Global Situational Awareness with Free Tools

Dennis M. Allen
CERT/SEI/CMU
1. REPORT DATE
15 JAN 2015

2. REPORT TYPE
N/A

3. DATES COVERED

4. TITLE AND SUBTITLE
Global Situational Awareness with Free Tools

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

6. AUTHOR(S)
Allen / Dennis

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213

8. PERFORMING ORGANIZATION REPORT NUMBER

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:
   a. REPORT
      unclassified
   b. ABSTRACT
      unclassified
   c. THIS PAGE
      unclassified

17. LIMITATION OF ABSTRACT
   SAR

18. NUMBER OF PAGES
   18

19a. NAME OF RESPONSIBLE PERSON

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18
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.


DM-0002094
Who We Are

CERT Work Areas

- Cyber Risk and Resilience Management
- Vulnerability Analysis
- Cybersecurity Engineering
- Digital Intelligence and Investigation
- Incident Management
- Insider Threat
- Network Situational Awareness
- Secure Coding

Cyber Security Solutions – Cyber Workforce Development Team

- Heterogeneous High-Performance Cloud Computing
- Cyber Intelligence
- Adaptive and Autonomous Systems
- Analytics/Applied Machine Learning
- Prototype Application Development
- Data Architectures
- Human-Information Interaction

© 2015 Carnegie Mellon University
Me – Not Me

- Not Me
  - 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

Bérelt vonalak az országban

- VI-Pécs
- VI-Békéscsaba
- VI-Szeged
- VI-Székesfehérvár
- VI-Győr
- VI-Debrecen
- VI-Staraj
- VI-Laborok
- VI-Eger
- VI-Miskolc
- VI-Nyíregyháza
- VI-Veszprém


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

Network Traffic Analysis

attempted-recon

Signature: ICMP test
ID: CID: 13, SID: 1
Time: 2012-08-20 17:39:24

Source IP: 173.194.73.104 NTOP
City: Mountain View
Country: US
Longitude: -122.05740356
Latitude: 37.41920089

Destination IP: 128.2.243.254 NTOP
City: Pittsburgh
Country: US
Longitude: -78
Latitude: 41

Name: IDS Alerts
Link: http://10.0.1.13/cop/kml/snorttest.kml

Allow this folder to be expanded
Show contents as options (radio button selection)
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

Data Query

MySQL
MK LiveStatus
CSV
MongoDB
Other

Kmlgen.py

CSV

KML

Web Server
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

- GE Examples from Texas A&M
  - [http://ticc.tamu.edu/Home/GECop.htm](http://ticc.tamu.edu/Home/GECop.htm)
  - [http://tfsfrp.tamu.edu/Earth/Layers/TexasCOP.kmz](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](https://cts.allenvanguard.com)

- Twitter Geolocation
  - [http://trendsmap.com](http://trendsmap.com)

- Geographical representation of intrusion events

- More Nagios
Questions?