



# Global Situational Awareness with Free Tools

**Dennis M. Allen**  
**CERT/SEI/CMU**



## Report Documentation Page

*Form Approved  
OMB No. 0704-0188*

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE <b>15 JAN 2015</b>	2. REPORT TYPE <b>N/A</b>	3. DATES COVERED			
4. TITLE AND SUBTITLE <b>Global Situational Awareness with Free Tools</b>		5a. CONTRACT NUMBER			
		5b. GRANT NUMBER			
		5c. PROGRAM ELEMENT NUMBER			
6. AUTHOR(S) <b>Allen /Dennis</b>		5d. PROJECT NUMBER			
		5e. TASK NUMBER			
		5f. WORK UNIT NUMBER			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213</b>		8. PERFORMING ORGANIZATION REPORT NUMBER			
		10. SPONSOR/MONITOR'S ACRONYM(S)			
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		11. SPONSOR/MONITOR'S REPORT NUMBER(S)			
		12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release, distribution unlimited.</b>			
13. SUPPLEMENTARY NOTES <b>The original document contains color images.</b>					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>SAR</b>	18. NUMBER OF PAGES <b>18</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

# 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.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Defense.

**NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.**

This material has been approved for public release and unlimited distribution except as restricted below.

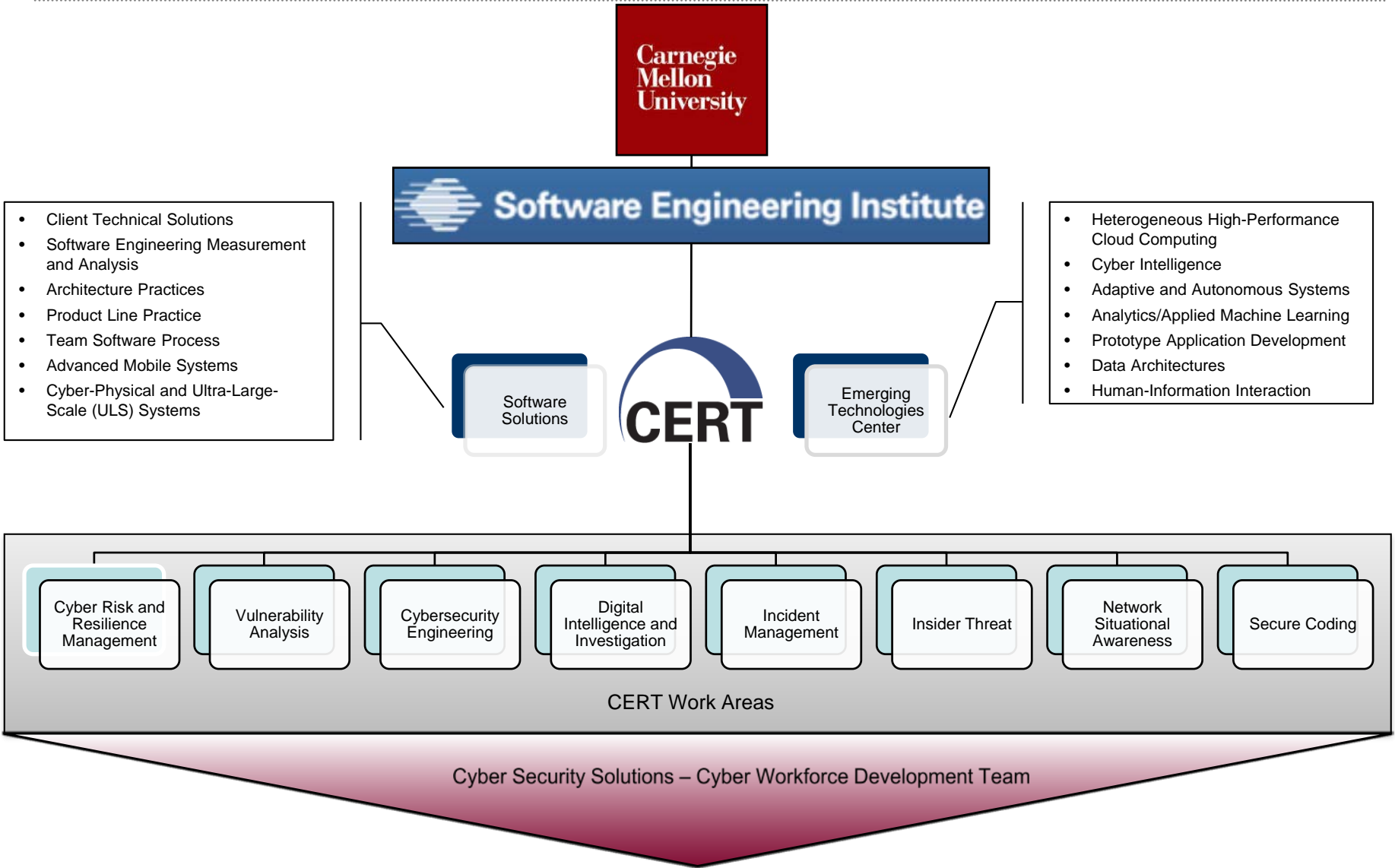
This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

Carnegie Mellon® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

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_(American_football))
- [http://en.wikipedia.org/wiki/Dennis\\_Allen\\_\(criminal\)](http://en.wikipedia.org/wiki/Dennis_Allen_(criminal))
- [www.dennisallen.com](http://www.dennisallen.com)

- Me

- [www.linkedin.com/pub/dennis-allen-cissp/4/972/a70](http://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](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](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?

---

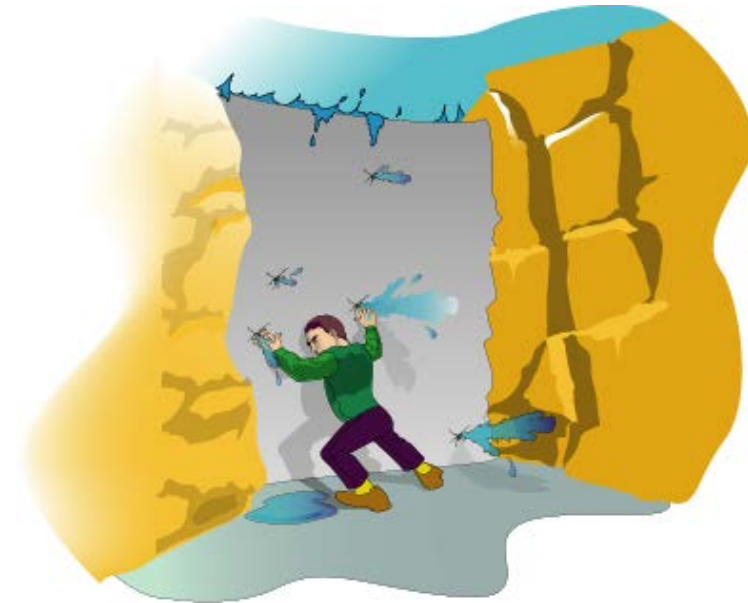
- Confidentiality
  - Data Loss Prevention (DLP)
- Integrity
  - File Integrity Monitoring (e.g. Tripwire)
  - Maybe performance monitoring (e.g. SNMP, MRTG)
- Availability
  - Easier to monitor (e.g. Nagios)
- Authentication/Authorization
  - Important, but often overlooked
  - Log management (e.g. 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\_standort\_6.jpg

Bérelt vonalak az országban

✓ VI-Pecs	✓ VI-Laborok	✓ VI-Starjan
✓ VI-Bekescsaba	✓ VI-Eger	✓ VI-Miskolc
✓ VI-Szeged	✓ VI-Tatabánya	✓ VI-Nyirehaza
✓ VI-Szfvár	✓ VI-Veszprem	
✓ VI-Gyor		
✓ VI-Debrecen		

http://www.nagvis.org/images/screenshots/nagvis\_map\_2.png

# 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

The screenshot shows a Google Earth interface with a map of the Great Lakes region. Several red triangle markers are scattered across the map, representing network links. A yellow line highlights a specific path across the lakes. A red line is also visible, labeled with the IP address 128.2.243.254. A popup window titled 'attempted-recon' provides details for a specific event:

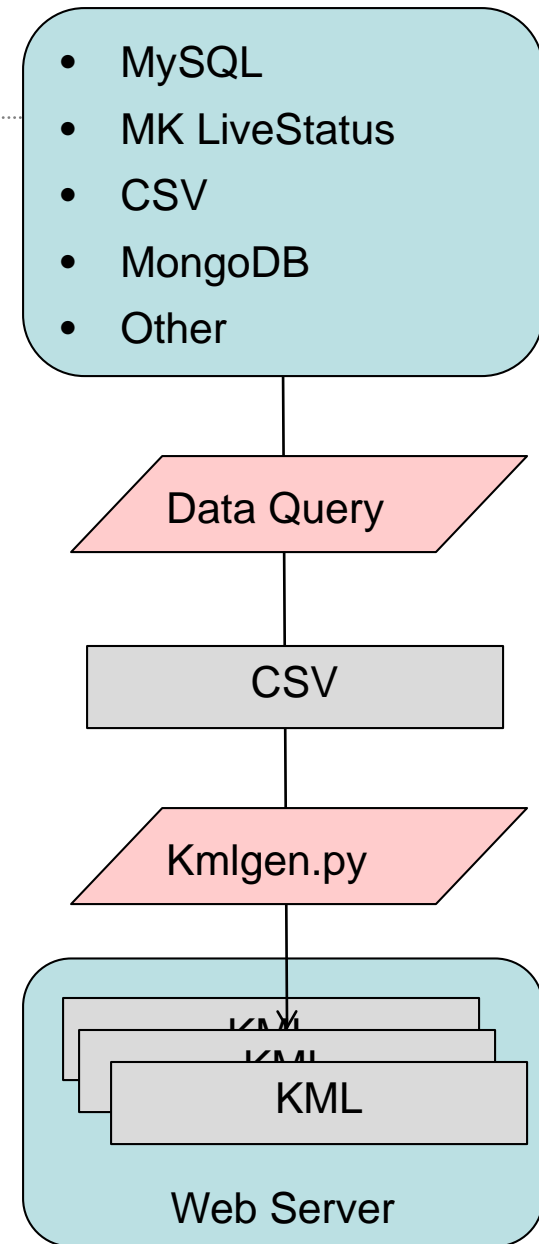
Field	Value
Signature:	ICMP test
ID:	CID: 13, SID: 1
Time:	2012-06-20 17:39:24
Source IP:	<a href="#">173.194.73.104</a> NTOP
City:	Mountain View
Country:	US
Longitude:	-122.057403564
Latitude:	37.4192008972
Destination IP:	<a href="#">128.2.243.254</a> NTOP
City:	Pittsburgh
Country:	US
Longitude:	-78
Latitude:	41

In the foreground, a 'Google Earth - Edit Network Link' dialog box is open. It contains the following information:

- Name:
- Link:
- Allow this folder to be expanded
- Show contents as options (radio button selection)
- Buttons: Description, View, Refresh
- Buttons: Add link..., Add image...

# 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, GeolP in your SOC
  - [http://www.cert.org/blogs/certcc/2013/04/geoip\\_in\\_your\\_soc\\_security\\_op.html](http://www.cert.org/blogs/certcc/2013/04/geoip_in_your_soc_security_op.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](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?

---

