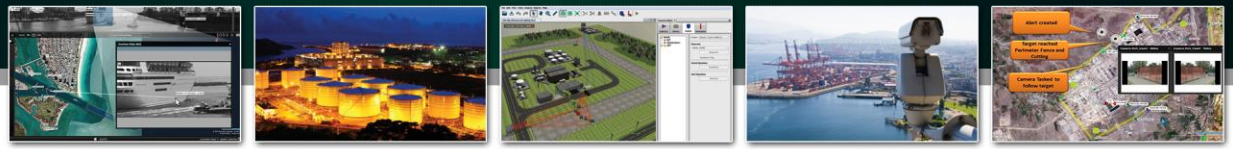
Emerging Security Technologies



Port and Coastal Security Executive Briefing

Agenda

- Our Current Security Environment
- Cyber: The Insider Threat
- The Current State of Security at U.S. Ports
- Emerging Technologies
- Real Time Security & Optimization

Current Security Situation

- Physical Security threats on the rise
  - Al-Qaida replaced by ISIS, Boka Haram, etc.
  - Cannot "Prevent." Can only "Detect-Respond."
- Terrorism is on the rise, primarily in Europe but this will spread:
  - Istanbul Airport Attacks, Brussels Train/Airports, Multiple attacks in Paris
  - Access to Western passports is a major concern for US as these attacks could spread here.
- Free world critical infrastructure is largely unprotected
  - Airports, Shipping ports, power grid, oil and water pipelines, production facilities.
  - Most of our "most critical" assets are using 1980's or older technology.
  - Special Forces concentrate on weapons systems; tech for take back/assessment is non existent.

Current Cyber Security Situation

Three key factors working against you…

- Rise of a highly organized criminal ecosystem
  - Multi-billion dollar black market economy
- Asymmetric nature of the battle
  - Cost of advanced exploits vs. cost of defenses
- Perimeter focused defense in depth strategies
  - Too siloed, too limited, too reactive


TECH SECURITY

China iCloud Attack Could Be State-Sponsored Hacking

Jack Linshi @jacklinshi

The iCloud attack coincided with the iPhone 6 releases in China

Chinese users recently attempting to access Apple's iCloud online data storage service may have had their personal information stolen in what one cybersecurity firm claims was a high-level cyberattack backed by Chinese authorities.

GreatFire, an independent Chinese censorship watchdog, said the hack was a "man-in-the-middle" attack, in which

A Chinese man sets up his new iPhone 6 inside an Apple store on October 17, 2014 in Beijing, China.


'Major' hacking attack in US looms: expert survey

By Rob Lever
52 minutes ago

In the mind of a hacker


Modern Healthcare

Medical device hack-attack issues resurface

AP

New hack attack at Albertsons, Supervalu stores

The Home Depot hack: How, why and what we can learn

IN DEPTH Another retailer suffers a cyberattack


Fallout coming from JPMorgan hack attack

BY JOSEPH LAWLER

JPMorgan Hack Caught by Routine Check

Bloomberg

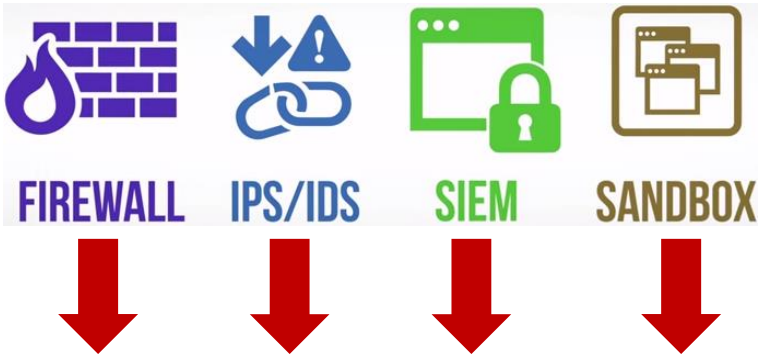
TWO SEVENTY PARK AVENUE

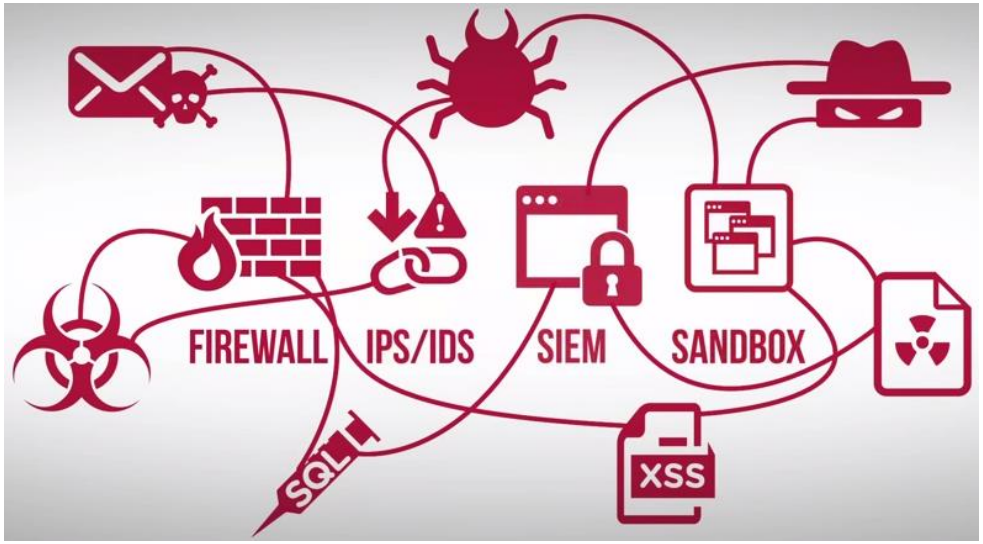
Bloomberg

Current Cyber Security Situation

Traditional defense in depth strategies are failing…

- Too many gaps in perimeter security solutions
- Over-reliance on signature-based threat detection
- Too many discreet, point solutions
- Massive number of alerts
- Diagnostic rather than predictive
- Big Data getting BIGGER





Current State of Security at U.S. Ports



- US Shipping/Passenger Ports are a primary and very soft target for terrorism
  - Most of the U.S. Ports are largely protected by fences, limited security infrastructure for detection.
  - Many are **accessible unprotected shipping corridors** which allow easy opportunity at mouth of port
  - Many depend on local law enforcement for primary security.

- Despite the security posture many ports offer a unique opportunity for our enemies:
  - Several ports may disembark up to **30,000-50,000 passengers a day**.
  - Many of our ports contain **large quantities of potentially dangerous materials**, near population centers.
  - They also tend to be **located near places where people like to live** and where commercial impact would be significant.

DHS's PSGP Priorities



Department of Homeland Security's Port Security Grant Program Specific Priorities

1. Enhance Maritime Domain Awareness
2. Port Resilience & Recovery Capabilities
3. Training & Exercises
4. Improve Cybersecurity Capabilities
5. Enhance IED & CBRNE Prevention, Protection, & Response
6. Equipment Associated with TWIC Implementation

Emerging Technology - Modeling and Simulation

Improve communication, effectiveness, and efficiency;

Measure security performance to support management decisions.

CHARACTERIZE

Security Goals
- Link to a threat and asset
- Link to business goals
- Clearly measure performance

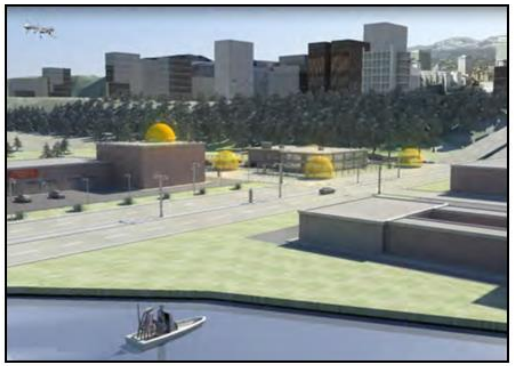
Site Layout
- Infrastructure
- Security layers
- Elevation / Terrain

Detect & Delay Systems
- Sensors & cameras
- Command / control
- Perimeter structure

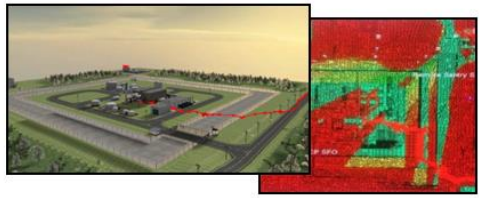
Response Force
- Patrol & response
- Concept of operations
- Capabilities & training

SYNTHESIZE

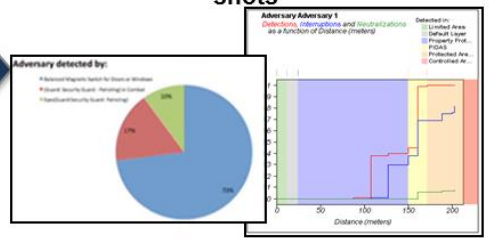
- Automatically simulate an incident with numerous threat profiles
- Evaluate 100s of scenarios varying in security configurations and facility operations within hours rather than weeks



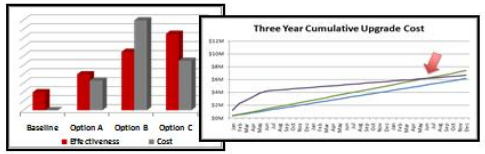
ANALYZE



Visuals of attack paths, intensity maps, & shots



Detection, interruption, & neutralization analysis



Conduct cost/benefit analysis

OPTIMIZE

- Produce simulated video of threat incident and your response
- Conduct cost benefit analysis to match budget with effectiveness needs

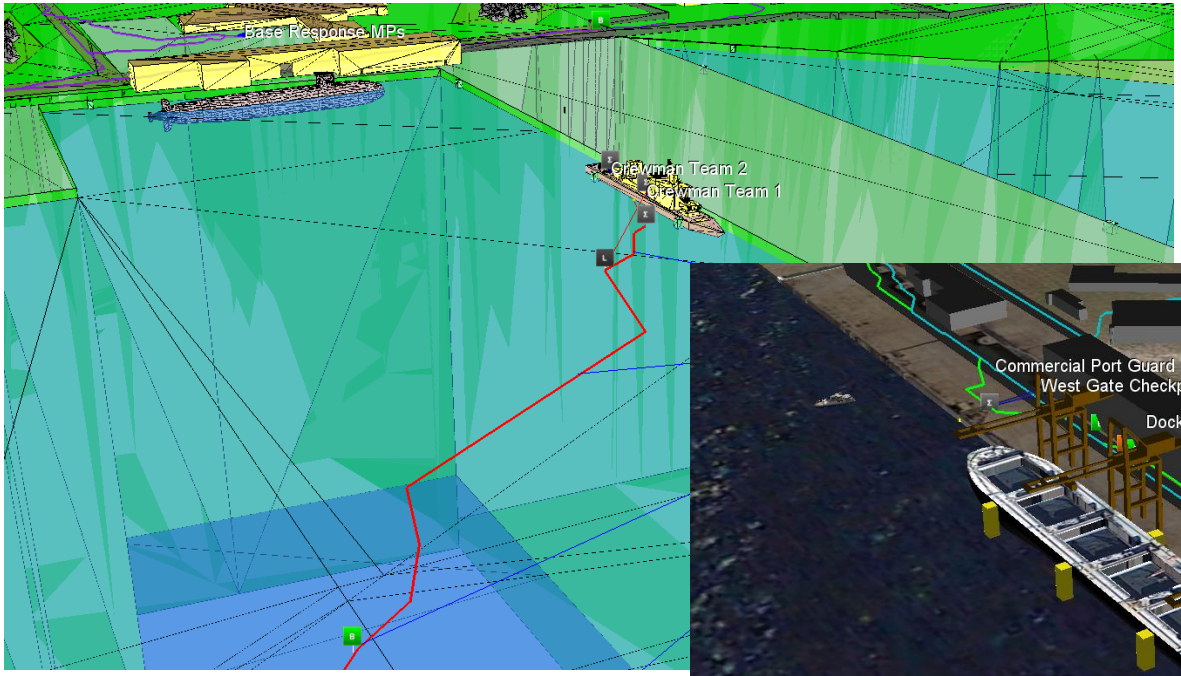
Overview

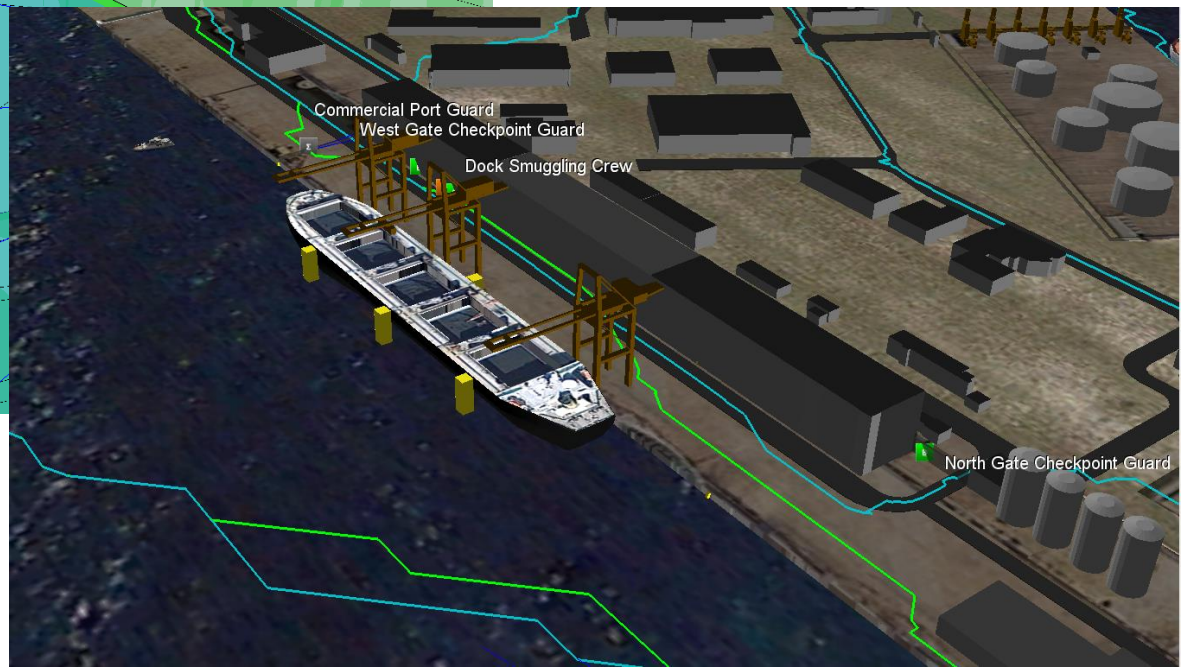
By using what-if scenarios, ports could model security concerns at commercial and military ports around the world, including USS Cole bomber style attacks, smuggling, and criminal activities. These Scenarios would help ports choose the most optimal security configuration.

Scenario Set	Description
Bomber Scenarios	USS Cole style attacks, utilizing small speed boats loaded with explosives attempting a suicide mission against a docked destroyer. Scenarios feature a variety of defensive strategies
Smuggling Scenarios	A Cargo Ship attempts to smuggle illegal (potentially dangerous) goods into port. The crew unloads the contraband cargo at the port warehouse, where a team of insider smugglers meets them and drives the cargo offsite.

Overview

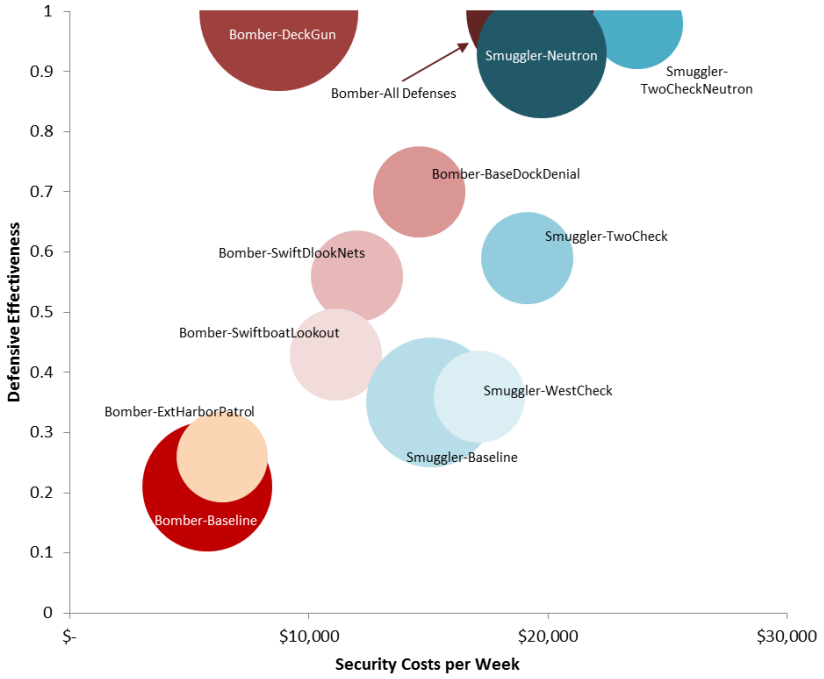
Simulations cover a wide range of scenarios, from a bomber attack on the docked Destroyer (seen on left) and the illegal smuggling operations at the port (seen on right).





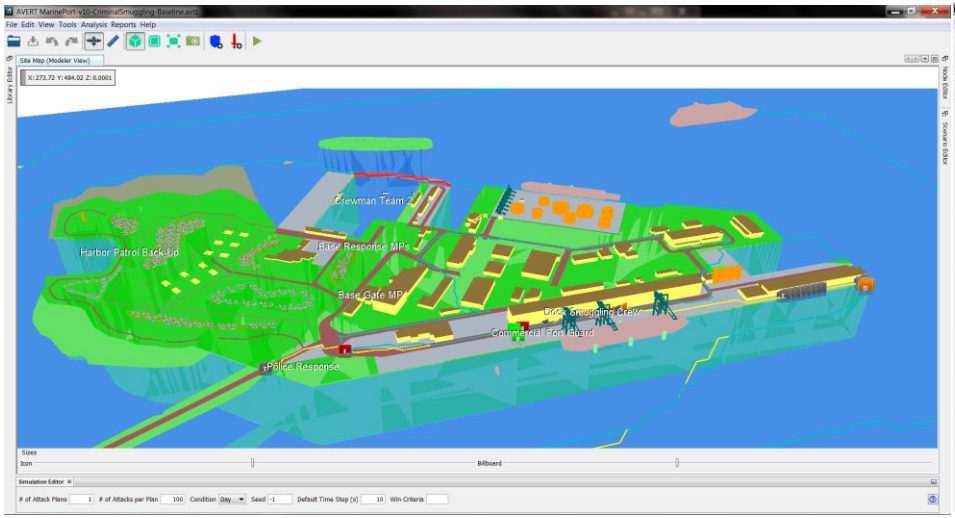
Results Summary

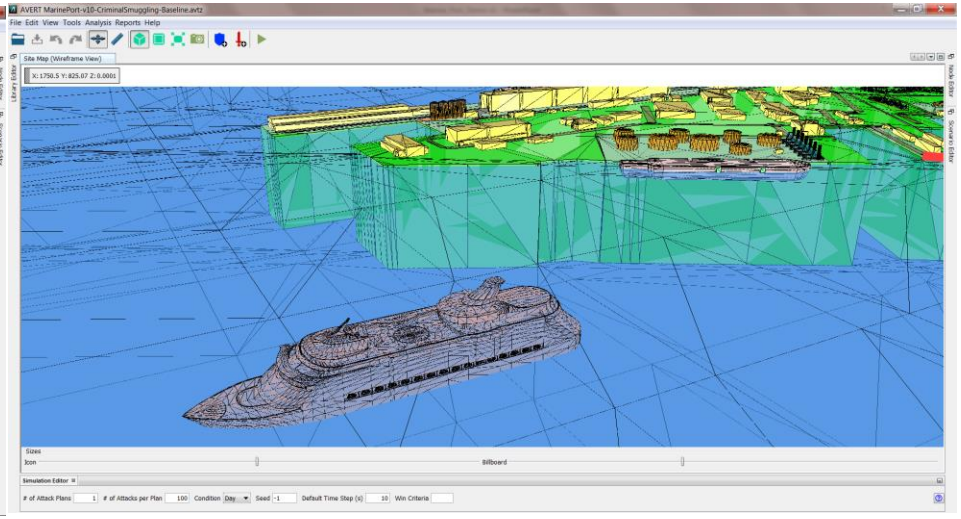
Below are the results of the two types of scenarios for various security configurations. The Bomber scenarios are shown in Reds and the Smuggling scenarios in Blues. Highly effective methods use a combination of high reliability detection, firepower, delay, and non-lethal neutralization systems. In essence, a layered defense works best.

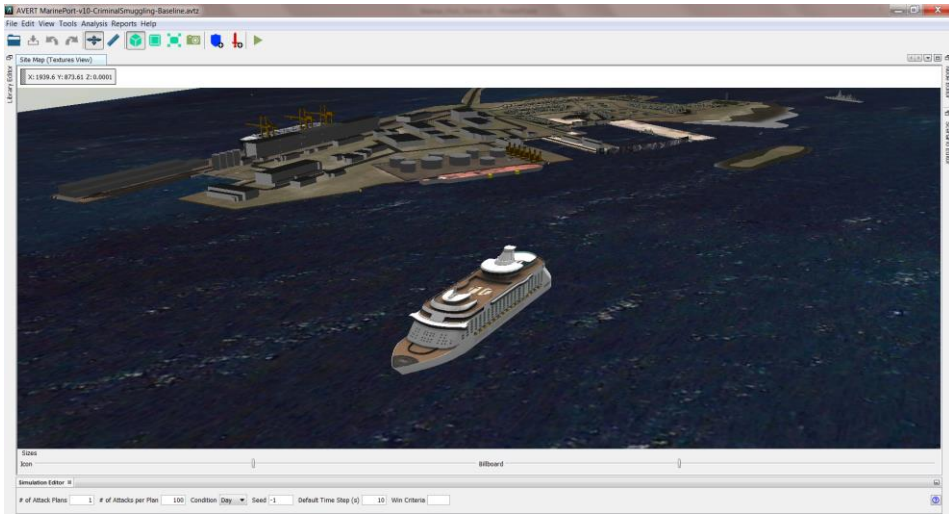


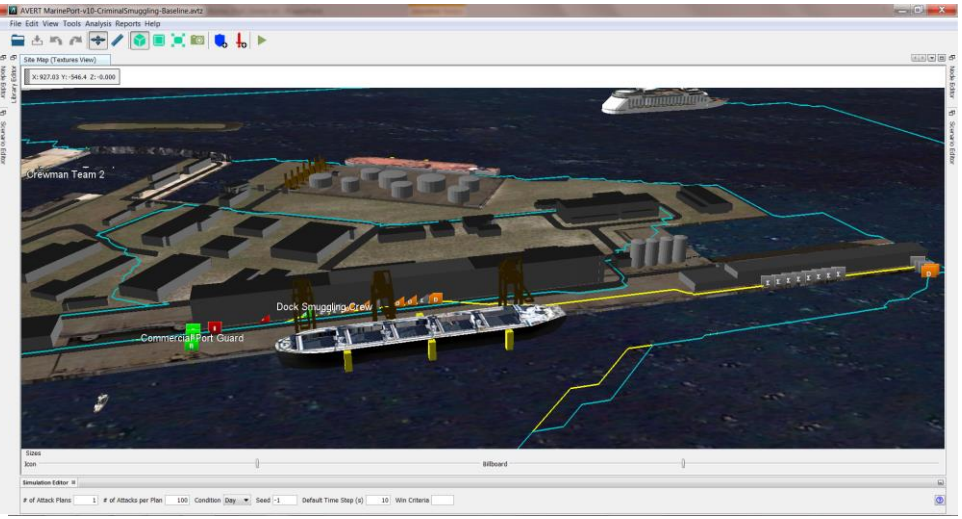
Scenario	Description	P(e)	Security Costs
Bomber-All Defenses	All Defenses	100%	$ 19,607.69
Bomber-DeckGun	1 Active Harbor Patrol + 1 Back-Up Harbor Patrol + Deck Gun	100%	$ 8,755.77
Bomber-BaseDockDenial	2 Active Harbor Patrol ships + Marines Swiftboat + Dock Lookout + Anti-Propellor Nets + Extended Detection Area	70%	$ 14,607.69
Bomber-Baseline	1 Active Harbor Patrol + 1 Back-Up Harbor Patrol + Dock Lookout	21%	$ 5,755.77
Bomber-ExtHarborPatrol	2 Active Harbor Patrol ships + Extended Detection Area	26%	$ 6,365.38
Bomber-SwiftDlookNets	1 Active Harbor Patrol + 1 Back-Up Harbor Patrol + Dock Lookout + Marines Swiftboat + Anti-Propellor Nets	56%	$ 11,998.08
Bomber-SwiftboatLookout	1 Active Harbor Patrol + 1 Back-Up Harbor Patrol + Dock Lookout + Marines Swiftboat	43%	$ 11,121.15
Smuggler-Baseline	1 Active Harbor Patrol + 1 Back-Up Harbor Patrol + 1 On-Foot Patrol + Offsite Police Response + Standard Cargo Check at Dock	35%	$ 15,121.15
Smuggler-WestCheck	Baseline + West Gate Checkpoint	36%	$ 17,121.15
Smuggler-TwoCheck	Baseline + Checkpoints at Both Gates	59%	$ 19,121.15
Smuggler-TwoCheckNeutron	Baseline + Checkpoints at Both Gates + Neutron Scanning at Dock	98%	$ 42,198.08
Smuggler-Neutron	Baseline + Neutron Scanning at Dock	93%	$ 38,198.08

Example screenshots – Modular view









Emerging Technology - All Hazards

Improve Security Design, Support Emergency Planning;

Evaluate beyond design basis threats and events to support management decisions.

Characterize

3D model of site with:
- Security Assets
- Site and facility details
- Operational Assets

Various event models (Tornado, Flood, Security)

Security
- Large numbers of configurations
- Set up to develop attack surface
- Model wide variety of threats

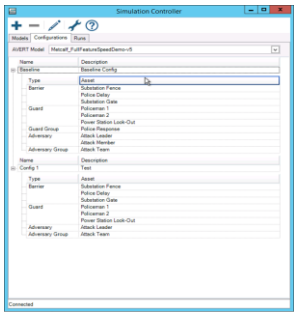
Future Modules
- Coastal Flooding
- Seismic
- Fire

Wind (Tornado)
- Run Tornado paths
- Characterize areas Impacted by wind

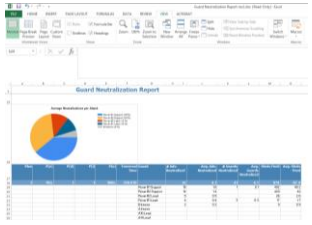
Riverine Flooding
- Identify floodplains
- Characterize areas impacted by rainfall runoff

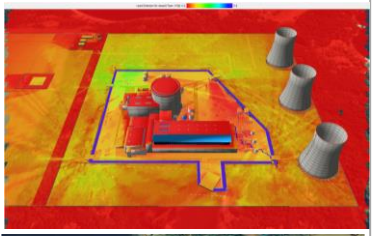
Synthesize

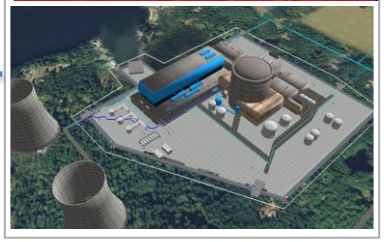
- Run 10^6 simulations
- Relational database to manage runs
- Cooperative Pathfinding
- Simulation Controller
- Advanced Tactics



Analyze





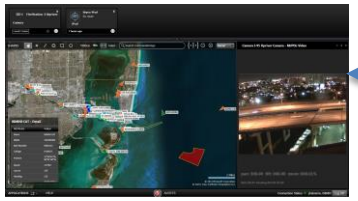


Optimize

- Margin Analysis
- Defense in Depth design support
- Sensitivity Analysis
- High Fidelity Visualization (BIS - VBS3)
- Assisted Optimization
- Automatic Placement of equipment

Simulation/Training

- Simulation using site geometry
- Scenarios come from AAH
- High Fidelity Visualization (BIS - VBS3)
- Virtual training (BIS – VBS3)
- Team training and battle labs
- Development of NON Security or combined security and operations scenarios



(Future) – Interface to Assure CommandBridge for Real Time Optimization

Virtual Tabletop Concept

Scoreboard

- Status metrics on scenario
- Rate overall performance to rank commanders

Higher Fidelity Model

- Combat
- Movement
- Line-of-sight

Modify Scenarios

- Add future events on the fly
- Remove responders

3D View

- Select assets and resources
- Deliver commands to respond

Practice Dispatch

- Select assets and resources
- Deliver commands to respond

Timeline View

- Record, replay, & rewind
- Walk team through CONOPS for familiarization

Emerging Technology - Command & Control

Improve situation awareness, response, and management;

Providing context from clutter to support management decisions.

CONTEXT TRANSFORMATION

Broad-based Situation Awareness & Response

- Across geographic boundaries
- Across intermodal transportation routes
- Across facilities

Configurable Platform
Tailorable by Organization/Position/User

Documents and Workflow

- Pictures/video clips
- Text Documents
- SOPs

Sensors

- AIS
- Radar
- River Gauge

Systems

- Access Control
- Video Management
- Dispatch Systems

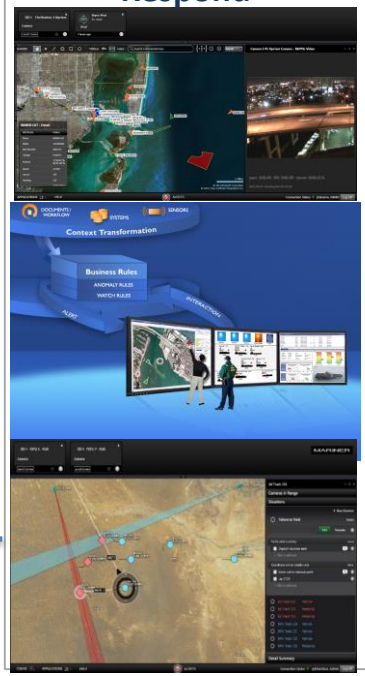
Synthesize

- Business Rules
- Anomaly Rules
- Watch Rules
- Actionable/Decreased clutter
- Zone Monitoring

INTERACT

ALERT

Respond



Reports

- Situation Reports
- Panels/Streams
- Planning Tool
- Situation Replay
- Temporal View of Past/Current/Future Activity

Mobile Devices
(iPad/iPhone/
Android)
Secure, segmented
access to outside agencies
During Emergency Mgmt.
Exercises and events.

What is Real Time Security & Optimization?

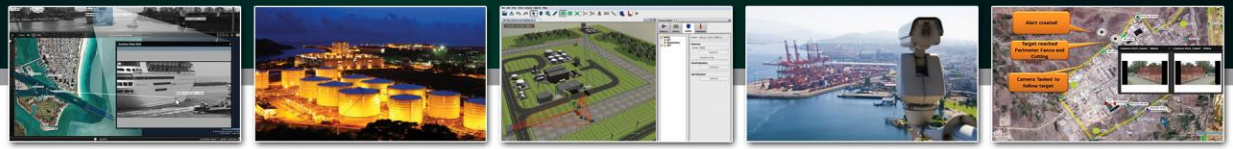
- A system that will not only detect but also correct
  - Stay ahead of physical & cyber threats

- Benefits
  - Learn possible outcomes
  - Real time anomaly/threat/cyber detection
  - Unified system
  - Real time optimization

Final Takeaways

- American ports have not been targeted… yet
- The ports are accessible & unprotected and contain a large number of civilians & dangerous materials
- The ports are facing a plethora of potential threats
  - Both Physical & Cyber
- Hard to obtain optimum security one piece at a time through the PSGP
- There is a strong need for a system that can not only Detect & Respond but can Predict & Prevent

Thank You



ARES SECURITY