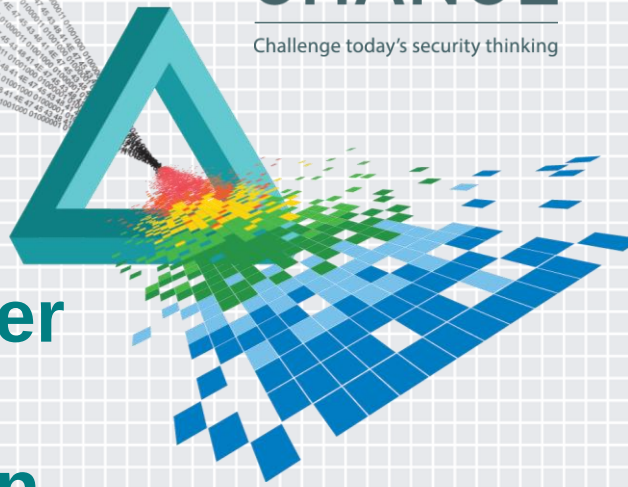
RSAConference2015
San Francisco | April 20-24 | Moscone Center

CHANGE
Challenge today's security thinking

SESSION ID: CXO-F02



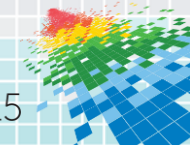
Cyber Security Operations Center (CSOC) for Critical Infrastructure Protection

Timothy Lee

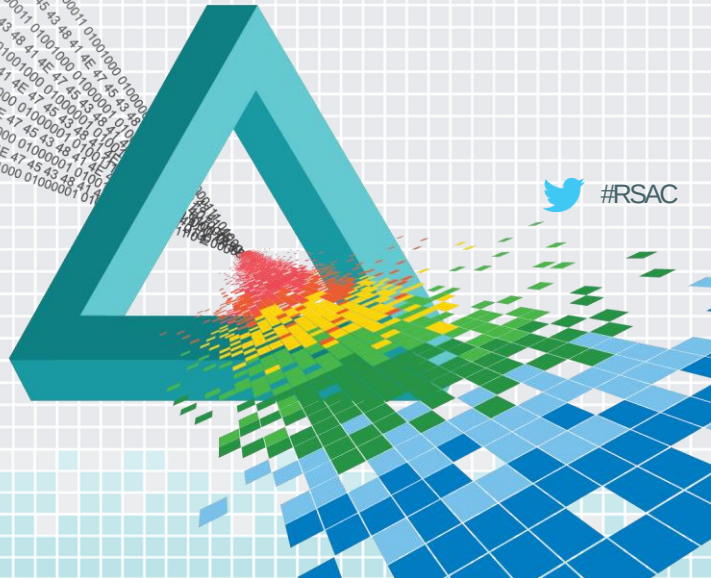
CISO
City of Los Angeles
@tswlj316

AGENDA

- Introduction
- Why do we need Cyber Security Operations Center (CSOC)?
- How did we sell it?
- How did we implement it?
- Results
- Summary



Introduction



The Port of Los Angeles

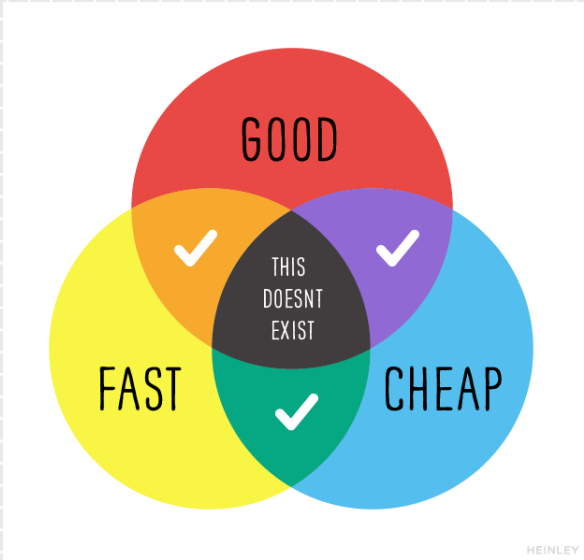
- 7,500 acres, 43 miles of waterfront, 270 berths, 23 cargo terminals, moving 8 million Twenty-foot Equivalent (TEU) per year
- Busiest container port in US
- $300 billion cargo value per year
- $23 billion tax revenue per year
- 1.2 million jobs throughout CA
- 3.6 million jobs throughout the US
- Identified by DHS as nation's critical infrastructure

The Project – CSOC

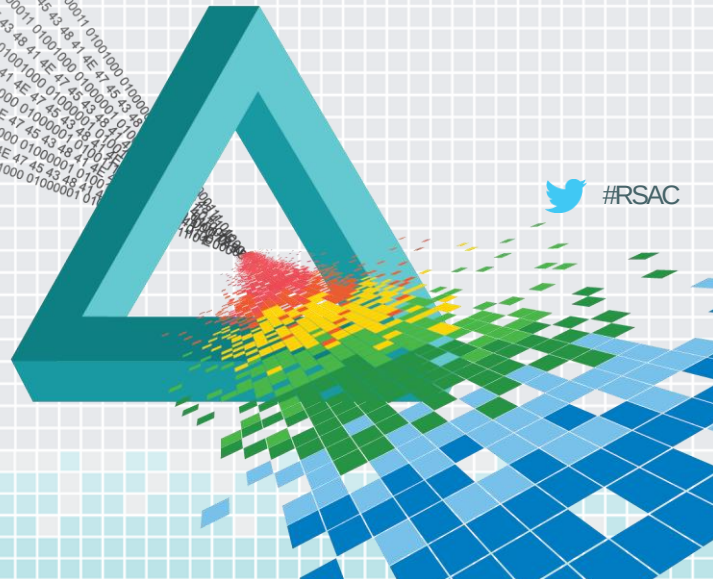
- Project Cost: $2.2 million
- Source of Funding: FEMA Port Security Grant Program (PSGP) FY 2012 (80/20)
- Project began: December 2013
- Project completed: August 2014
- Winner of 2014 American Association of Port Authorities (AAPA) Information Technology Award of Excellence

The Project - CSOC

- Technology/Services Included:
  - incident/threat Management
  - intrusion detection/prevention
  - security analytics
  - APT defense
  - network access control
  - network traffic aggregation and visibility
  - digital forensics
  - facility design and build



Why did we need CSOC?



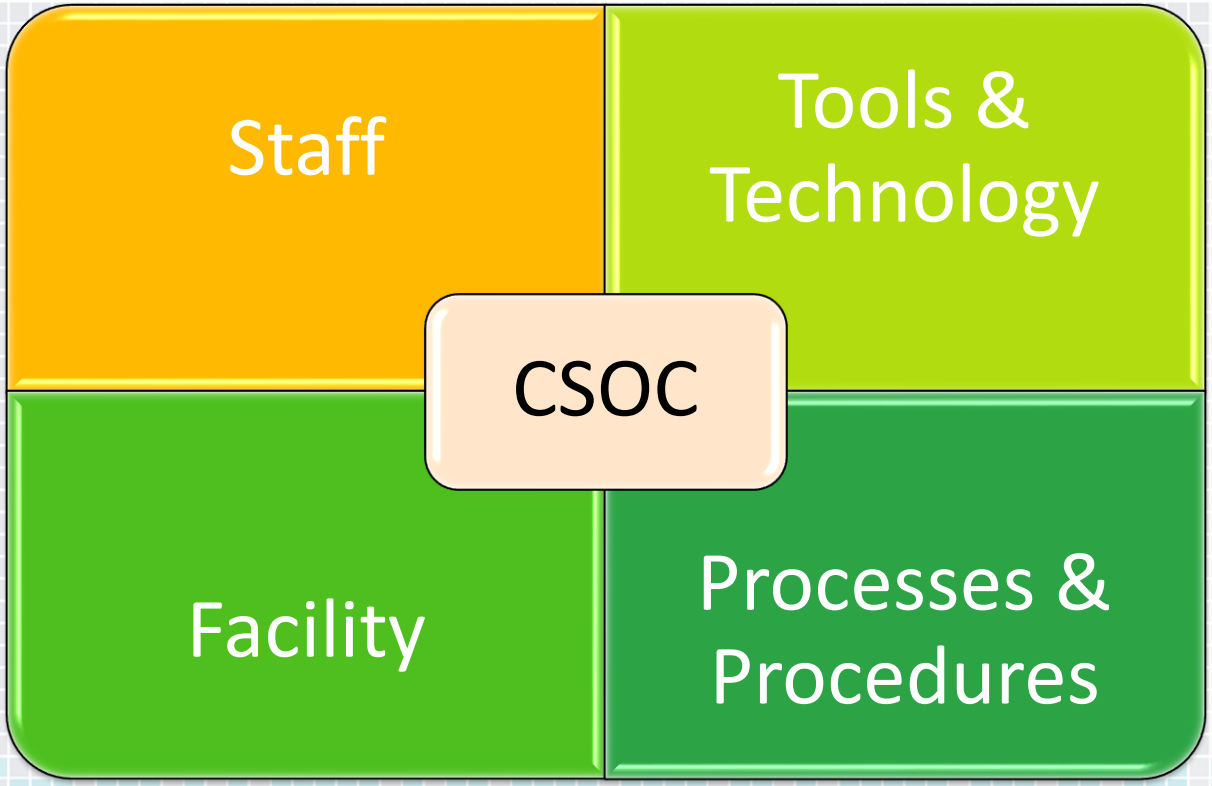
Nation's Critical Infrastructure

- President's Executive Order (EO) 13636 - *Improving Critical Infrastructure Cybersecurity*
- Presidential Policy Directive (PPD) 21 - *Critical Infrastructure Security and Resilience*
- Mayor of Los Angeles' Executive Directive No. 2 on *Cybersecurity*

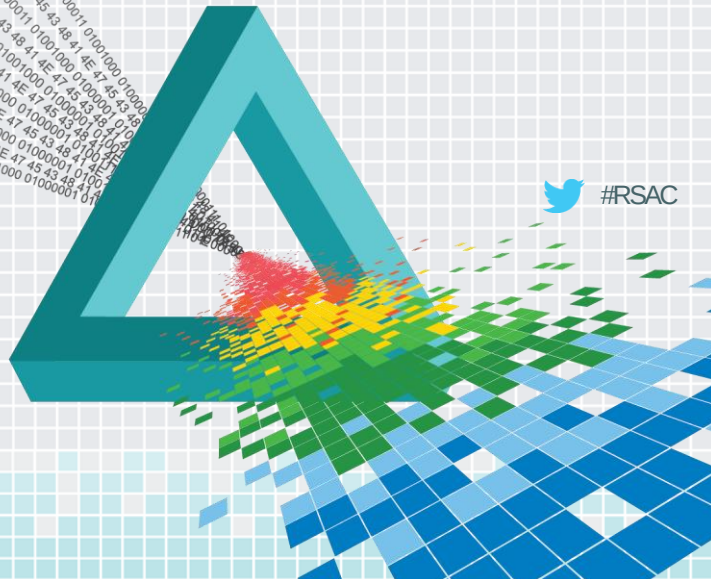
Problem

- IT Security team is understaffed
- Dispersed log capturing capabilities
- Minimal use of collaboration tools
- High value assets are not identified or tracked
- Lack of Incident Management System and IR training
- A threat intelligence program does not exist
- Incident workflow process and procedures
- Limited operational metrics
- Heavy reliance on vendor auto-updating of security tools
- Growing Cyber Threats

Solution – CSOC



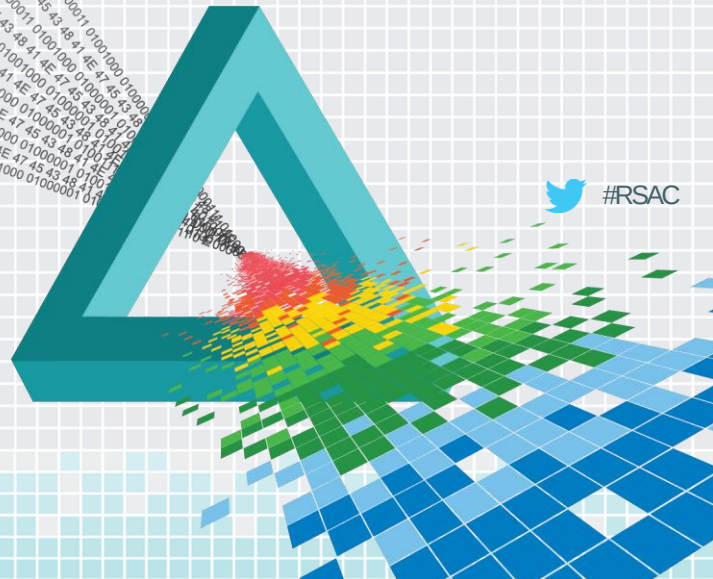
How did we sell it?



How did we sell it?

- Prepare to answer why you need CSOC
  - Security Audit Report (Recommendation and Action Plan)
  - Compliance Gap Assessment Report
  - Security metrics (numbers of intrusion attempts, incidents, outages caused by incidents, top attackers, threat activity and trends etc.
  - Present it from the business risk perspective
- Engage others outside of IT to also help sell it for us
- Provide potential risks of not implementing CSOC
- Provide real-world examples of cyber incidents and costs that your audience can relate to
- Provide source of funding for implementation and operations
- Align results to organizational goals

How did we implement it?



Methodology

Analysis

- Assess current state
- Visit vendor site to observe current technologies and best practices
- Identify desired future state
- Identify Gaps
- Develop baseline for the Design phase

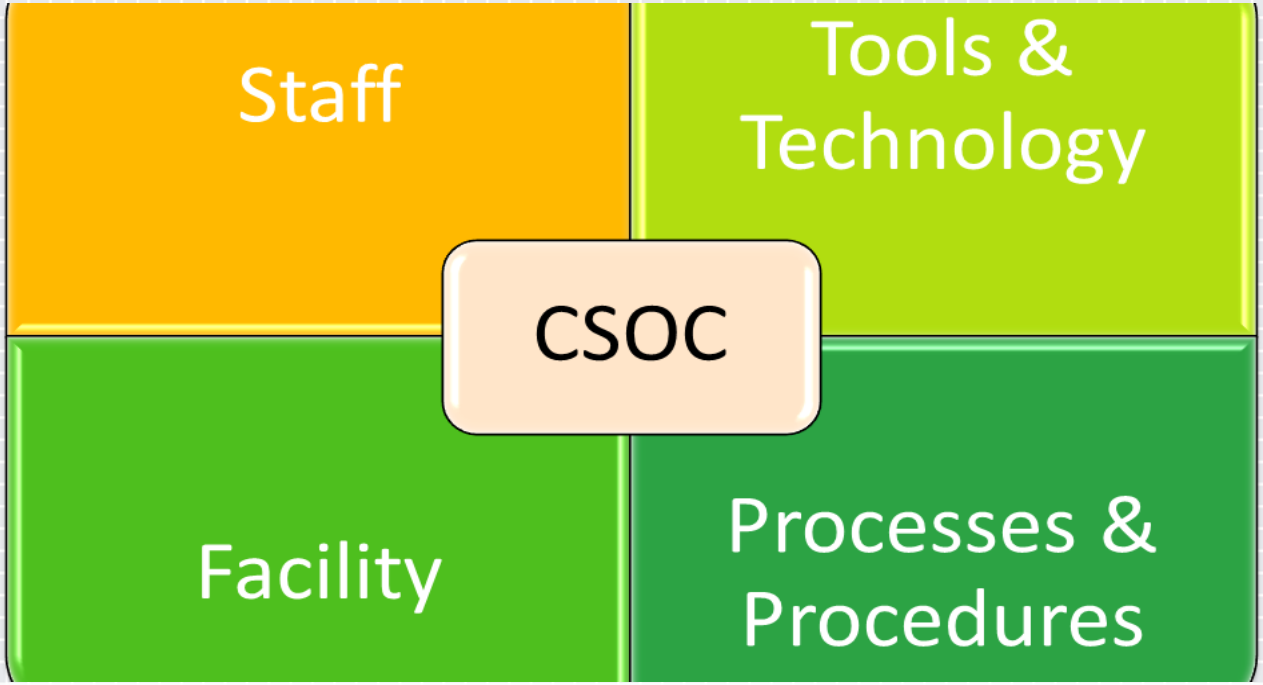
Design

- SOC organizational Structure
- Tool integration
- Develop Incident monitoring and response workflows
- Logical facilities design

Implement

- Technology integration
- SOC Operations Manual
- Alert aggregation process
- Key Performance Indicator /Metrics/Dashboard/Report
- Threat Intelligence integration
- Knowledge Transfer
- Training

CSOC Components



Tools and Technology

- Incident/Threat Management
- Intrusion Detection/Prevention
- Security Analytics
- APT Defense
- SIEM
- Network Access Control
- Network traffic aggregation and visibility
- Digital Forensics

Technology Integration

GRC

Situational Awareness, Metrics & Workflow

SIEM

Security Analytics

Correlation & Analysis

Log/Event Sources

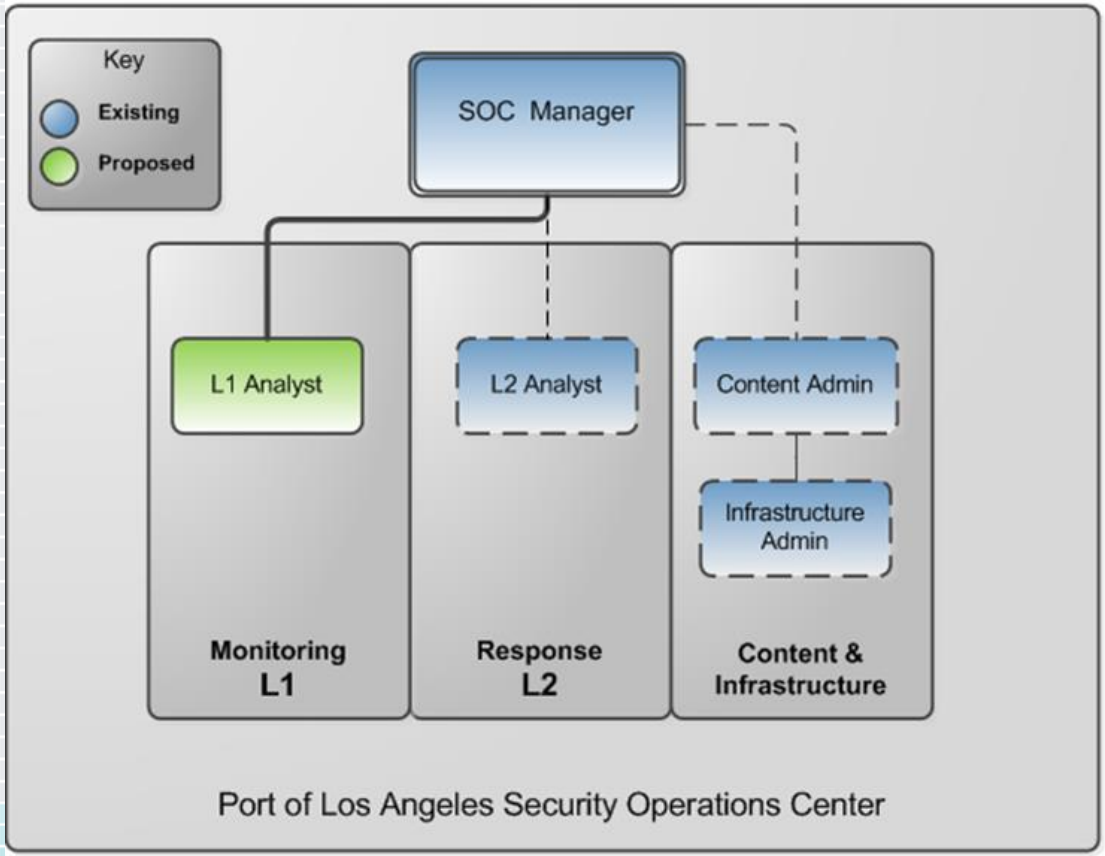
- Firewall
- IDS/IPS
- SSL VPN
- Network Access Control
- AD Event Logs
- APT
- Proxy
- Endpoint Protection
- Syslogs

Threat Intel Feeds

- MS-ISAC Feeds
- RSA Live Feeds
- In-house Threat Feeds

Data Sources

CSOC Organizational Structure



CSOC RACI

Activity	L1 Analyst	L2 Analyst	Content Admin	SOC Manager	CISO	Asset Owner	IT Help Desk
Initiate Incident Remediation	R	R		A			
Define Remediation Requirements	I	R		A			
Plan Remediation	I	C			A	R	R
Perform Remediation	I	C			A	R	R

R – Responsible A – Accountable C – Consulted I - Informed

Processes & Procedures

- SOC Operations Manual (Run Book)
  - SOC Policies
    - Incident Service Level Objective Policy
    - Incident Escalation Policy
    - Critical Incident Declaration Policy
  - Incident Response Plan
    - Level 1 , Level 2 Workflows
    - Critical Incident Management
  - Reporting and Metrics
    - CISO Dashboard, SOC Manager Dashboards
    - Situational Awareness, Daily Analysis Report

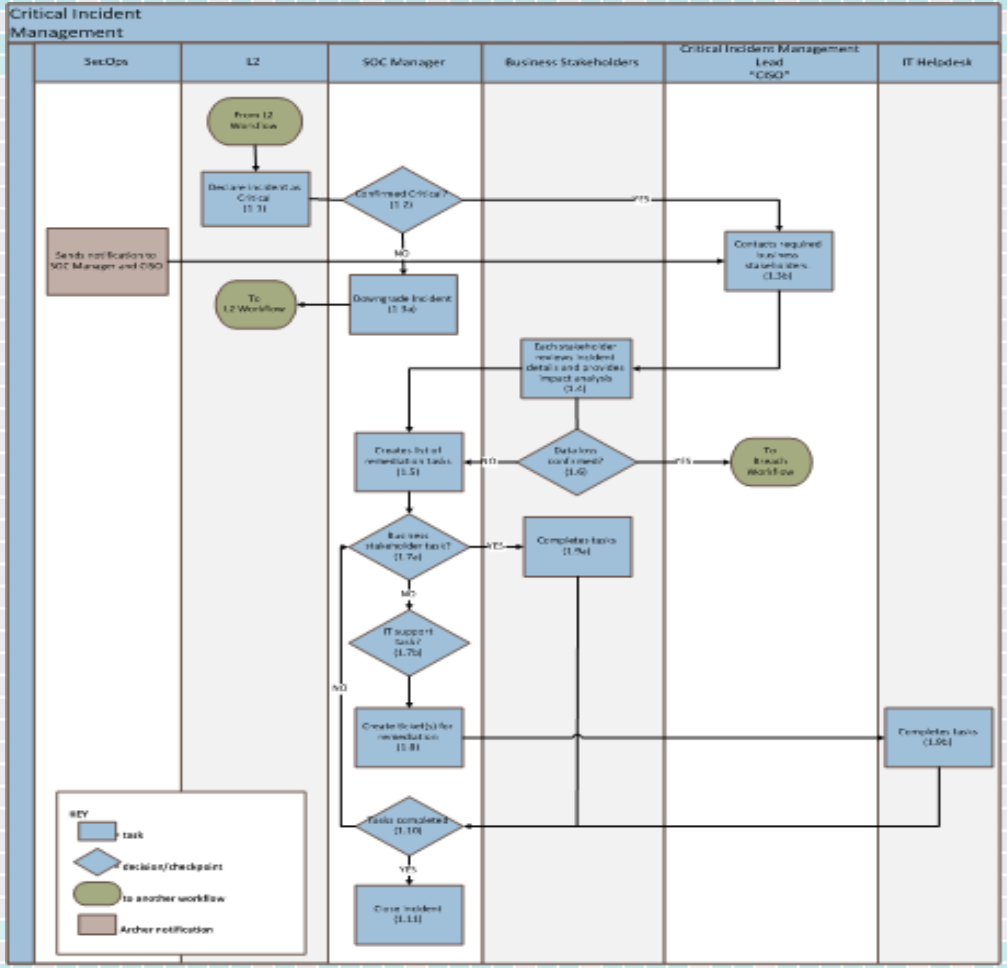
"We only have a few rules around here, but we really enforce them."

Incident Service Level Objective

Priority	Level	Response Time	Remediation/Escalation Time
P0	Critical	<= 1 Hour	<= 4 Hours
P1	High	<= 4 Hours	<= 1 Business Day
P2	Medium	<= 1 Business Day	<= 2 Business Days
P3	Low	>= 2 Business Days	> = 2 Business Days

Incident Escalation Flow

Critical Incident Handling Workflow



Facility Build Requirements

- Room Specifications
  - Length – 19’, Width 15’, Height – 20’
- Physical Security – Badge access, Privacy window film
- Power requirements
- Air conditioning
- Electrical and network requirements

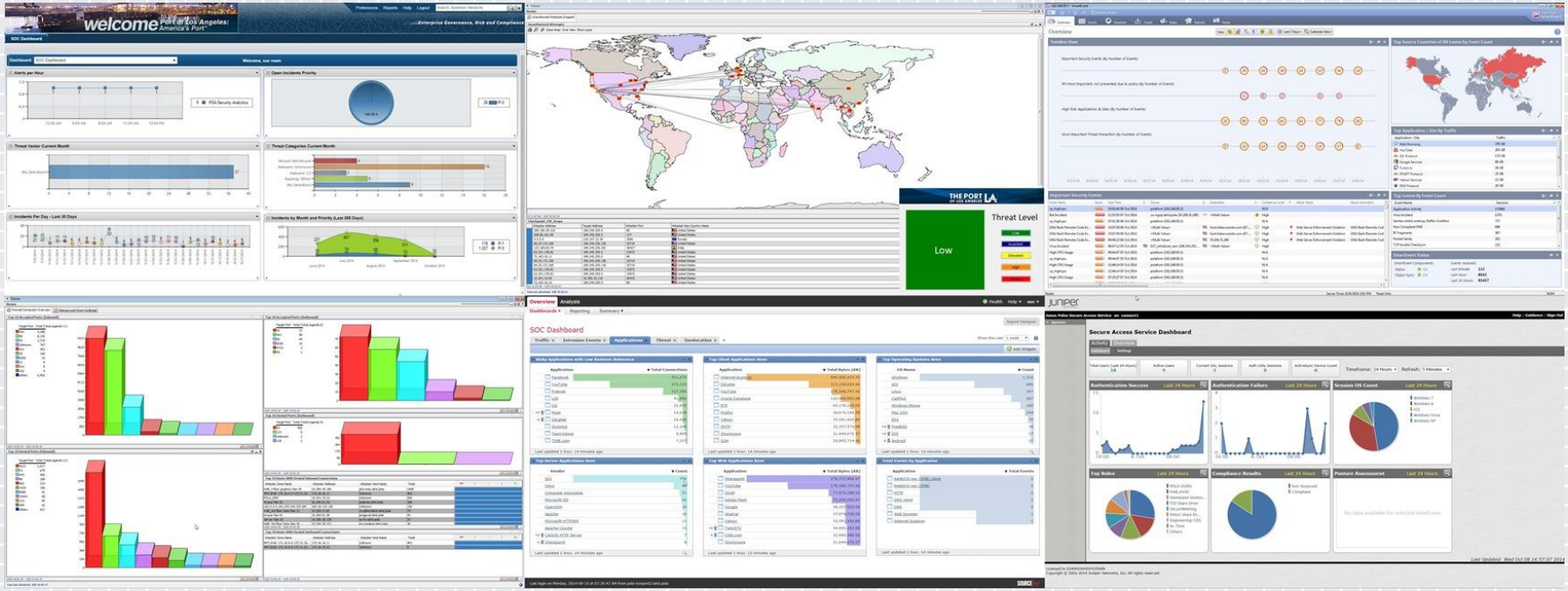
Facility Build Requirements - Continued

- SOC Room Consoles
- Remote Graphics Unit (RGU)
- Video Display Wall
  - 6 LED-based 55” full HD ultra narrow bezel arranged 2-high by 3-wide
  - Display wall controller
  - DVI cabling
  - Cabling and mounting hardware
  - The wall needed to be structurally enforced to hold the weight of the displays
- Audio System

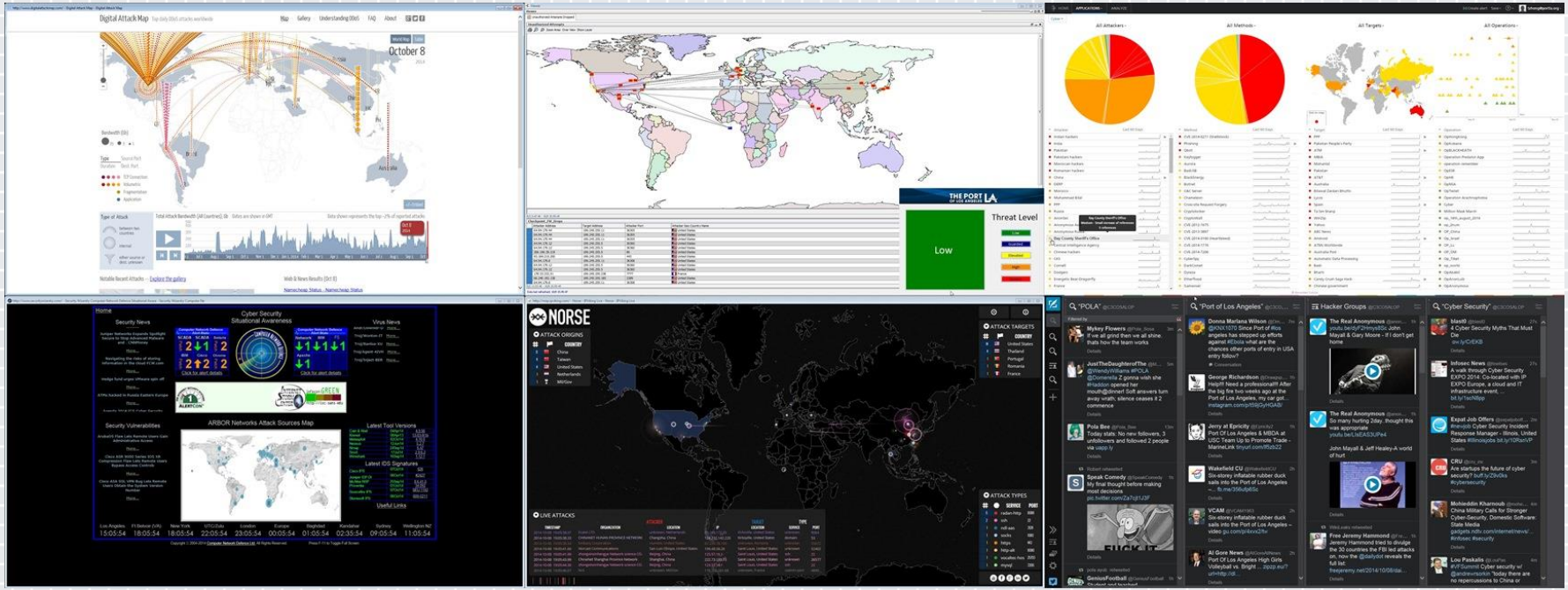
CSOC Conceptual Drawing

Results

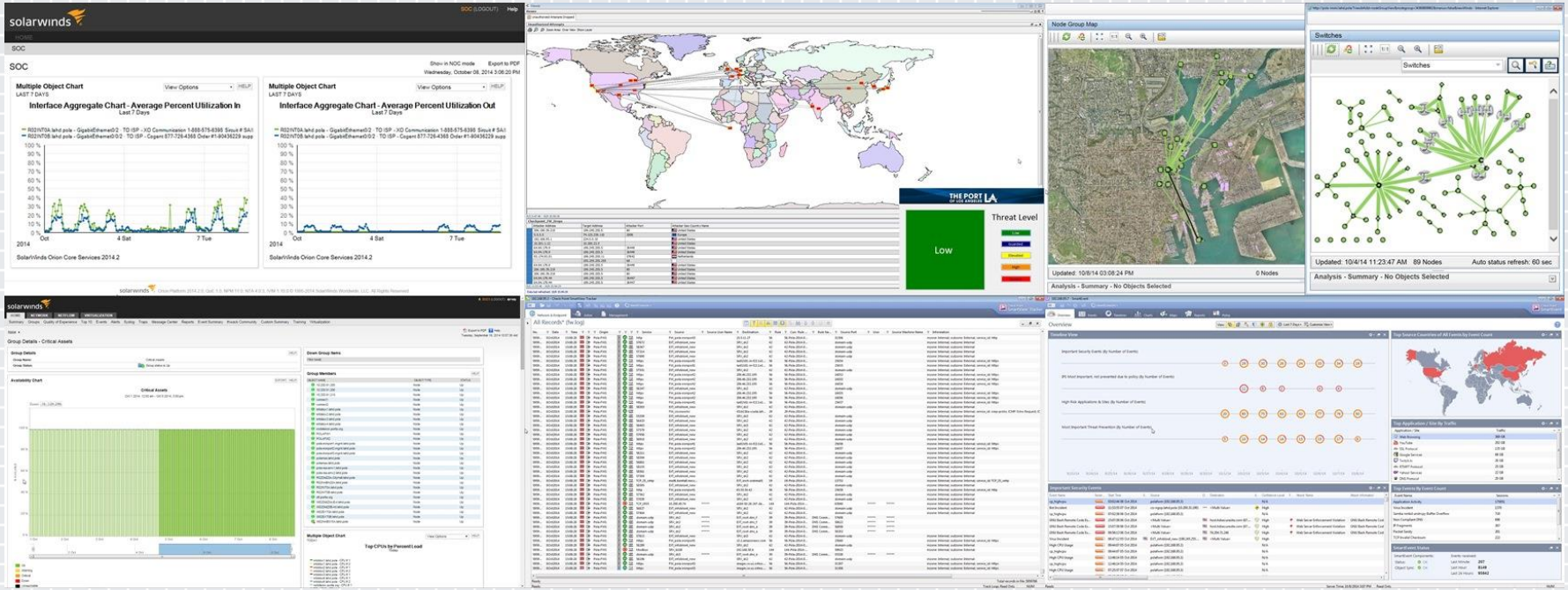
Dashboard 1 - Overview



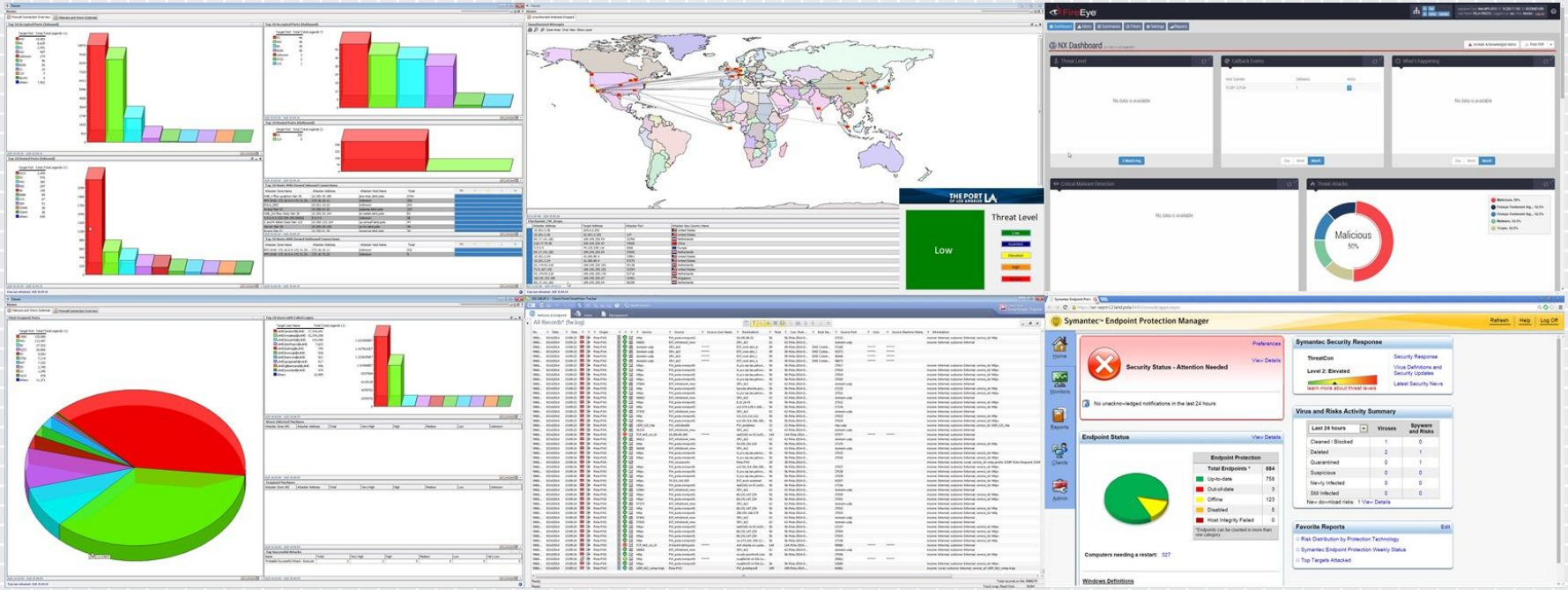
Dashboard 2 – National Cybersecurity Posture



Dashboard 3 – Denial of Service Attack

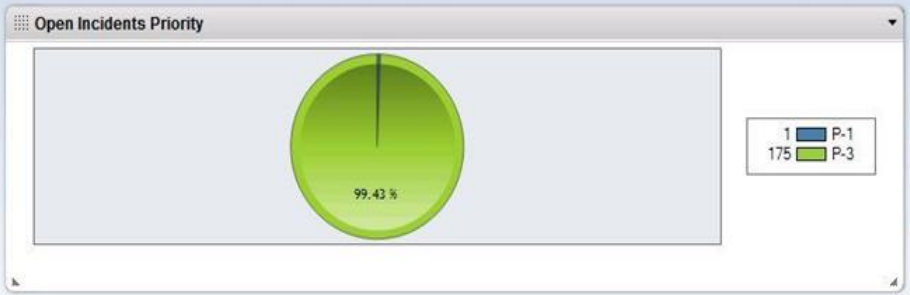


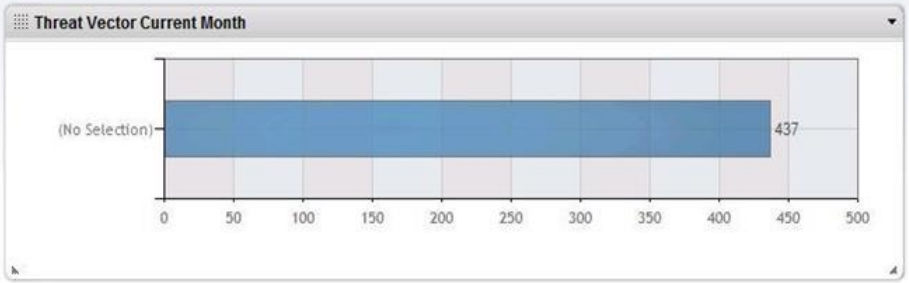
Dashboard 4 – Malware

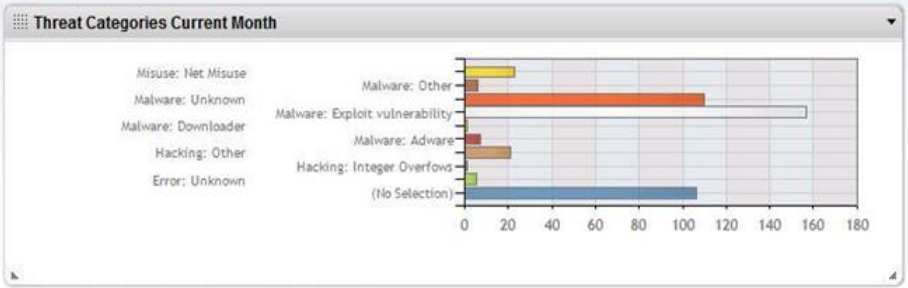


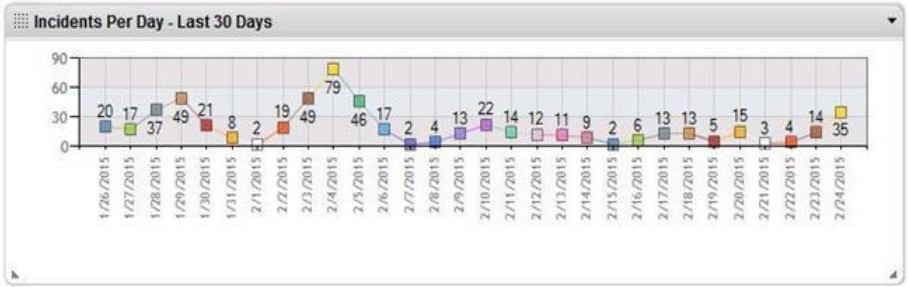
CISO Dashboard

Click to Expand the Navigation Menu









The Project was featured in Seaports Magazine

WINNERS HONORED
in AAPA's 2014 IT, Environmental Improvement and Communications
AWARDS PROGRAMS

Congratulations to all of the ports that submitted winning entries to the 2014 AAPA Communications, Environmental Improvement and Information Technology awards competitions.

The winners in these three programs were recognized during a luncheon on Thursday, Nov. 13, at AAPA's 103rd Annual Convention and Exposition, hosted by the Port of Houston Authority.

• • •

Since 1966, AAPA's Communications Awards Program has recognized excellence in the products and services that ports produce to meet their public relations and marketing goals.

Each year, one port receives the Dan Maynard Communications Award for Overall Excellence, based on the total score of all its winning entries. This year's Dan Maynard Communications Award winner is the **Port of Long Beach**, which will retain AAPA's only "traveling" trophy until a 2015 winner is announced.

The **Port of Los Angeles** and **Georgia Ports Authority** received second and third place overall awards – the AAPA 2014 Overall Communications Award of Distinction and AAPA 2014 Overall Communications Award of Merit.

Overall, 21 ports received awards in AAPA's 2014 Communications Awards competition; 34 submissions from 11 ports earned an Award of Excellence, while 36 submissions from 14 ports scored an Award of Distinction, and 36 submissions from 15 ports received an Award of Merit.

• • •

The **Port of Los Angeles**' "Cyber Security Operations Center" was named the overall winner of this year's Information Technology Award. The IT Awards program, which began in 2002, highlights port technology accomplishments in the areas of Port Operations and Management Systems and in Improvements in Intermodal Freight Transportation.

• • •

Since 1973, AAPA's Environmental Improvement Awards program has recognized activities that benefit the environment at its member ports. This awards program had four distinct project entry categories: 1) Environmental Enhancement; 2) Mitigation; 3) Stakeholder Awareness, Education & Involvement; and 4) Comprehensive Environmental Management.

The winner in the 2014 Environmental Improvement Awards' Comprehensive Environmental Management award was the **Port of Tacoma** with its entry, "Biofiltration: West Hylebos Log Yard." Also in this category, the **Maryland Port Administration** received an Honorable Mention for its entry, "Water Quality Master Plan," while the **Toledo-Lucas County Port Authority** received an Honorable Mention for its entry, with its successful project, "McKay Bay Restoration."

The Port of Los Angeles' Cyber Security Operations Center, which was the overall winner of the Information Technology Award program.

Georgia Ports Authority's Voluntary Diesel Emmissions Reduction Through Investment in Equipment.

Port of Portland's Environmental Initiatives at Seaports Worldwide: A Snapshot of Best Practices.

Port of Tacoma's Biofiltration: West Hylebos Log Yard.

Port Tampa Bay's McKay Restoration.

The winner of the 2014 Environmental Improvement Awards' Stakeholder Awareness, Education & Involvement category was the **Port of Portland** for its "Environmental Initiatives at Seaports Worldwide: A Snapshot of Best Practices" entry.

The winner of AAPA's 2014 Environmental Improvement Awards' **Authority** for its entry, "Voluntary Diesel Reduction Through Investment in Equipment."

AAPA Awards

AAPA's annual and biennial awards programs recognize the best practices in the port industry across five disciplines: Communications, Environmental Improvement, Information Technology, Facilities Engineering, and Cruise.

To learn more about AAPA's annual awards programs, visit www.aapa-ports.org and click on Annual Awards Program under the Programs & Events tab.

Apply

- Conduct SOC readiness assessment before anything
- Look for grant opportunities
- Pick the right tools and technology
- Be mindful of Operating Cost
- Pick the right contractor
- Pick the right team. Invest in people
- Cybersecurity collaboration and information sharing are essential

Resources

- Security Operation Center Concepts & Implementation – Renaud Bidou
- Cybercrime Kill Chain vs Defense Effectiveness – Stefan Frei, Phd; Francisco Artes – NSS Labs
- Ten Strategies of a World-Class Cybersecurity Operations Center – Carson Zimmerman, October 2014
- Building An Intelligence Driven Security Operations Center – RSA Technical Brief, June 2014

RSAConference2015

San Francisco | April 20-24 | Moscone Center

Timothy Lee, CISSP PMP
CISO
City of Los Angeles

timothy.lee@lacity.org

www.linkedin.com/in/timothyswlee