Global Situational Awareness with Free Tools

Dennis M. Allen
CERT/SEI/CMU

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 JAN 2015	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Global Situational Awareness with Free Tools	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Allen /Dennis	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**18**	

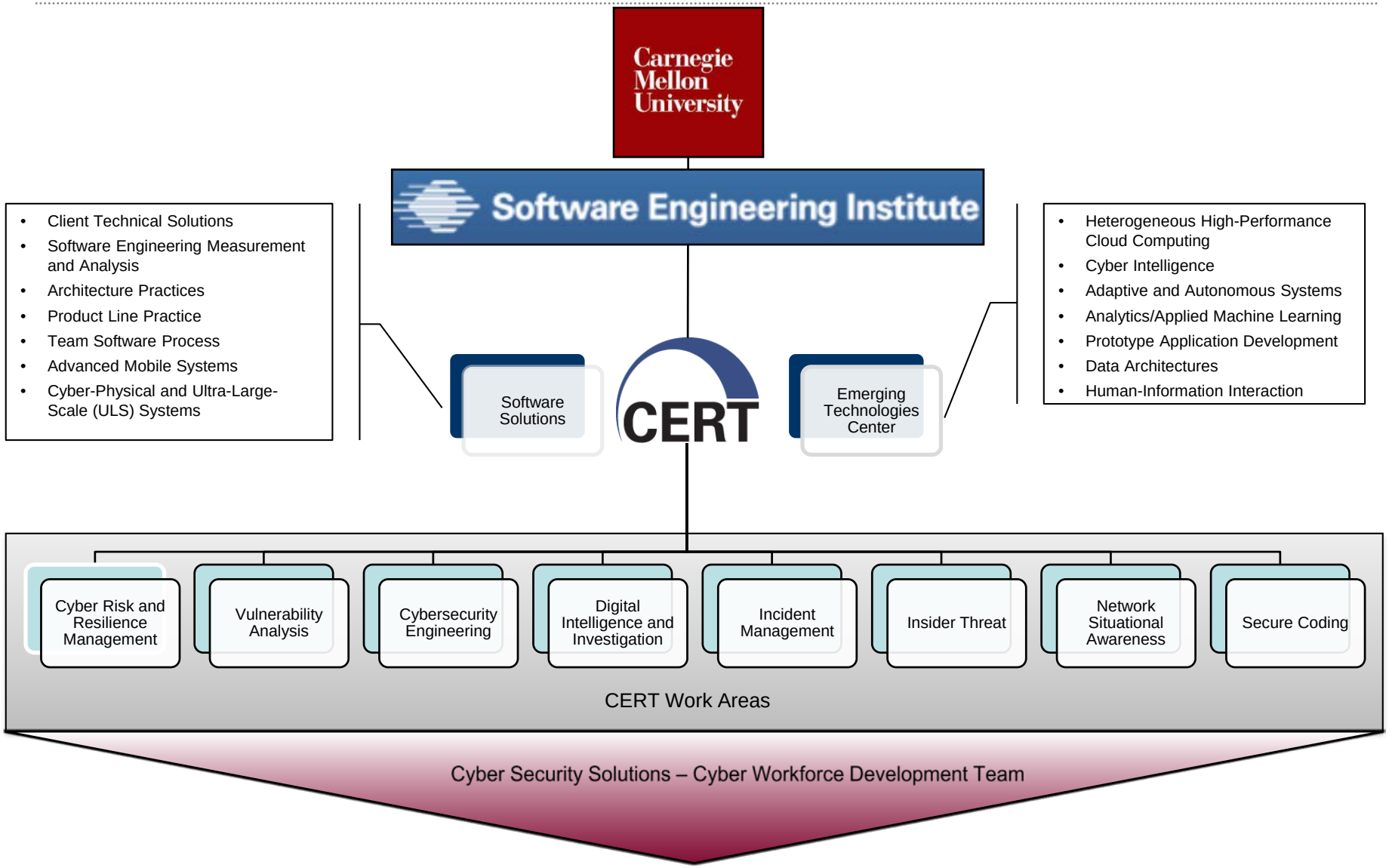
Copyright 2015 Carnegie Mellon University

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0002094

Who We Are

http://www.sei.cmu.edu



Me – Not Me

- Not Me
  - http://en.wikipedia.org/wiki/Dennis_Allen_(American_football)
  - http://en.wikipedia.org/wiki/Dennis_Allen_(criminal)
  - www.dennisallen.com
- Me
  - www.linkedin.com/pub/dennis-allen-cissp/4/972/a70
  - How to become a Cyber Warrior podcast http://www.cert.org/podcasts/podcast_episode.cfm?episodeid=34730
  - Digital Investigation Workforce Development http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=52445

Overview

- What is a Common Operating Picture (COP)
- COP Challenges
- Nagios and Google Earth (with a live demo)
- Lessons Learned

What is a COP?

"A common operational picture (COP) is a single identical display of relevant (operational) information (e.g. position of own troops and enemy troops, position and status of important infrastructure such as bridges, roads, etc.) shared by more than one Command. A COP facilitates collaborative planning and assists all echelons to achieve situational awareness."

Source: http://en.wikipedia.org/wiki/Common_operational_picture

Why me

Why Global Situational Awareness?

- Coordinate cyber events
  - Incident Response
  - Scope/Impact
- Optimization
- Continuity of Operations
- Proactive monitoring
  - Anomaly detection
  - Intel tipper

What data do we have?

- Availability
  - Servers & Services
- IDS/IPS Alerts
  - Network and/or Host
- Network Monitoring
  - MRTG, NTOP, Flow
- Tickets
- Other Logs
  - Security Events
  - System Events
  - Performance data

Anything Non-Cyber?

What data is important?

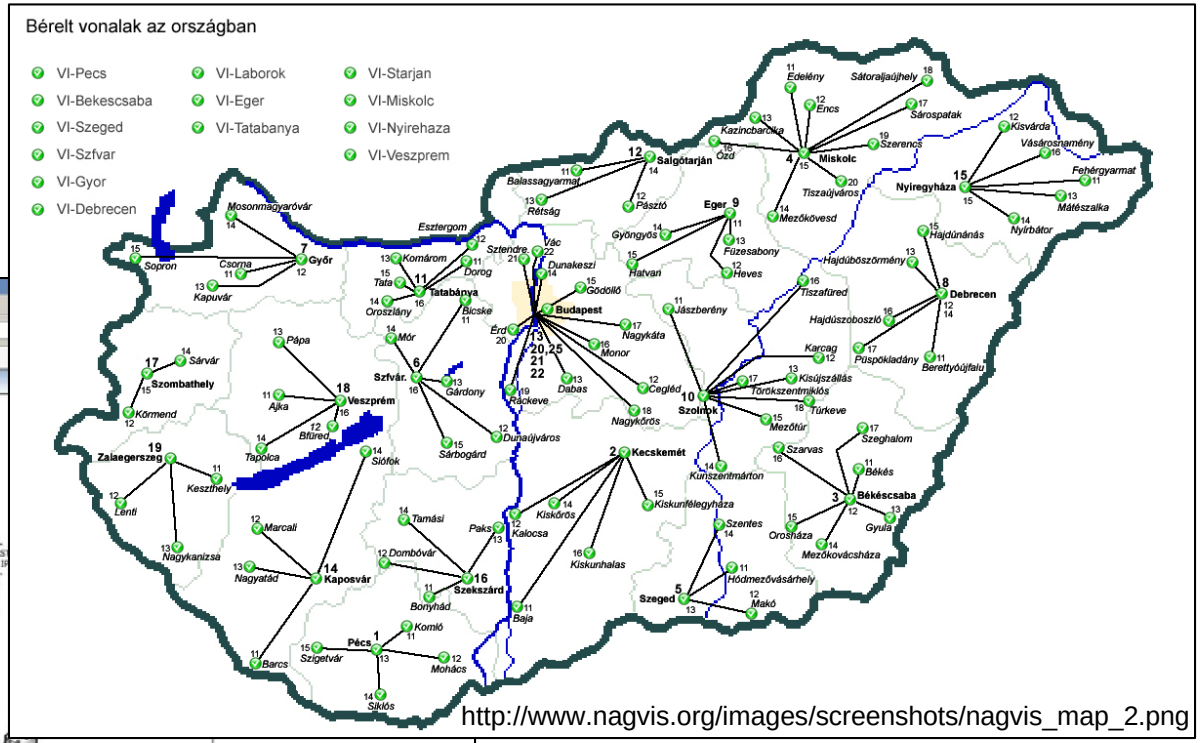
- Confidentiality
  - Data Loss Prevention (DLP)
- Integrity
  - File Integrity Monitoring (e.g. Tripwire)
  - Maybe performance monitoring (e.g. SNMP, MRTG)
- Availability
  - Easier to monitor (e.g. Nagios)
- Authentication/Authorization
  - Important, but often overlooked
  - Log management (e.g. Splunk)

Anything Non-Cyber?

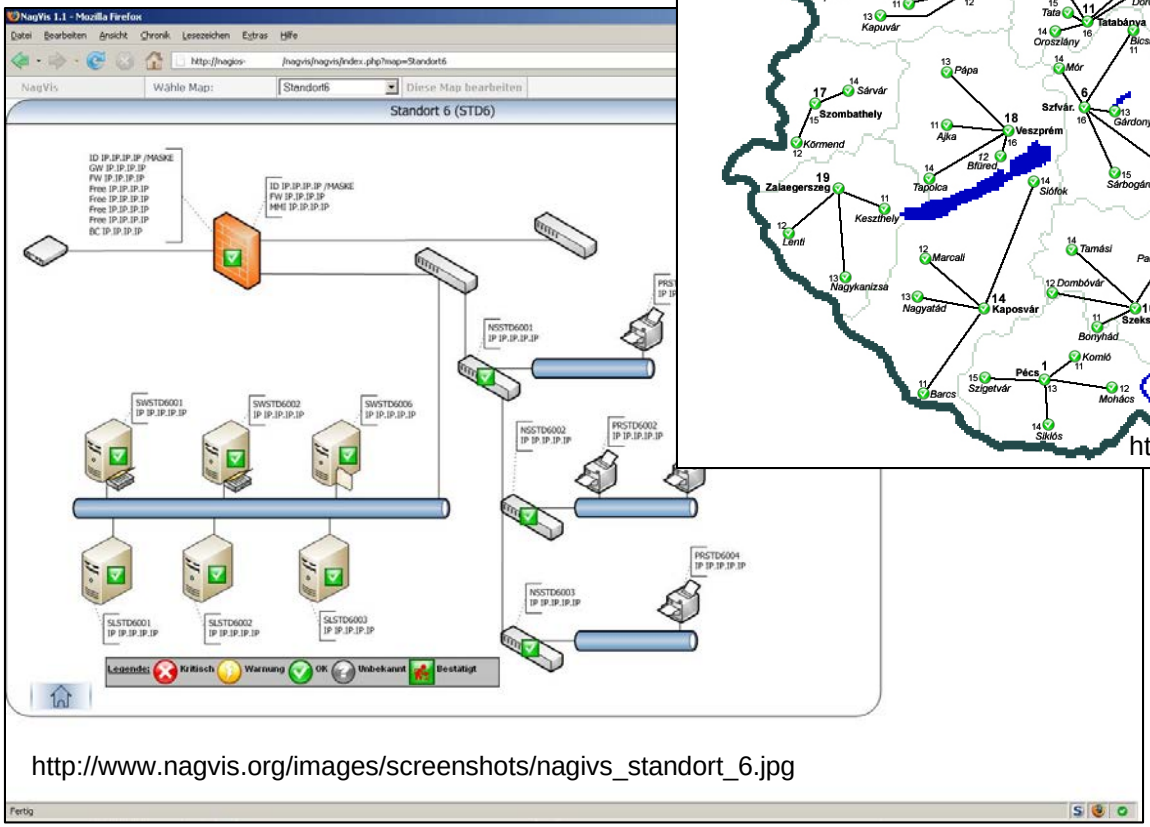
What is actionable?

- Initial Obstacles
  - False Positives
  - Information Overload
  - Information Relevance
- Cyber Response Actions…
  - Block IP
  - Attack back?
- Non-Cyber Response Actions
  - Notify Law Enforcement
  - Initiate internal procedures (e.g. employee termination)

Why Nagios®?



http://www.nagvis.org/images/screenshots/nagvis_map_2.png

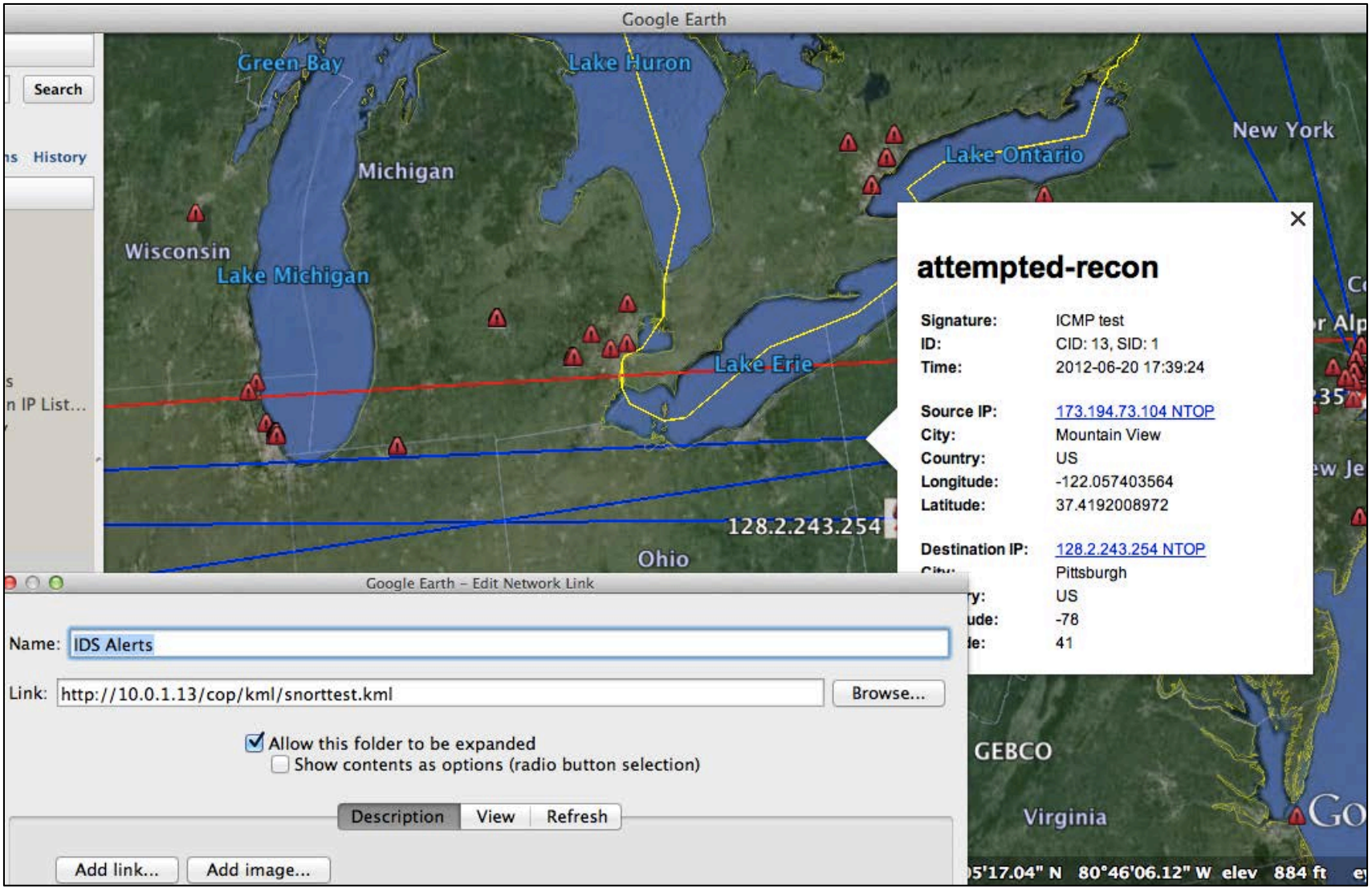


http://www.nagvis.org/images/screenshots/nagivs_standort_6.jpg

Why Google Earth?

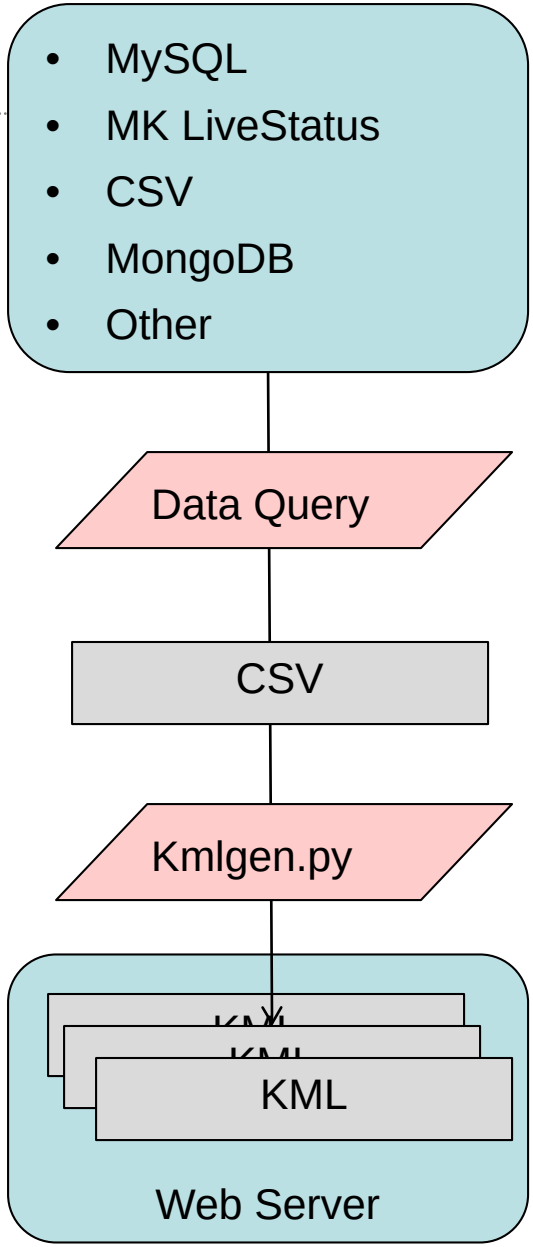
- Nagios wasn’t quite enough
- Wanted a better form of Geolocation
- No need to develop something new
- Numerous features
- Can also be use in a closed environment
- It’s cool, and people like cool

Google Earth Demo



How did we get there?

- Incorporated multiple data sources
  - Snort (Snorby on Security Onion)
  - Nagios
  - SharePoint RSS
  - Flow
  - Others
- Leverage standard data formats
  - Keyhole Markup Language (KML)
- Custom code
  - Linux Bash and Python scripts
  - KMLGEN python toolset



Lessons learned

- People like sizzle
- A COP is different things to different people
  - High Level – Senior Leader
  - Medium Level – Correlation and initial filtering
  - Low Level – Detailed Analysis capability
- Someone needs to “Own” the COP
  - Need to continuously validate feed Integrity
  - Need to assess value and customize
  - Need to ensure timely updates (e.g. maps, diagrams, TTP)
- Easier when you control all of the data
- Value of “Intelligence” may be higher than cyber monitoring data
- Google Earth, maps, and similar tools are useful for Geo-coordination

Other Geolocation samples

- CertCC Blog, GeoIP in your SOC
  - http://www.cert.org/blogs/certcc/2013/04/geoip_in_your_soc_security_ope.html
- GE Examples from Texas A&M
  - http://ticc.tamu.edu/Home/GECop.htm
  - http://tfsfrp.tamu.edu/Earth/Layers/TexasCOP.kmz
- KML Tutorial
  - https://developers.google.com/kml/documentation/kml_tut
- Sample Geolocated Intelligence feed
  - https://cts.allenvanguard.com
- Twitter Geolocation
  - http://trendsmap.com
- Geographical representation of intrusion events
  - http://leonward.wordpress.com/2009/03/15/geographic-representation-of-intrusion-events/
- More Nagios
  - http://exchange.nagios.org/directory/Addons/Maps-and-Diagrams/nagmap/details

Questions?