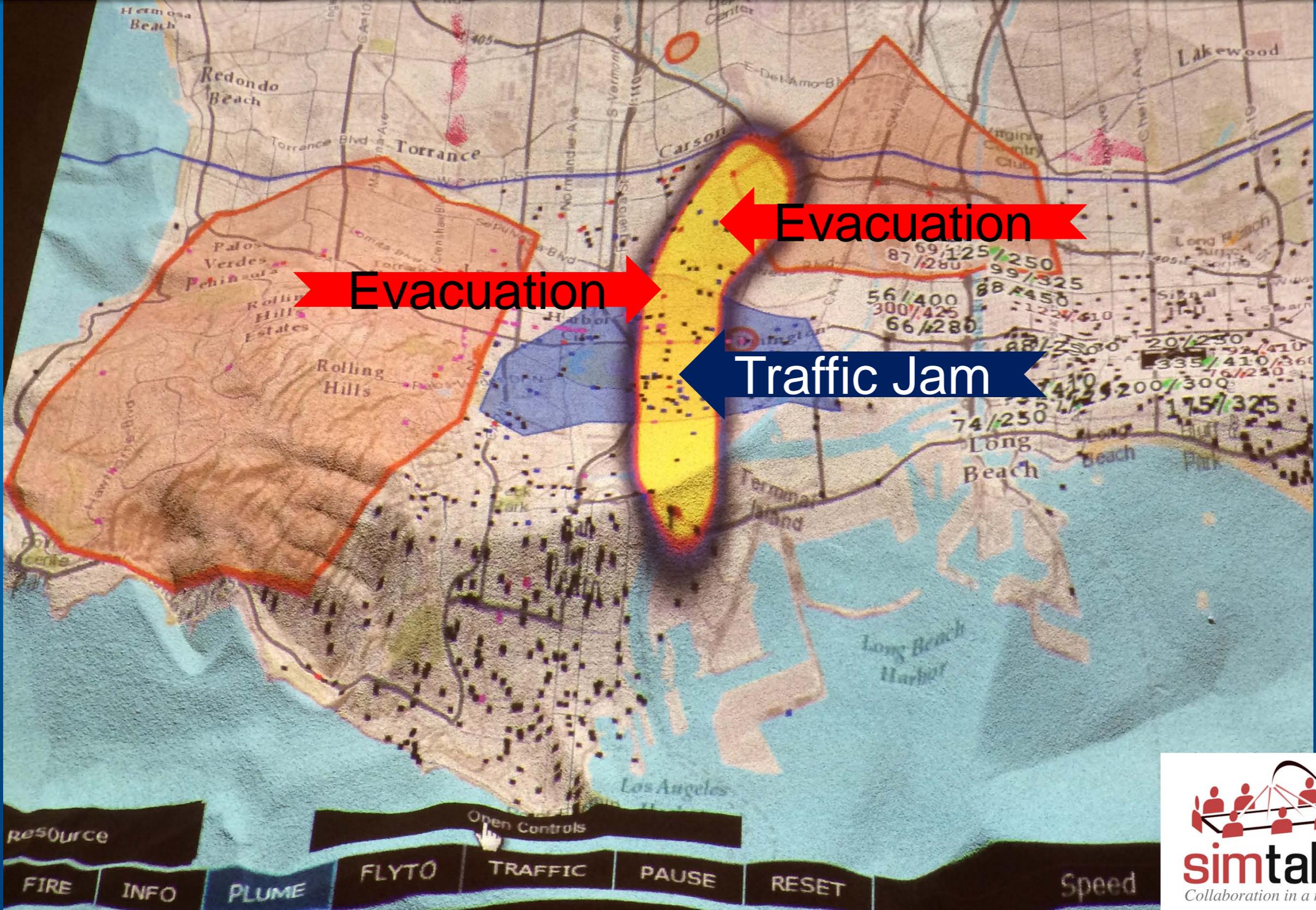
SAN DIEGO STATE
UNIVERSITY



Question: How do we alert medical threat (red) in the plume, and evacuation (yellow) ahead of the plume?



Question: Attack on responders: how is response prevented? (EAS & ITS Attacks)



Question: How do you develop and implement courses of actions against cyber attack?

The screenshot displays the VirtualAgility - DS software interface. The top navigation bar includes the VirtualAgility logo, the text "VirtualAgility - DS", a "CALEX" dropdown menu, a search bar, and a user profile for "Gideon Moran". Below this, a secondary navigation bar contains tabs for "Overview", "Details", "Decision Modeler", "Marine Data", "Long Beach Traffic Report", and "Geocortex". The main interface is divided into three sections:

- Left Panel:** A sidebar with a "Plans" section containing a tree view of response plans:
 - Cyber Attack on CIKR Response
 - .Notification to Agencies
 - Port of Long Beach Response
 - Fuel Operation Modification Plan
 - test
 - Contact Emergency Response
 - Verify Incident

- Center Panel:** A map of Long Beach, California, showing various incident markers. A callout box for an incident at Pier 103 provides the following details:
- Name: Incident at Pier
- Date & Time: 8/20/2013
- Status: Major Disaster
- Incident Type: [Additional Information]
- Right Panel:** A legend and list of objects on the map, including:
- Infrastructure: Gerald Desmond Bridge, Rail Bridge, Commodore Schuyler F. Helm Bridge- Terminal Island Freeway, HI- Sand Island Access Bridge, Bridge- Shoreline Drive.
- Vessels: Alaskan Legend, Tula, Hella Enterprise.
- Other: Hospitals, Fire, Police, Shelters (HORACE MANN, THOMAS A. EDISON, ELIZABETH HUDSON, PETER H BURNETT).

A legend at the bottom of the map area defines the symbols used for incident status: Major Disaster (black diamond), Mass Emergency (red diamond), Standby to Assist (yellow diamond), Under Control (orange diamond), and Unknown (grey diamond).

Question: How do we assign restoral tools across multiple platforms simultaneously?

Incident Management | Geocortex Demonstration Site

Search...

Home Resource Assignment Drawing Tools

Bomb Threat Evacuation ERG By Chemical Demographics Analysis Social Media Search Assign Resources Update Plume Threat Response

Scale: 1: 36,112

Jump to a map bookmark...

Demographics Analysis

I want to...

World Imagery w/ Labels

General Population Details

- Total Area Analysed: 7.50 square km
- Population (2010): 2590
- Population Per Square Km: 345.28

Familial Makeup

- Households: 2517
- Average Household Size: 1.77
- Single Males: 242
- Single Females: 180
- Married Households: 248
- Married With Children: 127
- Single Male With Children: 41
- Single Female With Children: 111
- Total Families: 513
- Average Family Size: 5.37

Housing

- Housing Units: 1228
- Vacant Units: 158
- Occupied Units: 1069
- Owner Occupied Units: 413
- Renter Occupied Units: 657

Special Needs

- Limited Mobility: 257
- Needs Wheelchair: 130
- Needs Oxygen: 105

Results (8) Demographics Analysis

Search for map features...

Demographic Breakdown of Evacuation Zone

COMPTON

PACIFIC COAST HWY

E ANAHEIM ST

W ANAHEIM ST

ALAMEDA ST

BRGS BLVD

N AVAILON BLVD

E 7TH ST

E ANAHEIM ST

W OCEAN BLVD

LONG BEACH

W 25TH ST

W 9TH ST

W PASEO DEL MAR

LOS ANGELES

LONG BEACH-LAKEWOOD

Married with children: 911

Married no children: 640

Single male with children: 159

Single female with children: 588

Families: 2,784

Average family size: 3.9

Housing

- Housing units: 4,445
- Vacant Units: 373
- Owner occupied: 3,119
- Renter occupied: 10,006

Download demographics data as CSV

Done

1mi 2km

9:00 AM 10/30/2013