EnergySec
SECURING CRITICAL INFRASTRUCTURE

Network Threat Hunting
Part 1: Visibility

EnergySec Webinar
March 30, 2017

Presented By:
Mike Meason and Trae Norman
Deep 6 Security, LLC

Network Threat Hunting

Visibility: Part 1 of 3

Network Threat Hunting

- Visibility
- Analysis
- Success

Intro

Michael Meason – Deep 6 Security, LLC

- Areas of Influence
  - Telecommunications Engineering
  - Network Engineering
  - Cyber Security Operations
- Letters
  - BS in CIS, MS in Telecomm., CISSP, CSFI-DCOE, NSTISSI 4011,4015, CNSSI 4012-4016, Certified Cyber Intel Tradecraft Professional
- Others
  - Husband/Father, KG5DQA, Aviation
- Handle
  - SigmetXray

Intro

Trae Norman – Deep 6 Security, LLC

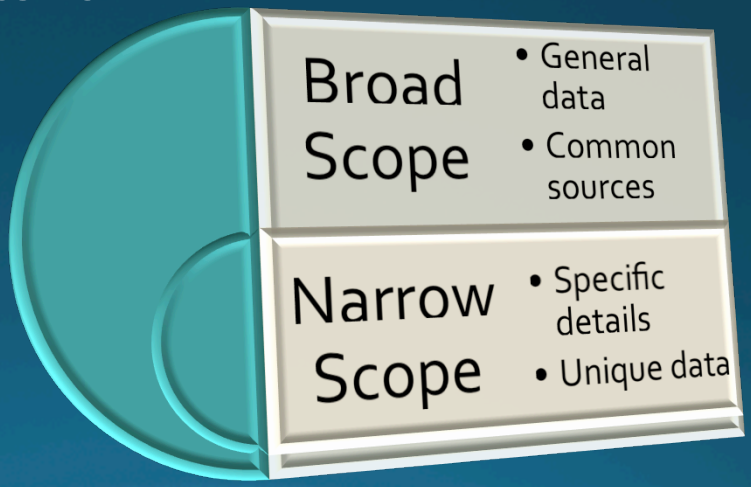
- Areas of Influence
  - Information Technology Administration and Engineering
  - Information Security
- Letters
  - CISSP, CEH, GCIA, GNFA, MCITP, MCSA, MCTS, BS in CIS
- Others
  - Husband/Father, Hobbyist Programmer
- Handle
  - SH

- Scope
- Identification
- Position
- Acquisition
- Operate
- Now What?

Scope

- *"The extent of the subject matter that something deals with or to which it is relevant."*

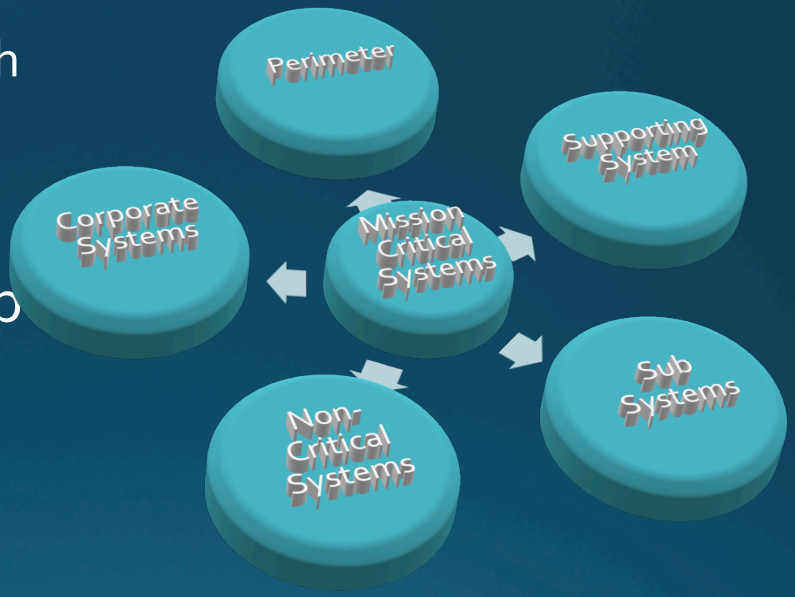
- Broad Scope
  - Most general, greater quantity
  - General knowledge of a lot of systems
  - Parse and filter are a must
  - NSA
- Narrow Scope
  - Most specific, less quantity
  - Focus on a particular aspect
  - Specialized knowledge needed
  - Seal Team 6



- Scope
- **Identification**
- Position
- Acquisition
- Operate
- Now What?

Identification

- Identify Critical Infrastructure
  - What are you trying to protect
  - Inside-Out vs Outside-In approach
- The Physical
  - Layer 1 (Wired and Wireless)
- Understand Gaps and Shore Up
  - Visibility Limitations
  - Overcome gaps



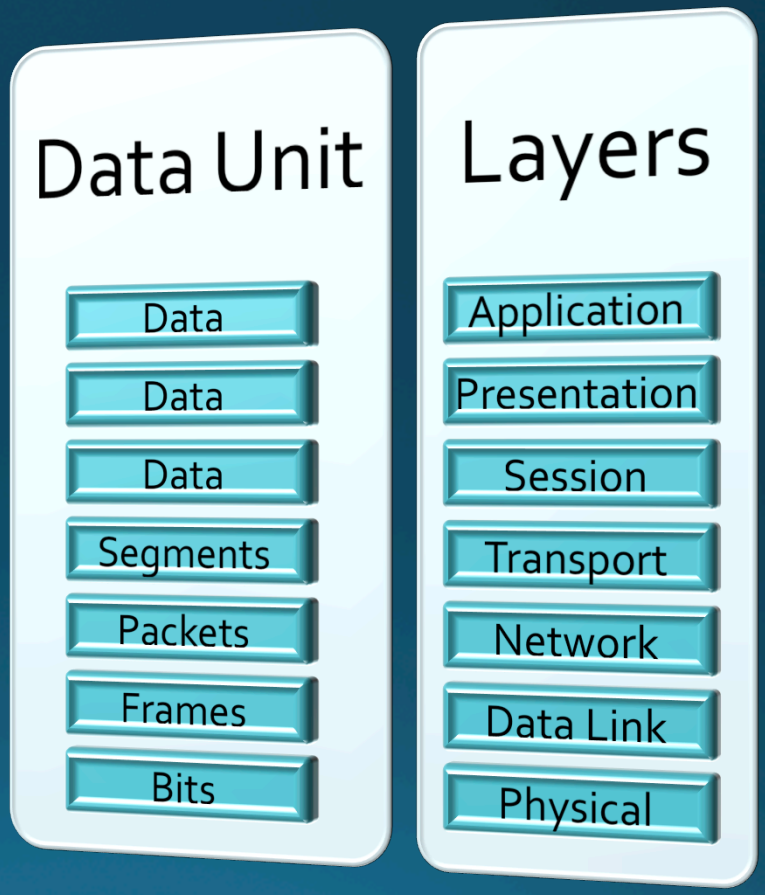
Identification Continued…

- Know What Systems Produce
  - Logging Levels
  - Formats
  - Windows / Linux / Appliance
  - Understand short comings
- Network and System Baselines
  - What is supposed to be on your network
  - Data flows
  - Allowed traffic across layer 3

- Scope
- Identification
- **Position**
- Acquisition
- Operate
- Now What?

Position

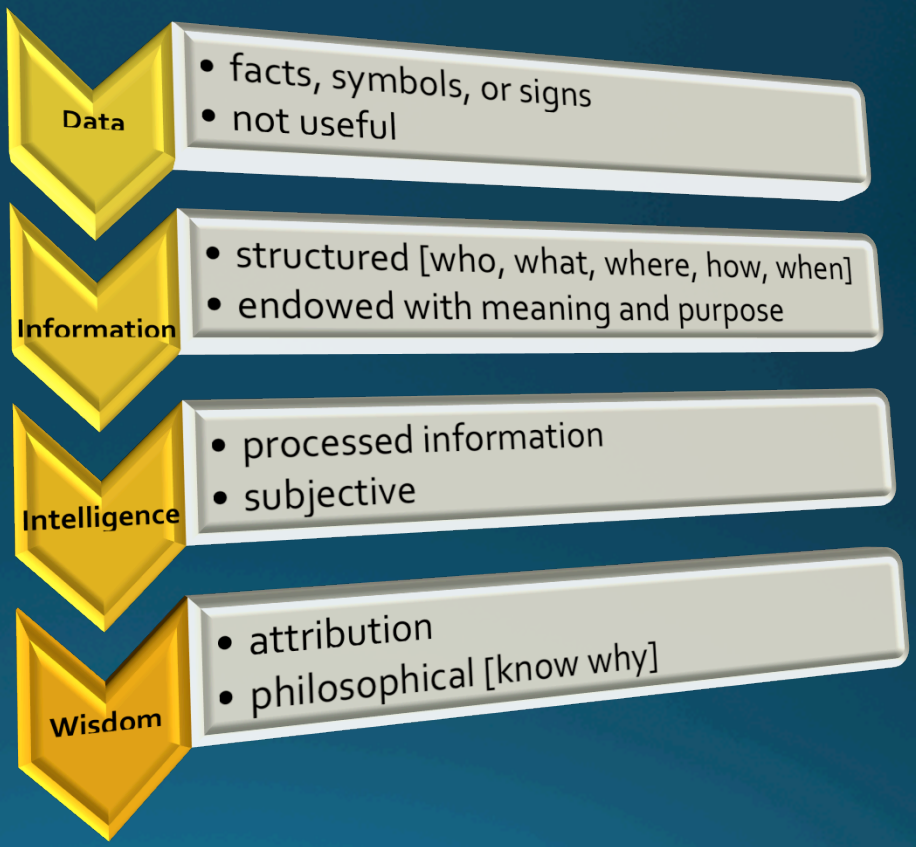
- Start Inside Work Out
  - Identify critical components and start there.
- All Layer 2/3 Traffic
  - L3 doesn't help with horizontal movement
  - Misconfigurations can be identified at L2
  - Persistence and footholds can be identified at L2
- Consider
  - Physical Topology
  - Placement of Data Acquisition Devices
  - Pre NAT Traffic –vs- Post NAT Traffic



- Scope
- Identification
- Position
- **Acquisition**
- Operate
- Now What?

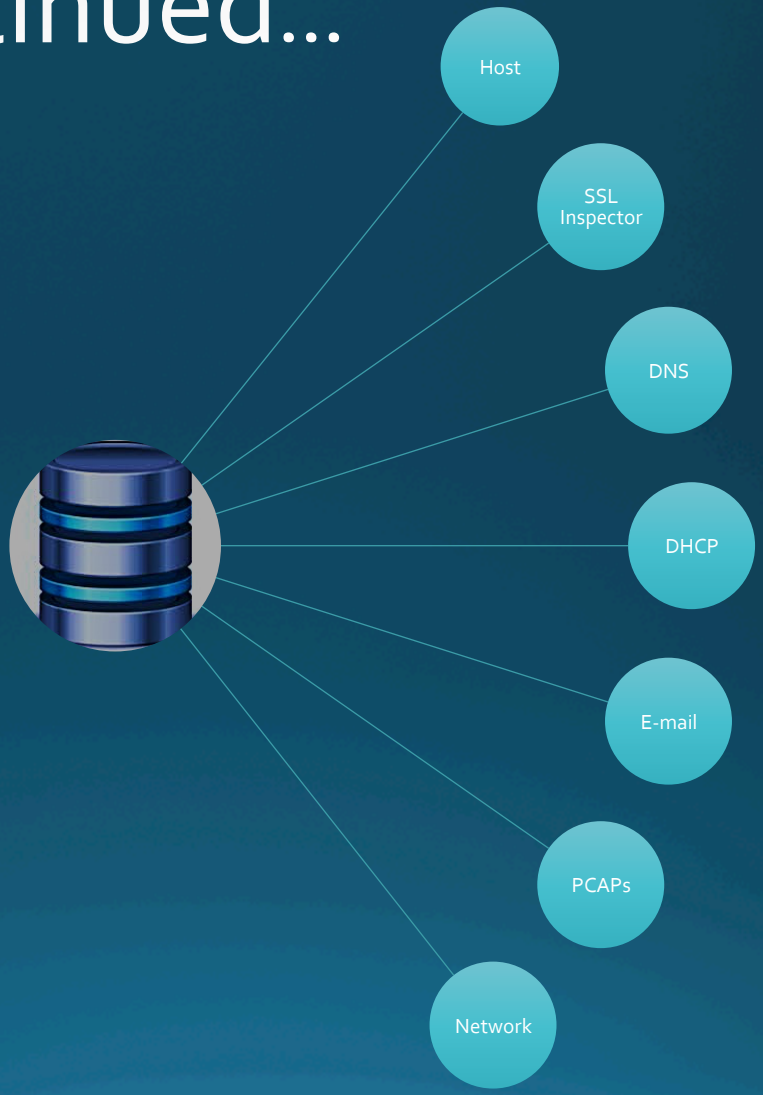
Acquisition

- What do I need?
  - Layer 2/3 Access
  - Understand Physical/Logical
  - Packet Capturing Tools
  - Log Receiver



Acquisition Continued…

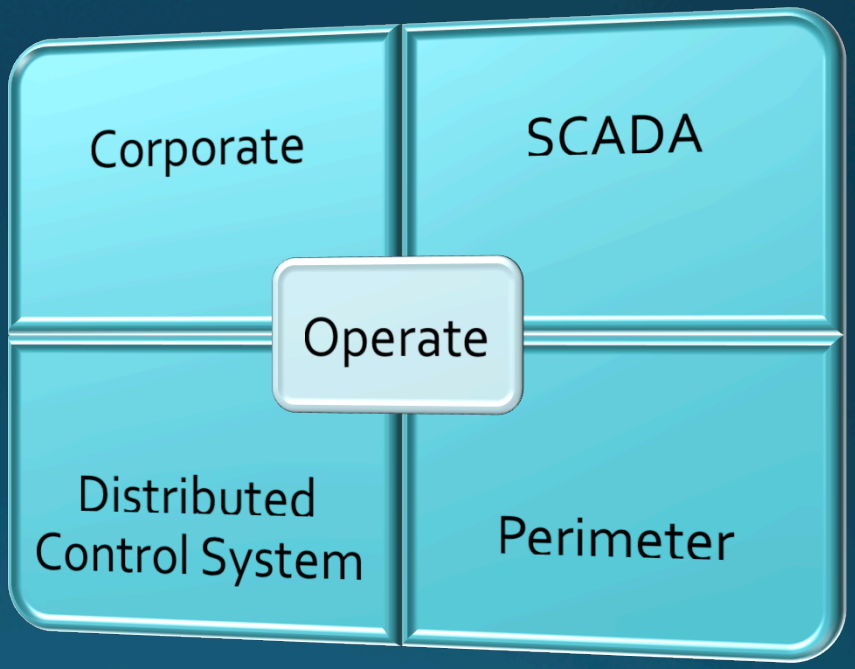
- How To Acquire
  - Logs (of all kinds)
  - Packet Captures (full time)
  - Encrypted Traffic
  - Common Data Locations
  - Hardware Devices



- Scope
- Identification
- Position
- Acquisition
- **Operate**
- Now What?

Operate

- Look for commonalities across traffic
- What should be there and what shouldn't
- Expectations –VS- Reality
  - Baselines –VS Data
- Parsing Tools
- Filter Tools
- Gaps

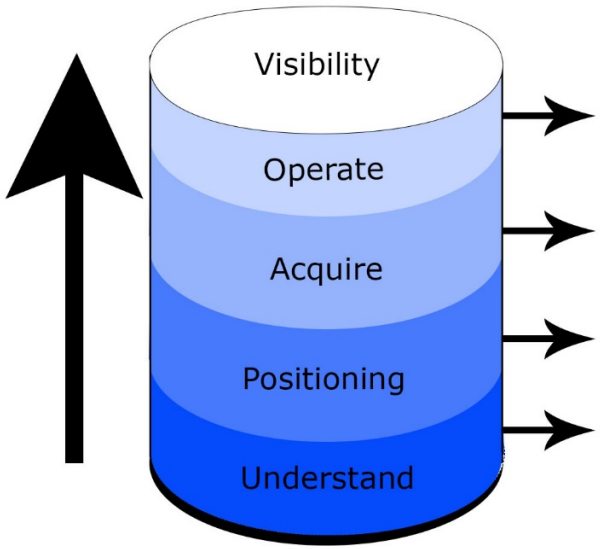


- Scope
- Identification
- Position
- Acquisition
- Operate
- **Now What?**

Now What?

- Dive into data
- Protocol Analysis
- Know what you don't know
- No one is an expert
- Help wanted

The Cylinder of Competence



Filter Data with Humans, At Scale, Apply Tools

PCAPS, SSL Inspection, All Logs

Pre/Post NAT, All L3 Boundaries, All L2 Traffic

Infrastructure, Protocols, Effects of Encryption, Baseline, Operating Systems, OS Event Sub-Systems, Networking

Questions?

mike@deep6cyber.com
trae@deep6cyber.com
Twitter - @deep6cyber.com

2017 Security Education Week

Austin, Texas -- May 15-19, 2017

time left: 46 days | 18 hrs | 06 min

Home | Agenda | Session Details | 2017 Instructors | Venue | Contact Us | Register!

Session Details

Introduction to Network Threat Hunting for Utilities (8 hours)

Mike Meason, Deep 6 Security, LLC

This session will instruct students on theoretical and practical concepts which facilitate the creation of network threat hunting operations in utilities. The concepts will be provided as a foundational approach to ensure that all audience members attain knowledge required to begin threat hunting operations no matter the maturity level of their current operations. This course will address prerequisites required as well as more in-depth technical approaches to threat hunting based on the day-to-day experience of utility security operations.

http://security-education-week.energysec.org/registration/