Harnessing the Power of Visualization for Industrial Control Systems

Industrial Control Systems Joint Working Group

Alan A. Hendricks, CISSP, CISM

Emily Frye

April 2010

We Will Cover

- Nutshell Summary of Cybersecurity in Critical Infrastructure
- Approaches to Date and Current Model
  - Case Study: TSA SOC
- Leap in thinking
- Next-Generation Cybersecurity for CI and ICS: Visualization
  - Case Study: FAA
- Comparative Analysis

How We Got Here

- Individual operations of entities across most sectors
- Concept of CI sector
  - 1996 – PCCIP
  - Early ISACs/PCIS: legacy of physical and cyber separation
- 9/11/2001 reinvigorated CI effort
- Situational awareness capability in physical
- Situational awareness capability for cyber evolves:
  - Entity SOC ⟶ Function-Wide SOC ⟶ Sector SOC

What Kinds of SOC Apply in ICS?

- Security Operations Center that covers all networks that support a given Function, Entity, or both
  - Function: flow of oil in a pipeline (classic ICS)
  - Entity: Chemical plant
  - Scaling up: State (Virginia, Alabama, California) or Sector: Energy
  - Or some mix of these: comprehensive system monitoring across many or all functions and networks within a given environment

Function/Sector SOC: An Example

- Function-wide SOCs provide the best situational awareness for cyber (that we know of)
- Some sectors are aware of the need and have moved to establish a (function-wide) sector-wide SOC:
  - The TSA Example

TSA SOC Overview

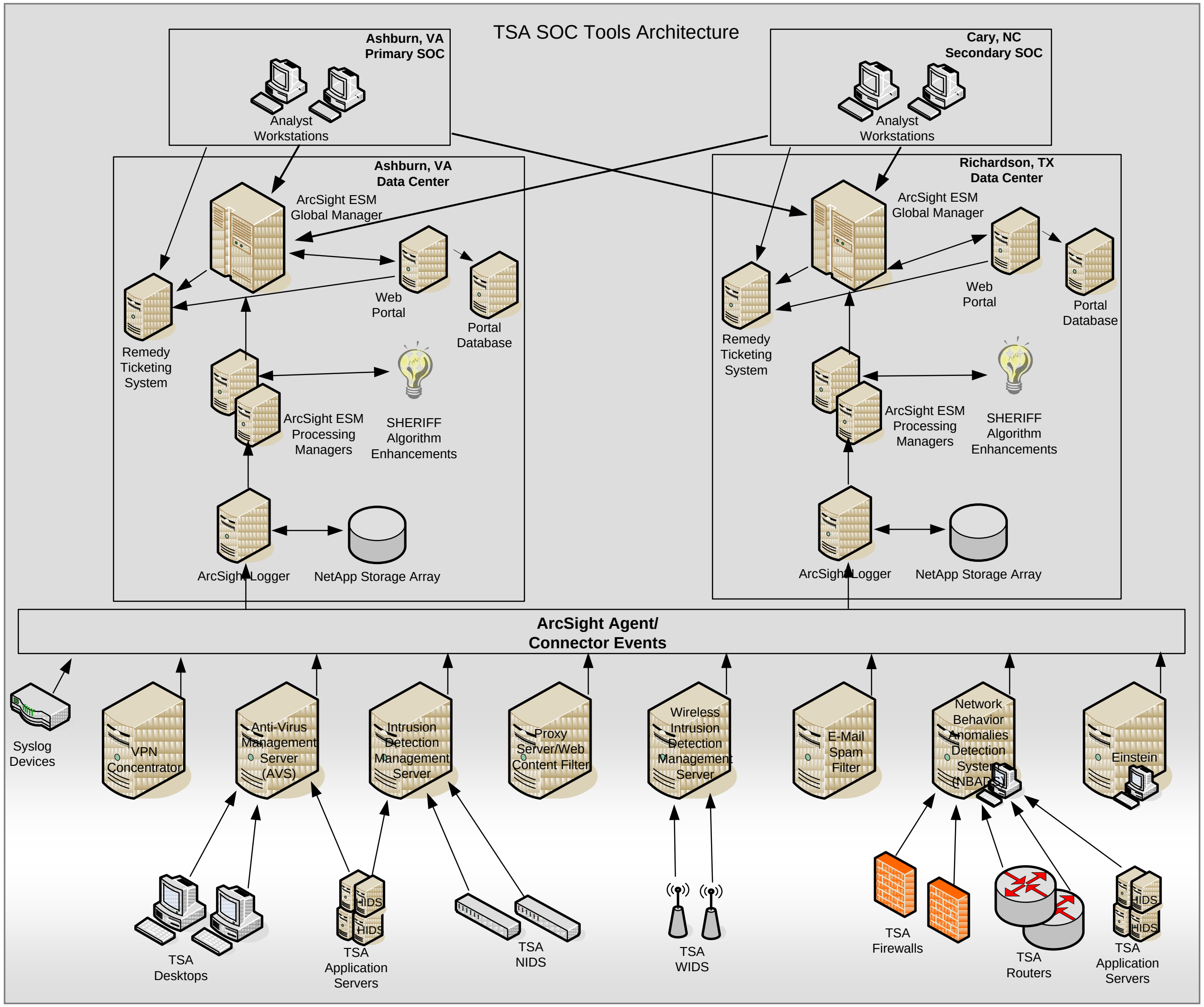
- Key objectives:
  - Partner with TSA to <u>independently</u> monitor their IT enterprise by detecting, analyzing and coordinating the response to cyber attacks
  - Serve as an <u>independent</u> security advocate for engineering future TSA IT infrastructure solution
  - Assess emerging security threats

- Approach to accomplishing objectives:
  - Provide a fully outsourced 24x7x365 SOC solution that leverages robust physical and technology platforms with proven SOC operations best practices
  - Provide a security engineering cadre and a research/evaluation environment to evaluate and provide feedback on potential IT solutions, as well as emerging security technologies and techniques

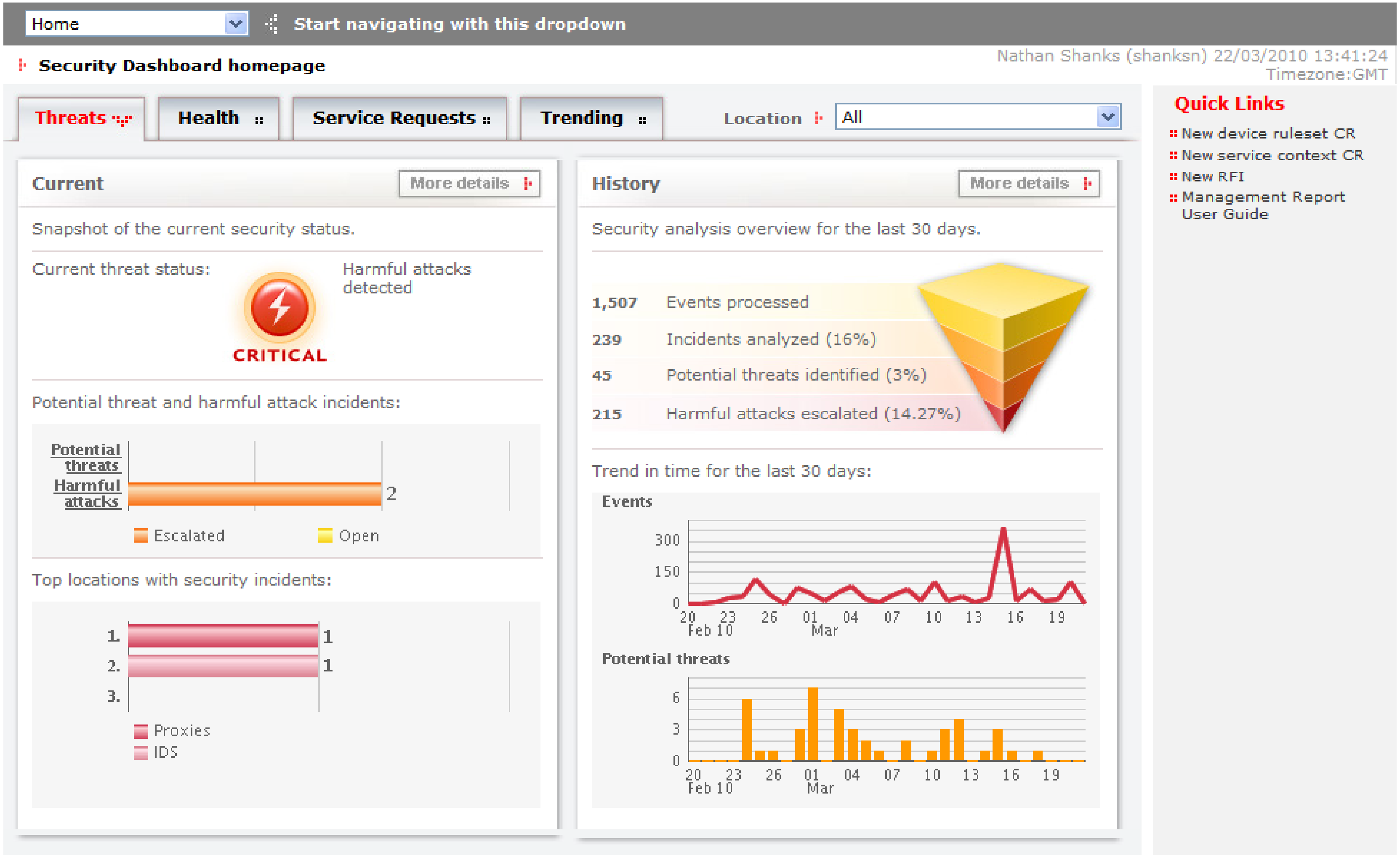
Objectives

- Review and evaluate the configurations of the security devices and recommends changes to remediate deficiencies
- Verify and validate any suspected security events, including breaches, intrusions, policy violations, and attacks against TSA
- Coordinate and support response to security events and incidents
- Analyze TSA IT infrastructure vulnerability scans, assess vulnerabilities and risks, recommend actions, and monitor progress and compliance against plan of action and milestones (POA&Ms)
- Monitor the IT industry and advise on emerging security technologies, architectures, methods, and practices
- Evaluate the TSA IT security infrastructure and IT security operations, and recommend improvements in security technologies, methods, process, and procedures

SOC Architecture



Portal View - Threats



Security Dashboard homepage

Nathan Shanks (shanksn) 22/03/2010 13:41:24
Timezone:GMT

Current

Snapshot of the current security status.

Current threat status: CRITICAL

Harmful attacks detected

Potential threat and harmful attack incidents:

Top locations with security incidents:

History

Security analysis overview for the last 30 days.

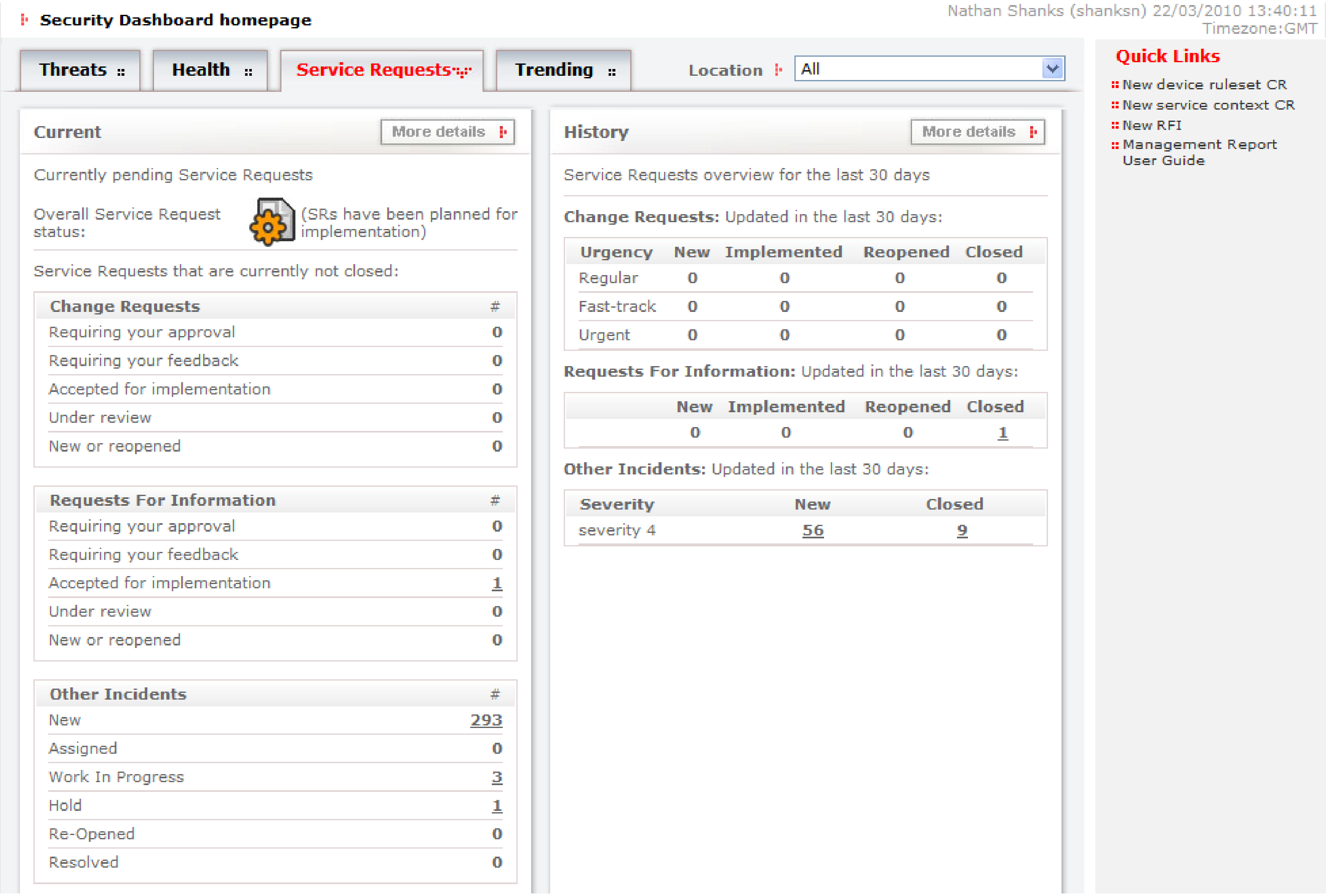
1,507	Events processed
239	Incidents analyzed (16%)
45	Potential threats identified (3%)
215	Harmful attacks escalated (14.27%)

Trend in time for the last 30 days:

Quick Links

- New device ruleset CR
- New service context CR
- New RFI
- Management Report User Guide

Portal View - Service Requests



Security Dashboard homepage

Nathan Shanks (shanksn) 22/03/2010 13:40:11
Timezone:GMT

Quick Links

- New device ruleset CR
- New service context CR
- New RFI
- Management Report User Guide

Current

Currently pending Service Requests

Overall Service Request status: (SRs have been planned for implementation)

Service Requests that are currently not closed:

Change Requests	#
Requiring your approval	0
Requiring your feedback	0
Accepted for implementation	0
Under review	0
New or reopened	0

Requests For Information	#
Requiring your approval	0
Requiring your feedback	0
Accepted for implementation	1
Under review	0
New or reopened	0

Other Incidents	#
New	293
Assigned	0
Work In Progress	3
Hold	1
Re-Opened	0
Resolved	0

History

Service Requests overview for the last 30 days

Change Requests: Updated in the last 30 days:

Urgency	New	Implemented	Reopened	Closed
Regular	0	0	0	0
Fast-track	0	0	0	0
Urgent	0	0	0	0

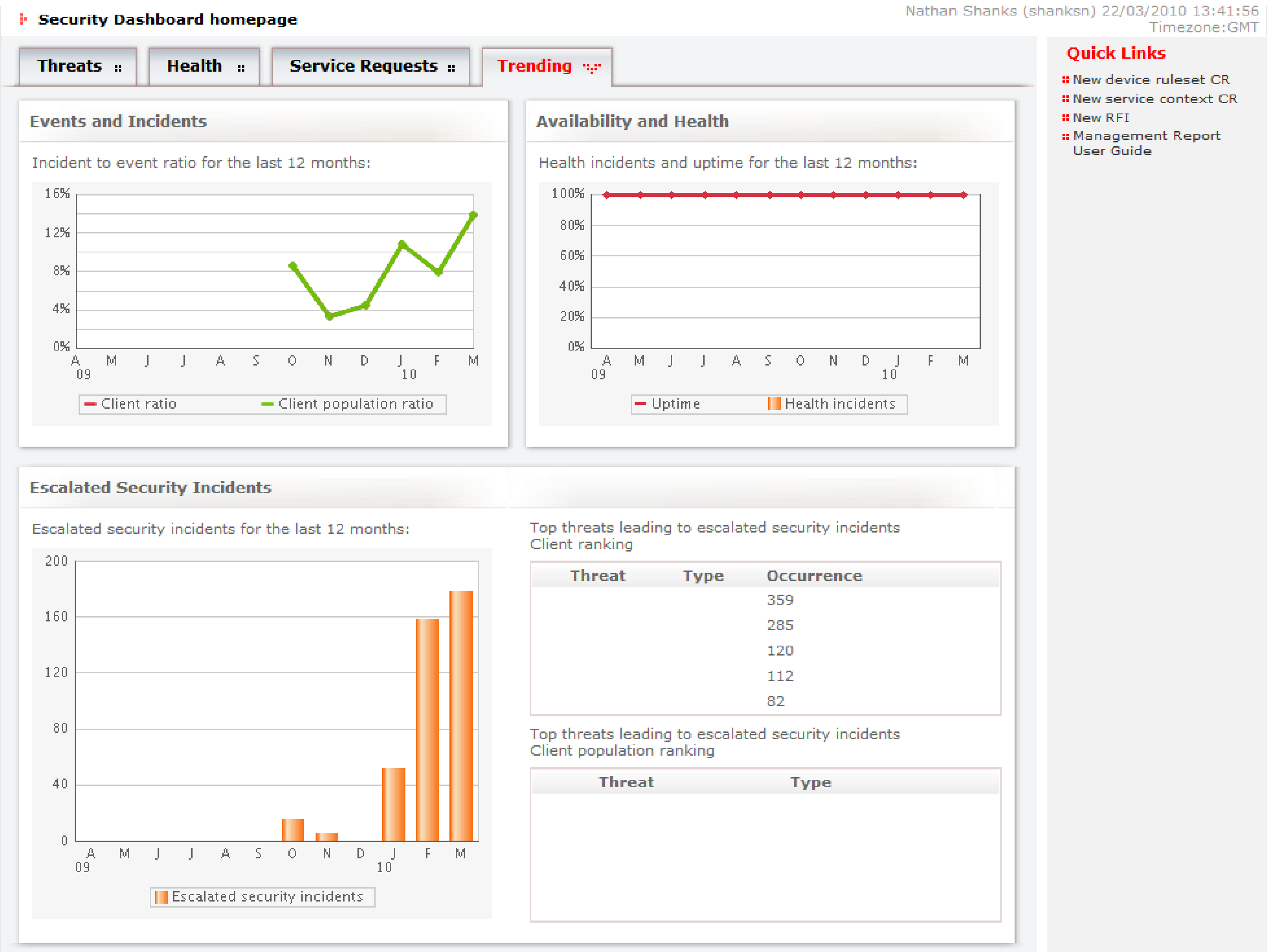
Requests For Information: Updated in the last 30 days:

New	Implemented	Reopened	Closed
0	0	0	1

Other Incidents: Updated in the last 30 days:

Severity	New	Closed
severity 4	56	9

Portal View - Trending



Security Dashboard homepage

Nathan Shanks (shanksn) 22/03/2010 13:41:56
Timezone:GMT

Quick Links

- New device ruleset CR
- New service context CR
- New RFI
- Management Report User Guide

Events and Incidents

Incident to event ratio for the last 12 months:

Availability and Health

Health incidents and uptime for the last 12 months:

Escalated Security Incidents

Escalated security incidents for the last 12 months:

Top threats leading to escalated security incidents
Client ranking

Threat	Type	Occurrence
		359
		285
		120
		112
		82

Top threats leading to escalated security incidents
Client population ranking

Threat	Type

Critical Infrastructure Physical Side … Leap Forward

- Burst of activity around Visualization capabilities
  - Google Earth started a whole new appreciation for the maturity of visualization techcnologies
  - Recent application in Homeland Security/Critical Infrastructure has moved to emergency-service support
  - VIPER/Virtual Alabama → VUSA Project are good examples
- 2009 issuance of 20 Critical Controls

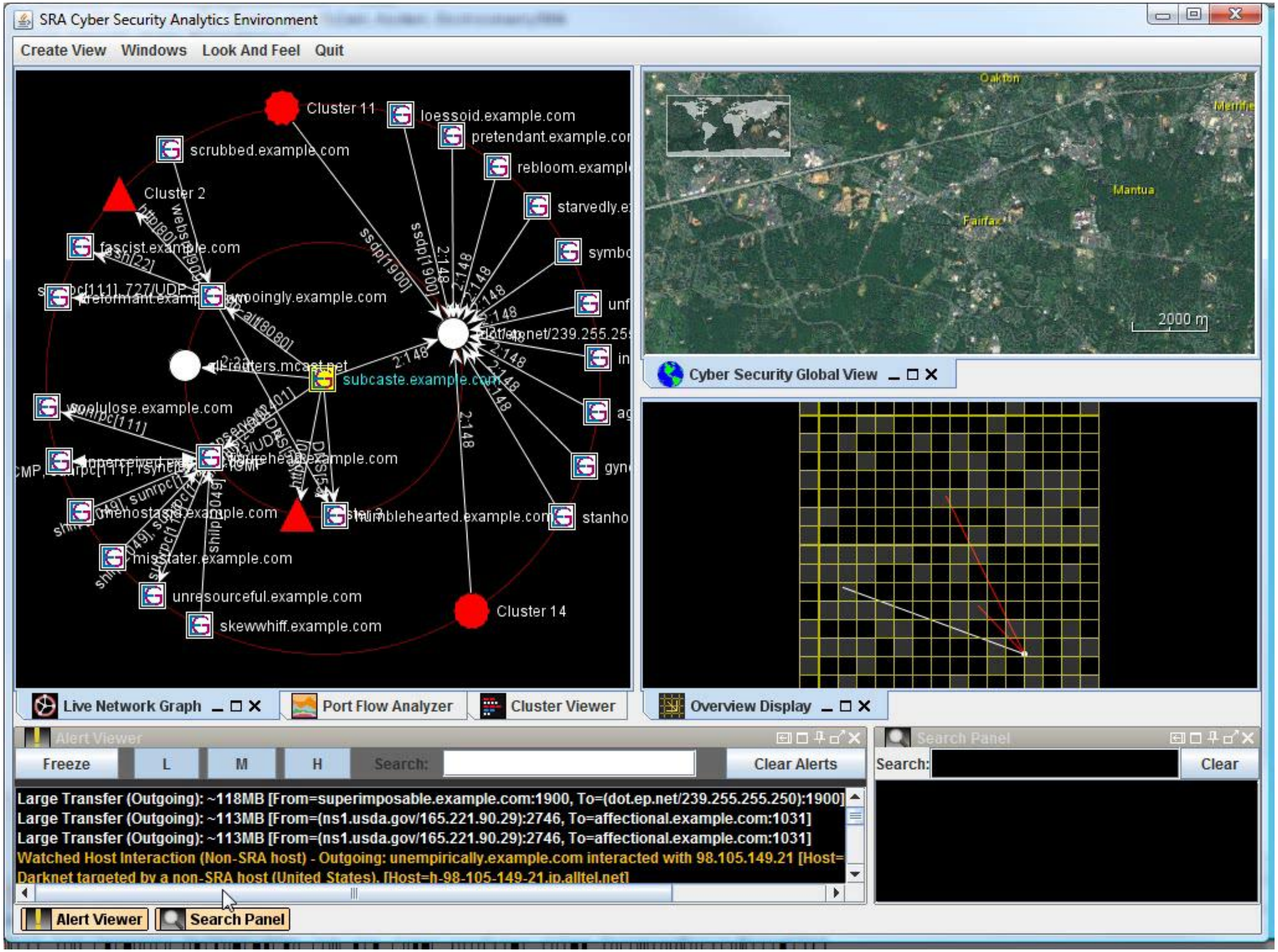
- ***If visualization offers great promise on the physical side, could it work on the cyber side too?***

Doppler
Light
Heavy

Visualization for CI - ICS Networks: What Could We See?

- ***Live Network Graph with customizable centricity***
- ***3D Geospatial View***
- ***Zoomable/Pannable IPV4 Map***
- PortFlow Display
- Ontology Viewer/Editor
- Rule Viewer
- Alert Viewer
- Annotation Viewer
- System Display
- Cluster Display
- Search Dialog

What Does This Look Like?



```
Large Transfer (Outgoing): ~118MB [From=superimposable.example.com:1900, To=(dot.ep.net/239.255.255.250):1900]
Large Transfer (Outgoing): ~113MB [From=(ns1.usda.gov/165.221.90.29):2746, To=affectional.example.com:1031]
Large Transfer (Outgoing): ~113MB [From=(ns1.usda.gov/165.221.90.29):2746, To=affectional.example.com:1031]
Watched Host Interaction (Non-SRA host) - Outgoing: unempirically.example.com interacted with 98.105.149.21 [Host=
Darknet targeted by a non-SRA host (United States). [Host=h-98-105-149-21.ip.alltel.net]
```

Summary: Compare and Contrast

Traditional SOC	Visualization-Enabled SOC
Low stakeholder buy-in required	Stakeholder acceptance important for optimizing function
Moderate-risk environment (Small Business Administration; lower-impact networks)	Moderate-high risk environment (Critical Infrastructures, ICS, known targets)
Quick implementation (based upon reporting-only paradigm – 1 B security events/month)	Less-rapid implementation
Summary Reporting and Analytics	System-Wide Awareness/Broad-Scale/System-of-Systems

Questions and Discussion

Contact Information/Feedback

Emily Frye

Emily_Frye@sra.com / 703-284-6645

Alan Hendricks

Alan_Hendricks@sra.com / 703-886-9255